Bitdefender®

GravityZone

GHIDUL ADMINISTRATORULUI

Bitdefender GravityZone
Ghidul administratorului

Publicat 2021.01.13

Copyright© 2021 Bitdefender

Termeni legali

Toate drepturile rezervate. Nicio parte a acestui document nu va putea fi reprodusă sau transmisă sub nicio formă și prin niciun mijloc, fie el electronic sau mecanic, inclusiv fotocopiere, înregistrare, sau orice sistem de stocare și recuperare de date, fără acordul scris al unui reprezentant autorizat al Bitdefender. Este posibilă includerea unor scurte citate în recenzii, dar numai cu condiția menționării sursei citate. Conținutul documentului nu poate fi modificat în niciun fel.

Avertisment și declinarea responsabilității. Acest produs și documentația aferentă sunt protejate de legea drepturilor de autor. Informațiile incluse în acest document sunt furnizate „ca atare", fără nicio garanție. Deși s-au luat toate măsurile de prevedere în momentul alcătuirii acestui document, autorii săi nu vor fi în niciun fel ținuți responsabili față de nici o persoană fizică sau juridică pentru pierderi sau daune cauzate sau care se presupune a fi fost cauzate, direct sau indirect, de informațiile cuprinse în acest material.

Acest document conține linkuri către siteuri web aparținând unor terți, care nu se află sub controlul Bitdefender; prin urmare, Bitdefendernu este responsabilă pentru conținutul respectivelor siteuri. Responsabilitatea accesării oricăruia dintre siteurile terților al căror link este furnizat în acest document vă aparține în totalitate. Bitdefender furnizează aceste linkuri exclusiv pentru ușurarea consultării documentului și prezența lor nu presupune faptul că Bitdefender susține sau își asumă responsabilitatea pentru conținutul siteurilor către care duc acestea.

Mărci înregistrate. Acest document poate conține nume de mărci înregistrate. Toate mărcile comerciale înregistrate sau neînregistrate din acest document aparțin exclusiv proprietarilor acestora și sunt redate ca atare.

Cuprins

Prefață ... ix
1. Convenții utilizate în ghid ... ix
1. Despre GravityZone ... 1
2. Straturi de protecție GravityZone ... 2
2.1. Antimalware ... 2
2.2. Advanced Threat Control ... 4
2.3. HyperDetect ... 4
2.4. Anti-Exploit avansat ... 4
2.5. Firewall ... 5
2.6. Content Control ... 5
2.7. Network Attack Defense ... 5
2.8. Administrarea patch-urilor ... 5
2.9. Device Control ... 6
2.10. Full Disk Encryption ... 6
2.11. Security for Exchange ... 6
2.12. Application Control ... 7
2.13. Sandbox Analyzer ... 7
2.14. Incidente ... 7
2.15. Hypervisor Memory Introspection (HVI) ... 8
2.16. Network Traffic Security Analytics (NTSA) ... 9
2.17. Security for Storage ... 9
2.18. Security for Mobile ... 10
2.19. Disponibilitatea straturilor de protecție GravityZone ... 10
3. Arhitectura GravityZone ... 11
3.1. VA GravityZone ... 11
3.1.1. Baza de date GravityZone ... 11
3.1.2. Server de actualizări GravityZone ... 12
3.1.3. Serverul de comunicații GravityZone ... 12
3.1.4. Serverul de incidente GravityZone ... 12
3.1.5. Consola web (GravityZone Control Center) ... 12
3.2. Security Server ... 12
3.3. Pachet suplimentar HVI ... 13
3.4. Agenți de securitate ... 13
3.4.1. Bitdefender Endpoint Security Tools ... 13
3.4.2. Endpoint Security for Mac ... 16
3.4.3. GravityZone Mobile Client ... 16
3.4.4. Bitdefender Tools (vShield) ... 17
3.5. Architectura Sandbox Analyzer ... 17
4. Introducere ... 19
4.1. Conectarea la Control Center ... 19
4.2. Control Center dintr-o privire ... 20
4.2.1. Vedere de ansamblu asupra Control Center ... 20
4.2.2. Date tabelare ... 22

4.2.3. Bare de instrumente pentru acțiuni . . . 23
4.2.4. Meniul contextual . . . 24
4.2.5. Selector vederi . . . 24
4.3. Administrarea contului dumneavoastră . . . 25
4.4. Schimbarea parolei de conectare . . . 28

5. Conturile de utilizator . . . 29
5.1. Roluri de utilizator . . . 30
5.2. Drepturile de utilizare . . . 31
5.3. Administrarea conturilor de utilizator . . . 32
5.3.1. Administrarea individuală a conturilor de utilizator . . . 32
5.3.2. Administrarea mai multor conturi de utilizator . . . 35
5.4. Resetarea parolelor de conectare . . . 39
5.5. Administrarea autentificării de tip „two-factor” . . . 40

6. Administrarea obiectelor din rețea . . . 42
6.1. Lucrul cu Ecranele de rețea . . . 44
6.1.1. Calculatoare și mașini virtuale . . . 44
6.1.2. Mașini virtuale . . . 45
6.1.3. Dispozitive mobile . . . 46
6.2. Calculatoare . . . 47
6.2.1. Verificarea Stării calculatoarelor . . . 47
6.2.2. Vizualizarea detaliilor calculatorului . . . 50
6.2.3. Organizarea calculatoarelor în grupuri . . . 64
6.2.4. Sortarea, filtrarea și căutarea calculatoarelor . . . 66
6.2.5. Executarea sarcinilor . . . 70
6.2.6. Crearea de rapoarte rapide . . . 104
6.2.7. Atribuirea unei politici . . . 105
6.2.8. . . . 106
6.2.9. Sincronizarea cu Active Directory . . . 107
6.3. Mașini virtuale . . . 107
6.3.1. Verificarea Stării Mașinilor Virtuale . . . 109
6.3.2. Vizualizarea detaliilor Mașinii virtuale . . . 112
6.3.3. Organizarea mașinilor virtuale în grupuri . . . 120
6.3.4. Sortarea, filtrarea și căutarea Mașinilor Virtuale . . . 122
6.3.5. Executarea sarcinilor pe mașinile virtuale . . . 127
6.3.6. Crearea de rapoarte rapide . . . 163
6.3.7. Atribuirea unei politici . . . 164
6.3.8. Utilizarea Managerului de recuperare pentru volumele criptate . . . 165
6.3.9. Ștergere licențe de utilizator . . . 166
6.4. Dispozitive mobile . . . 167
6.4.1. Adăugarea utilizatorilor personalizați . . . 168
6.4.2. Adăugarea dispozitivelor mobile utilizatorilor . . . 169
6.4.3. Organizarea utilizatorilor personalizați în grupuri . . . 172
6.4.4. Verificarea Stării Dispozitivelor Mobile . . . 174
6.4.5. Dispozitive mobile conforme și neconforme . . . 175
6.4.6. Verificarea detaliilor utilizatorului și dispozitivelor mobile . . . 176
6.4.7. Sortarea, filtrarea și căutarea dispozitivelor mobile . . . 180
6.4.8. Executarea sarcinilor pe dispozitive mobile . . . 184

6.4.9. Crearea de rapoarte rapide . . . 189
6.4.10. Atribuirea unei politici . . . 190
6.4.11. Sincronizarea cu Active Directory . . . 191
6.4.12. Ștergerea utilizatorilor și dispozitivelor mobile . . . 191
6.5. Inventar aplicații . . . 193
6.6. Inventarul de patch-uri . . . 199
6.6.1. Vizualizarea detaliilor patch-urilor . . . 200
6.6.2. Căutarea și filtrarea patch-urilor . . . 201
6.6.3. Ignorare patch-uri . . . 202
6.6.4. Instalarea patch-urilor . . . 203
6.6.5. Dezinstalarea patch-urilor . . . 205
6.6.6. Crearea statisticilor referitoare la patch-uri . . . 207
6.7. Vizualizarea și administrarea sarcinilor . . . 207
6.7.1. Verificarea stării sarcinii . . . 208
6.7.2. Vizualizarea rapoartelor referitoare la sarcină . . . 210
6.7.3. Repornire sarcini . . . 210
6.7.4. Se opresc sarcinile de scanare Exchange . . . 211
6.7.5. Ștergerea unei sarcini . . . 211
6.8. Ștergerea stațiilor de lucru din inventarul rețelei . . . 212
6.9. Configurarea setărilor de rețea . . . 213
6.9.1. Setări inventar de rețea . . . 213
6.9.2. Ștergere mașini offline . . . 214
6.10. Configurarea setărilor Security Server . . . 216
6.11. Manager Credențiale . . . 217
6.11.1. Sistem de operare . . . 217
6.11.2. Mediul virtualizat . . . 218
6.11.3. Ștergerea datelor din fereastra Administrare Date de Autentificare . . . 219

7. Politici de securitate . . . 220
7.1. Administrarea politicilor . . . 221
7.1.1. Crearea politicilor . . . 222
7.1.2. Atribuirea unei politici . . . 223
7.1.3. Modificarea setărilor politicii . . . 234
7.1.4. Redenumirea politicilor . . . 234
7.1.5. Ștergerea politicilor . . . 235
7.2. Politici referitoare la calculatoare și mașini virtuale . . . 235
7.2.1. General . . . 236
7.2.2. HVI . . . 251
7.2.3. Antimalware . . . 260
7.2.4. Sandbox Analyzer . . . 299
7.2.5. Firewall . . . 307
7.2.6. Protecție rețea . . . 321
7.2.7. Administrarea patch-urilor . . . 336
7.2.8. Application Control . . . 339
7.2.9. Device Control . . . 345
7.2.10. Relay . . . 350
7.2.11. Protecție Exchange . . . 352
7.2.12. Criptare . . . 383
7.2.13. NSX . . . 387

7.2.14. Protecție spațiu de stocare . . . 388
7.2.15. Senzor de incidente . . . 392
7.3. Politici pentru dispozitive mobile . . . 392
7.3.1. General . . . 393
7.3.2. Managementul dispozitivului . . . 394

8. Panoul de monitorizare . . . 415
8.1. Panou de bord . . . 415
8.1.1. Reîmprospătarea datelelor de portlet . . . 416
8.1.2. Editarea setărilor Portlet . . . 416
8.1.3. Adăugarea unui portlet nou . . . 417
8.1.4. Ștergerea unui portlet . . . 417
8.1.5. Rearanjarea portlet-urilor . . . 417

9. Investigarea Incidentelor . . . 418
9.1. Pagina Incidente . . . 418
9.1.1. Tabelul filtrelor . . . 420
9.1.2. Vizualizarea Listei evenimentelor de securitate . . . 422
9.1.3. Revizuirea unei amenințări detectate . . . 427
9.2. Fișiere în lista de blocare . . . 471

10. Utilizarea rapoartelor . . . 475
10.1. Tipuri de rapoarte . . . 475
10.1.1. Rapoarte referitoare la calculatoare și mașini virtuale . . . 476
10.1.2. Rapoarte Servere Exchange . . . 490
10.1.3. Rapoarte privind dispozitivele mobile . . . 493
10.2. Crearea rapoartelor . . . 495
10.3. Vizualizarea și gestionarea rapoartelor programate . . . 499
10.3.1. Vizualizarea rapoartelor . . . 499
10.3.2. Editarea unui raport programat . . . 500
10.3.3. Ștergerea unui raport programat . . . 502
10.4. Implementarea măsurilor bazate pe raport . . . 502
10.5. Salvarea rapoartelor . . . 503
10.5.1. Exportarea rapoartelor . . . 503
10.5.2. Descărcarea rapoartelor . . . 503
10.6. Transmiterea prin e-mail a rapoartelor . . . 504
10.7. Printarea rapoartelor . . . 504

11. Carantină . . . 505
11.1. Explorarea Carantinei . . . 505
11.2. Carantină calculatoare și mașini virtuale . . . 506
11.2.1. Vizualizarea Detaliilor carantinei . . . 506
11.2.2. Gestionarea fișierelor aflate în carantină . . . 507
11.3. Carantină Servere Exchange . . . 511
11.3.1. Vizualizarea Detaliilor carantinei . . . 512
11.3.2. Obiecte mutate în carantină . . . 514

12. Utilizarea Sandbox Analyzer . . . 518
12.1. Filtrarea înregistrărilor trimiterilor . . . 519
12.2. Vizualizarea detaliilor analizei . . . 520

12.3. Retrimiterea mostrelor . . . 522
12.4. Ștergerea înregistrărilor trimiterilor . . . 523
12.5. Transmitere manuală . . . 524
12.6. Administrarea infrastructurii Sandbox Analyzer . . . 526
12.6.1. Verificarea stării Sandbox Analyzer . . . 526
12.6.2. Configurarea detonărilor simultane . . . 528
12.6.3. Verificarea stării imaginilor de mașină virtuală . . . 528
12.6.4. Configurarea și administrarea imaginilor de mașină virtuală . . . 529

13. Jurnalul activității utilizatorului . . . 531

14. Utilizarea Instrumentelor . . . 533
14.1. Injectare instrumente personalizate cu HVI . . . 533

15. Notificări . . . 535
15.1. Tipuri de notificări . . . 535
15.2. Vizualizarea notificărilor . . . 544
15.3. Ștergerea notificărilor . . . 545
15.4. Configurarea setărilor de notificare . . . 546

16. Stare sistem . . . 549
16.1. Stare OK . . . 549
16.2. Stare Atenție! . . . 550
16.3. Metrică . . . 550

17. Obținere ajutor . . . 554
17.1. Centrul de asistență Bitdefender . . . 554
17.2. Solicitarea de asistență profesională . . . 555
17.3. Utilizarea Modulului de Suport Tehnic . . . 555
17.3.1. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Windows . . . 556
17.3.2. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Linux . . . 557
17.3.3. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Mac . . . 559
17.4. Informații de contact . . . 560
17.4.1. Adrese Web . . . 560
17.4.2. Distribuitori locali . . . 561
17.4.3. Filialele Bitdefender . . . 561

A. Anexe . . . 564
A.1. Tipuri de fișiere acceptate . . . 564
A.2. Tipurile și stările obiectelor de rețea . . . 565
A.2.1. Tipurile obiectelor de rețea . . . 565
A.2.2. Stările obiectelor din rețea . . . 566
A.3. Tipuri de fișiere de aplicații . . . 567
A.4. Tipuri de fișiere pentru filtrarea atașamentelor . . . 568
A.5. Variabile de sistem . . . 569
A.6. Instrumente Control aplicații . . . 570
A.7. Obiecte Sandbox Analyzer . . . 571
A.7.1. Tipuri și extensii de fișiere acceptate pentru trimitere manuală . . . 571
A.7.2. Tipurile de fișiere acceptate de modulul de filtrare preliminară a conținutului la trimiterea automată . . . 572

A.7.3. Excluderi implicite la trimiterea automată 572
A.7.4. Aplicații recomandate pentru mașinile virtuale de detonare 572
A.8. Instrumente de procesare de date 573
Vocabular 576

Prefață

Acest ghid este destinat administratorilor de rețea responsabili pentru gestionarea protecției GravityZone la sediul organizației lor.

Scopul acestui document este acela de a explica modalitatea de aplicare și vizualizare a setărilor de securitate pe terminalele rețelei din contul personal, folosind GravityZone Control Center. Veți afla cum să vizualizați inventarul de rețea în Control Center, cum să creați și să aplicați politicile de administrare a stațiilor de lucru, cum să generați rapoarte, cum să administrați articolele trecute în carantină și cum să folosiți panoul de comandă.

1. Convenții utilizate în ghid

Convenții tipografice

Acest ghid folosește mai multe stiluri de text pentru o lizibilitate îmbunătățită. Aflați mai multe despre aspectul și însemnătatea acestora din tabelul de mai jos.

Aspect	Descriere
`mostră`	Numele de comenzi inline, sintaxele, căile și numele de fișiere, output-urile fișierelor de configurare și textele de intrare sunt tipărite cu caractere de tip `monospațiat`.
http://www.bitdefender.com	Linkurile URL indică locații externe, pe serverele http sau ftp.
gravityzone-docs@bitdefender.com	Adresele de e-mail sunt inserate în text ca informație de contact.
„Prefață” (p. ix)	Acesta este un link intern, către o locație din document.
opțiune	Toate opțiunile produsului sunt tipărite cu caractere **bold**.
cuvânt cheie	Opțiunile de interfață, cuvintele cheie sau scurtăturile sunt evidențiate cu ajutorul caracterelor **aldine**.

Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.

Notă
Nota nu este decât o scurtă observație. Deși pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect asemănător.

Important
Acest lucru necesită atenția dumneavoastră și nu este recomandat să-l ocoliți. De obicei, aici sunt furnizate informații importante, dar care nu sunt critice.

Avertisment
Este vorba de informații cruciale, cărora trebuie să le acordați o mare atenție. Dacă urmați indicațiile, nu se va întâmpla nimic rău. Este indicat să citiți și să înțelegeți despre ce este vorba, deoarece este descris ceva extrem de riscant.

1. DESPRE GRAVITYZONE

GravityZone este o soluție de securitate pentru companii, construită de la bun început pentru mediul de virtualizare și cloud pentru a oferi servicii de securitate pentru stațiile de lucru fizice, dispozitive mobile și mașinile virtuale din cloud-ul privat, public și serverele de e-mail Exchange.

GravityZone este un produs prevăzut cu o consolă de administrare unică, disponibilă în cloud, găzduită de Bitdefender, sau ca aplicație virtuală ce se instalează la sediul companiei și asigură un punct unic pentru configurarea, aplicarea și administrarea politicilor de securitate pentru un număr nelimitat de stații de lucru de orice tip, indiferent de locul în care se află.

GravityZone oferă mai multe niveluri de securitate pentru stațiile de lucru și pentru serverele de e-mail Microsoft Exchange: antimalware cu monitorizarea comportamentului, protecția contra amenințărilor în ziua zero, controlul aplicațiilor și sandboxing, firewall, controlul dispozitivelor, controlul conținutului, anti-phishing și antispam.

2. STRATURI DE PROTECȚIE GRAVITYZONE

GravityZone oferă următoarele straturi de protecție:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Anti-Exploit avansat
- Firewall
- Content Control
- Administrarea patch-urilor
- Device Control
- Full Disk Encryption
- Security for Exchange
- Application Control
- Sandbox Analyzer
- Soluție EDR (Endpoint Detection and Response)
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Antimalware

Nivelul de protecție antimalware se bazează pe scanarea semnăturilor și analiza euristică (B-HAVE, ATC) împotriva: virușilor, troienilor, atacurilor de tip worm, spyware, adware, keylogger, rootkit și alte tipuri de software periculos

Tehnologia de scanare antimalware a Bitdefender se bazează pe următoarele tehnologii:

- În primul rând, se folosește o metodă de scanare tradițională acolo unde conținutul se potrivește cu baza de date de semnături. Baza de date de semnături conține modele de bytes specifice amenințărilor cunoscute și este actualizată în mod regulat de Bitdefender. Această metodă de scanare este eficientă împotriva amenințărilor confirmate care au fost cercetate și documentate. Cu toate acestea, indiferent cât de prompt este actualizată baza de date, există întotdeauna o fereastră de vulnerabilitate între momentul când se descoperă o nouă amenințare și momentul lansării unei remedieri..

- Împotriva amenințărilor noi și nedocumentate, se asigură un al doilea strat de protecție de către **B-HAVE**, motorul euristic al Bitdefender. Algoritmii euristici detectează programele malware pe baza caracteristicilor comportamentale. B-HAVE execută fișierele suspecte într-un mediu virtual pentru a testa impactul acestora asupra sistemului și pentru a se asigura că nu prezintă o amenințare. Dacă se detectează o amenințare, se blochează executarea programului.

Motoare de scanare

Bitdefender GravityZone poate configura automat motoarele de scanare la crearea pachetelor de agenți de securitate, în funcție de configurația endpointului.

Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:

1. **Scanare locală**, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având conținutul de securitate stocat local.
2. **Scanarea hibrid cu motoare light (Cloud public)**, cu o amprentă medie, folosind scanarea în cloud și, parțial, conținut de securitate. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
3. **Scanarea centralizată în cloud-ul public sau privat**, cu o amprentă redusă care necesită un Security Server pentru scanare. În acest caz, nu se stochează local niciun conținut de securitate, iar scanarea este transferată către Security Server.

   Notă
   Există un set minim de motoare stocate local, care sunt necesare pentru despachetarea fișierelor arhivate.

4. **Scanare centralizată (cloud public sau privat cu Security Server) cu fallback* pe Scanare locală (motoare full)**
5. **Scanare centralizată (Scanare în cloud public sau privat cu Security Server) cu fallback* pe Scanare hibrid (cloud public cu motoare light)**

* Atunci când se folosește scanarea cu motoare duble, dacă primul motor este indisponibil, se va folosi motorul de rezervă (fallback). Consumul de resurse și gradul de utilizare a rețelei vor depinde de motoarele folosite.

2.2. Advanced Threat Control

Pentru amenințări care scapă chiar și de motorul euristic, este prezent un alt strat de protecție sub forma unei funcții Advanced Threat Control (ATC).

Advanced Threat Control monitorizează în mod continuu procesele în curs și cataloghează comportamentele suspecte, precum tentativele de: deghizare a tipului de proces, executare de cod în spațiul altui proces (furtul de memorie a procesului pentru escaladarea drepturilor), reproducerea, eliminarea fișierelor, ascunderea de aplicațiile de enumerare a proceselor etc. Fiecare comportament suspect duce la creșterea punctajului acordat proceselor. Atunci când se atinge un prag, se declanșează alarma.

2.3. HyperDetect

Bitdefender HyperDetect este un strat suplimentar de securitate conceput special pentru a detecta atacurile avansate și activitățile suspecte în faza de pre-execuție. HyperDetect conține modele de învățare automată (machine learning) și tehnologii de detectare a atacurilor ascunse pentru combaterea amenințărilor precum: atacuri de tip „zero-day”, amenințări persistente avansate (APT), malware ascuns, atacuri fără fișiere (utilizarea necorespunzătoare a PowerShell, Windows Management Instrumentation etc.), furtul de date de autentificare, atacuri targetate, malware personalizat, atacuri bazate pe scripturi, exploit-uri, instrumente de hacking, trafic suspect în rețea, aplicații potențial nedorite (PUA), ransomware.

2.4. Anti-Exploit avansat

Având la bază tehnologia de învățare automată (machine learning), tehnologia proactivă de Anti-Exploit Avansat oprește atacurile de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive. Modulul Anti-exploit avansat depistează în timp real cele mai recente exploit-uri și diminuează vulnerabilitățile de corupere a memoriei care pot trece nedetectate de către alte soluții de securitate. Protejează aplicațiile utilizate cel mai frecvent, cum ar fi browser-ele, Microsoft Office sau Adobe Reader, precum și alte aplicații la care vă puteți gândi. Veghează asupra proceselor de sistem și protejează împotriva breșelor de securitate și a furturilor din procesele existente.

2.5. Firewall

Firewall-ul controlează accesul aplicațiilor la rețea și internet. Accesul este permis automat pentru o bază de date cuprinzătoare de aplicații cunoscute și sigure. În plus, firewall-ul poate proteja sistemul împotriva scanărilor de porturi, poate restricționa ICS și poate emite avertizări atunci când la o conexiune Wi-Fi se adaugă noi noduri.

2.6. Content Control

Modulul de control al conținutului susține aplicarea politicilor companiei privind traficul permis, accesul la internet, protecția datelor și controlul aplicațiilor. Administratorii pot defini opțiunile de scanare a traficului și excepțiile, pot stabili un program pentru accesul la internet, blocând anumite categorii web sau URL-uri, pot configura regulile de protecție a datelor și pot defini drepturile pentru utilizarea anumitor aplicații.

2.7. Network Attack Defense

Modulul de protecție Network Attack Defense se bazează pe o tehnologie Bitdefender ce vizează detectarea atacurilor din rețea concepute pentru a obține acces la endpoint-uri folosind tehnici specifice, cum ar fi: atacuri de tip „brute force”, exploit-uri la nivel de rețea, furt de parole, vectori de infectare drive-by-download, bot-uri și troieni.

2.8. Administrarea patch-urilor

Complet integrat în GravityZone, Patch Management menține actualizate sistemele de operare și aplicațiile software și oferă o imagine completă asupra stării de aplicare a patch-urilor pe stațiile de lucru administrate, cu sistem de operare Windows.

Modulul GravityZone Patch Management include mai multe funcții, cum ar fi scanarea la cerere / programată a patch-urilor, instalarea automată / manuală a patch-urilor sau raportarea patch-urilor absente.

Puteți afla mai multe despre distribuitorii autorizați și produsele compatibile cu GravityZone Patch Management din acest articol KB.

Notă
Patch Management este un add-on disponibil cu cheie de licență separată pentru toate pachetele GravityZone.

2.9. Device Control

Modulul Control dispozitiv împiedică scurgerile de date confidențiale și infecțiile cu malware folosind dispozitive externe atașate endpoint-ului, prin aplicarea unor reguli și excepții de blocare prin intermediul politicilor, pentru o gamă largă de tipuri de dispozitive (cum ar fi unități de stocare flash USB, dispozitive Bluetooth, CD/DVD playere, dispozitive de stocare etc.).

2.10. Full Disk Encryption

Acest strat de protecție vă permite să asigurați caracteristica Full Disk Encryption pe endpoint-uri, gestionând funcția BitLocker pe Windows și funcțiile FileVault și diskutil pe macOS. Puteți cripta și decripta volume boot și non-boot, cu doar câteva clicuri, în timp ce GravityZone gestionează întregul proces, cu intervenție minimă din partea utilizatorilor. În plus, GravityZone stochează codurile de recuperare necesare pentru a debloca volumele atunci când utilizatorii își uită parolele.

Notă
Full Disk Encryption este un add-on disponibil cu o cheie de licență separată pentru toate pachetele GravityZone disponibile.

2.11. Security for Exchange

Bitdefender Security for Exchange asigură protecție antimalware, antispam, antiphising, filtrare a conținutului și a fișierelor atașate, toate acestea complet integrate cu server-ul Microsoft Exchange, pentru a asigura un mediu securizat de comunicare prin mesaje și o productivitate sporită. Folosind tehnologiile antimalware și antispam premiate, aceasta protejează utilizatorii Exchange împotriva celor mai noi și mai sofisticate programe malware, precum și împotriva tentativelor de furt al datelor confidențiale sau valoroase ale utilizatorilor.

Important
Security for Exchange este proiectat pentru a proteja întreaga organizație Exchange de care aparține serverul Exchange protejat. Aceasta înseamnă că protejează toate căsuțele de e-mail active, inclusiv căsuțele de e-mail de tip user (utilizator) / room (cameră)/ equipment (echipament) / shared (partajat).

În plus față de protecția Microsoft Exchange, licența acoperă și modulele de protecție pentru stații de lucru instalate pe server.

2.12. Application Control

Modulul Control aplicații previne atacurile malware și de tip „ziua zero” și sporește securitatea fără a avea un impact asupra productivității. Modulul Control aplicații pune în aplicare politici flexibile de trecere în lista albă de aplicații, care identifică și previn instalarea și executarea oricăror aplicații nedorite, nesigure sau periculoase.

2.13. Sandbox Analyzer

Bitdefender Sandbox Analyzer oferă un nivel puternic de securitate împotriva amenințărilor avansate prin efectuarea unei analize automate și detaliate a fișierelor suspecte care nu sunt încă semnate de motoarele antimalware ale Bitdefender. Sandbox-ul utilizează o serie de tehnologii Bitdefender pentru a executa payload-uri într-un mediu virtual închis găzduit de Bitdefender sau instalat la nivel local, pentru a analiza comportamentul acestora și raporta orice schimbări subtile aduse sistemului, care semnalează intenții periculoase.

Sandbox Analyzer utilizează o serie de senzori pentru a detona conținut din endpoint-uri administrate, fluxuri ale traficului de endpoint rețea, carantină centralizată și servere ICAP (Internet Content Adaptation Protocol).

În plus, Sandbox Analyzer permite trimiterea manuală a mostrelor și prin API.

Notă
Această funcționalitate a modulului poate fi furnizată de Sandbox Analyzer Cloud și Sandbox Analyzer On-Premises. Sandbox Analyzer On-Premises este disponibil cu o cheie de licență separată.

2.14. Incidente

Caracteristica Incidente este o componentă de corelare a evenimentelor, capabilă să identifice amenințările avansate sau atacurile în curs de desfășurare. Ca parte a platformei noastre complete și integrate de protecție pentru endpoint-uri, caracteristica Incidente reunește informațiile despre dispozitive din întreaga rețea a companiei dumneavoastră. Această soluție vine în ajutorul eforturilor echipelor dumneavoastră responsabile cu răspunsul la incidente pentru a investiga și a reacționa la amenințări avansate.

Prin intermediul Bitdefender Endpoint Security Tools, puteți activa un modul de protecție numit Senzor de incidente pe endpoint-urile administrate, pentru a aduna date despre hardware și sistemul de operare. Respectând un cadru de lucru client-server, metadatele sunt colectate și procesate de ambele părți.

Această componentă aduce informații detaliate cu privire la incidentele detectate, o hartă interactivă a incidentelor, acțiuni de remediere și integrare cu Sandbox Analyzer și HyperDetect.

2.15. Hypervisor Memory Introspection (HVI)

Este cunoscut faptul că hackerii foarte bine organizați și orientați către profit caută vulnerabilități necunoscute (vulnerabilități de tip ziua zero) sau utilizează tehnici de exploatare concepute special, pentru utilizare unică (exploatări de tip ziua zero) și alte instrumente. De asemenea, hackerii folosesc tehnici avansate pentru a întârzia și structura succesiv sarcinile de atac în vederea mascării activității periculoase. Atacurile mai noi, orientate către profit, sunt concepute pentru a nu fi detectate și pentru a învinge instrumentele de securitate tradiționale.

Pentru mediile virtualizate, problema este acum soluționată, HVI protejând centre de date cu o densitate mare de mașini virtuale împotriva amenințărilor avansate și sofisticate, pe care motoarele pe bază de semnături nu le pot învinge. Aceasta susține o izolare puternică, asigurând detecția în timp real a atacurilor, blocându-le pe măsură ce apar și eliminând amenințările imediat.

Indiferent că mașina protejată este Windows sau Linux, server sau desktop, HVI oferă informații la un nivel imposibil de atins din sistemul de operare găzduit. Așa cum hypervisorul controlează accesul la hardware în numele fiecărei mașini virtuale găzduite, HVI cunoaște foarte bine memoria sistemelor găzduite atât în modul de utilizator, cât și în modul kernel. Rezultatul este că HVI are informații complete despre memoria sistemului găzduit și, prin urmare, deține întregul context. În același timp, HVI este izolată de sistemele găzduite protejate, așa cum este izolat și hypervisor-ul. Prin operarea la nivel de hypervisor și valorificarea funcționalităților acestuia, HVI depășește provocările tehnice ale securității tradiționale pentru a evidenția activități periculoase în centrele de date.

HVI identifică tehnicile de atac mai degrabă decât tiparele de atac. Astfel, această tehnologie poate identifica, raporta și preveni tehnicile de exploatare obișnuite. Kernel-ul este protejat împotriva tehnicilor rootkit folosite în timpul procesului de oprire a atacurilor pentru a împiedica detectarea. Procesele din modul de utilizator sunt protejate și împotriva injectării de cod, redirecționării funcțiilor și executării de cod din stivă sau segment.

Notă
Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

2.16. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) este o soluție de securitate pentru rețea, care analizează traficul IPFIX pentru a depista prezenta oricărui comportament periculos sau a unor programe malware.

Bitdefender NTSA este menit să acționeze în completarea măsurilor dvs. de securitate existente, ca protecție complementară, capabilă să acopere punctele oarbe pe care soluțiile tradiționale nu le monitorizează.

Instrumentele tradiționale de securitate pentru rețea încearcă, în general, să prevină infectarea cu malware analizând traficul de intrare (prin sandbox, firewall-uri, antivirus etc.). Bitdefender NTSA se concentrează exclusiv pe monitorizarea traficului de ieșire din rețea pentru a depista eventualele semne de comportament rău-intenționat.

2.17. Security for Storage

GravityZone Security for Storage oferă protecție în timp real pentru principalele sisteme de partajare a fișierelor și stocare în rețea. Actualizările de sistem și ale algoritmului de detectare a amenințărilor se efectuează automat, fără niciun efort din partea dvs. și fără a determina întreruperea lucrului pentru utilizatorii finali.

Două sau mai multe GravityZone Security Server multi-platformă funcționează ca server ICAP, furnizând servicii antimalware către dispozitivele de tip NAS (Network-Attached Storage) și sistemele de partajare de fișiere în conformitate cu protocolul ICAP (Internet Content Adaptation Protocol, așa cum este acesta definit în RFC 3507).

Atunci când un utilizator solicită deschiderea, citirea, scrierea sau închiderea unui fișier de pe un laptop, o stație de lucru, un telefon mobil sau un alt dispozitiv, clientul ICAP (NAS sau sistem de partajare de fișiere) transmite o solicitare de scanare către Security Server și primește un verdict referitor la fișier. În funcție de rezultat, Security Server permite, respinge accesul sau șterge fișierul.

Notă
Acest modul este un add-on disponibil în baza unui cod de licență separat.

2.18. Security for Mobile

Combină securitatea la nivel de companie cu funcțiile de administrare și control al conformității din iPhone, iPad și dispozitivele Android oferind un software fiabil și o distribuire a actualizărilor prin intermediul magazinelor de aplicații Apple sau Android. Soluția a fost proiectată pentru a permite adoptarea controlată a inițiativelor de tip bring-your-own-device (BYOD) prin aplicarea unor politici de utilizare în mod consecvent pe toate dispozitivele mobile. Funcțiile de securitate includ blocarea ecranului, controlul autentificării, locația dispozitivului, ștergerea de la distanță, detecția dispozitivelor rootate sau decodate și a profilurilor de securitate. Pe dispozitivele Android, nivelul de securitate este îmbunătățit prin funcțiile de scanare în timp real și criptare pentru dispozitive de stocare mobile. Drept rezultat, dispozitivele mobile sunt controlate, iar informațiile confidențiale ale companiei existente pe acestea sunt protejate.

2.19. Disponibilitatea straturilor de protecție GravityZone

Disponibilitatea nivelurilor de protecție GravityZone diferă în funcție de sistemul de operare al stației de lucru. Pentru a afla mai multe, consultați articolul KB Disponibilitatea nivelurilor de protecție GravityZone.

3. ARHITECTURA GRAVITYZONE

Arhitectura unică a GravityZone permite soluției scalarea cu ușurință și în siguranță a unui număr nelimitat de sisteme. GravityZone poate fi configurat astfel încât să folosească mai multe aplicații virtuale și mai multe instanțe cu roluri specifice (Bază de date, Server de comunicații, Server de actualizări și Consolă web) pentru a asigura fiabilitatea și scalabilitatea.

Fiecare instanță a rolului poate fi instalată pe o altă aplicație. Funcțiile integrate de echilibrare a rolurilor se asigură că instalarea GravityZone protejează chiar și cele mai mari rețele corporative fără a cauza încetiniri sau blocaje. De asemenea, în locul funcțiilor de echilibrare integrate se poate folosi software-ul sau hardware-ul existent de echilibrare a sarcinilor, dacă acestea sunt prezente în rețea.

Livrat într-un container virtual, GravityZone poate fi importat pentru a rula pe orice platformă de virtualizare, inclusiv VMware, Citrix, Microsoft Hyper-V, Nutanix Prism, Microsoft Azure.

Integrarea cu VMware vCenter, Citrix XenServer, Microsoft Active Directory și Nutanix Prism Element si Microsoft Azure reduce efortul de instalare a protecției pentru stațiile de lucru fizice și virtuale.

Soluția GravityZone include următoarele componente:

- Aplicația virtuală GravityZone
- Security Server
- Pachet suplimentar HVI
- Agenți de securitate

3.1. VA GravityZone

Soluția locală a GravityZone este livrată sub forma unei aplicații virtuale (VA) Linux Ubuntu consolidate și auto-configurabile, integrate într-o imagine de mașină virtuală, ușor de instalat și configurat prin intermediul unei interfețe CLI (Command Line Interface). Aplicația virtuală este disponibilă în mai multe formate, compatibilă cu principalele platforme de virtualizare (OVA, XVA, VHD, OVF, RAW).

3.1.1. Baza de date GravityZone

Logica de bază a arhitecturii GravityZone. Bitdefender folosește o bază de date non-relațională MongoDB, ușor de scalat și reprodus.

3.1.2. Server de actualizări GravityZone

Serverul de actualizări joacă un rol important de actualizare a soluției GravityZone și a agenților pentru stațiile de lucru prin reproducerea și publicarea pachetelor necesare sau a fișierelor de instalare.

3.1.3. Serverul de comunicații GravityZone

Serverul de comunicații este legătura dintre agenții de securitate și baza de date, transferând politicile și sarcinile de securitate către stațiile de lucru protejate, precum și evenimentele raportate de agenții de securitate.

3.1.4. Serverul de incidente GravityZone

Serverul de incidente reprezintă legătura dintre agenții de securitate și baza de date, colectând date de pe endpoint-uri și generând incidente în funcție de amenințările detectate de tehnologiile de prevenție și algoritmii de învățare automată.

3.1.5. Consola web (GravityZone Control Center)

Soluțiile de securitate Bitdefender sunt gestionate dintr-un punct unic de administrare, consola web Control Center. Aceasta asigură administrarea și accesarea cu mai multă ușurință a stării de de securitate generale, a amenințărilor de securitate globale și a controlului asupra tuturor modulelor de securitate care protejează stațiile de lucru, serverele fizice sau virtualizate, precum și dispozitivele mobile. Bazată pe arhitectura Gravity, Control Center poate acoperi chiar și necesitățile celor mai mari organizații.

Control Center se integrează cu sistemele existente de administrare și monitorizare, pentru a facilita aplicarea automată a protecției pe stațiile de lucru, serverele sau dispozitivele mobile neadministrate care apar în Microsoft Active Directory, VMware vCenter, Nutanix Prism Element sau Citrix XenServer, sau care sunt detectate pur și simplu în rețea.

3.2. Security Server

Security Server este o mașină virtuală dedicată, care anulează duplicatele și centralizează majoritatea funcționalităților antimalware ale agenților de securitate, acționând ca server de scanare.

Există trei versiuni de Security Server, pentru fiecare tip de mediu de virtualizare:

- **Security Server for VMware NSX.** Această versiune se instalează automat pe fiecare gazdă din clusterul pe care a fost instalat Bitdefender.
- **Security Server pentru VMware vShield Endpoint.** Această versiune trebuie să fie instalată pe fiecare gazdă care necesită protecție.
- **Security Server Multi-platformă.** Această versiune este dedicată unor diferite tipuri de medii de virtualizare și trebuie să fie instalată pe una sau mai multe gazde astfel încât să acopere numărul de mașini virtuale protejate. Dacă folosiți HVI, trebuie să instalați un Security Server pee ficare gazdă pe care se află mașini virtuale care trebuie protejate.

3.3. Pachet suplimentar HVI

Pachetul HVI asigură legătura dintre hypervisor și Security Server de pe gazda respectivă. Astfel, Security Server poate monitoriza memoria utilizată pe gazda pe care este instalat, pe baza politicilor de securitate GravityZone.

Notă
Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

3.4. Agenți de securitate

Pentru a proteja rețeaua cu Bitdefender, trebuie să instalați agenții de securitate GravityZone corespunzători pe stațiile de lucru din rețea.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac
- GravityZone Mobile Client
- Bitdefender Tools (vShield)

3.4.1. Bitdefender Endpoint Security Tools

GravityZone asigură protecția mașinilor Windows și Linux, fizice sau virtuale, cu Bitdefender Endpoint Security Tools, un agent de securitate inteligent, care ține cont de mediu și care se adaptează în funcție de tipul stației de lucru. Bitdefender Endpoint Security Tools poate fi instalat pe orice mașină, virtuală sau fizică, asigurând un sistem de scanare flexibil, fiind alegerea ideală pentru mediile mixte (fizice, virtuale și în cloud).

Pe lângă protecția sistemului de fișiere, Bitdefender Endpoint Security Tools include și protecția serverului e-mail pentru Serverele Microsoft Exchange.

Bitdefender Endpoint Security Tools folosește un singur model de politică pentru mașinile fizice și virtuale, precum și o singură sursă pentru kit-ul de instalare pentru toate mediile (fizice ori virtuale) care rulează sistemul de operare Windows.

Straturi de protecție

Următoarele straturi de protecție sunt disponibile în cadrul Bitdefender Endpoint Security Tools:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Firewall
- Content Control
- Network Attack Defense
- Administrarea patch-urilor
- Device Control
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Incidente
- Application Control

Roluri ale stațiilor de lucru

- Utilizator privilegiat
- Relay
- Server de cache pentru patch-uri
- Protecție Exchange

Utilizator privilegiat

Administratorii Control Center pot acorda drepturi de Utilizator privilegiat utilizatorilor de stații de lucru prin intermediul setărilor politicii de securitate. Modulul Utilizator privilegiat activează drepturile de administrare la nivel de utilizator, permițând utilizatorului stației de lucru să acceseze și să modifice setările de securitate prin intermediul unei console locale. Control Center primește o notificare atunci când o stație de lucru este în modul Utilizator privilegiat, iar

administratorul Control Center poate suprascrie oricând setările de securitate locale.

Important
Acest modul este disponibil numai pentru sistemele de operare pentru desktop și server Windows suportate. Pentru informații suplimentare, consultați Ghidul de instalare GravityZone.

Relay

Agenții pentru stațiile de lucru cu rol de Bitdefender Endpoint Security Tools Relay sunt folosiți ca servere de comunicații proxy și actualizări pentru alte stații de lucru din rețea. Agenții pentru stațiile de lucru cu rol de relay sunt necesari în special pentru organizațiile cu rețele izolate, unde întregul trafic se desfășoară printr-un singur punct de acces.

În companiile cu rețele mari distribuite, agenții de tip relay ajută la scăderea gradului de utilizare a lățimii de bandă, prevenind conectarea stațiilor de lucru protejate și a serverelor de securitate direct la aplicația GravityZone.

După ce în rețea a fost instalat un agent Bitdefender Endpoint Security Tools Relay, celelalte stații de lucru pot fi configurate prin intermediul politicii pentru a comunica cu Control Center prin agentul de tip relay.

Agenții Bitdefender Endpoint Security Tools Relay sunt utilizați în următoarele scopuri:

- Descoperirea tuturor stațiilor de lucru neprotejate din rețea.
- Instalarea agentului pentru stații de lucru în rețeaua locală.
- Actualizarea stațiilor de lucru protejate din rețea.
- Asigurarea comunicării între Control Center și stațiile de lucru conectate.
- Acționarea ca server proxy pentru stațiile de lucru protejate.
- Optimizarea traficului în rețea în timpul actualizărilor, instalărilor, scanărilor și al altor sarcini consumatoare de resurse.

Server de cache pentru patch-uri

Stațiile de lucru cu rol de releu pot funcționa și ca server de cache pentru patch-uri. Având activat acest rol, releele sunt folosite pentru stocarea patch-urilor descărcate de pe site-urile producătorilor de software și distribuirea lor pe stațiile de lucru din rețeaua dumneavoastră. De fiecare dată când o stație de lucru conține software cu patch-uri lipsă, acesta le ia de pe server și nu de pe site-ul producătorului, optimizând astfel traficul generat și gradul de ocupare a lățimii de bandă a rețelei.

Important
Acest rol suplimentar este disponibil cu un add-on Patch Management înregistrat.

Protecție Exchange

Bitdefender Endpoint Security Tools cu rolul de Exchange poate fi instalat pe serverele Microsoft Exchange cu scopul de a proteja utilizatorii Exchange de amenințările transmise prin e-mail.

Bitdefender Endpoint Security Tools cu rolul Exchange protejează atât serverul cât și soluția Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac este un agent de securitate conceput pentru a proteja stațiile de lucru și laptopurile Macintosh cu tehnologie Intel. Technologia de scanare disponibilă este **Scanare localizată**, având conținut de securitate stocat local.

Straturi de protecție

Următoarele straturi de protecție sunt disponibile în cadrul Endpoint Security for Mac:

- Antimalware
- Advanced Threat Control
- Content Control
- Device Control
- Full Disk Encryption

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client extinde politicile de securitate cu ușurință pe un număr nelimitat de dispozitive Android și iOS, protejându-le împotriva utilizării neautorizate, a riscurilor și pierderii de date confidențiale. Funcțiile de securitate includ blocarea ecranului, controlul autentificării, locația dispozitivului, ștergerea de la distanță, detecția dispozitivelor rootate sau decodate și a profilurilor de securitate. Pe dispozitivele Android, nivelul de securitate este îmbunătățit prin funcțiile de scanare în timp real și criptare pentru dispozitive de stocare mobile.

GravityZone Mobile Client este distribuit exclusiv prin Apple App Store și Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools este un agent care necesită puțin spațiu pentru mediile virtuale VMware integrate cu terminalul vShield. Agentul de securitate se instalează pe mașinile virtuale protejate cu Security Server, pentru a vă permite să profitați de funcțiile suplimentare pe care le oferă:

- Vă permite să rulați sarcinile Memory și Process Scan pe mașină.
- Informează utilizatorul cu privire la infestările detectate și măsurile luate pentru eliminarea acestora.
- Adaugă mai multe opțiuni pentru excepțiile la scanările antimalware.

3.5. Architectura Sandbox Analyzer

Bitdefender Sandbox Analyzer oferă un strat puternic de protecție împotriva amenințărilor avansate, efectuând analize automate în profunzime asupra fișierelor suspecte care nu sunt încă semnate de motoarele antimalware ale Bitdefender.

Sandbox Analyzer este disponibil în două variante:

- Sandbox Analyzer Cloud, găzduit de Bitdefender.
- Sandbox Analyzer On-Premises, disponibil ca aplicație virtuală care poate fi instalată local.

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud conține următoarele componente:

- **Sandbox Analyzer Portal** – un server de comunicare găzduit, utilizat pentru administrarea solicitărilor dintre stațiile de lucru și clusterul sandbox Bitdefender.
- **Sandbox Analyzer Cluster** – infrastructura sandbox găzduită, unde are loc analiza comportamentală a mostrelor. La acest nivel, fișierele încărcate sunt detonate pe mașini virtuale cu sistem de operare Windows 7.

GravityZone Control Center operează ca o consolă de administrare și raportare, unde puteți configura politicile de securitate, vizualiza rapoarte și notificări.

Bitdefender Endpoint Security Tools, agentul de securitate instalat pe endpoint-uri, acționează ca senzor de alimentare pentru Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises este livrat sub forma unei aplicații virtuale Linux Ubuntu integrată într-o imagine de mașină virtulă, ușor de instalat și configurat prin intermediul unei interfețe CLI (command-line interface). Sandbox Analyzer On-Premises este disponibil în format OVA și poate fi instalat pe VMWare ESXi.

O instanță Sandbox Analyzer On-Premises conține următoarele componente:

- **Sandbox Manager**. Această componentă coordonează sandbox-ul. Sandbox Manager se conectează la hypervisor-ul ESXi prin API și utilizează resursele hardware ale acestuia pentru crearea și operarea mediului de analiză a malware-ului.
- **Mașini virtuale de detonare**. Această componentă este reprezentată de mașini virtuale utilizate de Sandbox Analyzer pentru a executa fișierele și a analiza comportamentele acestora. Mașinile virtuale de detonare pot rula pe sisteme de operare Windows 7 și Windows 10 64-bit.

GravityZoneControl Center operează ca o consolă de administrare și raportare pe care o puteți utiliza pentru configurarea politicilor de securitate și vizualizarea de rapoarte și notificări.

Sandbox Analyzer On-Premises operează următorii senzori de alimentare:

- **Senzor endpoint**. Bitdefender Endpoint Security Tools pentru Windows îndeplinește rolul de senzor de alimentare instalat pe endpoint-uri. Agentul Bitdefender utilizează tehnologii avansate de învățare automată (machine learning) și algoritmi neurali de rețea pentru detectarea conținutului suspect și trimiterea acestuia către Sandbox Analyzer, inclusiv obiecte din carantina centralizată.
- **Senzor rețea**. Aplicația virtuală de securitate pentru rețea (NSVA) este o aplicație virtuală care poate fi instalată în același mediu virtualizat ESXi ca și instanța Sandbox Analyzer. Senzorul de rețea extrage conținut din fluxurile de rețea și îl trimite către Sandbox Analyzer.
- **Senzor ICAP**. Fiind instalat pe dispozitive NAS (network attached storage) utilizând protocolul ICAP, Bitdefender Security Server suportă trimiterea de conținut către Sandbox Analyzer.

În afară de acești senzori, Sandbox Analyzer On-Premises suportă trimiterea manuală și prin API. Pentru detalii, consultați capitolul **Utilizarea Sandbox Analyzer** din Ghidul administratorului GravityZone.

4. INTRODUCERE

Soluțiile GravityZone pot fi configurate și administrate printr-o platformă de control denumită Control Center. Consola Control Center are o interfață web, pe care o puteți accesa folosind numele de utilizator și parola.

4.1. Conectarea la Control Center

Accesul la Control Center se realizează prin conturile de utilizator. Veți primi informațiile dumneavoastră de autentificare prin e-mail odată ce contul dumneavoastră a fost creat.

Cerințe preliminare:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Rezoluție recomandată a ecranului: 1280 x 800 sau mai mare

Avertisment
Control Center nu va funcționa/nu se va afișa corespunzător în Internet Explorer 9+ cu funcția Compatibility View activată, care este echivalentă cu utilizarea unei versiuni de browser incompatibile.

Pentru conectarea la Control Center:

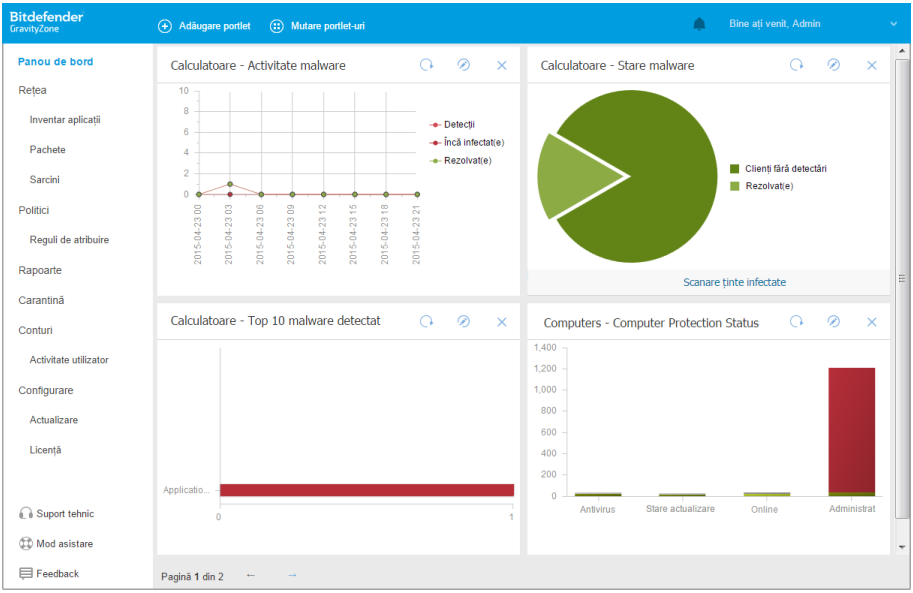
1. În bara de adrese a browser-ului web, introduceți adresa IP sau numele de gazdă DNS al aplicației Control Center (folosind prefixul `https://`).
2. Introduceți numele de utilizator și parola.
3. Introduceți codul din șase cifre din Google Authenticator, Microsoft Authenticator sau alt instrument de autentificare în doi pași de tip TOTP (Time-Based One-Time Password Algorithm) - compatibil cu standardul RFC6238. Pentru mai multe detalii, vă rugăm consultați „Administrarea contului dumneavoastră” (p. 25).
4. Faceți clic pe **Autentificare**.

Prima dată când vă autentificați, trebuie să acceptați Termenii și condițiile de furnizare a serviciilor Bitdefender. Selectați **Continuare** pentru a începe să utilizați GravityZone.

Notă
Dacă ați uitat parola, utilizați legătura de recuperare a parolei pentru a solicita o nouă parolă. Trebuie să furnizați adresa e-mail a contului dumneavoastră.

4.2. Control Center dintr-o privire

Consola Control Center este organizată astfel încât permite accesul facil la toate funcțiile. Utilizați bara de meniu din partea din dreapta sus pentru a naviga prin consolă. Funcțiile disponibile depind de tipul de utilizator care accesează consola.



Panoul de bord

4.2.1. Vedere de ansamblu asupra Control Center

Utilizatorii care dețin rolul de administrator al companiei dețin drepturi depline asupra configurației Control Center și setărilor de securitate a rețelei, în timp ce utilizatorii cu rol de administrator au acces la funcțiile de securitate a rețelei, inclusiv administrarea utilizatorilor.

Utilizați butonul **Meniu vizualizare** din colțul din stânga sus pentru a restrânge la vizualizare tip pictogramă, a ascunde sau a extinde opțiunile de meniu. Efectuați

clic pe buton pentru a trece secvențial prin opțiuni sau efectuați dublu clic pentru a trece peste.

În funcție de rolul dvs., puteți accesa următoarele opțiuni de meniu:

Panou de bord
Vizualizați grafice ușor de citit care furnizează informații cheie despre securitatea rețelei dumneavoastră.

Incidente
Vizualizați și administrați incidentele de securitate din rețeaua companiei.

Rețea
Instalați protecția, aplicați politici pentru a administra setările de securitate, rulați sarcini de la distanță și generați rapid rapoarte.

Politici
Creați și administrați politici de securitate.

Rapoarte
Obțineți rapoarte de securitate referitoare la clienții administrați.

Carantină
Administrați de la distanță fișierele aflate în carantină.

Conturi
Administrați accesul la Control Center pentru alți angajați ai companiei.

În acest meniu puteți găsi, de asemenea, pagina **Activitate utilizator**, care permite accesarea jurnalului de activitate al utilizatorului.

Notă
Acest meniu este disponibil numai pentru utilizatorii cu drepturi de **Administrare utilizatori**.

Configurare
Configurați setările Control Center, cum ar fi setările privind serverul de mail, integrarea cu Active Directory sau cu medii de virtualizare, certificatele de securitate și Inventarul de rețea, inclusiv reguli programate pentru ștergerea automată a mașinilor virtuale neutilizate.

Notă
Acest meniu este disponibil numai pentru utilizatorii cu drepturi de **Administrare soluție**.

Dacă apăsați pe numele de utilizator din colțul din dreapta sus al consolei, sunt disponibile opțiunile următoare:

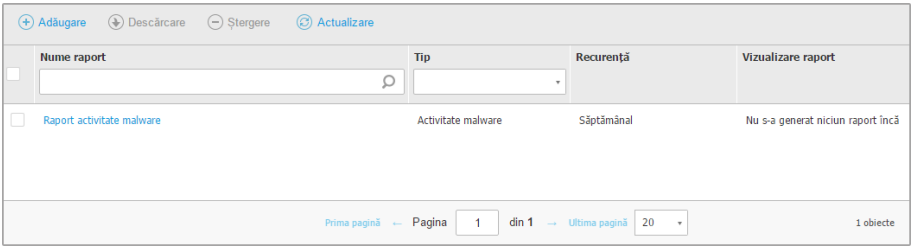
- **Contul meu**. Faceți clic pe această opțiune pentru a administra detaliile și preferințele contului dumneavoastră de utilizator.
- **Administrare date de autentificare**. Faceți clic pe această opțiune pentru adăugarea sau administrarea datelor de autentificare necesare pentru sarcinile de instalare de la distanță.
- **Ajutor & Asistență**. Efectuați clic pe această opțiune pentru ajutor și informații de asistență.
- **Trimiteți feedback**. Efectuați clic pe această opțiune pentru a afișa un formular care vă permite să modificați și să trimiteți mesaje de feedback cu privire la experiența dumneavoastră cu GravityZone.
- **Deconectare**. Faceți clic pe această opțiune pentru a ieși din contul dumneavoastră.

În plus, în colțul din dreapta sus al consolei, veți găsi:

- Pictograma **Mod Ajutor**, care activează casetele de indicații poziționate deasupra elementelor din Control Center. Puteți afla cu ușurință informații utile cu privire la caracteristicile Control Center.
- Pictograma **Notificări**, care asigură un acces ușor la mesajele de notificare și la pagina **Notificări**.

4.2.2. Date tabelare

Tabelele sunt deseori utilizate în cadrul consolei, pentru organizarea datelor într-un format ușor de utilizat.



Pagina Rapoarte

Navigarea prin pagini

Tabelele cu mai mult de 20 intrări au mai multe pagini. În mod implicit, se afișează numai 20 intrări/pagină. Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului. Puteți modifica numărul de intrări afișate pe pagină selectând o altă opțiune din meniul de lângă butoanele de navigație.

Căutarea anumitor intrări

Pentru a găsi cu ușurință anumite intrări, folosiți casetele de selectare de sub titlurile coloanelor.

Introduceți termenul căutarii în câmpul corespunzător. Elementele care corespund criteriilor de căutare sunt afișate în tabel pe măsură ce tastați. Pentru resetarea conținutului tabelului, ștergeți informațiile din câmpurile de căutare.

Sortarea datelor

Pentru a sorta datele dintr-o coloană, faceți clic pe titlul acesteia. Faceți clic pe titlul coloanei din nou pentru a inversa ordinea sortării.

Reîmprospătarea datelor tabelare

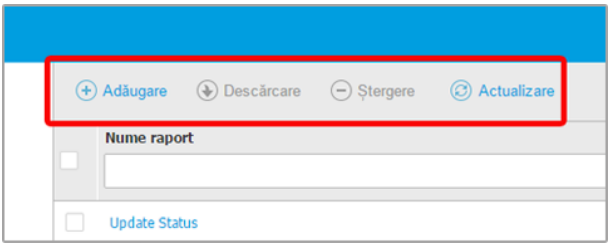
Pentru a vă asigura că în consolă se afișează cele mai recente informații, faceți clic pe butonul **Reîmprospătare** din colțul de sus al tabelului.

Acest lucru poate fi necesar atunci când petreceți mai mult timp pe pagină.

4.2.3. Bare de instrumente pentru acțiuni

În Control Center, barele de instrumente pentru acțiuni vă permit să efectuați anumite operațiuni aferente secțiunii în care vă aflați. Fiecare bară de instrumente include o serie de pictograme care se află în partea de sus a tabelului. De exemplu, bara de instrumente de acțiuni din secțiunea **Rapoarte** vă permite să efectuați următoarele operații:

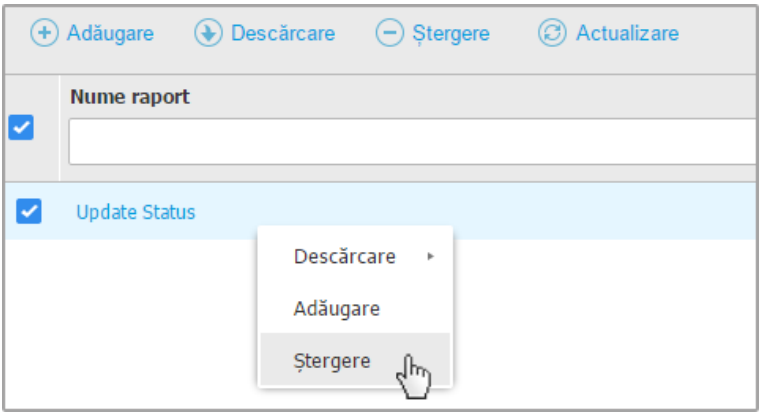
- Crearea unui nou raport.
- Descărcați un raport programat.
- Ștergerea unui raport programat.



Pagina de Rapoarte - Bara de instrumente pentru acțiuni

4.2.4. Meniul contextual

Comenzile de pe bara de instrumente pentru acțiuni sunt, de asemenea, accesibile din meniul contextual. Faceți clic dreapta pe secțiunea Control Center pe care o utilizați și selectați comanda de care aveți nevoie din listă.



Pagina de Rapoarte - Meniu contextual

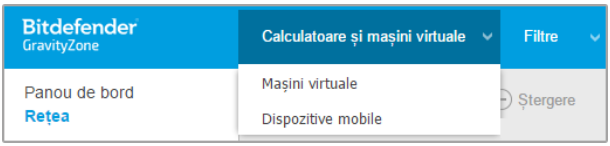
4.2.5. Selector vederi

Dacă lucrați cu diferite tipuri de stații de lucru, le puteți găsi organizate pe pagina **Rețea** după tip, în diferite vizualizări de rețea:

- **Calculatoare & și Mașini virtuale**: afișează grupurile Active Directory și calculatoarele, precum și stațiile de lucru fizice și virtuale din afara Active Directory identificate în rețea.

- **Mașinile virtuale**: afișează infrastructura mediului virtual integrat cu Control Center și toate mașinile virtuale conținute.
- **Dispozitive mobile**: afișează utilizatorii și dispozitivele mobile alocate acestora.

Pentru a selecta vizualizarea de rețea dorită, faceți clic pe meniul de vizualizări din colțul din dreapta sus al paginii.



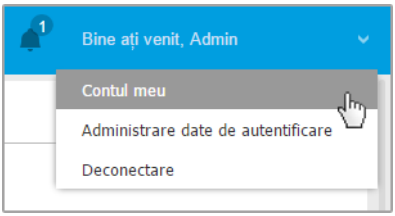
Opțiunea de selectare a vederilor

Notă
Veți vedea doar stațiile de lucru pe care aveți permisiunea să le vizualizați, permisiuni care vă sunt acordate de administratorul care a adăugat utilizatorul la Control Center.

4.3. Administrarea contului dumneavoastră

Pentru a verifica sau modifica detaliile și setările contului dumneavoastră:

1. Faceți clic pe numele de utilizator din colțul din dreapta sus al consolei și selectați **Contul meu**.



Meniul Cont de utilizator

2. În secțiunea **Detalii cont**, corectați sau actualizați detaliile contului dumneavoastră. Dacă utilizați un cont de utilizator Active Directory, nu puteți modifica detaliile contului.
   - **Utilizator.** Numele de utilizator este identificatorul unic al contului de utilizator și nu poate fi modificat.
   - **Nume complet.** Introduceți numele complet.

- **E-mail.** Aceasta este adresa dumneavoastră e-mail pentru autentificare și contact. Rapoartele și notificările importante de securitate sunt expediate la această adresă. Notificările prin e-mail sunt expediate automat oricând sunt detectate situații de risc în rețea.
- Linkul **Modificare parolă** vă permite să schimbați parola de conectare.

3. În secțiunea **Setări**, configurați setările contului conform preferințelor dumneavoastră.
   - **Fus orar.** Selectați din meniu fusul orar al contului. Consola va afișa informațiile referitoare la oră conform fusului orar selectat.
   - **Limba.** Selectați din meniu limba de afișare a consolei.
   - **Expirare sesiune.** Selectați intervalul de inactivitate înainte ca sesiunea dvs. ca utilizator să expire.
4. În **Siguranță la autentificare**, configurați autentificarea în doi pași și verificați starea politicilor disponibile pentru a securiza contul dumneavoastră GravityZone. Politicile valabile la nivelul întregii companii au doar drepturi de citire (read-only).

   Pentru a activa autentificarea de tip „two-factor”:

   a. **Autentificare în doi pași.** Autentificarea în doi pași adaugă un strat suplimentar de securitate contului dumneavoastră GravityZone, solicitând un cod de autentificare pe lângă datele dumneavoastră de conectare la Control Center.

      La prima autentificare în contul dumneavoastră GravityZone, vi se va solicita să descărcați și să instalați Google Authenticator, Microsoft Authenticator sau alt instrument de autentificare în doi pași de tip TOTP (Time-Based One-Time Password Algorithm) - compatibil cu standardul RFC6238 pe un dispozitiv mobil, să-l asociați contului dumneavoastră GravityZone și apoi să-l utilizați la fiecare autentificare în Control Center. Google Authenticator generează un cod de șase cifre la fiecare 30 de secunde. Pentru a finaliza conectarea la Control Center, după introducerea parolei, va trebui să furnizați codul de șase cifre generat de aplicația Google Authenticator.

      Notă
      Puteți sări peste această procedură de trei ori, după care nu vă veți mai putea autentifica fără autentificarea în doi pași.

      Pentru a activa autentificarea de tip „two-factor”:

      i. Apăsați butonul **Activare** din mesajul **Autentificare în doi pași**.

ii. În caseta de dialog, faceți clic pe linkul corespunzător pentru a descărca și instala aplicația Google Authenticator pe dispozitivul dumneavoastră mobil.

iii. Pe dispozitivul dvs. mobil, deschideți Google Authenticator.

iv. În fereastra **Adăugare cont**, scanați codul QR pentru a conecta aplicația la contul dvs. GravityZone.

De asemenea, puteți introduce manual codul secret.

Această acțiune este necesară numai o singură dată, pentru a activa această funcție în GravityZone.

Important
Asigurați-vă că ați copiat și salvat codul secret într-un loc sigur. Dați clic pe **Generare backup** pentru a crea un fișier PDF conținând codul QR și o întrebare secretă. Dacă dispozitivul mobil utilizat pentru activarea autentificării de tip two-factor este pierdut sau înlocuit, va trebui să instalați aplicația Google Authenticator pe un dispozitiv nou și să furnizați codul secret pentru a-l conecta la contul dvs. GravityZone.

v. Introduceți codul de șase cifre în câmpul **Cod Google Authenticator**.

vi. Faceți clic pe **Activare** pentru a finaliza activarea acestei funcții.

Notă
Este necesar să știți că, dacă autentificarea 2FA configurată la momentul actual este dezactivată pentru contul dumneavoastră, cheia secretă nu va mai fi valabilă.

b. **Politica de expirare a parolei.** Modificările aduse regulat parolei dumneavoastră oferă un nivel suplimentar de protecție împotriva utilizării neautorizate a parolei sau limitează durata utilizării neautorizate. După activare, GravityZone vă solicită să vă schimbați parola cel mult o dată la 90 de zile.

c. **Politica de blocare a contului.** Această politică împiedică accesarea contului dumneavoastră după cinci încercări eșuate consecutive de autentificare. Această măsură asigură protecție împotriva atacurilor de tip brute-force.

Pentru deblocarea contului dumneavoastră, este nevoie să vă resetați parola din pagina de autentificare sau să contactați un alt administrator GravityZone.

5. Faceți clic pe **Salvare** pentru a aplica modificările.

Notă
Nu vă puteți șterge propriul cont.

4.4. Schimbarea parolei de conectare

După ce contul dvs. a fost creat, veți primi un e-mail cu datele de autentificare.

Cu excepția cazului în care folosiți datele Active Directory pentru a accesa Control Center, se recomandă să procedați după cum urmează:

- Modificați parola de autentificare implicită la prima accesare a Control Center.
- Modificați periodic parola dumneavoastră de autentificare.

Pentru a modifica parola de autentificare:

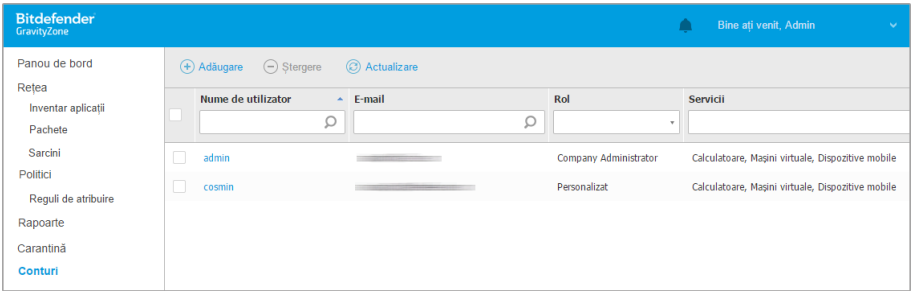
1. Faceți clic pe numele de utilizator din colțul din dreapta sus al consolei și selectați **Contul meu**.
2. În **Detalii cont**, faceți clic pe **Modificare parolă**.
3. Introduceți parola actuală și noua parolă în câmpurile corespunzătoare.
4. Faceți clic pe **Salvare** pentru a aplica modificările.

5. CONTURILE DE UTILIZATOR

Puteți crea primul cont de utilizator GravityZone în cursul configurării inițiale Control Center, după implementarea dispozitivului GravityZone. Contul de utilizator Control Center inițial are rol de administrator de companie, cu drepturi depline asupra configurării Control Center și de administrare a rețelei Din acest cont, puteți crea toate celelalte conturi de utilizator necesare pentru administrarea rețelei companiei dumneavoastră.

Ce trebuie să știți despre conturile de utilizator GravityZone:

- Pentru a permite altor angajați ai companiei să acceseze Control Center, puteți crea conturi de utilizator în mod individual sau puteți activa accesul dinamic pentru mai multe conturi prin integrări Active Directory sau reguli de acces. Puteți să atribuiți conturi de utilizator cu roluri diferite, în funcție de nivelul lor de acces în companie.
- Pentru fiecare cont de utilizator, puteți personaliza accesul la caracteristicile GravityZone sau la anumite părți ale rețelei din care face parte.
- Puteți administra doar conturile cu drepturi egale sau inferioare contului dumneavoastră.



Pagina Conturi

Conturile existente sunt afișate în tabel. Pentru fiecare cont de utilizator, puteți vizualiza:

- Numele de utilizator al contului (utilizat pentru a vă conecta la Control Center).
- Adresa de e-mail a contului (folosită ca o adresă de contact). Rapoartele și notificările importante de securitate sunt expediate la această adresă.

Notificările prin e-mail sunt expediate automat oricând sunt detectate situații de risc în rețea.

- Rolul utilizatorului (administrator companie / administrator rețea / analist securitate / particularizat).
- Cu serviciile de securitate GravityZone utilizatorul poate administra (calculatoare, mașini virtuale, dispozitive mobile).
- Starea 2FA (autentificare two-factor), care vă permite să verificați rapid dacă utilizatorul a activat autentificarea de tip „two factor”.
- Starea Regulii de acces, indică un cont de utilizator creat prin intermediul unei reguli privind drepturile de acces. Conturile de utilizator create manual vor afișa valoarea **N/A**.

5.1. Roluri de utilizator

Rolul de utilizator constă într-o combinație specifică de drepturi de utilizator. La crearea unui cont de utilizator, puteți alege unul dintre rolurile predefinite sau puteți crea un rol personalizat, selectând doar anumite drepturi de utilizator.

Notă
Puteți atribui doar conturi de utilizator cu drepturi egale sau inferioare contului dumneavoastră.

Sunt disponibile următoarele roluri de utilizator:

1. **Administrator de companie** - De regulă, pentru fiecare companie se crează un singur cont de utilizator cu rol de Administrator de companie cu drepturi depline de acces la toate caracteristicile de administrare ale soluțiilor GravityZone. Un administrator de companie configurează setările Control Center, administrează cheile de licență ale serviciilor de securitate, gestionează conturile de utilizator având în același timp drepturi administrative asupra setărilor de securitate ale rețelei companiei. Administratorii companiei pot partaja sau își pot delega responsabilitățile operaționale către administratorii subordonați și analistii de securitate.
2. **Administrator de rețea** - Pentru o companie, pot fi create mai multe conturi cu rol de Administrator de rețea, cu privilegii administrative asupra întregii instalări a agenților de siguranță ai companiei sau asupra unui anumit grup de stații de lucru, inclusiv asupra administrării utilizatorilor. Administratorii de rețea sunt responsabili pentru gestionarea activă a setărilor de securitate ale rețelei.

3. **Analist securitate** - Conturile de Analist securitate sunt conturi disponibile doar în citire. Acestea permit accesul numai la datele, rapoartele și jurnalele referitoare la securitate. Astfel de conturi pot fi alocate personalului cu responsabilități de monitorizare a securității sau altor angajați care trebuie să fie ținuți la curent cu starea de securitate.
4. **Particularizat** - Rolurile de utilizator predefinite includ o anumită combinație de drepturi de utilizator. În cazul în care un rol predefinit de utilizator nu este adecvat nevoilor dvs., puteți crea un cont personalizat prin selectarea drepturilor care vă interesează.

Tabelul de mai jos prezintă pe scurt relațiile dintre diferitele roluri de cont și drepturile lor. Pentru informații detaliate, consultați capitolul „Drepturile de utilizare" (p. 31).

Rol cont	Conturi subordonate permise	Drepturile de utilizare
Administrator companie	Administratori companie, Administratori rețea, Analisti de Securitate	Administrare soluție Administrare companie Administrare utilizatori Administrare rețele Vizualizare și analizare date
Administrator rețea	Administratori rețea, Analisti de Securitate	Administrare utilizatori Administrare rețele Vizualizare și analizare date
Analist de securitate	-	Vizualizare și analizare date

5.2. Drepturile de utilizare

Puteți atribui următoarele drepturi de utilizator conturilor de utilizator GravityZone:

- **Administrare soluție**. Permite configurarea setărilor Control Center (setările de server de mail și proxy, integrarea cu Active Directory și platforme de virtualizare, certificate de securitate și actualizări GravityZone). Acest privilegiu este specific pentru conturile de administrator ale companiei.
- **Administrare utilizatori**. Creați, modificați sau ștergeți conturi de utilizator.

- **Administrare companie**. Utilizatorii pot administra propria cheie de licență GravityZone și pot modifica setările de profil ale companiei lor. Acest privilegiu este specific pentru conturile de administrator ale companiei.
- **Administrare rețele**. Oferă privilegii administrative asupra setărilor de securitate de rețea (inventar de rețea, politici, activități, pachete de instalare, carantină). Acest privilegiu este specific conturilor de administrator de rețea.
- **Vizualizare și analizare date**. Vizualizarea evenimentelor și a jurnalelor referitoare la securitate, gestionarea rapoartelor și a panoului de control.

5.3. Administrarea conturilor de utilizator

Pentru a crea, modifica, șterge și configura conturi de utilizator, utilizați următoarele metode:

- Administrarea individuală a conturilor de utilizator. Utilizați această metodă pentru a adăuga conturi de utilizator la nivel local sau conturi Active Directory. Pentru a configura o integrare Active Directory, consultați Ghidul de instalare GravityZone.

  Înainte de a crea un cont de utilizator, asigurați-vă că aveți la îndemână adresa de e-mail necesară. Utilizatorul primește datele de autentificare GravityZone la adresa de e-mail furnizată.
- Administrarea mai multor conturi de utilizator. Utilizați această metodă pentru a activa accesul dinamic prin intermediul regulilor de acces. Această metodă necesită o integrare de domeniu Active Directory. Pentru informații suplimentare despre integrarea Active Directory, consultați Ghidul de instalare GravityZone.

5.3.1. Administrarea individuală a conturilor de utilizator

În Control Center, puteți să creați, să modificați și să ștergeți în mod individual conturile de utilizator.

Dependențe

- Conturile create la nivel local pot șterge conturi create prin integrarea Active Directory, indiferent de rolul acestora.
- Conturile create la nivel local nu pot șterge conturi similare, indiferent de rolul acestora.

Crearea individuală a conturilor de utilizator

Pentru a adăuga un cont de utilizator în Control Center:

1. Mergeți la pagina **Conturi**.
2. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Va apărea o fereastră de configurare.
3. În secțiunea **Detalii**, configurați următoarele:
   - Pentru conturile de utilizator Active Directory, configurați următoarele detalii:

     Nume de utilizator pentru conturile de utilizator Active Directory (AD). Selectați un cont de utilizator din lista derulantă și treceți la pasul 4.

     Puteți adăuga conturi de utilizator AD numai dacă integrarea este configurată. Când adăugați un cont de utilizator AD, datele utilizatorului sunt importate din domeniul asociat acestuia. Utilizatorul se autentifică în Control Center folosind numele de utilizator AD și parola aferentă.

     Notă

     – Pentru a vă asigura că cele mai recente modificări ale Active Directory sunt importate în Control Center, faceți click pe butonul **Sincronizare**.

     – Utilizatorii cu drept de **Administrare a soluției** pot configura intervalul de sincronizare Active Directory folosind opțiunile disponibile în secțiunea **Configurare > Active Directory**. Pentru detalii suplimentare, consultați capitolele **Instalarea protecției > Instalarea GravityZone** și **Configurare > Configurare setări centrale Control Center** din Ghidul de instalare GravityZone.

   - Pentru conturile locale, configurați următoarele detalii:

     – **Nume de utilizator** pentru conturile locale. Dezactivați funcția **Import din Active Directory** și introduceți un nume de utilizator.

     – **Email**. Introduceți adresa de e-mail a utilizatorului.

       Adresa de e-mail trebuie să fie unică. Nu puteți crea un alt cont de utilizator cu aceeași adresă e-mail.

       GravityZone utilizează această adresă de e-mail pentru a trimite notificări.

     – **Nume complet**. Introduceți numele complet al utilizatorului.

– **Parolă**. Introduceți o parolă pe care utilizatorul să o folosească pentru a se autentifica.

  Parola trebuie să includă cel puțin o literă mare, cel puțin o literă mică și cel puțin o cifră sau un caracter special.

– **Confirmare parolă**. Confirmați parola pentru validare.

4. La secțiunea **Setări și privilegii**, configurați următoarele setări:

   - **Fus orar**. Selectați din meniu fusul orar al contului. Consola va afișa informațiile referitoare la oră conform fusului orar selectat.
   - **Limba**. Selectați din meniu limba de afișare a consolei.
   - **Rol**. Selectați rolul utilizatorului. Pentru detalii cu privire la rolurile de utilizator, consultați „Roluri de utilizator” (p. 30).
   - **Drepturi**. Fiecare rol de utilizator predefinit are o anumită configurație de drepturi. Cu toate acestea, puteți selecta doar drepturile de care aveți nevoie. În acest caz, rolul utilizatorului se modifică în **Personalizat**. Pentru detalii cu privire la drepturile de utilizator, consultați „Drepturile de utilizare” (p. 31).
   - **Selectare ținte**. Selectați grupurile de rețea la care utilizatorul va avea acces pentru fiecare serviciu de securitate disponibil. Puteți restricționa accesul utilizatorilor la un anumit serviciu de securitate GravityZone sau pentru anumite zone ale rețelei.

     Notă
     Opțiunile de selecție a țintelor nu vor fi afișate pentru utilizatorii cu drept de Administrare soluție care au implicit privilegii asupra întregii rețele și asupra serviciilor de securitate.

     Important
     La fiecare modificare în structura rețelei sau la configurarea unei noi integrări cu Serverul vCenter sau cu sistemul XenServer, nu uitați să verificați și să actualizați drepturile de acces pentru utilizatorii existenți.

5. Faceți clic pe **Salvare** pentru a adăuga utilizatorul. Noul cont va apărea în lista conturilor de utilizatori.

   Control Center trimite automat utilizatorului un e-mail cu detaliile de conectare, cu condiția ca setările serverului de mail să fi fost configurate în mod

corespunzător. Pentru detalii suplimentare privind configurarea serverului de mail, consultați capitolul **Instalarea protecției > Instalarea și configurarea GravityZone >Configurare setări centrale Control Center** din Ghidul de instalare GravityZone.

Modificarea individuală a conturilor de utilizator

Pentru a adăuga un cont de utilizator în Control Center

1. Conectați-vă la Control Center.
2. Mergeți la pagina **Conturi**.
3. Faceți clic pe numele utilizatorului.
4. Modificați detaliile contului de utilizator și setările după cum este necesar.
5. Faceți clic pe **Salvare** pentru a aplica modificările.

Notă
Toate conturile cu drept **Administrare utilizatori** pot crea, edita și șterge alte conturi de utilizator. Puteți administra doar conturile cu drepturi egale sau inferioare contului dumneavoastră.

Ștergerea individuală a conturilor de utilizator

Pentru a șterge un cont de utilizator din Control Center

1. Conectați-vă la Control Center.
2. Mergeți la pagina **Conturi**.
3. Selectați din listă contul de utilizator.
4. Faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului.

   Faceți clic pe **Da** pentru confirmare.

5.3.2. Administrarea mai multor conturi de utilizator

Creați reguli de acces pentru a permite GravityZone Control Center accesul la utilizatorii Active Directory, pe baza grupurilor de securitate.

Cerințe preliminare

Pentru a gestiona mai multe conturi de utilizator, este necesară o integrare de domeniu Active Directory cu GravityZone. Pentru a integra și sincroniza un domeniu

Active Directory, consultați capitolul **Active Directory** din Ghidul de instalare GravityZone.

Dependențe

Regulile de acces sunt legate de grupurile de securitate Active Directory (AD) și de conturile de utilizator asociate. Orice modificare efectuată asupra domeniilor Active Directory poate avea un impact asupra regulilor de acces asociate. Iată ce trebuie să știți despre relația dintre reguli, utilizatori și domenii Active Directory:

- O regulă de acces determină adăugarea unui cont de utilizator numai dacă adresa de e-mail nu este deja asociată unui cont existent.
- Pentru adresele de e-mail duplicate dintr-un grup de securitate, regula de acces determină crearea unui cont de utilizator GravityZone numai pentru primul cont de utilizator Active Directory care se conectează la Control Center.

  De exemplu, un grup de securitate conține o adresă de e-mail duplicată pentru diferiți utilizatori și toți încearcă să se conecteze la Control Center utilizând propriile datele de autentificare Active Directory. Dacă o regulă de acces este asociată acestui domeniu Active Directory, acesta va crea un cont de utilizator numai pentru primul utilizator care s-a conectat la Control Center utilizând adresa de e-mail duplicată.
- Conturile utilizator create prin intermediul regulilor de acces devin inactive dacă sunt eliminate din grupul de securitate AD asociat. Aceiași utilizatori pot deveni activi dacă sunt asociați unei noi reguli de acces.
- Regulile de acces devin disponibile numai pentru citire (read-only) după ce un domeniu Active Directory asociat nu mai este integrat cu GravityZone. Utilizatorii asociați acestor reguli devin inactivi.
- Conturile de utilizator create prin reguli de acces nu pot șterge utilizatori creați la nivel local.
- Conturile de utilizator create prin reguli de acces nu pot șterge conturi similare cu rolul de Administrator al companiei.

Crearea mai multor conturi de utilizator

Pentru a adăuga mai multe conturi de utilizator, creați reguli de acces. Regulile de acces sunt asociate grupurilor de securitate Active Directory.

Pentru a adăuga o regulă referitoare la drepturile de acces:

1. Accesați pagina **Configurare > Active Directory > Drepturi de acces**.
2. Dacă aveți mai multe integrări, selectați un domeniu din partea stângă sus a tabelului.
3. Selectați ⊕ **Adaugă** din stânga tabelului.
4. Configurați următoarele setări referitoare la drepturile de acces:
   - **Prioritatea**. Regulile sunt ordonate în funcție de prioritate. Cu cât este mai mic numărul, cu atât este mai mare prioritatea.
   - **Nume**. Denumirea regulii de acces.
   - **Domeniu**. Domeniul din care se adaugă grupuri de securitate.
   - **Grupurile de securitate** . Grupurile de securitate care conțin viitorii utilizatori GravityZone. Puteți folosi caseta pentru completare automată. După ce salvați regula de acces, nu este permisă modificarea, adăugarea sau ștergerea grupurilor de securitate adăugate în această listă.
   - **Fus orar**. Fusul orar al utilizatorului.
   - **Limba**. Limba de afișare a consolei.
   - **Rol**. Rolurile de utilizator predefinite. Pentru informații suplimentare, consultați capitolul **Conturi de utilizator** din Ghidul administratorului GravityZone.

     Notă
     Puteți acorda și revoca drepturi pentru alți utilizatori care au drepturi de acces inferioare celor conferite contului dumneavoastră.

   - **Drepturi**. Fiecare rol de utilizator predefinit are o anumită configurație de drepturi. Pentru mai multe detalii, consultați capitolul **Drepturile utilizatorului** din Ghidul administratorului GravityZone.
   - **Selectare obiecte vizate** Selectați grupurile de rețea la care va avea acces utilizatorul pentru fiecare serviciu de securitate disponibil. Puteți restricționa accesul utilizatorilor la un anumit serviciu de securitate GravityZone sau pentru anumite zone ale rețelei.

     Notă
     Opțiunile de selecție a țintelor nu vor fi afișate pentru utilizatorii cu drept de Administrare soluție care au implicit privilegii asupra întregii rețele și asupra serviciilor de securitate.

5. Faceți clic pe **Save**.

   Regula de acces este salvată în cazul în care nu există niciun impact asupra utilizatorului. În caz contrar, vi se solicită să specificați excepțiile la nivel de utilizator. De exemplu, atunci când adăugați o regulă cu o prioritate mai mare, utilizatorii afectați asociați altor reguli sunt legați de regula anterioară.
6. Dacă este necesar, selectați utilizatorii pe care doriți să îi excludeți. Pentru mai multe informații, consultați Excepții privind conturile de utilizator.
7. Efectuați clic pe **Confirmare**. Regula este afișată în pagina **Drepturi de acces**.

Utilizatorii din cadrul grupurilor de securitate specificate în regulile de acces pot accesa acum GravityZone Control Center folosind datele lor de autentificare pentru domeniu. Control Center creează automat noi conturi de utilizator atunci când aceștia se conectează pentru prima dată, utilizând adresa de e-mail și parola lor pentru Active Directory.

Pentru conturile de utilizator create prin intermediul unei reguli de acces, denumirea regulii de acces va fi afișată în pagina **Conturi**, în coloana **Regulă de acces**.

Modificarea mai multor conturi de utilizator

Pentru a modifica o regulă referitoare la drepturile de acces:

1. Accesați pagina **Configurare > Active Directory > Drepturi de acces**.
2. Selectați numele regulii de acces pentru a deschide fereastra de configurare.
3. Editați setările referitoare la drepturile de acces. Pentru mai multe informații, consultați Adăugarea drepturilor de acces.
4. Faceți clic pe **Save**. Regula de este salvată dacă nu există niciun impact asupra utilizatorului. În caz contrar, vi se solicită să specificați excepțiile privind conturile de utilizator. De exemplu, dacă actualizați prioritatea unei reguli, utilizatorii afectați pot trece la o altă regulă.
5. Dacă este necesar, selectați utilizatorii pe care doriți să îi excludeți. Pentru mai multe informații, consultați Excepții privind conturile de utilizator.
6. Efectuați clic pe **Confirmare**.

Notă
Puteți elimina asocierea dintre conturile de utilizator create prin intermediul unei reguli de acces prin modificarea drepturilor acestora în Control Center. Contul de utilizator nu poate fi asociat cu regula de acces.

Ștergerea mai multor conturi de utilizator

Pentru a șterge o regulă de acces:

1. Accesați pagina **Configurare > Active Directory > Drepturi de acces**.
2. Selectați regula de acces pe care doriți să o ștergeți și selectați ⊖ **Ștergere**. Se va afișa o fereastră de dialog prin care vi se va solicita să confirmați acțiunea dumneavoastră. Dacă există un impact asupra utilizatorului, vi se solicită să specificați excepțiile pentru contul utilizatorului. De exemplu, este recomandat să specificați eventualele excepții pentru utilizatorii afectați de ștergerea regulii.
3. Dacă este necesar, selectați utilizatorii pe care doriți să îi excludeți. Pentru mai multe informații, consultați Excepții la nivel de utilizator .
4. Efectuați clic pe **Confirmare**.

Ștergerea unei reguli va determina revocarea accesului la conturile de utilizator asociate. Toți utilizatorii creați prin intermediul acesteia vor fi șterși, cu excepția cazului în care există alte reguli care permit accesul acestora.

Excepții privind conturile de utilizator

Când adăugați, modificați sau ștergeți reguli de acces care afectează utilizatorii, este recomandat să specificați eventualele excepții privind conturile de utilizator. De asemenea, puteți vedea raționamentul și efectele asociate utilizatorilor afectați.

Specificați excepțiile la nivel de utilizator după cum urmează:

1. Selectați utilizatorii pe care doriți să îi excludeți. Sau bifați caseta din partea de sus a tabelului pentru a adăuga toți utilizatorii în listă.
2. Selectați **X** în caseta cu numele unui utilizator pentru a-l elimina din listă.

5.4. Resetarea parolelor de conectare

Titularii conturilor care își uită parola o pot reseta folosind link-ul de recuperare a parolei de pe pagina de autentificare. De asemenea, puteți reseta o parolă de conectare uitată prin editarea contului corespunzător din consolă.

Pentru a reseta parola de conectare pentru un utilizator:

1. Conectați-vă la Control Center.
2. Mergeți la pagina **Conturi**.
3. Faceți clic pe numele utilizatorului.

4. Scrieți parola nouă în câmpurile corespunzătoare (în secțiunea **Detalii**).
5. Faceți clic pe **Salvare** pentru a aplica modificările. Titularul contului va primi un e-mail cu noua parolă.

5.5. Administrarea autentificării de tip „two-factor”

Dând clic pe contul unul utilizator, veți putea vizualiza starea 2FA a acestuia (activată sau dezactivată) în secțiunea **Autentificare de tip „two-factor”**. Aveți la dispoziție următoarele acțiuni:

- **Resetați sau dezactivați autentificarea de tip „two-factor” a utilizatorului**. Dacă un utilizator având funcția 2FA activată a modificat sau a șters datele de pe dispozitivul mobil pierzând astfel codul secret:
  1. Introduceți parola dvs. pentru GravityZone în câmpul disponibil.
  2. Dați clic pe **Resetare** (când funcția 2FA este activată) sau pe **Dezactivare** (când funcția 2FA nu este activată).
  3. Un mesaj de confirmare vă va informa că autentificarea de tip „two-factor” a fost resetată / dezactivată pentru utilizatorul curent.

     După resetarea autentificării 2FA, atunci când această funcție este activată, în momentul conectării, se va afișa o fereastră de configurare prin care i se va solicita utilizatorului să configureze din nou autentificarea de tip „two-factor” folosind un nou cod secret.
- Dacă utilizatorul a dezactivat autentificarea 2FA și doriți să o activați, este necesar să solicitați utilizatorului să activeze această funcție din setările contului său.

Notă
Dacă aveți un cont de administrator de companie, puteți configura autentificarea în doi pași astfel încât să fie obligatorie pentru toate conturile GravityZone. Puteți găsi mai multe informații în Ghidul de instalare, secțiunea **Instalarea protecției > Instalarea și configurarea GravityZone > Configurarea setărilor Control Center**.

Important
Aplicația de autentificare aleasă (Google Authenticator, Microsoft Authenticator sau alt instrument de autentificare în doi pași de tip TOTP (Time-Based One-Time Password Algorithm) - compatibil(ă) cu standardul RFC6238) combină cheia secretă cu marcajul temporal actual al dispozitivului mobil pentru a genera un cod format

din 6 cifre. Rețineți că amprentele temporale de pe dispozitivul mobil și din aplicația GravityZone trebuie să se potrivească cu codul de șase cifre pentru a fi considerate valide. Pentru a evita orice probleme de sincronizare a amprentelor temporale, vă recomandăm să activați opțiunea de setare automată a datei și orei pe dispozitivul mobil.

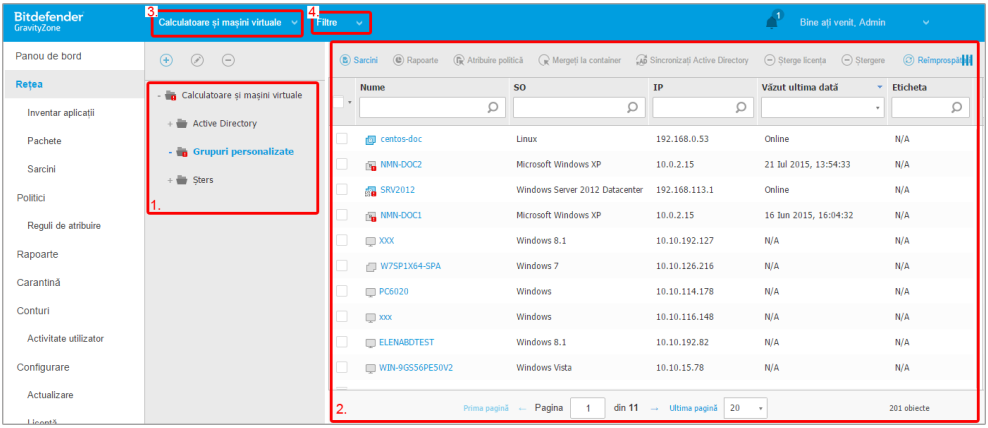
O altă metodă de verificare a modificărilor 2FA asociate conturilor de utilizator este de a accesa pagina **Conturi > Activitate utilizator** și de a filtra înregistrările din jurnalul de activități folosind următoarele filtre:

- Zonă > Conturi / Companie
- Acțiune > Modificate

Pentru informații suplimentare despre activarea autentificării 2FA, consultați„Administrarea contului dumneavoastră” (p. 25)

6. ADMINISTRAREA OBIECTELOR DIN REȚEA

Pagina **Rețea** oferă mai multe caracteristici pentru explorarea și administrarea fiecărui tip de obiect de rețea disponibil în Control Center (calculatoare, mașini virtuale și dispozitive mobile). Secțiunea **Rețea** include o interfață alcătuită din două panouri ce afișează starea în timp real a obiectelor din rețea:



Pagina Rețea

1. Fereastra din stânga afișează arborele de rețea disponibil. În funcție de ecranul de rețea selectat, această fereastră afișează infrastructura de rețea integrată cu Control Center, cum ar fi Active Directory, vCenter Server sau Xen Server.

   De asemenea, toate calculatoarele și mașinile virtuale detectate în rețeaua dvs. care nu corespund oricărei infrastructuri integrate sunt afișate în **Grupuri personalizate**.

   Toate stațiile de lucru șterse sunt stocate în directorul **Șterse**. Pentru informații suplimentare, consultați „Ștergerea stațiilor de lucru din inventarul rețelei” (p. 212).

   Notă
   Puteți vizualiza și gestiona numai grupurile pentru care dețineți drepturi de administrator.

2. Fereastra din dreapta afișează conținutul grupului selectat în fereastra din stânga. Această fereastră include o grilă, în care rândurile includ obiecte de rețea și coloanele afișează informații specifice pentru fiecare tip de obiect.

   Din această fereastră, puteți face următoarele:
   - Vizualizați informațiile detaliate referitoare la fiecare obiect din rețea din contul dumneavoastră. Puteți vizualiza starea fiecărui obiect verificând pictograma de lângă denumirea corespunzătoare. Mutați cursorul deasupra pictogramei pentru informații referitoare la aplicație. Faceți clic pe denumirea obiectului pentru afișarea unei ferestre care include detalii specifice.

     Fiecare tip de obiect, cum ar fi un calculator, o mașină virtuală sau un folder, este reprezentat printr-o pictogramă specifică. De asemenea, fiecare obiect din rețea poate avea o anumită stare de administrare, securitate, conectivitate și așa mai departe. Pentru detalii privind descrierea fiecărei pictograme a obiectelor din rețea și a stărilor disponibile, consultați „Tipurile și stările obiectelor de rețea” (p. 565).
   - Folosiți Bara de instrumente pentru acțiune din partea de sus a tabelului pentru efectuarea unor operațiuni specifice pentru fiecare obiect din rețea (cum ar fi rularea sarcinilor, crearea rapoartelor, alocarea politicilor și ștergere) și opțiunea de reîmprospătare a datelor din tabel.
3. Selectorul de vederi din partea de sus a paginii de rețea permite comutarea între diferitele conținuturi ale ale inventarului de rețea, conform tipului de terminal cu care doriți să lucrați.
4. Meniul **Filtre** disponibil în partea de sus a secțiunilor de rețea vă ajută să afișați cu ușurință numai anumite obiecte din rețea, oferindu-vă mai multe criterii de filtrare. Opțiunile din meniul **Filteree** se referă la ecranul rețelei selectat în momentul respectiv.

Din secțiunea **Rețea**, puteți administra, de asemenea, pachetele de instalare și sarcinile pentru fiecare tip de obiect din rețea.

Notă
Pentru mai multe informații referitoare la pachetele de instalare, consultați Ghidul de instalare GravityZone.

Pentru informații detaliate referitoare la obiectele din rețea, consultați:

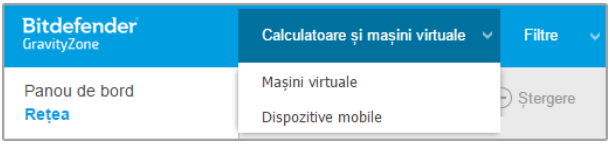
- „Lucrul cu Ecranele de rețea” (p. 44)
- „Calculatoare” (p. 47)
- „Mașini virtuale” (p. 107)

- „Dispozitive mobile” (p. 167)
- „Inventarul de patch-uri” (p. 199)
- „Vizualizarea și administrarea sarcinilor” (p. 207)
- „Ștergerea stațiilor de lucru din inventarul rețelei” (p. 212)
- „Configurarea setărilor de rețea” (p. 213)
- „Configurarea setărilor Security Server” (p. 216)
- „Manager Credențiale” (p. 217)

6.1. Lucrul cu Ecranele de rețea

Diferitele tipuri de stații de lucru disponibile în Control Center sunt grupate în pagina **Rețea**, pe diferite tipuri de vizualizări de rețea. Fiecare vizualizare a rețelei afișează un anumit tip de infrastructură de rețea, în funcție de stația de lucru pe care doriți să o administrați.

Pentru a modifica tipul de vedere asupra rețelei, mergeți în partea din stânga sus a paginii **Rețea** și faceți clic pe selectorul de vederi:



Opțiunea de selectare a vederilor

Sunt disponibile următoarele vizualizări de rețea:

- Calculatoare și mașini virtuale
- Mașini virtuale
- Dispozitive mobile

6.1.1. Calculatoare și mașini virtuale

Acest ecran este destinat calculatoarelor și mașinilor virtuale integrate în Active Directory, care oferă anumite acțiuni și opțiuni de filtrare pentru administrarea calculatoarelor din rețeaua dvs. Dacă integrarea cu Active Directory este disponibilă, se încarcă arborele Active Directory, alături de stațiile de lucru corespunzătoare.

Când lucrați în ecranul **Calculatoare și Mașini virtuale**, puteți sincroniza în orice moment conținutul Control Center cu Active Directory folosind butonul **Sincronizare cu Active Directory** din Bara de instrumente Acțiuni.

De asemenea, toate calculatoarele și mașinile virtuale care nu sunt integrate cu Active Directory sunt grupate în Grupurile personalizate. Acest folder poate conține următoarele tipuri de stații de lucru:

- Calculatoarele și mașinile virtuale disponibile în rețeaua dvs. în afara Active Directory.
- Mașinile virtuale integrate dintr-o infrastructură virtualizată disponibilă în rețeaua dvs.
- Serverele de securitate instalate deja și configurate pe o gazdă din rețeaua dvs.

Notă
Dacă este disponibilă o infrastructură virtualizată, puteți instala și administra Serverele de securitate din vizualizarea **Mașini virtuale**. În caz contrar, Serverele de securitate pot fi instalate și configurate doar local pe gazdă.

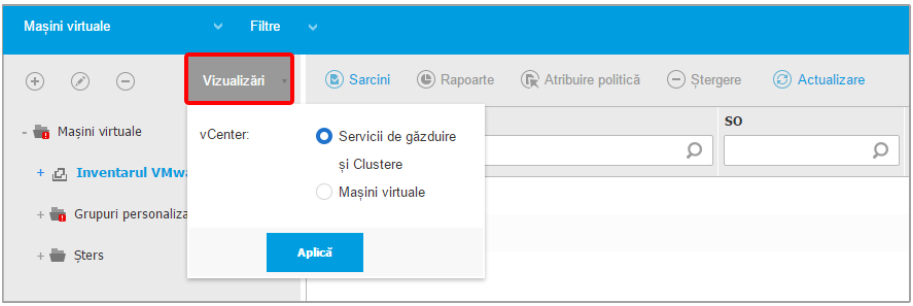
Important
Alocarea politicilor către mașinile virtuale din ecranul **Calculatoare și Mașini virtuale** poate fi restricționată de către administratorul soluției GravityZone la configurarea Serverului vCenter sau a unui Server Xen pe pagina **Configurare > Furnizori virtualizare**. Pentru informații suplimentare, consultați capitolul **Instalarea protecției > Instalarea și configurarea GravityZone** din Ghidul de instalare GravityZone.

6.1.2. Mașini virtuale

Acest ecran este destinat afișării integrărilor dvs. cu infrastructura virtualizată. Opțiunile de filtrare disponibile în acest ecran vă permit să alegeți criterii speciale pentru afișarea entităților din mediul virtual.

Puteți vizualiza inventarele virtuale Nutanix, VMware sau Citrix în fereastra din stânga.

În partea din sus a ferestrei din stânga, veți găsi meniul **Vizualizări** care vă permite să selectați modul de afișare al inventarelor virtuale.



Pagina Rețea - Vizualizările Mașinilor virtuale

Toate mașinile virtuale din rețeaua dvs. care nu sunt integrate într-o infrastructură virtuală sunt afișate în **Grupuri clienți**.

Pentru a avea acces la infrastructura virtualizată integrată cu Control Center, trebuie să furnizați datele de utilizator pentru fiecare sistem vCenter Server disponibil. Control Center folosește datele dumneavoastră pentru a se conecta la infrastructura virtualizată, afișând doar resursele la care aveți acces (așa cum sunt acestea definite în vCenter Server). Dacă nu ați specificat datele de autentificare, când încercați să parcurgeți inventarul unui vCenter Server vi se va solicita să le introduceți. După ce ați introdus datele, acestea sunt salvate în secțiunea Admnistrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

6.1.3. Dispozitive mobile

Această fereastră este destinată exclusiv vizualizării și administrării dispozitivelor mobile disponibile în rețea, incluzând acțiuni specifice și opțiuni de filtrare.

În acest ecran specific, puteți afișa entitățile din rețea după utilizatori și dispozitive.

Fereastra rețelei afișează structura arborelui Active Directory, dacă este disponibilă. În acest caz, toți utilizatorii Active Directory vor apărea în inventarul dvs. de rețea, alături de dispozitivele mobile alocate acestora.

Notă
Detaliile de utilizator Active Directory sunt încărcate automat și nu pot fi modificate.

Secțiunea Grupuri personalizate conține toți utilizatorii dispozitivelor mobile pe care i-ați adăugat manual în Control Center.

6.2. Calculatoare

Pentru a vizualiza calculatoarele din contul dumneavoastră, megeți la pagina **Rețea** și selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.

Puteți vizualiza structura rețelei disponibilă în fereastra din stânga, precum și detaliile referitoare la fiecare stație de lucru, în fereastra din dreapta.

Inițial, toate calculatoarele și mașinile virtuale identificate în rețea sunt afișate ca neadministrate, pentru a putea instala protecția pe acestea de la distanță.

Pentru a personaliza detaliile calculatorului afișate în tabel:

1. Faceți clic pe butonul **Coloane** din partea dreaptă a Barei de instrumente Acțiuni.
2. Selectați coloanele pe care doriți să le vizualizați.
3. Faceți clic pe butonul **Resetare** pentru a reveni la vizualizare implicită coloane.

Din pagina **Rețea**, puteți administra calculatoarele după cum urmează:

- Verificați starea calculatorului
- Vizualizați detaliile calculatorului
- Organizați calculatoarele în grupuri
- Sortare, filtrare și căutare
- Administrare patch-uri
- Executarea sarcinilor
- Creați rapoarte rapide
- Atribuie politici
- Sincronizare cu Active Directory

Pentru vedea cele mai recente informații din tabel, faceți clic pe butonul **Reîmprospătare** din colțul din stânga - jos al tabelului. Acest lucru poate fi necesar atunci când petreceți mai mult timp pe pagină.

6.2.1. Verificarea Stării calculatoarelor

Fiecare calculator este reprezentat în pagina de rețea prin intermediul unei pictograme specifice tipului și stării acesteia.

Consultați „Tipurile și stările obiectelor de rețea” (p. 565) pentru o listă a tuturor tipurilor de pictograme și stărilor disponibile.

Pentru informații detaliate referitoare la stare, consultați:

- Stare administrare

- Stare conectivitate
- Stare securitate

Stare administrare

Calculatoarele pot avea următoarele stări de administrare:

- **Administrat** - calculatoarele pe care este instalat agentul de securitate.
- **Repornire în așteptare** - stații de lucru care necesită o repornire a sistemului după instalarea sau actualizarea protecției Bitdefender.
- **Neadministrat** - calculatoarele detectate care agentul de securitate nu a fost instalat încă.
- **Șters** - calculatoarele pe care le-ați șters din Control Center. Pentru mai multe informații, consultați capitolul „Ștergerea stațiilor de lucru din inventarul rețelei” (p. 212).

Stare conectivitate

Starea de conectivitate se referă exclusiv la calculatoarele administrate. Din acest punct de vedere, calculatoarele administrate pot fi:

- **Online**. O pictogramă albastră indică faptul că un calculator este online.
- **Neconectat (offline)**. O pictogramă gri indică faptul că un calculator este offline.

Un calculator este offline dacă agentul de securitate este inactiv mai mult de 5 minute. Posibile motive pentru care calculatoarele apar ca fiind offline:

- Calculatorul este oprit, în stare de așteptare sau de hibernare.

  Notă
  Calculatoarele apar online când sunt blocate sau utilizatorul este deconectat.

- Agentul de securitate nu are conectivitate cu Serverul de comunicări GravityZone:
  - Calculatorul poate fi deconectat de la rețea.
  - Un firewall de rețea sau router poate obstrucționa comunicarea dintre agentul de securitate și Serverul de comunicații GravityZone.
  - Calculatorul este în spatele unui server proxy și setările proxy nu au fost configurate corespunzător în politica aplicată.

Avertisment
Pentru calculatoarele din spatele unui server proxy, setările proxy trebuie configurate corect în pachetul de instalare al agentului de securitate. În caz contrar, calculatorul nu va comunica cu consola GravityZone și va apărea întotdeauna offline, indiferent dacă se aplică sau nu o politică având setările proxy corecte după instalare.

- Este posibil ca agentul de securitate să nu funcționeze corect.

Pentru a afla cât timp au fost inactive calculatoarele:

1. Se afișează doar calculatoarele administrate. Faceți clic pe meniul **Filtre** din partea de sus a tabelului, selectați toate opțiunile "Administrate" dorite din secțiunea **Securitate**, alegeți opțiunea **Toate articolele recursiv** din secțiunea **Adâncime** și faceți clic pe **Salvare**.
2. Faceți clic pe titlul coloanei **Văzut ultima dată** pentru sortarea calculatoarelor în funcție de perioada de inactivitate.

Puteți ignora perioadele de inactivitate mai scurte (minute, ore), deoarece este posibil ca acestea să fie rezultatul unei stări temporare. De exemplu, calculatorul este în prezent oprit.

Perioadele de inactivitate mai lungi (zile, săptămâni) indică, în general, o problemă cu calculatorul.

Notă
Se recomandă reîmprospătarea periodică a tabelului rețelei, pentru actualizarea informațiilor referitoare la stațiile de lucru cu cele mai recente modificări.

Stare securitate

Starea de securitate se referă exclusiv la calculatoarele administrate. Puteți găsi calculatoarele cu probleme de securitate verificând pictogramele de stare care afișează un simbol de avertizare:

- Calculator administrat, probleme existente, online.
- Calculator administrat, probleme existente, offline.

Un calculator are probleme de securitate dacă se aplică cel puțin una dintre situațiile de mai jos:

- Protecția contra malware este dezactivată.
- Licența a expirat.

- Agentul de securitate nu este actualizat.
- Conținutul de securitate este expirat.
- S-a detectat malware.
- Conexiunea cu Serviciile Cloud Bitdefender nu a putut fi stabilită din următoarele motive posibile:
  - Calculagtorul are probleme de conectivitate la internet.
  - Un firewall al rețelei blochează conexiunea cu Serviciile Ckoud Bitdefender.
  - Portul 443, necesar pentru comunicarea cu Serviciile Cloud Bitdefender, este închis.

  În aces caz, protecția contra programelor periculoase se bazează exclusiv pe motoarele locale când scanarea in-the-cloud este deconectată, ceea ce înseamnă că agentul de securitate nu poate oferi protecție completă în timp real.

Dacă identificați un calculator cu probleme de securitate, faceți clic pe denumire pentru afișarea ferestrei **Informații**. Puteți identifica aspectele de securitate prin pictograma ! . Asigurați-vă că ați consultat informațiile privind securitatea furnizate pe toate filele de pe pagina pentru informații. Afișați informațiile oferite de pictogramă pentru detalii suplimentare. Este posibil să fie necesare investigații locale suplimentare.

Notă
Se recomandă reîmprospătarea periodică a tabelului rețelei, pentru actualizarea informațiilor referitoare la stațiile de lucru cu cele mai recente modificări.

6.2.2. Vizualizarea detaliilor calculatorului

Puteți obține informații detaliate despre fiecare computer pe pagina **Rețea**, după cum urmează:

- Verificarea paginii **Rețea**
- Verificarea ferestrei **Informații**

Verificarea paginii Rețea

Pentru a afla detalii despre un computer, consultați informațiile disponibile în tabelul de pe panoul din dreapta de pe pagina **Rețea**.

Puteți adăuga sau elimina coloane cuprinzând informații despre stația de lucru efectuând clic pe butonul III **Coloane** din partea dreaptă sus a panoului.

1. Mergeți la pagina **Rețea**.

2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga.

   Toate stațiile de lucru disponibile în grupul selectat se afișează în tabelul din fereastra din dreapta.
4. Puteți detecta cu ușurință starea calculatorului, verificând pictograma corespunzătoare. Pentru informații detaliate, consultați capitolul „Verificarea Stării calculatoarelor" (p. 47).
5. Verificați informațiile afișate în coloane pentru fiecare calculator.

   Folosiți antetul coloanei pentru a căuta anumite stații de lucru, conform criteriilor disponibile:

   - **Nume**: denumirea stației de lucru.
   - **FQDN**: nume de domeniu calificat complet care include denumirea gazdei și numele de domeniu.
   - **OS**: sistemul de operare instalat pe stația de lucru.
   - **IP**: adresa IP a stației de lucru.
   - **Văzut ultima dată**: data și ora la care stația de lucru a fost văzută online ultima dată.

     Notă
     Este important să monitorizați câmpul **Văzut ultima dată** deoarece intervalele lungi de inactivitate pot indica o problemă de comunicare sau un calculator deconectat.

   - **Etichetă**: un șir personalizat cu informații suplimentare despre stația de lucru. Puteți adăuga o etichetă în fereastra **Informații** a stației de lucru și să o folosiți apoi la căutare.
   - **Politica**: politica aplicată stației de lucru, cu un link pentru vizualizarea sau modificarea setările pentru politică.

Verificarea ferestrei Informații

Pe panoul din dreapta de pe pagina **Rețea**, efectuați clic pe numele stației de lucru care vă interesează, pentru afișarea ferestrei **Informații**. Pe această fereastră se afișează doar informațiile disponibile pentru stația de lucru selectată, grupate pe diverse file.

Aveți în continuare lista completă de informații pe care le puteți găsi în fereastra **Informații**, în funcție de stația de lucru introdusă și informațiile de securitate specifice acesteia.

Fila generală

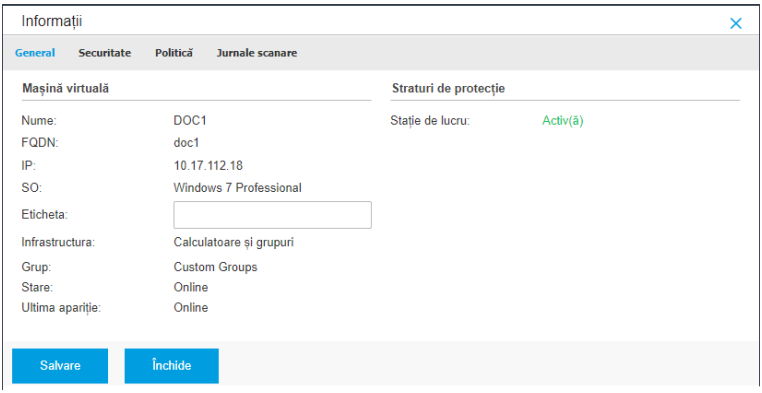
- Informații generale referitoare la calculator, cum ar fi numele, informații FQDN, adresa IP, sistemul de operare, infrastructura, grupul mamă și starea curentă a conexiunii.

  În această secțiune puteți desemna stația de lucru cu o etichetă. Veți putea găsi rapid stații de lucru cu aceeași etichetă și veți putea acționa asupra lor indiferent unde sunt ele localizate în rețea. Pentru mai multe informați despre cum se filtrează stațiile de lucru, consultați „Sortarea, filtrarea și căutarea calculatoarelor” (p. 66).

- Informații privind straturile de protecție, inclusiv lista cu tehnologiile de securitate pe care le obțineți cu soluția GravityZone, precum și situația licențelor acestora care poate fi:
  - **Disponibilă / Activă** – cheia de licență pentru acest strat de protecție este activă la stația de lucru.
  - **Expirată** – cheia de licență pentru acest strat de protecție a expirat.
  - **În așteptare** – cheia de licență nu a fost confirmată încă.

  Notă
  Informații suplimentare referitoare la straturile de protecție sunt disponibile în secțiunea **Protecție**.

- **Conexiune la releu**: numele, IP-ul și eticheta releului la care este conectată stația de lucru, dacă este cazul.



Fereastra de informații - secțiunea General

Fila pentru protecție

Această filă conține detalii privind protecția aplicată la nivelul endpoint-ului, referindu-se la:

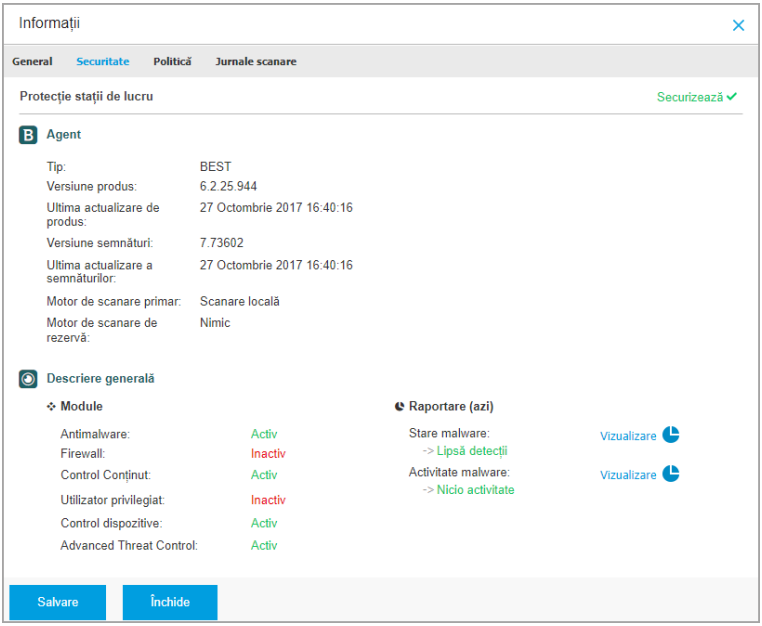
- Informații despre agentul de securitate, cum ar fi numele produsului, versiunea, statusul actualizării și locațiile actualizărilor, precum și configurația motoarelor de scanare și versiunile conținutului de securitate.For protecție Exchange, este disponibilă și versiunea motorului antispam.
- Starea de securitate pentru fiecare strat de protecție. Această stare apare în partea dreaptă a numelui stratului de protecție:
  - **Securizat**, când nu există probleme de securitate raportate pentru stațiile de lucru la care s-a aplicat strat de protecție.
  - **Vulnerabil**, când există probleme de securitate raportate pentru stațiile de lucru la care s-a aplicat strat de protecție. Pentru mai multe detalii, vă rugăm consultați „Stare securitate” (p. 49).
- Security Server asociat. Fiecare Security Server asociat este afișat în cazul configurării fără agent sau când motoarele de scanare ale agenților de securitate sunt setate pentru a utiliza scanarea la distanță. Informațiile Security Server vă ajută să identificați aplicația virtuală și să obțineți starea de actualizare a acesteia.

- Starea modulelor de protecție. Puteți vizualiza cu ușurință modulele de protecție care au fost instalate pe stația de lucru și, de asemenea, starea modulelor disponibile (**Pornit/Oprit**) setată prin intermediul politicii aplicate.
- O prezentare rapidă privind activitatea modulelor și raportarea programelor periculoase pe parcursul zilei în curs.

  Executați clic pe linkul **Vizualizare** pentru a accesa opțiunile de raportare și genera apoi raportul. Pentru mai multe informații, consultați „Crearea rapoartelor” (p. 495)
- Informații privind stratul de protecție Sandbox Analyzer:
  - Situația utilizărilor Sandbox Analyzer la stația de lucru, afișată în partea dreaptă a ferestrei:
    - **Active**: Sandbox Analyzer este licențiat (disponibil) și activat prin intermediul politicii pentru respectiva stație de lucru.
    - **Inactiv**: Sandbox Analyzer este licențiat (disponibil) dar nu este activat prin intermediul politicii pentru respectiva stație de lucru.
  - Denumirea agentului care acționează ca senzor de alimentare.
  - Starea modulului la stația de lucru:
    - **Pornit** - Sandbox Analyzer este activat prin intermediul politicii pentru respectiva stație de lucru.
    - **Oprit** - Sandbox Analyzer nu este activat pentru respectiva stație de lucru prin intermediul politicii.
  - Amenințările detectate în ultima săptămână efectuând clic pe linkul **Vizualizare** pentru accesarea raportului.
- Informațiile suplimentare cu privire la modulul de Criptare, de exemplu:
  - Volume detectate (menționând unitatea boot).
  - Starea criptării pentru fiecare volum (care poate fi **Criptat**, **Criptare în curs**, **Decriptare în curs**, **Necriptat**, **Blocat** or **În pauză**).

    Efectuați clic pe linkul **Recuperare** pentru a extrage cheia de recuperare pentru volumul criptat asociat. Pentru detalii referitoare la extragerea cheilor de recuperare, consultați „” (p. 106).

- Starea telemetriei de securitate, care vă informează dacă conexiunea dintre endpoint și serverul SIEM este activată și funcționează, este dezactivată sau prezintă probleme.



Fereastra pentru informații - Fila pentru protecție

Fila pentru politici

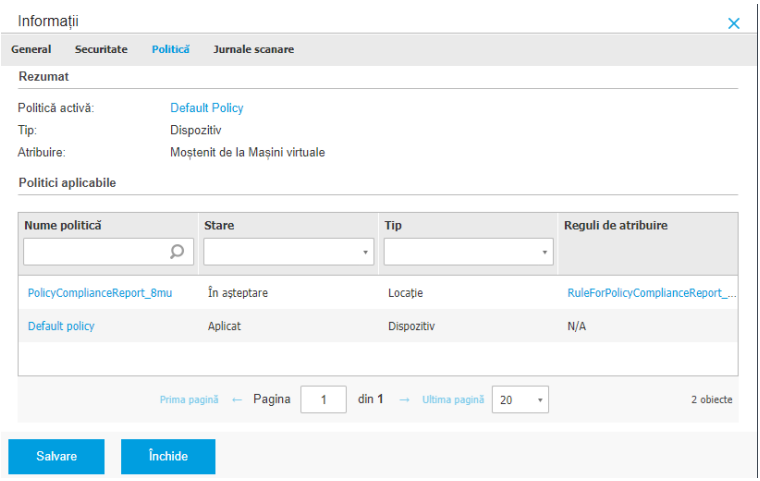
Unei stații de lucru i se pot aplica una sau mai multe politici, însă doar o singură politică poate fi activă la un moment dat. Fila **Polică** afișează informații despre toate politicile aplicabile acelei stații de lucru.

- Numele politicii active. Faceți clic pe denumirea politicii pentru a deschide un șablon și a-i vizualiza setările.
- Tipul politicii active, care poate fi:
  - **Dispozitiv**: când politica este atribuită manual stației de lucru de către administratorul de rețea.

- **Locație**: o politică bazată pe reguli, atribuită automat stației de lucru dacă setările de rețea ale respectivei stații de lucru corespund condițiilor regulii de atribuire existente.

  De exemplu, un laptop are atribuite două politici în funcție de locație: una denumită `Birou`, care este activă atunci când se conectează la rețeaua LAN a companiei, și `Mobilitate`, care devine activă atunci când utilizatorul lucrează de la distanță și se conectează la alte rețele.
- **Utilizator**: o politică bazată pe reguli, atribuită automat stației de lucru dacă corespunde țintei Active Directory specificată într-o regulă de atribuire existentă.
- **Extern (NSX)**: când politica este definită în mediul VMware NSX.

- Tipul de atribuire a politicii active, care poate fi:
  - **Direct**: când politica este aplicată direct stației de lucru.
  - **Preluată**: când stația de lucru preia politica de la un grup părinte.
- **Politici aplicabile**: afișează lista politicilor legate de regulile de atribuire existente. Aceste politici se pot aplica stației de lucru când aceasta corespunde condițiilor din regulile de atribuire aferente.

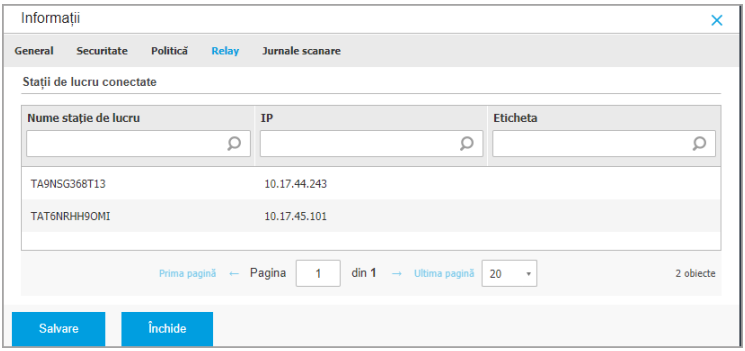


Fereastra de informații - secțiunea Politică

Pentru mai multe informații privind politicile, consultați„Modificarea setărilor politicii” (p. 234)

Fila Endpoint-uri conectate

Fila **Endpoint-uri conectate** este disponibilă doar pentru endpoint-urile cu rol de releu. Această secțiune afișează informații referitoare la stațiile de lucru conectate la releul curent, cum ar fi denumirea, adresa IP și eticheta.

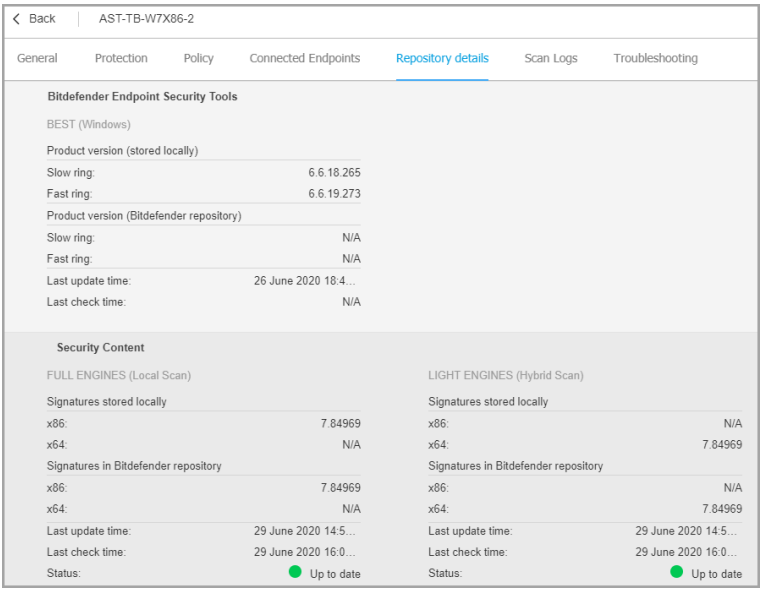


Fereastra Informații - Fila Endpoint-uri conectate

Fila Detalii depozit

Fila **Detalii depozit** este disponibilă doar pentru endpoint-urile cu rol de releu și afișează informații despre actualizările și conținutul de securitate al agentului de securitate.

Fila include informații despre produs și versiunile de semnături stocate pe releu și cele disponibile în depozitul oficial, cicluri de actualizări, data și ora actualizării și ultima verificare pentru versiuni noi.



Fereastra Informații - Fila Detalii depozit

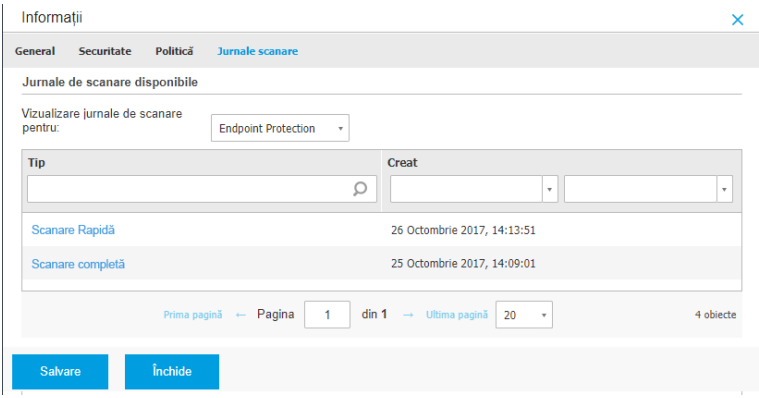
Fila pentru scanare jurnale

În secțiunea **Jurnale scanări** se afișează informații detaliate referitoare la toate sarcinile de scanare efectuate pe stația de lucru.

Jurnalele sunt grupate după stratul de protecție și puteți selecta din meniul derulant pentru ce strat doriți să afișați jurnalele.

Faceți clic pe sarcina de scanarea care vă interesează și se va deschide jurnalul într-o nouă pagină a browserului.

Dacă sunt disponibile multe jurnale de scanare, acestea pot ocupa mai multe pagini. Pentru a trece de la o pagină la alta, folosiți opțiunile de navigație din partea de jos a tabelului. Dacă există prea multe intrări, puteți folosi opțiunile de filtrare disponibile în partea de sus a tabelului.

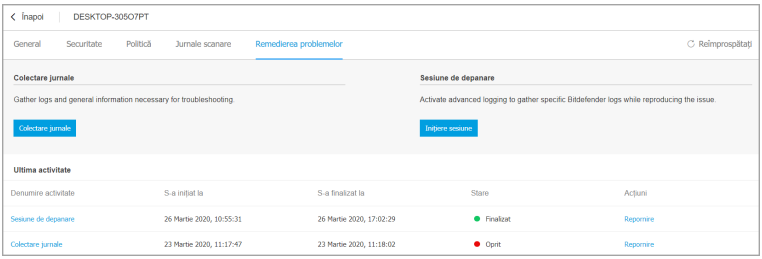


Fereastra de informații - secțiunea Jurnale de scanare

Fila de remediere a problemelor

Această secțiune este dedicată activității de remediere a problemelor asociate agentului. Puteți colecta jurnale generale sau specifice din secțiunea de verificare a endpoint-urilor sau puteți acționa asupra evenimentelor curente de remediere a problemelor și vizualiza activitatea anterioară.

Important
Remedierea problemelor este disponibilă pentru mașinile cu sistem de operare Windows, Linux,macOS și toate tipurile de servere de securitate.



Fereastră de informare - Fila de remediere a problemelor

- **Colectare jurnale**

  Această opțiune vă permite să colectați o serie de jurnale și informații generale necesare pentru remedierea problemelor, cum ar fi setările, modulele active sau

politica aplicată specifică mașinii vizate. Toate datele generate sunt salvate într-o arhivă.

Se recomandă utilizarea acestei opțiuni atunci când cauza problemei este neclară.

Pentru a începe procesul de remediere a problemelor:

1. Clic pe butonul**Colectare jurnale**. Este afișată o fereastră de configurare.
2. Din secțiunea **Stocarea jurnalelor**, selectați o locație de stocare:
   - **Mașină vizată**: arhiva jurnalelor este salvată în calea locală furnizată. Calea nu poate fi configurată pentru Serverele de securitate.
   - **Locație partajată în rețea**: arhiva jurnalelor este salvată în calea locală furnizată din locația partajată din rețea.

   Puteți folosi opțiunea **Salvare jurnale și pe mașina țintă** pentru a salva o copie de siguranță a arhivei de jurnale pe mașina afectată.
3. Completați informațiile necesare (calea locală, datele de autentificare pentru locațiile partajate în rețea, calea către locația partajată) în funcție de locația selectată.
4. Clic pe butonul**Colectare jurnale**.

- **Sesiune de depanare**

  Folosind sesiunea de Depanare, puteți activa autentificarea avansată pe mașina vizată pentru a colecta anumite jurnale, reproducând totodată problema.

  Ar trebui să utilizați această opțiune după ce descoperiți ce modul cauzează probleme sau la recomandarea serviciului Bitdefender Enterprise Support. Toate datele generate sunt salvate într-o arhivă.

  Pentru a începe procesul de remediere a problemelor:

  1. Clic pe butonul**Începere sesiune**. Este afișată o fereastră de configurare.
  2. În secțiunea **Tipul problemei**, selectați problema care considerați că afectează mașina respectivă.

     Tipuri de probleme pentru mașinile Windows și macOS:

Tip de problemă	Utilizare
Antimalware (scanare la accesare și la cerere)	– Încetinirea generală a endpoint-ului

Tip de problemă	Utilizare
	– Un program sau o resursă de sistem necesită prea mult timp de răspuns – Un proces de scanare durează mai mult decât în mod obișnuit – Eroare lipsă conexiune la serviciul de securitate al sistemului gazdă
Erori la actualizare	– S-au primit mesaje de eroare în timpul actualizării produsului sau conținutului de securitate
Control Conținut (scanare trafic și control utilizator)	– Acest site web nu se încarcă – Elementele paginii web nu sunt afișate corespunzător
Conectivitate Servicii Cloud	– Endpoint-ul nu are conectivitate la serviciile Cloud Bitdefender
Probleme generale ale produsului (nivel ridicat de detaliere a jurnalelor)	– Reproduceți o problemă generică raportată cu jurnale detaliate

Tipuri de probleme pentru mașinile Linux:

Tip de problemă	Utilizare
Antimalware și actualizări	– Un proces de scanare durează mai mult decât în mod normal și consumă mai multe resurse – S-au primit mesaje de eroare în timpul actualizării produsului sau conținutului de securitate – Endpoint-ul nu se poate conecta la consola GravityZone.
Probleme generale ale produsului (nivel ridicat de detaliere a jurnalelor)	– Reproduceți o problemă generică raportată cu jurnale detaliate

Tipuri de probleme pentru Serverele de securitate:

Tip de problemă	Utilizare
Antimalware (scanare la accesare și la cerere)	Orice comportament neașteptat al Serverului de securitate, inclusiv: – Mașinile virtuale nu sunt protejate corespunzător – Sarcinile de scanare antimalware nu rulează sau durează mai mult față de cum se preconiza – Actualizările produsului nu sunt instalate corespunzător – Defecțiune generică a Serverului de securitate (procesele bd daemon nu rulează)
Comunicarea cu GravityZone Control Center	Un comportament neașteptat observat din partea consolei GravityZone: – Mașinile virtuale nu sunt raportate corespunzător în consola GravityZone – Probleme cu politicile (politicile nu sunt aplicate) – Serverul de securitate nu poate stabili o conexiune cu consola GravityZone **Notă** Utilizați această metodă la recomandarea din partea Bitdefender Enterprise Support.

3. Pentru **Durata sesiunii de depanare**, alegeți intervalul de timp după care să fie oprită automat sesiunea de depanare.

   Notă
   Se recomandă oprirea manuală a sesiunii folosind opțiunea **Încheiere sesiune** imediat după ce reproduceți problema.

4. Din secțiunea **Stocarea jurnalelor**, selectați o locație de stocare:

– **Mașină vizată**: arhiva jurnalelor este salvată în calea locală furnizată. Calea nu poate fi configurată pentru Serverele de securitate.

– **Locație partajată în rețea**: arhiva jurnalelor este salvată în calea locală furnizată din locația partajată din rețea.

Puteți folosi opțiunea **Salvare jurnale și pe mașina țintă** pentru a salva o copie de siguranță a arhivei de jurnale pe mașina afectată.

5. Completați informațiile necesare (calea locală, datele de autentificare pentru locațiile partajate în rețea, calea către locația partajată) în funcție de locația selectată.
6. Clic pe butonul**Începere sesiune**.

Important
Nu puteți rula simultan mai multe procese de remediere a problemelor (**Colectare jurnale** / **Sesiune de depanare**) pe mașina afectată.

- **Istoric de remediere a problemelor**

Secțiunea **Ultima activitate** prezintă activitatea de remediere a problemelor de pe endpoint-ul afectat. În tabel sunt afișate doar ultimele 10 evenimente de remediere a problemelor în ordine cronologică inversă, iar activitățile mai vechi de 30 de zile sunt șterse automat.

În tabel sunt afișate detaliile fiecărui proces de remediere a problemelor.

Procesul are statusuri principale și intermediare. În funcție de setările personalizate, se poate afișa următorul status asupra căruia vi se solicită să acționați:

– **În desfășurare (Pregătit pentru reproducerea problemei)** – accesați manual sau de la distanță mașina afectată și reproduceți problema.

Aveți numeroase opțiuni pentru a opri procesul de remediere a problemelor, după cum urmează:

– **Încheiere sesiune**: încheie sesiunea de depanare și procesul de colectare pe mașina vizată, salvând totodată datele colectate în locația de stocare specificată.

  Se recomandă folosirea acestei opțiuni imediat după ce ați reprodus problema.

– **Anulare**: această opțiune anulează procesul și niciun jurnal nu este colectat.

Folosiți această opțiune atunci când nu doriți să colectați jurnale de pe mașina vizată.

– **Oprire forțată**: oprește forțat procesul de remediere a problemelor.

  Folosiți această opțiune atunci când anularea sesiunii durează prea mult sau dacă mașina vizată nu răspunde și veți putea începe din nou sesiunea în câteva minute.

Pentru a reîncepe procesul de remediere a problemelor:

– **Repornire**: acest buton, asociat cu fiecare eveniment și localizat în secțiunea **Acțiuni** repornește activitatea selectată de remediere a problemelor, păstrând setările anterioare ale acesteia.

Important

– Pentru a vă asigura că în consolă se afișează cele mai recente informații, folosiți butonul **Reîmprospătare** din partea din dreapta sus a paginii de **Remediere a problemelor**.

– Pentru informații suplimentare despre un anumit eveniment, clic pe numele evenimentului din tabel.

6.2.3. Organizarea calculatoarelor în grupuri

Puteți gestiona grupurile de calculatoare în fereastra din stânga a paginii **Rețea**.

Beneficiul major al acestei funcții este acela că puteți utiliza politicile de grup pentru a începlini diferite cerințe de securitate.

Calculatoarele importate din Active Directory sunt grupate în folderul **Active Directory**. Grupurile Active Directory nu pot fi editate. Puteți doar să vizualizați și să administrați calculatoarele corespunzătoare.

Toate calculatoarele care nu fac parte din Active Directory descoperite în rețea sunt amplasate în **Grupuri personalizate**, unde le puteți organiza în grupuri, după cum doriți. În **Grupuri personalizate** puteți crea, șterge, redenumi și muta grupuri de calculatoare într-o structură de tip arbore predefinită.

Notă

- Un grup poate include atât calculatoare, cât și alte grupuri.
- Dacă selectați un grup din fereastra din stânga, puteți vizualiza toate calculatoarele, cu excepția celor din sub-grupuri. Pentru a vizualiza toate

calculatoarele din grup și din sub-grupurile acestuia, faceți clic pe meniul **Filtre** din partea de sus din dreapta sus a tabelului și selectați **Toate obiectele recursiv** din secțiunea **Adâncime**.

Crearea unui nou grup

Înainte de a începe să creați grupuri, gândiți-vă la motivele pentru care aveți nevoie de ele și creați o schemă de grupare. De exemplu, puteți grupa stațiile de lucru pe baza unuia sau mai multora dintre următoarele criterii:

- Structura organizatorică (Vânzări, Marketing, Asigurarea calității, Dezvoltare software, Management etc.).
- Necesitățile de securitate (desktopuri, laptopuri, servere etc.).
- Locația (sediu central, birouri locale, personal la distanță, birouri de acasă etc.).

Pentru a organiza rețeaua în grupuri:

1. Selectați **Grupuri personalizate** din fereastra din stânga.
2. Faceți clic pe butonul **Adăugare grup** din partea de sus a ferestrei din stânga.
3. Introduceți o denumire sugestivă pentru grup și faceți clic pe **OK**. Noul grup va fi afișat în directorul **Grupuri personalizate**.

Redenumirea unui grup

Pentru a redenumi un grup:

1. Selectați grupul din fereastra din stânga.
2. Faceți clic pe butonul **Editare grup** din partea de sus a ferestrei din stânga.
3. Introduceți noua denumire în câmpul corespunzător.
4. Faceți clic pe **OK** pentru confirmare.

Mutarea grupurilor și calculatoarelor

Puteți muta entitățile în **Grupuri personalizate** oriunde în ierarhia grupului. Pentru a muta o entitate, trageți-o și inserați-o din fereastra din dreapta în grupul dorit din fereastra din stânga.

Notă

Entitatea mutată va moșteni setările de politică ale noului grup părinte, cu excepția cazului în care i s-a atribuit o politică diferită. Pentru detalii privind preluarea politicii, consultați „Politici de securitate” (p. 220).

Ștergerea unui grup

Ștergerea unui grup reprezintă o acțiune definitivă. În consecință, agentul de securitate instalat pe stația de lucru țintă va fi eliminat.

Pentru a șterge un grup:

1. Faceți clic pe grupul gol din partea stângă a **paginii Rețea**.
2. Faceți clic pe butonul **Ștergere grup** din partea de sus a ferestrei din stânga. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

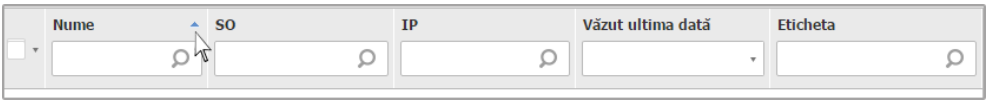
6.2.4. Sortarea, filtrarea și căutarea calculatoarelor

În funcție de numărul de stații de lucru, tabelul cu stații de lucru se poate întinde pe mai multe pagini (implicit, sunt afișate doar 20 de intrări pe pagină). Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului. Pentru a modifica numărul de intrări afișate pe pagină, selectați o opțiune din meniul de lângă butoanele de navigație.

Dacă există prea multe intrări, puteți folosi casetele de căutare de sub titlurile coloanelor sau meniul **Filtre** din partea de sus a paginii, pentru a afișa doar entitățile care vă interesează. De exemplu, puteți modifica o căutarea unui anumit calculator sau selecta să vizualizați numai calculatoarele administrate.

Sortarea calculatoarelor

Pentru a sorta datele după o anumită coloană, faceți clic pe titlurile coloanelor. De exemplu, dacă doriți să ordonați calculatoarele după nume, faceți clic pe titlul **Nume**. Dacă faceți din nou clic pe numele de coloană, calculatoarele vor fi afișate în ordine inversă.



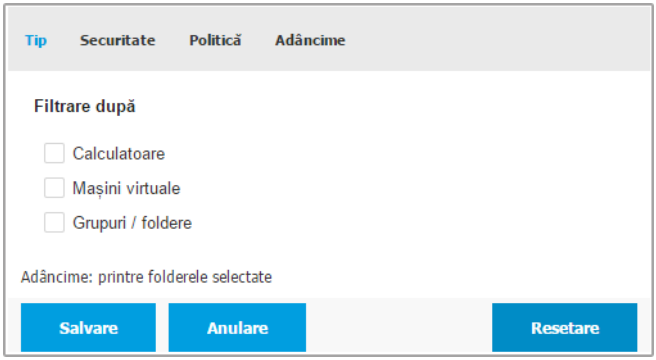
Sortarea calculatoarelor

Filtrarea calculatoarelor

Pentru a filtra entitățile din rețea, folosiți meniul **Filtre** din partea de sus a zonei ferestrelor de rețea.

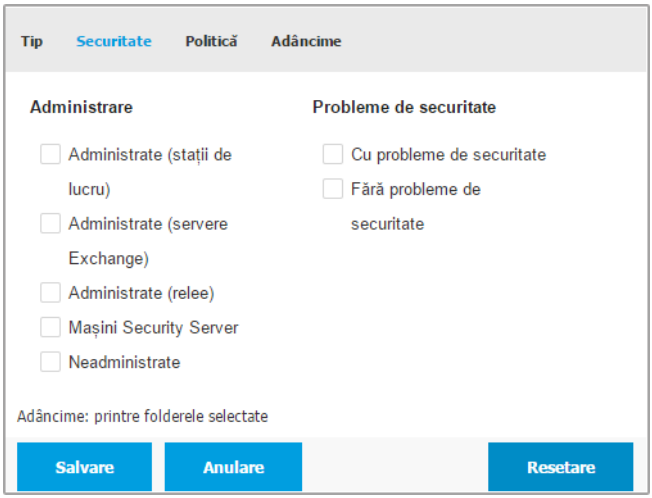
1. Selectați grupul dorit din fereastra din stânga.
2. Faceți clic pe meniul **Filtere** din partea de sus a zonei ferestrelor de rețea.

3. Folosiți criteriile de filtrare după cum urmează:
   - **Tip**. Selectați tipul de entități pe care doriți să le afișați (calculatoare, mașini virtuale, directoare).



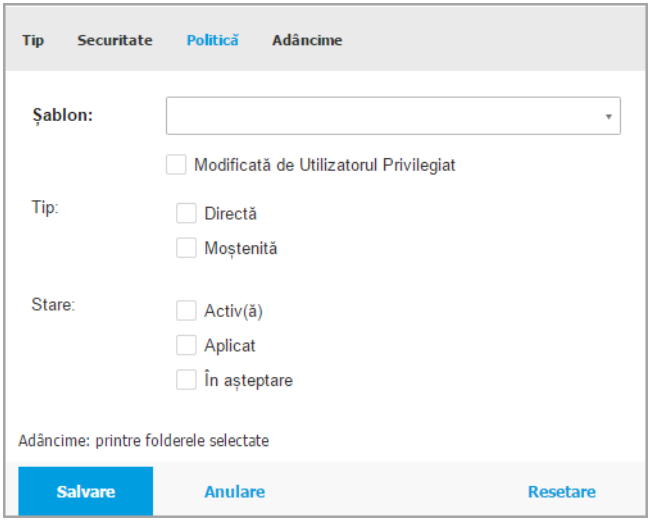
Calculatoare - Filtrare după tip

   - **Securitate**. Alegeți să afișați computerele în funcție de administrarea securității, starea de securitate sau activitatea în așteptare.



Calculatoare - Filtrare după securitate

- **Politică**. Selectați modelul de politică dorit pentru filtrarea calculatoarelor după tipul de atribuire a politicii (Directă sau Moștenită), precum și starea de atribuire a politicii (Activă, Aplicată sau În așteptare). De asemenea, puteți opta pentru afișarea doar a entităților cu politici editate în modul Utilizator avansat.



Calculatoare - Filtrare după politică

- **Adâncime**. Când administrați o rețea de tip arbore, calculatoarele din sub-grupuri nu sunt afișate la selectarea grupului rădăcină. Selectați opțiunea **Toate obiectele recursiv** pentru a vedea toate calculatoarele din grupul curent și din toate sub-grupurile.

Calculatoare - Filtrare după adâncime

Atunci când alegeți să vizualizați recursiv toate articolele, Control Center le afișează într-o listă simplă. Pentru a afla locația unui articol, selectați articolul care vă interesează și apoi faceți clic pe butonul **Mergeți la container** din partea de sus a tabelului. Se va face redirecționarea către containerul părinte al articolului selectat.

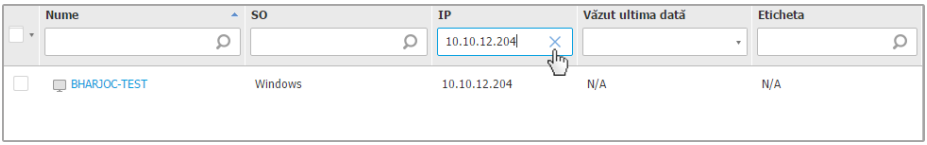
Notă
Puteți vizualiza toate criteriile de filtrare selectate din partea de jos a ferestrei **Filtre**.
Dacă doriți să eliminați toate filtrele, faceți clic pe butonul **Resetare**.

4. Faceți clic pe **Salvare** pentru a filtra calculatoarele după criteriile selectate. Filtrul rămâne activ în pagina **Rețea** până când vă deconectați sau resetați filtrul.

Căutarea unui calculator

1. Selectați grupul dorit din fereastra din stânga.
2. Introduceți termenul de căutare în caseta corespunzătoare de sub titlurile coloanelor din fereastra din dreapta. De exemplu, introduceți IP-ul calculatorului pe care îl căutați în câmpul **IP**. În tabel se va afișa doar calculatorul care corespunde criteriilor de căutare.

   Ștergeți informațiile din caseta de căutare pentru afișarea unei liste a tuturor calculatoarelor.



Căutare calculatoare

6.2.5. Executarea sarcinilor

De pe pagina **Rețea**, puteți rula de la distanță o serie de sarcini administrative pe calculatoare.

Iată ce puteți face:

- „Scanează” (p. 71)
- „Sarcini de aplicare a patch-urilor” (p. 81)
- „Scanare Exchange” (p. 84)
- „Instalare” (p. 88)
- „Dezinstalare client” (p. 95)
- „Actualizarea clientului” (p. 96)
- „Reconfigurare client” (p. 97)
- „Remediere client” (p. 99)
- „Repornire sistem” (p. 100)
- „Descoperire rețea” (p. 100)
- „Descoperire aplicații” (p. 101)
- „Actualizarea Security Server” (p. 102)
- „Injectați instrument personalizat” (p. 103)

Puteți opta pentru generarea unor sarcini individual pentru fiecare calculator sau pentru grupuri de calculatoare. De exemplu, puteți instala de la distanță agentul de securitate pe un grup de calculatoare neadministrate. Ulterior, puteți crea o sarcină de scanare pentru un anumit calculator din același grup.

Pentru fiecare calculator puteți rula doar sarcini compatibile. De exemplu, dacă selectați un calculator neadministrat, nu puteți selecta decât opțiunea de instalare a agentului de securitate, toate celelalte sarcini fiind dezactivate.

Pentru un grup, sarcina selectată va fi creată exclusiv pentru calculatoarele compatibile. Dacă niciunul dintre calculatoarele din grup nu este compatibil cu sarcina selectată, veți fi informat că sarcina nu a putut fi generată.

După ce a fost creată, sarcina va începe să ruleze imediat pe caculatoarele online. Dacă un calculator este offline, sarcina va rula imediat după ce calculatorul este din nou online.

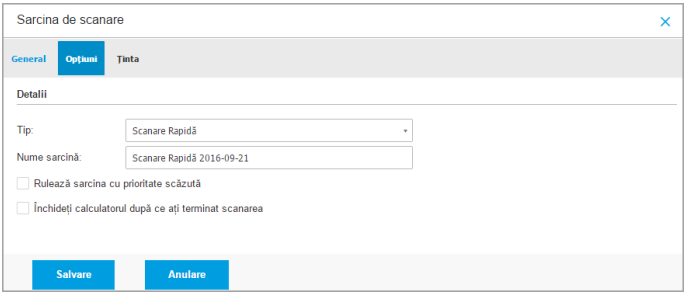
Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor" (p. 207).

Scanează

Pentru a rula de la distanță o sarcină de scanare pe unul sau pe mai multe calculatoare:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare care corespund calculatoarelor sau grupurilor pe care doriți să le scanați.
5. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Scanare**.

   Va apărea o fereastră de configurare.
6. Configurați opțiunile de scanare:
   - În secțiunea **General**, puteți selecta tipul de scanare și puteți introduce o denumire pentru sarcina de scanare. Scopul denumirii scanării este acela de a vă ajuta să identificați cu ușurință scanarea curentă pe pagina **Sarcini**.



Sarcină de scanare calculatoare - Configurarea setărilor generale

Selectați tipul unei scanări din meniul **Tip**:

– **Scanare rapidă** utilizează scanarea în cloud pentru a detecta malware-ul care rulează pe sistem. Acest tip de scanare este preconfigurată pentru a permite scanarea exclusiv a locațiilor critice din sistemele Windows și Linux. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o mică parte din resursele de sistem necesare pentru o scanare antivirus obișnuită.

  Atunci când se detectează programe malware sau rootkit-uri, Bitdefender începe automat procesul de dezinfectare. Dacă, din orice motiv, fișierul nu poate fi dezinfectat, atunci acesta este mutat în carantină. Acest tip de scanare ignoră fișierele suspecte.

– **Scanare completă** verifică întregul sistem, pentru identificarea tuturor tipurilor de programe periculoase care amenință securitatea acestuia, cum ar fi virușii, aplicațiile spion, rookit-urile și altele.

  Bitdefender încearcă automat să dezinfecteze fișierele detectate ca fiind infectate cu malware. În cazul în care malware-ul nu poate fi eliminat, acesta este mutat în carantină, unde nu poate face niciun rău. Fișierele suspecte sunt ignorate. Dacă doriți să întreprindeți acțiuni și asupra fișierelor suspecte sau dacă doriți alte acțiuni implicite pentru fișierele infectate, selectați efectuarea unei Scanări personalizate.

– **Scanare memorie** verifică programele care rulează în memoria calculatorului.

– **Scanare rețea** este un tip de scanare personalizată, care vă permite să scanați unitățile din rețea folosind agentul de securitate Bitdefender instalat pe stația de lucru țintă.

  Pentru ca sarcina de scanare a rețelei să funcționeze:

  - Trebuie să alocați sarcina unei singure stații de lucru din rețea.
  - Trebuie să introduceți datele de autentificare ale unui cont de utilizator cu permisiuni de citire/editare pe unitățile rețelei țintă, pentru ca agentul de securitate să poată accesa și să inițieze acțiuni în cadrul acestor unități de rețea. Datele de autentificare necesare pot fi configurate în secțiunea **Țintă** din fereastra de sarcini.

– **Scanare personalizată** vă permite să selectați locațiile pe care doriți să le scanați și să configurați opțiunile de scanare.

Pentru scanările de memorie, rețea și personalizate, aveți, de asemenea, următoarele opțiuni:

– **Rulează sarcina cu prioritate scăzută**. Selectați această casetă pentru a diminua prioritatea procesului de scanare și pentru a permite altor programe să ruleze mai rapid. Aceasta va mări timpul necesar pentru finalizarea procesului de scanare.

  Notă
  Această opțiune se aplică doar pentru Bitdefender Endpoint Security Tools și Endpoint Security (agent legacy).

– **Închideți calculatorul după ce ați terminat scanarea**. Bifați această casetă pentru a opri calculatorul dacă nu intenționați să îl utilizați pentru o perioadă.

  Notă
  Această opțiune se aplică pentru Bitdefender Endpoint Security Tools, Endpoint Security (agent legacy) și Endpoint Security for Mac.

Notă
Aceste două opțiuni se aplică numai pentru Bitdefender Endpoint Security Tools și Endpoint Security (agent vechi).

Pentru scanări personalizate, configurați următoarele setări:

– Mergeți la secțiunea **Opțiuni** pentru a seta opțiunile de scanare. Faceți clic pe nivelul de securitate care corespunde cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Folosiți descrierea din partea dreaptă a scalei, pentru a vă ghida alegerea.

  În funcție de profilul selectat, opțiunile de scanare din secțiunea **Setări** sunt configurate automat. Cu toate acestea, dacă doriți, le puteți configura detaliat. În acest scop, selectați caseta de bifare **Personalizat** și extindeți secțiunea **Setări**.

Sarcină de scanare calculatoare - Configurarea unei scanări personalizate

Sunt disponibile următoarele opțiuni:

- **Tipuri de fișiere.** Folosiți aceste opțiuni pentru a specifica tipurile de fișiere pe care doriți să le scanați. Puteți seta agentul de securitate să scaneze toate fișierele (indiferent de extensie), fișierele de aplicație sau extensiile specifice de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor asigură cea mai bună protecție în timp ce scanarea aplicațiilor poate fi utilizată pentru efectuarea unei scanări mai rapide.

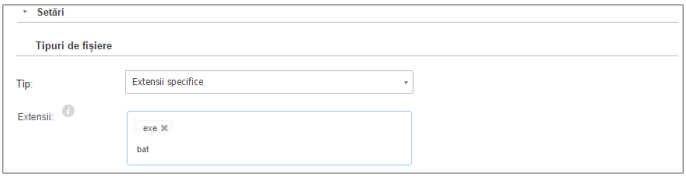
  Notă

  Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Tipuri de fișiere de aplicații” (p. 567).

  Dacă doriți să scanați doar fișiere cu anumite extensii, selectați **Extensii definite de utilizator** din meniu și introduceți extensiile în câmpul de editare, apăsând `Enter` după fiecare.

  Important

  Agenții de securitate Bitdefender instalați pe sistemele de operare Windows și Linux scanează majoritatea formatelor .ISO, dar nu aplică niciun fel de măsuri asupra acestora.



Opțiuni sarcină de scanare calculatoare - Adăugarea extensiilor definite de utilizator

- **Arhive.** Arhivele cu fișiere infestate nu sunt o amenințare directă pentru securitatea sistemului. Programele periculoase pot afecta sistemul numai dacă fișierul infestat este extras din arhivă și executat fără ca protecția în timp real să fie activată. Cu toate acestea, se recomandă să scanați arhivele pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

  Important
  Scanarea fișierelor arhivate crește timpul total necesar pentru scanare și necesită mai multe resurse de sistem.

  – **Scanare în arhive.** Selectați această opțiune dacă doriți să scanați fișierele arhivate, pentru identificarea de malware. Dacă decideți să utilizați această opțiune, puteți configura următoarele opțiuni de optimizare:

    - **Limitare dimensiune arhivă la (MB).** Puteți seta o dimensiune limită acceptată pentru arhivele care vor fi scanate. Selectați căsuța corespunzătoare și introduceți dimensiunea maximă a arhivei (exprimată în MB).

    - **Adâncime maximă arhivă (niveluri).** Selectați caseta de bifare corespunzătoare și alegeți adâncimea maximă a arhivei din meniu. Pentru performanțe superioare, alegeți cea mai mică valoare; pentru protecție maximă, alegeți cea mai mare valoare.

  – **Scanare arhive de e-mail.** Selectați această opțiune dacă doriți să activați scanarea fișierelor atașate la mesajele e-mail și bazele de date e-mail, inclusiv format de fișiere de tipul .eml, .msg, .pst, .dbx, .mbx, .tbb și altele.

Important
Scanarea arhivei e-mail necesită numeroase resurse și poate afecta performanțele sistemului.

- **Diverse.** Selectați casetele de bifare corespunzătoare pentru a activa opțiunile de scanare dorite.
  - **Scanare sectoare de boot.** Scanează sectoarele de boot ale sistemului. Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot. Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.
  - **Scanează regiștrii.** Selectați această opțiune pentru a scana cheile de regiștri. Regiștrii Windows sunt o bază de date care stochează setările de configurare și opțiunile pentru componentele sistemului de operare Windows, precum și pentru aplicațiile instalate.
  - **Scanează după rootkituri.** Selectați această opțiune pentru a lansa procesul de scanare pentru identificarea rootkit-urilor și a obiectelor ascunse, cu ajutorul acestui software.
  - **Scanare după keyloggers.** Selectați această opțiune pentru a scana software-urile de tip keylogger.
  - **Scanează directoare comune din rețea.** Această opțiune scanează unități de rețea montate.

    Pentru scanările rapide, această opțiune este dezactivată în mod implicit. Pentru scanări complte, este activată în mod implicit. Pentru scanări personalizate, dacă setați nivelul de securitate pe **Agresiv/Normal**, opțiunea **Scanare directoare comune din rețea** este activată automat. Dacă setați nivelul de securitate pe **Permisiv**, opțiunea **Scanare directoare comune din rețea** este dezactivată automat.
  - **Scanează memoria.** Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului.
  - **Scanează fișiere cookie.** Selectați această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe calculator.

- **Scanează doar fișierele noi și cele modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
- **Scanare pentru aplicații potențial nedorite (PUA).** O aplicație potențial nedorită (PUA) este un program care ar putea fi nedorit pe PC, care uneori vine la pachet cu software-ul freeware. Astfel de programe pot fi instalate fără consimțământul utilizatorului (numite și adware), sau vor fi incluse în mod implicit în kit-ul de instalare în mod expres (ad-supported). Efectele potențiale ale acestor programe includ afișarea de pop-up-uri, instalarea de bare de instrumente nedorite în browser-ul implicit sau rularea mai multor procese în fundal și încetinirea performanței PC-ului.
- **Scanare volume detașabile.** Selectați această opțiune pentru a scana toate unitățile detașabile atașate la calculator.

- **Acțiuni.** În funcție de tipul de fișier detectat, următoarele acțiuni sunt aplicate în mod automat:
  - **La detectarea unui fișier infectat.** Bitdefender detectează fișierele ca fiind infectate folosind diverse mecanisme avansate, printre care semnăturile malware, învățarea automată și tehnologiile bazate pe inteligență artificială (AI). În mod normal, agentul de securitate Bitdefender poate șterge codul malware din fișierul infestat și poate reconstitui fișierul inițial. Această operațiune este cunoscută sub denumirea de dezinfectare.

    În cazul în care este detectat un fișier infectat, agentul de securitate Bitdefender va încerca în mod automat să-l dezinfecteze. Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

    Important
    Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

  - **La detectarea unui fișier suspect.** Fișierele sunt detectate ca fiind suspecte de către analiza euristică și alte tehnologii Bitdefender. Acestea asigură o rată mare de detecție, însă utilizatorii trebuie

să fie conștienți că există și rezultate fals pozitive (fișiere neinfectate detectate ca fiind suspecte) în unele cazuri. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

Sarcinile de scanare sunt configurate implicit să ignore fișierele suspecte. Ar putea fi util să modificați sarcina implicită, pentru a trece fișierele suspecte sub carantină. Fișierele sub carantină sunt transmise regulat spre analiză la Laboratoarele Bitdefender. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

– **La detectarea unui rootkit.** Rootkit-urile reprezintă aplicații specializate utilizate pentru ascunderea fișierelor de sistemul de operare. Deși nu sunt periculoase, rootkit-urile sunt adesea utilizate pentru ascunderea programelor periculoase sau pentru a disimula prezența unui intrus în sistem.

  Rootkit-urile și fișierele ascunse detectate sunt ignorate implicit.

Deși nu este recomandat, puteți modifica acțiunile implicite. Puteți preciza o a doua acțiune de aplicat în cazul în care prim eșuează, precum și acțiuni diferite pentru fiecare categorie. Alegeți din meniurile corespunzătoare prima și a doua acțiune de aplicat pentru fiecare tip de fișier detectat. Următoarele acțiuni sunt disponibile:

Dezinfectează

Elimină codul periculos din fișierele infectate. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate.

Mută fișierele în carantină

Mutați fișierele detectate din locația curentă, în folderul de carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Fișierele în carantină pot fi gestionate de pe pagina Carantină a consolei.

Ștergere

Ștergeți fișierele detectate de pe disc, fără nicio avertizare. Se recomandă să evitați această acțiune.

Ignoră
Nu se vor lua niciun fel de măsuri împotriva fișierelor detectate. Acește fișiere vor fi doar afișate în jurnalul de scanare.

– Mergeți la secțiunea **Țintă**, pentru a configura locațiile pe care doriți să le scanați din calculatoarele țintă.

  În secțiunea **Țintă scanare**, puteți adăuga un fișier sau folder nou pentru a fi scanat:

  a. Selectați o locație predefinită din meniul derulant sau introduceți **Căi specifice** pe care doriți să le folosiți.

  b. Specificați calea către obiectul de scanat în câmpul de editare.

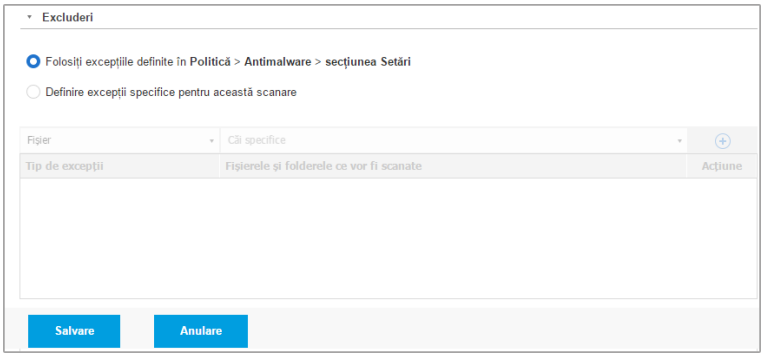
  - Dacă ați ales o locație predefinită, completați calea, după caz. De exemplu, pentru a scana integral folderul `Program Files`, este suficient să selectați locația predefinită corespunzătoare din meniul derulant. Pentru a scana un anumit folder din `Program Files`, trebuie să completați calea adăugând o bară oblică inversă (\) și denumirea folderului.
  - Dacă ați selectat **Căi specifice**, introduceți calea completă către obiectul de scanat. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă. Pentru informații suplimentare referitoare la variabilele de sistem, consultați „Variabile de sistem” (p. 569).

  c. Faceți clic pe butonul ⊕ **Adăugare** corespunzător.

  Pentru a edita o locație existentă, faceți clic pe aceasta. Pentru a elimina o locație din listă, faceți clic pe butonul corespunzător ⊗ **Ștergere**.

  Pentru sarcinile de scanare a rețelei, trebuie să introduceți datele de autentificare ale unui cont de utilizator cu permisiuni de citire/editare pe unitățile rețelei țintă, pentru ca agentul de securitate să poată accesa și să inițieze acțiuni în cadrul acestor unități de rețea.

  Accesați secțiunea **Excepții** dacă doriți să definiți excepțiile pentru obiectele vizate.



Sarcină de scanare calculatoare - Definirea excepțiilor

Puteți utiliza excepții definite de politică sau puteți defini excluderi explicite pentru sarcina de scanare curentă. Pentru detalii referitoare la excepții, consultați „Excluderi” (p. 289).

7. Faceți clic pe **Salvare** pentru a crea sarcina de scanare. Va apărea un mesaj de confirmare.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Notă
Pentru a programa o sarcină de scanare, accesați pagina **Politici**, selectați politica atribuită calculatoarelor care vă interesează și adăugați o sarcină de scanare în secțiunea **Antimalware > La cerere**. Pentru mai multe informații, consultați capitolul „Scanare la cerere” (p. 269).

Scanare pentru identificarea riscurilor

Puteți alege în orice moment să rulați sarcini la cerere de scanare a riscurilor pe stațiile de lucru selectate, după cum urmează:

1. Mergeți la pagina **Rețea**.
2. Navigați prin secțiunile din panoul din partea stângă și selectați stațiile de lucru pe care doriți să le scanați.
3. Selectați **Sarcini** și alegeți **Scanare pentru identificarea riscurilor**.

   Va apărea un mesaj care vă solicită să confirmați rularea sarcinii de scanare pentru identificarea riscurilor.

Notă
Sarcina de scanare pentru identificarea riscurilor va rula cu toți indicatorii de risc activați în mod implicit.

4. După finalizarea cu succes a sarcinii, puteți accesa fila Configurări necorespunzătoare din pagina **Riscuri de securitate**, le puteți analiza și puteți alege care dintre indicatori vor fi ignorați, după caz.

   Scorul general de risc al companiei va fi recalculat pe baza indicatorilor de risc ignorați.

   Notă
   Pentru a vizualiza lista completă a indicatorilor și descrierea acestora, consultați acest articol KB.

Important
Sarcinile de **Scanare riscuri** nu vo rula / vor produce erori pe stațiile de lucru în următoarele situații:

- Stația de lucru nu are sistem de operare Windows.
- Licența de agent a Bitdefender pentru stația de lucru nu este valabilă.
- Politica aplicată pe stația de lucru are modulul de Administrare a riscurilor dezactivat.

Sarcini de aplicare a patch-urilor

Se recomandă să verificați periodic actualizările de software și să le aplicați cât mai curând posibil. GravityZone automatizează acest proces prin politici de securitate, însă dacă aveți nevoie să actualizați imediat software-ul pe anumite stații de lucru, executați în ordine următoarele sarcini:

1. Scanare patch-uri
2. Instalarea patch-urilor

Cerințe preliminare

- Agentul de securitate cu modulul Patch Management este instalat pe stațiile de lucru vizate.
- Pentru ca sarcinile de scanare și instalare să se finalizeze cu succes, stațiile de lucru Windows trebuie să îndeplinească următoarele condiții:

- **Trusted Root Certification Authorities** stochează certificatul **DigiCert Assured ID Root CA**.
- **Intermediate Certification Authorities** include **DigiCert SHA2 Assured ID Code Signing CA**.
- Endpoint-urile au instalat patch-urile pentru Windows 7 și Windows Server 2008 R2 menționate în acest articol Microsoft: Microsoft Security Advisory 3033929

Scanare patch-uri

Stațiile de lucru cu software neactualizat sunt vulnerabile în fața atacurilor. Se recomandă să verificați periodic software-ul instalat pe stațiile dumneavoastră de lucru și să efectuați actualizările necesare cât mai curând posibil. Pentru a vă scana stațiile de lucru în vederea identificării patch-urilor lipsă:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate stațiile de lucru din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați stațiile de lucru vizate.
5. Efectuați clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Scanare patch-uri**. Va apărea o fereastră de configurare.
6. Efectuați clic pe **Da** pentru a confirma sarcina de scanare.

   Atunci când sarcina s-a finalizat, GravityZone adaugă în inventarul de patch-uri toate patch-urile de care au nevoie programele software ale dumneavoastră. Pentru mai multe detalii, vă rugăm consultați „Inventarul de patch-uri” (p. 199).

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Notă
Pentru a programa scanarea patch-urilor, modificați politicile atribuite stațiilor de lucru vizate și configurați setările din secțiunea **Patch Management**. Pentru mai multe informații, consultați capitolul „Administrarea patch-urilor” (p. 336).

Instalarea patch-urilor

Pentru a instala unul sau mai multe patch-uri pe stațiile de lucru vizate:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate stațiile de lucru din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Efectuați clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Instalare patch-uri**.

   Va apărea o fereastră de configurare. Aici, puteți vizualiza toate patch-urile care lipsesc de pe stațiile de lucru vizate.
5. Dacă este nevoie, folosiți opțiunile de sortare și filtrare din partea de sus a tabelului pentru a găsi anumite patch-uri.
6. Efectuați clic pe butonul **Coloane** din partea dreaptă-sus a panoului pentru a vizualiza numai informațiile relevante.
7. Selectați patch-urile pe care doriți să le instalați.

   Unele patch-uri depind de altele. În astfel de cazuri, acestea sunt selectate automat odată cu patch-ul.

   Când efectuați clic pe numerele **CVE-urilor** sau ale **produselor** se va afișa un panou în partea stângă. Panoul conține informații suplimentare, cum ar fi CVE-urile pe care le remediază patch-ul sau produsele pentru care se aplică patch-ul. După ce terminați de citit, efectuați clic pe **Închidere** pentru a ascunde panoul.
8. Selectați **Repornire stații de lucru după instalarea patch-ului, dacă este necesar**, pentru a reporni stațiile de lucru imediat după instalarea patch-ului, dacă sistemul trebuie repornit. Rețineți că această acțiune poate întrerupe activitatea utilizatorului.
9. Faceți clic pe **Instalare**.

   Sarcina de instalare este creată, împreună cu sub-sarcinile pentru fiecare stație de lucru.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Notă

- Pentru a programa instalarea patch-urilor, modificați politicile atribuite stațiilor de lucru vizate și configurați setările din secțiunea **Patch Management**. Pentru mai multe informații, consultați capitolul „Administrarea patch-urilor" (p. 336).
- Puteți instala un patch și de pe pagina **Inventar patch-uri**, pornind de la un anumit patch care vă interesează. În acest caz, selectați patch-ul din listă, faceți clic pe butonul **Instalare** din partea de sus a tabelului și configurați detaliile de instalare a patch-ului. Pentru mai multe detalii, vă rugăm consultați „Instalarea patch-urilor" (p. 203).
- După ce ați instalat un patch, vă recomandăm să transmiteți o sarcină Scanare patch-uri către stațiile de lucru țintă. Această acțiune va actualiza informațiile patch-ului stocate în GravityZone pentru rețelele dvs. administrate.

Puteți dezinstala patch-uri:

- De la distanță, transmițând o sarcină de dezinstalare a patch-urilor din GravityZone.
- Local, pe stația de lucru. În acest caz, va trebui să vă autentificați ca administrator pe stația de lucru și să rulați manual aplicația de dezinstalare.

Scanare Exchange

Puteți scana de la distanță baza de date a unui Server Exchange prin executarea unei sarcini **Scanare Exchange**.

Pentru a putea scana baza de date Exchange, trebuie să activați scanarea la cerere furnizând datele de autentificare ale unui administrator Exchange. Pentru mai multe informații, consultați capitolul „Scanarea bazei de date Exchange" (p. 361).

Pentru a scana baza de date a unui Server Exchange:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Din fereastra din stânga, selectați grupul care conține Serverul Exchange țintă. Serverul este afișat în fereastra din dreapta.

Notă

Opțional, puteți aplica filtre pentru a găsi rapid serverul țintă:

- Faceți clic pe meniul **Filtre** și selectați următoarele opțiuni: **Administrat (Server Exchange)** din secțiunea **Securitate** și **Toate obiectele recursiv** din secțiunea **Adâncime**.

- Introduceți numele gazedei serverului sau adresa IP în câmpurile antetelor corespunzătoare ale coloanelor.

4. Selectați caseta de bifare a Serverului Exchange a cărei bază de date doriți să o scanați.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Scanare Exchange**. Va apărea o fereastră de configurare.
6. Configurați opțiunile de scanare:
   - **General.** Introduceți o denumire sugestivă pentru sarcină.

     Pentru bazele de date mari, sarcina de scanare poate dura mult și poate afecta performanța serverului. În aceste cazuri, selectați caseta de bifare **Oprește scanarea dacă durează mai mult de** și alegeți un interval de tip convenabil din meniurile corespunzătoare.
   - **Țintă.** Selectați containerele și obiectele pe care doriți să le scanați. Puteți opta pentru scanarea căsuțelor poștale, a folderelor publice sau a ambelor. În afară de e-mail-uri, puteți opta pentru scanarea altor obiecte, cum ar fi **Contacte**, **Sarcini**, **Programări** și **Articole poștale**. De asemenea, puteți seta următoarele limitări pentru conținutul care urmează să fie scanat:
     – Doar mesajele necitite
     – Doar articolele cu atașamente
     – Doar articolele noi, primite într-un interval de timp specificat

     De exemplu, puteți opta pentru a scana doar e-mail-urile din căsuțele poștale ale utilizatorilor primite în ultimele șapte zile.

     Selectați caseta de bifare **Excepții**, dacă doriți să definiți excepții de scanare. Pentru a crea o excepție, folosiți câmpurile din antetul tabelului, după cum urmează:
     a. Selectați tipul de director din meniu.
     b. În funcție de tipul directorului, specificați obiectele pe care doriți să le excludeți:

Tipul directorului	Formatul obiectului
Mailbox	Adresă e-mail
Folder public	Calea folderului, începând de la rădăcină
Bază de date	Informațiile de identificare ale bazei de date

Notă
Pentru a obține informațiile de identificare ale bazei de date, folosiți comanda shell Exchange:
`Get-MailboxDatabase | fl name,identity`

Nu puteți introduce mai multe articole simultan. Dacă aveți mai multe articole de același tip, trebuie să definiți un număr de reguli egal cu numărul de articole.

c. Faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului pentru a salva excepția și a o include în listă.

Pentru a șterge o regulă referitoare la excepții din listă, faceți clic pe butonul ⊖ **Ștergere** corespunzător.

- **Opțiuni.** Configurați opțiunile de scanare pentru e-mail-urile care corespund regulii:
  - **Tipurile de fișiere scanate.** Folosiți această opțiune pentru a specifica tipurile de fișiere pe care doriți să le scanați. Puteți decide să scanați toate fișierele (indiferent de extensia acestora), exclusiv fișierele de aplicații sau anumite extensii de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor asigură cea mai bună protecție, în timp ce scanarea aplicațiilor este recomandată doar pentru efectuarea unei scanări mai rapide.

    Notă
    Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Tipuri de fișiere de aplicații” (p. 567).

    Dacă doriți să scanați doar fișiere cu anumite extensii, aveți două opțiuni:
    - **Extensii definite de utilizator**, unde trebuie să indicați doar extensiile pe care doriți să le scanați.
    - **Toate fișierele, cu excepția anumitor extensii**, unde trebuie să introduceți doar extensiile pe care nu doriți să le includeți în scanare.
  - **Dimensiunea maximă a atașamentului / cuprinsului e-mail-ului (MB).** Selectați această casetă de bifare pentru a introduce o valoare în câmpul corespunzător, pentru setarea dimensiunii maxime acceptate a fișierului atașat sau a cuprinsului e-mail-ului pe care doriți să îl scanați.
  - **Capacitatea maximă a arhivei (niveluri).** Selectați caseta de bufare și alegeți capacitatea maximă a arhivei din câmpul corespunzător. Cu cât

capacitatea este mai redusă, cu atât performanțele sunt mai ridicate, iar nivelul de protecție este mai mic.
  – **Scanare Posibile aplicații nedorite(PUA).** Selectați această casetă de bifare pentru scanarea posibilelor aplicații periculoase sau nedorite, cum ar fi adware, care se pot instala în sisteme fără consimțământul utilizatorului, pot schimba comportamentul diferitelor produse software și reduce performanțele sistemului.
- **Acțiuni.** Puteți specifica diverse acțiuni pentru agentul de securitate pentru a prelua automat fișiere pe baza tipului de detecție.

  Tipul de detecție separă fișierele în trei categorii:
  – **Fișiere infectate.** Bitdefender detectează fișierele ca fiind infectate folosind diverse mecanisme avansate, printre care semnăturile malware, învățarea automată și tehnologiile bazate pe inteligență artificială (AI).
  – **Fișiere suspecte.** Aceste fișiere sunt detectate ca fiind suspecte de către analiza euristică și alte tehnologii Bitdefender. Acestea asigură o rată mare de detecție, însă utilizatorii trebuie să fie conștienți că există și rezultate fals pozitive (fișiere neinfectate detectate ca fiind suspecte) în unele cazuri.
  – **Fișiere care nu pot fi scanate .**Aceste fișiere nu pot fi scanate. Fișierele care nu pot fi scanate includ dar nu se limitează la fișiere protejate cu parolă, criptate sau supra-arhivate.

  Pentru fiecare tip de detecție, aveți o acțiune implicită sau principală și o acțiune alternativă, în cazul în care cea principală eșuează. Deși nu se recomandă, puteți modifica aceste acțiuni din meniurile corespunzătoare. Selectați acțiunile care vor fi implementate:
  – **Dezinfectare.** Șterge codul malware din fișierele infectate și reconstruiește fișierul original. Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.
  – **Respingere / Ștergere e-mail.** Pe serverele cu rol Edge Transport, mesajele e-mail detectate sunt respinse cu un cod de eroare 550 SMTP. În toate celelalte cazuri, mesajul e-mail este șters fără nicio avertizare. Se recomandă să evitați această acțiune.
  – **Ștergere fișier.** Șterge atașamentele cu probleme, fără avertizare. Se recomandă să evitați această acțiune.

- **Înlocuire fișier.** Șterge fișierele cu probleme și introduce un fișier text care informează utilizatorul cu privire la măsurile luate.
- **Trecerea fișierelor în carantină.** Mută fișierele detectate în folderul carantină și introduce un fișier text care informează utilizatorul cu privire la măsurile luate. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Puteți administra fișierele în carantină de pe pagina **Carantină**.

  Notă
  Vă rugăm să rețineți că, în cazul Serverelor Exchange, carantina necesită spațiu suplimentar pe hard-disk, pe partiția pe care este instalat agentul de securitate. Dimensiunea carantinei depinde de numărul de articole stocate și de dimensiunea acestora.

- **Nu se vor lua măsuri.** Nu vor fi luate măsuri cu privire la fișierele detectate. Acește fișiere vor fi doar afișate în jurnalul de scanare. Sarcinile de scanare sunt configurate implicit să ignore fișierele suspecte. Ar putea fi util să modificați sarcina implicită, pentru a trece fișierele suspecte sub carantină.
- În mod implicit, dacă un e-mail corespunde domeniului de aplicare al regulii, acesta este procesat exclusiv în conformitate cu regula, fără a fi verificat cu privire la orice alte reguli rămase. Dacă doriți să continuați să verificați în baza celorlalte reguli, debifați caseta de selectare **Oprire procesare reguli, dacă condițiile regulii sunt îndeplinite**.

7. Faceți clic pe **Salvare** pentru a crea sarcina de scanare. Va apărea un mesaj de confirmare.
8. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Instalare

Pentru a vă proteja calculatoarele folosind agentul de securitate Bitdefender, trebuie să îl instalați pe fiecare dintre acestea.

Important
În rețele izolate, care nu au conectivitate directă cu aplicația GravityZone, puteți instala agentul de securitate cu rol de Releu. În acest caz, comunicarea dintre aplicația GravityZone și ceilalți agenți de securitate se va realiza prin agentul Releu, care va

acționa și ca și server local de actualizări pentru agenții de securitate, protejând rețeaua izolată.
După ce ați instalat un agent Releu, acesta va detecta automat calculatoarele neprotejate din aceeași rețea.

Notă

- Se recomandă ca acel calculator pe care instalați agentul Releu să fie întotdeauna pornit.
- Dacă nu aveți niciun agent Releu instalat în rețea, calculatoarele neprotejate pot fi detectate manual, prin transmiterea unei sarcini **Descoperire rețea** către o stație de lucru protejată.

Protecția Bitdefender poate fi apoi instalată pe calculatoare de la distanță, de pe Control Center.

Instalarea la distanță este efectuată în fundal, fără ca utilizatorul să știe despre acest lucru.

Avertisment

Înainte de instalare, asigurați-vă că ați dezinstalat aplicația firewall contra programelor periculoase de pe calculatoare. Instalarea protecției Bitdefender peste aplicațiile de securitate existente le poate afecta funcționarea și poate cauza probleme majore în sistem. Windows Defender și Windows Firewall se dezactivează automat la demararea instalării.

Dacă doriți să instalați agentul de securitate pe un computer cu Bitdefender Antivirus for Mac 5.X, trebuie mai întâi să îl dezinstalați manual pe acesta din urmă. Pentru îndrumări, consultați acest articol KB.
La instalarea agentului prin intermediul unui Releu Linux, trebuie respectate următoarele condiții:

- Endpoint-ul cu rol de Releu trebuie să aibă instalat pachetul Samba (`smbclient`) versiunea 4.1.0 sau mai recentă și să suporte comanda `net` binary/command, astfel încât să poată instala de la distanță agenți Windows.

  Notă

  De regulă, funcționalitatea `net` binary/command este livrată împreună cu pachetele samba-client și/sau samba-common. Pe anumite distribuții Linux (precum CentOS 7.4), comanda `net` se instalează numai în cazul instalării versiunii complete a suitei Samba (Common + Client + Server).

Asigurați-vă că pe endpoint-ul cu rol de Releu este disponibilă comanda `net`.

- Stațiile de lucru Windows trebuie să aibă activate funcțiile Partajare administrativă și Partajare rețea.
- Stațiile de lucru țintă Linux și Mac trebuie să aibă funcția SSH activată și firewall-ul dezactivat.

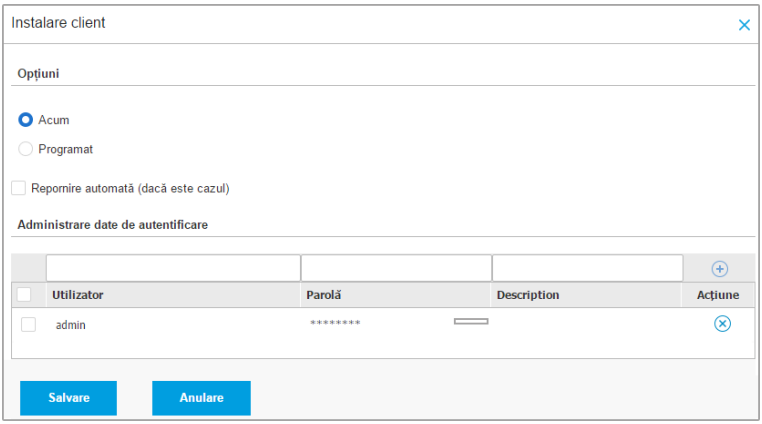
Pentru a rula o sarcină de instalare de la distanță:

1. Conectați-vă și autentificați-vă la Control Center.
2. Mergeți la pagina **Rețea**.
3. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
4. Selectați grupul dorit din fereastra din stânga. Entitățile din grupul selectat sunt afișate în tabelul din fereastra din dreapta.

   Notă
   Opțional, puteți aplica filtre pentru a afișa exclusiv stațiile de lucru neadministrate. Dați clic pe meniul **Filtre** și selectați următoarele opțiuni: **Neadministrat** din fila **Securitate** și **Toate obiectele recursiv** din fila **Adâncime**.

5. Selectați entitățile (stațiile de lucru sau grupurile de stații de lucru) pe care doriți să instalați protecția.
6. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Instalare**.

   Se afișează asistentul **Instalare client**.



Instalarea Bitdefender Endpoint Security Tools din meniul Sarcini

7. În secțiunea **Opțiuni**, configurați timpul de instalare:
   - **Acum**, pentru a lansa instalarea imediat.
   - **Programat**, pentru a configura intervalul de recurență al instalării. În acest caz, selectați intervalul de timp dorit (orar, zilnic sau săptămânal) și configurați-l conform necesităților dvs.

   Notă
   De exemplu, dacă sunt necesare anumite operațiuni pe mașina țintă înainte de a instala clientul (cum ar fi dezinstalarea altor aplicații și repornirea sistemului de operare), puteți programa sarcina de instalare să ruleze la fiecare 2 ore. Sarcina va începe pe fiecare mașină țintă la fiecare 2 ore până la finalizarea cu succes a instalării.

8. Dacă doriți ca stațiile de lucru țintă să fie repornite automat pentru finalizarea instalării, selectați **Repornire automată (dacă este necesar)**.
9. În secțiunea **Administrare date de autentificare**, specificați drepturile de administrare necesare pentru autentificarea de la distanță pe stațiile de lucru țintă. Puteți adăuga datele de autentificare introducând numele de utilizator și parola pentru fiecare sistem de operare țintă.

Important
Pentru stații de lucru cu sistem de operare Windows 8.1, este necesar să furnizați datele de autentificare ale contului de administrator încorporat sau ale unui cont de administrator de domeniu. Pentru mai multe informații, consultați acest articol KB.

Pentru a adăuga datele SO necesare:

a. Introduceți numele de utilizator și parola unui cont de administrator în câmpurile corespunzătoare din capul de tabel.

   În cazul în care calculatoarele sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

   Folosiți convențiile Windows la introducerea denumirii contului de utilizator:

   - Pentru mașinile Active Directory folosiți următoarele sintaxe: `username@domain.com` și `domain\username`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`user@domain.comusername@domain.com` și `domain\userusername`).
   - Pentru mașinile din grupul de lucru, e suficient să introduceți numai numele de utilizator, fără numele grupului de lucru.

   Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont.

b. Faceți clic pe butonul ⊕ **Adăugare**. Contul este adăugat la lista de date de autentificare.

Notă
Datele specificate sunt salvate automat în secțiunea Administrare date de autentificare, astfel încât nu trebuie să le reintroduceți. Pentru a accesa funcția de Administrare date de autentificare, nu trebuie decât să dați clic pe numele dvs. de utilizator din colțul din dreapta sus al consolei.

Important
Dacă datele de autentificare furnizate nu sunt valabile, instalarea aplicației client va eșua pe stațiile de lucru respective. Asigurați-vă că actualizați datele de autentificare pentru sistemul de operare introduse în funcționalitatea de Administrare date de autentificare atunci când acestea se schimbă pe stațiile de lucru țintă.

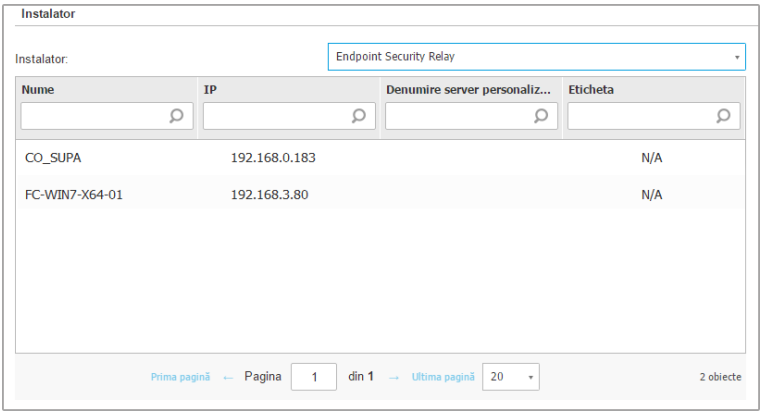
10. Selectați casetele corespunzătoare conturilor pe care doriți să le folosiți.

Notă
Dacă nu ați selectat datele de autentificare, se va afișa un mesaj de avertizare. Acest pas este obligatoriu pentru instalarea de la distanță a agentului de securitate pe stațiile de lucru.

11. În secțiunea **Agent de instalare**, alegeți entitatea la care se vor conecta stațiile de lucru țintă pentru instalarea și actualizarea clientului:
    - **Aplicația GravityZone**, atunci când stațiile de lucru se conectează direct la aplicația GravityZone.

      În acest caz, puteți defini de asemenea:
      - Un server de comunicații personalizat introducând IP-ul sau numele de gazdă al acestuia, dacă este necesar.
      - Setări proxy, dacă stațiile de lucru țintă comunică cu aplicația GravityZone prin proxy. În acest caz, selectați **Utilizare proxy pentru comunicații** și introduceți setările de proxy necesare în câmpurile de mai jos.
    - **Releu Endpoint Security**, dacă doriți să conectați stațiile de lucru la un client de tip releu instalat în rețeaua dvs. Toate mașinile cu rolul de releu detectate în rețeaua dvs. vor fi afișate în tabelul afișat mai jos. Selectați mașina de tip releu dorită. Stațiile de lucru conectate vor comunica cu Control Center exclusiv prin releul specificat.

      Important
      Portul 7074 trebuie să fie deschis pentru ca instalarea prin agentul releu să funcționeze.



12. Utilizați secțiunea **Ținte suplimentare** dacă doriți să instalați clientul pe anumite mașini din rețeaua dumneavoastră care nu sunt incluse în inventarul rețelei. Extindeți secțiunea și introduceți adresa IP sau numele de domeniu pentru mașinile respective în câmpul dedicat, separate printr-o virgulă. Puteți adăuga numărul necesar de adrese IP.
13. Trebuie să selectați un pachet de instalare pentru instalarea curentă. Dați clic pe lista **Utilizare pachet** și selectați pachetul de instalare dorit. Puteți găsi aici toate pachetele de instalare create anterior pentru contul dumneavoastră, precum și pachetul de instalare implicit disponibil în Control Center.
14. Dacă este necesar, puteți modifica o parte din setările pachetului de instalare făcând clic pe butonul **Personalizare** de lângă câmpul **Utilizare pachet**.

    Setările pachetului de instalare vor apărea mai jos și veți putea efectua modificările de care aveți nevoie. Pentru mai multe informații referitoare la editarea pachetelor de instalare, consultați Ghidul de instalare GravityZone.

    Dacă doriți să salvați modificările ca pachet nou, selectați opțiunea **Salvare ca pachete** situată în partea de jos a listei de setări a pachetului și introduceți o denumire pentru noul pachet de instalare.
15. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

Important
Dacă utilizați VMware Horizon View Persona Management, vă recomandăm să configurați Politica grupului activ de directoare pentru a exclude următoarele procese Bitdefender (fără calea completă):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Aceste excepții trebuie să fie aplicate atât timp cât agentul de securitate rulează la nivelul stației de lucru. Pentru detalii, consultați această pagină cu documentație VMware Horizon.

Upgrade client

Această opțiune este disponibilă numai atunci când agentul Endpoint Security este instalat și detectat în rețea. Bitdefender recomandă efectuarea unui upgrade de la Endpoint Security la noul Bitdefender Endpoint Security Tools, pentru o protecție de ultimă generație a stațiilor de lucru.

Pentru a găsi cu ușurință clienții fără upgrade, puteți genera un raport de stare pentru upgrade. Pentru detalii cu privire la crearea rapoartelor, consultați „Crearea rapoartelor” (p. 495).

Dezinstalare client

Pentru a dezinstala de la distanță protecția Bitdefender:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare ale calculatoarelor de pe care doriți să dezinstalați agentul de securitate Bitdefender.

5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Dezinstalare client**.
6. Se afișează o fereastră de configurare, care vă permite să efectuați următoarele setări:
   - Puteți opta pentru menținerea articolelor trecute în carantină pe mașina client.
   - Pentru mediile integrate cu vShield, trebuie să selectați datele de autentificare necesare pentru fiecare mașină. Ăn caz contrar, instalarea va eșua. Selectați **Utilizare date de autentificare pentru integrarea cu vShield**, apoi faceți clic pe toate datele de autentificare corespunzătoare din tabelul Administrare date de autentificare afișat mai jos.
7. Faceți clic pe **Salvare** pentru a genera sarcina. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Notă
Dacă doriți să reinstalați protecția, asigurați-vă mai întâi că ați repornit calculatorul.

Actualizarea clientului

Verificați periodic starea calculatoarelor administrate. Dacă identificați un calculator cu probleme de securitate, faceți clic pe denumire pentru afișarea paginii **Informații**. Pentru mai multe informații, consultați capitolul „Stare securitate” (p. 49).

Clienții sau conținutul de securitate care nu este la zi reprezintă probleme de securitate. În aceste cazuri, trebuie să executați o actualizare pe calculatorul corespunzător. Această sarcină poate fi efectuată local de pe calculator sau de la distanță din Control Center.

Pentru a actualiza de la distanță clientul și conținutul de securitate pe calculatoarele administrate:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.

4. Selectați casetele de bifare ale calculatoarelor pe care doriți să rulați o actualizare a clientului.
5. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Actualizare**. Va apărea o fereastră de configurare.
6. Puteți alege să actualizați numai produsul, numai conținutul de securitate sau ambele.
7. Pentru SO Linux și mașinile integrate cu vShield, trebuie să selectați și datele de autentificare necesare. Bifați caseta **Utilizare date de autentificare pentru Linux și integrarea cu vShield**, apoi seleczați toate datele de autentificare corespunzătoare din tabelul Administrare date de autentificare afișat mai jos.
8. Faceți clic pe **Actualizare** pentru a executa sarcina. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Reconfigurare client

Modulele de protecție, rolurile și modurile de scanare ale agentului de securitate sunt inițial configurate în pachetul de instalare. După ce ați instalat agentul de securitate în rețea, puteți modifica în orice moment setările inițiale prin transmiterea unei sarcini de **Reconfigurare client** de la distanță către stațiile de lucru care vă interesează.

Avertisment
Vă informăm că sarcina **Reconfigurare Client** suprascrie toat setările de securitate și niciuna dintre setările inițiale nu este menținută. În timp ce utilizați această sarcină, asigurați-vă că reconfigurați toate setările de instalare ale stațiilor de lucru țintă.

Notă
Sarcina **Reconfigurare client** va șterge toate modulele incompatibile de pe instalările existente ale versiunilor Widows mai vechi.

Puteți modifica setările de instalare din zona **Rețea** sau din raportul **Status module endpoint**.

Pentru a schimba setările de instalare pentru unul sau mai multe calculatoare:

1. Mergeți la pagina **Rețea**.

2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare ale calculatoarelor pentru care doriți să modificați setările de instalare.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Reconfigurare client**.
6. Selectați una dintre următoarele acțiuni:
   - **Adăugare**. Adăugați module noi pe lângă cele deja existente.
   - **Eliminare**. Eliminați anumite module dintre cele deja existente.
   - **Potrivire listă**. Potriviți modulele instalate cu selecția dumneavoastră.
7. Selectați modulele și rolurile pe care intenționați să le instalați sau să le eliminați de pe endpoint-urile vizate.

   Avertisment
   Vor fi instalate doar modulele compatibile. Spre exemplu, Firewall-ul se va instala doar pe stațiile de lucru Windows compatibile.
   Pentru mai multe informații, consultați Disponibilitate niveluri de protecție GravityZone.

8. Selectați **Eliminare concurenți, după caz** pentru a vă asigura că modulele selectate nu vor intra în conflict cu alte soluții de securitate instalate pe endpoint-urile vizate.
9. Alegeți unul dintre modurile disponibile de scanare:
   - **Automat**. Agentul de securitate detectează care motoare de scanare sunt potrivite pentru resursele endpoint-ului.
   - **Personalizat**. Dumneavoastră alegeți în mod explicit ce motoare de scanare sunt utilizate.

     Pentru detalii despre opțiunile disponibile, consultați secțiunea Crearea pachetelor de instalare din Ghidul de instalare.

   Notă
   Această secțiune este disponibilă doar cu **Potrivire listă**.

10. În secțiunea **Planificator**, alegeți când va rula sarcina:
    - **Acum**, pentru a lansa sarcina imediat.
    - **Programat**, pentru a configura intervalul de recurență al sarcinii.

      În acest caz, selectați intervalul de timp (o dată pe oră, zilnic sau săptămânal) și configurați-l conform necesităților dumneavoastră.
11. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

    Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Remediere client

Utilizați sarcina Remediere client ca o sarcină inițială de remediere pentru diferite probleme la nivelul endpoint-urilor. Sarcina va descărca cel mai recent pachet de instalare pe endpoint-ul vizat și apoi va reinstala agentul.

Notă

- The modules currently configured on the agent will not be changed.
- Sarcina de remediere va reseta agentul de securitate la versiunea publicată în pagina **Configurare>Actualizare > Componente**.

Pentru a transmite o sarcină de Remediere client clientului:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare ale computerelor pe care doriți să rulați o remediere a clientului.
5. Faceți clic pe butonul **Sarcini** din partea superioară a tabelului și selectați **Remediere client**. Va apărea o fereastră de configurare.
6. Bifați caseta **Înțeleg și sunt de acord** și faceți clic pe butonul **Salvare** pentru a rula sarcina.

Notă
Pentru finalizarea sarcinii de remediere, este posibil să fie nevoie de o repornire a clientului.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Repornire sistem

Puteți opta pentru repornirea de la distanță a calculatoarelor administrate.

Notă
Verificați pagina **Rețea > Sarcini** înainte de a reporni anumite calculatoare. Este posibil ca sarcinile create anterior să fie în continuare în curs de procesare pe calculatoarele țintă.

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare ale calculatoarelor pe care doriți să le reporniți.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Repornire sistem**.
6. Selectați opțiunea programului de repornire:
   - Selectați **Repornire imediată** pentru a reporni imediat calculatoarele.
   - Selectați **Repornire la** și folosiți câmpurile de mai jos, pentru a programa repornirea la data și ora dorită.
7. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Descoperire rețea

Funcția de descoperire a rețelelor este executată automat de către agenții de securitate cu rol de Releu. Dacă nu aveți un agent Releu instalat în rețea, trebuie

să transmiteți manual o sarcină de descoperire rețea de pe o stație de lucru protejată.

Pentru a rula o sarcină de descoperire a rețelei în rețeaua dumneavoastră:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați caseta de bifare a calculatorului cu care doriți să efectuați sarcina de descoperire a rețelei.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Descoperire rețea**.
6. Va apărea un mesaj de confirmare. Faceti clic pe **Da**.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Descoperire aplicații

Pentru a descoperi aplicațiile din rețeaua dumneavoastră:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați calculatoarele pe care doriți să executați funcția de descoperire aplicații.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Descoperire aplicații**.

   Notă
   Bitdefender Endpoint Security Tools cu modulul Control aplicații trebuie să fie instalat și activat pe calculatoarele selectate. În caz contrar, sarcina va fi inactivă. Atunci când un grup selectat conține ținte valide și nevalide, sarcina va fi trimisă numai către stațiile de lucru valide.

6. Apăsați **Da** în fereastra de confirmare pentru a continua.

Aplicațiile și procesele descoperite sunt afișate în pagina **Rețea > Inventar aplicații**. Pentru mai multe informații, consultați capitolul „Inventar aplicații” (p. 193).

Notă
Executarea sarcinii **Descoperire aplicații** ar putea dura câteva momente, în funcție de numărul de aplicații instalate. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Actualizarea Security Server

Security Server instalat poate fi vizualizat și administrat și din secțiunea **Calculatoare și mașini virtuale** din directorul **Grupuri personalizate**.

Dacă un Security Server nu este la zi, îi puteți transmite o sarcină de actualizare:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați grupul în care este instalat Security Server.

   Pentru a localiza cu ușurință Security Server, puteți folosi meniul **Filtre**, după cum urmează:

   - Mergeți la secțiunea **Securitate** și selectați exclusiv **Security Servers**.
   - Mergeți la secțiunea **Adâncime** și selectați **Toate obiectele recursiv**.
4. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Actualizare Security Server**.
5. Va trebui să confirmați operațiunea. Faceți clic pe **Da** pentru generarea sarcinii.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Important
Este recomandat să utilizați această metodă pentru actualizarea Security Server pentru NSX, în caz contrar veți pierde carantina salvată în aplicație.

Injectați instrument personalizat

Notă
Această sarcină este legată de modulul HVI care poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Pentru injectarea instrumentelor în sistemele de operare ale gazdei vizate:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga. Toate stațiile de lucru din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele stațiilor de lucru vizate.
5. Efectuați clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Injectare instrument personalizat**. Este afișată o fereastră de configurare.
6. Din meniul derulant, selectați toate instrumentele pe care doriți să le injectați. Pentru fiecare instrument selectat va fi afișată o secțiune pliantă cu setările acestuia.

   Aceste instrumente au fost încărcate anterior în GravityZone. Dacă nu găsiți instrumentul potrivit pe listă, accesați **Centru administrare instrumente** și adăugați-l de acolo. Pentru mai multe informații, consultați capitolul „Injectare instrumente personalizate cu HVI” (p. 533).
7. Pentru fiecare instrument afișat în fereastră:
   a. Efectuați clic pe numele instrumentului pentru a vizualiza sau ascunde secțiunea acestuia.
   b. Introduceți linia de comandă a instrumentului împreună cu toți parametrii de intrare necesari, exact la fel cum procedați pentru Command Prompt sau Terminal. De exemplu:

      ```
      bash script.sh <param1> <param2>
      ```

      Pentru Instrumentele BD de remediere, puteți selecta doar acțiunea de remediere și acțiunea de remediere de backup din cele două meniuri derulante.
   c. Indicați locația de unde Security Server trebuie să culeagă jurnalele:

- **stdout**. Selectați această căsuță pentru a prelua jurnalele din canalul standard de comunicare de ieșire.
- **Fișier ieșire**. Selectați această căsuță pentru a prelua fișierul jurnal salvat pe stația de lucru. În acest caz, trebuie să introduceți calea unde poate Security Server să găsească fișierul. Puteți folosi căi absolute sau variabile de sistem.

  Aici aveți o opțiune suplimentară: **Ștergere fișiere jurnal de la sistemul găzduit după ce au fost transferate**. Selectați-o dacă nu mai aveți nevoie de fișiere la stația de lucru.

8. Dacă doriți să transferați fișierul jurnal din Security Server într-o altă locație trebuie să furnizați calea către locația de destinație și datele de autentificare.
9. Câteodată instrumentul poate necesita un timp mai îndelungat decât cel preconizat pentru finalizarea acțiunii sau poate să nu mai răspundă la comenzi. Pentru a evita căderile de sistem în astfel de situații, selectați din secțiunea **Configurare siguranță** după câte ore trebuie ca Security Server să oprească automat acțiunea instrumentului.
10. Faceți clic pe **Save**.

    Veți putea vizualiza starea sarcinii pe pagina **Sarcini**. Pentru mai multe detalii, puteți să consultați și raportul **HVI Stare injectare de la terți**.

6.2.6. Crearea de rapoarte rapide

Puteți opta pentru crearea de rapoarte rapide pe calculatoarele administrate, din pagina **Rețea**:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.

   Opțional, puteți filtra conținutul grupului selectat numai după calculatoarele administrate.
4. Selectați casetele de bifare ale aclculatoarelor pe care doriți să le includeți în raport.
5. Faceți clic pe butonul **Rapoarte** din partea de sus a tabelului și selectați tipul de raport din meniu.

Pentru mai multe informații, consultați capitolul „Rapoarte referitoare la calculatoare și mașini virtuale” (p. 476).

6. Configurați opțiunile pentru raport. Pentru mai multe informații, consultați capitolul „Crearea rapoartelor” (p. 495).
7. Faceți clic pe **Generare**. Raportul este afișat imediat.

   Intervalul necesar pentru crearea rapoartelor poate varia în funcție de numărul de calculatoare selectate.

6.2.7. Atribuirea unei politici

Puteți administra setările de securitate pe calculatoare folosind politicile.

Din pagina **Rețea**, puteți vizualiza, modifica și atribui politici pentru fiecare calculator sau grup de calculatoare.

Notă
Setările de securitate sunt disponibile exclusiv pentru calculatoarele administrate. Pentru a vizualiza și administra mai ușor setările de securitate, puteți filtra inventarul de rețea numai după calculatoarele administrate.

Pentru a vizualiza politica atribuită unui anumit calculator:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Faceți clic pe denumirea calculatorului administrat dorit. O fereastră conținând diverse informații va apare.
5. În secțiunea **General**, în **Politică**, faceți clic pe denumirea politicii curente pentru a-i vizualiza setările.
6. Puteți modifica setările de securitate în funcție de necesități, cu condiția ca deținătorul politicii să fi permis celorlalți utilizatori să modifice politica respectivă. Vă rugăm să rețineți că orice modificare va afecta toate calculatoarele cărora le este atribuită aceeași politică.

   Pentru mai multe informații despre modificarea setărilor calculatorului, vă rugăm să consultați „Politici referitoare la calculatoare și mașini virtuale” (p. 235).

Pentru alocarea unei politici pentru un calculator sau un grup:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați caseta de bifare a calculatorului sau grupului care vă interesează. Puteți selecta unul sau mai multe obiecte de același timp, numai dacă aparțin aceluiași nivel.
5. Faceți clic pe butonul **Alocare politică** din partea de sus a tabelului.
6. Efectuați setările necesare în fereastra **Atribuire politică**. Pentru mai multe informații, consultați capitolul „Atribuirea unei politici" (p. 223).

Utilizarea Managerului de recuperare pentru volumele criptate

Atunci când utilizatorii endpoint-urilor își uită parolele de criptare și nu mai pot accesa volumele criptate pe mașinile lor, îi puteți ajuta extrăgând cheile de recuperare din pagina **Rețea**.

Pentru a extrage o cheie de recuperare:

1. Mergeți la pagina **Rețea**.
2. Selectați butonul **Manager de recuperare** din bara de acțiuni din partea stângă. Se afișează o nouă fereastră.
3. În secțiunea **Identificator** a ferestrei, introduceți datele următoare:
   a. ID-ul cheii de recuperare pentru volumul criptat. ID-ul cheii de recuperare este un șir de numere și litere disponibile pe endpoint, în ecranul de recuperare BitLocker.

      Pe Windows, ID-ul cheii de recuperare este un șir de numere și litere disponibile pe endpoint, în ecranul de recuperare BitLocker.

      Alternativ, puteți utiliza opțiunea **Recuperare** din fila **Protecție** din detalii computer pentru introducerea automată a ID-ului cheii de recuperare, atât pentru endpoint-urile Windows, cât și pentru endpoint-urile macOS.

   b. Parola contului dumneavoastră GravityZone.
4. Efectuați clic pe **Arată**. Fereastra se extinde.

   În secțiunea **Informații volume** sunt prezentate următoarele date:

   a. Nume volum

b. Tipul volumului (boot sau non-boot).

c. Numele endpoint-ului (așa cum este menționat în Inventarul de rețea)

d. Cheie de recuperare. Pe Windows, cheia de recuperare este o parolă generată automat la criptarea volumului. Pe Mac, cheia de recuperare este, de fapt, parola contului utilizatorului.

5. Trimiteți cheia de recuperare utilizatorului endpoint-ului.

Pentru detalii despre criptarea și decriptarea volumelor din GravityZone, consultați „Criptare" (p. 383).

6.2.9. Sincronizarea cu Active Directory

Inventarul rețelei estee sincronizat automat cu Active Directory la intervalul specificat în secțiunea de configurare Control Center. Pentru mai multe informații, consultați capitolul de Instalare și Configurare GravityZone din Ghidul de instalare GravityZone.

Pentru sincronizarea manuală a inventarului rețelei afișat în prezent cu Active Directory:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Faceți clic pe butonul **Sincronicare cu Active Directory** din partea de sus a tabelului.
4. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

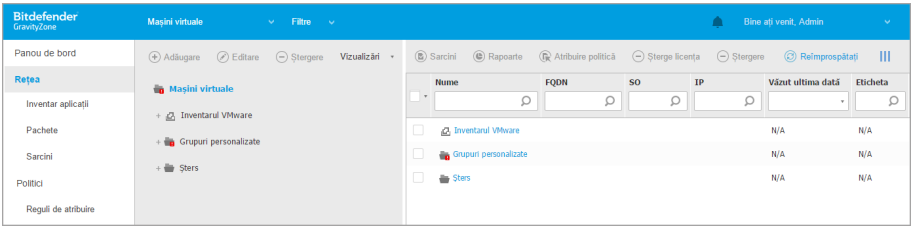
Notă
Pentru rețelele Active Directory extinse, sincronizarea poate dura mai mult.

6.3. Mașini virtuale

Pentru a vizualiza infrastructurile virtuale din contul dumneavoastră, mergeți la pagina **Rețea** și selectați **Mașini virtuale** din selectorul de vederi.

Notă
Puteți administra mașinile virtuale din ecranul **Calculatoare și mașini virtuale**, dar puteți vizualiza infrastructura virtuală și filtra conținutul acesteia folosind anumite criterii doar în ecranul **Mașini virtuale**.

Pentru detalii privind lucrul cu vizualizările de rețea, consultați „Lucrul cu Ecranele de rețea” (p. 44).



Ecranul Rețea - Mașini virtuale

Puteți vizualiza mașinile virtuale disponibile în fereastra din stânga și detalii referitoare la fiecare mașină virtuală în fereastra din dreapta.

Pentru a personaliza detaliile referitoare la mașina virtuală afișate în tabel:

1. Faceți clic pe butonul **Coloane** din partea din dreapta sus a ferestrei din dreapta.
2. Selectați coloanele pe care doriți să le vizualizați.
3. Faceți clic pe butonul **Resetare** pentru a reveni la vizualizare implicită coloane.

Fereastra din stânga afișează o vedere de tip arbore a infrastructurii virtuale. Rădăcina arborelui poartă denumirea **Mașini virtuale** și mașinile virtuale sunt grupate sub rădăcină, în următoarele categorii, în funcție de furnizorul de tehnologie:

- **Inventar Nutanix.** Conține lista de sisteme Nutanix Prism Element la care aveți acces.
- **Inventarul VMware.** Include lista serverelor vCenter la care aveți acces.
- **Inventarul Citrix.** Include lista sistemelor XenServer la care aveți acces.
- **Grupuri personalizate.** Include serverele de securitate și mașinile virtuale detectate în rețea dvs. în afara oricărui sistem vCenter Server sau XenServer.

Fereastra din stânga include și un meniu denumit **Vizualizări** din care utilizatorul poate selecta tipul de vizualizare pentru fiecare furnizor de tehnologie de virtualizare.

Pentru a avea acces la infrastructura virtualizată integrată cu Control Center, trebuie să furnizați datele de utilizator pentru fiecare sistem vCenter Server disponibil. După ce ați introdus datele, acestea sunt salvate în secțiunea Admnistrare date

de autentificare, astfel încât nu trebuie să le reintroduceți. Pentru mai multe informații, consultați capitolul „Manager Credențiale” (p. 217).

Din secțiunea **Rețea** puteți administra mașinile virtuale după cum urmează:

- Verificați starea mașinii virtuale
- Vizualizați detalii privind mașina virtuală
- Organizați mașinile virtuale în grupuri
- Sortare, filtrare și căutare
- Executarea sarcinilor
- Creați rapoarte rapide
- Atribuie politici
- Ștergerea licențelor de utilizator

Din secțiunea **Configurare > Setări rețea**, puteți configura reguli programate pentru ștergerea automată a mașinilor virtuale neutilizate din Inventarul de rețea.

6.3.1. Verificarea Stării Mașinilor Virtuale

Fiecare mașină virtuală este reprezentată în pagina de rețea prin intermediul unei pictograme specifice tipului și stării acesteia.

Consultați „Tipurile și stările obiectelor de rețea” (p. 565) pentru o listă a tuturor tipurilor de pictograme și stărilor disponibile.

Pentru informații detaliate referitoare la stare, consultați:

- Stare administrare
- Stare conectivitate
- Stare securitate

Stare administrare

Mașinile Virtuale pot avea următoarele stări de administrare:

- **Administrat** - mașinile virtuale pe care este instalată protecția Bitdefender.
- **Repornire în așteptare** - mașinile virtuale care necesită repornirea sistemului după instalarea sau actualizarea protecției Bitdefender.
- **Neadministrat** - mașini virtuale detectate pe care nu a fost instalată încă protecția Bitdefender.
- **Șters** - mașinile virtuale pe care le-ați șters din Control Center. Pentru mai multe informații, consultați capitolul „Ștergerea stațiilor de lucru din inventarul rețelei” (p. 212).

Stare conectivitate

Starea de conectivitate vizează mașinile virtuale și serverele Security Server administrate. Din acest punct de vedere, mașinile virtuale administrate pot fi:

- **Online**. O pictogramă albastră indică faptul că mașina este online.
- **Offline**. O pictogramă gri indică faptul că mașina este offline.

O mașină virtuală este offline dacă agentul de securitate este inactiv mai mult de 5 minute. Posibile motive pentru care mașinile virtuale apar ca fiind offline:

- Mașina virtuală este oprită, în stare de așteptare sau de hibernare.

  Notă
  Mașinile virtuale apar online, chiar dacă sunt blocate sau utilizatorul nu este conectat.

- Agentul de securitate nu are conectivitate cu Serverul de comunicări GravityZone:
  - Mașina virtuală poate fi deconectată de la rețea.
  - Un firewall de rețea sau router poate obstrucționa comunicarea dintre agentul de securitate și Bitdefender Control Center sau Endpoint Security Relay atribuit.
  - Mașina virtuală este în spatele unui server proxy și setările proxy nu au fost configurate corespunzător în politica aplicată.

  Avertisment
  Pentru mașinile virtuale din spatele unui server proxy, setările proxy trebuie configurate corect în pachetul de instalare al agentului de securitate. În caz contrar, mașina virtuală nu va comunica cu consola GravityZone și va apărea întotdeauna offline, indiferent dacă se aplică sau nu o politică având setările proxy corecte după instalare.

- Agentul de securitate a fost dezinstalat manual de pe mașina virtuală când aceasta nu avea conectivitate la Bitdefender Control Center sau Endpoint Security Relay atribuit. În mod normal, atunci când agentul de securitate este dezinstalat manual de pe o mașină virtuală, Control Center este notificat cu privire la acest eveniment, iar mașina virtuală este marcată ca fiind neadministrată.
- Este posibil ca agentul de securitate să nu funcționeze corect.

Pentru a afla cât timp au fost inactive mașinile virtuale:

1. Afișați exclusiv mașinile virtuale administrate. Faceți clic pe meniul **Filtre** din partea de sus a tabelului, selectați toate opțiunile "Administrate" dorite din secțiunea **Securitate**, alegeți opțiunea **Toate articolele recursiv** din secțiunea **Adâncime** și faceți clic pe **Salvare**.
2. Faceți clic pe titlul coloanei **Văzut ultima dată** pentru sortarea mașinilor virtuale după perioada de inactivitate.

Puteți ignora perioadele de inactivitate mai scurte (minute, ore), deoarece este posibil ca acestea să fie rezultatul unei stări temporare. De exemplu, mașina virtuală este în prezent oprită.

Perioadele de inactivitate mai lungi (zile, săptămâni) indică, în general, o problemă cu mașina virtuală.

Notă
Se recomandă reîmprospătarea periodică a tabelului rețelei, pentru actualizarea informațiilor referitoare la stațiile de lucru cu cele mai recente modificări.

Stare securitate

Starea de securitate vizează mașinile virtuale și serverele Security Server administrate. Puteți identifica mașinile virtuale sau serverele Security Server cu probleme de securitate verificând pictogramele de stare care afișează un simbol de avertizare:

- Cu probleme.
- Fără probleme.

O mașină virtuală sau un Security Server are probleme de securitate dacă se aplică cel puțin una dintre situațiile de mai jos:

- Protecția antimalware este dezactivată (numai pentru mașinile virtuale).
- Licența a expirat.
- Produsul Bitdefender nu este actualizat.
- Conținutul de securitate este expirat.
- Pachetul suplimentar HVI nu este actualizat.
- S-a detectat un program malware (numai pentru mașinile virtuale).
- Conexiunea cu Serviciile Cloud Bitdefender nu a putut fi stabilită din următoarele motive posibile:
  – Mașina virtuală are probleme de conectivitate la internet.

– Un firewall al rețelei blochează conexiunea cu Serviciile Ckoud Bitdefender.
– Portul 443, necesar pentru comunicarea cu Serviciile Cloud Bitdefender, este închis.

În aces caz, protecția contra programelor periculoase se bazează exclusiv pe motoarele locale când scanarea in-the-cloud este deconectată, ceea ce înseamnă că agentul de securitate nu poate oferi protecție completă în timp real.

Dacă identificați o mașină virtuală cu probleme de securitate, faceți clic pe denumire pentru afișarea ferestrei **Informații**. Puteți identifica aspectele de securitate prin pictograma ! . Asigurați-vă că ați consultat informațiile privind securitatea furnizate pe toate filele de pe pagina pentru informații. Afișați informațiile oferite de pictogramă pentru detalii suplimentare. Este posibil să fie necesare investigații locale suplimentare.

Notă
Se recomandă reîmprospătarea periodică a tabelului rețelei, pentru actualizarea informațiilor referitoare la stațiile de lucru cu cele mai recente modificări.
Endpoint-urile care nu primesc actualizări în ultimele 24 de ore sunt marcate automat drept **Cu probleme**, indiferent de versiunea conținutului de securitate de pe releu sau de pe GravityZone Update Server.

6.3.2. Vizualizarea detaliilor Mașinii virtuale

De pe pagina **Rețea**,puteți obține informații detaliate despre fiecare mașină virtuală, după cum urmează:

- Verificarea paginii **Rețea**
- Verificarea ferestrei **Informații**

Verificarea paginii Rețea

Pentru a afla detalii despre o mașină virtuală, consultați informațiile disponibile în tabelul de pe panoul din dreapta de pe pagina **Rețea**

Puteți adăuga sau elimina coloane cuprinzând informații despre mașina virtuală efectuând clic pe butonul III **Coloane** din partea dreaptă sus a panoului.

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga.

Toate mașinile virtuale disponibile din grupul selectat sunt afișate în tabelul din panoul din dreapta.

4. Puteți detecta cu ușurință starea mașinilor virtuale, verificând pictograma corespunzătoare. Pentru informații detaliate, consultați capitolul „Verificarea Stării Mașinilor Virtuale” (p. 109).
5. Verificați informațiile afișate în tabel pentru fiecare mașină virtuală.

   Utilizați antetul coloanei pentru a căuta anumite mașini virtuale, conform criteriilor disponibile:

   - **Nume**: denumirea mașinii virtuale.
   - **FQDN**: nume de domeniu calificat complet care include denumirea gazdei și numele de domeniu.
   - **SO**: sistemul de operare instalat pe mașina virtuală.
   - **IP**: adresa IP a mașinii virtuale.
   - **Vazut ultima dată**: data și ora la care mașina virtuală a fost văzură ultima dată online.

     Notă
     Este important să monitorizați câmpul **Văzut ultima dată** deoarece intervalele lungi de inactivitate pot indica o problemă de comunicare sau o mașină virtuală deconectată.

   - **Etichetă**: un șir personalizat cu informații suplimentare despre stația de lucru. Puteți adăuga o etichetă în fereastra **Informații**a mașinii virtuale și să o folosiți apoi la căutare.
   - **Politică**: politica aplicată mașinii virtuale, cu link pentru vizualizarea sau modificarea setărilor pentru politică.

Verificarea ferestrei Informații

Pe panoul din dreapta de pe pagina **Network**, efectuați clic pe numele mașinii virtuale care vă interesează, pentru afișarea ferestrei **Informații**. În această fereastră se afișează doar datele disponibile pentru mașina virtuală selectată, grupate pe câteva file.

Aveți în continuare lista completă de informații pe care le puteți găsi în fereastra **Information**, în funcție de tipul mașinii (mașină virtuală, instanță Security Server) și informațiile de securitate specifice acesteia.

Fila generală

- Informații generale despre mașina virtuală, cum ar fi numele, informații FQDN, adresa IP, sistemul de operare, infrastructura, grupul părinte și situația conexiunilor actuale.

  În această secțiune puteți atribui o etichetă mașinii virtuale. Veți putea găsi rapid mașini virtuale cu aceeași etichetă și veți putea acționa asupra lor, indiferent unde sunt ele localizate în rețea. Pentru mai multe informații despre filtrarea mașinilor virtuale, consultați „Sortarea, filtrarea și căutarea Mașinilor Virtuale" (p. 122).

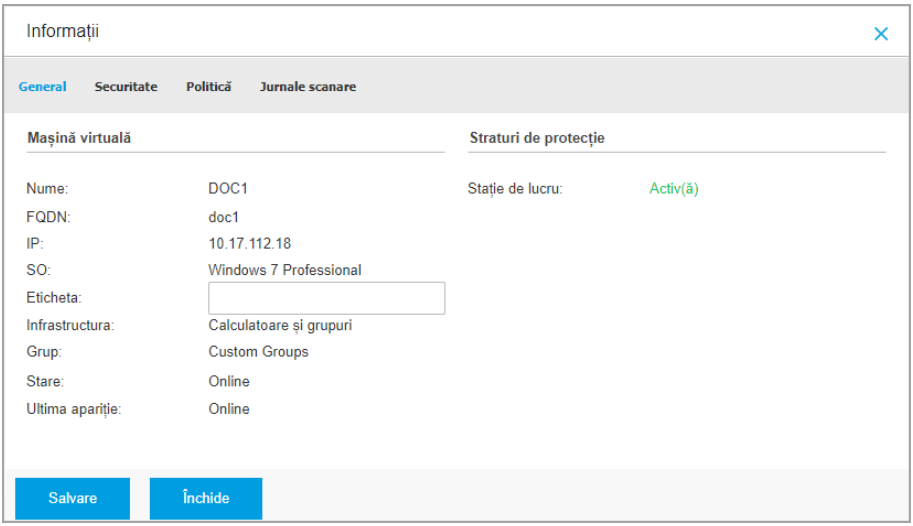
- **Cerințe preliminare HVI**, conținând informații despre posibilitatea sau imposibilitatea de a utiliza Security Server pentru instalarea protecției HVI. Astfel, dacă gazda Security Server funcționează pe o versiune XenServer suportată, iar pachetul suplimentar este instalat, puteți activa HVI pe mașinile virtuale de pe gazda respectivă.

  Notă
  Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

- Informații privind straturile de protecție, inclusiv lista cu tehnologiile de securitate pe care le obțineți cu soluția GravityZone, precum și situația licențelor acestora care poate fi:
  - **Disponibilă / Activă** – cheia de licență pentru acest nivel de protecție este activă pe mașina virtuală.
  - **Expirată** – cheia de licență pentru acest strat de protecție a expirat.
  - **În așteptare** – cheia de licență nu a fost confirmată încă.

  Notă
  Informații suplimentare referitoare la straturile de protecție sunt disponibile în secțiunea **Protecție**.

- **Conexiune la releu**: numele, IP-ul și eticheta releului la care este conectată mașina virtuală, dacă este cazul.



Fereastra de informații - secțiunea General

Fila pentru protecție

Această filă conține detalii despre fiecare strat de protecție cu licență pentru această stație de lucru. Detaliile se referă la:

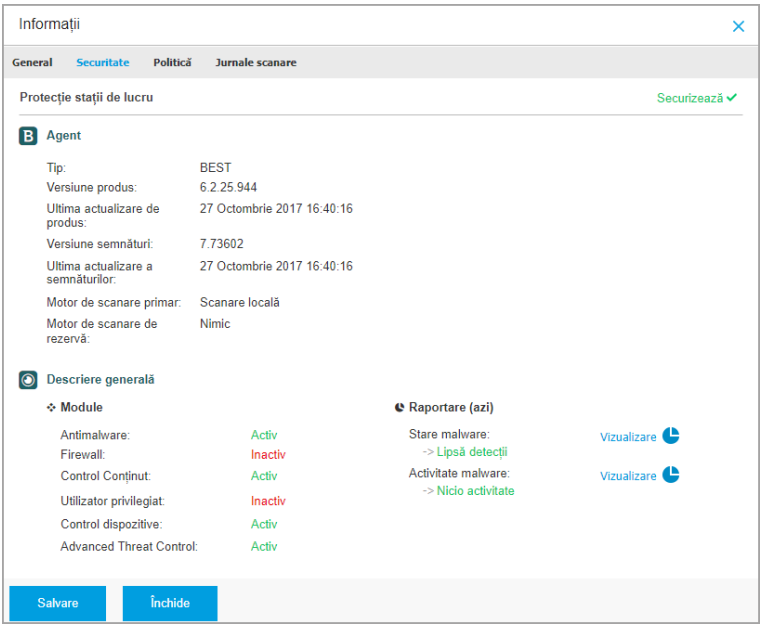
- Informații privind agentul de securitate, cum ar fi denumirea și versiunea produsului, configurația motoarelor de scanare și starea de actualizare. Pentru Protecția Exchange, sunt disponibile, de asemenea, motorul antispam și versiunea semnăturilor.
- Starea de securitate pentru fiecare strat de protecție. Această stare apare în partea dreaptă a numelui stratului de protecție:
  - **Securizat**, când nu există probleme de securitate raportate pentru stațiile de lucru la care s-a aplicat strat de protecție.
  - **Vulnerabil**, când există probleme de securitate raportate pentru stațiile de lucru la care s-a aplicat strat de protecție. Pentru mai multe detalii, vă rugăm consultați „Stare securitate” (p. 111).

- Security Server asociat. Fiecare Security Server asociat este afișat în cazul configurării fără agent sau când motoarele de scanare ale agenților de securitate sunt setate pentru a utiliza scanarea la distanță. Informațiile Security Server vă ajută să identificați aplicația virtuală și să obțineți starea de actualizare a acesteia.
- Informațiile referitoare la NSX, cum ar fi starea de etichetare viruși și grupul de securitate căruia îi aparține mașina virtuală. Dacă ați aplicat o etichetă de securitate, aceasta vă informează că mașina este infestată. În caz contrar, mașina este curată sau nu s-au folosit etichete de securitate.
- Starea modulelor de protecție. Puteți vizualiza cu ușurință modulele de protecție care au fost instalate pe stația de lucru și, de asemenea, starea modulelor disponibile (**Pornit/Oprit**) setată prin intermediul politicii aplicate.
- O prezentare rapidă privind activitatea modulelor și raportarea programelor periculoase pe parcursul zilei în curs.

  Executați clic pe linkul **Vizualizare** pentru a accesa opțiunile de raportare și genera apoi raportul. Pentru mai multe informații, consultați „Crearea rapoartelor" (p. 495)
- Informații privind stratul de protecție Sandbox Analyzer:
  - Situația utilizărilor Sandbox Analyzer pe mașina virtuală, afișată în partea dreaptă a ferestrei:
    - **Activ**: Sandbox Analyzer este licențiat (disponibil) și activat prin intermediul politicii pe mașina virtuală.
    - **Inactiv**: Sandbox Analyzer este licențiat (disponibil) dar nu este activat prin intermediul politicii pentru mașina virtuală.
  - Denumirea agentului care acționează ca senzor de alimentare.
  - Starea modulului pe mașina virtuală:
    - **Pornit** - Sandbox Analyzer este activat prin intermediul politicii pentru mașina virtuală.
    - **Oprit** - Sandbox Analyzer nu este activat pentru mașina virtuală prin intermediul politicii.
  - Amenințările detectate în ultima săptămână efectuând clic pe linkul **Vizualizare** pentru accesarea raportului.
- Informațiile suplimentare cu privire la modulul de Criptare, de exemplu:

– Volume detectate (menționând unitatea boot).
– Starea criptării pentru fiecare volum (care poate fi **Criptat**, **Criptare în curs**, **Decriptare în curs**, **Necriptat**, **Blocat** or **În pauză**).

  Efectuați clic pe linkul **Recuperare** pentru a extrage cheia de recuperare pentru volumul criptat asociat. Pentru detalii referitoare la extragerea cheilor de recuperare, consultați „Utilizarea Managerului de recuperare pentru volumele criptate” (p. 165).



Fereastra pentru informații - Fila pentru protecție

Pentru Security Server, această filă conține informații referitoare la modulul Protecție dispozitive stocare. Detaliile se referă la:

- Stare serviciu:
  – **N/A** – Există o licență pentru modulul Protecția dispozitivelor de stocare, dar serviciul nu a fost configurat încă.
  – **Activat** – serviciul este activat în politică și funcțional.
  – **Dezactivat** – serviciul nu funcționează, fie pentru că a fost dezactivat din politică, fie pentru din cauza expirării codului de licență.

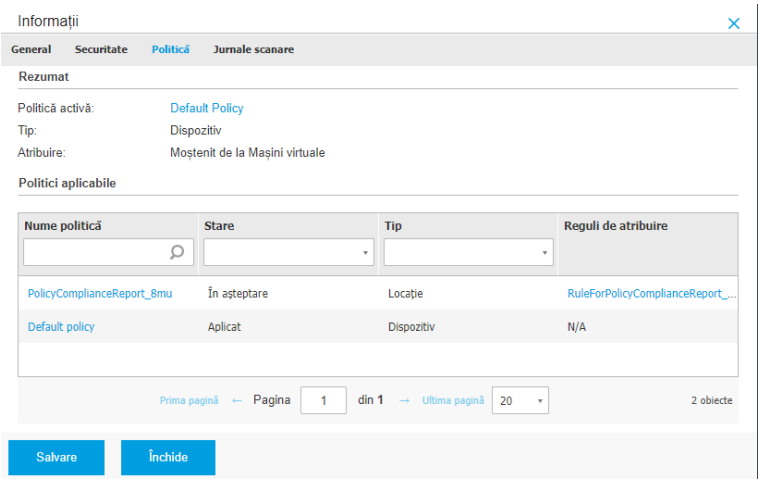
- Lista dispozitivelor de stocare conectate conforme cu ICAP, cu următoarele detalii:
  - Numele dispozitivului de stocare
  - IP-ul dispozitivului de stocare
  - Tipul dispozitivului de stocare
  - The date and time of the last communication between the storage device and Security Server.

Fila pentru politici

Unei mașini virtuale i se pot aplica una sau mai multe politici, însă doar o singură politică poate fi activă la un moment dat. Fila **Polică** afișează informații despre toate politicile aplicabile acelei mașini virtuale.

- Numele politicii active. Faceți clic pe denumirea politicii pentru a deschide un șablon și a-i vizualiza setările.
- Tipul politicii active, care poate fi:
  - **Dispozitiv**: când politica este atribuită manual mașinii virtuale de către administratorul de rețea.
  - **Locație**: o politică bazată pe reguli, atribuită automat mașinii virtuale dacă setările de rețea ale respectivei mașini virtuale corespund condițiilor regulii de atribuire existente.
  - **Utilizator**: o politică bazată pe reguli, atribuită automat stației de lucru dacă corespunde țintei Active Directory specificată într-o regulă de atribuire existentă.

    De exemplu, o mașină poate avea atribuite două politici în funcție de utilizator, una pentru administratori și una pentru alți angajați. O politică devine activă în momentul în care se autentifică utilizatorul care deține drepturile corespunzătoare.
  - **Extern (NSX)**: când politica este definită în mediul VMware NSX.
- Tipul de atribuire a politicii active, care poate fi:
  - **Direct**: când politica este aplicată direct mașinii virtuale.
  - **Preluată**: când mașina virtuală preia politica de la un grup părinte.
- **Politici aplicabile**: afișează lista politicilor legate de regulile de atribuire existente. Aceste politici se pot aplica mașinii virtuale când aceasta corespunde condițiilor din regulile de atribuire aferente.

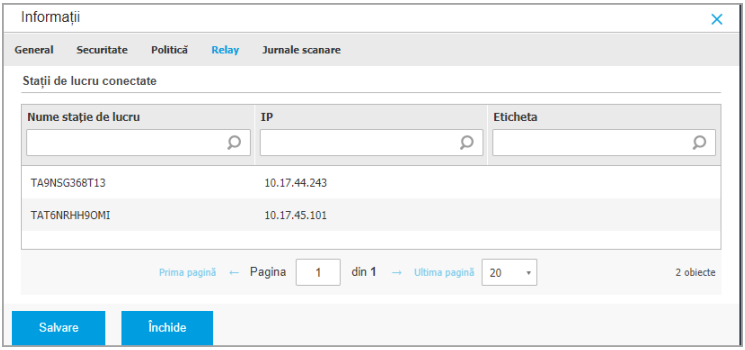


Fereastra de informații - secțiunea Politică

Pentru mai multe informații privind politicile, consultați„Administrarea politicilor” (p. 221)

Fila pentru releu

Secțiunea **Releu** este disponibilă numai pentru mașinile virtuale cu rol de releu. Această secțiune afișează informații referitoare la stațiile de lucru conectate la releul curent, cum ar fi denumirea, adresa IP și eticheta.



Fereastra de informații - secțiunea Releu

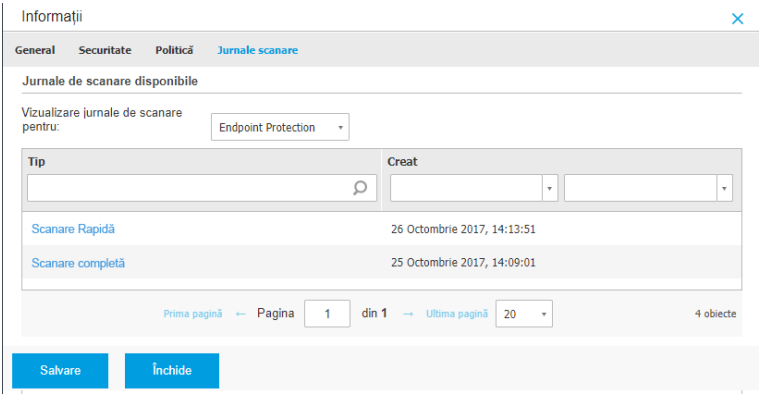
Fila pentru scanare jurnale

În secțiunea **Jurnale scanări** se afișează informații detaliate referitoare la toate sarcinile de scanare efectuate pe mașina virtuală.

Jurnalele sunt grupate după stratul de protecție și puteți selecta din meniul derulant pentru ce strat doriți să afișați jurnalele.

Faceți clic pe sarcina de scanarea care vă interesează și se va deschide jurnalul într-o nouă pagină a browserului.

Dacă sunt disponibile multe jurnale de scanare, acestea pot ocupa mai multe pagini. Pentru a trece de la o pagină la alta, folosiți opțiunile de navigație din partea de jos a tabelului. Dacă există prea multe intrări, puteți folosi opțiunile de filtrare disponibile în partea de sus a tabelului.



Fereastra de informații - secțiunea Jurnale de scanare

Fiecare proprietate din această fereastră care generează probleme de securitate este marcată cu pictograma ! . Verificați informațiile oferite de pictogramă pentru detalii suplimentare. Este posibil să fie necesare investigații locale suplimentare.

6.3.3. Organizarea mașinilor virtuale în grupuri

Puteți administra grupurile de mașini virtuale în fereastra din stânga a paginii **Rețea** în folderul **Grupuri personalizate**.

Mașinile virtuale importate din Nutanix Prism Element sunt grupate în directorul **Inventar Nutanix**. Mașinile virtuale importate din VMware vCenter sunt grupate în folderul **Inventarul VMware**. Mașinile virtuale importate din XenServer sunt grupate

în folderul **Inventarul Citrix**. Nu puteți modifica Inventarul Nutanix, Inventarul VMware sau Inventarul Citrix. Nu puteți decât să vizualizați și să administrați mașinile virtuale corespunzătoare.

Toate mașinile virtuale care nu sunt administrate de sistemele Nutanix Prism, vCenter sau XenServer sunt detectate de funcția Descoperire rețea și amplasate în **Grupuri personalizate**, de unde le puteți organiza în grupuri după cum doriți. Beneficiul major este acela că puteți utiliza politicile de grup pentru a începlini diferite cerințe de securitate.

În **Grupuri personalizate**, puteți crea, șterge, redenumi și muta grupurile de mașini virtuale, într-o structură personalizată de tip arbore.

Notă

- Un grup poate conține atât mașini virtuale, cât și alte grupuri.
- Dacă selectați un grup din fereastra din stânga, puteți vizualiza toate mașinile virtuale, cu excepția celor din sub-grupuri. Pentru a vizualiza toate mașinile virtuale din grup și din sub-grupurile acestuia, faceți clic pe meniul **Filtre** din partea de sus din dreapta sus a tabelului și selectați **Toate obiectele recursiv** din secțiunea **Adâncime**.

Crearea unui nou grup

Înainte de a începe să creați grupuri, gândiți-vă la motivele pentru care aveți nevoie de ele și creați o schemă de grupare. De exemplu, puteți grupa mașinile virtuale pe baza unuia sau mai multora dintre criteriile următoare:

- Structura organizatorică (Vânzări, Marketing, Asigurarea calității, Dezvoltare software, Management etc.).
- Necesitățile de securitate (desktopuri, laptopuri, servere etc.).
- Locația (sediu central, birouri locale, personal la distanță, birouri de acasă etc.).

Pentru a organiza rețeaua în grupuri:

1. Selectați **Grupuri personalizate** din fereastra din stânga.
2. Faceți clic pe butonul ⊕ **Adăugare grup** din partea de sus a ferestrei din stânga.
3. Introduceți o denumire sugestivă pentru grup și faceți clic pe **OK**. Noul grup este afișat în **Grupuri personalizate** .

Redenumirea unui grup

Pentru a redenumi un grup:

1. Selectați grupul din fereastra din stânga.
2. Faceți clic pe butonul **Editare grup** din partea de sus a ferestrei din stânga.
3. Introduceți noua denumire în câmpul corespunzător.
4. Faceți clic pe **OK** pentru confirmare.

Mutarea grupurilor și a mașinilor virtuale

Puteți muta entitățile oriunde în interiorul ierarhiei **Grupuri personalizate**. Pentru a muta o entitate, trageți-o și inserați-o din fereastra din dreapta în grupul dorit din fereastra din stânga.

Notă

Entitatea mutată va prelua politicile de politică ale noului grup mamă, cu excepția cazului în care funcția de preluare a politicii a fost dezactivată și i s-a alocat o nouă politică. Pentru detalii privind preluarea politicii, consultați „Politici de securitate” (p. 220).

Ștergerea unui grup

Un grup nu poate fi șters dacă include cel puțin o mașină virtuală. Mutați toate mașinile virtuale pe care doriți să le ștergeți din grupul curent în alte grupuri. Dacă grupul include sub-grupuri, puteți opta pentru mutarea integrală a sub-grupurilor mai degrabă decât a mașinilor virtuale individuale.

Pentru a șterge un grup:

1. Selectați grupul gol.
2. Faceți clic pe butonul **Ștergere grup** din partea de sus a ferestrei stânga. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

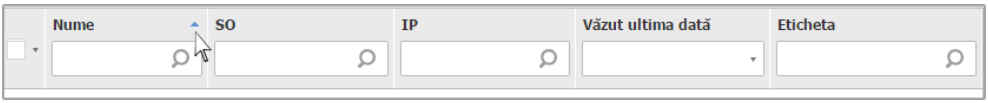
6.3.4. Sortarea, filtrarea și căutarea Mașinilor Virtuale

În funcție de numărul de mașini virtuale, tabelul acestora se poate întinde pe mai multe pagini (implicit, sunt afișate doar 20 intrări pe pagină). Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului. Pentru a modifica numărul de intrări afișate pe pagină, selectați o opțiune din meniul de lângă butoanele de navigație.

Dacă există prea multe intrări, puteți folosi casetele de căutare de sub titlurile coloanelor sau meniul **Filtre** din partea de sus a paginii, pentru a afișa doar entitățile care vă interesează. De exemplu, puteți căuta o anumită mașină virtuală sau alege să vizualizați doar mașinile virtuale administrate.

Sortarea mașinilor virtuale

Pentru a sorta datele după o anumită coloană, faceți clic pe titlurile acestora. De exemplu, dacă doriți să ordonați mașinile virtuale după denumire, faceți clic pe titlul **Nume**. Dacă faceți din nou clic pe titlu, mașinile virtuale vor fi afișate în ordine inversă.



Sortarea calculatoarelor

Filtrarea mașinilor virtuale

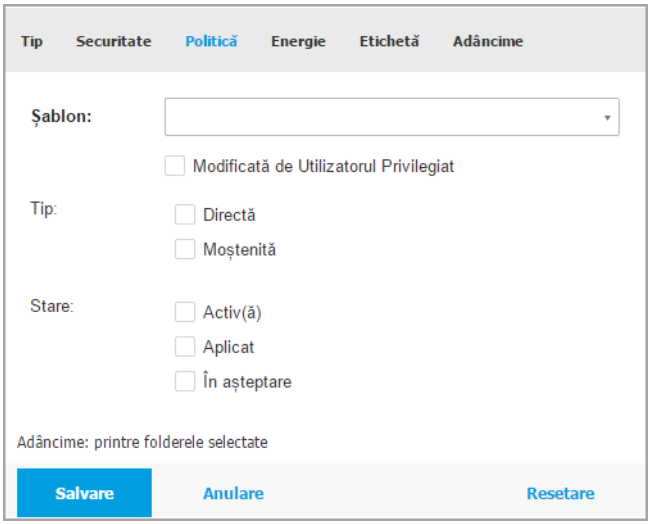
1. Selectați grupul dorit din fereastra din stânga.
2. Faceți clic pe meniul **Filtere** din partea de sus a zonei ferestrelor de rețea.
3. Folosiți criteriile de filtrare după cum urmează:
   - **Tip**. Selectați tipul de entități virtuale care vor fi afișate.

Mașini virtuale - Filtrare după tip

- **Securitate**. Selectați starea de administrare a proitecției și/sau starea de securitate după care doriți să filtrați obiectele din rețea. De exemplu, puteți alege să vizualizați doar mașinile Security Server sau puteți vizualiza doar stațiile de lucru cu probleme de securitate.

Mașini virtuale - Filtrare după securitate

- **Politică**. Selectați modelul de politică dorit pentru filtrarea mașinilor virtuale după tipul de atribuire a politicii (Directă sau Moștenită), precum și starea de atribuire a politicii (Activă, Aplicată sau În așteptare).

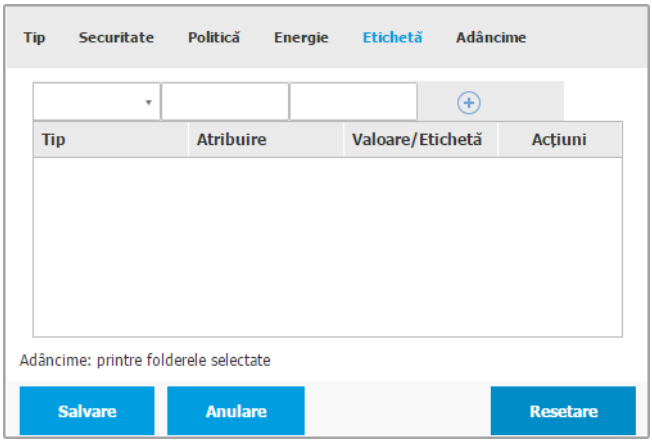


Mașini virtuale - Filtrare după politică

- **Energie**. Puteți selecta să afișați mașinile virtuale online, offline și suspendate.

Mașini virtuale - Filtrare după stare

- **Etichete**. Puteți opta pentru filtrarea mașinilor virtuale după etichetele și atributele definite în mediul de virtualizare.



Mașini virtuale - Filtrare după etichete

- **Adâncime**. Când administrați o rețea de mașini virtuale de tip arbore, mașinile virtuale din sub-grupuri nu sunt afișate implicit. Selectați opțiunea **Toate obiectele recursiv** pentru a vedea toate mașinile virtuale din grupul curent și din sub-grupuri.

Mașini virtuale - Filtrare după adâncime

Notă
Faceți clic pe **Resetare** pentru a șterge filtrul și pentru afișarea tuturor mașinilor virtuale.

4. Faceți clic pe **Salvare** pentru a filtra mașinile virtuale conform criteriilor selectate.

Căutarea mașinilor virtuale

1. Selectați containerul dorit din fereastra din stânga.
2. Introduceți termenul de căutare în caseta corespunzătoare de sub titlurile coloanelor (Nume, SO sau IP) din fereastra din dreapta. De exemplu, introduceți IP-ul mașinii virtuale pe care o căutați în câmpul **IP**. În tabel se va afișa doar mașina virtuală care corespunde criteriilor de căutare.

   Ștergeți informațiile din caseta de căutare pentru afișarea listei complete de mașini virtuale.

6.3.5. Executarea sarcinilor pe mașinile virtuale

De pe pagina **Rețea**, puteți executa de la distanță o serie de sarcini administrative pe mașinile virtuale.

Iată ce puteți face:

- „Scanează” (p. 128)
- „Sarcini de aplicare a patch-urilor” (p. 138)
- „Scanare Exchange” (p. 141)
- „Instalare” (p. 145)
- „Dezinstalare client” (p. 150)
- „Actualizare” (p. 151)
- „Reconfigurare client” (p. 152)
- „Descoperire rețea” (p. 153)
- „Descoperire aplicații” (p. 154)
- „Repornire sistem” (p. 154)
- „Instalarea Security Server” (p. 155)
- „Dezinstalarea Security Server” (p. 158)
- „Actualizarea Security Server” (p. 158)
- „Instalați pachetul suplimentar HVI” (p. 159)
- „Dezinstalare pachet suplimentar HVI” (p. 160)
- „Actualizare Pachet suplimentar HVI” (p. 161)

Puteți opta pentru generarea unor sarcini individual pentru fiecare mașină virtuală sau pentru grupuri de mașini virtuale. De exemplu, puteți instala Bitdefender Endpoint Security Tools de la distanță, pe un grup de mașini virtuale neadministrate. Ulterior, puteți crea o sarcină pentru o anumită mașină virtuală din același grup.

Pentru fiecare mașină virtuală, puteți executa sarcini compatibile. De exemplu, dacă selectați o mașină virtuală neadministrată, nu puteți selecta decât opțiunea de instalare a agentului de securitate, toate celelalte sarcini fiind dezactivate.

Pentru un grup, sarcina selectată va fi creată exclusiv pentru mașinile virtuale compatibile. Dacă niciuna dintre mașinile virtuale din grup nu este compatibilă cu sarcina selectată, veți fi informat că sarcina nu a putut fi generată.

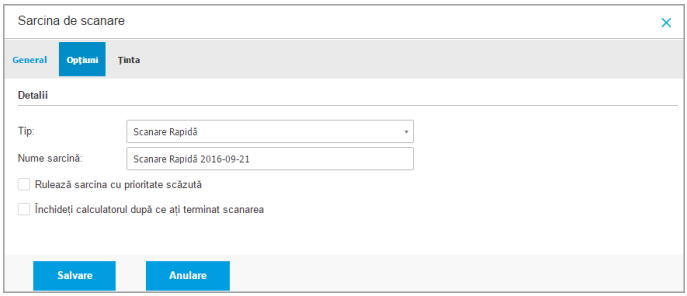
După ce a fost generată, sarcina va începe să ruleze imediat pe mașinile virtuale online. Dacă o mașină virtuală este offline, sarcina va rula imediat după ce aceasta este din nou online.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Scanează

Pentru a executa o sarcină de scanare de la distanță pe mai multe mașini virtuale:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate entitățile din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare corespunzătoare obiectelor pe care doriți să le scanați.
5. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Scanare**. Va apărea o fereastră de configurare.
6. Configurați opțiunile de scanare:
   - În secțiunea **General**, puteți selecta tipul de scanare și puteți introduce o denumire pentru sarcina de scanare. Scopul denumirii scanării este acela de a vă ajuta să identificați cu ușurință scanarea curentă pe pagina **Sarcini**.



Sarcină de scanare mașini virtuale - Configurarea setărilor generale

Selectați tipul unei scanări din meniul **Tip**:

– Funcția **Scanare rapidă** este preconfigurată pentru a permite numai scanarea locațiilor de sistem critice și a noilor fișiere. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o mică parte din resursele de sistem necesare pentru o scanare antivirus obișnuită.

  Atunci când se detectează programe malware sau rootkit-uri, Bitdefender începe automat procesul de dezinfectare. Dacă, din orice motiv, fișierul nu poate fi dezinfectat, atunci acesta este mutat în carantină. Acest tip de scanare ignoră fișierele suspecte.

– **Scanare completă** verifică întregul sistem, pentru identificarea tuturor tipurilor de programe periculoase care amenință securitatea acestuia, cum ar fi virușii, aplicațiile spion, rookit-urile și altele.

  Bitdefender încearcă automat să dezinfecteze fișierele detectate ca fiind infectate cu malware. În cazul în care malware-ul nu poate fi eliminat, acesta este mutat în carantină, unde nu poate face niciun rău. Fișierele suspecte sunt ignorate. Dacă doriți să întreprindeți acțiuni și asupra fișierelor suspecte sau dacă doriți alte acțiuni implicite pentru fișierele infectate, selectați efectuarea unei Scanări personalizate.

– **Scanare memorie** verifică programele care rulează în memoria mașinii virtuale.

– **Scanare rețea** este un tip de scanare personalizată, care vă permite să scanați unitățile din rețea folosind agentul de securitate Bitdefender instalat pe mașina virtuală țintă.

  Pentru ca sarcina de scanare a rețelei să funcționeze:

- Trebuie să alocați sarcina unei singure stații de lucru din rețea.
- Trebuie să introduceți datele de autentificare ale unui cont de utilizator cu permisiuni de citire/editare pe unitățile rețelei țintă, pentru ca agentul de securitate să poată accesa și să inițieze acțiuni în cadrul acestor unități de rețea. Datele de autentificare necesare pot fi configurate în secțiunea **Țintă** din fereastra de sarcini.

– **Scanare personalizată** vă permite să selectați locațiile pe care doriți să le scanați și să configurați opțiunile de scanare.

Pentru scanările de memorie, rețea și personalizate, aveți, de asemenea, următoarele opțiuni:

– **Rulează sarcina cu prioritate scăzută**. Selectați această casetă pentru a diminua prioritatea procesului de scanare și pentru a permite altor programe să ruleze mai rapid. Aceasta va mări timpul necesar pentru finalizarea procesului de scanare.

Notă
Această opțiune se aplică doar pentru Bitdefender Endpoint Security Tools și Endpoint Security (agent legacy).

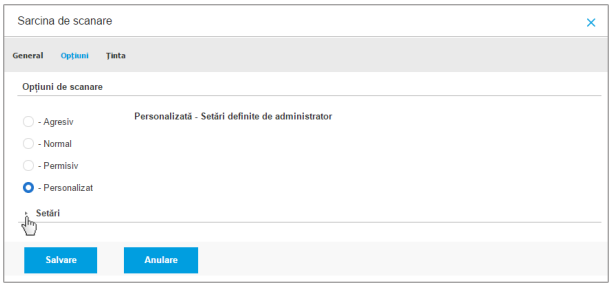
– **Închideți calculatorul după ce ați terminat scanarea**. Bifați această casetă pentru a opri calculatorul dacă nu intenționați să îl utilizați pentru o perioadă.

Notă
Această opțiune se aplică pentru Bitdefender Endpoint Security Tools, Endpoint Security (agent legacy) și Endpoint Security for Mac.

Pentru scanări personalizate, configurați următoarele setări:

– Mergeți la secțiunea **Opțiuni** pentru a seta opțiunile de scanare. Faceți clic pe nivelul de securitate care corespunde cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Folosiți descrierea din partea dreaptă a scalei, pentru a vă ghida alegerea.

  În funcție de profilul selectat, opțiunile de scanare din secțiunea **Setări** sunt configurate automat. Cu toate acestea, dacă doriți, le puteți configura detaliat. În acest scop, selectați opțiunea **Personalizat** și apoi extindeți secțiunea **Setări**.



Sarcină de scanare mașini virtuale - Configurarea scanării personalizate

Sunt disponibile următoarele opțiuni:

- **Tipuri de fișiere.** Folosiți aceste opțiuni pentru a specifica tipurile de fișiere pe care doriți să le scanați. Puteți seta agentul de securitate să scaneze toate fișierele (indiferent de extensie), fișierele de aplicație sau extensiile specifice de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor asigură cea mai bună protecție în timp ce scanarea aplicațiilor poate fi utilizată pentru efectuarea unei scanări mai rapide.

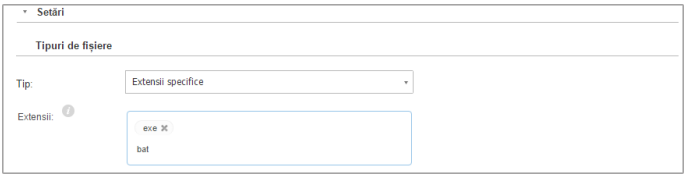
  Notă

  Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Tipuri de fișiere de aplicații" (p. 567).

  Dacă doriți să scanați doar fișiere cu anumite extensii, selectați **Extensii definite de utilizator** din meniu și introduceți extensiile în câmpul de editare, apăsând `Enter` după fiecare.

  Important

  Agenții de securitate Bitdefender instalați pe sistemele de operare Windows și Linux scanează majoritatea formatelor .ISO, dar nu aplică niciun fel de măsuri asupra acestora.



Opțiuni sarcină de scanare Mașini Virtuale - Adăugarea extensiilor definite de utilizator

- **Arhive.** Arhivele cu fișiere infestate nu sunt o amenințare directă pentru securitatea sistemului. Programele periculoase pot afecta sistemul numai dacă fișierul infestat este extras din arhivă și executat fără ca protecția în timp real să fie activată. Cu toate acestea, se recomandă să scanați arhivele pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

  Important
  Scanarea fișierelor arhivate crește timpul total necesar pentru scanare și necesită mai multe resurse de sistem.

  – **Scanare în arhive.** Selectați această opțiune dacă doriți să scanați fișierele arhivate, pentru identificarea de malware. Dacă decideți să utilizați această opțiune, puteți configura următoarele opțiuni de optimizare:

    - **Limitare dimensiune arhivă la (MB).** Puteți seta o dimensiune limită acceptată pentru arhivele care vor fi scanate. Selectați căsuța corespunzătoare și introduceți dimensiunea maximă a arhivei (exprimată în MB).

    - **Adâncime maximă arhivă (niveluri).** Selectați caseta de bifare corespunzătoare și alegeți adâncimea maximă a arhivei din meniu. Pentru performanțe superioare, alegeți cea mai mică valoare; pentru protecție maximă, alegeți cea mai mare valoare.

  – **Scanare arhive de e-mail.** Selectați această opțiune dacă doriți să activați scanarea fișierelor atașate la mesajele e-mail și bazele de date e-mail, inclusiv format de fișiere de tipul .eml, .msg, .pst, .dbx, .mbx, .tbb și altele.

Important
Scanarea arhivei e-mail necesită numeroase resurse și poate afecta performanțele sistemului.

- **Diverse.** Selectați casetele de bifare corespunzătoare pentru a activa opțiunile de scanare dorite.
  - **Scanare sectoare de boot.** Scanează sectoarele de boot ale sistemului. Acest sector al hard disk-ului conține codul de mașină virtuală necesar pentru a iniția procesul de boot. Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.
  - **Scanează regiștrii.** Selectați această opțiune pentru a scana cheile de regiștri. Regiștrii Windows sunt o bază de date care stochează setările de configurare și opțiunile pentru componentele sistemului de operare Windows, precum și pentru aplicațiile instalate.
  - **Scanează după rootkituri.** Selectați această opțiune pentru a lansa procesul de scanare pentru identificarea rootkit-urilor și a obiectelor ascunse, cu ajutorul acestui software.
  - **Scanare după keyloggers.** Selectați această opțiune pentru a scana software-urile de tip keylogger. Aplicațiile de tip keylogger nu sunt periculoase prin natura lor, însă pot fi utilizate cu intenții răuvoitoare. Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.
  - **Scanează memoria.** Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului.
  - **Scanează fișiere cookie.** Selectați această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe mașina virtuală.
  - **Scanează doar fișierele noi și cele modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
  - **Scanare pentru aplicații potențial nedorite (PUA).** O aplicație potențial nedorită (PUA) este un program care ar putea fi nedorit pe PC, care uneori vine la pachet cu software-ul freeware. Astfel

de programe pot fi instalate fără consimțământul utilizatorului (numite și adware), sau vor fi incluse în mod implicit în kit-ul de instalare în mod expres (ad-supported). Efectele potențiale ale acestor programe includ afișarea de pop-up-uri, instalarea de bare de instrumente nedorite în browser-ul implicit sau rularea mai multor procese în fundal și încetinirea performanței PC-ului.

– **Scanare volume detașabile.** Selectați această opțiune pentru a scana toate unitățile detașabile atașate la mașina virtuală.

- **Acțiuni.** În funcție de tipul de fișier detectat, următoarele acțiuni sunt aplicate în mod automat:

  – **La detectarea unui fișier infectat.** Bitdefender detectează fișierele ca fiind infectate folosind diverse mecanisme avansate, printre care semnăturile malware, învățarea automată și tehnologiile bazate pe inteligență artificială (AI). În mod normal, agentul de securitate Bitdefender poate șterge codul malware din fișierul infestat și poate reconstitui fișierul inițial. Această operațiune este cunoscută sub denumirea de dezinfectare.

    În cazul în care este detectat un fișier infectat, agentul de securitate Bitdefender va încerca în mod automat să-l dezinfecteze. Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

    Important
    Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

  – **La detectarea unui fișier suspect.** Fișierele sunt detectate ca fiind suspecte de către analiza euristică și alte tehnologii Bitdefender. Acestea asigură o rată mare de detecție, însă utilizatorii trebuie să fie conștienți că există și rezultate fals pozitive (fișiere neinfectate detectate ca fiind suspecte) în unele cazuri. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

    Sarcinile de scanare sunt configurate implicit să ignore fișierele suspecte. Ar putea fi util să modificați sarcina implicită, pentru a trece fișierele suspecte sub carantină. Fișierele sub carantină sunt

transmise regulat spre analiză la Laboratoarele Bitdefender. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

– **La detectarea unui rootkit.** Rootkit-urile reprezintă aplicații specializate utilizate pentru ascunderea fișierelor de sistemul de operare. Deși nu sunt periculoase, rootkit-urile sunt adesea utilizate pentru ascunderea programelor periculoase sau pentru a disimula prezența unui intrus în sistem.

  Rootkit-urile și fișierele ascunse detectate sunt ignorate implicit.

Atunci când pe o mașină virtuală NSX este identificat un virus, Security Server aplică automat mașinii virtuale o Etichetă de securitate, cu condiția ca această opțiune să fi fost selectată la integrarea vCenter Server.

În acest scop, NSX include trei etichete de securitate, specifice severității amenințării:

– `ANTI_VIRUS.VirusFound.threat=redus`, se aplică atunci când Bitdefender identifică un program malware cu risc redus, pe care îl poate șterge.

– `ANTI_VIRUS.VirusFound.threat=mediu`, se aplică în cazul în care Bitdefender nu poate șterge fișierele infectate, dar le dezinfectează.

– `ANTI_VIRUS.VirusFound.threat=ridicat`, e aplică în cazul în care Bitdefender nu poate șterge și nu poate dezinfecta fișierele infectate, dar blochează accesul la acestea.

Puteți izola mașinile infestate prin crearea unor grupuri de securitate cu participare dinamică, bazată pe etichetele de securitate.

Important

– Dacă Bitdefender identifică pe o mașină amenințări cu niveluri de securitate diferitem va aplica toate etichetele corespunzătoare.

– O etichetă de securitate este ștearsă de pe o mașină doar după efectuarea unei Scanări complete și după dezinfestarea mașinii.

Deși nu este recomandat, puteți modifica acțiunile implicite. Puteți preciza o a doua acțiune de aplicat în cazul în care prim eșuează,

precum și acțiuni diferite pentru fiecare categorie. Alegeți din meniurile corespunzătoare prima și a doua acțiune de aplicat pentru fiecare tip de fișier detectat. Următoarele acțiuni sunt disponibile:

Dezinfectează
Elimină codul periculos din fișierele infectate. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate.

Mută fișierele în carantină
Mutați fișierele detectate din locația curentă, în folderul de carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Fișierele în carantină pot fi gestionate de pe pagina Carantină a consolei.

Ștergere
Ștergeți fișierele detectate de pe disc, fără nicio avertizare. Se recomandă să evitați această acțiune.

Ignoră
Nu se vor lua niciun fel de măsuri împotriva fișierelor detectate. Acește fișiere vor fi doar afișate în jurnalul de scanare.

– Mergeți la secțiunea **Țintă** pentru a adăuga locațiile pe care doriți să le scanați de pe mașinile virtuale.

  În secțiunea **Țintă scanare**, puteți adăuga un fișier sau folder nou pentru a fi scanat:

  a. Selectați o locație predefinită din meniul derulant sau introduceți **Căi specifice** pe care doriți să le folosiți.

  b. Specificați calea către obiectul de scanat în câmpul de editare.

  - Dacă ați ales o locație predefinită, completați calea, după caz. De exemplu, pentru a scana integral folderul `Program Files`, este suficient să selectați locația predefinită corespunzătoare din meniul derulant. Pentru a scana un anumit folder din `Program Files`, trebuie să completați calea adăugând o bară oblică inversă (\) și denumirea folderului.
  - Dacă ați selectat **Căi specifice**, introduceți calea completă către obiectul de scanat. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe

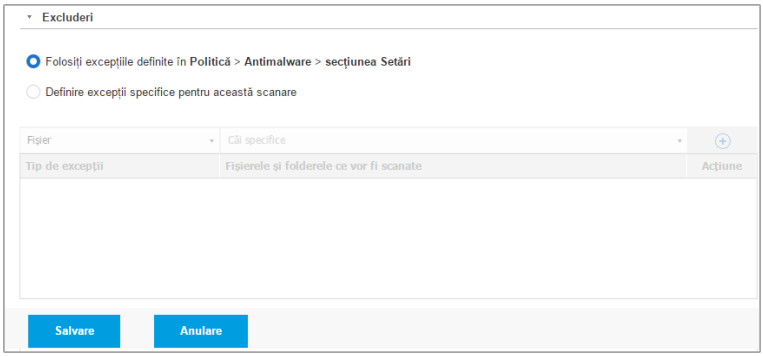
toate mașinile virtuale țintă. Pentru informații suplimentare referitoare la variabilele de sistem, consultați „Variabile de sistem” (p. 569).

c. Faceți clic pe butonul ⊕ **Adăugare** corespunzător.

Pentru a edita o locație existentă, faceți clic pe aceasta. Pentru a elimina o locație din listă, faceți clic pe butonul corespunzător ⊗ **Ștergere**.

Pentru sarcinile de scanare a rețelei, trebuie să introduceți datele de autentificare ale unui cont de utilizator cu permisiuni de citire/editare pe unitățile rețelei țintă, pentru ca agentul de securitate să poată accesa și să inițieze acțiuni în cadrul acestor unități de rețea.

Accesați secțiunea **Excepții** dacă doriți să definiți excepțiile pentru obiectele vizate.



Sarcina de scanare a mașinilor virtuale - Definirea excepțiilor

Puteți utiliza excepții definite de politică sau puteți defini excluderi explicite pentru sarcina de scanare curentă. Pentru detalii referitoare la excepții, consultați „Excluderi” (p. 289).

7. Faceți clic pe **Salvare** pentru a crea sarcina de scanare. Va apărea un mesaj de confirmare.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Notă
Pentru a programa o sarcină de scanare, accesați pagina **Politici**, selectați politica atribuită mașinilor virtuale care vă interesează și adăugați o sarcină de scanare în secțiunea **Antimalware > La cerere**. Pentru mai multe informații, consultați capitolul „Scanare la cerere" (p. 269).

Sarcini de aplicare a patch-urilor

Se recomandă să verificați periodic actualizările de software și să le aplicați cât mai curând posibil. GravityZone automatizează acest proces prin politici de securitate, însă dacă aveți nevoie să actualizați imediat software-ul pe anumite mașini virtuale, executați în ordine următoarele sarcini:

1. Scanare patch-uri
2. Instalarea patch-urilor

Cerințe preliminare

- Agentul de securitate cu modulul Patch Management este instalat pe mașinile vizate.
- Pentru ca sarcinile de scanare și instalare să se finalizeze cu succes, mașinile Windows trebuie să îndeplinească următoarele condiții:
  - **Trusted Root Certification Authorities** stochează certificatul **DigiCert Assured ID Root CA**.
  - **Intermediate Certification Authorities** include **DigiCert SHA2 Assured ID Code Signing CA**.
  - Endpoint-urile au instalat patch-urile pentru Windows 7 și Windows Server 2008 R2 menționate în acest articol Microsoft: Microsoft Security Advisory 3033929

Scanare patch-uri

Mașinile virtuale cu software neactualizat sunt vulnerabile în fața atacurilor. Se recomandă să verificați periodic software-ul instalat pe mașinile dumneavoastră și să efectuați actualizările necesare cât mai curând posibil. Pentru scanarea mașinilor virtuale în vederea identificării patch-urilor care lipsesc:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.

3. Selectați containerul dorit din fereastra din stânga. Toate stațiile de lucru din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați stațiile de lucru vizate.
5. Efectuați clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Scanare patch-uri**. Va apărea o fereastră de configurare.
6. Efectuați clic pe **Da** pentru a confirma sarcina de scanare.

   Atunci când sarcina s-a finalizat, GravityZone adaugă în inventarul de patch-uri toate patch-urile de care au nevoie programele software ale dumneavoastră. Pentru mai multe detalii, vă rugăm consultați „Inventarul de patch-uri" (p. 199).

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor" (p. 207).

Notă
Pentru a programa scanarea patch-urilor, modificați politicile atribuite mașinilor vizate și configurați setările din secțiunea **Patch Management**. Pentru mai multe informații, consultați capitolul „Administrarea patch-urilor" (p. 336).

Instalarea patch-urilor

Pentru a instala unul sau mai multe patch-uri pe mașinile virtuale vizate:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate stațiile de lucru din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Efectuați clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Instalare patch-uri**.

   Va apărea o fereastră de configurare. Aici, puteți vizualiza toate patch-urile care lipsesc de pe mașinile virtuale vizate.
5. Dacă este nevoie, folosiți opțiunile de sortare și filtrare din partea de sus a tabelului pentru a găsi anumite patch-uri.
6. Efectuați clic pe butonul **Coloane** din partea dreaptă-sus a panoului pentru a vizualiza numai informațiile relevante.
7. Selectați patch-urile pe care doriți să le instalați.

Unele patch-uri depind de altele. În astfel de cazuri, acestea sunt selectate automat odată cu patch-ul.

Când efectuați clic pe numerele **CVE-urilor** sau ale **produselor** se va afișa un panou în partea stângă. Panoul conține informații suplimentare, cum ar fi CVE-urile pe care le remediază patch-ul sau produsele pentru care se aplică patch-ul. După ce terminați de citit, efectuați clic pe **Închidere** pentru a ascunde panoul.

8. Selectați **Repornire stații de lucru după instalarea patch-ului, dacă este necesar**, pentru a reporni stațiile de lucru imediat după instalarea patch-ului, dacă sistemul trebuie repornit. Rețineți că această acțiune poate întrerupe activitatea utilizatorului.
9. Faceți clic pe **Instalare**.

   Sarcina de instalare este creată, împreună cu sub-sarcinile pentru fiecare mașină virtuală.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Notă

- Pentru a programa instalarea patch-urilor, modificați politicile atribuite mașinilor vizate și configurați setările din secțiunea **Patch Management**. Pentru mai multe informații, consultați capitolul „Administrarea patch-urilor” (p. 336).
- Puteți instala un patch și de pe pagina **Inventar patch-uri**, pornind de la un anumit patch care vă interesează. În acest caz, selectați patch-ul din listă, faceți clic pe butonul **Instalare** din partea de sus a tabelului și configurați detaliile de instalare a patch-ului. Pentru mai multe detalii, vă rugăm consultați „Instalarea patch-urilor” (p. 203).
- După ce ați instalat un patch, vă recomandăm să transmiteți o sarcină Scanare patch-uri către stațiile de lucru țintă. Această acțiune va actualiza informațiile patch-ului stocate în GravityZone pentru rețelele dvs. administrate.

Puteți dezinstala patch-uri:

- De la distanță, transmițând o sarcină de dezinstalare a patch-urilor din GravityZone.
- Local, pe mașină. În acest caz, va trebui să vă autentificați ca administrator pe stația de lucru și să rulați manual aplicația de dezinstalare.

Scanare Exchange

Puteți scana de la distanță baza de date a unui Server Exchange prin executarea unei sarcini **Scanare Exchange**.

Pentru a putea scana baza de date Exchange, trebuie să activați scanarea la cerere furnizând datele de autentificare ale unui administrator Exchange. Pentru mai multe informații, consultați capitolul „Scanarea bazei de date Exchange" (p. 361).

Pentru a scana baza de date a unui Server Exchange:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Din fereastra din stânga, selectați grupul care conține Serverul Exchange țintă. Serverul este afișat în fereastra din dreapta.

   Notă
   Opțional, puteți aplica filtre pentru a găsi rapid serverul țintă:
   - Faceți clic pe meniul **Filtre** și selectați următoarele opțiuni: **Administrat (Server Exchange)** din secțiunea **Securitate** și **Toate obiectele recursiv** din secțiunea **Adâncime**.
   - Introduceți numele gazedei serverului sau adresa IP în câmpurile antetelor corespunzătoare ale coloanelor.

4. Selectați caseta de bifare a Serverului Exchange a cărei bază de date doriți să o scanați.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Scanare Exchange**. Va apărea o fereastră de configurare.
6. Configurați opțiunile de scanare:
   - **General.** Introduceți o denumire sugestivă pentru sarcină.

     Pentru bazele de date mari, sarcina de scanare poate dura mult și poate afecta performanța serverului. În aceste cazuri, selectați caseta de bifare **Oprește scanarea dacă durează mai mult de** și alegeți un interval de tip convenabil din meniurile corespunzătoare.
   - **Țintă.** Selectați containerele și obiectele pe care doriți să le scanați. Puteți opta pentru scanarea căsuțelor poștale, a folderelor publice sau a ambelor. În afară de e-mail-uri, puteți opta pentru scanarea altor obiecte, cum ar fi **Contacte**, **Sarcini**, **Programări** și **Articole poștale**. De asemenea, puteți seta următoarele limitări pentru conținutul care urmează să fie scanat:
     – Doar mesajele necitite
     – Doar articolele cu atașamente

– Doar articolele noi, primite într-un interval de timp specificat

De exemplu, puteți opta pentru a scana doar e-mail-urile din căsuțele poștale ale utilizatorilor primite în ultimele șapte zile.

Selectați caseta de bifare **Excepții**, dacă doriți să definiți excepții de scanare. Pentru a crea o excepție, folosiți câmpurile din antetul tabelului, după cum urmează:

a. Selectați tipul de director din meniu.
b. În funcție de tipul directorului, specificați obiectele pe care doriți să le excludeți:

Tipul directorului	Formatul obiectului
Mailbox	Adresă e-mail
Folder public	Calea folderului, începând de la rădăcină
Bază de date	Informațiile de identificare ale bazei de date

Notă
Pentru a obține informațiile de identificare ale bazei de date, folosiți comanda shell Exchange:
`Get-MailboxDatabase | fl name,identity`

Nu puteți introduce mai multe articole simultan. Dacă aveți mai multe articole de același tip, trebuie să definiți un număr de reguli egal cu numărul de articole.

c. Faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului pentru a salva excepția și a o include în listă.

Pentru a șterge o regulă referitoare la excepții din listă, faceți clic pe butonul ⊖ **Ștergere** corespunzător.

- **Opțiuni.** Configurați opțiunile de scanare pentru e-mail-urile care corespund regulii:
  – **Tipurile de fișiere scanate.** Folosiți această opțiune pentru a specifica tipurile de fișiere pe care doriți să le scanați. Puteți decide să scanați toate fișierele (indiferent de extensia acestora), exclusiv fișierele de aplicații sau anumite extensii de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor asigură cea mai bună protecție, în timp ce scanarea aplicațiilor este recomandată doar pentru efectuarea unei scanări mai rapide.

Notă
Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Tipuri de fișiere de aplicații” (p. 567).

Dacă doriți să scanați doar fișiere cu anumite extensii, aveți două opțiuni:
- **Extensii definite de utilizator**, unde trebuie să indicați doar extensiile pe care doriți să le scanați.
- **Toate fișierele, cu excepția anumitor extensii**, unde trebuie să introduceți doar extensiile pe care nu doriți să le includeți în scanare.

– **Dimensiunea maximă a atașamentului / cuprinsului e-mail-ului (MB).** Selectați această casetă de bifare pentru a introduce o valoare în câmpul corespunzător, pentru setarea dimensiunii maxime acceptate a fișierului atașat sau a cuprinsului e-mail-ului pe care doriți să îl scanați.
– **Capacitatea maximă a arhivei (niveluri).** Selectați caseta de bufare și alegeți capacitatea maximă a arhivei din câmpul corespunzător. Cu cât capacitatea este mai redusă, cu atât performanțele sunt mai ridicate, iar nivelul de protecție este mai mic.
– **Scanare Posibile aplicații nedorite(PUA).** Selectați această casetă de bifare pentru scanarea posibilelor aplicații periculoase sau nedorite, cum ar fi adware, care se pot instala în sisteme fără consimțământul utilizatorului, pot schimba comportamentul diferitelor produse software și reduce performanțele sistemului.

- **Acțiuni.** Puteți specifica diverse acțiuni pentru agentul de securitate pentru a prelua automat fișiere pe baza tipului de detecție.

Tipul de detecție separă fișierele în trei categorii:
– **Fișiere infectate.** Bitdefender detectează fișierele ca fiind infectate folosind diverse mecanisme avansate, printre care semnăturile malware, învățarea automată și tehnologiile bazate pe inteligență artificială (AI).
– **Fișiere suspecte.** Aceste fișiere sunt detectate ca fiind suspecte de către analiza euristică și alte tehnologii Bitdefender. Acestea asigură o rată mare de detecție, însă utilizatorii trebuie să fie conștienți că există și rezultate fals pozitive (fișiere neinfectate detectate ca fiind suspecte) în unele cazuri.
– **Fișiere care nu pot fi scanate .**Aceste fișiere nu pot fi scanate. Fișierele care nu pot fi scanate includ dar nu se limitează la fișiere protejate cu parolă, criptate sau supra-arhivate.

Pentru fiecare tip de detecție, aveți o acțiune implicită sau principală și o acțiune alternativă, în cazul în care cea principală eșuează. Deși nu se recomandă, puteți modifica aceste acțiuni din meniurile corespunzătoare. Selectați acțiunile care vor fi implementate:

- **Dezinfectare.** Șterge codul malware din fișierele infectate și reconstruiește fișierul original. Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.
- **Respingere / Ștergere e-mail.** Pe serverele cu rol Edge Transport, mesajele e-mail detectate sunt respinse cu un cod de eroare 550 SMTP. În toate celelalte cazuri, mesajul e-mail este șters fără nicio avertizare. Se recomandă să evitați această acțiune.
- **Ștergere fișier.** Șterge atașamentele cu probleme, fără avertizare. Se recomandă să evitați această acțiune.
- **Înlocuire fișier.** Șterge fișierele cu probleme și introduce un fișier text care informează utilizatorul cu privire la măsurile luate.
- **Trecerea fișierelor în carantină.** Mută fișierele detectate în folderul carantină și introduce un fișier text care informează utilizatorul cu privire la măsurile luate. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Puteți administra fișierele în carantină de pe pagina **Carantină**.

  Notă
  Vă rugăm să rețineți că, în cazul Serverelor Exchange, carantina necesită spațiu suplimentar pe hard-disk, pe partiția pe care este instalat agentul de securitate. Dimensiunea carantinei depinde de numărul de articole stocate și de dimensiunea acestora.

- **Nu se vor lua măsuri.** Nu vor fi luate măsuri cu privire la fișierele detectate. Acește fișiere vor fi doar afișate în jurnalul de scanare. Sarcinile de scanare sunt configurate implicit să ignore fișierele suspecte. Ar putea fi util să modificați sarcina implicită, pentru a trece fișierele suspecte sub carantină.
- În mod implicit, dacă un e-mail corespunde domeniului de aplicare al regulii, acesta este procesat exclusiv în conformitate cu regula, fără a fi verificat cu privire la orice alte reguli rămase. Dacă doriți să continuați

să verificați în baza celorlalte reguli, debifați caseta de selectare **Oprire procesare reguli, dacă condițiile regulii sunt îndeplinite**.

7. Faceți clic pe **Salvare** pentru a crea sarcina de scanare. Va apărea un mesaj de confirmare.
8. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Instalare

Pentru a proteja mașinile virtuale cu Security for Virtualized Environments, trebuie să instalați agentul de securitate Bitdefender pe fiecare dintre acestea. Agentul de securitate Bitdefender administrează protecția de pe mașinile virtuale. Comunică de asemenea cu Control Center pentru a primi comenzile administratorului și a expedia rezultatele acțiunilor sale. După ce ați instalat un agent de securitate Bitdefender într-o rețea, aplicația va detecta automat mașinile virtuale neprotejate din rețeaua respectivă. Protecția Security for Virtualized Environments poate fi ulterior instalată de la distanță pe mașinile virtuale respective, de pe Control Center. Instalarea la distanță este efectuată în fundal, fără ca utilizatorul să știe despre acest lucru.

În rețele izolate, care nu au conectivitate directă cu aplicația GravityZone, puteți instala agentul de securitate cu rol de Releu. În acest caz, comunicarea dintre aplicația GravityZone și ceilalți agenți de securitate se va realiza prin agentul Releu, care va acționa și ca și server local de actualizări pentru agenții de securitate, protejând rețeaua izolată.

Notă
Se recomandă ca mașina virtuală pe care instalați agentul Releu să fie întotdeauna pornită.

Avertisment
Înainte de instalare, asigurați-vă că ați dezinstalat aplicația firewall existentă contra malware-ului de pe mașinile virtuale. Instalarea protecției Bitdefender peste aplicațiile de securitate existente le poate afecta funcționarea și poate cauza probleme majore în sistem. Windows Defender și Windows Firewall se dezactivează automat la demararea instalării.

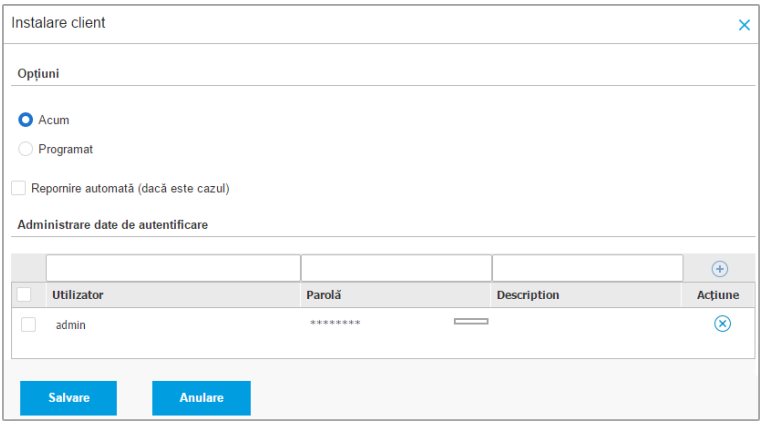
Pentru a instala protecția Security for Virtualized Environments de la distanță, pe una sau mai multe mașini virtuale:

1. Conectați-vă și autentificați-vă la Control Center.
2. Mergeți la pagina **Rețea**.
3. Selectați **Mașini virtuale** din selectorul de vederi.
4. Selectați containerul dorit din fereastra din stânga. Entitățile din grupul selectat sunt afișate în tabelul din fereastra din dreapta.

   Notă
   Opțional, puteți aplica filtre pentru a afișa exclusiv mașinile virtuale neadministrate. Dați clic pe meniul **Filtre** și selectați următoarele opțiuni: **Neadministrat** din fila **Securitate** și **Toate obiectele recursiv** din fila **Adâncime**.

5. Selectați entitățile (mașini virtuale, gazde, clustere sau grupuri) pe care doriți să instalați protecția.
6. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Instalare > BEST**.

   Se afișează asistentul **Instalare client**.



Instalarea Bitdefender Endpoint Security Tools din meniul Sarcini

7. În secțiunea **Opțiuni**, configurați timpul de instalare:
   - **Acum**, pentru a lansa instalarea imediat.

- **Programat**, pentru a configura intervalul de recurență al instalării. În acest caz, selectați intervalul de timp dorit (orar, zilnic sau săptămânal) și configurați-l conform necesităților dvs.

  Notă
  De exemplu, dacă sunt necesare anumite operațiuni pe mașina țintă înainte de a instala clientul (cum ar fi dezinstalarea altor aplicații și repornirea sistemului de operare), puteți programa sarcina de instalare să ruleze la fiecare 2 ore. Sarcina va începe pe fiecare mașină țintă la fiecare 2 ore până la finalizarea cu succes a instalării.

8. Dacă doriți ca stațiile de lucru țintă să fie repornite automat pentru finalizarea instalării, selectați **Repornire automată (dacă este necesar)**.
9. În secțiunea **Administrare date de autentificare**, specificați drepturile de administrare necesare pentru autentificarea de la distanță pe stațiile de lucru țintă. Puteți adăuga datele de autentificare introducând numele de utilizator și parola pentru fiecare sistem de operare țintă.

   Important
   Pentru stații de lucru cu sistem de operare Windows 8.1, este necesar să furnizați datele de autentificare ale contului de administrator încorporat sau ale unui cont de administrator de domeniu. Pentru mai multe informații, consultați acest articol KB.

   Notă
   Dacă nu ați selectat datele de autentificare, se va afișa un mesaj de avertizare. Acest pas este obligatoriu pentru instalarea de la distanță a Bitdefender Endpoint Security Tools pe stațiile de lucru.

   Pentru a adăuga datele SO necesare:

   a. Introduceți numele de utilizator și parola unui cont de administrator pentru fiecare sistem de operare țintă, în câmpurile corespunzătoare din capătul tabelului cu datele de autentificare. Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont.

      Dacă mașinile sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

      Folosiți convențiile Windows la introducerea denumirii contului de utilizator:

- Pentru mașinile Active Directory folosiți următoarele sintaxe: `username@domain.com` și `domain\username`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`user@domain.comusername@domain.com` și `domain\userusername`).
- Pentru mașinile din grupul de lucru, e suficient să introduceți numai numele de utilizator, fără numele grupului de lucru.

b. Faceți clic pe butonul ⊕ **Adăugare**. Contul este adăugat la lista de date de autentificare.

> **Notă**
> Datele specificate sunt salvate automat în secțiunea Administrare date de autentificare, astfel încât nu trebuie să le reintroduceți. Pentru a accesa funcția de Administrare date de autentificare, nu trebuie decât să faceți clic pe numele dvs. de utilizator din colțul din dreapta sus al consolei.

> **Important**
> Dacă datele de autentificare furnizate nu sunt valabile, instalarea aplicației client va eșua pe stațiile de lucru respective. Asigurați-vă că actualizați datele de autentificare pentru sistemul de operare introduse în funcționalitatea de Administrare date de autentificare atunci când acestea se schimbă pe stațiile de lucru țintă.

c. Selectați casetele corespunzătoare conturilor pe care doriți să le folosiți.

10. În secțiunea **Agent de instalare**, alegeți entitatea la care se vor conecta mașinile țintă pentru instalarea și actualizarea clientului:

- **Aplicația GravityZone**, atunci când mașinile se conectează direct la aplicația GravityZone.

  Pentru această situație, puteți defini și un Server de comunicații personalizat introducând adresa IP sau Numele de gazdă al acestuia, dacă este necesar.

- **Endpoint Security Relay**, dacă doriți să conectați stațiile de lucru la un client de tip releu instalat în rețeaua dvs. Toate mașinile cu rolul de releu detectate în rețeaua dvs. vor fi afișate în tabelul afișat mai jos. Selectați mașina de tip releu dorită. Stațiile de lucru conectate vor comunica cu Control Center exclusiv prin releul specificat.

Important

- Portul 7074 trebuie să fie deschis pentru ca instalarea prin agentul releu să funcționeze.
- La instalarea agentului prin intermediul unui Releu Linux, trebuie respectate următoarele condiții:
  - Endpoint-ul cu rol de Releu trebuie să aibă instalat pachetul Samba (`smbclient`) versiunea 4.1.0 sau mai recentă și să suporte comanda `net` binary/command, astfel încât să poată instala de la distanță agenți Windows.

    Notă
    De regulă, funcționalitatea `net` binary/command este livrată împreună cu pachetele samba-client și/sau samba-common. Pe anumite distribuții Linux (precum CentOS 7.4), comanda `net` se instalează numai în cazul instalării versiunii complete a suitei Samba (Common + Client + Server). Asigurați-vă că pe endpoint-ul cu rol de Releu este disponibilă comanda `net`.

  - Stațiile de lucru Windows trebuie să aibă activate funcțiile Partajare administrativă și Partajare rețea.
  - Stațiile de lucru țintă Linux și Mac trebuie să aibă funcția SSH activată și firewall-ul dezactivat.

11. Trebuie să selectați un pachet de instalare pentru instalarea curentă. Dați clic pe lista **Utilizare pachet** și selectați pachetul de instalare dorit. Aici găsiți toate pachetele de instalare create anterior pentru compania dvs.
12. Dacă este necesar, puteți modifica o parte din setările pachetului de instalare făcând clic pe butonul **Personalizare** de lângă câmpul **Utilizare pachet**.

    Setările pachetului de instalare vor apărea mai jos și veți putea efectua modificările de care aveți nevoie. Pentru mai multe informații referitoare la editarea pachetelor de instalare, consultați Ghidul de instalare GravityZone.

    Avertisment
    Vă informăm că modulul Firewall este disponibil numai pentru stațiile de lucru Windows.

Dacă doriți să salvați modificările ca pachet nou, selectați opțiunea **Salvare ca pachete** situată în partea de jos a listei de setări a pachetului și introduceți o denumire pentru noul pachet de instalare.

13. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

Dezinstalare client

Pentru a dezinstala de la distanță protecția Bitdefender:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate entitățile din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare ale mașinilor virtuale de pe care doriți să dezinstalați agentul de securitate Bitdefender.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Dezinstalare client**.
6. Se afișează o fereastră de configurare, care vă permite să efectuați următoarele setări:
   - Puteți opta pentru menținerea articolelor trecute în carantină pe mașina client.
   - Pentru mediile integrate cu vShield, trebuie să selectați datele de autentificare necesare pentru fiecare mașină. Ăn caz contrar, instalarea va eșua. Selectați **Utilizare date de autentificare pentru integrarea cu vShield**, apoi faceți clic pe toate datele de autentificare corespunzătoare din tabelul Administrare date de autentificare afișat mai jos.
7. Faceți clic pe **Salvare** pentru a genera sarcina. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Notă
Dacă doriți să reinstalați protecția, asigurați-vă mai întâi că ați repornit calculatorul.

Actualizare

Verificați periodic starea mașinilor virtuale administrate. Dacă identificați o mașină virtuală cu probleme de securitate, faceți clic pe denumire pentru afișarea paginii **Informații**. Pentru mai multe informații, consultați capitolul „Stare securitate” (p. 111).

Clienții sau conținutul de securitate care nu este la zi reprezintă probleme de securitate. În aceste cazuri, trebuie să executați o actualizare pe mașinile virtuale corespunzătoare. Această sarcină poate fi efectuată local de pe mașina virtuală sau de la distanță din Control Center.

Pentru a actualiza de la distanță clientul și conținutul de securitate pe mașinile virtuale administrate:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate entitățile din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare ale mașinilor virtuale pe care doriți să rulați o actualizare a clientului.
5. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Actualizare**. Va apărea o fereastră de configurare.
6. Puteți alege să actualizați numai produsul, numai conținutul de securitate sau ambele.
7. Pentru SO Linux și mașinile integrate cu vShield, trebuie să selectați și datele de autentificare necesare. Bifați caseta **Utilizare date de autentificare pentru Linux și integrarea cu vShield**, apoi seleczați toate datele de autentificare corespunzătoare din tabelul Administrare date de autentificare afișat mai jos.
8. Faceți clic pe **Actualizare** pentru a executa sarcina. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Reconfigurare client

Modulele de protecție, rolurile și modurile de scanare ale agentului de securitate sunt inițial configurate în pachetul de instalare. După ce ați instalat agentul de securitate în rețea, puteți modifica în orice moment setările inițiale prin transmiterea unei sarcini de **Reconfigurare client** de la distanță către stațiile de lucru care vă interesează.

Avertisment
Vă informăm că sarcina **Reconfigurare Client** suprascrie toat setările de securitate și niciuna dintre setările inițiale nu este menținută. În timp ce utilizați această sarcină, asigurați-vă că reconfigurați toate setările de instalare ale stațiilor de lucru țintă.

Pentru a schimba setările de instalare pentru una sau mai multe mașini virtuale:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate entitățile din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare ale mașinilor virtuale pentru care doriți să modificați setările de instalare.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Reconfigurare client**.
6. În secțiunea **General**, configurați ora de executare a sarcinii:
   - **Acum**, pentru a lansa sarcina imediat.
   - **Programat**, pentru a configura intervalul de recurență al sarcinii. În acest caz, selectați intervalul de timp dorit (orar, zilnic sau săptămânal) și configurați-l conform necesităților dvs.

     Notă
     De exemplu, dacă trebuie să ruleze și alte procese importante pe mașina țintă, puteți programa sarcina să ruleze la fiecare 2 ore. Sarcina va începe pe fiecare mașină țintă la fiecare 2 ore până la finalizarea cu succes.

7. Configurați modulele, rolurile și modurile de scanare pentru stația de lucru țintă, după cum doriți. Pentru informații suplimentare, consultați Ghidul de instalare GravityZone.

Avertisment

- Se vor instala doar modulele suportate pentru fiecare sistem de operare.

  Vă informăm că modulul Firewall este disponibil numai pentru stațiile de lucru Windows.
- Bitdefender Tools (agent vechi) suportă numai Scanarea centralizată.

8. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Descoperire rețea

Funcția de descoperire a rețelelor este executată automat numai de către agenții de securitate cu rol de Releu. Dacă nu aveți un agent Releu instalat în rețea, trebuie să transmiteți manual o sarcină de descoperire rețea de pe o stație de lucru protejată.

Pentru a rula o sarcină de descoperire a rețelei în rețeaua dumneavoastră:

Important

Dacă se utilizează un releu Linux pentru a descoperi alte stații de lucru Linux sau Mac, este necesar fie să instalați Samba pe stațiile de lucru țintă, fie să le uniți în Active Directory și să folosiți DHCP. În acest fel, NetBIOS va fi configurat automat pe acestea.

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate entitățile din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați caseta de bifare a mașini cu care doriți să efectuați sarcina de descoperire a rețelei.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Descoperire rețea**.
6. Va apărea un mesaj de confirmare. Faceti clic pe **Da**.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Descoperire aplicații

Pentru a descoperi aplicațiile din rețeaua dumneavoastră:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate mașinile virtuale din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați mașinile virtuale pe care doriți să executați funcția de descoperire aplicații.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Descoperire aplicații**.

   Notă
   Bitdefender Endpoint Security Tools cu modulul Control aplicații trebuie să fie instalat și activat pe mașinile virtuale selectate. În caz contrar, sarcina va fi inactivă. Atunci când un grup selectat conține ținte valide și nevalide, sarcina va fi trimisă numai către stațiile de lucru valide.

6. Apăsați **Da** în fereastra de confirmare pentru a continua.

Aplicațiile și procesele descoperite sunt afișate în pagina **Rețea > Inventar aplicații**. Pentru mai multe informații, consultați capitolul „Inventar aplicații” (p. 193).

Notă
Executarea sarcinii **Descoperire aplicații** ar putea dura câteva momente, în funcție de numărul de aplicații instalate. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Repornire sistem

Puteți opta pentru repornirea de la distanță a mașinilor virtuale administrate.

Notă
Verificați pagina **Rețea > Sarcini** înainte de a reporni anumite mașini virtuale. Este posibil ca sarcinile create anterior să fie în continuare în curs de procesare pe mașinile țintă.

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate entitățile din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele de bifare ale mașinilor virtuale pe care doriți să le reporniți.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Repornire sistem**.
6. Selectați opțiunea programului de repornire:
   - Selectați **Repornire imediată** pentru a reporni imediat mașinile virtuale.
   - Selectați **Repornire la** și folosiți câmpurile de mai jos, pentru a programa repornirea la data și ora dorită.
7. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru informații suplimentare, consultați Vizualizarea și administrarea sarcinilor.

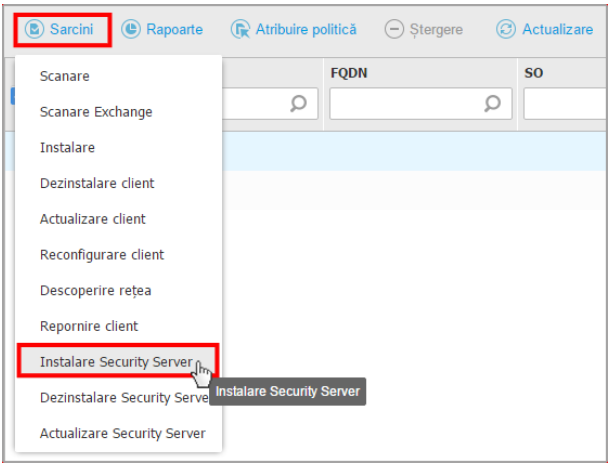
Instalarea Security Server

Pentru instalarea Security Server în mediul virtualizat:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Parcurgeți inventarul Nutanix, VMware sau Citrix și bifați casetele corespunzătoare sistemelor gazdă sau containerelor(Nutanix Prism, vCenter Server, XenServer sau centru de date) dorite. Pentru o selecție rapidă, puteți selecta direct containerul rădăcină (Inventarul Nutanix, VMware sau Citrix). Veți putea selecta gazdele individual din asistentul de instalare.

   Notă
   Nu puteți selecta gazde din diferite foldere.

4. Dați clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Instalare Security Server** din meniu. Se afișează fereastra **Instalare Security Server**.



Instalarea Security Server din meniul Sarcini

5. Toate gazdele detectate în containerul selectat vor fi afișate în listă. Selectați gazdele pe care doriți să instalați instanțele Security Server.
6. Alegeți setările de configurare pe care doriți să le folosiți.

Important
Folosirea unor setări comune la rularea mai multor instanțe Security Server simultan necesită ca gazdele să împărtășească același spațiu de stocare, să aibă adrese IP alocate de un server DHCP și să facă parte din aceeași rețea.

7. Faceți clic pe **Înainte**.
8. Furnizați datele de autentificare VMware vShield corespunzătoare pentru fiecare mașină vCenter.
9. Introduceți o denumire sugestivă pentru Security Server.
10. În cazul mediilor VMware, selectați containerul în care doriți să includeți Security Server din meniul **Configurare container**.
11. Selectați spațiul de stocare destinație.

12. Selectați tipul de administrare. Se recomandă să instalați aplicația folosind o administrare de disc standard.

Important
Dacă folosiți alocarea dinamică de resurse (la cerere) și nu mai există spațiu disponibil de stocare a datelor, Security Server va îngheța și, prin urmare, gazda va rămâne neprotejată.

13. Configurați memoria și alocarea resurselor CPU în funcție de procentul de consolidare MV de pe gazdă. Selectați **Scăzut**, **Mediu** sau **Ridicat** pentru a încărca setările recomandate pentru alocarea resurselor sau **Manual** pentru a configura manual alocarea resurselor.
14. Este necesar să setați o parolă de administrator pentru consola Security Server. Setarea unei parole administrative suprascrie parola principală implicită ("sve").
15. Setați fusul orar al aplicației.
16. Selectați tipul de configurare a rețelei pentru rețeaua Bitdefender. Adresa IP a Security Server nu trebuie să se modifice în timp, deoarece este utilizată de agenți Linux pentru comunicare.

    Dacă alegeți DHCP, asigurați-vă că ați configurat serverul DHCP pentru rezervarea adresei IP pentru aplicație.

    Dacă alegeți opțiunea statică, trebuie să introduceți adresa IP, masca de sub-rețea, portalul și informațiile DNS.
17. Selectați rețeaua vShield și introduceți datele vShield. Eticheta implicită pentru rețeaua vShield este `vmservice-vshield-pg`.
18. Faceți clic pe **Salvare** pentru a genera sarcina. Va apărea un mesaj de confirmare.

Important

- Pachetele Security Server nu sunt incluse implicit în aplicația GravityZone. În funcție de setările efectuate de administratorul principal, pachetul Security Server necesar mediului dumneavoastră va fi descărcat la lansarea sarcinii de instalare Security Server sau administratorul va fi informat cu privire la lipsa imaginii și instalarea nu va continua. Dacă pachetul lipsește, administratorul principal va trebui să îl descarce manual înainte de a putea efectua instalarea.

- Instalarea Security Server pe Nutanix prin intermediul unei sarcini de la distanță poate eșua atunci când clusterul Prism Element este înregistrat în Prism Central sau din alte motive. În astfel de situații, se recomandă să efectuați o configurare manuală a Security Server. Pentru detalii suplimentare, consultați acest articol KB.

19. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Dezinstalarea Security Server

Pentru a dezinstala Security Server:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați centrul de date sau folderul care conține gazda pe care este instalat Security Server.
4. Selectați caseta de bifare corespunzătoare gazdei pe care este instalat Security Server.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Dezinstalare Security Server**.
6. Introduceți datele de autentificare vShield și faceți clic pe **Da** pentru generarea sarcinii.
7. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Actualizarea Security Server

Pentru a actualiza Security Server:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați gazda pe care este instalat Security Server.

   Pentru a localiza cu ușurință Security Server, puteți folosi meniul **Filtre**, după cum urmează:

- Mergeți la secțiunea **Securitate** și selectați exclusiv **Security Servers**.
- Mergeți la secțiunea **Adâncime** și selectați **Toate obiectele recursiv**.

Notă
Dacă utilizați un instrument de management de virtualizare care nu este integrat în prezent cu Control Center, Security Server va fi plasat în **Grupuri personalizate**. Pentru informații suplimentare referitoare la platformele virtuale acceptate, consultați Ghidul de instalare GravityZone.

4. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Actualizare Security Server**.
5. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.
6. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Important
Este recomandat să utilizați această metodă pentru actualizarea Security Server pentru NSX, în caz contrar veți pierde carantina salvată în aplicație.

Instalați pachetul suplimentar HVI

Pentru a proteja mașinile virtuale cu HVI, este necesar să instalați pe gazdă un pachet suplimentar. Rolul acestui pachet este de a asigura comunicarea între hypervisor și Security Server instalat pe gazdă. Odată instalat, HVI va proteja mașinile virtuale care au funcția HVI activată în politică.

Important
- HVI protejează mașinile virtuale numai pe hypervisorii Citrix Xen.
- Nu este necesar să dezinstalați agentul de securitate existent de pe mașinile virtuale.

Pentru a instala pachetul suplimentar pe o gazdă:

1. Mergeți la pagina **Configurare > Actualizare**.
2. Selectați pachetul suplimentar HVI din lista de **Componente** și faceți clic pe butonul **Download** din partea de sus a tabelului.

3. Mergeți la pagina **Rețea** și selectați **Mașini virtuale** din selectorul de vizualizări.
4. Selectați **Server** din meniul **Vizualizări** din secțiunea din stânga.
5. Selectați una sau mai multe gazde Xen din inventarul rețelei. Puteți vizualiza cu ușurință gazdele disponibile selectând opțiunea **Tip > Gazde** din meniul **Filtre**.
6. Faceți clic pe butonul **Sarcini** din secțiunea din dreapta și selectați **Instalare pachet suplimentar HVI**. Se va deschide fereastra de instalare.
7. Programați sarcina de instalare pentru când doriți să fie executată. Puteți opta pentru executarea sarcinii imediat după salvare sau la un anumit moment. În cazul în care instalarea nu poate fi realizată la momentul specificat, sarcina se repetă automat conform setărilor de recurență. De exemplu, dacă selectați mai multe gazde și una dintre acestea nu este disponibilă atunci când pachetul este programat pentru instalare, sarcina se va executa din nou la momentul specificat.
8. Gazda trebuie să fie repornită pentru aplicarea modificărilor și finalizarea instalării. Dacă doriți să reporniți gazda fără supraveghere, selectați **Repornire automată gazdă (dacă este necesar)**.
9. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

Dezinstalare pachet suplimentar HVI

Notă
Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Pentru a dezinstala Pachetul suplimentar de pe gazde:

1. Mergeți la pagina **Rețea** și selectați **Mașini virtuale** din selectorul de vizualizări.
2. Selectați **Server** din meniul **Vizualizări** din secțiunea din stânga.
3. Selectați una sau mai multe gazde Xen din inventarul rețelei. Puteți vizualiza cu ușurință gazdele disponibile selectând opțiunea **Tip > Gazde** din meniul **Filtre**.
4. Faceți clic pe butonul **Sarcini** din secțiunea din dreapta și selectați **Dezinstalare pachet suplimentar HVI**. Se deschide fereastra de configurare.
5. Programați momentul eliminării pachetului. Puteți opta pentru executarea sarcinii imediat după salvare sau la un anumit moment. În cazul în care

dezinstalarea nu poate fi realizată la momentul specificat, sarcina se repetă automat conform setărilor de recurență. De exemplu, dacă selectați mai multe gazde și una dintre acestea nu este disponibilă atunci când pachetul este programat pentru dezinstalare, sarcina se va executa din nou la momentul specificat.

6. Gazda trebuie să fie repornită pentru finalizarea dezinstalării. Dacă doriți să reporniți gazda fără supraveghere, selectați **Repornire automată gazdă (dacă este necesar)**.
7. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

Actualizare Pachet suplimentar HVI

Pentru a actualiza Pachetul suplimentar de pe gazde:

1. Instalați cel mai recent pachet suplimentar HVI disponibil.

   Pentru mai multe informații, consultați capitolul „Instalați pachetul suplimentar HVI” (p. 159).
2. Mergeți la pagina **Rețea**.
3. Selectați **Mașini virtuale** din selectorul modului de vizualizare.
4. Selectați **Server** din meniul **Vizualizări** din secțiunea din stânga.
5. Selectați una sau mai multe gazde Xen din inventarul rețelei.

   Puteți vizualiza cu ușurință gazdele disponibile selectând opțiunea **Tip > Gazde** din meniul **Filtre**.
6. Efectuați clic pe butonul **Sarcini** din secțiunea din dreapta și selectați **Actualizare Pachet suplimentar HVI**. Se deschide fereastra de configurare.
7. Programați momentul actualizării pachetului. Puteți opta pentru executarea sarcinii imediat după salvare sau la un anumit moment.

   În cazul în care actualizarea nu poate fi realizată la momentul specificat, sarcina se repetă automat conform setărilor de recurență. De exemplu, dacă selectați mai multe gazde și una dintre acestea nu este disponibilă atunci când pachetul este programat pentru actualizare, sarcina se va executa din nou la momentul specificat.

8. Selectați **Repornire automată (dacă este cazul)** dacă doriți să reporniți gazda fără supraveghere. În caz contrar, trebuie să reporniți gazda manual pentru aplicarea actualizării.
9. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

Puteți verifica starea sarcinilor pe pagina **Rețea > Sarcini**.

Injectați instrument personalizat

Notă
Această sarcină este legată de modulul HVI care poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Pentru injectarea instrumentelor în sistemele de operare ale gazdei vizate:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga. Toate stațiile de lucru din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați casetele stațiilor de lucru vizate.
5. Efectuați clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Injectare instrument personalizat**. Este afișată o fereastră de configurare.
6. Din meniul derulant, selectați toate instrumentele pe care doriți să le injectați. Pentru fiecare instrument selectat va fi afișată o secțiune pliantă cu setările acestuia.

   Aceste instrumente au fost încărcate anterior în GravityZone. Dacă nu găsiți instrumentul potrivit pe listă, accesați **Centru administrare instrumente** și adăugați-l de acolo. Pentru mai multe informații, consultați capitolul „Injectare instrumente personalizate cu HVI” (p. 533).
7. Pentru fiecare instrument afișat în fereastră:
   a. Efectuați clic pe numele instrumentului pentru a vizualiza sau ascunde secțiunea acestuia.
   b. Introduceți linia de comandă a instrumentului împreună cu toți parametrii de intrare necesari, exact la fel cum procedați pentru Command Prompt sau Terminal. De exemplu:

```
bash script.sh <param1> <param2>
```

Pentru Instrumentele BD de remediere, puteți selecta doar acțiunea de remediere și acțiunea de remediere de backup din cele două meniuri derulante.

c. Indicați locația de unde Security Server trebuie să culeagă jurnalele:

- **stdout**. Selectați această căsuță pentru a prelua jurnalele din canalul standard de comunicare de ieșire.
- **Fișier ieșire**. Selectați această căsuță pentru a prelua fișierul jurnal salvat pe stația de lucru. În acest caz, trebuie să introduceți calea unde poate Security Server să găsească fișierul. Puteți folosi căi absolute sau variabile de sistem.

  Aici aveți o opțiune suplimentară: **Ștergere fișiere jurnal de la sistemul găzduit după ce au fost transferate**. Selectați-o dacă nu mai aveți nevoie de fișiere la stația de lucru.

8. Dacă doriți să transferați fișierul jurnal din Security Server într-o altă locație trebuie să furnizați calea către locația de destinație și datele de autentificare.
9. Câteodată instrumentul poate necesita un timp mai îndelungat decât cel preconizat pentru finalizarea acțiunii sau poate să nu mai răspundă la comenzi. Pentru a evita căderile de sistem în astfel de situații, selectați din secțiunea **Configurare siguranță** după câte ore trebuie ca Security Server să oprească automat acțiunea instrumentului.
10. Faceți clic pe **Save**.

    Veți putea vizualiza starea sarcinii pe pagina **Sarcini**. Pentru mai multe detalii, puteți să consultați și raportul **HVI Stare injectare de la terți**.

6.3.6. Crearea de rapoarte rapide

Puteți opta pentru crearea de rapoarte rapide cu privire la mașinile virtuale, de pe pagina **Rețea**:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate mașinile virtuale din containerul selectat sunt afișate în tabelul din fereastra din dreapta.

4. Filtrați conținutul grupului selectat exclusiv după mașinile virtuale administrate.
5. Selectați casetele de bifare corespunzătoare mașinilor virtuale pe care doriți să le includeți în raport.
6. Faceți clic pe butonul **Rapoarte** din partea de sus a tabelului și selectați tipul de raport din meniu. Pentru mai multe informații, consultați capitolul „Rapoarte referitoare la calculatoare și mașini virtuale" (p. 476).
7. Configurați opțiunile pentru raport. Pentru mai multe informații, consultați capitolul „Crearea rapoartelor" (p. 495)
8. Faceți clic pe **Generare**. Raportul este afișat imediat. Intervalul necesar pentru generarea rapoartelor diferă în funcție de numărul de mașini virtuale selectate.

6.3.7. Atribuirea unei politici

Puteți administra setările de securitate pe mașinile virtuale folosind politicile.

Din pagina **Rețea** puteți vizualiza, modifica și aloca politici pentru fiecare mașină virtuală sau grup de mașini virtuale.

Notă
Setările de securitate sunt disponibile exclusiv pentru mașinile virtuale administrate. Pentru a vizualiza și administra mai ușor setările de securitate, puteți filtra inventarul de rețea numai după mașinile virtuale administrate.

Pentru a vizualiza setările de securitate atribuite unei anumite mașini virtuale:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate mașinile virtuale din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Faceți clic pe denumirea mașinii virtuale administrate dorite. O fereastră conținând diverse informații va apare.
5. În secțiunea **General**, în **Politică**, faceți clic pe denumirea politicii curente pentru a-i vizualiza setările.
6. Puteți modifica setările de securitate în funcție de necesități, cu condiția ca deținătorul politicii să fi permis celorlalți utilizatori să modifice politica respectivă. Vă rugăm să rețineți că orice modificare va afecta toate mașinile virtuale cărora le este atribuită aceeași politică.

Pentru mai multe informații despre setările politicii mașinii virtuale, vă rugăm să consultați„Politici de securitate” (p. 220)

Pentru a atribui o politică unei mașini virtuale sau unui grup de mașini virtuale:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate mașinile virtuale din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați caseta de bifare a entității care vă interesează. Puteți selecta unul sau mai multe obiecte de același timp, numai dacă aparțin aceluiași nivel.
5. Faceți clic pe butonul **Alocare politică** din partea de sus a tabelului.
6. Efectuați setările necesare în fereastra **Atribuire politică**.

   Pentru mai multe informații, consultați capitolul „Atribuirea unei politici” (p. 223).

Avertisment
În cazul politicilor cu Hypervisor Memory Introspection activat, este posibil ca sistemele țintă să necesite o repornire imediat după atribuirea politicilor. Mașinile cu această stare sunt marcate în pagina **Rețea** cu pictograma **Se așteaptă repornirea**.

6.3.8. Utilizarea Managerului de recuperare pentru volumele criptate

Atunci când utilizatorii endpoint-urilor își uită parolele de criptare și nu mai pot accesa volumele criptate pe mașinile lor, îi puteți ajuta extrăgând cheile de recuperare din pagina **Rețea**.

Pentru a extrage o cheie de recuperare:

1. Mergeți la pagina **Rețea**.
2. Selectați butonul **Manager de recuperare** din bara de acțiuni din partea stângă. Se afișează o nouă fereastră.
3. În secțiunea **Identificator** a ferestrei, introduceți datele următoare:
   a. ID-ul cheii de recuperare pentru volumul criptat. ID-ul cheii de recuperare este un șir de numere și litere disponibile pe endpoint, în ecranul de recuperare BitLocker.

Pe Windows, ID-ul cheii de recuperare este un șir de numere și litere disponibile pe endpoint, în ecranul de recuperare BitLocker.

Alternativ, puteți utiliza opțiunea **Recuperare** din fila **Protecție** din detalii mașină virtuală pentru introducerea automată a ID-ului cheii de recuperare, atât pentru endpoint-urile Windows, cât și pentru endpoint-urile macOS.

b. Parola contului dumneavoastră GravityZone.

4. Efectuați clic pe **Arată**. Fereastra se extinde.

   În secțiunea **Informații volume** sunt prezentate următoarele date:

   a. Nume volum

   b. Tipul volumului (boot sau non-boot).

   c. Numele endpoint-ului (așa cum este menționat în Inventarul de rețea)

   d. Cheie de recuperare. Pe Windows, cheia de recuperare este o parolă generată automat la criptarea volumului. Pe Mac, cheia de recuperare este, de fapt, parola contului utilizatorului.

5. Trimiteți cheia de recuperare utilizatorului endpoint-ului.

Pentru detalii despre criptarea și decriptarea volumelor din GravityZone, consultați „Criptare” (p. 383).

6.3.9. Ștergere licențe de utilizator

În inventarele Active Directory, vCenter Server (fără vShield, NSX sau HVI) și Xen Server, puteți elibera cu ușurință licențele de utilizator utilizate de mașinile virtuale de pe care agentul de securitate a fost îndepărtat fără rularea operațiunii de dezinstalare.

După această operațiune, mașinile vizate devin neadministrate în inventarul rețelei.

Pentru a șterge o licență de utilizator:

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și mașini virtuale** sau **Mașini virtuale** din selectorul de vizualizări.
3. Selectați grupul dorit din fereastra din stânga. Toate mașinile virtuale se vor afișa în tabelul din partea dreaptă.
4. Selectați mașina virtuală de pe care doriți să ștergeți licența.

5. Faceți clic pe butonul ⊖ **Ștergere licență** din partea superioară a tabelului.
6. Apăsați **Da** în fereastra de confirmare pentru a continua.

6.4. Dispozitive mobile

Pentru administrarea securității dispozitivelor mobile utilizate în companie, trebuie să le asociați mai întâi unor anumiți utilizatori din Control Center și apoi să instalați și să activați aplicația GravityZone Mobile Client pe fiecare dintre acestea.

Dispozitivele mobile pot fi deținute de companie sau personale. Puteți instala și activa GravityZone Mobile Client pe fiecare dispozitiv mobil; apoi îl puteți înmâna utilizatorului corespunzător. Utilizatorii pot, de asemenea, să instaleze și să activeze GravityZone Mobile Client individual, conform instrucțiunilor primite prin e-mail. Pentru informații suplimentare, consultați Ghidul de instalare GravityZone.

Pentru a vizualiza dispozitivele mobile ale utilizatorilor din contul dumneavoastră, mergeți la secțiunea **Rețea** și selectați **Dispozitive mobile** din selectorul de servicii. Pagina **Rețea** afișează grupurile de utilizatori disponbile în fereastra din stânga și utilizatorii și dispozitivele corespunzătoare în fereastra din dreapta.

Dacă integrarea cu Active Directory a fost configurată, puteți adăuga dispozitive mobile la utilizatorii Active Directory existenți. De asemenea, puteți crea utilizatori în **Grupuri personalizate** și le puteți adăuga dispozitive mobile.

Puteți comuta fereastra din dreapta pe **Utilizatori** sau **Dispozitive** folosind secțiunea **Vizualizări** din meniul **Filtre** din partea de sus a tabelului. Fereastra **Utilizatori** vă permite să administrați utilizatorii din Control Center, cum ar fi adăugarea de utilizatori și dispozitive mobile, să verificați numărul de dispozitive pentru fiecare utilizator Folosiți ecranul **Dispozitive** pentru a administra cu ușurință și a verifica detaliile fiecărui dispozitiv mobil din Control Center.

Puteți administra utilizatorii și dispozitivele mobile din Control Center după cum urmează:

- Adăugați utilizatori personalizați
- Adăugați dispozitive mobile utilizatorilor
- Organizați utilizatorii personalizați în grupuri
- Filtrați și căutați utilizatori și dispozitive
- Verificați starea utilizatorului sau dispozitivelor și detaliile
- Executați sarcini pe dispozitive mobile
- Generați rapoarte rapide referitoare la dispozitivele mobile
- Verificați și modificați setările de securitate ale dispozitivului

- Sincronizați inventarul Control Center cu Active Directory
- Ștergeți utilizatori și dispozitive mobile

6.4.1. Adăugarea utilizatorilor personalizați

Dacă integrarea cu Active Directory a fost configurată, puteți adăuga dispozitive mobile la utilizatorii Active Directory existenți.

În situații care nu includ Active Directory, trebuie să creați mai întâi utilizatori personalizați, pentru a avea o modalitate de identificare a deținătorilor de dispozitive mobile.

Există două modalități prin care puteți crea utilizatori personalizați. Puteți fie să îi adăugați pe rând, fie să importați un fișier CSV.

Pentru a adăuga un utilizator personalizat:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de servicii.
3. Faceți clic pe meniul **Filtre** din partea de sus a tabelului și mergeți la secțiunea **Vizualizare**. Asigurați-vă că opțiunea **Utilizatori** este selectată.
4. În fereastra din stânga, selectați **Grupuri personalizate**.
5. Faceți clic pe butonul **Adăugare Utilizator** din partea de sus a tabelului. Va apărea o fereastră de configurare.
6. Specificați detaliile de utilizator necesare:
   - Un nume de utilizator sugestiv (de exemplu, numele complet al utilizatorului)
   - Adresa e-mail a utilizatorului

   Important
   - Asigurați-vă că introduceți o adresa e-mail valabilă. Utilizatorul va primi instrucțiuni de instalare prin e-mail, în momentul în care adăugați un dispozitiv.
   - Fiecare adresă e-mail poate fi asociată exclusiv unui utilizator.

7. Faceți clic pe **OK**.

Pentru a importa utilizatori de dispozitive mobile:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de servicii.

3. Faceți clic pe meniul **Filtre** din partea de sus a tabelului și mergeți la secțiunea **Vizualizare**. Asigurați-vă că opțiunea **Utilizatori** este selectată.
4. În fereastra din stânga, selectați **Grupuri personalizate**.
5. Dați clic pe **Import utilizatori**. Se afișează o nouă fereastră.
6. Selectați fișierul CSV și faceți clic pe **Importă** Fereastra se închide și tabelul este populat cu utilizatorii importați.

Notă
Dacă apar erori, se afișează un mesaj și tabelul este populat numai cu utilizatorii valizi. Utilizatorii existenți sunt omiși.

Ulterior, puteți crea grupuri de utilizatori în **Grupuri personalizate**.

Politica și sarcinile alocate unui utilizator se aplică tuturor dispozitivelor deținute de utilizatorul corespunzător.

6.4.2. Adăugarea dispozitivelor mobile utilizatorilor

Un utilizator poate avea un număr nelimitat de dispozitive mobile. Puteți adăuga dispozitive pentru unul sau mai mulți utilizatori, însă pe rând, câte un dispozitiv pe utilizator.

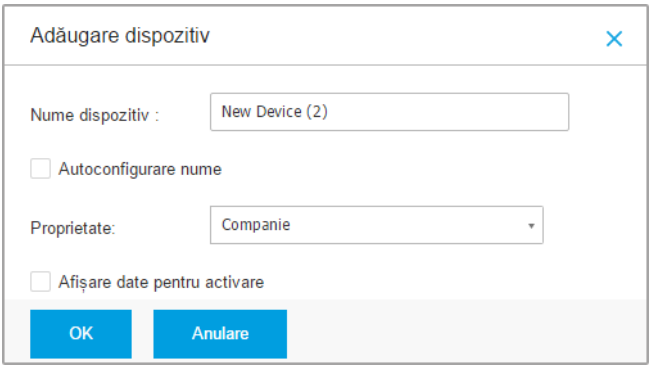
Adăugarea unui dispozitiv la un singur utilizator

Pentru a adăuga un dispozitiv mobil unui utilizator:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Localizați utilizatorul în grupul **Active Directory** sau în **Grupuri personalizate** și bifați caseta corespunzătoare din panoul din dreapta.

Notă
Opțiunea **Filtre** trebuie să fie setată pe **Utilizatori** în secțiunea **Vizualizare**.

4. Faceți clic pe butonul **Adăugare dispozitiv** din partea de sus a tabelului. Va apărea o fereastră de configurare.



Adăugarea unui dispozitiv mobil la un utilizator

5. Configurați detaliile dispozitivului mobil:
   a. Introduceți o denumire sugestivă pentru dispozitiv.
   b. Utilizați opțiunea **Configurare automată nume** dacă doriți ca numele dispozitivului să fie generat automat. Atunci când este adăugat, acest dispozitiv are o denumire generică. După ce dispozitivul a fost activat, acesta este redenumit automat cu informațiile corespunzătoare referitoare la producător și model.
   c. Selectați tipul de proprietate al dispozitivului (de serviciu sau personal). Puteți filtra în orice moment dispozitivele mobile în funcție de tipul de proprietate și le puteți administra după necesități.
   d. Selectați opțiunea **Afișare date de activare** dacă urmează să instalați GravityZone Mobile Client pe dispozitivul utilizatorului.
6. Faceți clic pe **OK** pentru a adăuga dispozitivul. Utilizatorului i se transmite imediat un e-mail cu instrucțiunile de instalare și detaliile de activare care trebuie configurate pe dispozitiv. Detaliile de activare includ token-ul de activare și adresa serverului de comunicații (și codul QR corespunzător).
7. Dacă ați selectat opțiunea **Afișare date de activare**, va apărea fereastra **Detalii de activare**, afișând token-ul unic de activare, adresa serverului de comunicare și codul QR corespunzător noului dispozitiv.

Detalii de activare pentru dispozitive mobile

După instalarea GravityZone Mobile Client, când vi se solicită să activați dispozitivul, introduceți token-ul de activare și adresa serverului de comunicații sau scanați codul QR furnizat.

Adăugarea dispozitivelor la mai mulți utilizatori

Pentru a adăuga mai multe dispozitive mobile la anumiți utilizatori și anumite grupuri:

1. Mergeți la pagina **Rețea**.
2. Localizați utilizatorii sau grupurile în folderele **Active Directory** sau în **Grupurile personalizate** și bifați casetele corespunzătoare din panoul din dreapta.

   Notă
   Opțiunea **Filtre** trebuie să fie setată pe **Utilizatori** în secțiunea **Vizualizare**.

3. Faceți clic pe butonul **Adăugare dispozitiv** din dreapta tabelului. În acest caz, trebuie să definiți în fereastra de configurare doar proprietarul dispozitivului.

Dacă există utilizatori cu adresă e-mail nespecificată, veți fi informat imediat printr-un mesaj. Lista utilizatorilor corespunzători va fi disponibilă în zona de **Notificare** din Control Center.

Dispozitivele mobile create prin selecție multiplă au implicit o denumire generică în Control Center. După ce un dispozitiv a fost activat, acesta este redenumit automat cu informațiile corespunzătoare referitoare la producător și model.

4. Faceți clic pe **OK** pentru a adăuga dispozitivele. Se transmite imediat un e-mail către utilizatori conținând instrucțiunile de instalare și detaliile de activare care trebuie configurate pe dispozitivele acestora. Detaliile de activare includ token-ul de activare și adresa serverului de comunicații (și codul QR corespunzător).

Puteți verifica numărul de dispozitive alocate fiecărui utilizator în fereastra din dreapta, în coloana **Dispozitive**.

6.4.3. Organizarea utilizatorilor personalizați în grupuri

Puteți vizualiza grupurile de utilizatori disponibile în fereastra din stânga a paginii **Rețea**.

Utilizatorii Active Directory sunt grupați în **Active Directory**. Grupurile Active Directory nu pot fi editate. Nu puteți decât să vizualizați și să adăugați dispozitive utilizatorilor corespunzători.

Puteți include toți utilizatorii care nu fac parte din Active Directory în **Grupuri personalizate**, unde puteți crea și organiza grupurile după cum doriți. Beneficiul major este acela că puteți utiliza politicile de grup pentru a începlini diferite cerințe de securitate.

În **Grupuri personalizate**, puteți crea, șterge, redenumi și muta grupurile de utilizatori într-o structură de tip arbore adaptată.

Important
Vă rugăm să rețineți următoarele:

- Un grup poate include atât utilizatori, cât și alte grupuri.
- La selectarea ferestrei din stânga, puteți vizualiza toți utilizatorii, cu excepția celor din sub-grupuri. Pentru a vizualiza toți utilizatorii din grup și din sub-grupurile acestuia, faceți clic pe meniul **Filtre** din partea de sus a tabelului și selectați **Toate obiectele recursiv** din secțiunea **Adâncime**.

Crearea unui nou grup

Pentru a crea un grup personalizat:

1. Selectați **Grupuri personalizate** din fereastra din stânga.
2. Faceți clic pe butonul **Adăugare grup** din partea de sus a ferestrei din stânga.
3. Introduceți o denumire sugestivă pentru grup și faceți clic pe **OK**. Noul grup este afișat în **Grupuri personalizate**.

Redenumirea unui grup

Pentru a redenumi un grup personalizat:

1. Selectați grupul din fereastra din stânga.
2. Faceți clic pe butonul **Editare grup** din partea de sus a ferestrei din stânga.
3. Introduceți noua denumire în câmpul corespunzător.
4. Faceți clic pe **OK** pentru confirmare.

Mutarea grupurilor și utilizatorilor

Puteți muta grupurile și utilizatorii oriunde în ierarhia **Grupuri personalizate**. Pentru a muta un grup sau un utilizator, trageți-l și inserați-l din locația curentă în cea nouă.

Notă

Entitatea mutată va prelua politicile de politică ale noului grup mamă, cu excepția cazului în care funcția de preluare a politicii a fost dezactivată și i s-a alocat o nouă politică.

Ștergerea unui grup

Un grup nu poate fi șters dacă include cel puțin un utilizator. Mutați toți utilizatorii pe care doriți să îi ștergeți din grupul curent, într-un grup nou. Dacă grupul include sub-grupuri, puteți opta pentru mutarea tuturor sub-grupurilor mai degrabă decât a utilizatorilor individuali.

Pentru a șterge un grup:

1. Selectați grupul gol.
2. Faceți clic pe butonul **Șetergere grup** din partea de sus a ferestrei stânga. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

6.4.4. Verificarea Stării Dispozitivelor Mobile

Fiecare dispozitiv mobil este reprezentat în pagina de rețea prin intermediul unei pictograme specifice tipului și stării acestuia.

Consultați „Tipurile și stările obiectelor de rețea” (p. 565) pentru o listă a tuturor tipurilor de pictograme și stărilor disponibile.

Dispozitivele mobile pot avea următoarele stări de administrare:

- **Administrat (Activ)**, dacă sunt îndeplinite cumulativ condițiile următoare:
  - GravityZone Mobile Client este activat pe dispozitiv.
  - GravityZone Mobile Client s-a sincronizat cu Control Center în ultimele 48 de ore.
- **Administrat (Inactiv)**, dacă sunt îndeplinite cumulativ toate condițiile următoare:
  - GravityZone Mobile Client este activat pe dispozitiv.
  - GravityZone Mobile Client nu s-a sincronizat cu Control Center mai mult de 48 de ore.
- **Neadministrat**, în următoarele situații:
  - GravityZone Mobile Client nu a fost încă instalat și activat pe dispozitivul mobil.
  - GravityZone Mobile Client a fost dezinstalat de pe dispozitivul mobil (exclusiv pentru dispozitivele Android).
  - Profilul MDM al Bitdefender a fost șters de pe dispozitiv (exclusiv pentru dispozitivele iOS).

Pentru a verifica starea de administrare a dispozitivelor:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. În fereastra din stânga, selectați grupul care vă interesează.
4. Faceți clic pe meniul **Filtre** de partea de sus a tabelului și efectuați setările următoare:
   a. Mergeți la secțiunea **Vizualizare** și selectați **Dispozitive**.

b. Megeți la secțiunea **Securitate** și selectați starea care vă interesează, în secțiunea **Administrare**. Puteți selecta unul sau mai multe criterii de filtrare simultan.

c. De asemenea, puteți selecta vizualizarea recursivă a tuturor dispozitivelor, selectând opțiunea corespunzătoare în secțiunea **Adâncime**.

d. Faceți clic pe **Save**.

Toate dispozitivele mobile care corespund criteriilor selectate sunt afișate în tabel.

De asemenea, puteți genera raportul de stare pentru Sincronizare dispozitiv pe unul sau mai multe dispozitive mobile. Acest raport oferă informații detaliate referitoare la starea de sincronizare a fiecărui dispozitiv selectat, inclusiv data și ora ultimei sincronizări. Pentru mai multe informații, consultați capitolul „Crearea de rapoarte rapide” (p. 189)

6.4.5. Dispozitive mobile conforme și neconforme

După ce aplicația GravityZone Mobile Client a fost activată pe un dispozitiv mobil, Control Center verifică dacă dispozitivul corespunzător îndeplinește toate cerințele de conformitate. Dispozitivele mobile pot avea următoarele stări de securitate:

- **Fără probleme de securitate**, dacă toate cerințele de conformitate sunt îndeplinite.
- **Cu probleme de securitate**, dacă există cel puțin o condiție de securitate neîndeplinită. Dacă un dispozitiv este declarat neconform, utilizatorului i se cere să remedieze neconformitatea. Utilizatorul trebuie să efectueze modificările necesare într-un anumit interval. În caz contrar, se va aplica acțiunea pentru dispozitivele neconforme definită în politică.

  Pentru informații suplimentare referitoare la măsurile și criteriile pentru neconformități, consultați „Conformitate” (p. 399).

Pentru a verifica starea de conformitate a dispozitivelor:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. În fereastra din stânga, selectați grupul care vă interesează.
4. Faceți clic pe meniul **Filtre** de partea de sus a tabelului și efectuați setările următoare:

a. Mergeți la secțiunea **Vizualizare** și selectați **Dispozitive**.

b. Mergeți la secțiunea **Securitate** și selectați starea dorită, din secțiunea **Probleme de securitate**. Puteți selecta unul sau mai multe criterii de filtrare simultan.

c. De asemenea, puteți selecta vizualizarea recursivă a tuturor dispozitivelor, selectând opțiunea corespunzătoare în secțiunea **Adâncime**.

d. Faceți clic pe **Save**.

Toate dispozitivele mobile care corespund criteriilor selectate sunt afișate în tabel.

5. Puteți vizualiza procentul de conformitate al dispozitivelor, pentru fiecare utilizator:

a. Faceți clic pe meniul **Filtre** din partea de sus a tabelului și selectați **Utilizatori** din categoria **Vizualizare**. Toți utilizatorii din grupul selectat sunt afișați în tabel.

b. Verificați coloana **Conformitate** pentru a vedea numărul de dispozitive conforme din totalul dispozitivelor deținute de utilizator.

De asemenea, puteți genera un raport de Conformitate dispozitiv pentru unul sau mai multe dispozitive mobile. Acest raport oferă informații detaliate referitoare la starea de conformitate a fiecărui dispozitiv seelctat, inclusiv motivul neconformității. Pentru mai multe informații, consultați capitolul „Crearea de rapoarte rapide” (p. 189)

6.4.6. Verificarea detaliilor utilizatorului și dispozitivelor mobile

Puteți obține informații detaliate referitoare la fiecare utilizator și dispozitiv mobil din pagina **Rețea**.

Verificarea detaliilor utilizatorului

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga.
4. Faceți clic pe meniul **Filtre** din partea de sus a tabelului, mergeți în fereastra **Vizualizare** din dreapta și selectați **Utilizatori**. Pentru afișarea recursivă a

utilizatorilor, mergeți la secțiunea **Adâncime** și selectați **Toate articolele recursiv**. Faceți clic pe **Save**. Toți utilizatorii din grupul selectat sunt afișați în tabel.

5. Verificați informațiile afișate în coloanele tabelului pentru fiecare utilizator:
   - **Nume**. Numele de utilizator.
   - **Dispozitive**. Numărul de dispozitive aferente utilizatorului. Faceți clic pe număr pentru a trece la ecranul **Dispozitive** și pentru a afișa exclusiv dispozitivele conforme.
   - **Conformitate**. Procentul de dispozitive conforme din numărul total de dispozitive aferente utilizatorului. Faceți clic pe prima valoare pentru a trece la ecranul **Dispozitive** și a afișa exclusiv dispozitivele conforme.
6. Faceți clic pe numele utilizatorului dorit. Se afișează o fereastră de configurare, în care puteți vizualiza și edita numele utilizatorului și adresa e-mail.

Verificarea detaliilor dispozitivului

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga.
4. Faceți clic pe meniul **Filtre** din partea de sus a tabelului, mergeți în fereastra **Vizualizare** din dreapta și selectați **Dispozitive**. Faceți clic pe **Save**. Toate dispozitivele care aparțin utilizatorilor din grupul selectat sunt afișate în tabel.
5. Verificați informațiile afișate în coloanele tabelului pentru fiecare dispozitiv:
   - **Nume**. Numele dispozitivului.
   - **Utilizator**. Numele utilizatorului care este prorpietarul dispozitivului respectiv.
   - **SO**. Sitemul de operare al dispozitivului corespunzător.
6. Faceți clic pe denumirea dispozitivului pentru detalii suplimentare. Se afișează fereastra **Detalii dispozitiv mobil**, în care puteți verifica următoarele informații grupate în secțiunile **Descriere generală** și **Detalii**:
   - **General**.
     - **Nume**. Numele specificat la adăugarea dispozitivului pe Control Center.
     - **Utilizator**. Numele proprietarului dispozitivului.
     - **Grup**. Grupul mamă al dispozitivului mobil din inventarul rețelei.

- **SO**. Sistemul de operare al dispozitivului mobil.
- **Proprietate**. Tipul de proprietate al dispozitivului mobil (de serviciu sau personal).

- **Securitate**.
  - **Versiune client**. Versiunea aplicației GravityZone Mobile Client instalată pe dispozitiv, detectată numai după înregistrare.
  - **Politică**. Politica atribuită în prezent dispozitivului mobil. Faceți clic pe denumirea dispozitivului mobil pentru a merge la pagina **Politică** corespunzătoare și a verifica setările de securitate.

    Important
    În mod implicit, numai utilizatorul care a creat politica o poate modifica. Pentru a schimba această setare, deținătorul politicii trebuie să bifeze opțiunea **Permite altor utilizatori să modifice această politică** din pagina **Detalii** a politicii. Modificările aduse unei politici vor afecta toate dispozitivele alocate politicii respective. Pentru mai multe informații, consultați capitolul „Atribuirea unei politici" (p. 190).

  - **Stare licență**. Vizualizați informațiile referitoare la licență pentru dispozitivele corespunzătoare.
  - **Stare conformitate**. Starea de conformitate este disponibilă pentru dispozitivele mobile administrate. Un dispozitiv mobil poate fi Conform sau Neconform.

    Notă
    Pentru dispozitivele mobile neconforme, se afișează pictograma de notificare ! . Verificați informațiile oferite de pictogramă pentru a identifica motivul neconformității.
    Pentru detalii suplimentare referitoare la conformitatea dispozitivului mobil, consultați „Conformitate" (p. 399).

  - **Activitate malware (ultimele 24h)**. O prezentare rapidă a numărului de programe malware detectate pentru dispozitivul corespunzător, în ziua curentă.

- **Parolă blocare**. O parolă unică generată automat la înregistrarea dispozitivului, utilizată pentru blocarea de la distanță a dispozitivului (exclusiv pentru dispozitive Android).
- **Stare Criptare**. Unele dispozitive Android 3.0 sau mai recente acceptă funcția de criptare. Verificați starea de criptare pe pagina de detalii a dispozitivului pentru a afla dacă acesta acceptă funcția de criptare. În cazul în care criptarea a fost impusă de politica de pe dispozitiv, puteți, de asemenea, să vedeți starea de activare a criptării.

- **Detalii de activare**
  - **Cod de activare**. Token-ul unic de activare alocat dispozitivului.
  - Adresa serverului de comunicații.
  - **Cod QR**. Codul QR unic care conține token-ul de activare și adresa serverului de comunicații.
- **Hardware**. Puteți vizualiza informații referitoare la hardware-ul dispozitivului, disponibile exclusiv pentru dispozitivele administrate (activate) Informațiile referitoare la harware sunt verificate la fiecare 12 ore și actualizate dacă apar modificări.

Important
Începând cu Android 10, GravityZone Mobile Client nu are acces la numărul de serie, codul IMEI, IMSI și adresa MAC a dispozitivului. Această restricție duce la următoarele situații:
- Dacă pentru dispozitivul mobil, care are deja instalat GravityZone Mobile Client, se face upgrade de la o versiune Android mai veche la Android 10, Control Center va afișa detaliile corecte ale dispozitivului. Înainte de upgrade, dispozitivul trebuie să ruleze cea mai recentă versiune de GravityZone Mobile Client.
- Dacă GravityZone Mobile Client se instalează pe un dispozitiv Android 10, Control Center va afișa detalii incorecte despre acest dispozitiv din cauza limitelor impuse de sistemul de operare.

- **Rețea**. Aici puteți vizualiza informații referitoare la conectivitatea rețelei, disponibile exclusiv pentru dispozitivele administrate (activate).

6.4.7. Sortarea, filtrarea și căutarea dispozitivelor mobile

Tabelul inventarului Dispozitive mobile se poate întinde pe mai multe pagini, în funcție de numărul de utilizatori sau dispozitive (implicit, se afișează doar 10 intrări pe pagină). Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului. Pentru a modifica numărul de intrări afișate pe pagină, selectați o opțiune din meniul de lângă butoanele de navigație.

Dacă sunt prea multe intrări, puteți utiliza opțiunile de filtrare pentru a afișa doar intrările care vă interesează. De exemplu, puteți căuta un anumit dispozitiv mobil sau selecta să vizualizați numai dispozitive administrate.

Sortarea inventarului Dispozitive mobile

Pentru a sorta datele după o anumită coloană, faceți clic pe titlurile coloanelor. De exemplu, dacă doriți să ordonați dispozitivele după nume, faceți clic pe titlul **Nume**. Dacă faceți din nou clic pe numele de coloană, dispozitivele vor fi afișate în ordine inversă.

Filtrarea inventarului Dispozitive mobile

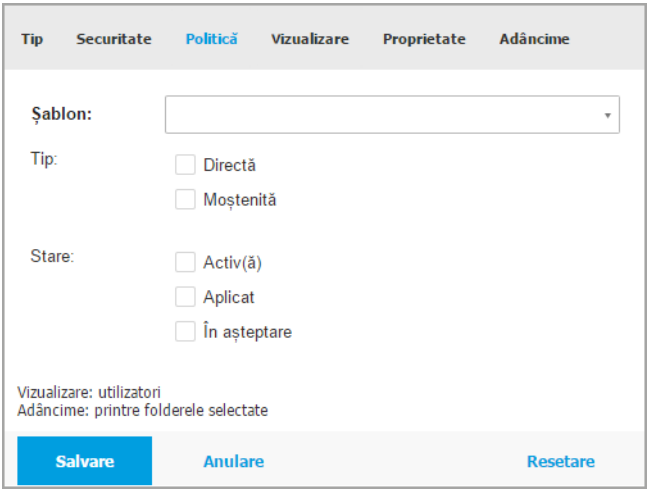
1. Selectați grupul dorit din fereastra din stânga.
2. Faceți clic pe meniul **Filtere** din partea de sus a zonei ferestrelor de rețea.
3. Folosiți criteriile de filtrare după cum urmează:
   - **Tip**. Selectați tipul de entități pe care doriți să le afișați (Utilizatori/Dispozitive și Foldere).

Dispozitive mobile - Filtrare după tip

- **Securitate**. Alegeți afișarea calculatoarelor după starea de administrare și securitate.

Dispozitive mobile - Filtrare după securitate

- **Politică**. Selectați modelul de politică dorit pentru filtrarea dispozitivelor mobile după tipul de atribuire a politicii (Directă sau Moștenită), precum și starea de atribuire a politicii (Activă, Aplicată sau În așteptare).



Dispozitive mobile - Filtrare după politică

- **Vizualizare**. Selectați **Utilizatori** pentru a afișa exclusiv utilizatorii din grupul selectat. Selectați **Dispozitive** pentru a afișa exclusiv dispozitivele din grupul selectat.

Dispozitive mobile - Filtrare după Vizualizare

- **Proprietate**. Puteți filtra dispozitivele mobile în funcție de proprietar, selectând afișarea dispozitivelor **Companie** sau **Personal**. Atributul de proprietate este definit în detaliile dispozitivelor mobile.

Dispozitive mobile - Filtrare după tip proprietate

- **Adâncime**. Când administrați o rețea de tip arbore, dispozitivele mobile sau utilizatorii din sub-grupuri nu sunt afișate la selectarea grupului rădăcină. Selectați opțiunea **toate obiectele recursiv** pentru a vedea toate entitățile din grupul curent și din sub-grupuri.

Dispozitive mobile - Filtrare după adâncime

4. Faceți clic pe **Salvare** pentru a filtra inventarul dispozitivelor mobile după criteriile selectate.

   Filtrul rămâne activ în pagina **Rețea** până când vă deconectați sau resetați filtrul.

Căutarea Dispozitivelor Mobile

Tabelul din fereastra din dreapta oferă informații specifice referitoare la utilizatori și dispozitivele mobile. Puteți utiliza categoriile disponibile în fiecare coloană, pentru a filtra conținutul tabelului.

1. Selectați grupul dorit din fereastra din stânga.
2. Treceți la ecranul dorit (Utilizatori sau Dispozitive mobile) folosind meniul **Filtre** din partea de sus a ferestrei rețea.
3. Căutați entitățile dorite folosind câmpurile de căutare din titlul fiecărei coloane din fereastra din dreapta:
   - Introduceți termenul de căutare orit în câmpul de căutare corespunzător.

     De exemplu, treceți la ecranul **Dispozitive** și introduceți numele utilizatorului căutat în câmpul **Utilizator**. În tabel se vor afișa doar dispozitivele mobile care corespund criteriilor de căutare.
   - Selectați atributul după care doriți să efectuați căutarea în casetele corespunzătoare din lista derulantă.

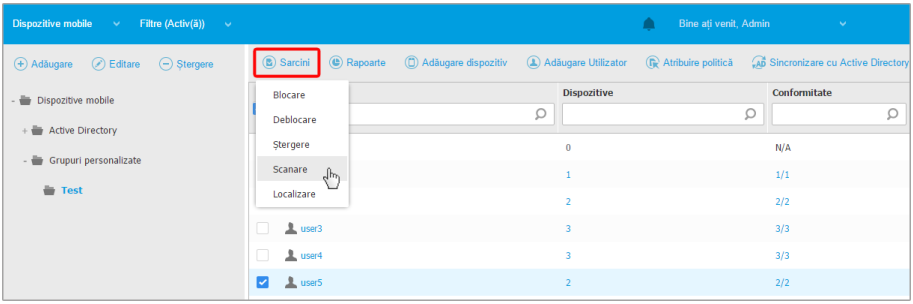
De exemplu, treceți la ecranul **Dispozitive**, faceți clic pe caseta listei **OS** și selectați **Android** pentru a vizualiza doar dispozitivele mobile Android.

Notă
Pentru a șterge termenul de căutare și a afișa toate entitățile, așezați cursorul mausului deasupra casetei corespunzătoare și faceți clic pe pictograma ×.

6.4.8. Executarea sarcinilor pe dispozitive mobile

De pe pagina **Rețea**, puteți rula de la distanță o serie de sarcini administrative pe dispozitivele mobile. Iată ce puteți face:

- „Blochează” (p. 185)
- „Ștergere” (p. 186)
- „Scanează” (p. 187)
- „Localizează” (p. 188)



Sarcini pentru dispozitive mobile

Pentru a rula sarcini de la distanță pe dispozitivele mobile, trebuie îndeplinite anumite cerințe preliminare. Pentru informații suplimentare, consultați secțiunea Instalare și cerințe din Ghidul de instalare GravityZone.

Puteți opta pentru generarea unor sarcini individual pentru fiecare dispozitiv mobil, fiecare utilizator sau pentru grupuri de utilizatori. De exemplu, puteți scana de la distanță dispozitivele mobile dintr-un grup de utilizatori pentru identificarea malware-ului. De asemenea, puteți executa o sarcină de localizare pentru un anumit dispozitiv mobil.

Inventarul rețelei poate include dispozitive mobile active, inactive sau neadministrate. După ce au fost create, sarcinile vor începe să ruleze imediat pe

dispozitivele mobile active. Pentru dispozitivele care sunt inactive, sarcinile vor începe să ruleze imediat ce acestea sunt din nou online. Sarcinile nu vor fi generate pentru dispozitive mobile neadministrate. În acest caz, se va afișa o notificare cu privire la faptul că sarcina nu a putut fi generată.

Puteți vizualiza și gestiona sarcinile pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor" (p. 207).

Blochează

Opțiunea Blocare blochează imediat ecranul dispozitivelor mobile țintă. Opțiunea Blocare depinde de sistemul de operare:

- Sarcina de blocare pentru dispozitivele Android (7.0 sau mai recent) va pune în aplicare setul de parole din consola dumneavoastră GravityZone numai dacă pe dispozitiv nu este configurată o protecție la blocare. În caz contrar, pentru protejarea dispozitivului se vor utiliza opțiunile existente de blocare a ecranului, precum model, PIN, parolă, amprentă sau blocare inteligentă.

  Notă

  – Parola ecranului de blocare generată de Control Center este afișată în fereastra Detalii dispozitiv mobil.

  – Sarcina de deblocare nu mai este disponibilă pentru dispozitivele Android (7.0 sau mai recent). În schimb, utilizatorii își pot debloca dispozitivele manual. Cu toate acestea, trebuie să vă asigurați din timp că acele dispozitive acceptă cerințele de complexitate preconizate pentru parola de deblocare.

  – Din cauza unor limitări de ordin tehnic, sarcina Blocare nu este disponibilă pe Android 11.

- Pe dispozitivele iOS, dacă acestea au o parolă pentru blocarea ecranului, parola va fi solicitată pentru deblocare.

Pentru blocarea dispozitivelor de la distanță:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga.
4. Faceți clic pe meniul **Filtre** din partea de sus a ferestrelor de rețea și selectați **Utilizatori** din categoria **Vizualizare**. Faceți clic pe **Save**. Toți utilizatorii din grupul selectat sunt afișați în tabel.

5. Selectați casetele de bifare care corespund utilizatorilor doriți. Puteți selecta unul sau mai mulți utilizatori simultan.
6. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Blocare**.
7. Vi se va solicita să confirmați alegerea făcând clic pe **Da**. Se va afișa un mesaj de informare cu privire la generarea sarcinii.
8. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Ștergere

Sarcina **Ștergere** readuce dispozitivele mobile țintă la setările din fabrică. Executați această sarcină pentru a șterge toate informațiile sensibile și aplicațiile stocate pe dispozitivele mobile țintă de la distanță.

Avertisment

Folosiți sarcina **Ștergere** cu atenție. Verificați tipul de proprietate al dispozitivelor țintă (dacă doriți să evitați ștergerea datelor de pe dispozitivele personale) și asigurați-vă că doriți într-adevăr să ștergeți datele stocate pe dispozitivele selectate. După ce a fost transmisă, sarcina **Ștergere** nu poate fi revocată.

Notă

Din cauza unor limitări de ordin tehnic, sarcina Ștergere nu este disponibilă pe Android 11.

Pentru a șterge datele de pe un dispozitiv mobil de la distanță:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga.
4. Faceți clic pe meniul **Filtre** din partea de sus a ferestrelor de rețea și selectați **Dispozitive** din categoria **Vizualizare**. Faceți clic pe **Save**. Toate dispozitivele din grupul selectat sunt afișate în tabel.

   Notă

   De asemenea, puteți selecta **Toate articolele recursiv** din secțiunea **Adâncime** pentru a vedea toate dispozitivele din grupul curent.

5. Selectați caseta de bifare corespunzătoare dispozitivului de pe care doriți să ștergeți datele.
6. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Ștergere**.
7. Vi se va solicita să confirmați alegerea făcând clic pe **Da**. Se va afișa un mesaj de informare cu privire la generarea sarcinii.
8. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Scanează

Sarcina **Scanare** vă permite să scanați dispozitivele mobile selectate pentru identificarea malware-ului. Utilizatorul dispozitivului este informat cu privire la orice malware detectat și i se solicită să îl elimine. Scanarea este efectuată în cloud. Prin urmare, dispozitivul trebuie să aibă acces la Internet.

Notă
Scanarea de la distanță nu funcționează pe dispozitivele iOS (limitarea platformei).

Pentru a scana dispozitivele mobile de la distanță:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga.
4. Faceți clic pe meniul **Filtre** din partea de sus a ferestrelor de rețea și selectați **Dispozitive** din categoria **Vizualizare**. Faceți clic pe **Save**. Toate dispozitivele din grupul selectat sunt afișate în tabel.

   Notă
   De asemenea, puteți selecta **Toate articolele recursiv** din secțiunea **Adâncime** pentru a vedea toate dispozitivele din grupul curent.
   Pentru a afișa doar dispozitivele Android din grupul selectat, mergeți la titlul coloanei **SO** din fereastra din dreapta și selectați **Android** din caseta corespunzătoare din listă.

5. Selectați casetele de bifare care corespund dispozitivelor pe care doriți să le scanați.

6. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Scanare**.
7. Vi se va solicita să confirmați alegerea făcând clic pe **Da**. Se va afișa un mesaj de informare cu privire la generarea sarcinii.
8. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. La finalizarea scanării, se generează un raport de scanare. Faceți clic pe pictograma corespunzătoare din coloana **Rapoarte** pentru a genera un raport rapid.

   Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

Localizează

Sarcina Localizare deschide o hartă care indică locația dispozitivelor selectate. Puteți localiza unul sau mai multe dispozitive mobile simultan.

Pentru ca sarcina Localizare să funcționeze, serviciile de localizare trebuie să fie activate pe dispozitivele mobile.

Pentru localizarea dispozitivelor mobile:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga.
4. Faceți clic pe meniul **Filtre** din partea de sus a ferestrelor de rețea și selectați **Dispozitive** din categoria **Vizualizare**. Faceți clic pe **Save**. Toate dispozitivele din grupul selectat sunt afișate în tabel.

   Notă
   De asemenea, puteți selecta **Toate articolele recursiv** din secțiunea **Adâncime** pentru a vedea recursiv toate dispozitivele din grupul curent.

5. Selectați caseta de bifare care corespunde dispozitivului pe care doriți să îl localizați.
6. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Localizare**.
7. Se deschide fereastra **Locație**, care include următoarele informații:

- O hartă cu poziția dispozitivelor mobile selectate. Dacă un dispozitiv nu este sincronizat, harta va afișa ultima locație cunoscută.
- Un tabel cu detaliile dispozitivelor selectate (nume, utilizator, data și ora ultimei sincronizări). Pentru a vedea locația unui anumit dispozitiv pe hartă, nu trebuie decât să selectați caseta de bifare corespunzătoare. Harta va centra automat pe locația corespunzătoare a dispozitivului.
- Opțiunea **Reîmprospătare automată** actualizează automat locațiile dispozitivelor mobile selectate, după fiecare 10 secunde.

8. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul „Vizualizarea și administrarea sarcinilor” (p. 207).

6.4.9. Crearea de rapoarte rapide

Puteți opta pentru crearea de rapoarte rapide pe dispozitivele mobile, din pagina **Rețea**:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Selectați grupul dorit din fereastra din stânga.
4. Faceți clic pe meniul **Filtre** din partea de sus a ferestrelor de rețea și selectați **Dispozitive** din categoria **Vizualizare**. De asemenea, puteți selecta opțiunile Administrate din secțiunea **Securitate**, pentru a filtra grupul selectat exclusiv după dispozitivele administrate. Faceți clic pe **Save**. Toate dispozitivele corespunzătoare criteriilor de filtrare din grupul selectat sunt afișate în tabel.
5. Selectați casetele de bifare care corespund tipurilor de dispozitive mobile de care sunteți interesat. Puteți selecta unul sau mai multe dispozitive mobile simultan.
6. Faceți clic pe butonul **Rapoarte** din partea de sus a tabelului și selectați tipul de raport din meniu. Pentru mai multe informații, consultați capitolul „Rapoarte privind dispozitivele mobile” (p. 493)
7. Configurați opțiunile pentru raport. Pentru mai multe informații, consultați capitolul „Crearea rapoartelor” (p. 495)

8. Faceți clic pe **Generare**. Raportul este afișat imediat. Intervalul necesar pentru generarea rapoartelor poate diferi în funcție de numărul de dispozitive mobile selectate.

6.4.10. Atribuirea unei politici

Puteți administra setările de securitate pe dispozitivele mobile folosind politicile.

Din secțiunea **Rețea**, puteți vizualiza, modifica și atribui politicile pentru dispozitivele mobile din contul dumneavoastră.

Puteți atribui politici grupurilor, utilizatorilor sau anumitor dispozitive mobile.

Notă

O atribuire a unei politici unui utilizator afectează dispozitivele deținute de utilizator. Pentru mai multe informații, consultați capitolul „Alocarea politicilor locale" (p. 224).

Pentru a vizualiza setările de securitate alocate unui dispozitiv mobil:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Faceți clic pe meniul **Filtre** din partea de sus a ferestrelor de rețea și selectați **Dispozitive** din categoria **Vizualizare**. Faceți clic pe **Save**. Toate dispozitivele care aparțin utilizatorilor din grupul selectat sunt afișate în tabel.
4. Faceți clic pe denumirea dispozitivului mobil dorit. Se va afișa o fereastră cu detalii.
5. În secțiunea **Securitate** din pagina **Prezentare generală**faceți clic pe denumirea politicii curente, pentru vizualizarea setărilor.
6. Puteți modifica setările de securitate, după caz. Vă rugăm să rețineți că orice modificări efectuate se vor aplica și tuturor celorlalte dispozitive pe care este activă politica.

   Pentru mai multe informații, consultați capitolul „Politici pentru dispozitive mobile" (p. 392)

Pentru atribuirea unei politici unui dispozitiv mobil:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. În fereastra din stânga, selectați grupul care vă interesează.

4. Faceți clic pe meniul **Filtre** din partea de sus a ferestrelor de rețea și selectați **Dispozitive** din categoria **Vizualizare**. Faceți clic pe **Save**. Toate dispozitivele care aparțin utilizatorilor din grupul selectat sunt afișate în tabel.
5. În fereastra din dreapta, selectați caseta de bifare a dispozitivului mobil dorit.
6. Faceți clic pe butonul **Alocare politică** din partea de sus a tabelului.
7. Efectuați setările necesare în fereastra **Atribuire politică**. Pentru mai multe informații, consultați capitolul „Alocarea politicilor locale" (p. 224).

6.4.11. Sincronizarea cu Active Directory

Inventarul rețelei estee sincronizat automat cu Active Directory la intervalul specificat în secțiunea de configurare Control Center. Pentru mai multe informații, consultați capitolul de Instalare și Configurare GravityZone din Ghidul de instalare GravityZone.

Pentru sincronizarea manuală a utilizatorilor afișați în prezent cu Active Directory:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Faceți clic pe butonul **Sincronicare cu Active Directory** din partea de sus a tabelului.
4. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

Notă

Pentru rețelele Active Directory extinse, sincronizarea poate dura mai mult.

6.4.12. Ștergerea utilizatorilor și dispozitivelor mobile

Dacă inventarul rețelei conține utilizatori sau dispozitive mobile inactive, se recomandă ștergerea acestora.

Ștergerea dispozitivelor mobile din Inventarul rețelei

Atunci când ștergeți un dispozitiv din Control Center:

- GravityZone Mobile Client nu este conectat, dar nu este dezinstalat de pe dispozitiv.

- Pentru dispozitivele iOS, profilul MDM este șters. Dacă dispozitivul nu este conectat la internet, profilul MDM rămâne instalat până când devine disponibilă o nouă conexiune.
- Toate jurnalele referitoare la dispozitivul șters sunt încă disponibile.
- Informațiile personale și aplicațiile dvs. nu sunt afectate.

Avertisment

- Dispozitivele mobile șterse nu pot fi recuperate.
- Dacă ștergeți din greșeală un dispozitiv blocat, este necesar să resetați dispozitivul la setările din fabrică pentru a-l debloca.

Pentru ștergerea unui dispozitiv mobil:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. În fereastra din stânga, selectați grupul care vă interesează.
4. Faceți clic pe meniul **Filtre** din partea de sus a ferestrelor de rețea și selectați **Dispozitive** din categoria **Vizualizare**.
5. Faceți clic pe **Save**.
6. Selectați caseta de bifare care corespunde dispozitivelor mobile pe care doriți să le ștergeți.
7. Faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

Ștergerea utilizatorilor din Inventarul rețelei

Utilizatorii asociați în prezent cu dispozitive mobile nu pot fi șterși. Va trebui să ștergeți mai întâi dispozitivele mobile corespunzătoare.

Notă
Puteți șterge doar utilizatorii din Grupurile personalizate.

Pentru a șterge un utilizator:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.

3. În fereastra din stânga, selectați grupul care vă interesează.
4. Faceți clic pe meniul **Filtre** din partea de sus a ferestrelor de rețea și selectați **Utilizatori** din categoria **Vizualizare**.
5. Faceți clic pe **Save**.
6. Selectați caseta de bifare corespunzătoare utilizatorului pe care doriți să îl ștergeți.
7. Faceți clic pe butonul ⊖ **Ștergere** din dreapta tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

6.5. Inventar aplicații

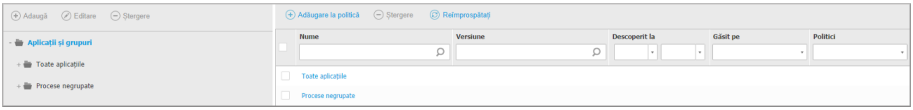
Puteți vizualiza toate aplicațiile descoperite în rețeaua dvs. prin intermediul sarcinii **Descoperire aplicații**, în secțiunea **Aplicații grupuri**. Pentru mai multe informații, consultați capitolul „Descoperire aplicații" (p. 101).

Aplicațiile și procesele sunt adăugate automat în folderul **Aplicații și grupuri**, în secțiunea din stânga.

Puteți organiza aplicațiile și procesele în grupuri personalizate.

Toate aplicațiile/procesele din folderul selectat sunt afișate în tabelul din secțiunea din dreapta. Puteți efectua o căutare după nume, versiune, editor/autor, program de actualizare, locație și politică.

Pentru vedea cele mai recente informații din tabel, efectuați clic pe butonul **Reîmprospătare** din partea de sus a tabelului. Acest lucru poate fi necesar atunci când petreceți mai mult timp pe pagină.



Inventar aplicații

Important
Noile aplicații descoperite de fiecare dată când executați sarcina **Descoperire aplicații** sunt puse automat în folderul **Aplicații negrupate**. Procesele care nu au legătură cu anumite aplicați sunt puse în folderul **Procese negrupate**.

Arbore de aplicații și grupuri

Pentru a adăuga un grup personalizat în arborele **Aplicații și grupuri**:

1. Selectați folderul **Toate aplicațiile**.
2. Efectuați clic pe butonul ⊕ **Adăugare** din partea de sus a arborelui.
3. Introduceți o denumire în noua fereastră.
4. Efectuați clic pe **OK** pentru a crea noul grup.
5. Selectați folderul **Aplicații negrupate**. Toate aplicațiile grupate într-un folder selectat sunt afișate în tabelul din secțiunea din dreapta.
6. Selectați aplicațiile dorite din tabelul din secțiunea din dreapta. Trageți și inserați obiectele selectate din secțiunea din dreapta pentru a le muta în grupul personalizat dorit din secțiunea din stânga.

Pentru a adăuga o aplicație personalizată:

1. Selectați folderul țintă din **Toate aplicațiile**.
2. Efectuați clic pe butonul ⊕ **Adăugare** din partea de sus a arborelui.
3. Introduceți o denumire în noua fereastră.
4. Efectuați clic pe **OK** pentru a crea aplicația personalizată.
5. Puteți adăuga procese legate de noua aplicație personalizată din folderul **Procese negrupate** sau din alte foldere afișate în arborele **Aplicații și grupuri**. După ce selectați folderul, toate procesele sunt afișate în tabelul din secțiunea din dreapta.
6. Selectați procesele dorite din tabelul din secțiunea din dreapta. Trageți și inserați elementele selectate din secțiunea din stânga pentru a le muta în aplicația personalizată.

Notă
O aplicație poate face parte dintr-un singur grup.

Pentru a edita un nume de folder sau aplicație:

1. Selectați-l din arborele **Aplicații și grupuri**.
2. Efectuați clic pe butonul ✎ **Editare** din partea de sus a arborelui.
3. Schimbați denumirea în cea dorită.

4. Faceți clic pe **OK**.

Puteți muta grupurile și aplicațiile oriunde în ierarhia **Aplicații și grupuri**. Pentru a muta un grup sau o aplicație, trageți-o și inserați-o din locația curentă în cea nouă.

Pentru a elimina un folder sau o aplicație personalizată, selectați-l(o) în arborele **Aplicații și grupuri** și apoi efectuați clic pe butonul ⊖ **Eliminare** din partea de sus a arborelui.

Adăugarea aplicațiilor la politici

Pentru a adăuga o aplicație sau un proces la o regulă direct din Inventarul de aplicații:

1. Selectați folderul dorit din arborele **Aplicații și grupuri**. Conținutul folderului este afișat în secțiunea din dreapta.
2. Selectați procesele sau aplicațiile dorite din secțiunea din dreapta.
3. Efectuați clic pe butonul ⊕ **Adăugare la politică** pentru a deschide fereastra de configurare.
4. În secțiunea **Aplicare regulă la aceste politici**, introduceți denumirea unei politici existente. Utilizați caseta de căutare pentru a găsi politica după denumire sau autor.
5. În secțiunea **Detalii regulă**, introduceți o **Denumire de regulă**.
6. Bifați caseta **Activat** pentru a activa regula.
7. Tipul țintei este recunoscut automat. Dacă este nevoie, modificați criteriile existente:
   - **Procese specifice**, pentru a defini un proces a cărui pornire este permisă sau respinsă. Puteți face autorizarea în funcție de cale, codul hash sau certificat. Condițiile din cadrul regulii sunt potrivite cu ajutorul operatorului logic AND.
     - Pentru a autoriza o aplicație dintr-o cale specifică:
       a. Selectați **Cale** în coloana **Tip**. Specificați calea către obiect. Puteți specifica un nume de cale absolut sau relativ și puteți utiliza caractere wildcard. Simbolul asterisc (*) corespunde oricărui fișier dintr-un director. Un simbol asterisc dublu (**) se potrivește cu toate fișierele și directoarele din directorul definit. Semnul întrebării (?) corespunde

unui singur caracter. De asemenea, puteți adăuga o descriere pentru a ajuta la identificarea procesului.

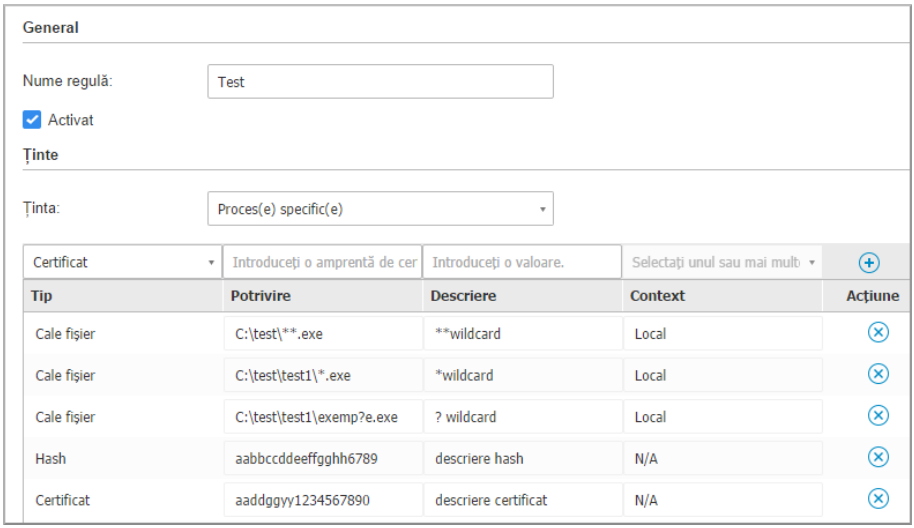
b. Din meniul derulant **Selectați unul sau mai multe contexte** puteți alege între local, CD-ROM, unitate detașabilă și rețea. Puteți bloca o aplicație executată de pe o unitate detașabilă sau puteți permite executarea acesteia dacă aplicația este executată local.

– Pentru a autoriza o aplicație pe baza codului hash, selectați **Hash** din coloana **Tip** și introduceți o valoare hash. De asemenea, puteți adăuga o descriere pentru a ajuta la identificarea procesului.

Important
Pentru a genera valoarea hash, descărcați instrumentul Amprentă. Pentru mai multe informații, consultați capitolul „Instrumente Control aplicații” (p. 570)

– Pentru a efectua autorizarea pe baza certificatului, selectați **Certificat** din coloana **Tip** și introduceți o amprentă de certificat. De asemenea, puteți adăuga o descriere pentru a ajuta la identificarea procesului.

Important
Pentru a obține o amprentă de certificat, descărcați instrumentul Amprentă. Pentru mai multe informații, consultați capitolul „Instrumente Control aplicații” (p. 570)



Reguli privind aplicația

Faceți clic pe ⊕**Adăugare** pentru a adăuga regula. Regula nou creată va avea cea mai mare prioritate din această politică.

- **Aplicații sau grupuri inventar**, pentru a adăuga un grup sau o aplicație descoperită în rețeaua dumneavoastră. Puteți vizualiz aplicațiile în curs de execuție în rețeaua dumneavoastră în pagina **Rețea > Inventar aplicații**.

  Introduceți denumirile aplicațiilor sau grupurilor în câmpul corespunzător, separate prin virgulă. Funcția de completare automată va afișa sugestii pe măsură ce tastați.

8. Bifați caseta **Includere subprocese** pentru a aplica regula la procese subordonate generate.

Avertisment
Atunci când configurați reguli pentru aplicațiile de browser, se recomandă să dezactivați această opțiune pentru a preveni riscurile de securitate.

9. Opțional, puteți defini excepții de la regula de pornire a proceselor. Operațiunea de adăugare este similară celei descrise la pașii anteriori.

10. În secțiunea **Drepturi de acces**, alegeți dacă să permiteți sau să interziceți executarea regulii.
11. Faceți clic pe **Salvare** pentru a aplica modificările.

Pentru a șterge o aplicație sau un proces:

1. Selectați folderul dorit din arborele **Aplicații și grupuri**.
2. Selectați procesele sau aplicațiile dorite din secțiunea din dreapta.
3. Faceți clic pe butonul **Ștergere**.

Programe de actualizare

Trebuie să definiți programe de actualizare pentru aplicațiile descoperite în rețeaua dvs.

Avertisment
Dacă nu atribuiți programe de actualizare, nu va fi permisă actualizarea aplicațiilor incluse în lista albă.

Pentru a atribui un program de actualizare:

1. Selectați folderul dorit din arborele **Aplicații și grupuri**. Conținutul folderului este afișat în secțiunea din dreapta.
2. În partea dreaptă a secțiunii laterale, selectați fișierul pe care doriți să-l utilizați ca program de actualizare.
3. Efectuați clic pe butonul **Atribuire programe de actualizare**.
4. Efectuați clic pe **Da** pentru a confirma atribuirea. Programele de actualizare sunt marcate cu o pictogramă specifică:

Program de actualizare

Pentru a anula un program de actualizare:

1. Selectați folderul dorit din arborele **Aplicații și grupuri**. Conținutul folderului este afișat în secțiunea din dreapta.

2. În partea dreaptă a secțiunii laterale, selectați programul de instalare pe care doriți să-l anulați.
3. Efectuați clic pe butonul **Anulare program de actualizare**.
4. Faceți clic pe **Da** pentru confirmare.

6.6. Inventarul de patch-uri

GravityZone identifică patch-urile necesare software-ului prin sarcinile de **Scanare patch-uri** și apoi le include în inventarul patch-urilor.

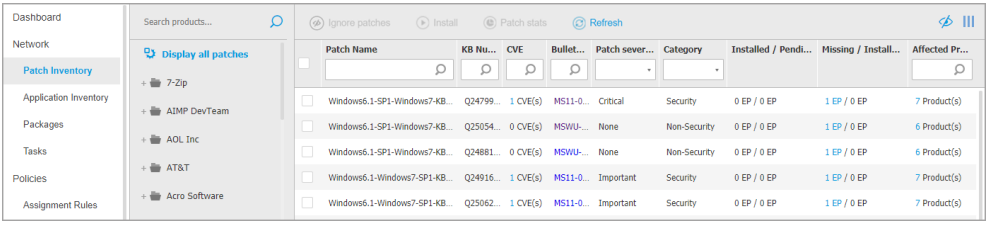
Pagina **Inventar patch-uri** afișează toate patch-urile identificate pentru software-ul instalat pe stațiile dvs. de lucru și oferă o serie de măsuri pe care le puteți lua pentru aceste patch-uri.

Folosiți inventarul de patch-uri de fiecare dată când aveți nevoie să instalați imediat anumite patch-uri. Această alternativă vă permite să rezolvați cu ușurință anumite probleme pe care le cunoașteți. De exemplu, ați citit un articol despre o vulnerabilitate software și cunoașteți ID-ul CVE. Puteți efectua căutări în inventar după patch-uri care vizează respectivul CVE și apoi puteți vizualiza stațiile de lucru care ar trebui actualizate.

Pentru a accesa inventarul de patch-uri, efectuați clic pe opțiunea **Rețea > Inventar de patch-uri** din meniul principal al Control Center.

Pagina este organizată în două secțiuni:

- Secțiunea din stânga afișează produsele software instalate în rețeaua dumneavoastră, grupate după producător.
- Secțiunea din dreapta conține un tabel cu patch-urile disponibile și detalii despre acestea.



Inventarul de patch-uri

În continuare, veți afla cum să utilizați inventarul. Iată ce puteți face:

- Vizualizare detalii patch-uri
- Căutare și filtrare patch-uri
- Ignorare patch-uri
- Instalare patch-uri
- Dezinstalare patch-uri
- Creare statistici patch-uri

6.6.1. Vizualizarea detaliilor patch-urilor

Tabelul de patch-uri oferă informații care vă ajută să identificați patch-urile, să evaluați importanța lor, să vizualizați starea de instalare și sfera de aplicare. Detaliile sunt descrise în continuare:

- **Denumirea patch-ului.** Aceasta este denumirea fișierului executabil care conține patch-ul.
- **Număr KB.** Acest număr identifică articolul KB care anunță lansarea patch-ului.
- **CVE.** Acesta este numărul vulnerabilităților CVE remediate prin patch. Dacă efectuați clic pe număr, se va afișa lista ID-urilor CVE.
- **ID-ul buletinului.** Acesta este codul de identificare al buletinului de securitate emis de producător. Acest ID face conexiunea la articolul în cauză, care descrie patch-ul și oferă detalii privind instalarea.
- **Severitatea patch-ului.** Acest scor vă informează cu privire la importanța patch-ului în raport cu problemele pe care le previne.
- **Categorie.** În funcție de tipul problemelor pe care le remediază, patch-urile sunt grupate în două categorii: de securitate și non-securitate. Acest câmp vă informează în ce categorie se încadrează patch-ul.
- **Instalate / În așteptare.** Aceste numere arată câte stații de lucru au patch-ul respectiv instalat și câte sunt în așteptarea instalării patch-ului. Numerele fac conexiunea la lista acestor stații de lucru.
- **Lipsă / Instalare nereușită.** Aceste numere arată câte stații de lucru nu au patch-ul respectiv instalat și pe câte nu a reușit instalarea. Numerele fac conexiunea la lista acestor stații de lucru.

- **Produse afectate.** Acesta este numărul de produse pentru care a fost lansat patch-ul. Acest număr face conexiunea la lista acestor produse software.
- **Amovibil.** Dacă trebuie să dezinstalați un anumit patch, trebuie mai întâi să verificați dacă acest lucru este posibil. Folosiți acest filtru pentru a afla ce patch-uri pot fi eliminate (dezinstalate). Pentru informații suplimentare, consultați Dezinstalarea patch-urilor.

Pentru a personaliza detaliile afișate în tabel:

1. Faceți clic pe butonul **Coloane** din partea dreaptă a Barei de instrumente Acțiuni.
2. Selectați coloanele pe care doriți să le vizualizați.
3. Faceți clic pe butonul **Resetare** pentru a reveni la vizualizare implicită coloane.

În timp ce vă aflați în această pagină, procesele GravityZone care sunt executate în fundal pot afecta baza de date. Asigurați-vă că vizualizați cele mai recente informații din tabel efectuând clic pe butonul **Reîmprospătare** din partea de sus a tabelului.

GravityZone revizuiește săptămânal lista de patch-uri disponibile și le șterge pe cele care nu mai sunt aplicabile din cauza faptului că aplicațiile sau endpoint-urile aferente nu mai există.

De asemenea, GravityZone revizuiește și șterge zilnic patch-urile indisponibile din listă, cu toate că este posibil ca acestea să existe pe unele endpoint-uri.

6.6.2. Căutarea și filtrarea patch-urilor

În mod implicit, Control Center afișează toate patch-urile disponibile pentru produsele software ale dumneavoastră. GravityZone vă pune la dispoziție mai multe opțiuni pentru a găsi rapid patch-urile de care aveți nevoie.

Filtrarea patch-urilor în funcție de produs

1. Localizați produsul în secțiunea din stânga.

   Puteți face acest lucru fie prin parcurgerea listei în vederea identificării producătorului, fie tastând denumirea în caseta de căutare din partea de sus a secțiunii.

2. Efectuați clic pe numele producătorului pentru a extinde lista și pentru a vizualiza produsele aferente.

3. Selectați produsul pentru care doriți să vizualizați patch-urile disponibile sau deselectați-l pentru a ascunde patch-urile asociate acestuia.
4. Repetați pașii anteriori pentru alte produse care vă interesează.

Dacă doriți să vizualizați din nou patch-urile pentru toate produsele, efectuați clic pe butonul **Afișează toate patch-urile** din partea de sus a secțiunii din stânga.

Filtrarea patch-urilor în funcție de utilitate

Un patch devine inutil dacă, de exemplu, acesta sau o nouă versiune a sa este deja instalat pe stația de lucru. Întrucât inventarul poate conține uneori astfel de patch-uri, GravityZone vă permite să le ignorați. Selectați aceste patch-uri și apoi efectuați clic pe butonul **Ignorare patch-uri** din partea de sus a tabelului.

Control Center afișează patch-urile ignorate într-un alt mod de vizualizare. Faceți clic pe butonul **Administrate/Ignorate** din partea dreaptă a Barei de instrumente de acțiune pentru a comuta între modurile de vizualizare:

- - pentru a vizualiza patch-urile ignorate.
- - pentru a vizualiza patch-urile administrate.

Filtrarea patch-urilor în funcție de detalii

Folosiți funcția de căutare pentru a filtra patch-urile în funcție de anumite criterii sau detalii cunoscute. Introduceți cuvintele cheie în casetele de căutare din partea de sus a tabelului de patch-uri. Patch-urile care corespund căutării sunt afișate în tabel pe măsură ce tastați sau în momentul efectuării selecției.

Ștergerea datelor din câmpurile de căutare va duce la resetarea căutării.

6.6.3. Ignorare patch-uri

Este posibil să fie necesar să excludeți anumite patch-uri din inventar, dacă nu plănuiți să le instalați pe stațiile dvs. de lucru, folosind comanda **Ignorare patch-uri**.

Un patch ignorat va fi exclus automat din sarcinile automate pentru patch-uri și din rapoarte și nu va fi numărat ca patch lipsă.

Pentru a ignora un patch:

1. Pe pagina **Inventar patch-uri**, selectați unul sau mai multe patch-uri pe care doriți să le ignorați.
2. Faceți clic pe butonul **Ignorare patch-uri** din partea de sus a tabelului.

Se va afișa o fereastră de configurare, în care puteți vedea detaliile patch-urilor selectate, alături de orice patch-uri subordondate.

3. Faceți clic pe **Ignoră**. Patch-ul va fi șters din lista inventarului patch-urilor.

Puteți găsi patch-urile ignorate într-un ecran dedicat și puteți iniția acțiuni cu privire la acestea:

- Faceți clic pe butonul **Afișare patch-uri ignorate** din colțul din dreapta sus al tabelului. Se va afișa o listă a tuturor patch-urilor ignorate.
- Puteți obține informații suplimentare referitoare la anumite patch-uri ignorate generând un raport de statistici ale patch-urilor. Selectați patch-ul ignorat dorit și faceți clic pe butonul **Stări patch-uri** din partea de sus a tabelului. Pentru mai multe detalii, consultați „Crearea statisticilor referitoare la patch-uri” (p. 207)
- Pentru a restaura patch-urile ignorate, selectați-le și faceți clic pe butonul **Restaurare patch-uri** din partea de sus a tabelului.

  Se va afișa o fereastră de configurare, în care puteți vedea detaliile patch-urilor selectate.

  Faceți clic pe butonul **Restaurare** pentru a trimite patch-ul în inventar.

6.6.4. Instalarea patch-urilor

Pentru instalarea patch-urilor din inventarul de patch-uri:

1. Mergeți la **Rețea > Inventar patch-uri**.
2. Localizați patch-urile pe care doriți să le instalați. Dacă este necesar, utilizați opțiunile de filtrare pentru a le găsi rapid.
3. Selectați patch-urile și apoi faceți clic pe butonul **Instalare** din partea de sus a tabelului. Se va afișa o fereastră de configurare, în care puteți edita detaliile de instalare ale patch-ului.

   Veți vedea patch-urile selectate, alături de orice patch-uri subordonate.

   - Selectați grupurile de stații de lucru vizate.
   - **Repornirea stațiilor de lucru după instalarea patch-ului, dacă este necesar**. Această opțiune va reporni stațiile de lucru imediat după instalarea patch-ului, dacă sistemul trebuie repornit. Rețineți că această acțiune poate întrerupe activitatea utilizatorului.

Dacă lăsați această opțiune dezactivată, în cazul în care este necesară o repornire a sistemului pe mașinile de lucru țintă, acestea vor afișa pictograma de stare pentru repornire în curs în inventarul de rețea GravityZone. În acest caz, aveți următoarele opțiuni:

– Transmiteți o sarcină **Repornire mașină** stațiilor de lucru cu repornirea în curs în orice moment. Pentru mai multe detalii, vă rugăm consultați „Repornire sistem” (p. 100).

– Configurați politica activă pentru a informa utilizatorul stației de lucru că sistemul trebuie repornit. Pentru a face acest lucru, accesați politica activă de pe stația de lucru țintă, mergeți la **General > Notificări** și activați opțiunea **Notificare repornire stație de lucru**. În acest caz, utilizatorului i se va afișa un mesaj derulant de fiecare dată când este necesară o repornire a sistemului ca urmare a modificărilor efectuate de componentele GravityZone specificate (în acest caz, Administrarea patch-urilor). Fereastra derulantă include opțiunea de amânare a repornirii. Dacă utilizatorul alege să amâne repornirea, notificarea de repornire va apărea periodic pe ecran până când utilizatorul repornește sistemul sau până când expiră timpul setat de administratorul companiei.

  Pentru mai multe detalii, vă rugăm consultați „Notificare de repornire a stației de lucru” (p. 242).

4. Faceți clic pe **Instalare**.

   Sarcina de instalare este creată, împreună cu sub-sarcinile pentru fiecare stație de lucru.

Notă

- Puteți instala un patch și de pe pagina **Rețea**, începând de la stațiile de lucru specifice pe care doriți să le administrați. În acest caz, selectați stațiile de lucru din inventarul rețelei, faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Instalare patch**. Pentru mai multe informații, consultați capitolul „Instalarea patch-urilor” (p. 82).
- După ce ați instalat un patch, vă recomandăm să transmiteți o sarcină Scanare patch-uri către stațiile de lucru țintă. Această acțiune va actualiza informațiile patch-ului stocate în GravityZone pentru rețelele dvs. administrate.

6.6.5. Dezinstalarea patch-urilor

Este posibil să fie necesar să eliminați patch-urile din cauza defecțiunile de pe stațiile de lucru țintă. GravityZone oferă o opțiune de dezinstalare pentru patch-urile din rețea, care readuce software-ul la starea anterioară aplicării respectivului patch.

Funcția de dezinstalare este disponibilă doar pentru patch-urile care pot fi eliminate. Inventarul patch-urilor GravityZone include o rubrică **Eliminabil**, în care puteți filtra patch-urile după posibilitatea de eliminare.

Notă
Posibilitatea de eliminare depinde caracteristicile atribuite patch-ului de către producător sau de modificările pe care acesta le aduce software-ului. Pentru patch-urile care nu pot fi eliminate, este posibil să fie necesar să reinstalați software-ul.

Pentru a dezinstala un patch:

1. Mergeți la **Rețea > Inventar patch-uri**.
2. Selectați patch-ul pe care doriți să îl dezinstalați. Pentru a căuta un anumit patch, folosiți filtrele disponibile în diferitele rubrici, cum ar fi numărul KB sau CVE. Utilizați rubrica **Eliminabil** pentru a afișa doar patch-urile care pot fi dezinstalate.

   Notă
   Patch-urile pot fi dezinstalate pe rând, pentru una sau mai multe stații de lucru.

3. Faceți clic pe butonul ⊗ **Dezinstalare** din partea de sus a tabelului. Se va afișa o fereastră de configurare, unde puteți edita detaliile sarcinii de dezinstalare.
   - **Nume sarcină**. Dacă doriți, puteți edita numele implicit al sarcinii de dezinstalare a patch-ului. Astfel, veți putea identifica mai ușor sarcina pe pagina **Sarcini**.
   - **Adăugare patch în lista patch-urilor ignorate**. În general, nu veți mai avea nevoie de un patch pe care doriți să îl dezinstalați. Această opțiune adaugă automat patch-ul în lista celor ignorate, după dezinstalare.
   - **Repornirea stațiilor de lucru după dezinstalarea patch-ului, dacă este necesar**. Această opțiune repornește stațiile de lucru imediat după dezinstalarea patch-ului, dacă sistemul trebuie repornit. Rețineți că această acțiune poate întrerupe activitatea utilizatorului.

Dacă lăsați această opțiune dezactivată, în cazul în care este necesară o repornire a sistemului pe mașinile de lucru țintă, acestea vor afișa pictograma de stare pentru repornire în curs în inventarul de rețea GravityZone. În acest caz, aveți următoarele opțiuni:

– Transmiteți o sarcină **Repornire mașină** stațiilor de lucru cu repornirea în curs în orice moment. Pentru mai multe detalii, vă rugăm consultați „Repornire sistem” (p. 100).

– Configurați politica activă pentru a informa utilizatorul stației de lucru că sistemul trebuie repornit. Pentru a face acest lucru, accesați politica activă de pe stația de lucru țintă, mergeți la **General > Notificări** și activați opțiunea **Notificare repornire stație de lucru**. În acest caz, utilizatorului i se va afișa un mesaj derulant de fiecare dată când este necesară o repornire a sistemului ca urmare a modificărilor efectuate de componentele GravityZone specificate (în acest caz, Administrarea patch-urilor). Fereastra derulantă include opțiunea de amânare a repornirii. Dacă utilizatorul alege să amâne repornirea, notificarea de repornire va apărea periodic pe ecran până când utilizatorul repornește sistemul sau până când expiră timpul setat de administratorul companiei.

  Pentru mai multe detalii, vă rugăm consultați „Notificare de repornire a stației de lucru” (p. 242).

- În tabelul **Ținte dezinstalare**, selectați stațiile de lucru de pe care doriți să dezinstalați patch-ul.

  Puteți selecta una sau mai multe stații de lucru din rețea. Utilizați filtrele disponibile pentru a localiza stația de lucru dorită.

  Notă
  Tabelul afișează doar stațiile de lucru pe care este instalat patch-ul selectat.

4. Efectuați clic pe **Confirmare**. Va fi creată o sarcină de **Dezinstalare patch**, care va fi transmisă către stațiile de lucru țintă.

   Va fi generat automat un raport **Dezinstalare patch** pentru fiecare sarcină de dezinstalare a patch-urilor finalizată, cu detalii referitoare la patch, la stațiile de lucru țintă și la starea sarcinii de dezinstalare a patch-ului.

Notă
După dezinstalarea unui patch, vă recomandăm să transmiteți o sarcină Scanare patch-uri către stațiile de lucru țintă. Această acțiune va actualiza informațiile patch-ului stocate în GravityZone pentru rețelele dvs. administrate.

6.6.6. Crearea statisticilor referitoare la patch-uri

Dacă aveți nevoie de detalii despre starea unui anumit patch pentru toate stațiile de lucru, utilizați funcția **Statistici patch**, care generează instantaneu un raport pentru patch-ul selectat:

1. În pagina **Inventar de patch-uri**, selectați patch-ul dorit din secțiunea din partea dreaptă.
2. Faceți clic pe butonul **Statistici patch** din partea de sus a tabelului.

   Se afișează un raport cu statisticile patch-urilor, care oferă detalii despre starea patch-urilor, inclusiv:

   - O diagramă, care arată procentajul patch-urilor instalate, eșuate, lipsă și în așteptare pentru stațiile de lucru care au raportat patch-ul respectiv.
   - Un tabel cu următoarele informații:
     - **Denumirea**, **FQDN**, **adresa IP** și **sistemul de operare** pentru fiecare stație de lucru care a raportat patch-ul.
     - **Data ultimei verificări**: momentul ultimei verificări a patch-ului pe stația de lucru.
     - **Stare patch**: instalat, eșuat, absent sau ignorat.

Notă
Funcționalitatea „Statistici patch” este disponibilă atât pentru patch-urile administrate, cât și pentru cele ignorate.

6.7. Vizualizarea și administrarea sarcinilor

Pagina **Rețea > Sarcini** vă permite să vizualizați și să gestionați toate sarcinile generate.

După ce ați generat o sarcină pentru unul sau mai multe obiecte din rețea, o puteți vizualiza în tabelul sarcinilor.

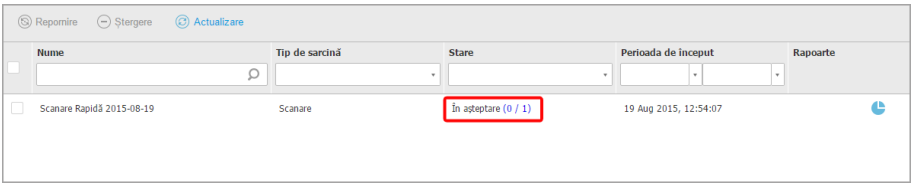
Puteți efectua următoarele operațiuni de pe pagina **Rețea > Sarcini**:

- Verificarea stării sarcinii
- Vizualizarea rapoartelor sarcinii
- Repornirea sarcinilor
- Oprește sarcinile de scanare Exchange
- Ștergere sarcini

6.7.1. Verificarea stării sarcinii

De fiecare dată când creați o sarcină pentru unul sau mai multe obiecte din rețea, trebuie să verificați progresul acesteia și să fiți informat în cazul apariției erorilor.

Mergeți la pagina **Rețea > Sarcini** și verificați coloana **Stare** pentru fiecare sarcină dorită. Puteți verifica starea sarcinii principale și puteți de asemenea să obțineți informații detaliate referitoare la fiecare sub-sarcină.



Pagina Sarcini

- **Verificarea stării sarcinii principale**.

  Sarcina principală se referă la acțiunile lansate asupra obiectelor din rețea (cum ar fi instalarea clientului sau scanare) și include o serie de sub-sarcini, una pentru fiecare obiect din rețea selectat. De exemplu, o sarcină de instalare principală creată pentru opt calculatoare include opt sub-sarcini. Numerele dintre paranteze reprezintă procentul de finalizare a sub-sarcinilor. De exemplu, (2/8) înseamnă că au fost finalizate două din opt sub-sarcini.

  Starea principală a sarcinii poate fi:
  - **În așteptare**, dacă nu a fost inițiată încă niciuna dintre sub-sarcini sau dacă numărul de instalări simultane a fost depășit. Numărul maxim de instalări simultane poate fi configurat din meniul **Configurare**. Pentru informații suplimentare, consultați Ghidul de instalare GravityZone.
  - **În curs**, dacă toate sub-categoriile rulează. Starea sarcinii principale rămâne În curs până la finalizarea ultimei sub-sarcini.
  - **Finalizat**, dacă toate sub-sarcinile au fost finalizate (cu sau fără succes). În cazul sub-sarcinilor finalizate cu succes, se afișează un simbol de avertizare.

- **Verificarea stării sub-sarcinilor**.

  Mergeți la sarcina dorită și faceți clic pe link-ul disponibil în coloana **Stare** pentru a deschide fereastra **Stare**. Puteți vizualiza o listă a obiectelor din rețea alocate sarcinii principale și starea sub-sarcinii aferente. Starea sub-sarcinii poate fi:

  – **În curs,** când sub-sarcina încă se execută.

    În plus, pentru sarcinile de scanare Exchange la cerere, puteți vizualiza, de asemenea, starea de finalizare.

  – **Finalizat**, dacă sub-sarcina a fost finalizată cu succes.

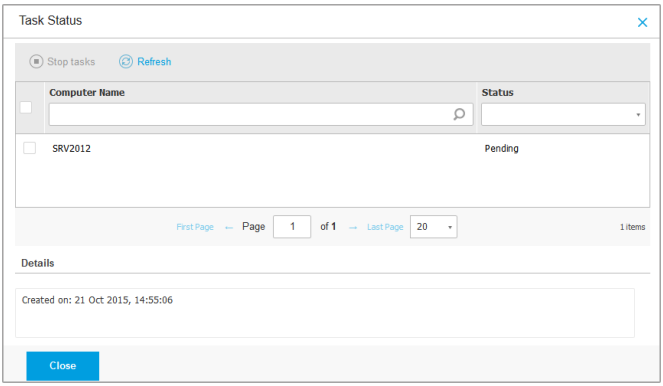
  – **În așteptare**, dacă sub-sarcina nu a început încă. Aceasta se poate întâmpla în următoarele situații:

    - Sub-sarcina este într-o coadă de așteptare.
    - Există probleme de conectivitate între Control Center și obiectul rețelei țintă.
    - Dispozitivul țintă este Inactiv (deconectat), în cazul dispozitivelor mobile. Sarcina va rula pe dispozitivul țintă imediat ce acesta revine online.

  – **Eșuată**, dacă sub-sarcina nu a putut fi inițiată sau a fost întreruptă din cauza erorilor, cum ar fi datele de autentificare și spațiul redus de memorie.

  – **Oprire**, când scanarea la cerere durează prea mult și ați optat pentru oprirea acesteia.

  Pentru a vizualiza detaliile fiecărei sub-sarcini, selectați-o și bidați secțiunea **Detalii** din partea de jos a tabelului.



Detalii privind starea sarcinilor

Veți obține informații referitoare la:

- Data și ora începerii sarcinii.
- Data și ora la care s-a încheiat sarcina.
- Descrierea erorilor întâlnite.

6.7.2. Vizualizarea rapoartelor referitoare la sarcină

Din pagina **Rețea > Sarcini** puteți opta pentru vizualizarea rapoartelor cu privire la sarcinile de scanare rapidă.

1. Mergeți la pagina **Rețea > Sarcini**.
2. Selectați obiectul de rețea dorit din selectorul de vederi.
3. Selectați caseta de bifare care corespunde sarcinilor de scanare care vă interesează.
4. Faceți clic pe butonul corespunzător din coloana **Rapoarte**. Așteptați până când se afișează raportul. Pentru mai multe informații, consultați capitolul „Utilizarea rapoartelor” (p. 475).

6.7.3. Repornire sarcini

Din diverse motive, este posibil ca sarcinile de instalare, dezinstalare sau actualizare a clientului să nu se finalizeze. Puteți alege să reporniți sarcinile nereușite în loc să creați unele noi, urmând acești pași:

1. Mergeți la pagina **Rețea > Sarcini**.
2. Selectați obiectul de rețea dorit din selectorul de vederi.
3. Selectați căsuțele corespunzătoare sarcinilor nereușite.
4. Faceți clic pe butonul **Repornire** din partea de sus a tabelului. Sarcinile selectate vor fi repornite, iar starea sarcinilor se va modifica în **Reîncercare**.

Notă
Pentru sarcinile cu sub-sarcini multiple, opțiunea **Repornire** este disponibilă numai atunci când toate sub-sarcinile s-au finalizat și va executa doar sub-sarcinile nereușite.

6.7.4. Se opresc sarcinile de scanare Exchange

Scanarea Bazei de date Exchange poate necesita un interval de timp considerabil. Dacă din orice motiv doriți să opriți o sarcină de scanare Exchange la cerere, urmați pașii descriși aici:

1. Mergeți la pagina **Rețea > Sarcini**.
2. Selectați modul de vizualizare a rețelei din selectorul de vederi.
3. Faceți clic în coloana **Stare** pentru a deschide fereastra **Stare sarcină**.
4. Bifați căsuța corespunzătoare subsarcinilor aflate în așteptare sau în curs pe care doriți să le opriți.
5. Faceți clic pe butonul **Oprire sarcini** din partea de sus a tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

Notă
De asemenea, puteți opri o sarcină de scanare la cerere a Bazei de date Exchange din zona de notificări a Bitdefender Endpoint Security Tools.

6.7.5. Ștergerea unei sarcini

GravityZone șterge automat sarcinile în așteptare, după două zile, și sarcinile finalizate, după 30 de zile. Dacă aveți în continuare multe sarcini, este recomandat să ștergeți sarcinile de care nu mai aveți nevoie pentru a evita aglomerarea listei.

1. Mergeți la pagina **Rețea > Sarcini**.
2. Selectați obiectul de rețea dorit din selectorul de vederi.
3. Selectați caseta de bifare care corespunde sarcinii pe care doriți să o ștergeți.

4. Faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

Avertisment
Ștergerea unei sarcini în curs va anula sarcina respectivă.
Dacă este ștearsă o sarcină în curs, orice sub-sarcini în așteptare vor fi anulate.
În acest caz, sub-sarcinile finalizate nu pot fi anulate.

6.8. Ștergerea stațiilor de lucru din inventarul rețelei

Inventarul rețelei conține în mod implicit directorul **Șterse** , destinat stocării stațiilor de lucru pe care nu doriți să le administrați.

Acțiunea **Ștergere** are următoarele efecte:

- Atunci când stațiile de lucru sunt șterse, acestea sunt mutate direct în directorul **Șterse**.
- Atunci când stațiile de lucru administrate sunt șterse:
  - Se creează o sarcină de dezinstalare a aplicației client
  - Se eliberează o unitate de licență
  - Stațiile de lucru sunt mutate în directorul **Șterse**

Pentru a șterge stațiile de lucru din inventarul rețelei:

1. Mergeți la pagina **Rețea**.
2. Selectați tipul de vedere a rețelei pe care îl doriți din selectorul de vederi.
3. Selectați **Grupuri personalizate** din fereastra din stânga. Toate stațiile de lucru disponibile în acest grup se afișează în tabelul din fereastra din dreapta.

Notă
Puteți șterge doar stațiile de lucru afișate în **Grupurile personalizate**, detectate în afara oricărei infrastructuri de rețea inegrate.

4. În fereastra din dreapta, bifați caseta aferentă stației de lucru pe care doriți să o ștergeți.
5. Faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

Dacă stația de lucru ștearsă este administrată, se va crea o sarcină de **Dezinstalare aplicație client** în pagina **Sarcini**, iar agentul de securitate este dezinstalat de pe stația de lucru, eliberând o unitate de licență.

6. Stația de lucru este mutată în directorul **Șterse**.

Puteți muta în orice moment stațiile de lucru din directorul **Șterse** în **Grupuri personalizate** prin glisare și lipire (drag-and-drop).

Notă

- Dacă doriți să excludeți permanent anumite stații de lucru de la administrare, trebuie să le păstrați în directorul **Șterse**.
- Dacă ștergeți stațiile de lucru din directorul **Șterse** folder, acestea vor fi șterse definitiv din baza de date GravityZone. Cu toate acestea, stațiile de lucru excluse care sunt online vor fi detectate la executarea următoarei sarcini de Descoperire rețea și vor apărea în Inventarul de rețea ca stații de lucru noi.

6.9. Configurarea setărilor de rețea

În pagina **Configurare > Setări rețea** puteți configura setările referitoare la Inventarul de rețea, cum ar fi: salvarea filtrelor, păstrarea ultimei locații accesate, crearea și administrarea regulilor programate pentru ștergerea mașinilor virtuale neutilizate.

Opțiunile sunt organizate în următoarele secțiuni:

- Setări inventar de rețea
- Ștergere mașini offline

6.9.1. Setări inventar de rețea

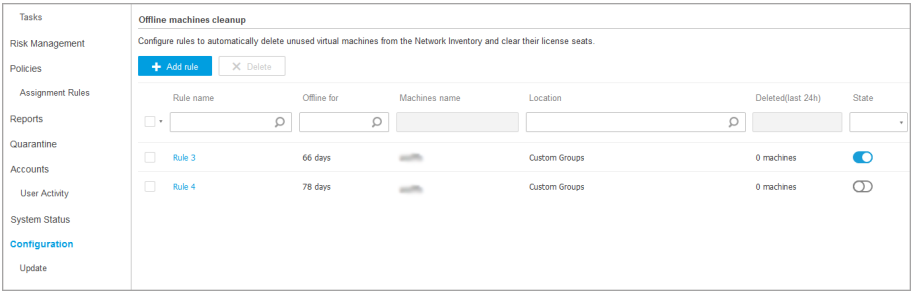
În secțiunea **Setări inventar de rețea** sunt disponibile următoarele opțiuni:

- **Salvare filtre pentru Inventarul de rețea**. Selectați această casetă pentru salvarea filtrelor dumneavoastră în pagina **Rețea** între sesiunile Control Center.
- **Reține ultima locație accesată din inventarul de rețea până la deconectare**. Selectați această casetă pentru a salva ultima locație pe care ați accesat-o la părăsirea paginii **Rețea**. Locația nu este salvată de la o sesiune la alta.
- **Evitați crearea duplicatelor endpoint-urilor clonate**. Selectați această opțiune pentru activarea unui nou tip de obiecte din rețea în GravityZone, numite obiecte de tip „golden image”. Astfel puteți diferenția între endpoint-urile sursă și clonele acestora. În plus, trebuie să marcați fiecare endpoint clonat după cum urmează:

1. Mergeți la pagina **Rețea**.
2. Selectați endpoint-ul pe care doriți să îl clonați.
3. Din meniul său contextual, selectați **Marcare ca obiect de tip „golden image”**.

6.9.2. Ștergere mașini offline

În secțiunea **Ștergere mașini offline** puteți programa reguli pentru ștergerea automată a mașinilor virtuale neutilizate din Inventarul de rețea.



Configurare - Setări rețea - Ștergere mașini offline

Creare reguli

Pentru a crea o regulă de ștergere:

1. În secțiunea **Ștergere mașini offline**, clic pe butonul **Adăugare regulă**.
2. În pagina de configurare:
   a. Introduceți numele regulii.
   b. Alegeți ora la care să fie efectuată ștergerea în fiecare zi.
   c. Definiți criteriile de ștergere:
      - Numărul zilelor în care mașinile au fost offline (de la 1 la 90).
      - Un model de nume, care poate fi aplicat unei singure mașini virtuale sau mai multor mașini virtuale.

        De exemplu, utilizați `machine_1` pentru a șterge mașinile cu acest nume. Ca alternativă, adăugați `machine_*` pentru a șterge toate mașinile al căror nume începe cu `machine_`.

Acest câmp este sensibil la litere mari și mici și acceptă doar litere, cifre și caracterele speciale asterisc (*), underscore (_) și cratimă (-). Numele nu poate începe cu asterisc (*).

d. Selectați grupurile vizate de endpoint-uri din Inventarul de rețea unde va fi aplicată regula.

3. Faceți clic pe **Save**.

Vizualizarea și administrarea regulilor

Secțiunea **Setări rețea > Ștergere mașini offline** afișează toate regulile pe care le-ați creat. Tabelul dedicat vă va oferi următoarele informații:

- Numele regulii.
- Numărul de zile de când mașinile sunt offline.
- Modelul de nume pentru mașini.
- Locația din Inventarul de rețea.
- Numărul de mașini șterse în ultimele 24 de ore.
- Stare: activat, dezactivat sau nevalid.

Notă
O regulă este nevalidă când mașinile vizate nu mai sunt valide, din cauza anumitor motive. Spre exemplu, dacă mașinile virtuale au fost șterse sau dacă dumneavoastră nu mai aveți acces la ele.

O regulă nouă este activată implicit. Puteți activa și dezactiva reguli oricând, utilizând butonul de Activare/Dezactivare din coloana **Stare**.

Dacă este nevoie, folosiți opțiunile de sortare și filtrare din partea de sus a tabelului pentru a găsi anumite reguli.

Pentru a modifica o regulă:

1. Clic pe numele regulii.
2. În pagina de configurare, modificați detaliile regulii.
3. Faceți clic pe **Save**.

Pentru a șterge una sau mai multe reguli:

1. Bifați căsuțele pentru a selecta mai multe reguli.

2. Efectuați clic pe butonul **Ștergere** din partea de sus a tabelului.

6.10. Configurarea setărilor Security Server

Serverele Security Server utilizează mecanismul propriu de introducere în memoria cache pentru eliminarea duplicării sarcinilor de scanare antimalware, optimizând acest proces. Un pas suplimentar privind optimizarea scanării este partajarea acestei memorii cache cu alte servere Security Server.

Partajarea memoriei cache funcționează numai între Security Server de același tip. Spre exemplu, Security Server Multi-platformă își va partaja memoria cache doar cu un alt Security Server Multi-platformă și nu cu un server Security Server pentru NSX.

Pentru activarea și configurarea partajării memoriei cache:

1. Accesați pagina **Configurare >Setări Security Server**.
2. Bifați caseta **Partajare memorie cache Security Server**.
3. Alegeți sfera de aplicare a partajării:
   - Toate serverele Security Server disponibile.

     Se recomandă utilizarea acestei opțiuni dacă toate serverele Security Server sunt în aceeași rețea.
   - Serverele Security Server disponibile în Lista de atribuire.

     Utilizați această opțiune când serverele Security Server sunt distribuite în rețele diferite și partajarea memoriei cache poate genera un volum mare de trafic.
4. În cazul limitării sferei de aplicare, creați un grup de servere Security Server. Selectați serverele Security Server din lista derulantă și alegeți **Adăugare**.

   Doar serverele Security Server din tabel își vor partaja memoria cache.

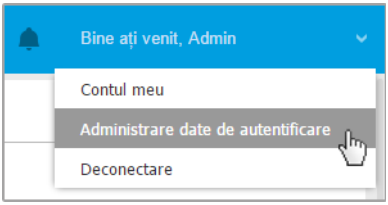
   Notă
   Serverele Security Server pentru NSX-T și NSX-V schimbă între ele informații din memoria cache doar în cadrul aceluiași server vCenter Server.

5. Faceți clic pe **Save**.

6.11. Manager Credențiale

Funcția Administrare date de autentificare vă ajută să definiți drepturile necesare pentru accesarea inventarelor vCenter Server existente, precum și să vă autentificați de la distanță pe diferite sisteme de operare din rețea.

Pentru a deschide fereastra Administrare date de autentificare, faceți clic pe numele de utilizator din colțul din dreapta sus al paginii și selectați **Administrare date de autentificare**.



Meniul Administrare date de autentificare

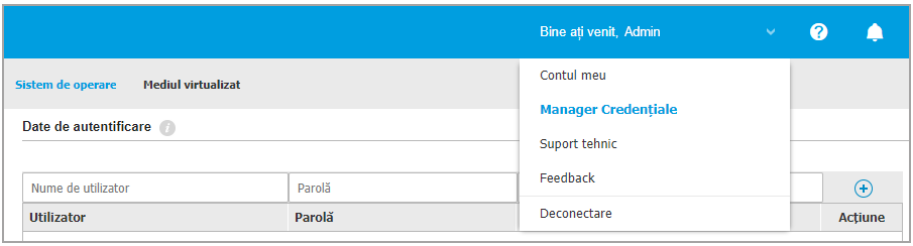
Fereastra **Administrare date de autentificare** include două secțiuni:

- Sistem de operare
- Mediul virtualizat

6.11.1. Sistem de operare

Din secțiunea **Sistem de operare**, puteți administra drepturile necesare pentru autentificarea de la distanță la executarea sarcinilor de instalare transmise calculatoarelor și mașinilor virtuale din rețea.

Pentru a adăuga un set de date de autentificare:



Manager Credențiale

1. Introduceți numele de utilizator și parola unui cont de administrator pentru fiecare sistem de operare țintă, în câmpurile corespunzătoare din partea de sus a capului de tabel. Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont. În cazul în care calculatoarele sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

   Folosiți convențiile Windows la introducerea denumirii contului de utilizator:

   - Pentru mașinile Active Directory folosiți următoarele sintaxe: `username@domain.com` și `domain\username`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`user@domain.comusername@domain.com` și `domain\userusername`).
   - Pentru mașinile din grupul de lucru, e suficient să introduceți numai numele de utilizator, fără numele grupului de lucru.

2. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului. Noul set de date de autentificare este adăugat la tabel.

   Notă
   Dacă nu ați specificat datele de autentificare, vi se va solicita să le introduceți atunci când executați sarcinile de instalare. Datele specificate sunt salvate automat în secțiunea Administrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

6.11.2. Mediul virtualizat

Din fereastra Mediul virtual puteți administra drepturile de autentificare pentru sistemele de server virtualizat disponibile.

Pentru a accesa infrastructura virtualizată integrată cu Control Center, trebuie să introduceți datele de utilizator pentru fiecare sistem de server virtualizat. Control Center folosește datele dumneavoastră pentru a se conecta la infrastructura virtualizată, afișând doar resursele la care aveți acces (așa cum sunt acestea definite în serverul virtual).

Pentru a specifica datele de autentificare necesare pentru conectarea la un server virtual:

1. Selectați serverul din meniul corespunzător.

Notă
Dacă meniul nu este disponibil, fie nu s-a configurat încă nicio integrare, fie toate datele au fost deja configurate.

2. Introduceți numele de utilizator și parola și o descriere sugestivă.
3. Faceți clic pe butonul ⊕ **Adăugare**. Noul set de date de autentificare este adăugat la tabel.

Notă
Dacă nu configurați datele de autentificare în fereastra Administrare date de autentificare, va trebui să le introduceți când încercați să parcurgeți inventarul oricărui sistem de server virtual. După ce ați introdus datele, acestea sunt salvate în secțiunea Admnistrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

Important
Ori ce câte ori modificați parola de utilizator pentru serverul virtual, nu uitați să o și actualizați în fereastra Administrare date de autentificare.

6.11.3. Ștergerea datelor din fereastra Administrare Date de Autentificare

Pentru a șterge datele de autentificare care nu mai sunt valabile din fereastra Administrare date de autentificare:

1. Îndreptați cursorul către rândul din tabel care include datele pe care doriți să le ștergeți.
2. Faceți clic pe butonul ⊗ **Ștergere** din dreapta rândului corespunzător din tabel. Contul selectat va fi șters.

7. POLITICI DE SECURITATE

Odată instalată, protecția Bitdefender poate fi configurată și administrată din Control Center utilizând politicile de securitate. O politică specifică setările de securitate care vor fi aplicate pe obiectele inventarului rețelei (calculatoare, mașini virtuale sau dispozitive mobile).

Imediat după instalare, politica implicită este alocată obiectelor din rețea, această politică fiind preconfigurată cu setările recomandate de protecție. Dacă integrarea NSX este activată, alte trei politici de securitate implicite sunt disponibile pentru NSX, câte una pentru fiecare nivel de securitate: permisiv, normal și agresiv. Aceste politici sunt preconfigurate cu setările de protecție recomandate. Politicile implicite nu pot fi modificate sau șterse.

Puteți crea oricâte politici doriți pe baza cerințelor de securitate, pentru fiecare tip de obiect din rețea administrat.

Iată ce trebuie să știți despre politici:

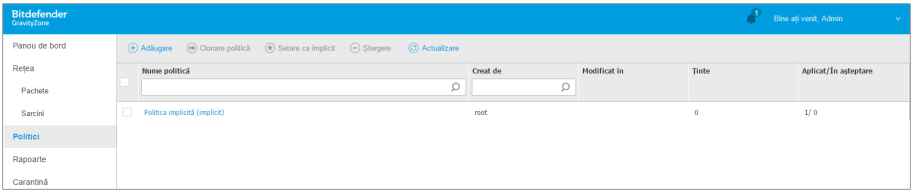
- Politicile sunt create în pagina **Politici** și atribuite obiectelor de rețea din pagina **Rețea**.
- Politicile pot prelua mai multe setări ale modulelor de la alte politici.
- Puteți configura atribuirea politicilor către stațiile de lucru astfel încât o politică să poată fi aplicată numai în anumite condiții, în funcție de locație sau de utilizatorul autentificat. Prin urmare, o stație de lucru poate avea mai multe politici atribuite.
- Stațiile de lucru nu pot avea mai multe politici active simultan.
- Puteți aloca o politică stațiilor de lucru individuale sau grupurilor de stații de lucru. La alocarea unei politici, veți defini de asemenea și opțiunile de moștenire ale politicii respective. În mod implicit, fiecare stație de lucru preia politica grupului mamă.
- Politicile sunt expediate către obiectele țintă din rețea imediat după crearea sau modificarea acestora. Setările trebuie aplicate obiectelor din rețea în mai puțin de un minut (cu condiția ca acestea să fie online). Dacă un obiect din rețea nu este online, setările vor fi aplicate imediat ce obiectul revine online.
- Politica se aplică exclusiv pentru modulele de protecție instalate.
- Pagina **Politici** afișează exclusiv următoarele tipuri de politici:
  - Politicile create de dvs.
  - Alte politici (cum ar fi politica implicită sau șabloanele create de alți utilizatori) alocate stațiilor de lucru din contul dvs.

- Nu puteți edita politicile create de alți utilizatori (cu excepția cazului în care autorii politicilor permit acest lucru din setări), însă le puteți suprascrie prin aplicarea unei alte politici obiectelor țintă.

Avertisment
Stațiilor țintă li se vor aplica doar modulele de politică acceptate.
Vă rugăm rețineți că pentru sistemele de operare pentru servere este acceptat doar modulul împotriva programelor periculoase.

7.1. Administrarea politicilor

Politicile pot fi vizualizate și administrate pe pagina **Politici**.



Pagina Politici

Fiecare tip de stație de lucru are anumite setări de politică. Pentru administrarea politicilor, trebuie să selectați mai întâi tipul de stație de lucru din rețea (**Calculatoare și Mașini virtuale** sau **Dispozitive mobile**) din selectorul de vederi.

Politicile existente sunt afișate în tabel. Pentru fiecare politică puteți vedea:

- Nume politică.
- Utilizatorul care a creat politica.
- Data și ora ultimei modificări a politicii.
- Numărul de destinatari către care a fost trimisă politica.*
- Numărul de obiective pentru care s-a aplicat/este în așteptare politica.*

Pentru politicile cu modulul NSX activat, sunt disponibile informații suplimentare:

- Denumirea politicii NSX, utilizată pentru identificarea politicii Bitdefender în VMware vSphere.

- Vizibilitatea politicii în consolele de administrare, care vă permit să filtrați politicile pentru NSX. Astfel, dacă politicile **Local** sunt vizibile doar în Bitdefender Control Center, politicile **Globale** sunt vizibile în VMware NSX.

Detaliile sunt ascunse implicit.

Pentru a personaliza detaliile politicii afișată în tabel:

1. Faceți clic pe butonul **Coloane** din partea dreaptă a Barei de instrumente Acțiuni.
2. Selectați coloanele pe care doriți să le vizualizați.
3. Faceți clic pe butonul **Resetare** pentru a reveni la vizualizare implicită coloane.

* Dacă faceți clic pe număr, veți fi direcționat către pagina **Rețea**, de unde puteți vizualiza terminalele corespunzătoare. Vi se va solicita să selectați modul de vizualizare rețea. Această acțiune va crea un filtru folosind criteriile politicii.

Puteți sorta politicile existente și căuta anumite politici folosind criteriile disponibile.

7.1.1. Crearea politicilor

Puteți crea politici fie prin adăugarea unei politici noi, fie prin duplicarea (clonarea) unei politici existente.

Pentru a crea o politică de securitate:

1. Mergeți la pagina **Politici**.
2. Selectați tipul de stație de lucru dorit din selectorul de vederi.
3. Selectați metoda de creare a politicii:
   - **Adăugare politică nouă**.
     - Dați clic pe butonul **Adăugare** situat în partea de sus a tabelului. Această comandă generează o politică nouă pornind de la modelul politicii implicite.
   - **Clonarea unei politici existente**.
     a. Selectați caseta de bifare a politicii pe care doriți să o duplicați.
     b. Faceți clic pe butonul **Clonare** din partea de sus a tabelului.
4. Configurați setările politicii. Pentru informații detaliate, consultați:
   - „Politici referitoare la calculatoare și mașini virtuale” (p. 235)
   - „Politici pentru dispozitive mobile” (p. 392)

5. Faceți clic pe **Salvare** pentru a genera politica și a reveni la lista politicilor.

Când definiți politicile care doriți să fie utilizate în VMware NSX, pe lângă configurarea setărilor protecției antimalware în GravityZone Control Center, trebuie să creați și o politică în NSX, prin care solicitați utilizarea GravityZone ca profil de serviciu. Pentru a crea o politică de securitate NSX:

1. Conectați-vă la vSphere Web Client.
2. Mergeți la secțiunea **Securitate & rețea > Structură servicii > Politici de securitate**.
3. Faceți clic pe butonul **Creare politică de securitate** din bara de instrumente din partea de sus a tabelului politicilor. Este afișată fereastra de configurare.
4. Introduceți denumirea politicii și apoi faceți clic pe **Următorul**.

   Opțional, puteți adăuga și o descriere scurtă.
5. Faceți clic pe butonul **Adăugare serviciu Guest Introspection** din partea de sus a tabelului. Se afișează fereastra serviciului Guest Introspection.
6. Introduceți denumirea și descrierea serviciului.
7. Lăsați acțiunea implicită selectată pentru a permite aplicarea profilului de servicii Bitdefender pentru grupul de securitate.
8. Din meniul **Denumire serviciu**, selectați **Bitdefender**.
9. Din meniul **Profil servicii**, selectați o politică de securitate GravityZone existentă.
10. Lăsați valorile implicite pentru opțiunile **Stare** și **Aplicare**.

> **Notă**
> Pentru mai multe informații privind setările politicii de securitate, consultați documentația VMware NSX.

11. Faceți clic pe **OK** pentru a adăuga serviciul.
12. Faceți clic pe **Următorul** până ajungeți la ultimul pas și apoi faceți clic pe **Terminare**.

7.1.2. Atribuirea unei politici

Inițial, stațiilor de lucru le este atribuită politica implicită. Odată ce ați definit politicile necesare în pagina **Politici**, le puteți atribui stațiilor de lucru.

Procedura de alocare a politicii este asociatp diferitelor medii cu care se integrează GravityZone. Pentru anumite integrări, cum ar fi VMware NSX, politicile sunt accesibile din exteriorul GravityZone Control Center. Sunt asociate și politicilor externe.

Alocarea politicilor locale

Există două modalități de alocare a politicilor locale:

- Atribuire pe bază de dispozitiv, care înseamnă că selectați manual stațiile de lucru cărora doriți să le alocați politicile. Aceste politici sunt cunoscute sub denumirea de politici pentru dispozitive.
- Atribuire pe bază de reguli, care înseamnă că o politică este atribuită unei stații de lucru administrate dacă setările de rețea ale stației de lucru respectă condițiile regulii de atribuire existente.

Notă

- Puteți atribui numai politici create de dumneavoastră. Pentru a atribui o politică creată de alt utilizator, trebuie prima dată să o clonați în pagina **Politici**.
- Pe mașinile virtuale protejate individual de HVI, puteți atribui numai politici pentru dispozitive. Atunci când pe acestea este instalat și Bitdefender Endpoint Security Tools, puteți atribui și politici pe bază de reguli, agentul de securitate ocupându-se de activarea politicilor.

  Notă
  Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Atribuirea politicilor pentru dispozitive

Prin intermediul GravityZone, puteți aloca politici în mai multe modalități:

- Alocare politică direct la țintă.
- Alocarea politicii grupului părinte prin moștenire.
- Moștenire forțată a politicii de către țintă.

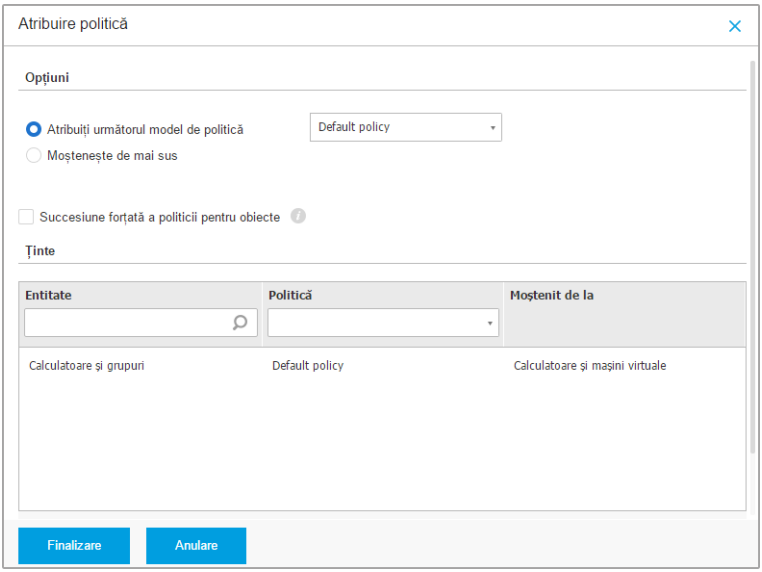
În mod implicit, fiecare stație de lucru sau grup de stații de lucru preia politica grupului mamă. În cazul în care modificați politica grupului mamă, toți descendenții vor fi afectați, cu excepția celor care au o politică în vigoare.

Pentru a atribui o politică pentru dispozitive:

1. Mergeți la pagina **Rețea**.
2. Selectați tipul de vizualizare a rețelei folosind selectorul de vizualizări .
3. Selectați stațiile de lucru vizate. Puteți selecta una sau mai multe stații de lucru sau grupuri de stații de lucru.

   Din motive ce țin de preluarea setărilor, nu puteți modifica politica implicită a grupului rădăcină. De exemplu, pentru **Computer și mașini virtuale** se va atribui întotdeauna **Politica implicită**.
4. Faceți clic pe butonul **Alocare politică** din partea superioară a tabelului sau selectați opțiunea **Alocare politică** din meniul contextual.

   Este afișată pagina **Atribuire politică**:



Setări atribuire politică

5. Verificați tabelul cu stațiile de lucru țintă. Pentru fiecare stație de lucru, puteți vizualiza:
   - Politica atribuită.

- Grupul părinte de la care ținta preia politica, dacă este cazul.

  În cazul în care grupul aplică politica, puteți face clic pe denumirea sa pentru a vizualiza pagina **Alocare politică**, acest grup fiind ținta.

- Starea de aplicare.

  Această stare indică dacă ținta forțează moștenirea politicii sau dacă este forțată să moștenească politica.

  Observați țintele cu politică aplicată (stare **Este forțat**). Politicile lor nu pot fi înlocuite. Într-un asfel de caz, este afișat un mesaj de avertizare.

6. În cazul apariției unui mesaj de avertizare, faceți clic pe linkul **Excludeți aceste ținte** pentru a continua.
7. Selectați una dintre opțiunile disponibile pentru alocarea politicii:
   - **Alocarea modelului următor de politică** - pentru a aloca direct o anumită politică stațiilor de lucru țintă.
   - **Moștenire de mai sus** - pentru a utiliza politica grupului mamă.
8. Dacă alegeți să alocați un model de politică:
   a. Selectați politica din lista derulantă.
   b. Selectați **Forțare moștenire politică pentru grupurile copil** pentru a obține următoarele:
      - Alocați politica tuturor descendenților grupurilor țintă, fără nicio excepție.
      - Împiedicarea modificării acesteia din alt loc inferior în ierarhie.

      Este afișat un nou tabel care afișează în mod recurent toate endpoint-urile și grupurile de endpoint-uri afectate, împreună cu politicile care vor fi înlocuite.
9. Faceți click pe **Terminare** pentru a salva și a aplica modificările. Altfel, faceți clic pe **Înapoi** sau **Anulare** pentru a reveni la pagina anterioară.

La finalizare, politicile sunt expediate imediat către stațiile de lucru țintă. Setările ar trebui aplicate pe stațiile de lucru în mai puțin de un minut (cu condiția ca acestea să fie online). Dacă o stație de lucru nu este online, setările vor fi aplicate de îndată ce stația de lucru revine online.

Pentru a verifica dacă politica a fost alocată cu succes:

1. În pagina **Rețea**, faceți clic pe denumirea stației de lucru care vă interesează. Control Center va afișa fereastra **Informații**.
2. Verificați secțiunea **Politică** pentru a vizualiza starea politicii curente. Trebuie să indice **Aplicat**.

O altă metodă de verificare a stării de atribuire se referă la detaliile politicii:

1. Mergeți la pagina **Politici**.
2. Găsiți politica pe care ați atribuit-o.

   În coloana **Activă/Aplicată/În așteptare**, puteți vedea numărul de endpoint-uri pentru fiecare dintre cele trei statusuri.
3. Selectați orice număr pentru a vizualiza lista de endpoint-uri cu statusul respectiv în pagina **Rețea**.

Atribuirea politicilor pe bază de reguli

Pagina **Politici > Reguli de atribuire** vă permite să definiți politici în funcție de utilizator și locație. De exemplu, puteți aplica reguli de firewall mai restrictive atunci când utilizatorii se conectează la internet din afara companiei sau puteți activa funcția de Control acces web pentru utilizatorii care nu fac parte din grupul de administratori.

Iată ce trebuie să știți despre regulile de atribuire:

- Stațiile de lucru nu pot avea mai multe politici active simultan.
- O politică aplicată prin intermediul unei reguli va suprascrie politica dispozitivului setată pentru stația de lucru.
- Dacă niciuna dintre regulile de atribuire nu este aplicabilă, atunci se aplică politica privind dispozitivul.
- Regulile sunt ordonate și procesate în funcție de prioritate, unde 1 reprezintă prioritatea cea mai mare. Puteți avea mai multe reguli pentru aceeași țintă. În acest caz, se va aplica prima regulă care respectă setările de conexiune active pe stația de lucru țintă.

  De exemplu, dacă o stație de lucru corespunde unei reguli privind utilizatorul cu prioritatea 4 și unei reguli privind locația cu prioritatea 3, se va aplica regula privind locația.

Avertisment
La crearea regulilor, asigurați-vă că luați în considerare setările sensibile, cum ar fi excepțiile, detaliile de comunicare sau proxy.
Ca cea mai bună practică, se recomandă să utilizați funcția de preluare a politicilor pentru a păstra setările critice ale politicii dispozitivelor și în politica folosită de regulile de atribuire.

Pentru a crea o nouă regulă:

1. Mergeți la pagina **Reguli de atribuire**.
2. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului.
3. Selectați tipul de regulă:
   - Regulă locație
   - Regulă utilizator
   - Regulă pentru etichete
4. Configurați setările regulii după cum este nevoie.
5. Faceți clic pe **Salvare** pentru a salva modificările și pentru a aplica regula pe stațiile de lucru țintă ale politicii.

Pentru a modifica setările unei reguli existente:

1. În pagina **Reguli de atribuire**, găsiți regula dorită și faceți clic pe denumire pentru a o edita.
2. Configurați setările regulii după cum este nevoie.
3. Faceți clic pe **Salvare** pentru a aplica modificările și închide fereastra. Pentru a ieși din fereastră fără a salva modificările, faceți clic pe **Anulare**.

Dacă nu doriți să mai folosiți o anumită regulă, selectați-o și faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

Pentru a vă asigura că sunt afișate cele mai recente informații, faceți clic pe butonul ⟲ **Reîmprospătare** din partea de sus a tabelului.

Configurarea regulilor privind locația

O locație reprezintă un segment de rețea identificat printr-una sau mai multe setări de rețea, cum ar fi un anumit gateway, un anumit DNS utilizat pentru soluționarea

URL-urilor sau un subset de IP-uri. De exemplu, puteți defini locații precum rețeaua LAN a companiei, ferma de servere sau un departament.

În fereastra de configurare a regulilor, urmați acești pași:

1. Introduceți o denumire sugestivă și o descriere pentru regula pe care doriți să o creați.
2. Setați prioritatea regulii. Regulile sunt ordonate în funcție de prioritate, prima regulă având cea mai mare prioritate. Aceeași prioritate nu poate fi setată de două sau mai multe ori.
3. Selectați politica pentru care creați regula de atribuire.
4. Definiți locațiile pentru care se aplică regula.
   a. Selectați tipul setărilor de rețea din meniul din partea de sus a tabelului Locații. Tipurile disponibile sunt următoarele:

Tip	Valoare
IP/Domeniu de adresă IP	Adrese IP specifice într-o rețea sau o subrețea. Pentru subrețele, folosiți formatul CIDR. De exemplu: `10.10.0.12` sau `10.10.0.0/16`
Adresă Gateway	Adresa IP a gateway-ului
Adresă server WINS	Adresa IP a serverului WINS **Important** Această opțiune nu se aplică pe sistemele Linux și Mac.
Adresă server DNS	Adresa IP a serverului DNS
Sufix DNS pentru conexiunea DHCP	Denumirea DNS fără numele gazdei pentru o anumită conexiune DHCP De exemplu: `hq.company.biz`
Stația de lucru poate soluționa gazda.	Numele gazdei. De exemplu: `fileserv.company.biz`
Stația de lucru se poate conecta la GravityZone	Da/Nu

Tip	Valoare
Tip rețea	Wireless/Ethernet Atunci când selectați opțiunea Wireless, puteți adăuga și numele SSID al rețelei. **Important** Această opțiune nu se aplică pe sistemele Linux și Mac.

Nume gazdă	Nume gazdă
	De exemplu: `cmp.bitdefender.com`
	Important
	Puteți folosi și metacaractere. Asteriscul (*) înlocuiește zero sau mai multe caractere, iar semnul întrebării (?) înlocuiește exact un caracter. Exemple:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

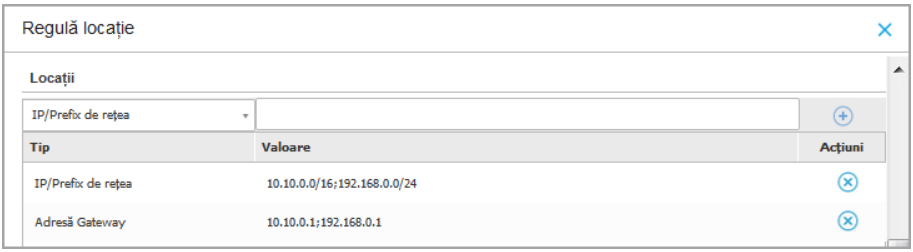
b. Introduceți valoarea pentru tipul selectat. Dacă este cazul, puteți introduce mai multe valori în câmpul dedicat, separate prin punct și virgulă (;) și fără spații suplimentare. De exemplu, atunci când introduceți `10.10.0.0/16;192.168.0.0/24`, regula se aplică pentru orice stație de lucru cu un IP ce corespunde oricăreia dintre aceste subrețele.

Avertisment
Puteți utiliza un singur tip de setare de rețea pentru o regulă privind locația. De exemplu, dacă ați introdus o locație folosind **IP-ul/prefixul de rețea**, nu puteți reutiliza această setare în cadrul aceleiași reguli.

c. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului.

Setările de rețea ale stațiilor de lucru trebuie să se potrivească cu TOATE locațiile furnizate pentru ca regula să se aplice în cazul lor. De exemplu, pentru a identifica rețeaua LAN de la birou puteți introduce gateway-ul, tipul de rețea și

DNS; în plus, dacă adăugați o subrețea, puteți identifica un departament în cadrul rețelei LAN a companiei.



Regulă locație

Faceți clic pe câmpul **Valoare** pentru a edita criteriile existente și apoi faceți clic pe `Enter` pentru salvarea moificărilor.

Pentru a șterge o locație, selectați-o și faceți clic pe butonul ⊗ **Ștergere**.

5. Puteți opta pentru excluderea anumitor locații din regulă. Pentru a crea o excepție, definiți locațiile ce urmează a constitui excepția de la regulă:

   a. Bifați caseta **Excepții** de sub tabelul Locații.

   b. Selectați tipul setărilor de rețea din meniul din partea de sus a tabelului Excepții. Pentru mai multe informații despre opțiuni, consultați „Configurarea regulilor privind locația” (p. 228).

   c. Introduceți valoarea pentru tipul selectat. Puteți introduce mai multe valori în câmpul dedicat, separate prin punct și virgulă (;) și fără spații suplimentare.

   d. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului.

   Setările de rețea ale stațiilor de lucru trebuie să respecte TOATE condițiile prevăzute în tabelul Excepții, pentru ca excepția să fie aplicată.

   Faceți clic pe câmpul **Valoare** pentru a edita criteriile existente și apoi faceți clic pe `Enter` pentru salvarea moificărilor.

   Pentru a șterge o excepție, faceți clic pe butonul ⊗ **Ștergere** din partea dreaptă a tabelului.

6. Efectuați clic pe **Salvare** pentru a salva regula de atribuire și aplicați-o.

   Odată creată, regula privind locația se aplică automat pe toate stațiile de lucru țintă care sunt administrate.

Configurarea regulilor privind utilizatorul

Important

- Puteți crea reguli în funcție de utilizator numai dacă integrarea Active Directory este disponibilă.
- Puteți defini roluri de utilizator numai pentru utilizatorii și grupurile Active Directory. Regulile bazate pe grupurile Active Directory nu sunt suportate pe sistemele Linux.

În fereastra de configurare a regulilor, urmați acești pași:

1. Introduceți o denumire sugestivă și o descriere pentru regula pe care doriți să o creați.
2. Setați prioritatea. Regulile sunt ordonate în funcție de prioritate, prima regulă având cea mai mare prioritate. Aceeași prioritate nu poate fi setată de două sau mai multe ori.
3. Selectați politica pentru care creați regula de atribuire.
4. În secțiunea **Ținte**, selectați utilizatorii și grupurile de securitate pentru care doriți să se aplice regula politicii. Puteți vizualiza selecția dumneavoastră în tabelul din partea dreaptă.
5. Faceți clic pe **Save**.

   Odată creată, regula în funcție de utilizator se aplică pentru toate stațiile de lucru administrate în momentul autentificării utilizatorului.

Configurarea regulilor etichetelor

Important

Puteți crea reguli pentru etichete doar dacă este disponibilă o integrare cu Amazon EC2 sau cu Microsoft Azure.

Puteți utiliza etichetele definite în infrastructurile cloud pentru a atribui o anumită politică GravityZone mașinilor virtuale găzduite în cloud. Pentru toate mașinile virtuale cu etichetele specificate într-o regulă pentru etichete se va aplica politica instituită de regulă.

Notă

Potrivit infrastructurii cloud, puteți defini etichetele mașinii virtuale după cum urmează:

- Pentru Amazon EC2: în fila **Etichete** a instanței EC2.

- Pentru Microsoft Azure: în secțiunea **Vedere de ansamblu** a mașinii virtuale.

O regulă pentru etichete poate include una sau mai multe etichete. Pentru a crea o regulă pentru etichete:

1. Introduceți o denumire sugestivă și o descriere pentru regula pe care doriți să o creați.
2. Setați prioritatea regulii. Regulile sunt ordonate în funcție de prioritate, prima regulă având cea mai mare prioritate. Aceeași prioritate nu poate fi setată de două sau mai multe ori.
3. Selectați politica pentru care doriți să creați regula etichetelor.
4. În tabelul **Etichetă**, adăugați una sau mai multe etichete.

   O etichetă este formată dintr-o pereche de valori cheie sensibilă la litere mari/mici. Asigurați-vă că introduceți etichetele așa cum sunt definite acestea în infrastructura cloud. Doar perechile de valori cheie valabile vor fi luate în considerare.

   Pentru a adăuga o etichetă:

   a. În câmpul **Cheie etichetă**, introduceți numele cheii.

   b. În câmpul **Valoare etichetă**, introduceți numele valorii.

   c. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului.

Alocarea politicilor NSX

În NSX, politicile de securitate sunt alocate grupurilor de securitate. Un grup de securitate poate include diferite obiecte vCenter, cum ar fi centrele de date, clusterele și mașinile virtuale.

Pentru a aloca o politică de securitate unui grup de securitate:

1. Conectați-vă la vSphere Web Client.
2. Mergeți la secțiunea **Securitate & rețea > Structură servicii** și faceți clic pe **Grupuri de securitate**.
3. Creați numărul dorit de grupuri de securitate. Pentru informații suplimentare, consultați Documentația VMware.

   Puteți crea grupuri de securitate dinamice, pe baza etichetelor de securitate. Astfel, puteți grupa toate mașinile virtuale pe care le identificați ca fiind infestate.

4. Faceți clic dreapta pe grupul de securitate care vă interesează și apăsați pe **Aplicare politică**.
5. Selectați politica pe care doriți să o aplicați și faceți clic pe **OK**.

7.1.3. Modificarea setărilor politicii

Setările politicilor pot fi configurate inițial la crearea politicii. Acestea pot fi ulterior modificate după caz, în orice moment.

Notă
În mod implicit, numai utilizatorul care a creat politica o poate modifica. Pentru a schimba această setare, deținătorul politicii trebuie să bifeze opțiunea **Permite altor utilizatori să modifice această politică** din pagina **Detalii** a politicii.

Pentru a modifica setările unei politici existente:

1. Mergeți la pagina **Politici**.
2. Selectați tipul de stație de lucru dorit din selectorul de vederi.
3. Identificați politica dorită în listă și faceți clic pe denumirea acesteia pentru a o edita.
4. Configurați setările politicii după caz. Pentru informații detaliate, consultați:
   - „Politici referitoare la calculatoare și mașini virtuale” (p. 235)
   - „Politici pentru dispozitive mobile” (p. 392)
5. Faceți clic pe **Save**.

   Politicile expediate către obiectele țintă ale rețelei imediat după realocare sau după modificarea setărilor politicii. Setările trebuie aplicate pe obiectele din rețea în mai puțin de un minut (cu condiția ca acestea să fie online). Dacă un obiect din rețea nu este online, setările vor fi aplicate imediat ce obiectul revine online.

7.1.4. Redenumirea politicilor

Politicile trebuie să aibă denumiri sugestive, astfel încât dumneavoastră sau un alt administrator să le puteți identifica rapid.

Pentru a redenumi o politică:

1. Mergeți la pagina **Politici**.

2. Selectați tipul de stație de lucru dorit din selectorul de vederi.
3. Faceți clic pe denumirea politicii. Aceasta va deschide pagina politicii.
4. Introduceți o nouă denumire a politicii.
5. Faceți clic pe **Save**.

Notă
Denumirea politicii este unică. Trebuie să introduceți o denumire diferită pentru fiecare politică nouă.

7.1.5. Ștergerea politicilor

Dacă nu mai aveți nevoie de o politică, ștergeți-o. După ce ați șters o politică, obiectelor de rețea pentru care se aplica aceasta li se va aloca politica grupului mamă. Dacă nu se aplică nicio altă politică, în final, va fi activată cea implicită. La ștergerea unei politici cu secțiuni preluate de alte politici, setările secțiunilor moștenite sunt salvate în politicile subordonate.

Notă
În mod implicit, numai utilizatorul care a creat politica o poate șterge. Pentru a schimba această setare, deținătorul politicii trebuie să bifeze opțiunea **Permite altor utilizatori să modifice această politică** din pagina **Detalii** a politicii.

Pentru a putea șterge o politică NSX din GravityZone Control Center, trebuie să vă asigurați că aceasta nu este utilizată. Prin urmare, trebuie să alocați un alt profil de securitate grupului de securitate țintă. Pentru mai multe informații, consultați capitolul „Alocarea politicilor NSX” (p. 233).

Pentru a șterge o politică:

1. Mergeți la pagina **Politici**.
2. Selectați tipul de stație de lucru dorit din selectorul de vederi.
3. Selectați caseta de bifare a politicii pe care doriți să o ștergeți.
4. Faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

7.2. Politici referitoare la calculatoare și mașini virtuale

Setările politicilor pot fi configurate inițial la crearea politicii. Acestea pot fi ulterior modificate după caz, în orice moment.

Pentru a configura setările unei politici:

1. Mergeți la pagina **Politici**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Faceți clic pe denumirea politicii. Aceasta va deschide pagina de setări ale politicii.
4. Configurați setările politicii după caz. Setările sunt organizate în următoarele secțiuni:
   - General
   - HVI
   - Antimalware
   - Sandbox Analyzer
   - Firewall
   - Protecție rețea
   - Administrarea patch-urilor
   - Application Control
   - Device Control
   - Relay
   - Protecție Exchange
   - Criptare
   - NSX
   - Protecție spațiu de stocare
   - Senzor de incidente

   Navigați prin secțiuni folosind meniul din partea stângă a paginii.
5. Faceți clic pe **Salvare** pentru a salva modificările și a le aplica la calculatoarele țintă. Pentru a părăsi pagina de politici fără a salva modificările, faceți clic pe **Anulare**.

Notă
Pentru a învăța modul de lucru cu politicile, consultați „Administrarea politicilor” (p. 221).

7.2.1. General

Setările generale vă ajute să administrați opțiunile de afișare a interfeței cu utilizatorul, protecția prin parolă, setările proxy, setările pentru utilizatori privilegiați, opțiunile de comunicare și preferințele de actualizare pentru stațiile de lucru țintă.

Setările sunt organizate în următoarele secțiuni:

- Detalii
- Notificări
- Setări
- Comunicații
- Actualizare

Detalii

Pagina **Detalii** include detalii generale privind politica:

- Nume politică
- Utilizatorul care a creat politica
- Data și ora când a fost creată politica
- Data și ora când a fost modificată politica ultima dată

Politici referitoare la calculatoare și mașini virtuale

Puteți redenumi politica introducând noua denumire în câmpul corespunzător și făcând clic pe butonul **Salvare** din partea de jos a paginii. Politicile trebuie să aibă denumiri sugestive, astfel încât dumneavoastră sau un alt administrator să le puteți identifica rapid.

Notă
În mod implicit, numai utilizatorul care a creat politica o poate modifica. Pentru a schimba această setare, deținătorul politicii trebuie să bifeze opțiunea **Permite altor utilizatori să modifice această politică** din pagina **Detalii** a politicii.

Reguli de preluare

Puteți seta secțiunile ce urmează a fi preluate de la alte politici. Pentru a face acest lucru:

1. Selectați modulul și secțiunea care doriți să fie preluate de politica existentă. Toate secțiunile pot fi preluate, cu excepția **General > Detalii**.
2. Specificați politica de la care doriți să preluați secțiunea.
3. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului.

Dacă se șterge o politică sursă, preluarea se întrerupe, iar setările secțiunilor preluate sunt salvate în politica subordonată.

Secțiunile preluate nu pot fi preluate mai departe de alte politici. Luați în considerare următorul exemplu:

Politica A preia secțiunea **Antimalware > La cerere** de la politica B. Politica C nu poate prelua secțiunea **Antimalware > La cerere** de la politica A.

Informații privind asistența

Puteți personaliza informațiile privind asistența tehnică și datele de contact disponibile în fereastra **Despre** a agentului de securitate prin completarea câmpurilor corespunzătoare.

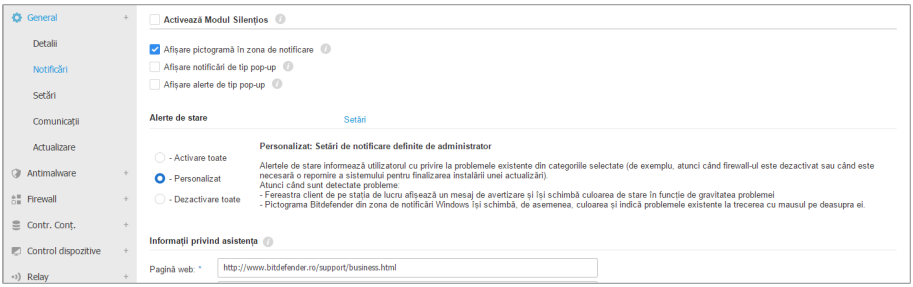
Pentru a configura o adresă de e-mail în fereastra **Despre** astfel încât aceasta să deschidă aplicația de e-mail implicită de pe stația de lucru, trebuie să o adăugați în câmpul **E-mail**cu prefixul „mailto:”. Exemplu: `mailto: name@domain.com`.

Utilizatorii pot accesa aceste informații din consola agentului de securitate făcând clic dreapta pe pictograma B Bitdefender din tava de sistem și selectând **Despre**.

Notificări

În această secțiune puteți configura opțiunile de afișare a interfeței cu utilizatorul a agentului de securitate Bitdefender într-un mod intuitiv și cuprinzător.

Cu un singur clic, puteți activa sau dezactiva un întreg tip de notificări, păstrând numai ceea ce contează cu adevărat pentru dvs. De asemenea, în aceeași pagină, vi se oferă control total asupra vizibilității problemelor stațiilor de lucru.



Politici - Setări de afișare

- **Mod silențios.** Utilizați caseta de selecție pentru a activa sau opri Modul Silențios. Modul Silențios este conceput pentru a vă ajuta să dezactivați cu ușurință interacțiunea cu utilizatorul în agentul de securitate. La activarea opțiunii Modul Silențios, sunt aduse următoarele modificări la configurația politicii:
  - Opțiunile **Afișare pictogramă în zona de notificare**, **Afișare notificări de tip pop-up** și **Afișare alerte de tip pop-up** din această secțiune vor fi dezactivate.
  - Dacă nivelul de protecție firewall a fost fixat pe **Set de reguli și întreabă** sau **Set de reguli, fișiere cunoscute și întreabă** acesta se va modifica în **Set de reguli, fișiere cunoscute și permite**. În caz contrar, setarea nivelului de protecție va rămâne neschimbată.
- **Afișare pictogramă în zona de notificare.** Selectați această opțiune pentru a afișa B pictograma Bitdefender din zona de notificare (cunoscută și sub numele de bară de sistem). Pictograma informează utilizatorii cu privire la statutul de protecție prin schimbarea aspectul său și prin afișarea unei notificări de tip pop – up corespunzătoare. În plus, utilizatorii pot face clic dreapta pe acesta pentru a deschide rapid fereastra principală a agentului de securitate sau fereastra **Despre**.
- **Afișare alerte de tip pop-up.** Utilizatorii sunt informați prin ferestre de alertă pop-up cu privire la evenimentele de securitate care necesită o acțiune din partea lor. Dacă alegeți să nu se afișeze pop-up-urile de alertă, agentul de securitate întreprinde automat acțiunea recomandată. Pop-up-urile sunt generate în următoarele situații:

- În cazul în care firewall-ul este setat pentru a solicita utilizatorului luarea de măsuri ori de câte ori aplicații necunoscute solicită acces la rețea sau Internet.
- În cazul în care este activată opțiunea Advanced Threat Control sau Sistemul de Detectare a Intruziunilor, ori de câte ori este detectată o aplicație potențial periculoasă.
- Dacă scanarea dispozitivului este activată, ori de câte ori este conectat la computer un dispozitiv de stocare extern. Puteți configura această setare în secțiunea **Antimalware > Scanare la cerere**.

- **Afișare notificări de tip pop-up.** Fiind diferite de ferestrele pop-up de alertă, ferestrele pop-up de notificare informează utilizatorii cu privire la diverse evenimente de securitate. Ferestrele de tip pop-up dispar automat în câteva secunde, fără intervenția utilizatorului.

  Selectați **Afișare ferestre pop-up de notificare**, apoi faceți clic pe linkul **Afișare setări modulare** pentru a alege în legătură cu ce evenimente doriți să fie notificați utilizatorii, grupate după modul. Există trei tipuri de ferestre pop-up de notificare, în funcție de gravitatea evenimentelor:

  - **Info**. Utilizatorii sunt informați în legătură cu evenimente de securitate semnificative dar inofensive. De exemplu, o aplicație care s-a conectat la internet.
  - **Scăzut**. Utilizatorii sunt informați în legătură cu evenimente de securitate importante, care ar putea necesita atenția acestora. De exemplu, modulul de Scanare la accesare a detectat o amenințare și fișierul a fost șters sau trecut în carantină.
  - **Critic**. Aceste ferestre pop-up de notificare informează utilizatorul cu privire la situații periculoase, cum ar fi modulul de Scanare la accesare care a detectat o amenințare și acțiunea din politica implicită este setată pe **Nicio acțiune**, astfel încât programul malware este în continuare prezent pe stația de lucru, sau un proces de actualizare care nu s-a finalizat cu succes.

  Bifați caseta aferentă denumirii tipului pentru a activa acel tip de ferestre pop-up în mod concomitent pentru toate modulele. Bifați casetele aferente modulelor individuale pentru a activa sau dezactiva anumite notificări.

  Spre exemplu, după selectarea casetelor aferente Sandbox Analyzer, Bitdefender Endpoint Security Tools îl informează pe utilizator când fișierul este supus analizei comportamentale.

Lista modulelor variază în funcție de licența dvs.

- **Vizibilitate probleme pentru stația de lucru.** Utilizatorii determină atunci când stația de lucru întâmpină probleme de configurare a securității sau alte riscuri de securitate în baza alertelor de stare. De exemplu, utilizatorii pot vedea când există o problemă cu protecția antimalware, cum ar fi: Modulul de scanare la accesare este dezactivat sau este necesară o scanare completă a sistemului. Utilizatorii sunt informați cu privire la stadiul lor de protecție în două moduri:
  - Verificând zona de status a ferestrei principale, care afișează un mesaj de stare corespunzător și își schimbă culoarea în funcție de nivelul de severitate al problemelor de securitate. De asemenea, utilizatorii au posibilitatea de a vizualiza detaliile problemelor detectate făcând clic pe butonul disponibil.
  - Verificând B pictograma Bitdefender din bara de sistem, care își modifică aspectul atunci când sunt detectate probleme.

  Agentul de securitate Bitdefender folosește următoarea convenție de culori în zona de notificare:
  - Verde: Nu sunt detectate probleme.
  - Galben: Stația de lucru prezintă probleme minore care îi afectează securitatea. Nu este necesar ca utilizatorii să-ți întrerupă lucrul pentru a soluționa aceste probleme.
  - Roșu: Stația de lucru prezintă probleme grave care necesită atenția imediată a utilizatorului.

  Selectați **Vizibilitate probleme stații de lucru**, apoi efectuați clic pe linkul **Afișare setări modulare** pentru a personaliza alertele de stare afișate în interfața pentru utilizator a agentului Bitdefender.

  Pentru fiecare modul, puteți opta pentru afișarea alertei ca avertizare sau problemă critică sau pentru neafișarea acesteia. Opțiunile sunt descrise aici:
  - **General**. Alerta de stare este generată ori de câte ori este necesară o repornire a sistemului sau după instalarea produsului, precum și dacă agentul de securitate nu se poate conecta la Serviciile cloud Bitdefender.
  - **Antimalware**. Alertele de stare sunt generate în următoarele situații:
    - Scanarea la accesare este activată, dar multe fișiere locale sunt excluse.
    - A trecut un anumit număr de zile de la data ultimei scanări complete a sistemului.

Puteți selecta modul de afișare a alertelor și defini numărul de zile de la ultima scanare a sistemului.

  - Este necesară repornirea pentru finalizarea procesului de dezinfectare.

  - **Firewall**. Această alertă de stare este generată atunci când modulul Firewall este dezactivat.
  - **Control aplicații**. Această alertă de stare este generată atunci când modulul Control aplicații este modificat.
  - **Control Conținut**. Această alertă de stare este generată atunci când modulul Control conținut este dezactivat.
  - **Actualizare**. Alerta de stare este generată de fiecare dată când este necesară repornirea sistemului pentru finalizarea unei operațiuni de actualizare.

- **Notificare de repornire a stației de lucru.** Această opțiune afișează o alertă de repornire pe stația de lucru de fiecare dată când este necesară o repornire a sistemului ca urmare a modificărilor aduse stației de lucru de modulele GravityZone selectate din setările pentru module.

  Notă
  Stațiile de lucru care necesită o repornire a sistemului au o pictogramă de stare specifică ( ) în inventarul GravityZone.

  Puteți personaliza și mai mult alertele de repornire selectând opțiunea **Afișare setări modulare**. Sunt disponibile următoarele opțiuni:

  - **Actualizare** - Selectați această opțiune pentru a activa notificările de repornire după actualizarea agentului.
  - **Actualizare** - Selectați această opțiune pentru a activa notificările de repornire după instalarea patch-urilor.

  Notă
  De asemenea, puteți stabili o limită în ore pentru cât timp un utilizator poate amâna o repornire. Pentru a face acest lucru, selectați **Repornirea automată a mașinii după** și introduceți o valoare de la 1 la 46.

  Alerta de repornire solicită utilizatorului să selecteze una dintre următoarele acțiuni:

  - **Repornește acum**. În acest caz, sistemul va fi repornit imediat.

– **Amânare repornire**. În acest caz, o notificare de repornire va apărea periodic pe ecran până când utilizatorul repornește sistemul sau până când expiră timpul setat de administratorul companiei.

Setări

În această secțiune puteți configura următoarele setări:

- **Configurare parolă.** Pentru a împiedica utilizatorii care beneficiază de drepturi de administrare să dezinstaleze protecția, trebuie să setați o parolă.

  Parola de dezinstalare poate fi configurată înainte de instalare prin personalizarea pachetului de instalare. Dacă ați făcut acest lucru, selectați **Păstrare setări instalare** pentru a păstra parola curentă.

  Pentru a seta parola sau pentru a schimba parola curentă, selectați **Activare parolă** și introduceți parola dorită. Pentru a elimina protecția cu parolă, selectați **Dezactivare parolă**.

- **Configurație proxy**

  Dacă rețeaua de instalare este asociată unui server proxy, trebuie să definiți setările proxy care să permită stațiilor de lucru să comunice cu componentele soluției GravityZone. În acest caz, trebuie să activați opțiunea **Configurare proxy** și să introduceți parametrii necesari:
  – **Server** - introduceți adresa IP a serverului proxy.
  – **Port.** - Introduceți portul utilizat pentru conectarea la serverul proxy.
  – **Nume utilizator** - introduceți un nume de utilizator recunoscut de proxy.
  – **Parolă** - introduceți parola corectă pentru utilizatorul specificat

- **Utilizator privilegiat**

  Modulul Utilizator privilegiat activează drepturile de administrare la nivel de stație de lucru, permițând utilizatorului stației de lucru să acceseze și să modifice setările de politică prin intermediul unei console locale, folosind interfața Bitdefender Endpoint Security Tools.

  Dacă doriți ca anumite stații de lucru să aibă drepturi de Utilizator privilegiat, trebuie să includeți mai întâi acest modul în agentul de securitate instalat pe stațiile de lucru țintă. Apoi, trebuie să configurați setările pentru Utilizatorul privilegiat din politica aplicată stațiilor de lucru:

Important
Modulul Utilizator privilegiat este disponibil numai pentru sistemele de operare Windows suportate pentru desktop și server.

1. Activați opțiunea **Utilizator privilegiat**.
2. Definiți o parolă pentru Utilizatorul privilegiat în câmpurile de mai jos.

   Utilizatorilor care accesează modul Utilizator privilegiat de pe stația de lucru locală li se va solicita să introducă parola definită.

Pentru a accesa modulul Utilizator privilegiat, utilizatorii trebuie să facă clic dreapta pe pictograma Bitdefender din tava de sistem și să slecteze opțiunea **Utilizator privilegiat** din meniul contextual. După introducerea parolei în fereastra de autentificare, se afișează o consolă cu setările de politică aplicate în prezent, în care utilizatorul stației de lucru poate vizualiza și modifica setările politicii.

Notă
Numai anumite funcții de securitate pot fi accesate local prin intermediul consolei Utilizator privilegiat, privind modulele Antimalware, Firewall, Control conținut și Control dispozitive.

Anularea modificărilor efectuate în modul Utilizator privilegiat:

– În Control Center, deschideți șablonul de politică alocat stației de lucru cu drepturile aferente Utilizatorului privilegiat și faceți clic pe **Salvare**. Astfel, se vor reaplica setărie originale stației de lucru țintă.
– Alocați o nouă politică stației de lucru cu drepturi de Utilizator privilegiat.
– Autentificați-vă la stația de lucru locală, deschideți consola Utilizator privilegiat și faceți clic pe **Resincronizare**.

Pentru a identifica ușor stațiile de lucru cu politici modificate în modul Utilizator privilegiat:

– În pagina **Rețea**, faceți clic pe meniul **Filtre** și selectați opțiunea **Editat de Utilizatorul privilegiat** din secțiunea **Politică**.
– Pe pagina **Rețea**, faceți clic pe stația de lucru care vă interesează pentru afișarea ferestrei **Informații**. Dacă politica a fost modificată în modul Utilizator privilegiat, se va afișa o notificare în secțiunea **General** > **Politică**.

Important
Modulul Utilizator privilegiat este creat special pentru depanare, permițând administratorilor de rețea să vizualizeze și să modifice cu ușurință setările de politică pe calculatoarele locale. Alocarea drepturilor Utilizatorului privilegiat altor utilizatori din companie trebuie să fie limitată la personalul autorizat, pentru a asigura faptul că politicile de securitate se aplică întotdeauna pe toate stațiile de lucru din rețeaua companiei.

- **Opțiuni**

  În această secțiune puteți defini următoarele setări:

  – **Îndepărtați evenimentele mai vechi de (zile).** Agentul de securitate Bitdefender păstrează un jurnal detaliat al evenimentelor referitoare la activitatea sa pe computer (inclusiv, de asemenea, activitățile calculatorului monitorizate de Content Control). În mod implicit, evenimentele sunt șterse din jurnal după 30 de zile. Dacă doriți să schimbați acest interval, alegeți o altă opțiune din meniu.

  – **Transmiteți rapoarte de avarie la Bitdefender.** Selectați această opțiune astfel încât rapoartele să fie trimise la Laboratoarele Bitdefender pentru analiză în cazul în care agentul de securitate se blochează. Rapoartele vor ajuta inginerii noștri să își dea seama ce a cauzat problema și să prevină reapariția ei. Nu vor fi transmise informații cu caracter personal.

  – **Trimitere fișiere executabile suspecte pentru analiză.** Selectați această opțiune astfel încât fișierele care par nesigure sau prezintă un comportament suspect să fie trimise către Laboratoarele Bitdefender pentru analiză.

  – **Transmiteți violările de memorie HVI la Bitdefender.** HVI trimite implicit către serverele cloud ale Bitdefender informații anonimizate privind violările detectate, pentru a fi folosite în statistici în scopul îmbunătățirii ratei de detecție a produsului. Puteți debifa această casetă dacă nu doriți să transmiteți astfel de informații din rețeaua dumneavoastră.

  Notă
  Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Comunicații

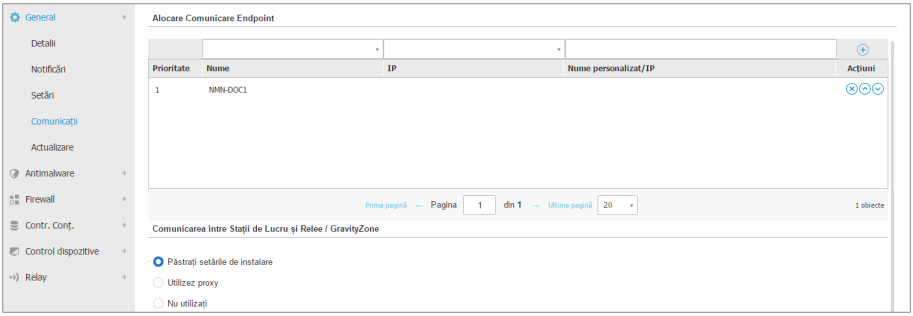
În această secțiune, puteți aloca una din mai multe mașini releu stațiilor de lucru țintă, apoi configurați preferințele proxy pentru comunicarea între stațiile de lucru țintă și GravityZone.

Alocare Comunicare Endpoint

Când sunt instalate mai multe servere de comunicare pe dispozitivul GravityZone, aveți posibilitatea să alocați calculatoarele țintă cu unul sau mai multe servere de comunicare prin intermediul politicii. Stațiile de lucru releu disponibile, care servesc ca servere de comunicare sunt și ele luate în considerare.

Pentru a atribui servere de comunicare la calculatoarele țintă:

1. În tabelul **Alocare Comunicare Endpoint**, faceți clic pe câmpul **Nume**. Este afișată lista de servere de comunicații detectate.
2. Selectați o entitate.



Politici referitoare la calculatoare și mașini virtuale - Setări de comunicare

3. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului.

   Serverul de comunicație este adăugată în listă. Toate calculatoarele țintă vor comunica cu Control Center prin intermediul serverului de comunicație specificat.
4. Urmați aceiași pași pentru a adăuga mai multe servere de comunicare, dacă sunt disponibile.
5. Puteți configura prioritatea serverelor de comunicare, folosind săgețile în sus și în jos disponibile în partea dreaptă a fiecărei entități. Comunicarea cu

calculatoarele țintă va fi efectuată prin intermediul entității localizată în partea de sus a listei. În cazul în care nu se poate realiza comunicarea cu această entitate, va fi luată în considerare următoarea.

6. Pentru a șterge o entitate din listă, faceți clic pe butonul ⊗ **Ștergere** din partea dreaptă a tabelului.

Comunicarea între stațiile de lucru și relee / GravityZone

În această secțiune, puteți configura preferințele proxy pentru comunicarea între stațiile de lucru țintă și mașinile releu alocate sau între stațiile de lucru țintă și aplicația GravityZone (dacă nu s-a alocat niciun releu):

- **Păstrează setările de instalare**, pentru a folosi aceleași setări proxy ca și cele definite în pachetul de instalare.
- **Folosește proxy-ul definit în secțiunea General**, pentru a folosi setările proxy definite în politica curentă, în secțiunea **General > Setări**.
- **Nu folosi**, dacă stațiile de lucru țintă nu comunică cu componentele GravityZone specifice printr-un proxy.

Comunicarea între Stații de Lucru și Cloud Services

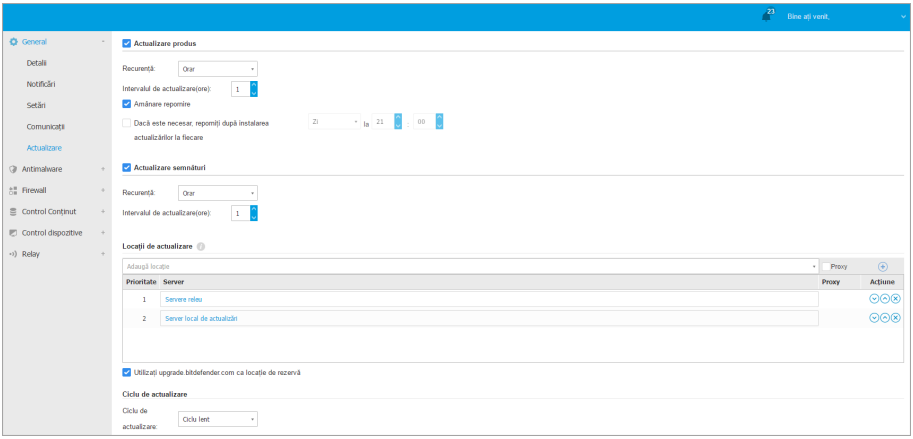
În această secțiune, puteți configura preferințele proxy pentru comunicarea între stațiile de lucru țintă și Serviciile cloud Bitdefender (care necesită conexiune la internet):

- **Păstrează setările de instalare**, pentru a folosi aceleași setări proxy ca și cele definite în pachetul de instalare.
- **Folosește proxy-ul definit în secțiunea General**, pentru a folosi setările proxy definite în politica curentă, în secțiunea **General > Setări**.
- **Nu folosi**, dacă stațiile de lucru țintă nu comunică cu componentele GravityZone specifice printr-un proxy.

Actualizare

Actualizările sunt foarte importante, întrucât permit combaterea celor mai noi amenințări. Bitdefender publică pe internet toate actualizările de produse și conținut de securitate prin intermediul serverelor Bitdefender. Toate actualizările sunt criptate și semnate digital astfel încât să nu poată fi modificate. Atunci când este disponibilă o nouă actualizare, agentul de securitate Bitdefender verifică autenticitatea semnăturii digitale a actualizării și integritatea conținutului

pachetului. În continuare, fiecare fișier de actualizare este analizat și se verifică dacă versiunea sa corespunde celei instalate. Fișierele mai noi sunt descărcate local și codul lor hash MD5 este verificat pentru a se asigura că acestea nu sunt modificate. În această secțiune, puteți configura agentul de securitate Bitdefender și setările de actualizare a conținutului de securitate.



Politici referitoare la calculatoare și mașini virtuale - Opțiuni de actualizare

- **Actualizare produs.** Agentul de securitate Bitdefender verifică, descarcă și instalează automat actualizările în fiecare oră (setare implicită). Actualizările automate sunt efectuate discret, în fundal.
  - **Recurență**. Pentru a modifica recurența de actualizare automată, selectați o altă opțiune din meniu și configurați-o conform necesităților dvs. în câmpurile ulterioare.
  - **Amânare repornire**. Unele actualizări necesită o repornire a sistemului pentru instalarea și funcționarea coresponzătoare. În mod implicit, produsul va funcționa în continuare cu vechile fișiere până la repornirea computerului, după care va aplica cele mai recente actualizări. O notificare în interfața cu utilizatorul va solicita utilizatorului să repornească sistemul de fiecare dată când este necesară o actualizare. Se recomandă să păstrați activă această opțiune. În caz contrar, sistemul se va reporni automat după instalarea unei actualizări care necesită acest lucru. Utilizatorii vor fi notificați pentru a-și salva munca, însă repornirea nu poate fi anulată.

– Dacă alegeți să amânați repornirea, puteți seta un timp convenabil atunci când calculatoarele vor reporni în mod automat dacă este (încă) necesar. Acest lucru poate fi foarte util pentru servere. Selectați **Repornire după instalarea actualizărilor, dacă este cazul** și precizați când este convenabil să se facă repornirea (zilnic sau săptămânal într-o anumită zi, la un anumit moment al zilei).

– Pentru mai mult control la modificarea configurării și la actualizarea procesului de testare, puteți configura agentul BEST pe mașinile dumneavoastră Linux pentru a executa actualizările modulului kernel EDR prin **Actualizare produs**.

  Când caseta de bifare **Actualizare produs** este bifată:

  - Dacă bifați caseta **Actualizare module EDR pe Linux utilizând actualizările produsului**, GravityZone va actualiza versiunile de kernel prin **Actualizare produs**.
  - Dacă nu bifați caseta respectivă, versiunile de kernel vor fi actualizate prin **Actualizare conținut de securitate**.

  Notă
  Dacă bifați caseta **Actualizare module EDR pe Linux utilizând actualizările produsului**, dar dezactivați opțiunea **Actualizare produs**, modulele EDR de pe Linux nu vor fi actualizate.

- **Actualizare conținut de securitate.** Conținutul de securitate se referă la mijloace statice și dinamice de detectare a amenințărilor, cum ar fi, dar fără a se limita la, motoare de scanare, modele de învățare prin intermediul mașinilor, euristică, reguli, semnături și liste negre. Agentul de securitate Bitdefender caută automat actualizări de conținut de securitate în fiecare oră (setare implicită). Actualizările automate sunt efectuate discret, în fundal. Pentru a modifica recurența de actualizare automată, selectați o altă opțiune din meniu și configurați-o conform necesităților dvs. în câmpurile ulterioare.
- **Locații de actualizare**. Locația implicită a actualizării agentului de securitate Bitdefender este serverul de actualizări GravityZone. Adăugați o locație de actualizare folosind denumirile predefinite din meniul derulant sau introducând IP-ul sau numele gazdei unare sau mai multor servere de actualizare din rețeaua dvs. Configurați prioritatea folosind butoanele săgeți în sus și în jos afișate când poziționați mouse-ul deasupra opțiunilor. Dacă prima locație de actualizare nu este disponibilă, se utilizează următoarea și așa mai departe.

Pentru a seta o adresă de actualizare locală:

1. Introduceți adresa serverului de actualizări în câmpul **Adăugare locație**. Puteți:
   - Selectați locația predefinintă:
     - **Servere releu**. Stația de lucru se va conecta automat la Serverul releu alocat.

       Avertisment
       Serverele de tip releu nu sunt compatibile cu sistemele de operare mai vechi. Pentru informații suplimentare, consultați Ghidul de instalare.

       Notă
       Puteți vedea Serverul releu alocat în fereastra **Informații**. Pentru detalii suplimentare, consultați Vizualizare detalii calculator.

     - **Server local de actualizări**
   - Introduceți IP-ul sau numele gazdei unuia sau mai multor servere de actualizări din rețeaua dvs. Utilizați una dintre aceste sintaxe:
     - `ip_server_actualizări:port`
     - `nume_server_actualizări:port`

     Portul implicit este 7074.

     Căsuța **Utilizați serverele Bitdefender ca adresă de fallback** este selectată implicit. Dacă locațiile pentru actualizări nu sunt disponibile, se va utiliza locația de rezervă.

   Avertisment
   Dezactivarea locației de rezervă va întrerupe actualizările automate, iar rețeaua dvs. va fi vulnerabilă dacă locațiile furnizate nu sunt disponibile.

2. În cazul în care calculatoarele client se conectează la serverul local de actualizări, printr-un server proxy, selectați **Folosește Proxy**.
3. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului.

4. Folosiți săgețile Sus / Jos din coloana **Acțiune** pentru a seta prioritatea locațiilor de actualizare definite. Dacă prima locație de actualizare nu este disponibilă, se verifică următoarea și așa mai departe.

Pentru a elimina o locație din listă, faceți clic pe butonul corespunzător **Ștergere**. Deși puteți elimina adresa implicită a locației de actualizare, acest lucru nu este recomandat.

- **Ciclu de actualizare.** Puteți rula actualizările de produse în mai multe faze, folosind ciclurile de actualizare:
  - **Ciclu lent**. Mașinile cu o politică pe bază de cicluri lente vor primi actualizări la o dată ulterioară, în funcție de răspunsul primit de la stațiile de lucru cu cicluri rapide. Este o măsură de precauție în procesul de actualizare. Aceasta este opțiunea implicită.
  - **Ciclu rapid**. Mașinile cu o politică de ciclu rapid vor primi cele mai noi actualizări disponibile. Această setare este recomandată pentru mașinile non-critice în producție.

Important

- În situați puțin probabilă a producerii unui eveniment în ciclul rapid pe mașinile cu o anumită configurație, problema în cauză va fi remediată înaintea actualizării din ciclul lent.
- BEST for Windows Legacy nu acceptă etapizarea. Stațiile de lucru mai vechi din locația de etapizare trebuie mutate în locația de producție.

7.2.2. HVI

Notă

HVI asigură protecție numai pentru mașinile virtuale de pe hypervisori Citrix Xen. Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Hypervisor Memory Introspection protejează mașinile virtuale împotriva amenințărilor avansate la adresa mașinilor virtuale pe care motoarele pe bază de semnături nu le pot învinge. Acesta asigură detecția în timp real a atacurilor prin monitorizarea proceselor din exteriorul sistemului de operare găzduit. Mecanismul de protecție include mai multe opțiuni de blocare a atacurilor pe măsură ce acestea se produc și de eliminare imediată a amenințării.

Urmând principiul sistemului de operare de separare a memoriei, HVI include două module de protecție organizate în categoriile aferente:

- Spațiu utilizator, ce vizează procesele normale ale aplicațiilor utilizatorului.
- Spațiu nucleu, ce vizează procesele rezervate părții de bază a sistemului de operare.

În plus, politica HVI include două caracteristici care vă ajută să gestionați securitatea și să întrețineți mașinile virtuale protejate:

- Excluderi, pentru vizualizarea și gestionarea proceselor exceptate de la scanare.
- Instrumente personalizate, pentru injectarea instrumentelor necesare activităților operaționale și de analiză în sistemele de operare ale sistemului găzduit.

Spațiu utilizator

În această secțiune puteți configura setările de protecție pentru procesele ce rulează în memoria spațiului de utilizator.

Folosiți caseta **Introspecție memorie spațiu utilizator** pentru a activa sau dezactiva protecția.

Funcționalitatea acestui modul se bazează pe reguli, permițându-vă să configurați protecția separat pentru diferite grupuri de procese. În plus, puteți alege să colectați mai multe informații de analiză.

- Reguli privind spațiul utilizatorului
- Informații de analiză

Reguli privind spațiul utilizatorului

Acest modul vine cu un set de reguli predefinite, care acoperă majoritatea aplicațiilor vulnerabile. Tabelul din această secțiune afișează regulile existente, furnizând informații importante despre fiecare dintre acestea:

- Nume regulă
- Procesele pentru care se aplică regula
- Modul de monitorizare
- Acțiune ce blochează atacul detectat
- Acțiuni de eliminare a amenințării

De asemenea, puteți furniza o listă de reguli personalizate pentru procesele pe care doriți să le monitorizați. Pentru a crea o nouă regulă:

1. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Această acțiune deschide fereastra de configurare a regulii.
2. Configurați modulul folosind următoarele setări de reguli:
   - **Nume regulă.** Introduceți numele cu care regula va fi introdusă în tabelul de reguli. De exemplu, pentru procese cum ar fi `firefox.exe` sau `chrome.exe`, puteți denumi regula `Browsere`.
   - **Procese.** Introduceți denumirile proceselor pe care doriți să le monitorizați, separate prin punct și virgulă (;).
   - **Mod de monitorizare.** Pentru o configurare rapidă, faceți clic pe nivelul de securitate care se potrivește cel mai bine necesităților dumneavoastră (**Agresiv**, **Normal** sau **Permisiv**). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

     Puteți configura în detaliu setările modulului selectând nivelul de protecție **Personalizat** și selectând una sau mai multe dintre următoarele opțiuni:
     - **Legături setate pe DLL-uri critice în modul de utilizator.** Detectează injecțiile DLL, care încarcă cod periculos în procesul de apelare.
     - **Tentative de dezarhivare/decriptare în fișierul executabil principal.** Detectează tentativele de descifrare a codului din executabilul procesului principal și protejează procesul de modificare prin cod periculos.
     - **Scriere în procesul țintă de către entități străine.** Protejează împotriva injectării de cod în procesele protejate.
     - **Exploatări.** Detectează comportamentul proceselor neintenționate cauzat de exploatarea unei erori sau a unei vulnerabilități nedivulgate anterior. Folosiți această opțiune dacă doriți să monitorizați executarea codului din segmentul și stiva aplicațiilor protejate.
     - **Conectarea WinSock.** Blochează interceptările bibliotecilor de rețea (DLL) utilizate de către sistemul de operare, asigurând o bună comunicare TCP/IP.
   - **Acțiuni.** Există o serie de acțiuni pe care le puteți implementa în cazul amenințărilor detectate. Fiecare acțiune are, la rândul său, o serie de opțiuni posibile sau acțiuni secundare. Acestea sunt descrise mai jos:

– **Acțiune primară.** Aceasta este acțiunea imediată pe care o puteți întreprinde atunci când se detectează un atac pe mașina găzduită, permițându-vă să o blocați. Acestea sunt opțiunile disponibile:

- **Jurnal.** Doar înregistrează evenimentul în baza de date. În acest caz, veți primi numai o notificare (dacă este configurată) și veți putea vizualiza incidentul din raportul **Activitate HVI**.
- **Respingere.** Se respinge orice încercare a unei amenințări de a modifica procesul țintă.
- **Oprire mașină.** Oprește mașina virtuală pe care rulează procesul țintă.

Important
Se recomandă să setați mai întâi acțiunea acțiunea primară pe **Înregistrare**. Apoi utilizați politica pentru o perioadă de timp rezonabilă pentru a vă asigura că totul funcționează conform așteptărilor. După aceea, puteți selecta ce acțiuni doriți să fie întreprinse în cazul în care se detectează o violare de memorie.

– **Acțiune de remediere.** În funcție de opțiunea selectată, Security Server injectează un instrument de remediere în sistemul de operare găzduit. Instrumentul pornește automat scanarea după programe malware și atunci când se detectează o amenințare, acesta continuă cu acțiunea selectată. Acestea sunt opțiunile disponibile:

- **Dezinfectare.** Elimină codul periculos din fișierele infectate. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate.
- **Ștergere.** Șterge fișierele detectate de pe disc, fără nicio avertizare. Se recomandă să evitați această acțiune.
- **Ignorare.** Instrumentul de remediere detectează și raportează doar fișierele detectate.
- **Nicio acțiune.** Instrumentul de remediere nu va fi injectat în sistemul de operare găzduit.

Notă
Închiderea instrumentului va cauza eliminarea acestuia din sistem, fără a lăsa urme în sistemul de operare găzduit.

– **Acțiune de remediere de rezervă.** Atunci când acțiunea de remediere eșuează, puteți selecta o altă acțiune de remediere dintre opțiunile disponibile.

3. Faceți clic pe **Save**.

După ce regula a fost creată, o puteți modifica oricând. Dacă faceți clic pe denumirea regulii, se va a deschide fereastra de configurare a regulii.

De asemenea, GravityZone vă permite să configurați rapid comportamentul de Introspecție memorie în momentul detecției, prin modificarea simultană a mai multor reguli. Pentru a configura mai multe reguli folosind aceleași acțiuni:

1. Selectați regulile pe care doriți să le modificați.
2. Faceți clic pe butonul **Acțiune și remediere** din partea de sus a tabelului.
3. Selectați opțiunea dorită pentru fiecare acțiune.
4. Faceți clic pe **Save**. Noile acțiuni vor intra în vigoare după salvarea politicii, cu condiția ca mașinile țintă să fie online.

Pentru a șterge una sau mai multe reguli din listă, selectați-le și apoi faceți clic pe butonul ⊗ **Ștergere** din partea de sus a tabelului.

Informații de analiză

Bifați caseta **Erori de aplicații** de sub tabelul cu regulile spațiului utilizatorului pentru a permite colectarea de informații detaliate atunci când aplicațiile sunt închise.

Puteți vizualiza aceste informații în raportul de activitate HVI și puteți identifica motivul care a cauzat închiderea aplicației. Dacă evenimentul are legătură cu un atac, detaliile sale vor apărea grupate cu alte evenimente sub incidentul care a dus la apariția evenimentului.

Spațiu Kernel

HVI protejează elementele cheie ale sistemului de operare, cum ar fi:

- Drivere de kernel de importanță critică și obiectele asociate, care implică tabele de dispatch intrare/ieșire rapid asociate cu driverele principale.
- Driverele de rețea, a căror modificare ar permite unui program malware să intercepteze traficul și să injecteze componente periculoase în fluxul de trafic.

- Imaginea kernel-ului sistemului de operare, ce implică următoarele: secțiunea de cod, secțiunea de date și secțiunea numai în citire, inclusiv tabela de adrese de import (Import Address Table - IAT), tabela de adrese de export (Export Address Table - EAT) și resurse.

În această secțiune puteți configura setările de protecție pentru procesele ce rulează în memoria spațiului kernel.

Folosiți caseta **Introspecție memorie spațiu kernel** pentru a activa sau dezactiva protecția.

Pentru o configurare rapidă, faceți clic pe nivelul de securitate care se potrivește cel mai bine necesităților dumneavoastră (**Agresiv**, **Normal** sau **Permisiv**). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

Puteți configura în detaliu setările modulului selectând nivelul de protecție **Personalizat** și selectând una sau mai multe dintre următoarele opțiuni:

- **Regiștri de control**. Regiștrii de control (CR) sunt regiștri de procesor, care controlează comportamentul general al unui procesor sau al altor dispozitive digitale. Selectați această opțiune pentru a detecta tentativele de încărcare a unor valori nevalide în anumiți Regiștri de control.
- **Model Specific Registers**. Acești regiștri se referă la oricare dintre regiștrii de control din setul de instrucțiuni x86 folosiți pentru depanare, urmărirea executării programelor, monitorizarea performanței computerului și comutarea anumitor caracteristici ale procesorului. Selectați această opțiune pentru a detecta tentativele de modificare a acestor regiștri.
- **Integritate IDT/GDT**. Tabelele de descriptori de întrerupere sau globali (IDT/GDT) sunt folosite de procesor pentru a determina răspunsul corect la întreruperi și excepții. Selectați această opțiune pentru a detecta orice tentativă de modificare a acestor tabele.
- **Protecția driverelor antimalware.** Selectați această opțiune pentru a detecta tentativele de modificare a driverelor utilizate de software-ul antimalware.
- **Protecție drivere Xen.** Selectați această opțiune pentru a detecta tentativele de modificare a driverelor hypervisor-ului Citrix XenServer.

Există o serie de acțiuni pe care le puteți implementa în cazul amenințărilor detectate. Fiecare acțiune are, la rândul său, o serie de opțiuni posibile sau acțiuni secundare. Acestea sunt descrise mai jos:

- **Acțiune primară.**

- **Jurnal.** Doar înregistrează evenimentul în baza de date. În acest caz, veți primi numai o notificare (dacă este configurată) și veți putea vizualiza incidentul din raportul **Activitate introspecție memorie**.
- **Respingere.** Se respinge orice încercare a unei amenințări de a modifica procesul țintă.
- **Oprire mașină.** Oprește mașina virtuală pe care rulează procesul țintă.

Important
Se recomandă să setați mai întâi acțiunea acțiunea primară pe **Înregistrare**. Apoi utilizați politica pentru o perioadă de timp rezonabilă pentru a vă asigura că totul funcționează conform așteptărilor. După aceea, puteți selecta ce acțiuni doriți să fie întreprinse în cazul în care se detectează o violare de memorie.

- **Acțiune de remediere.**
  - **Dezinfectare.** Elimină codul periculos din fișierele infectate. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate.
  - **Ștergere.** Șterge fișierele detectate de pe disc, fără nicio avertizare. Se recomandă să evitați această acțiune.
  - **Ignorare.** Instrumentul de remediere detectează și raportează doar fișierele detectate.
  - **Nicio acțiune.** Instrumentul de remediere nu va fi injectat în sistemul de operare găzduit.
- **Acțiune de remediere de rezervă.** Atunci când acțiunea de remediere eșuează, puteți selecta o altă acțiune de remediere dintre opțiunile disponibile.

În plus, puteți alege să colectați informații care vor completa datele furnizate echipelor de analiză. Bifați casetele aferente **evenimentelor referitoare la erori ale sistemului de operare** și **evenimentelor referitoare la drivere** pentru a activa colectarea informațiilor referitoare la erorile sistemului de operare al gazdei sau la evenimentele generate de modulele suplimentare încărcate de sistemul de operare. Aceste evenimente, anterioare unui incident, vor ajuta echipele de investigație să identifice mai rapid cauza de bază a atacului.

Aceste evenimente sunt afișate în raportul de activitate HVI sub incidentul care le-a cauzat.

Excluderi

GravityZone vă permite să excludeți procese de la scanarea HVI folosind rapoartele **Aplicații blocate** și **Activitate HVI**. Secțiunea **Excluderi** adună toate procesele acestea din rapoartele menționate și le afișează sub forma unui tabel.

Pentru fiecare proces exclus puteți vizualiza un comentariu cuprinzând motivul excluderii.

Dacă vă răzgândiți cu privire la procesul exclus, efectuați clic pe butonul **Delete** din partea de sus a tabelului iar acesta va fi inclus în scanările viitoare.

Instrumente personalizate

În această secțiune puteți configura injectarea instrumentelor în sistemele de operare ale sistemului găzduit vizat. Aceste instrumente trebuie încărcate pe GravityZone înainte de a fi utilizate. Pentru mai multe informații, consultați capitolul „Injectare instrumente personalizate cu HVI” (p. 533).

Pentru configurarea injectărilor:

1. Utilizați caseta **Activare injectări** pentru a activa sau dezactiva funcția.
2. Efectuați clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului pentru a adăuga un nou instrument. Este afișată o fereastră de configurare.
3. Selectați instrumentul pe care doriți să îl utilizați din lista derulantă **Alegere instrument**.

   Aceste instrumente au fost încărcate anterior în GravityZone. Dacă nu găsiți instrumentul potrivit pe listă, accesați **Centru administrare instrumente** și adăugați-l de acolo. Pentru mai multe informații, consultați capitolul „Injectare instrumente personalizate cu HVI” (p. 533).
4. Din **Descriere instrument** introduceți utilizarea dorită pentru instrument sau orice altă informație pe care o considerați utilă.
5. Introduceți linia de comandă a instrumentului împreună cu toți parametrii de intrare necesari, exact la fel cum procedați pentru Command Prompt sau Terminal. De exemplu:

   ```
   bash script.sh <param1> <param2>
   ```

   .

Pentru Instrumentele BD de remediere, puteți selecta doar acțiunea de remediere și acțiunea de remediere de backup din cele două meniuri derulante.

6. Indicați locația de unde Security Server trebuie să culeagă jurnalele:
   - **stdout**. Selectați această căsuță pentru a prelua jurnalele din canalul standard de comunicare de ieșire.
   - **Fișier ieșire**. Selectați această căsuță pentru a prelua fișierul jurnal salvat pe stația de lucru. În acest caz, trebuie să introduceți calea unde poate Security Server să găsească fișierul. Puteți folosi căi absolute sau variabile de sistem.

     Aici aveți două opțiuni suplimentare:

     a. **Ștergere fișiere jurnal din sistemul găzduit după ce au fost transferate**. Selectați această opțiune dacă nu mai aveți nevoie de fișiere pe stația de lucru.

     b. **Transferați jurnalele la**. Selectați această opțiune pentru a muta fișierele jurnal din Security Server într-o altă locație. În acest caz, trebuie să furnizați calea către locația de destinație și datele de autentificare.
7. Selectați cum doriți să fie declanșată injectarea. Aveți la dispoziție următoarele opțiuni:
   - **După detectarea unei violări pe mașina virtuală găzduită.** Instrumentul este injectat exact în momentul în care este detectată o amenințare pe una dintre mașinile virtuale.
   - **Printr-o programare specifică.** Utilizați opțiunile de programare pentru a configura programarea injectării. Puteți alege să executați instrumentul la interval de câteva ore, zile, sau săptămâni, începând cu o anumită dată sau oră.

     Vă rugăm să aveți în vedere că mașina virtuală trebuie să fie pornită la termenul programat. Injectarea programată nu va fi executată la termen dacă mașina nu este pornită sau se află în pauză de funcționare. În astfel de situații, este recomandabil să activați caseta **Dacă ora de injectare programată este ratată, executați sarcina cât mai curând posibil** .
   - Câteodată instrumentul poate necesita un timp mai îndelungat decât cel preconizat pentru finalizarea acțiunii sau poate să nu mai răspundă la comenzi. Pentru a evita căderile de sistem în astfel de situații, selectați din

secțiunea **Configurare siguranță** după câte ore trebuie ca Security Server să oprească automat acțiunea instrumentului.

- Faceți clic pe **Save**. Instrumentul va fi adăugat în tabel.

Puteți adăuga câte instrumente aveți nevoie urmând pașii menționați anterior.

7.2.3. Antimalware

Notă
Acest modul este disponibil pentru:

- Windows pentru stații de lucru
- Windows pentru servere
- Linux
- macOS

Modulul Antimalware protejează sistemul contra tuturor tipurilor de malware (viruși, troieni, aplicații spion, rootkit-uri, adware și așa mai departe). Protecția se împarte în trei categorii:

- Scanare la acces: previne pătrunderea în sistem a noilor amenințări de programe periculoase.
- Scanare la executare: protejează în mod proactiv împotriva amenințărilor și detectează și blochează automat atacurile fără fișiere în faza de pre-execuție.
- Scanare la cerere: permite detectarea și îndepărtarea programelor periculoase care există deja în sistem.

Atunci când detectează un virus sau un alt cod periculos,agentul de securitate Bitdefender va încerca în mod automat să elimine codul periculos din fișierul infectat și să reconstruiască fișierul original. Această operațiune este denumită dezinfectare. Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a izola infecția. Atunci când sunt în carantină, virușii sunt inofensivi deoarece nu pot fi executați sau citiți.

Utilizatorii avansați pot configura excluderile de la scanare în cazul în care nu doresc ca anumite fișiere sau tipuri de fișiere să fie scanate.

Setările sunt organizate în următoarele secțiuni:

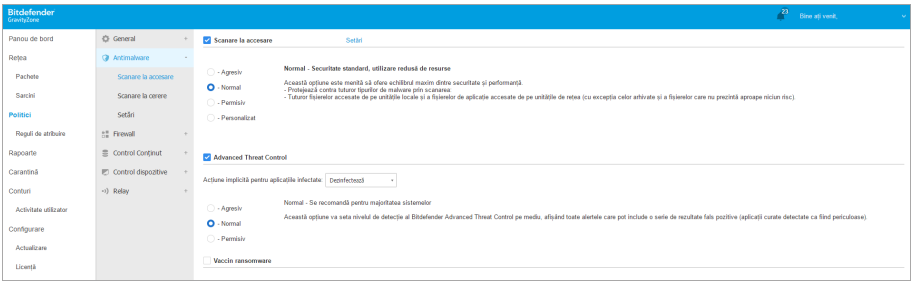
- Scanare la accesare
- La executare
- Scanare la cerere

- HyperDetect
- Anti-Exploit avansat
- Setări
- Mașini Security Server

Scanare la accesare

In this section you can configure the components that provide protection when a file or application is accessed:În această secțiune puteți configura componentele care oferă protecție la accesarea unui fișier sau a unei aplicații:

- Scanare la accesare
- Vaccin anti-ransomware



Politici - Setări la accesare

Scanare la accesare

Scanarea la accesare previne pătrunderea în sistem a noilor amenințări malware prin scanarea fișierelor locale și din rețea atunci când acestea sunt accesate (deschise, mutate, copiat sau executate), a sectoarelor de boot și a eventualelor aplicații nedorite.

Notă
Această caracteristică are anumite limitări pe sistemele pe bază de Linux. Pentru detalii, consultați capitolul de cerințe din Ghidul de instalare GravityZone.

Pentru a configura scanarea la accesare:

1. Utilizați caseta de selecție pentru a porni sau opri scanarea la accesare.

Avertisment
Dacă opriți scanarea la accesare, stațiile de lucru vor fi vulnerabile la malware.

2. Pentru o configurare rapidă, faceți clic pe nivelul de securitate care se potrivește cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.
3. Puteți configura setările de scanare în detaliu prin selectarea nivelului de protecție **Personalizat** și făcând clic pe link-ul **Setări**. Se va deschide fereastra de **Setări scanare la accesare**, care conține mai multe opțiuni organizate structurate în două file, **Setări generale** și **Setări avansate**.

   Opțiunile din fila **General** sunt descrise în continuare:

   - **Locație fișier**. Folosiți aceste opțiuni pentru a specifica tipurile de fișiere pe care doriți să le scanați. Preferințele de scanare pot fi configurate separat pentru fișiere locale (stocate pe stația de lucru locală) sau fișiere în rețea (stocate pe partajările în rețea). În cazul în care protecția antimalware este instalată pe toate computerele din rețea, puteți dezactiva scanarea fișierelor de rețea, pentru a permite un acces mai rapid la rețea.

     Puteți seta agentul de securitate să scaneze toate fișierele accesate (indiferent de extensie), fișierele de aplicație sau extensiile specifice de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor accesate asigură cea mai bună protecție, în timp ce scanarea exclusivă a aplicațiilor poate fi utilizată pentru asigurarea unei performanțe ridicate a sistemului.

     Notă
     Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Tipuri de fișiere de aplicații” (p. 567).

     Dacă doriți să fie scanate doar extensii specifice, alegeți **Extensii definite de utilizator** din meniu și apoi introduceți extensiile în câmpul de editare și apăsați `Enter` după fiecare extensie.

     Notă
     Pe sistemele Linux, extensiile de fișiere sunt sensibile la caracterele mici și mari, iar fișierele cu aceeași denumire dar extensie diferită sunt considerate obiecte distincte. De exemplu, `file.txt` este diferit de `file.TXT`.

     Din motive ce țin de performanța sistemului, puteți exclude de la scanare și fișiere de dimensiuni mari. Selectați caseta de selecție **Dimensiune maximă**

(MB) și specificați limita de mărime a fișierelor ce vor fi scanate. Folosiți această opțiune cu înțelepciune, deoarece programele periculoase poate afecta și fișiere mai mari.

- **Scanează.** Selectați casetele de bifare corespunzătoare pentru a activa opțiunile de scanare dorite.
  - **Doar fișiere noi sau modificate.** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
  - **Sectoare de boot.** Scanează sectoarele de boot ale sistemului. Acest sector al hard disk-ului conține codul necesar pentru a iniția procesul de boot. Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.
  - **Pentru keyloggers.** Aplicațiile keyloggers înregistrează ceea ce introduceți de pe tastatură și trimit raporte pe Internet către o persoană rău intenționată (hacker). Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.
  - **Pentru aplicații potențial nedorite (PUA).** O aplicație potențial nedorită (PUA) este un program care ar putea fi nedorit pe PC, care uneori vine la pachet cu software-ul freeware. Astfel de programe pot fi instalate fără consimțământul utilizatorului (numite și adware), sau vor fi incluse în mod implicit în kit-ul de instalare în mod expres (ad-supported). Efectele potențiale ale acestor programe includ afișarea de pop-up-uri, instalarea de bare de instrumente nedorite în browser-ul implicit sau rularea mai multor procese în fundal și încetinirea performanței PC-ului.
  - **Arhive**. Selectați această opțiune dacă doriți să activați scanarea la accesare a fișierelor arhivate. Scanarea în interiorul arhivelor este un proces lent și care necesită multe resurse, nefiind recomandată, prin urmare, pentru protecția în timp real. Arhivele cu fișiere infestate nu sunt o amenințare directă pentru securitatea sistemului. Programele periculoasevă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția la accesare.

    Dacă decideți să utilizați această opțiune, puteți configura următoarele opțiuni de optimizare:
    - **Dimensiunea maximă a arhivei (MB).** Puteți seta o limită maximă de dimensiune acceptată pentru arhive pentru a fi scanate la accesare.

Selectați căsuța corespunzătoare și introduceți dimensiunea maximă a arhivei (exprimată în MB).

- **Adâncimea maximă a arhivei (niveluri).** Selectați caseta de bifare corespunzătoare și alegeți adâncimea maximă a arhivei din meniu. Pentru performanțe superioare, alegeți cea mai mică valoare; pentru protecție maximă, alegeți cea mai mare valoare.

– **Scanare amânată.** Amânarea scanării îmbunătățește performanța sistemului la efectuarea operațiunilor de accesare. De exemplu, resursele de sistem nu sunt afectate atunci când se copiază fișiere mari. Această opțiune este activată în mod implicit.

- **Acțiuni la scanare**. În funcție de tipul de fișier detectat, următoarele acțiuni sunt aplicate în mod automat:

  – **Acțiune implicită pentru fișierele infectate.** Bitdefender detectează fișierele ca fiind infectate folosind diverse mecanisme avansate, printre care semnăturile malware, învățarea automată și tehnologiile bazate pe inteligență artificială (AI). În mod normal, agentul de securitate Bitdefender poate șterge codul malware din fișierul infestat și poate reconstitui fișierul inițial. Această operațiune este cunoscută sub denumirea de dezinfectare.

    În cazul în care este detectat un fișier infectat, agentul de securitate Bitdefender va încerca în mod automat să-l dezinfecteze. Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția. Puteți modifica acest flux recomandat în funcție de nevoile dumneavoastră.

    Important
    Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

  – **Acțiune implicită pentru fișierele suspecte.** Fișierele sunt detectate ca fiind suspecte de către analiza euristică și alte tehnologii Bitdefender. Acestea asigură o rată mare de detecție, însă utilizatorii trebuie să fie conștienți că există și rezultate fals pozitive (fișiere neinfectate detectate ca fiind suspecte) în unele cazuri. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

    Atunci când este detectat un fișier suspect, utilizatorilor le se va refuza accesul la acel fișier, pentru a preveni o potențială infecție.

Deși nu este recomandat, puteți modifica acțiunile implicite. Puteți defini două acțiuni pentru fiecare tip de fișier. Următoarele acțiuni sunt disponibile:

Interzice accesul
Interzice accesul la fișiere detectate.

Important
Pentru stații de lucru MAC, se implementează acțiunea **"Mută în carantină"** în loc de **"Interzice accesul"**.

Dezinfectează
Elimină codul periculos din fișierele infectate. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate.

Ștergere
Ștergeți fișierele detectate de pe disc, fără nicio avertizare. Se recomandă să evitați această acțiune.

Mută fișierele în carantină
Mutați fișierele detectate din locația curentă, în folderul de carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Fișierele în carantină pot fi gestionate de pe pagina Carantină a consolei.

Nicio acțiune
Raportează numai fișierele infectate detectate de Bitdefender.

Fila **Avansat** face referire la scanarea la accesare pentru mașinile Linux. Utilizați caseta de selecție pentru a-l activa sau opri.

În tabelul de mai jos puteți configura directoarele Linux pe care doriți să le scanați. În mod implicit, există cinci intrări, fiecare corespunzând unei locații specifice pe stațiile de lucru: `/home`, `/bin`, `/sbin`, `/usr` `/etc`.

Pentru a adăuga mai multe înregistrări:

- Introduceți numele oricărei locații în câmpul de căutare, în partea de sus a tabelului.
- Selectați directoarele predefinite din lista afișată atunci când executați clic pe săgeata din capătul din dreapta al câmpului de căutare.

Executați clic pe butonul ⊕ **Adăugare** pentru a salva o locație în tabel și pe butonul ⊗ **Ștergere** pentru a o elimina.

Vaccin anti-ransomware

Vaccinul anti-ransomware vă imunizează mașinile împotriva programelor ransomware **cunoscute** blocând procesul de criptare chiar dacă calculatorul este infectat. Utilizați caseta de selecție pentru a activa sau dezactiva protecția Vaccin anti-ransomware.

Funcția Vaccin anti-ransomware este dezactivată în mod implicit. Bitdefender Labs analizează comportamentul programelor ransomware larg răspândite și noile semnături sunt livrate odată cu fiecare actualizare de conținut de securitate pentru a asigura protecție împotriva celor mai recente amenințări.

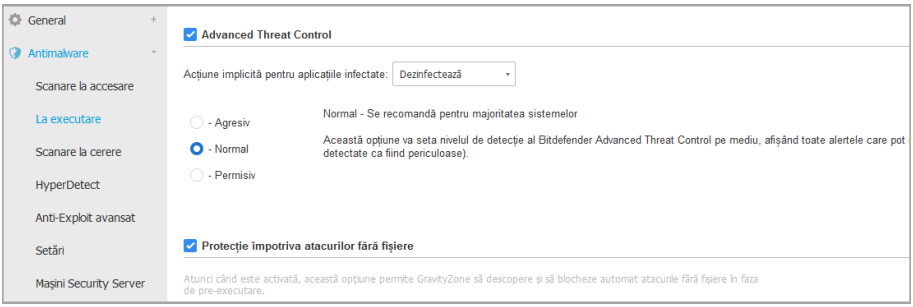
Avertisment
Pentru a crește și mai mult protecția împotriva infecțiilor ransomware, fiți precauți în legătură cu atașamentele nesolicitate sau suspecte și asigurați-vă că baza de date de conținut de securitate este actualizată.

Notă
Funcția Vaccin anti-ransomware este disponibilă doar în Bitdefender Endpoint Security Tools pentru Windows.

La executare

În această secțiune puteți configura protecția împotriva proceselor periculoase atunci când acestea sunt executate. Secțiunea acoperă următoarele niveluri de protecție:

- Detecție a amenințărilor bazată pe Cloud
- Advanced Threat Control
- Protecție împotriva atacurilor fără fișiere
- Remediere ransomware



Politici - Setări la executare

Advanced Threat Control

Notă

Acest modul este disponibil pentru:

- Windows pentru stații de lucru
- Windows pentru servere
- macOS

Bitdefender Advanced Threat Control este o tehnologie de detecție proactivă, care utilizează metode euristice avansate pentru a detecta noi potențiale amenințări în timp real.

Modulul Advanced Threat Control monitorizează continuu aplicațiile care rulează pe stația dumneavoastră de lucru, căutând acțiuni periculoase. Fiecare dintre aceste acțiuni are un anumit punctaj iar punctajul global este calculat pentru fiecare proces. În cazul în care scorul total pentru un proces atinge un anumit prag, procesul este considerat a fi dăunător.

Advanced Threat Control va încerca automat să dezinfecteze fișierul detectat. Dacă procedura de dezinfecție eșuează, Advanced Threat Control va șterge fișierul.

Notă

Înainte de a aplica acțiunea de dezinfectare, o copie a fișierului este trimisă în carantină, pentru ca dvs. să puteți recupera fișierul mai târziu, în cazul unui rezultat fals pozitiv. Acțiunea poate fi configurată folosind opțiunea **Copiere fișiere în carantină înaintea aplicării acțiunii de dezinfectare** din fila **Setări Antimalware >** a setărilor politicii. Această opțiune este activată implicit în modelul politicii.

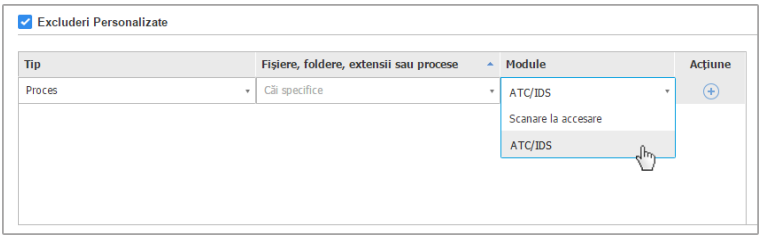
Pentru a configura Advanced Threat Control:

1. Utilizați caseta de selecție pentru a activa sau opri Advanced Threat Control.

Avertisment
Dacă opriți Advanced Threat Control, computerele vor fi vulnerabile la programele periculoase necunoscute.

2. Acțiunea implicită pentru aplicațiile infectate detectate de Advanced Threat Control este dezinfectarea. Puteți seta o altă acțiune implicită, folosind meniul disponibil.
   - **Blocare**, pentru a bloca accesul la aplicația infectată.
   - **Nu lua măsuri**, pentru a raporta doar aplicațiile infestate detectate de Bitdefender.
3. Clic pe nivelul de protecție care se potrivește cel mai bine nevoilor dumneavoastră (**Agresiv, Normal sau Permisiv**). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

Notă
După ce setați un nivel de protecție superior, Advanced Threat Control va necesita mai puține semne de comportament tipic malware pentru a raporta un anumit proces. Acest lucru va contribui la raportarea unui număr mai mare de aplicații și, în același timp, la o probabilitate sporită de false pozitive (aplicații legitime detectate ca fiind nocive).
Se recomandă creați reguli de excludere pentru aplicațiile utilizate frecvent sau cunoscute pentru a preveni alarmele false (detectarea greșită de aplicații legitime). Accesați secțiunea Setări Antimalware > și configurați regulile ATC/SD pentru excluderi de procese pentru aplicațiile de încredere.



Politici referitoare la calculatoare și mașinile virtuale - excepții proces ATC/IDS

Protecție împotriva atacurilor fără fișiere

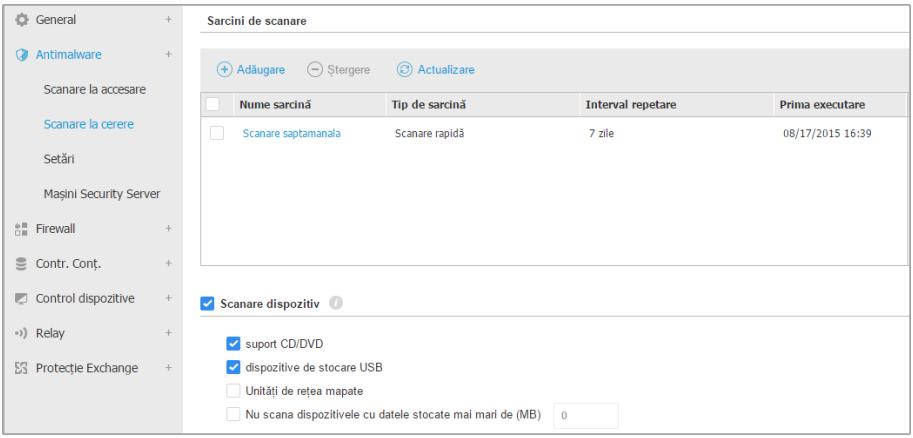
Notă
Acest modul este disponibil pentru:

- Windows pentru stații de lucru
- Windows pentru servere

Protecția împotriva atacurilor fără fișiere detectează și blochează malware-ul fără fișiere, inclusiv oprind PowerShell-uri care rulează linii de comandă periculoase, blocând traficul periculos, analizând buffer-ul de memorie înainte de injectarea codului și blocând procesul de injectare a codului.

Scanare la cerere

În această secțiune puteți adăuga și configura sarcini de scanare antimalware, care vor rula în mod regulat pe calculatoarele țintă, în funcție de programul definit.



Politici referitoare la calculatoare și mașini virtuale - Sarcini de scanare la cerere

Scanarea se efectuează în mod silențios, în fundal, indiferent dacă utilizatorul este sau nu autentificat în sistem.

Deși nu este obligatoriu, este recomandat să programați rularea unei scanări complete de sistem o dată pe săptămână pe toate stațiile de lucru. Scanarea stațiilor de lucru în mod regulat este o măsură de securitate proactivă, care pot

ajuta la detectarea și blocarea malware-ului care s-ar putea sustrage caracteristicilor de protecție în timp real.

În afară de scanările periodice, puteți configura și detectarea automată și scanarea mijloacelor externe de stocare.

Administrarea sarcinilor de scanare

Tabelul Scan Tasks vă informează cu privire la sarcinile de scanare existente, furnizând informații importante despre fiecare dintre ele:

- Numele și tipul sarcinii.
- Program pe baza căruia sarcina rulează regulat (recurență).
- Momentul când a fost rulată sarcina pentru prima dată.

Puteți adăuga și configura următoarele tipuri de sarcini de scanare:

- **Scanare rapidă** utilizează scanarea în cloud pentru a detecta malware-ul care rulează pe sistem. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o mică parte din resursele de sistem necesare pentru o scanare antivirus obișnuită.

  Atunci când se detectează programe malware sau rootkit-uri, Bitdefender începe automat procesul de dezinfectare. Dacă, din orice motiv, fișierul nu poate fi dezinfectat, atunci acesta este mutat în carantină. Acest tip de scanare ignoră fișierele suspecte.

  Scanarea rapidă este o sarcină implicită de scanare cu opțiuni preconfigurate, care nu pot fi modificate. Puteți adăuga o singură sarcină de scanare rapidă pentru aceeași politică.

- **Scanare completă** verifică întreaga stație de lucru pentru identificarea tuturor tipurilor de malware care îi amenință siguranța, cum ar fi virușii, aplicațiile spion, adware, rootkit-uri și altele.

  Bitdefender încearcă automat să dezinfecteze fișierele detectate ca fiind infectate cu malware. În cazul în care malware-ul nu poate fi eliminat, acesta este mutat în carantină, unde nu poate face niciun rău. Fișierele suspecte sunt ignorate. Dacă doriți să întreprindeți acțiuni și asupra fișierelor suspecte sau dacă doriți alte acțiuni implicite pentru fișierele infectate, selectați efectuarea unei Scanări personalizate.

Scanarea completă este o sarcină implicită de scanare cu opțiuni preconfigurate, care nu pot fi modificate. Puteți adăuga o singură sarcină de scanare completă pentru aceeași politică.

- **Scanare personalizată** vă permite să alegeți locațiile specifice care trebuie scanate și să configurați opțiunile de scanare.
- **Scanare rețea** este un tip de scanare personalizată, care permite alocarea unei singure stații de lucru administrate pentru scanarea unităților din rețea și apoi configurarea opțiunilor de scanare și locațiilor specifice care urmează să fie scanate. Pentru sarcinile de scanare a rețelei, trebuie să introduceți datele de autentificare ale unui cont de utilizator cu permisiuni de citire/editare pe unitățile rețelei țintă, pentru ca agentul de securitate să poată accesa și să inițieze acțiuni în cadrul acestor unități de rețea.

  Sarcina recurentă de scanare a rețelei va fi transmisă exclusiv către stația de lucru de scanare. Dacă stația de lucru selectată nu este disponibilă, se vor aplica setările locale de scanare.

  Notă
  Puteți crea sarcini de scanare în rețea doar cu o politică aplicată deja unei stații de lucru care poate fi utilizată ca scanner.

Pe lângă sarcinile de scanare implicite (care nu pot fi șterse sau duplicate), aveți posibilitatea de a crea câte sarcini de scanare personalizate și de rețea doriți.

Pentru a crea și a configura o nouă sarcină de scanare personalizată sau de rețea, faceți clic pe butonul ⊕ **Adăugare** din partea dreaptă a tabelului. Pentru a modifica setările unei sarcini de scanare existente, faceți clic pe numele sarcinii respective. Consultați următorul subiect pentru a afla modalitatea de configurare a setărilor sarcinii.

Pentru a elimina o sarcină din listă, selectați sarcina și faceți clic pe butonul ⊖ **Ștergere** din partea dreaptă a tabelului.

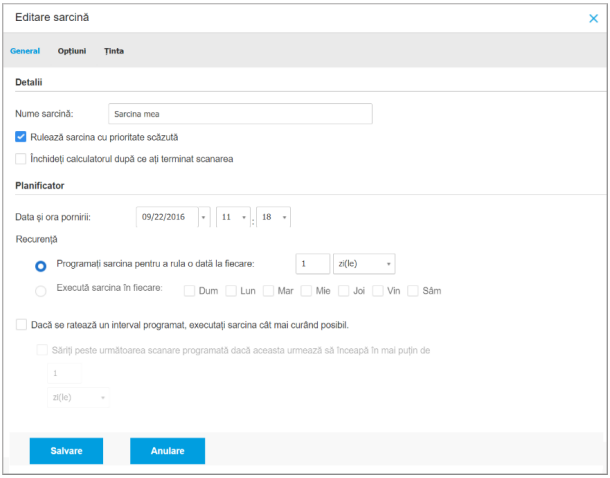
Configurarea sarcinilor de scanare

Setările sarcinii de scanare sunt organizate în trei file:

- **General**: se stabilește numele sarcinii și graficul de execuție.
- **Opțiuni**: se alege un profil de scanare pentru configurarea rapidă a setărilor de scanare și se definesc setările de scanare pentru o scanare personalizată.

- **Țintă**: selectați fișierele și directoarele pe care doriți să le scanați și definiți excepțiile de scanare.

Opțiunile sunt descrise în continuare de la prima până la ultima secțiune:



Politici pentru calculatoare și mașini virtuale - Configurarea setărilor generale ale sarcinilor de scanare la cerere

- **Detalii.** Alegeți o denumire sugestivă pentru sarcină care să vă ajute la identificarea cu ușurință la ce se referă. Atunci când alegeți un nume, luați în considerare obiectivul sarcinii de scanare și, eventual, setările de scanare.

  În mod implicit, sarcinile de scanare sunt executate în ordinea descrescătoare a priorității. Astfel, Bitdefender permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va crește. Bifați caseta **Executare sarcină cu prioritate redusă** pentru dezactivarea sau reactivarea acestei funcții.

  Notă
  Această opțiune se aplică doar pentru Bitdefender Endpoint Security Tools și Endpoint Security (agent legacy).

  Selectați caseta **Opriți calculatorul la terminarea scanării** pentru a opri calculatorul dacă intenționați să nu îl utilizați pentru o perioadă.

Notă
Această opțiune se aplică pentru Bitdefender Endpoint Security Tools, Endpoint Security (agent legacy) și Endpoint Security for Mac.

- **Planificator.** Folosiți opțiunile de planificare pentru a configura programul de scanare. Puteți seta ca scanarea să ruleze la fiecare câteva ore, zile sau săptămâni, începând cu o anumită dată și oră.

  Stațiile de lucru trebuie să fie pornite în momentul în care este programată scanarea. Scanarea programată nu va funcționa conform programului în cazul în care calculatorul este oprit, în hibernare sau în modul sleep. În astfel de situații, scanarea va fi amânată până data viitoare.

  Notă
  Scanare programată va rula la ora locală a punctului terminus. De exemplu, în cazul în care scanarea programată este setată să pornească la ora 18:00, ăi punctul terminus se află pe un fus orar diferit față de Control Center, scanarea va începe la ora 18:00 (ora punctului terminus).

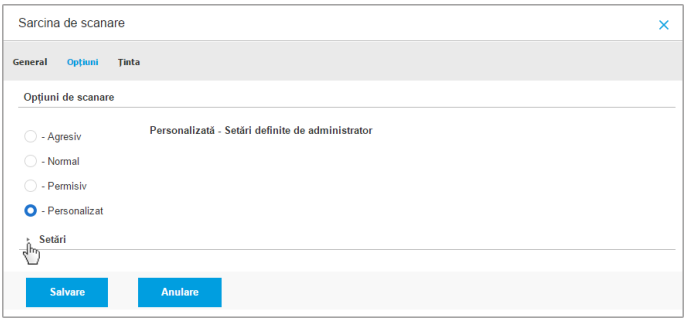
  Opțional, puteți specifica ce se întâmplă când sarcina de scanare poate să nu pornească la momentul programat (stația de lucru a fost offline sau oprită). Utilizați opțiunea **Dacă se ratează un interval programat, executați sarcina cât mai curând posibil** conform necesităților dumneavoastră:

  – Când lăsați opțiunea nebifată, sarcina de scanare va încerca să ruleze din nou la următorul interval programat.

  – Când selectați opțiunea, forțați scanarea să ruleze cât mai curând posibil. Pentru a optimiza intervalul de rulare a scanării și a evita perturbarea utilizatorului în timpul orelor de muncă, selectați **Omiteți dacă următoarea scanare programată va începe în mai puțin de**, apoi specificați intervalul dorit.

- **Opțiuni de scanare.** Faceți clic pe nivelul de securitate care corespunde cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

  În funcție de profilul selectat, opțiunile de scanare din secțiunea **Setări** sunt configurate automat. Cu toate acestea, dacă doriți, le puteți configura detaliat. În acest scop, selectați caseta de bifare **Personalizat** și mergeți la secțiunea **Setări**.



Sarcină de scanare calculatoare - Configurarea unei scanări personalizate

- **Tipuri de fișiere.** Folosiți aceste opțiuni pentru a specifica tipurile de fișiere pe care doriți să le scanați. Puteți seta agentul de securitate să scaneze toate fișierele (indiferent de extensie), fișierele de aplicație sau extensiile specifice de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor asigură cea mai bună protecție în timp ce scanarea aplicațiilor poate fi utilizată pentru efectuarea unei scanări mai rapide.

  Notă

  Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Tipuri de fișiere de aplicații” (p. 567).

  Dacă doriți să fie scanate doar extensii specifice, alegeți **Extensii definite de utilizator** din meniu și apoi introduceți extensiile în câmpul de editare și apăsați `Enter` după fiecare extensie.

- **Arhive.** Arhivele cu fișiere infestate nu sunt o amenințare directă pentru securitatea sistemului. Programele periculoase pot afecta sistemul numai dacă fișierul infestat este extras din arhivă și executat fără ca protecția în timp real să fie activată. Cu toate acestea, se recomandă să utilizați această opțiune pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

  Notă

  Scanarea fișierelor arhivate crește timpul total necesar pentru scanare și necesită mai multe resurse de sistem.

- **Scanare în arhive.** Selectați această opțiune dacă doriți să scanați fișierele arhivate, pentru identificarea de malware. Dacă decideți să utilizați această opțiune, puteți configura următoarele opțiuni de optimizare:
  - **Limitare dimensiune arhivă la (MB).** Puteți seta o dimensiune limită acceptată pentru arhivele care vor fi scanate. Selectați căsuța corespunzătoare și introduceți dimensiunea maximă a arhivei (exprimată în MB).
  - **Adâncime maximă arhivă (niveluri).** Selectați caseta de bifare corespunzătoare și alegeți adâncimea maximă a arhivei din meniu. Pentru performanțe superioare, alegeți cea mai mică valoare; pentru protecție maximă, alegeți cea mai mare valoare.
- **Scanare arhive de e-mail.** Selectați această opțiune dacă doriți să activați scanarea fișierelor atașate la mesajele e-mail și bazele de date e-mail, inclusiv format de fișiere de tipul .eml, .msg, .pst, .dbx, .mbx, .tbb și altele.

  Notă
  Scanarea arhivei e-mail necesită numeroase resurse și poate afecta performanțele sistemului.

- **Diverse.** Selectați casetele de bifare corespunzătoare pentru a activa opțiunile de scanare dorite.
  - **Scanare sectoare de boot.** Scanează sectoarele de boot ale sistemului. Acest sector al hard disk-ului conține codul necesar pentru a iniția procesul de boot. Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.
  - **Scanează regiștrii.** Selectați această opțiune pentru a scana cheile de regiștri. Regiștrii Windows sunt o bază de date care stochează setările de configurare și opțiunile pentru componentele sistemului de operare Windows, precum și pentru aplicațiile instalate.
  - **Scanează după rootkituri.** Selectați această opțiune pentru a lansa procesul de scanare pentru identificarea rootkit-urilor și a obiectelor ascunse, cu ajutorul acestui software.
  - **Scanare după keyloggers.** Selectați această opțiune pentru a scana software-urile de tip keylogger.

- **Scanează directoare comune din rețea.** Această opțiune scanează unități de rețea montate.

  Pentru scanările rapide, această opțiune este dezactivată în mod implicit. Pentru scanări complte, este activată în mod implicit. Pentru scanări personalizate, dacă setați nivelul de securitate pe **Agresiv/Normal**, opțiunea **Scanare directoare comune din rețea** este activată automat. Dacă setați nivelul de securitate pe **Permisiv**, opțiunea **Scanare directoare comune din rețea** este dezactivată automat.

- **Scanează memoria.** Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului.

- **Scanează fișiere cookie.** Selectați această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe stația de lucru.

- **Scanează doar fișierele noi și cele modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.

- **Scanare pentru aplicații potențial nedorite (PUA).** O aplicație potențial nedorită (PUA) este un program care ar putea fi nedorit pe PC, care uneori vine la pachet cu software-ul freeware. Astfel de programe pot fi instalate fără consimțământul utilizatorului (numite și adware), sau vor fi incluse în mod implicit în kit-ul de instalare în mod expres (ad-supported). Efectele potențiale ale acestor programe includ afișarea de pop-up-uri, instalarea de bare de instrumente nedorite în browser-ul implicit sau rularea mai multor procese în fundal și încetinirea performanței PC-ului.

- **Acțiuni.** În funcție de tipul de fișier detectat, următoarele acțiuni sunt aplicate în mod automat:

  - **Acțiune implicită pentru fișierele infectate.** Bitdefender detectează fișierele ca fiind infectate folosind diverse mecanisme avansate, printre care semnăturile malware, învățarea automată și tehnologiile bazate pe inteligență artificială (AI). În mod normal, agentul de securitate poate șterge codul malware din fișierul infectat și poate reconstitui fișierul inițial. Această operațiune este cunoscută sub denumirea de dezinfectare.

    În cazul în care este detectat un fișier infectat, agentul de securitate va încerca în mod automat să-l dezinfecteze. Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

Important
Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

– **Acțiune implicită pentru fișierele suspecte.** Fișierele sunt detectate ca fiind suspecte de către analiza euristică și alte tehnologii Bitdefender. Acestea asigură o rată mare de detecție, însă utilizatorii trebuie să fie conștienți că există și rezultate fals pozitive (fișiere neinfectate detectate ca fiind suspecte) în unele cazuri. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

  Sarcinile de scanare sunt configurate implicit să ignore fișierele suspecte. Ar putea fi util să modificați sarcina implicită, pentru a trece fișierele suspecte sub carantină. Fișierele sub carantină sunt transmise regulat spre analiză la Laboratoarele Bitdefender. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

– **Acțiune implicită pentru rootkit-uri.** Rootkit-urile reprezintă aplicații specializate utilizate pentru ascunderea fișierelor de sistemul de operare. Deși nu sunt periculoase, rootkit-urile sunt adesea utilizate pentru ascunderea programelor periculoase sau pentru a disimula prezența unui intrus în sistem.

  Rootkit-urile și fișierele ascunse detectate sunt ignorate implicit.

Deși nu este recomandat, puteți modifica acțiunile implicite. Puteți preciza o a doua acțiune de aplicat în cazul în care prim eșuează, precum și acțiuni diferite pentru fiecare categorie. Alegeți din meniurile corespunzătoare prima și a doua acțiune de aplicat pentru fiecare tip de fișier detectat. Următoarele acțiuni sunt disponibile:

Nicio acțiune
Nu se vor lua niciun fel de măsuri împotriva fișierelor detectate. Aceste fișiere vor fi doar afișate în jurnalul de scanare.

Dezinfectează
Elimină codul periculos din fișierele infectate. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate.

Ștergere
Ștergeți fișierele detectate de pe disc, fără nicio avertizare. Se recomandă să evitați această acțiune.

Mută fișierele în carantină

Mutați fișierele detectate din locația curentă, în folderul de carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Fișierele în carantină pot fi gestionate de pe pagina Carantină a consolei.

- **Țintă scanare.** Adăugați la listă de toate locațiile care doriți să fie scanate pe calculatoarele țintă.

  Pentru a adăuga un nou fișier sau un folder care să fie scanat:

  1. Selectați o locație predefinită din meniul derulant sau introduceți **Căi specifice** pe care doriți să le folosiți.
  2. Specificați calea către obiectul de scanat în câmpul de editare.
     - Dacă ați ales o locație predefinită, completați calea, după caz. De exemplu, pentru a scana integral folderul `Program Files`, este suficient să selectați locația predefinită corespunzătoare din meniul derulant. Pentru a scana un anumit folder din `Program Files`, trebuie să completați calea adăugând o bară oblică inversă (\) și denumirea folderului.
     - Dacă ați selectat **Căi specifice**, introduceți calea completă către obiectul de scanat. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.
  3. Faceți clic pe butonul ⊕ **Adăugare** corespunzător.

  Pentru a edita o locație existentă, faceți clic pe aceasta. Pentru a șterge o locație din listă, deplasați cursorul peste aceasta și faceți clic pe butonul ⊖ **Ștergere** corespunzător.

- Pentru sarcinile de scanare a rețelei, trebuie să introduceți datele de autentificare ale unui cont de utilizator cu permisiuni de citire/editare pe unitățile rețelei țintă, pentru ca agentul de securitate să poată accesa și să inițieze acțiuni în cadrul acestor unități de rețea.

- **Excluderi.** Puteți utiliza excepțiile definite în secțiunea **Antimalware > Excluderi** a politicii curente au puteți defini excluderile personalizate pentru sarcina de scanare curentă. Pentru detalii referitoare la excepții, consultați „Excluderi” (p. 289).

Scanare dispozitiv

Puteți configura agentul de securitate pentru a detecta automat și scana dispozitivele de stocare externe atunci când acestea sunt conectate la stația de lucru. Unitățile detectate fac parte din următoarele categorii:

- CD-uri/DVD-uri
- unități de stocare pe USB, cum ar fi memoriile flash sau hard discurile externe
- Dispozitive cu mai mult de o anumită sumă de date stocate.

Scanările dispozitivului încercă automat să dezinfecteze fișierele detectate ca fiind infectate sau să le mute în carantină dacă dezinfectarea nu este posibilă. Vă atragem atenția asupra faptului că unele dispozitive, cum ar fi CD-urile/DVD-urile, sunt needitabile (read-only). Nu poate fi demarată nicio acțiune pentru fișierele infectate de pe astfel de locații de stocare.

Notă
În timpul scanării dispozitivului, utilizatorul poate accesa orice date de pe dispozitiv.

Dacă sunt activate alertele pop-up în secțiunea **General > Notificări**, utilizatorului i se solicită să precizeze dacă dorește sau nu să scaneze dispozitivul detectat, în locul pornirii automate a scanării.

Atunci când este pornită scanarea unui dispozitiv:

- O notificare de tip pop-up informează utilizatorul cu privire la scanarea dispozitivului, cu condiția ca notificările de tip pop-up să fie activate în secțiunea **General > Notificări**.

După finalizarea scanării, utilizatorul trebuie să verifice amenințările detectate, dacă este cazul.

Selectați opțiunea **Scanare dispozitive** pentru a activa detectarea și scanarea automată a dispozitivelor de stocare. Pentru a configura scanarea dispozitivului individual pentru fiecare tip de dispozitiv, folosiți următoarele opțiuni:

- **suport CD/DVD**
- **dispozitive de stocare USB**
- **Nu scana dispozitivele cu datele stocate mai mari de (MB)**. Utilizați această opțiune pentru a evita automat scanarea unui dispozitiv detectat în cazul în care cantitatea de date stocate depășește dimensiunea specificată. Introduceți

limita de dimensiune (în megabytes) în câmpul corespunzător. Zero semnifică neimpunerea nici unei restricții de dimensiuni.

HyperDetect

Notă
Acest modul este disponibil pentru:

- Windows pentru stații de lucru
- Windows pentru servere
- Linux

HyperDetect adaugă un nivel suplimentar de securitate la tehnologiile de scanare existente (Scanare la accesare, Scanare la cerere și Scanare trafic), pentru a lupta împotriva noii generații de atacuri cibernetice, inclusiv amenințările avansate persistente. HyperDetect îmbunătățește modulele de protecție Antimalware și Control conținut cu metodele sale euristice puternice bazate pe inteligență artificială și învățare automată.

Cu abilitatea sa de a intui atacurile targetate și de a detecta cele mai sofisticate programe malware în stadiul de preexecuție, HyperDetect expune amenințările mult mai repede decât tehnologiile de scanare bazate pe semnătură sau comportament.

Pentru configurarea HyperDetect:

1. Utilizați caseta **HyperDetect** pentru a activa sau a dezactiva modulul.
2. Selectați tipul de amenințare față de care doriți să oferiți protecție rețelei dvs. Protecția este activată implicit pentru toate tipurile de amenințări: atacuri targetate, fișiere suspecte și trafic de rețea, exploatări, ransomware sau grayware.

   Notă
   Modelul euristic pentru traficul de rețea necesită ca funcțiile de **Control conținut > Scanare trafic** să fie active.

3. Personalizați nivelul de protecție împotriva amenințărilor din categoriile selectate.

   Utilizați butonul principal din partea superioară a listei de amenințări pentru a selecta un nivel unic de protecție pentru toate tipurile de amenințări sau pentru a selecta niveluri individuale pentru a regla protecția.

Setarea modulului la un anumit nivel va duce la anumite acțiuni ce vor fi întreprinse până la nivelul respectiv. De exemplu, dacă este setat la nivelul **Normal**, modulul detectează și blochează amenințările care declanșează pragurile **Permisiv** și **Normal**, dar nu și pe cel **Agresiv**.

Nivelul de protecție crește de la **Permisiv** la **Agresiv**.

Rețineți că un nivel agresiv de detecție poate duce la rezultate fals pozitive, în timp ce un nivel permisiv poate expune rețeaua dvs. la anumite amenințări. Se recomandă ca inițial să setați nivelul de protecție la maxim și apoi să îl scădeți în cazul în care primiți multe rezultate fals pozitive, până când atingeți nivelul optim de echilibru.

Notă
Oricând activați protecția pentru un tip de amenințări, detecția este setată automat la valoarea implicită (nivel **Normal**).

4. În secțiunea **Acțiuni**, configurați modul de reacție la amenințări al HyperDetect. Utilizați opțiunile din lista derulantă pentru a seta acțiunile care vor fi întreprinse cu privire la amenințări:
   - Pentru fișiere: blocare acces, dezinfectare, ștergere, carantină sau doar raportare fișier.
   - Pentru trafic de rețea: blocare sau doar raportare trafic suspect.
5. Selectați caseta **Extindere raportare la nivelurile superioare** de lângă meniul derulant dacă doriți să vizualizați amenințările detectate la niveluri de protecție mai ridicate decât cele setate.

Dacă nu sunteți sigur cu privire la configurația actuală, puteți reveni cu ușurință la setările inițiale efectuând clic pe butonul **Revenire la valorile implicite** din partea de jos a paginii.

Anti-Exploit avansat

Notă
Acest modul este disponibil pentru:
- Windows pentru stații de lucru

Modulul Anti-exploit avansat este o tehnologie proactivă care detectează exploit-urile în timp real. Bazându-se pe învățarea cu ajutorul mașinilor, protejează

împotriva unei serii de exploit-uri cunoscute și necunoscute, inclusiv atacuri fără fișier asupra memoriei.

Pentru a activa protecția împotriva exploit-urilor, selectați căsuța **Anti-Exploit avansat**.

Modulul Anti-exploit avansat este setat să ruleze cu setările recomandate. Puteți regla protecția diferit, dacă este necesar. Pentru a restabili setările inițiale, efectuați clic pe link-ul **Resetare la modul implicit** din partea dreaptă a titlului secțiunii.

GravityZone dispune de setările anti-exploit organizate în trei secțiuni:

- **Detecții la nivelul întregului sistem**

  Tehnicile anti-exploit din această secțiune monitorizează procesele de sistem care reprezintă țintele exploit-urilor.

  Pentru a afla mai multe informații despre tehnicile disponibile și cum puteți configura setările acestora, consultați „Configurare diminuare la nivelul sistemului” (p. 282).

- **Aplicații predefinite**

  Modulul Anti-exploit avansat este preconfigurat cu o listă de aplicații obișnuite, cum ar fi Microsoft Office, Adobe Reader sau Flash Player, care sunt cele mai expuse exploatărilor.

  Pentru a afla mai multe informații despre tehnicile disponibile și cum puteți configura setările acestora, consultați „Configurarea tehnicilor specifice aplicațiilor” (p. 283).

- **Aplicații suplimentare**

  Din această secțiune, puteți adăuga și configura protecție pentru oricâte aplicații suplimentare doriți.

  Pentru a afla mai multe informații despre tehnicile disponibile și cum puteți configura setările acestora, consultați „Configurarea tehnicilor specifice aplicațiilor” (p. 283).

Puteți extinde sau restrânge fiecare secțiune printr-un clic pe titlul acesteia. Astfel, veți ajunge rapid la setările pe care doriți să le configurați.

Configurare diminuare la nivelul sistemului

În această secțiune, aveți următoarele opțiuni:

Tehnică	Descriere
Elevare de privilegii	Împiedică obținerea de către procese a unor privilegii neautorizate și a accesului la resurse. Acțiune implicită: Oprește procesul
Protecție proces LSASS	Protejează procesul LSASS împotriva scurgerii de informații secrete, cum ar fi valorile hash ale parolelor și setările de securitate. Acțiune implicită: Blochează procesul

Aceste tehnici anti-exploit sunt activate în mod implicit. Pentru a dezactiva oricare dintre acestea, debifați căsuța aferentă.

Opțional, puteți modifica acțiunea întreprinsă automat în momentul detectării. Selectați o acțiune disponibilă din meniul asociat:

- **Oprește procesul**: oprește imediat procesul exploatat.
- **Blochează procesul**: previne accesarea de către procesul malițios a resurselor neautorizate.
- **Doar raportare**: GravityZone raportează evenimentul fără a lua nicio măsură de diminuare. Puteți vizualiza detaliile evenimentului în notificarea **Anti-Exploit avansat**, și în rapoartele Aplicații blocate și Audit de securitate.

Configurarea tehnicilor specifice aplicațiilor

Indiferent dacă sunt aplicații predefinite sau suplimentare, toate împărtășesc același set de tehnici anti-exploit. Le puteți găsi descrierea în această secțiune:

Tehnică	Descriere
Emulare ROP	Detectează încercările de a face pagini de memorie executabile pentru date, utilizând tehnica Return-Oriented Programming (ROP - Programare orientată invers). Acțiune implicită: Oprește procesul
Pivot stivă ROP	Detectează încercările de furt a fluxului de cod utilizând tehnica ROP, prin validarea localizării stivei. Acțiune implicită: Oprește procesul

Tehnică	Descriere
Apelare ilegală ROP	Detectează încercările de furt a fluxului de cod utilizând tehnica ROP, prin validarea apelării funcțiilor sensibile de sistem. Acțiune implicită: Oprește procesul
Stivă ROP aliniată incorect	Detectează încercările de corupere a stivei utilizând tehnica ROP, prin validarea alinierii adresei stivei. Acțiune implicită: Oprește procesul
Revenire la stivă ROP	Detectează încercările de executare a codului direct pe stivă utilizând tehnica ROP, prin validarea gamei adresei de retur. Acțiune implicită: Oprește procesul
ROP Setare stivă ca fișier executabil	Detectează încercările de corupere a stivei utilizând tehnica ROP, prin validarea protecției paginii stivei. Acțiune implicită: Oprește procesul
Flash Generic	Detectează încercările de exploatare Flash Player. Acțiune implicită: Oprește procesul
Flash Payload	Detectează încercările de executare a codului malițios în Flash Player, prin scanarea obiectelor Flash în memorie. Acțiune implicită: Oprește procesul
VBScript Generic	Detectează încercările de exploatare VBScript. Acțiune implicită: Oprește procesul
Executare Shellcode	Detectează încercările de creare a unor noi procese sau fișiere de descărcare, utilizând cod shell. Acțiune implicită: Oprește procesul
Shellcode LoadLibrary	Detectează încercările de executare a codului prin intermediul căilor de rețea, utilizând cod shell. Acțiune implicită: Oprește procesul
Anti-redirecționare	Detectează încercările de a trece de verificările de securitate pentru crearea de noi procese. Acțiune implicită: Oprește procesul

Tehnică	Descriere
Shellcode EAF (Filtrare adrese de export)	Detectezî încercările codului malițios de a accesa funcții sensibile de sistem din exporturile DLL. Acțiune implicită: Oprește procesul
Fir de execuție cod shell	Detectează încercările de injectare a codului malițios prin validarea firelor de execuție nou create. Acțiune implicită: Oprește procesul
Anti-Meterpreter	Detectează încercările de creare a unui shell invers, prin scanarea paginilor de memorie executabile. Acțiune implicită: Oprește procesul
Creare procese perimate	Detectează încercările de creare a proceselor noi utilizând tehnici învechite. Acțiune implicită: Oprește procesul
Creare procese subordonate	Blochează crearea oricărui proces copil. Acțiune implicită: Oprește procesul
Implementare Windows DEP	Activezaă Prevenirea Executării Datelor (DEP) pentru a bloca executarea codului din paginile de date. Implicit: Dezactivat
Implementare relocare modul (ASLR)	Împiedică încărcarea codului în locuri previzibile prin relocarea modulelor de memorie. Implicit: Activat
Exploit-uri apărute recent	Protejează împotriva oricăror amenințări sau exploit-uri apărute recent. Actualizările rapide sunt utilizate pentru această categorie înainte să poată fi efectuate modificări mai comprehensive. Implicit: Activat

Pentru a monitoriza alte aplicații cu excepția celor predefinite, efectuați clic pe butonul **Adăugare aplicație** disponibil în partea de sus și în partea de jos a paginii.

Pentru a configura setările anti-exploit pentru o aplicație:

1. Pentru aplicațiile existente, efectuați clic pe denumirea aplicației. Pentru aplicații noi, efectuați clic pe butonul **Adăugare**.

O pagină nouă afișează toate tehnicile și setările acestora pentru aplicația selectată.

Important
Fiți prudent când adăugați noi aplicații care urmează a fi monitorizate. Bitdefender nu poate garanta compatibilitatea cu orice aplicație. Prin urmare, se recomandă testarea acestei funcții mai întâi pe câteva stații de lucru non-critice, și abia apoi rularea acesteia în rețea.

2. Dacă adăugați o aplicație nouă, introduceți denumirea acesteia și denumirile proceselor în câmpurile dedicate. Folosiți caracterul punct și virgulă (;) pentru a separa denumirile proceselor.
3. Dacă aveți nevoie să verificați rapid descrierea unei tehnici, efectuați clic pe săgeata de lângă denumirea acesteia.
4. Selectați sau debifați căsuțele tehnicilor de exploatare, conform necesităților.

   Utilizați opțiunea **Toate** dacă doriți să marcați toate tehnicile simultan.
5. Dacă este necesar, modificați acțiunea automată de la momentul detectării. Selectați o acțiune disponibilă din meniul asociat:
   - **Oprește procesul**: oprește imediat procesul exploatat.
   - **Doar raportare**: GravityZone raportează evenimentul fără a lua nicio măsură de diminuare. Puteți vizualiza detaliile evenimentului în notificarea **Anti-Exploit avansat** și în rapoarte.

   Implicit toate tehnicile pentru aplicații predefinite sunt setate pentru a diminua problema, în timp ce pentru aplicațiile suplimentare, sunt setate doar să raporteze evenimentul.

   Pentru a modifica rapid acțiunea întreprinsă pentru toate tehnicile dintr-o dată, selectați acțiunea din meniul asociat cu opțiunea **Toate**.

Efectuați clic pe butonul **Înapoi** din partea superioară a paginii pentru a reveni la setările generale Anti-Exploit.

Setări

În această secțiune, puteți configura setările de carantină și regulile de excludere de la scanare.

- Configurarea setărilor carantinei

- Configurarea excluderilor de la scanare

Carantină

Puteți configura următoarele opțiuni pentru fișierele trecute în carantină de pe stațiile de lucru țintă:

- **Șterge fișierele mai vechi de (zile).** Implicit, fișierele aflate în carantină de mai mult de 30 de zile sunt șterse automat. Dacă doriți să schimbați acest interval, alegeți o altă opțiune din meniu.
- **Trimite fișierele trecute în carantină către Laboratoarele Bitdefender la (ore).** În mod implicit, fișierele trecute în carantină sunt transmise automat Laboratoarelor Bitdefender la intervale orare. Puteți edita intervalul de timp când sunt trimise fișierele aflate în carantină (o oră în mod implicit). Fișierele mostră vor fi analizate de către cercetătorii Bitdefender în materie de malware. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.
- **Rescanează carantina după actualizarea conținutului de securitate.** Păstrați această opțiune selectată pentru a scana automat fișierele aflate în carantină după fiecare actualizare a conținutului de securitate. Fișierele curățate sunt mutate automat în locația lor originală.
- **Copiază fișierele în carantină înainte de aplicarea acțiunii de dezinfectare.** Selectați această opțiune pentru a preveni pierderea de date în caz de pozitive false și copiați fiecare fișier detectat ca infectat în carantină înainte de a aplica acțiunea de dezinfectare. Ulterior puteți recupera fișiere legitime din pagina **Carantină**.
- **Permite utilizatorilor să acționeze în carantina locală.** Această opțiune controlează acțiunile pe care le pot întreprinde utilizatorii în fișierele aflate în carantină locală prin intermediul interfeței Bitdefender Endpoint Security Tools. În mod implicit,utilizatorii locali pot restaura sau șterge fișierele aflate în carantină locală pe computerele lor folosind opțiunile disponibile în Bitdefender Endpoint Security Tools. Dacă dezactivează această opțiune, utilizatorii nu vor mai avea acces la butoanele prin care să acționeze, prin interfața Bitdefender Endpoint Security Tools, asupra fișierelor aflate în carantină.

Carantină centralizată

Dacă doriți să păstrați fișierele aflate în carantină din stațiile de lucru pe care le administrați pentru a continua analiza lor, folosiți opțiunea **Carantină centralizată**

care trimite o copie arhivată a fișierelor locale aflate în carantină la un director comun din rețea.

După activarea acestei opțiuni, fiecare fișier aflat în carantină din stațiile de lucru administrate este copiat și arhivat într-o arhivă ZIP protejată cu parolă, în locația specificată din rețea. Numele arhivei este codul hash al fișierului aflat în carantină.

Important
Mărimea arhivei nu poate depăși 100 MB. Dacă arhiva depășește 100 MB, ea nu va fi salvată în locația partajată din rețea.

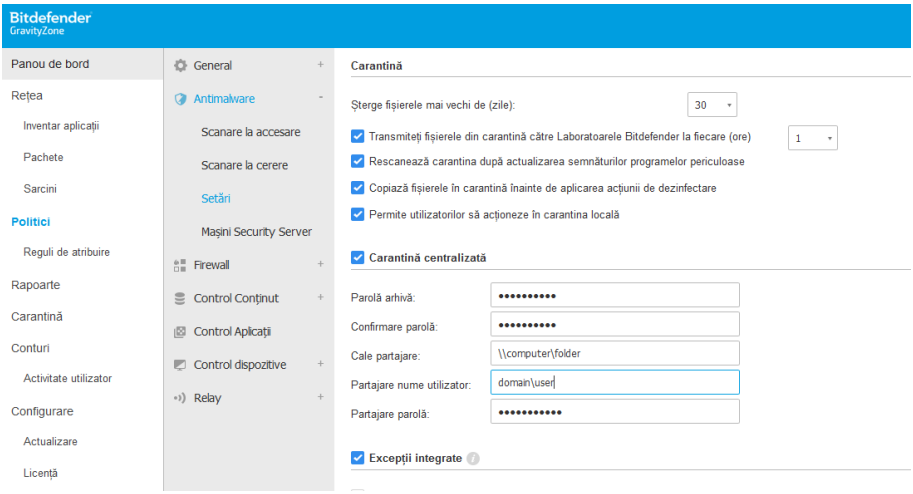
Pentru configurarea setărilor centralizate pentru carantină, completați următoarele câmpuri:

- **Parolă arhivă**: introduceți parola pentru arhiva cu fișiere aflate în carantină. Parola trebuie să includă cel puțin o literă mare, cel puțin o literă mică și cel puțin o cifră sau un caracter special. Confirmați parola în câmpul următor.
- **Partajare cale**: introduceți calea de rețea unde doriți să stocați arhivele (de exemplu, `\\computer\director`).
- Numele de utilizator și parola pentru conectare la partajarea din rețea. Formatele acceptate pentru acest nume de utilizator sunt următoarele:
  - `username@domain`
  - `domeniu \ nume de utilizator`
  - `nume de utilizator`.

Pentru funcționarea corectă a carantinei centralizate, asigurați-vă că au fost îndeplinite următoarele condiții:

- Locația partajată este accesibilă în rețea.
- Stațiile de lucru sunt conectate la directoarele comune din rețea.
- Datele de autentificare pentru conectare sunt valabile și oferă dreptul de scriere în partiția de rețea.
- Directorul comun din rețea are suficient spațiu pe disk.

Notă
Carantina centralizată nu este aplicabilă în cazul carantinei serverelor de mail.



Carantină centralizată

Dacă aveți o instanță locală Sandbox Analyzer configurată în secțiunea **Sandbox Analyzer > Senzor endpoint**, puteți bifa opțiunea **Trimiteți automat obiecte din carantină către un Sandbox Analyzer**. Vă informăm că obiectele trimise pot avea maxim 50 MB.

Excluderi

Agentul de securitate Bitdefender poate exclude anumite tipuri de obiecte din scanare. Excluderile de la scanarea programelor periculoase vor fi utilizate în cazuri speciale, sau la recomandarea Microsoft sau a Bitdefender. Pentru o listă actualizată a excluderilor recomandate de Microsoft, vă rugăm consultați acest articol.

În această secțiune, puteți configura utilizarea diferitelor tipuri de excepții disponibile cu agentul de securitate Bitdefender.

- **Excepțiile încorporate** sunt activate în mod implicit și incluse în agentul de securitate Bitdefender.

  Puteți opta pentru dezactivarea excluderilor implicite, dacă doriți să scanați toate tipurile de obiecte, însă această opțiune va afecta considerabil performanțele mașinii și va prelungi intervalul de scanare.

- Puteți de asemenea defini **Excluderi personalizate** pentru aplicații dezvoltate local sau pentru instrumente personalizate, în conformitate cu nevoile dumneavoastră specifice.

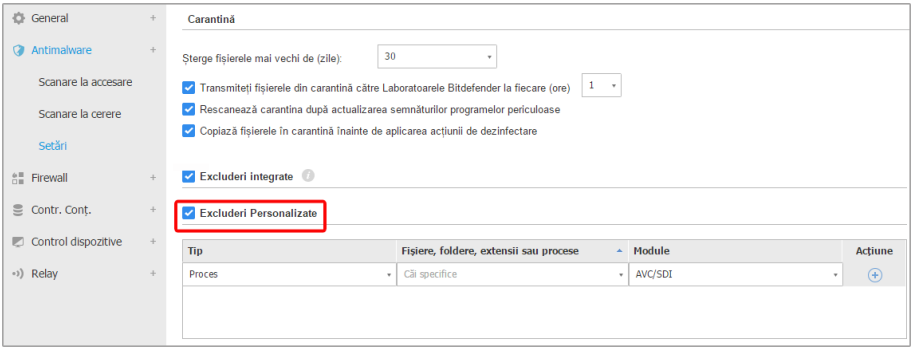
  Excluderile personalizate de la scanarea programelor periculoase se aplică pentru una sau mai multe dintre următoarele metode de scanare:

  – Scanare la accesare
  – Scanare la cerere
  – Advanced Threat Control
  – Protecție împotriva atacurilor fără fișiere

  Important

  – Dacă aveți un fișier cu un test EICAR pe care îl folosiți periodic pentru a testa protecția antimalware, este recomandat să-l excludeți de la scanarea la acces.
  – Dacă utilizați VMware Horizon View 7 și App Volumes AppStacks, consultați acest Document VMware.

  Pentru a exclude anumite elemente de la scanare, selectați opțiunea **Excluderi personalizate** și apoi adăugați regulile în tabelul de dedesubt.



Politici referitoare la calculatoare și mașini virtuale - Excepții personalizate

Pentru a adăuga o regulă de excludere personalizată:

1. Selectați tipul de excludere din meniu:
   – **Fișier**: numai fișierul specificat

- **Director**: toate fișierele și procesele din interiorul directorului specificat și din toate directoarele sale secundare
- **Extensie**: toate elementele care au extensia specificată
- **Proces**: orice obiect accesat de către procesul exclus
- **Hash fișier**: fișierul cu hash specificat
- **Hash certificat**: toate aplicațiile care au hash-ul specificat de certificat (amprentă)
- **Nume amenințare**: orice obiect cu numele detecției (indisponibil pentru sistemele de operare Linux)
- **Linia de comandă**: linia de comandă specificată (disponibilă doar pentru sistemele de operare Windows)

Avertisment
În mediile VMware fără agent integrate cu vShield, puteți exclude doar folderele și extensiile. Dacă instalați Bitdefender Tools pe mașinile virtuale, puteți exclude fișiere și procese.
În timpul procesului de instalare, când configurați pachetul, trebuie să bifați caseta **Implementează terminalul cu vShield dacă se detectează un mediu VMware integrat cu vShield**. Pentru informații suplimentare, consultați secțiunea **Crearea pachetelor de instalare** din Ghidul de instalare.

2. Furnizeazî detaliile specifice tipului de excludere selectat:

   Fișier, Director sau Proces

   Introduceți calea către elementul care va fi exclus de la scanare. Aveți câteva opțiuni ajutătoare pentru a scrie calea:

   - Declarați calea în mod explicit.

     De exemplu: `C:  emp`

     Pentru a adăuga excluderi pentru căile UNC, utilizați oricare dintre sintaxele următoare:

     `\\hostName\shareName\filePath`

     `\\IPaddress\shareName\filePath`

   - Utilizați variabilele de sistem disponibile în meniul derulant.

Pentru excluderi de proces, trebuie să adăugați și numele fișierului executabil al aplicației.

De exemplu:

`%ProgramFiles%` - exclude directorul Program Files

`%WINDIR%\system32` – exclude directorul system32 din directorul Windows

Notă
Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.

– Utilizați metacaractere.

Asteriscul (*) este substitut pentru zero sau mai multe caractere. Semnul de întrebare (?) este substitut pentru exact un caracter. Puteți folosi mai multe semne de întrebare pentru a defini orice combinație a unui anumit număr de caractere. De exemplu, ??? înlocuiește orice combinație de exact trei caractere.

De exemplu:

Excepții fișiere:

`C:\Test\*` – exclude toate fișierele din directorul Test

`C:\Test\*.png` – exclude toate fișierele PNG, din directorul Test

Excepții directoare:

`C:\Test\*` - exclude toate directoarele din directorul Test

Excepții procese:

`C:\Program Files\WindowsApps\Microsoft.Not??.exe` – exclude procesele Microsoft Notes.

Notă
Excepțiile procesate nu sunt compatibile cu metacaractere pe sistemele de operare Linux.

Extensie

Introduceți una sau mai multe extensii de fișiere care să fie excluse de la scanare, separându-le prin punct și virgulă ";". Puteți introduce extensii, cu

sau fără punctul care le precede. De exemplu, introduceți txt pentru a exclude fișierele text.

Notă
Pe sistemele Linux, extensiile de fișiere sunt sensibile la caracterele mici și mari, iar fișierele cu aceeași denumire dar extensie diferită sunt considerate obiecte distincte. De exemplu, `file.txt` este diferit de `file.TXT`.

Hash fișier, hash certificat, denumire amenințare sau linie de comandă

Introduceți codul hash al fișierului, amprenta certificatului (hash), denumirea exactă a amenințării sau linia de comandă în funcție de regula de excludere. Puteți utiliza un element pentru fiecare excludere.

3. Selectați metodele de scanare pentru care se aplică regula. Anumite excluderi pot fi relevante pentru scanarea la accesare, scanarea la cerere, ATC/IDS, în timp ce altele pot fi recomandate pentru toate cele trei module.
4. Opțional, efectuați clic pe butonul **Arată observații** pentru a adăuga o notă în coloana **Observații** cu privire la regulă.
5. Faceți clic pe butonul ⊕ **Adăugare**.

   Noua regulă va fi adăugată în listă.

Pentru a elimina o regulă din listă, faceți clic pe butonul ⊗ **Ștergere**.

Important
Vă rugăm să rețineți că excluderile de scanare la cerere nu se vor aplica scanării contextuale. Scanarea contextuală este inițiată făcând clic-dreapta pe un fișier sau director și selectând **Scan with Bitdefender Endpoint Security Tools**.

Importare și exportare de excepții

Dacă intenționați să reutilizați regulile de excludere pentru mai multe politici, puteți alege opțiunile de export și import.

Pentru a exporta excepții personalizate:

1. Dați clic pe **Export** în partea de sus a tabelului de excluderi.
2. Salvați fișierul CSV în calculator. În funcție de setările browser-ului, fișierul poate fi descărcat automat sau se poate cere salvarea lui într-o locație implicită.

Fiecare rând din fișierul CSV corespunde unei singure reguli, având câmpurile în următoarea ordine:

```
<exclusion type>, <object to be excluded>, <modules>
```

Acestea sunt valorile disponibile pentru câmpurile CSV:

Tip de excepție:

1, pentru excluderi de fișiere

2, pentru excluderi de foldere

3, pentru excluderi de extensii

4, pentru excepții de proces

5, pentru excluderi hash fișier

6, pentru excluderi hash certificate

7, pentru excluderi denumiri amenințări

8, pentru excluderi linie de comandă

Obiecte ce vor fi excluse:

O cale sau o extensie de fișier

Module:

1, pentru scanare la cerere

2, pentru scanare la accesare

3, pentru toate modulele

4, pentru ATC/IDS

De exemplu, un fișier CSV ce conține excepții antimalware poate arăta astfel:

```
1,"d:\\temp",1
1,%WinDir%,3
4,"%WINDIR%\\system32",4
```

Notă
Căile Windows trebuie să conțină caracterul „\” dublat. De exemplu, `%WinDir%\\System32\\LogFiles`.

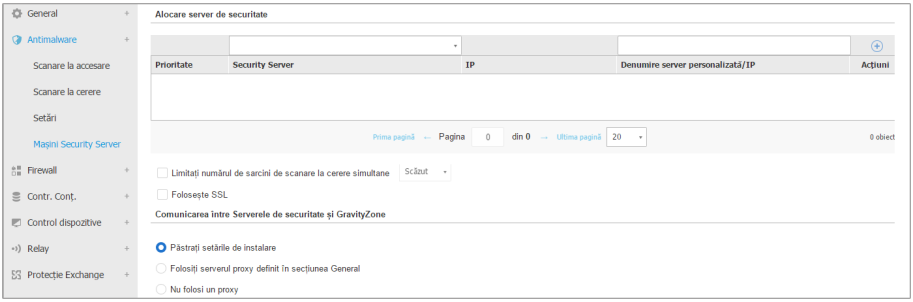
Pentru a importa excepții personalizate:

1. Faceți clic pe **Importă**. Se deschide fereastra **Excepții ale politicii de import**.
2. Faceți clic pe **Adăugare** și apoi selectați fișierul CSV.
3. Faceți clic pe **Save**. Tabelul este populat cu regulile valide. Dacă fișierul CSV conține reguli nevalide, un avertisment vă va informa cu privire la numerele de rând corespunzătoare.

Aplicații Security Server

În această secțiune, puteți configura următoarele:

- Atribuire Security Server
- Setări specifice ale Security Server



Politică - Computere și mașini virtuale - Antimalware - Servere de securitate

Alocare Security Server

Puteți atribui unul sau mai multe Security Server endpoint-urilor vizate și puteți seta prioritatea în care endpoint-urile vor alege un Security Server pentru a trimite solicitări de scanare.

Notă
Se recomandă utilizarea Security Server pentru scanarea mașinilor virtuale sau a computerelor cu resurse reduse.

Pentru a atribui un Security Server endpoint-urilor vizate, adăugați Security Server pe care doriți să le utilizați în tabelul **Atribuire Security Server**, după cum urmează:

1. Accesați lista derulantă de **Security Server** și apoi selectați un Security Server.
2. În cazul în care Security Server este în DMZ sau în spatele unui server de tip NAT, introduceți codul FQDN sau adresa IP a serverului NAT în câmpul **Nume personalizat server/adresă IP**.

   Important
   Asigurați-vă că funcția „port forwarding" este configurată corect pe serverul NAT, astfel încât traficul de la endpoint-uri să poată ajunge la Security Server. Pentru detalii suplimentare, consultați articolul Porturi de comunicații GravityZone din baza de cunoștințe (KB).

3. Selectați ⊕ **Adaugă** din coloana **Acțiuni**.

   Se adaugă Security Server în listă.
4. Repetați pașii anteriori pentru a adăuga alte Security Server, dacă sunt disponibile sau dacă este necesar.

Pentru a seta prioritatea Security Server:

1. Utilizați săgețile sus și jos disponibile în coloana **Acțiuni** pentru a mări sau a reduce nivelul de prioritate pentru fiecare Security Server.

   La atribuirea mai multor Security Server, cel din partea de sus a listei are prioritate maximă și va fi selectat mai întâi. Dacă acest Security Server este indisponibil sau suprasolicitat, atunci se selectează următorul Security Server. Scanarea traficului este redirecționată către primul Security Server care este disponibil și are un nivel de încărcare convenabil.
2. Selectați **Conectare mai întâi la Security Server instalat pe același sistem gazdă fizic, dacă este disponibil, indiferent de prioritatea atribuită** pentru o distribuție uniformă a endpoint-urilor și pentru o latență optimizată. Dacă acest Security Server nu este disponibil, atunci se va selecta un alt Security Server din listă, în ordinea priorității.

   Important
   Această opțiune funcționează numai cu în cazul Security Server multi-platformă și numai dacă GravityZone este integrat cu mediul virtual.

Pentru a șterge din listă un Security Server, selectați opțiunea ⊗ **Șterge** corespunzătoare din coloana **Acțiuni**.

Setările Security Server

În momentul asocierii politicii cu Security Server, puteți configura următoarele setări pentru acestea:

- **Limitarea numărului de scanări simultane la cerere**.

  Executarea mai multor sarcini de scanare la cerere pe mașinile virtuale care folosesc același depozit de date poate genera așa-numitele furtuni de scanare antimalware . Pentru a preveni acest lucru și pentru a permite executarea unui număr limitat de sarcini de scanare în același timp:

  1. Selectați opțiunea **Limitează numărul de scanări la cerere concomitente**.
  2. Selectați nivelul permis de sarcini de scanare concomitente din meniul derulant. Puteți alege un nivel predefinit sau puteți introduce o valoare personalizată.

     Formula pentru a determina limita maximă de sarcini de scanare pentru fiecare nivel predefinit este: `N = a x MAX(b ; vCPUs - 1)`, unde:

     – `N` = limita maximă de sarcini de scanare

     – `a` = coeficientul de multiplicare, având următoarele valori: `1` - pentru Redus; 2 - pentru Mediu; 4 - pentru Ridicat

     – `MAX(b;vCPU-1)` = o funcție care returnează numărul maxim de sloturi de scanare disponibile pe Security Server.

     – `b` = numărul implicit de sloturi de scanare la cerere, setat actualmente la patru.

     – `vCPUs` = numărul de procesoare virtuale alocate Security Server

     De exemplu:

     Pentru un Security Server cu 12 CPU-uri și un nivel Ridicat de scanări concomitente, avem o limită de:

     `N = 4 x MAX(4 ; 12-1) = 4 x 11 = 44` sarcini de scanare la cerere concomitente.

- **Activați regulile de afinitate pentru Security Server Multi-Platformă**

Alegeți comportamentul pe care Security Server să-l adopte atunci când sistemul gazdă intră în modul de mentenanță:

– Dacă este activat, Security Server rămâne legat de sistemul gazdă, iar GravityZone îl va opri. După finalizarea procesului de mentenanță, GravityZone repornește automat Security Server.

  Acesta este comportamentul implicit.

– Dacă este dezactivat, Security Server este transferat către un alt sistem gazdă și va continua să funcționeze. În acest caz, denumirea Security Server se modifică în Control Center pentru a indica sistemul gazdă anterior. Modificarea denumirii persistă până la mutarea Security Server înapoi pe sistemul său gazdă nativ.

  Dacă resursele sunt suficiente, Security Server poate ajunge pe un sistem gazdă pe care este instalat un alt Security Server.

Important
Această opțiune nu are niciun efect dacă Security Server este utilizat și de HVI.

- **Folosește SSL**

  Activați această opțiune dacă doriți să criptați conexiunea dintre endpoint-urile vizate și aplicațiile Security Server specificate.

  În mod implicit, GravityZone utilizează certificate de securitate auto-semnate. Le puteți înlocui cu propriile dumneavoastră certificate accesând pagina **Configurare > Certificate** din Control Center. Pentru informații suplimentare, consultați capitolul „Configurarea setărilor Control Center” din Ghidul de instalare.

- **Comunicarea dintre Security Server și GravityZone**

  Alegeți una dintre opțiunile disponibile pentru a defini preferințele dvs. în materie de proxy pentru comunicarea dintre mașinile Security Server selectate și GravityZone:

  – **Păstrează setările de instalare**, pentru a folosi aceleași setări proxy ca și cele definite în pachetul de instalare.

  – **Folosește proxy-ul definit în secțiunea General**, pentru a folosi setările proxy definite în politica curentă, în secțiunea **General > Setări**.

– **Nu utiliza proxy** , atunci când endpoint-urile vizate nu comunică cu anumite componente Bitdefender prin proxy.

7.2.4. Sandbox Analyzer

Notă
Acest modul este disponibil pentru:

- Windows pentru stații de lucru
- Windows pentru servere

Sandbox Analyzer oferă un strat puternic de protecție împotriva amenințărilor avansate, efectuând analize automate în profunzime asupra fișierelor suspecte care nu sunt încă semnate de motoarele antimalware ale Bitdefender.

În această secțiune, puteți configura:

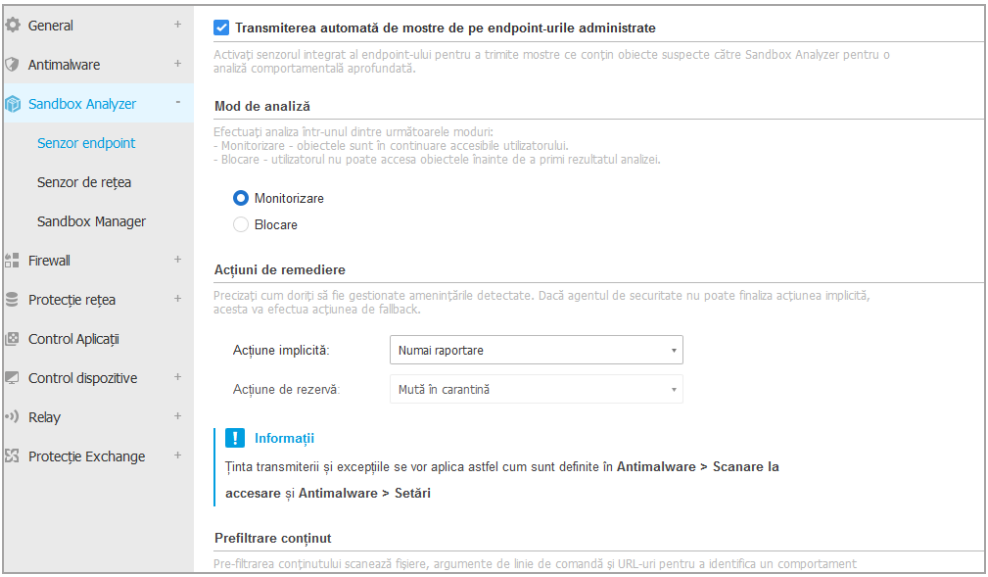
- Trimiterea prin senzorul endpoint-ului
- Trimiterea prin senzorul de rețea
- Trimiterea prin senzorul ICAP
- Setările Sandbox Manager

În setările politicii, puteți configura și trimiterea automată din carantina centralizată. Pentru detalii, consultați „Carantină centralizată” (p. 287).

Pentru mai multe informații despre trimiterea manuală, accesați „Transmitere manuală” (p. 524). Pentru detalii privind trimiterea prin API, consultați capitolele **Sandbox** și **Portal Sandbox** din Ghidul API GravityZone (On-Premises).

Senzor endpoint

Bitdefender Endpoint Security Tools poate opera ca senzor de alimentare pentru Sandbox Analyzer de pe endpoint-urile Windows.



Politici > Sandbox Analyzer> Senzor endpoint

Pentru configurarea trimiterii automate prin senzorul endpoint-ului:

1. În meniul **Setări conexiune**, selectați una dintre opțiuni:
   - **Utilizare Cloud Sandbox Analyzer** - senzorul endpoint-ului va trimite mostrele către o instanță Sandbox Analyzer găzduită de Bitdefender, în funcție de regiunea dumneavoastră.
   - **Utilizare instanță locală Sandbox Analyzer** - senzorul endpoint-ului va trimite mostrele către o instanță Sandbox Analyzer On-Premises. Alegeți instanța Sandbox Analyzer dorită din meniul derulant.

   Dacă rețeaua dumneavoastră este protejată de un senzor de tip proxy sau de un firewall, puteți configura un server proxy pentru conectarea la Sandbox Analyzer bifând căsuța **Utilizare configurație proxy**.

   Trebuie să completați următoarele câmpuri:
   - **Server** - adresa IP a serverului proxy.
   - **Port** - portul utilizat pentru conexiunea la serverul proxy.
   - **Nume utilizator** - un nume de utilizator recunoscut de către proxy.

- **Parolă** - parola valabilă pentru utilizatorul specificat.

2. Bifați opțiunea **Transmitere automată a mostrelor de pe endpoint-urile administrate** pentru a permite transmiterea automată a fișierelor suspecte către Sandbox Analyzer.

Important

- Sandbox Analyzer necesită scanarea la accesare. Asigurați-vă că modulul **Antimalware > Scanare la accesare** este activat.
- Sandbox Analyzer utilizează aceleași ținte și excluderi precum cele definite în **Antimalware > Scanare la accesare**. Revizuiți cu atenție setările funcției Scanare la accesare când configurați Sandbox Analyzer.
- Pentru a împiedica apariția rezultatelor fals pozitive (detectarea incorectă a aplicațiilor legitime), puteți seta excluderi în funcție de denumirea fișierului, extensia, dimensiunea și calea fișierului. Pentru mai multe informații despre Scanarea la accesare, consultați „Antimalware” (p. 260).
- Limita de încărcare pentru orice fișier sau arhivă este de 50 MB.

3. Selectați **Mod Analiză**. Sunt disponibile două opțiuni:
   - **Monitorizare**. Utilizatorul poate accesa fișierul în timpul analizei în sandbox, dar se recomandă să nu îl execute înainte de primirea rezultatelor analizei.
   - **Blocare**. Utilizatorul nu poate executa fișierul până când rezultatele analizei nu sunt retrimise pe endpoint de pe Clusterul Sandbox Analyzer, prin Portalul Sandbox Analyzer.
4. Specificați **Acțiunile de remediere**. Acestea sunt întreprinse când Sandbox Analyzer detectează o amenințare. Pentru fiecare mod de analiză vi se furnizează o setare dublă, care constă dintr-o acțiune implicită și una de fallback. Sandbox Analyzer realizează inițial acțiunea implicită, apoi pe cea de fallback, dacă cea anterioară nu poate fi finalizată.

   La prima accesare a acestei secțiuni sunt disponibile următoarele setări:

Notă
Din categoria celor mai bune practici, se recomandă să utilizați acțiuni de remediere în această configurație.

- În modul **Monitorizare**, acțiunea implicită este **Doar raportare**, acțiunea de fallback fiind dezactivată.

- În modul **Blocare**, acțiunea implicită este **Carantină**, în timp ce acțiunea de fallback este **Ștergere**.

Sandbox Analyzer vă oferă următoarele acțiuni de remediere:

- **Dezinfectare**. Îndepărtează codul malware din fișierele infectate.
- **Ștergere**. Șterge de pe disc fișierul detectat.
- **Carantină**. Mută fișierele detectate din locul actual în directorul de carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Puteți administra fișierele din carantină din pagina **Carantină** a Control Center.
- **Doar raportare**. Sandbox Analyzer raportează numai amenințările detectate fără a lua niciun fel de măsură cu privire la acestea.

Notă
În funcție de acțiunea implicită, acțiunea de fallback poate fi indisponibilă.

5. Atât acțiunile de remediere implicite, cât și cele de backup, sunt configurate la **Doar raportare**.
6. În secțiunea **Pre-filtrare conținut**, personalizați nivelul de protecție împotriva potențialelor amenințări. Senzorul stației de lucru are inclus un mecanism de filtrare a conținutului care stabilește dacă un fișier suspect trebuie detonat în Sandbox Analyzer.

   Tipurile de obiecte acceptate sunt: aplicații, documente, script-uri, arhive, e-mail-uri. Pentru mai multe detalii cu privire la tipurile de obiecte acceptate, consultați „Tipurile de fișiere acceptate de modulul de filtrare preliminară a conținutului la trimiterea automată” (p. 572).

   Utilizați butonul principal din partea superioară a listei de amenințări pentru a selecta un nivel unic de protecție pentru toate tipurile de obiecte sau pentru a selecta niveluri individuale pentru a regla protecția.

   Setarea modulului la un anumit nivel va duce la un anumit număr de mostre trimise:

   - **Permisiv**. Senzorul endpoint-ului trimite automat către Sandbox Analyzer doar obiectele cu cea mai mare probabilitate de a fi periculoase și le ignoră pe celelalte.

- **Normal**. Senzorul endpoint-ului găsește un echilibru între obiectele trimise și cele ignorate și trimite către Sandbox Analyzer ambele tipuri de obiecte cu o probabilitate mai mare sau mai mică de a fi periculoase.
- **Agresiv**. Senzorul endpoint-ului trimite către Sandbox Analyzer aproape toate obiectele, indiferent de potențialul risc.

Într-un câmp dedicat, puteți defini excepții pentru tipurile de obiecte pe care nu doriți să le trimiteți către Sandbox Analyzer.

Puteți defini de asemenea limite pentru dimensiunile obiectelor trimise prin selectarea căsuței corespunzătoare și prin introducerea oricăror valori dorite între 1 KB și 50 MB.

7. În secțiunea **Profil detonare**, ajustați nivelul de complexitate al analizei comportamentale, ceea ce va afecta rata de procesare a Sandbox Analyzer. De exemplu, dacă este setat pe **Ridicat**, Sandbox Analyzer ar efectua o analiză mai precisă pentru mai puține mostre decât modul **Mediu** sau **Redus**, în același interval de timp.

Sandbox Analyzer acceptă transmiterea locală de fișiere prin intermediul stațiilor de lucru cu rol de releu, care se pot conecta la adrese diferite ale Sandbox Analyzer Portal, în funcție de regiunea dvs. Pentru detalii cu privire la setările de configurare ale releului, consultați secțiunea „Relay" (p. 350).

Notă
Un proxy configurat în setările de conexiune Sandbox Analyzer va înlocui orice stații de lucru cu rol de releu.

Senzor de rețea

În această secțiune puteți configura trimiterea automată a mostrelor de trafic de rețea către Sandbox Analyzer prin senzorul de rețea. Pentru acest modul este necesară instalarea și configurarea Aplicației virtuale de securitate pentru rețea cu Sandbox Analyzer On-Premises.

Pentru configurarea trimiterii automate prin senzorul de rețea:

1. Bifați opțiunea **Transmitere automată a mostrelor de pe senzorul de rețea** pentru a permite transmiterea automată a fișierelor suspecte către Sandbox Analyzer.
2. În secțiunea **Pre-filtrare conținut**, personalizați nivelul de protecție împotriva potențialelor amenințări. Senzorul de rețea are integrat un mecanism de filtrare

a conținutului care stabilește dacă un fișier suspect trebuie detonat în Sandbox Analyzer.

Tipurile de obiecte acceptate sunt: aplicații, documente, script-uri, arhive, e-mail-uri. Pentru mai multe detalii cu privire la tipurile de obiecte acceptate, consultați „Tipurile de fișiere acceptate de modulul de filtrare preliminară a conținutului la trimiterea automată" (p. 572).

Utilizați butonul principal din partea superioară a listei de amenințări pentru a selecta un nivel unic de protecție pentru toate tipurile de obiecte sau pentru a selecta niveluri individuale pentru a regla protecția.

Setarea modulului la un anumit nivel va duce la un anumit număr de mostre trimise:

- **Permisiv**. Senzorul de rețea trimite automat către Sandbox Analyzer doar obiectele cu cea mai mare probabilitate de a fi periculoase și le ignoră pe celelalte.
- **Normal**. Senzorul de rețea găsește un echilibru între obiectele trimise și cele ignorate și trimite către Sandbox Analyzer ambele tipuri de obiecte cu o probabilitate mai mare sau mai mică de a fi periculoase.
- **Agresiv**. Senzorul de rețea trimite către Sandbox Analyzer aproape toate obiectele, indiferent de potențialul risc.

Într-un câmp dedicat, puteți defini excepții pentru tipurile de obiecte pe care nu doriți să le trimiteți către Sandbox Analyzer.

Puteți defini de asemenea limite pentru dimensiunile obiectelor trimise prin selectarea căsuței corespunzătoare și prin introducerea oricăror valori dorite între 1 KB și 50 MB.

3. Accesați **Setări conexiune** și selectați instanța preferată Sandbox Analyzer pentru trimiterea conținutului de rețea.

   Dacă rețeaua dumneavoastră este protejată de un senzor de tip proxy sau de un firewall, puteți configura un server proxy pentru conectarea la Sandbox Analyzer bifând căsuța **Utilizare configurație proxy**.

   Trebuie să completați următoarele câmpuri:

   - **Server** - adresa IP a serverului proxy.
   - **Port** - portul utilizat pentru conexiunea la serverul proxy.
   - **Nume utilizator** - un nume de utilizator recunoscut de către proxy.

- **Parolă** - parola valabilă pentru utilizatorul specificat.

4. În secțiunea **Profil detonare**, ajustați nivelul de complexitate al analizei comportamentale, ceea ce va afecta rata de procesare a Sandbox Analyzer. De exemplu, dacă este setat pe **Ridicat**, Sandbox Analyzer ar efectua o analiză mai precisă pentru mai puține mostre decât modul **Mediu** sau **Redus**, în același interval de timp.

Senzor ICAP

În această secțiune puteți configura trimiterea automată către Sandbox Analyzer prin senzorul ICAP.

Notă
Sandbox Analyzer necesită configurarea Security Server pentru scanarea dispozitivelor NAS (network-attached storage) care utilizează protocolul ICAP. Pentru detalii, consultați„Protecție spațiu de stocare" (p. 388)

1. Bifați opțiunea **Transmitere automată a mostrelor de pe senzorul ICAP** pentru a permite transmiterea automată a fișierelor suspecte către Sandbox Analyzer.
2. În secțiunea **Pre-filtrare conținut**, personalizați nivelul de protecție împotriva potențialelor amenințări. Senzorul de rețea are integrat un mecanism de filtrare a conținutului care stabilește dacă un fișier suspect trebuie detonat în Sandbox Analyzer.

   Tipurile de obiecte acceptate sunt: aplicații, documente, script-uri, arhive, e-mail-uri. Pentru mai multe detalii cu privire la tipurile de obiecte acceptate, consultați „Tipurile de fișiere acceptate de modulul de filtrare preliminară a conținutului la trimiterea automată" (p. 572).

   Utilizați butonul principal din partea superioară a listei de amenințări pentru a selecta un nivel unic de protecție pentru toate tipurile de obiecte sau pentru a selecta niveluri individuale pentru a regla protecția.

   Setarea modulului la un anumit nivel va duce la un anumit număr de mostre trimise:

   - **Permisiv**. Senzorul ICAP trimite automat către Sandbox Analyzer doar obiectele cu cea mai mare probabilitate de a fi periculoase și le ignoră pe celelalte.

- **Normal**. Senzorul ICAP găsește un echilibru între obiectele trimise și cele ignorate și trimite către Sandbox Analyzer ambele tipuri de obiecte cu o probabilitate mai mare sau mai mică de a fi periculoase.
- **Agresiv**. Senzorul ICAP trimite către Sandbox Analyzer aproape toate obiectele, indiferent de potențialul risc.

Într-un câmp dedicat, puteți defini excepții pentru tipurile de obiecte pe care nu doriți să le trimiteți către Sandbox Analyzer.

Puteți defini de asemenea limite pentru dimensiunile obiectelor trimise prin selectarea căsuței corespunzătoare și prin introducerea oricăror valori dorite între 1 KB și 50 MB.

3. Accesați **Setări conexiune** și selectați instanța preferată Sandbox Analyzer pentru trimiterea conținutului de rețea.

   Dacă rețeaua dumneavoastră este protejată de un senzor de tip proxy sau de un firewall, puteți configura un server proxy pentru conectarea la Sandbox Analyzer bifând căsuța **Utilizare configurație proxy**.

   Trebuie să completați următoarele câmpuri:

   - **Server** - adresa IP a serverului proxy.
   - **Port** - portul utilizat pentru conexiunea la serverul proxy.
   - **Nume utilizator** - un nume de utilizator recunoscut de către proxy.
   - **Parolă** - parola valabilă pentru utilizatorul specificat.

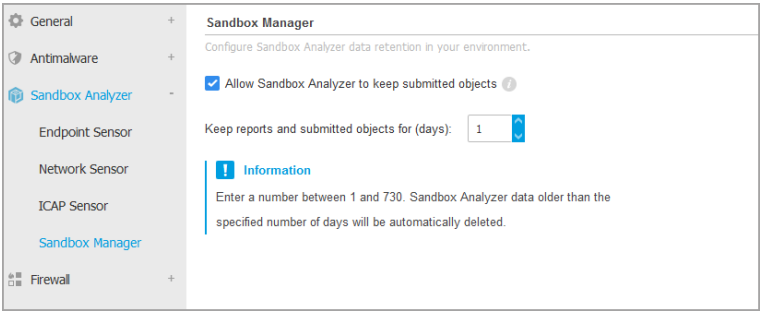
4. În secțiunea **Profil detonare**, ajustați nivelul de complexitate al analizei comportamentale, ceea ce va afecta rata de procesare a Sandbox Analyzer. De exemplu, dacă este setat pe **Ridicat**, Sandbox Analyzer ar efectua o analiză mai precisă pentru mai puține mostre decât modul **Mediu** sau **Redus**, în același interval de timp.

Sandbox Manager

În această secțiune puteți configura reținerea datelor pentru instanțele dvs. Sandbox Analyzer:

- Bifați opțiunea **Permite Sandbox Analyzer să păstreze obiectele trimise**. Această setare vă permite să utilizați opțiunea **Retrimite pentru analiză** aflată în secțiunea de trimiteri din interfața de raportare a Sandbox Analyzer.

- Specificați numărul de zile pentru care doriți ca Sandbox Analyzer să păstreze rapoarte și obiecte trimise în spațiul de stocare a datelor. Numărul maxim de date pe care le puteți introduce este 730. După expirarea perioadei definite, toate datele vor fi șterse.



Politici > Sandbox Analyzer > Sandbox Manager

7.2.5. Firewall

Notă
Acest modul este disponibil pentru stațiile de lucru Windows.

Firewallul vă protejează stația de lucru de tentativele de conectare neautorizate, atât la intrare, cât și la ieșire.

Funcționalitatea firewall-ului se bazează pe profile de rețea. Profilele se bazează pe niveluri de încredere, care trebuie definite pentru fiecare rețea.

Firewall-ul detectează orice conexiune nouă, compară informațiile adaptorului pentru acea conexiune cu informațiile din profilurile existente și aplică profilul corect. Pentru informații detaliate cu privire la modul în care sunt aplicate profilele, consultați „Setări de rețea” (p. 310).

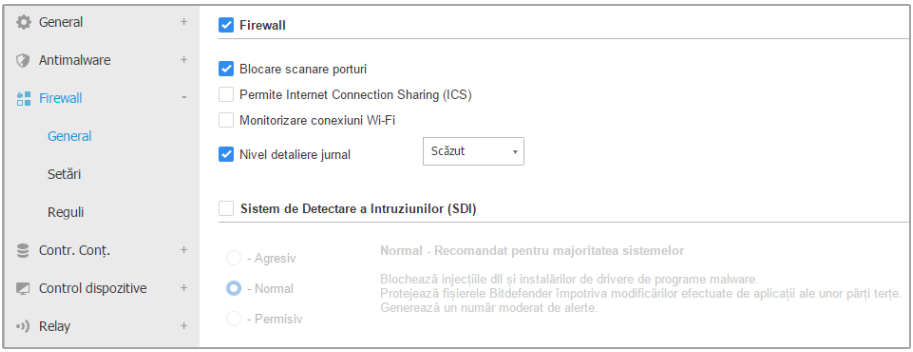
Important
Modulul Firewall este disponibil numai pentru stațiile de lucru Windows.

Setările sunt organizate în următoarele secțiuni:

- General
- Setări
- Reguli

General

În această secțiune puteți activa sau dezactiva firewallul Bitdefender și puteți configura setările generale.



Politici referitoare la calculatoare și mașini virtuale - Setări generale firewall

- **Firewall.** Utilizați caseta de selecție pentru a activa sau opri Firewall-ul.

  Avertisment
  Dacă dezactivați protecția firewall, computerele vor fi vulnerabile la atacurile de rețea și de pe Internet.

- **Blocare scanare porturi.** Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculator. Dacă este detectat un port vulnerabil, aceștia pot pătrunde în calculator.
- **Permite Internet Connection Sharing (ICS).** Selectați această opțiune pentru a seta firewall-ul pentru a permite traficul Internet Connection Sharing.

  Notă
  Această opțiune nu activează automat ICS pe sistemul utilizatorului.

- **Monitorizare conexiuni Wi-Fi.** Agentul de securitate Bitdefender poate informa utilizatorii conectați la o rețea Wi-Fi atunci când un nou computer devine membru al rețelei. Selectați această opțiune pentru a afișa astfel de notificări pe ecranul utilizatorului.

- **Nivel detaliere jurnal.** Agentul de securitate Bitdefender păstreză un jurnal al evenimentelor referitoare la activitatea modulului Firewall (activare/dezactivare firewall, blocare trafic, modificare setări) sau generate de activitățile detectate de firewall (scanare porturi, blocare tentative de conectare sau trafic conform regulilor). Alegeți o opțiune din **Log verbosity level** tpentru a specifica câte informații va include registrul.
- **Sistem de detecție a intruziunilor.** Sistem de Detectare a Intruziunilor (SDI) monitorizează sistemul pentru activități suspecte (de exemplu, încercările neautorizate de a modifica fișierele Bitdefender, injecții DLL, încercări de utilizare keyloggere etc.).

  Notă
  Setările Sistemului de Detectare a Intruziunilor (IDS) se aplică numai pentru Endpoint Security (agent de securitate în versiune mai veche). Agentul Bitdefender Endpoint Security Tools integrează capacitățile sistemului de detectare a intruziunilor instalat pe un sistem gazdă în modulul său Advanced Threat Control (ATC).

  Pentru a configura sistemul de detectare a intruziunilor:

  1. Utilizați caseta de selecție pentru a activa sau opri Sistemul de detecție a intruziunilor.
  2. Faceți clic pe nivelul de securitate care corespunde cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

  Pentru a preveni cazul în care o aplicație legitimă este detectată de Sistemul de detectare a intruziunilor, adăugați o **regulă ATC/IDS pentru excluderi de procese** pentru respectiva aplicație în secțiunea **Antimalware > Setări > Excluderi personalizate**.

Important
Sistemul de Detectare a Intruziunilor este disponibil exclusiv pentru clienții Endpoint Security.

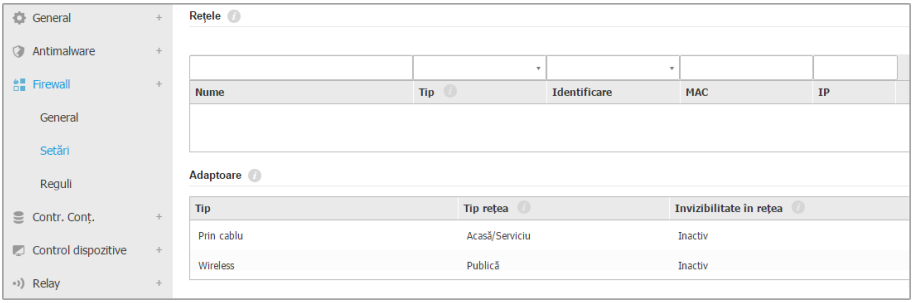
Setări

Firewall-ul aplică în mod automat un profil bazat pe nivelul de încredere. Puteți avea diferite niveluri de încredere pentru conexiunile de rețea, în funcție de arhitectura rețelei sau de tipul adaptorului folosit pentru stabilirea conexiunii. De

exemplu, dacă aveți sub-rețele în cadrul rețelei companiei dumneavoastră, puteți seta un nivel de încredere pentru fiecare sub-rețea.

Setările sunt organizate în următoarele tabele:

- Rețele
- Adaptoare



Politici - Setări firewall

Setări de rețea

Dacă doriți ca Firewall-ul să aplice profiluri diferite pentru mai multe segmente de rețea din cadrul companiei dumneavoastră, trebuie să specificați rețelele administrate în tabelul **Rețele**. Completați câmpurile din tabelul **Rețele**, după cum este descris aici:

- **Nume.** Introduceți numele după care puteți recunoaște rețeaua din listă.
- **Tip.** Selectați din meniu tipul de profil alocat rețelei.

  Agentul de securitate Bitdefender aplică în mod automat unul din cele patru profiluri de rețea pentru fiecare conexiune de rețea detectată pe stația de lucru, pentru a defini opțiunile de bază de filtrare a traficului. Tipurile de profiluri sunt următoarele:

  – Rețea **Sigură**. Dezactivează firewall-ul pentru adaptorii respectivi.

  – Rețea **Acasă/Serviciu**. Permite tot traficul către și de la calculatoarele din rețeaua locală, în timp ce restul traficului este filtrat.

  – Rețea **Publică**. Tot traficul este filtrat.

  – Rețea **Nesigură**. Blochează complet traficul de rețea și Internet prin adaptorii respectivi.

- **Identificare.** Selectați din meniu metoda prin care rețeaua va fi identificată prin agentul de securitate Bitdefender. Rețelele pot fi identificate prin trei metode: **DNS**, **Gateway** și **Rețea**.
  - **DNS**: identifică toate stațiile de lucru care folosesc DNS-ul specificat.
  - **Gateway**: identifică toate stațiile de lucru care comunică prin intermediul gateway-ului specificat.
  - **Rețea**: identifică toate stațiile de lucru din segmentul de rețea specificat, definit de adresa de rețea a acestuia.
- **MAC**. Folosiți acest câmp pentru a specifica adresa MAC a serverului DNS sau a unui gateway ce delimitează rețeaua, în funcție de metoda de identificare selectată.

  Trebuie să introduceți adresa MAC în format hexazecimal, separată prin liniuțe (-) sau două puncte (:). De exemplu, ambele adrese `00-50-56-84-32-2b` și `00:50:56:84:32:2b` sunt considerate valabile.
- **IP.** Utilizați acest câmp pentru a defini anumite adrese IP într-o rețea. Formatul IP-ului depinde de metoda de identificare, după cum urmează:
  - **Rețea.** Introduceți numărul de rețea în format CIDR. De exemplu, `192.168.1.0/24`, unde `192.168.1.0` este adresa de rețea și `/24` este masca de rețea.
  - **Gateway.** Introduceți adresa IP a gateway-ului.
  - **DNS.** Introduceți adresa IP a serverului DNS.

După ce ați definit o rețea, faceți clic pe butonul **Adăugare** din partea dreaptă a tabelului pentru a o adăuga la listă.

Setările adaptoarelor

În cazul în care este detectată o rețea care nu este definită în tabelul **Rețele**, agentul de securitate Bitdefender detectează tipul de adaptor de rețea și aplică un profil corespunzător conexiunii.

Câmpurile din tabelul **Adaptoare** sunt descrise după cum urmează:

- **Tip.** Afișează tipul de adaptoare de rețea. Agentul de securitate Bitdefender poate detecta trei tipuri de adaptoare predefinite: **Prin cablu**, **Wireless** și **Virtual** (Virtual Private Network).

- **Tip rețea.** Descrie profilul de rețea alocat unui tip anume de adaptor. Profilurile de rețea sunt descrise în secțiunea setări de rețea. Dacă faceți clic pe câmpul tip de rețea puteți să schimbați setarea.

  Dacă selectați **Lasă Windows să decidă**, pentru orice nouă conexiune de rețea detectată după aplicarea politicii, agentul de securitate Bitdefender aplică un profil pentru firewall bazat pe clasificarea rețelei în Windows, ignorând setările din tabelul **Adaptoare**.

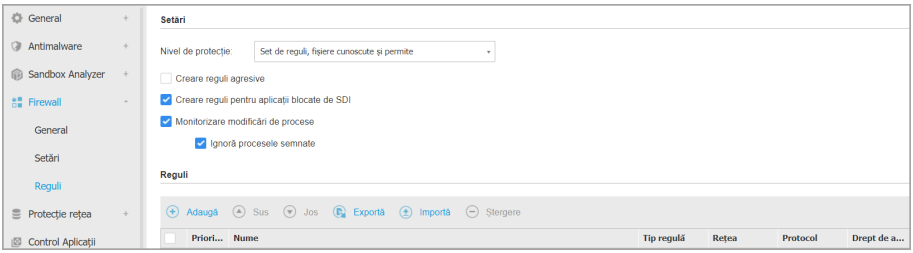
  În cazul în care detectarea bazată pe Windows Network Manager eșuează, se încearcă o detectare de bază. Se utilizează un profil generic în care profilul de rețea este considerat **Publică** iar setările ascunse sunt setate pe **Activ**.

  Când stația de lucru inclusă în Active Directory se conectează la domeniu, profilul firewall este setat automat pe **Acasă/Serviciu**, iar setările de ascundere sunt setate pe **La distanță**. În cazul în care calculatorul nu este într-un domeniu, această condiție nu se aplică.

- **Descoperire rețea.** Ascunde calculatorul față de aplicații periculoase și de hackeri din rețea sau din Internet. Configurați vizibilitatea computerului în rețea în funcție de necesități pentru fiecare tip de adaptor, selectând una dintre următoarele opțiuni:
  - **Da.** Oricine din rețeaua locală sau de pe Internet poate trimite un ping pentru a detecta computerul.
  - **No.** Computerul este invizibil în rețeaua locală și pe Internet.
  - **La distanță.** Calculatorul nu poate fi detectat din Internet. Oricine din rețeaua locală poate da ping și detecta calculatorul.

Reguli

În această secțiune puteți configura accesul aplicației la rețea și regulile de trafic de date, puse în aplicare de către firewall. Rețineți că setările disponibile se aplică numai pentru **Acasă/Serviciu** și profilele de tip **Publică** .



Politici referitoare la calculatoare și mașini virtuale - Reguli generale firewall

Setări

Puteți configura următoarele setări:

- **Nivel de protecție.** Nivelul de protecție selectat definește logica de luare a deciziilor firewall folosită atunci când aplicațiile solicită acces la servicii de rețea și de Internet. Sunt disponibile următoarele opțiuni:

  Set de reguli și permite
  Se aplică regulile firewall existente și permite în mod automat toate celelalte încercări de conectare. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

  Set de reguli și întreabă
  Se aplică regulile firewall existente și cere utilizatorului acțiune pentru toate celelalte încercări de conectare. Pe ecranul utilizatorului apare o fereastră de alertă cu informații detaliate despre încercarea de conectare necunoscută. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

  Set de reguli și respinge
  Se aplică regulile firewall existente și se respinge în mod automat toate celelalte încercări de conectare. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

  Set de reguli, fișiere cunoscute și permite
  Se aplică regulile firewall existente, se permite în mod automat tentativele de conexiune realizate de aplicații cunoscute și se solicit[utilizatorului acțiune pentru toate celelalte încercări de conectare necunoscute. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

Set de reguli, fișiere cunoscute și întreabă

Se aplică regulile firewall existente, se permit în mod automat tentativele de conectare realizate de aplicații cunoscute și în mod automat se resping toate celelalte încercări de conectare necunoscute. Pe ecranul utilizatorului apare o fereastră de alertă cu informații detaliate despre încercarea de conectare necunoscută. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

Set de reguli, fișiere cunoscute și respinge

Se aplică regulile firewall existente, se permit în mod automat tentativele de conectare realizate de aplicații cunoscute și în mod automat se resping toate celelalte încercări de conectare necunoscute. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

Notă

Fișierele cunoscute, reprezintă o colecție mare de aplicații sigure, de încredere, care sunt compilate și întreținute în mod continuu de către Bitdefender.

- **Creare reguli agresive.** Fiind selectată această opțiune, firemwall-ul va crea reguli pentru fiecare proces diferit care deschide aplicația care necesită acces la rețea sau Internet.
- **Creare reguli pentru aplicații blocate de SDI.** Fiind selectată această opțiune, firewall-ul va crea automat o regulă **Interzice** de fiecare dată când Sistemul de detectare a intruziunilor blochează o aplicație.
- **Monitorizare modificări de procese.** Selectați această opțiune dacă doriți ca fiecare aplicație care încearcă să se conecteze la Internet să fie verificată dacă a fost modificată de la momentul adăugării regulii care controlează accesul ei la Internet. În cazul în care aplicația a fost modificată, va fi creată o nouă regulă în funcție de nivelul de protecție existent.

Notă

De obicei, aplicațiile sunt modificate de actualizări. Dar, există riscul ca acestea să fie modificate de aplicații periculoase, în scopul infectării calculatorului local și a altor stații din rețea.

Aplicațiile semnate sunt presupuse a fi sigure și au un grad sporit de securitate. Puteți selecta **Ignoră procesele semnate** pentru a permite automat conectarea aplicațiilor semnate la Internet.

Reguli

Tabelul de reguli enumeră regulile firewall existente, furnizândinformații importante despre fiecare dintre ele:

- Numele regulii sau aplicația la care se referă.
- Protocolul căruia i se aplică regula.
- Acțiunea prevăzută de regulă (permite sau respinge accesul pachetelor).
- Acțiunile pe care le puteți întreprinde cu privire la regulă.
- Prioritatea regulii.

Notă

Acestea sunt regulile de firewall impuse în mod explicit de politică. Ca urmare a aplicării setărilor firewall pot fi configurate reguli suplimentare pe calculatoare.

O serie de reguli implicite de firewall vă ajută să permiteți sau să refuzați cu ușurință tipuri de trafic populare. Alegeți opțiunea dorită din meniul **Permisiune**.

ICMP / ICMPv6 în curs de recepționare
Permite sau respinge mesajele ICMP / ICMPv6. Mesajele ICMP sunt folosite adesea de hackeri pentru a lansa atacuri asupra rețelelor computerului. În mod implicit, acest tip de trafic este permis.

Conexiuni desktop de la distanță în curs de recepționare
Permite sau respinge accesul altor computere la conexiunile desktop de la distanță. În mod implicit, acest tip de trafic este permis.

Trimitere mesaje e-mail
Permite sau respinge trimiterea de mesaje e-mail prin SMTP. În mod implicit, acest tip de trafic este permis.

Navigare internet HTTP
Permite sau respinge navigare web HTTP. În mod implicit, acest tip de trafic este permis.

Tipărire în rețea
Permite sau refuză accesul la imprimante într-o altă rețea locală. În mod implicit, acest tip de trafic nu este permis.

Trafic Windows Explorer pe HTTP / FTP
Permite sau respinge traficul HTTP sau FTP de la Windows Explorer. În mod implicit, acest tip de trafic nu este permis.

În afară de regulile implicite, puteți crea reguli de firewall suplimentare pentru alte aplicații instalate pe stațiile de lucru. Însă această configurație este rezervată administratorilor cu abilități dezvoltate de networking.

Pentru a crea și a configura o nouă regulă, faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului. Pentru mai multe informații consultați următorul subiect.

Pentru a șterge o regulă din listă, selectați-o și faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului.

Notă
Nu puteți șterge sau modifica regulile implicite de firewall.

Configurarea Regulilor personalizate

Puteți configura două tipuri de reguli firewall:

- **Reguli bazate pe aplicații.** Aceste reguli se aplică software-uilor specifice care se găsesc pe calculatoarele client.
- **Reguli bazate pe conexiune.** Aceste reguli se aplică la orice aplicație sau serviciu care utilizează o conexiune specifică.

Pentru a crea și configura o nouă regulă, faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului și selectați din meniu tipul de regulă dorit. Pentru a edita o regulă existentă, faceți clic pe numele regulii.

Pot fi configurate următoarele setări:

- **Nume regulă.** Introduceți numele cu care regula va fi introdusă în tabelul de reguli (de exemplu, numele aplicației la cere se aplică de regulă).
- **Calea către aplicație** (numai pentru regulile bazate pe aplicație). Trebuie să specificați calea către fișierul executabil al aplicației de pe calculatoarele țintă.
  - Alegeți din meniu o locație prestabilită și completați calea după cum este necesar. De exemplu, pentru o aplicație instalată în directorul `Program Files`, selectați `%ProgramFiles%` și completați calea prin adăugarea unei bare oblice inversă (\) și numele directorului aplicației.
  - Introduceți calea completă în câmpul editabil. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.
- **Linie de comandă** (numai pentru regulile bazate pe aplicații). Dacă doriți ca regula să fie aplicată doar atunci când aplicația specificată este deschisă cu o

anumită comandă în linia de comandă Windows, introduceți respectiva comandă în câmpul corespunzător. În caz contrar, lăsați-l necompletat.

- **MD5-ul aplicației** (numai pentru regulile bazate pe aplicație). Dacă doriți ca regula să verifice integritatea datelor din fișierul aplicației bazat pe codul hash MD5, introduceți-l în câmpul editabil. Dacă nu este cazul, lăsați acest câmp necompletat.
- **Adresă locală.** Specificați adresa IP locală și portul local cărora li se aplică regula. Dacă aveți mai multe adaptoare de rețea, puteți debifa căsuța **Oricare** și introduce o anumită adresă IP. De asemenea, pentru a filtra conexiunile pe un anumit port sau o gamă de porturi, debifați caseta de selecție **Oricare** și introduceți portul dorit sau gama de porturi în câmpul corespunzător.
- **Adresă de la distanță.** Specificați adresa IP și portul la distanță cărora li se aplică regula. Pentru a filtra traficul către și de la un anumit calculator, debifați căsuța **Oricare** și introduceți adresa IP a acestuia.
- **Aplicați regula numai pentru calculatoare conectate direct.** Puteți filtra accesul bazat pe adresa Mac.
- **Protocol.** Selectați protocolul IP căruia i se aplică regula.
  - Dacă doriți ca regula să fie aplicată tuturor protocoalelor, selectați **Oricare**.
  - Dacă doriți ca regula să fie aplicată pentru TCP, selectați **TCP**.
  - Dacă doriți ca regula să fie aplicată pentru UDP, selectați **UDP**.
  - Dacă doriți ca regula să se aplice unui anumit protocol, selectați protocolul din meniul **Altul**.

  Notă

  Numerele protocoalelor IP sunt atribuite de către Internet Assigned Numbers Authority (IANA). Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa http://www.iana.org/assignments/protocol-numbers.

- **Direcție.** Selectați direcția de trafic căreia i se aplică regula.

Direcție	Descriere
La ieșire	Regula nu se va aplica decât pentru traficul la ieșire.
La intrare	Regula nu se aplica decât pentru traficul la intrare.

Direcție	Descriere
Ambele	Regula se va aplica în ambele direcții.

- **Versiune IP.** Selectați versiunea IP (IPv4, IPv6 sau ambele) căreia i se aplică regula.
- **Rețea.** Selectați tipul de rețea pentru care se aplică regula.
- **Drept de acces.** Selectați una dintre permisiunile disponibile:

Drept de acces	Descriere
Permite	Aplicației specificate îi va fi permis accesul la rețea / Internet în condițiile specificate.
Interzice	Aplicației specificate îi va fi refuzat accesul la rețea / Internet în condițiile specificate.

Faceți clic pe **Salvare** pentru a adăuga regula.

Pentru regulile create de dvs., folosiți săgețile din partea dreaptă a tabelului pentru a seta prioritatea fiecărei reguli. Regula cu prioritatea mai mare va fi mai aproape de partea de sus a listei.

Reguli de import și export

Puteți exporta și importa reguli de firewall pentru a le utiliza în alte politici sau companii. Pentru exportarea regulilor:

1. Selectați **Export** în partea de sus a tabelului cu reguli.
2. Salvați fișierul CSV în calculator. În funcție de setările browser-ului, fișierul poate fi descărcat automat sau se poate cere salvarea lui într-o locație implicită.

Important

- Fiecare rând din fișierul CSV corespunde unei singure reguli și are câmpuri multiple.
- Poziția regulilor de firewall din fișierul CSV determină prioritatea acestora. Puteți modifica prioritatea unei reguli prin mutarea întregului rând.

Pentru setul implicit de reguli, puteți modifica doar următoarele elemente:

- **Prioritate**: Configurați prioritatea regulii în orice ordine doriți, prin mutarea rândului CSV.
- **Drepturi de acces**: Modificați câmpul `set.Permission` folosind următoarele setări disponibile:
  - 1 pentru **Permite**
  - 2 pentru **Refuză**

Orice alte modificări sunt eliminate la importare.

Pentru regulile personalizate de firewall, toate valorile câmpurilor personalizabile sunt configurabile după cum urmează:

Câmp	Nume și valoare
`ruleType`	**Tip regulă**: 1 pentru **Regulă aplicare** 2 pentru **Regulă conexiune**
`tip`	Valoarea pentru acest câmp este opțională.
`details.name`	**Nume regulă**
`details.applicationPath`	**Application path** (numai pentru regulile bazate pe aplicație)
`details.commandLine`	**Command line** (numai pentru regulile bazate pe aplicații)
`details.applicationMd5`	**Application MD5** (numai pentru regulile bazate pe aplicație)
`settings.protocol`	**Protocol** 1 pentru **Oricare** 2 pentru **TCP** 3 pentru **UDP** 4 pentru **Altul**
`settings.customProtocol`	Necesar doar dacă **Protocolul** este configurat ca **Altul**.

Câmp	Nume și valoare
	Pentru valori specifice, consultați această pagină. Valorile 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34-37, 141-143 nu sunt compatibile.
`settings.direction`	**Direcție**: 1 pentru **Ambele** 2 pentru **La intrare** 3 pentru **La ieșire**
`settings.ipVersion`	**Versiune IP**: 1 pentru **Oricare** 2 pentru **IPv4** 3 pentru **IPv6**
`settings.localAddress.any`	**Adresa locală** este configurată ca **Oricare**: 1 pentru Adevărat 0 pentru gol sau Fals
`settings.localAddress.ipMask`	**Adresa locală** este configurată ca **IP sau IP/Mască**
`settings.remoteAddress.portRange`	**Adresa la distanță** este configurată ca **Port sau gamă de porturi**
`settings.directlyConnected.enable`	**Aplicați regula numai pentru calculatoare conectate direct.**: 1 pentru activat 0 pentru gol sau dezactivat
`settings.directlyConnected.remoteMac`	**Aplicați regula doar pentru computerele conectate direct** cu filtru pentru **adresă MAC**.
`permission.home`	**Rețeaua** pentru care se aplică regula este **Acasă/Serviciu**:

Câmp	Nume și valoare
	1 pentru Adevărat 0 pentru gol sau Fals
`permission.public`	**Rețeaua** pentru care se aplică regula este **Publică**: 1 pentru Adevărat 0 pentru gol sau Fals
`permission.setPermission`	Drepturi de acces disponibile: 1 pentru **Permite** 2 pentru **Refuză**

Pentru importarea regulilor:

1. Selectați **Import** în partea de sus a tabelului cu reguli.
2. În noua fereastră, selectați **Adăugare** și apoi fișierul CSV.
3. Faceți clic pe **Save**. Tabelul este populat cu regulile valide.

7.2.6. Protecție rețea

Utilizați secțiunea Protecție rețea pentru a configura preferințele dumneavoastră cu privire la filtrarea conținutului, protecția datelor pentru activitatea utilizatorului, inclusiv navigarea web, aplicații de e-mail și software, și detecția tehnicilor de atac în rețea care au ca scop obținerea de drepturi de acces pe anumite endpoint-uri. Puteți restricționa sau permite accesul web și folosirea aplicației, configura scanarea traficului, regulile antiphishing și de protecție a datelor.

Rețineți că setările de Protecție rețea configurate se vor aplica tuturor utilizatorilor care se autentifică pe computerele țintă.

Setările sunt organizate în următoarele secțiuni:

- General
- Content Control
- Protecție web
- Atacuri de rețea

Notă

- Modulul Control conținut este disponibil pentru:
  - Windows pentru stații de lucru
  - macOS
- Modulul Network Attack Defense este disponibil pentru:
  - Windows pentru stații de lucru

Important

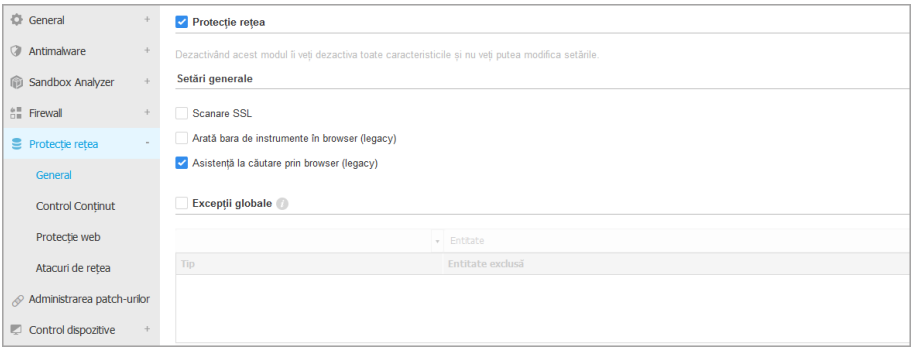
Pentru macOS, Controlul conținutului se bazează pe extensia nucleului. Instalarea unei extensii kernel necesită aprobarea dvs. pe macOS High Sierra (10.13) sau mai recent. Sistemul informează utilizatorul că o extensie de sistem de la Bitdefender a fost blocată. O puteți accepta din **Securitate & Confidentialitate** preferinte. Până când utilizatorul acceptă extensia de sistem Bitdefender, acest modul nu va funcționa, iar pe interfața utilizatorului Endpoint Security for Mac se afișa un mesaj de problemă critică pentru care este necesară aprobarea dvs.
Pentru a elimina intervenția utilizatorului, puteți pre-aproba extensia kernel a Bitdefender prin adăugarea ei în lista de excepții utilizând un instrument de administrare a dispozitivelor mobile. Pentru detalii despre extensiile de kernel ale Bitdefender, consultați acest articol din Baza de cunoștințe.

General

În această pagină, puteți configura opțiuni cum ar fi activarea sau dezactivarea funcționalităților sau configurarea excepțiilor.

Setările sunt organizate în următoarele secțiuni:

- Setări generale
- Excepții globale



Politici computere și mașini virtuale - Protecție rețea - General

Setări generale

- **Scanează SSL**. Selectați această opțiune dacă doriți ca traficul web al Secure Sockets Layer (SSL) să fie verificat de modulele de protecție ale agentului de securitate Bitdefender.
- **Afișare bară de instrumente în browser (legacy)**. Bara de instrumente Bitdefender informează utilizatorii cu privire la rating-ul paginilor web pe care le vizualizează. Bara de instrumente Bitdefender nu este aceeași cu bara de instrumente obișnuită a browser-ului dumneavoastră. Singurul lucru pe care îl adaugă browser-ului dumneavoastră este un mic instrument care glisează în partea superioară a fiecărei pagini web. Făcând clic pe acest buton se deschide bara de instrumente.

  În funcție de cum este clasificată pagina web de către Bitdefender, va fi afișată, în partea stângă a barei de instrumente, una dintre următoarele clasificări:

  – Apare mesajul "Această pagină nu este sigură", pe un fond de culoare roșie.

  – Mesajul "Se recomandă prudență" apare pe un fundal portocaliu.

  – Mesajul "Această pagină este sigură" apare pe un fond verde.

Notă

– Această opțiune nu este disponibilă pentru macOS.

– Această opțiune este eliminată din Windows începând cu noile instalări ale Bitdefender Endpoint Security Tools, versiunea 6.6.5.82.

- **Asistență la căutare prin browser (legacy).** Funcția „Asistență la căutare” clasifică rezultatele afișate în urma căutărilor efectuate prin intermediul Google, Bing și Yahoo!, precum și link-urile de pe Facebook și Twitter, introducând o pictogramă în fața fiecărui rezultat. Pictograme utilizate și semnificația lor:

  Nu este recomandat să vizitați această pagină web.
  Această pagină web poate avea conținut periculos. Vizitați cu atenție această pagină.
  Această pagină este sigură.

  Notă
  - Această opțiune nu este disponibilă pentru macOS.
  - Această opțiune este eliminată din Windows începând cu noile instalări ale Bitdefender Endpoint Security Tools, versiunea 6.6.5.82.

Excepții globale

Puteți alege să săriți peste scanarea antimalware pentru un anumit trafic în timp ce sunt activate opțiunile de **Protecție rețea**.

Notă
Aceste excepții se aplică pentru **Scanarea traficului** și **Antiphishing**, în secțiunea **Protecție web**, și pentru **Network Attack Defense**, în secțiunea **Network Attacks**. Excepțiile pentru **Protecția datelor** pot fi configurate separat, în secțiunea **Controlul conținutului**.

Pentru a defini o excepție:

1. Selectați tipul de excludere din meniu.
2. În funcție de tipul de excludere, definiți entitatea de trafic care să fie exclusă de la scanare, după cum urmează:
   - **IP/mască**. Introduceți adresa IP sau masca IP pentru care nu doriți să scanați traficul de intrare sau de ieșire, care include tehnicile de atac la nivelul rețelei.
   - **URL**. Exclude de la scanare adresele web menționate. Luați în considerare faptul că excepțiile de la scanare bazate pe adresa URL se aplică în mod diferit pentru conexiunile HTTP față de cele HTTPS, după cum este detaliat mai jos.

     Puteți defini o excepție de la scanare bazată pe adresa URL astfel:

– Introduceți URL-ul specific, precum `www.example.com/example.html`
  - În cazul conexiunilor HTTP, numai adresa URL respectivă este exclusă de la scanare.
  - În ceea ce privește conexiunile HTTPS, adăugarea unei anumite adrese URL determină excluderea întregului domeniu și a tuturor subdomeniilor acestuia. Prin urmare, în acest caz, puteți specifica direct domeniul care să fie exclus de la scanare.
– Utilizați metacaractere pentru a defini șabloane de adrese web (numai pentru conexiunile HTTP).

Important
Excepțiile ce conțin metacaractere nu funcționează în cazul conexiunilor HTTPS.

Puteți utiliza următoarele caractere wildcard:

- Asterisc (*) este substitut pentru zero sau mai multe caractere.
- Semnul întrebării (?) înlocuiește un singur caracter. Puteți folosi mai multe semne de întrebare pentru a defini orice combinație a unui anumit număr de caractere. De exemplu, ??? înlocuiește orice combinație de exact trei caractere.

În tabelul de mai jos, puteți găsi mai multe exemple de sintaxă pentru specificarea adreselor web (URL).

Sintaxă	Aplicabilitatea excepției
`www.example*`	Orice adresă URL care începe cu `www.example` (indiferent de extensia domeniului). Excluderea nu se va aplica la subdomeniile site-ului specificat, cum ar fi `subdomain.example.com`.
`*example.com`	Orice adresă URL care se termină în `example.com`, inclusiv subdomeniile aferente.
`*example.com*`	Orice adresă URL care conține șirul specificat.

Sintaxă	Aplicabilitatea excepției
`*.com`	Orice site web care are extensia de domeniu `.com`, inclusiv subdomeniile aferente. Utilizați această sintaxă pentru a exclude de la scanare toate domeniile de nivel superior.
`www.example?.com`	Orice adresă web care începe cu `www.example?.com`, unde ? poate fi înlocuit cu orice caracter unic. Aceste site-uri pot include: `www.example1.com` sau `www.exampleA.com`.

Notă
Puteți utiliza adrese URL de tip „protocol-relative”.

- **Aplicație**. Exclude de la scanare procesul specificat sau aplicația specificată. Pentru a defini o excludere de scanare pentru o aplicație:
  - Introduceți întreaga cale către aplicație. De exemplu, `C:\Program Files\Internet Explorer\iexplore.exe`
  - Utilizați variabile de mediu pentru a specifica calea aplicației. De exemplu: `%programfiles%\Internet Explorer\iexplore.exe`
  - Utilizați metacaractere pentru a specifica orice aplicații care se potrivesc unui anumit model de nume. De exemplu:
    - `c*.exe` vizează toate aplicațiile care încep cu "c" (chrome.exe).
    - `??????.exe` vizează toate aplicațiile care au șase caractere în nume (chrome.exe, safari.exe, etc.).
    - `[^c]*.exe` vizează toate aplicațiile cu excepția celor care încep cu "c".
    - `[^ci]*.exe` vizează toate aplicațiile cu excepția celor care încep cu "c" sau "i".

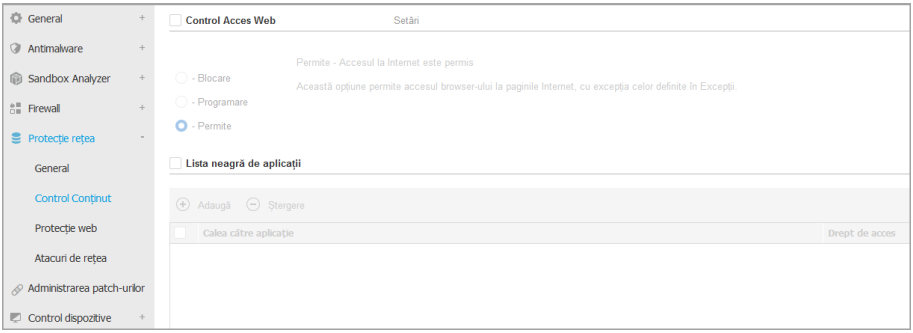
3. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului.

Pentru a elimina o entitate din listă, faceți clic pe butonul corespunzător ⊗ **Ștergere**.

Content Control

Setările de Control conținut sunt organizate în următoarele secțiuni:

- Control Acces Web
- Lista neagră de aplicații
- Protecție Date



Control Acces Web

Cu ajutorul opțiunii Web Access Control puteți permite sau bloca accesul utilizatorilor sau al aplicațiilor în anumite intervale de timp.

Paginile web blocate de Web Access Control nu sunt afișate în browser. În locul acestora se afișează o pagină web implicită, prin care utilizatorul este informat că pagina web solicitată a fost blocată de Web Access Control.

Utilizați selectorul pentru a activa sau dezactiva opțiunea **Control Acces Web**.

Dispuneți de trei opțiuni de configurare:

- Selectați **Permite** pentru a acorda întotdeauna acces web.
- Selectați **Blocare** pentru a bloca întotdeauna accesul web.
- Selectați **Programare** pentru a permite restricții de timp pentru accesul web la un program detaliat.

Indiferent dacă alegeți să permiteți sau să blocați accesul web, puteți defini excepții de la aceste acțiuni pentru toate categoriile de web sau doar pentru adresele de web specifice. Faceți clic pe **Setări** pentru a configura programul dvs. de acces web și excepțiile, după cum urmează:

Planificator

Pentru a restricționa accesul la Internet la anumite ore din zi, pe o bază săptămânală:

1. Selectați din grilă intervalele temporale în care accesul la internet doriți să fie blocat.

   Puteți face clic pe celule individuale sau puteți face clic și trage pentru a acoperi perioade mai lungi de timp. Faceți clic din nou în celulă pentru a inversa selecția.

   Pentru a începe o nouă selecție, faceți clic pe **Permite tot** sau **Blochează tot**, în funcție de tipul de restricție pe care doriți să îl puneți în aplicare.

2. Faceți clic pe **Save**.

Notă
Agentul de securitate Bitdefender va efectua actualizări în fiecare oră indiferent dacă accesul la internet este blocat.

Categorii

Filtrul de categorii web filtrează în mod dinamic accesul la site-uri web în funcție de conținutul acestora. Puteți utiliza Filtrul de categorii web pentru a defini excepții de la acțiunea de control acces web selectată (Permite sau Blochează) pentru categorii web întregi (cum ar fi jocuri, conținut matur sau Rețele Online).

Pentru a configura Filtrul de categorii web:

1. Activați **Filtru Categorii Web**.
2. Pentru o configurație rapidă, faceți clic pe unul dintre profilurile predefinite(**Agresiv**, **Normal** sau **Permisiv**). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea. Puteți vizualiza acțiunile predefinite pentru categorii web disponibile extinzând secțiunea **Reguli web** localizat mai jos.
3. Dacă setările implicite nu sunt satisfăcătoare, puteți defini dun filtru personalizat.
   a. Selectați **Personalizat**.
   b. Faceți clic pe **Reguli web** pentru a extinde secțiunea corespunzătoare.
   c. Identificați categoria pe care o doriți în listă și alegeți acțiunea dorită din meniu. Pentru mai multe informații referitoare la categoriile website disponibile, consultați acest articol KB.
4. Selectați opțiunea **Tratează categoriile web ca excepții pentru Acces Web** dacă doriți să ignorați setările de acces web existente și să aplicați numai Filtrul categoriilor web.

5. Mesajul implicit afișat utilizatorului care accesează site-uri web restricționate conține, de asemenea, categoria potrivită conținutului site-urilor web respective. Deselectați opțiunea **Afișare alerte detaliate pe client** dacă doriți ca utilizatorul să nu vadă aceste informații.

   Notă
   Această opțiune nu este disponibilă pentru macOS.

6. Faceți clic pe **Save**.

Notă

- Setarea **Permite** pentru categorii specifice de web este și ea luată în considerare în timpul intervalelor de timp când accesul la internet este blocat de Control acces web.
- Setările **Permite** funcționează numai atunci când accesul la internet este blocat de Control acces web, în timp ce permisiunile **Blocare** funcționează numai atunci când accesul web este permis de Control acces web.
- Puteți înlocui permisiunea de categorie pentru adrese web individuale, adăugându-le în lista de permisiuni opuse în **Control Acces Web > Setări > Excluderi**. De exemplu, dacă o adresă web este blocată de Filtrul Categorii Web, adăugați o regulă web pentru adresa respectivă cu caracteristica de permisiune setată pe **Permite**.

Excluderi

De asemenea, puteți defini reguli web pentru a bloca în mod explicit sau permite anumite adrese de web, modificând setările Control acces web existente. De exemplu, utilizatorii vor putea accesa o anumită pagină Web și atunci când navigarea pe web este blocată de Control acces web.

Pentru a crea o regulă web:

1. Activați opțiunea **Utilizare excepții**.
2. Introduceți adresa pe care doriți să o permiteți sau blocați în câmpul **Adresă Web**.
3. Selectați **Permite** sau**Blochează** din meniul **Permisiune**.
4. Faceți click pe butonul ⊕ **Adăugare** din partea dreaptă a tabelului pentru a adăuga adresa la lista de excepții.
5. Faceți clic pe **Save**.

Pentru a edita o regulă web:

1. Faceți clic pe adresa de web pe care doriți să o editați.
2. Modificați URL-ul existent.
3. Faceți clic pe **Save**.

Pentru a elimina o regulă web, faceți clic pe butonul ⊗ **Șterge** corespunzător.

Lista neagră de aplicații

În această secțiune, puteți configura funcția Lista neagră de aplicații, care vă ajută să blocați complet sau să restricționați accesul utilizatorilor la aplicațiile de pe calculatoarele lor. Astfel puteți bloca jocurile, fișierele video/audio și aplicațiile de mesagerie, precum și alte categorii de aplicații, inclusiv cele periculoase.

Pentru a configura Lista neagră de aplicații:

1. Activați opțiunea **Lista neagră de aplicații**.
2. Specificați aplicațiile la care doriți să restricționați accesul. Pentru a restricționa accesul la o aplicație:
   a. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Este afișată o fereastră de configurare.
   b. Trebuie să specificați calea către fișierul executabil al aplicației de pe calculatoarele țintă. Există două moduri de a face acest lucru:
      - Alegeți din meniu o locație prestabilită și completați calea după cum este necesar în câmpul de editare. De exemplu, pentru o aplicație instalată în directorul `Program Files`, selectați `%ProgramFiles%` și completați calea prin adăugarea unei bare oblice inversă (\) și numele directorului aplicației.
      - Introduceți calea completă în câmpul editabil. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.
   c. **Accesare Planificator**. Planificați accesul aplicațiilor în anumite intervale ale zilei, săptămânal:
      - Selectați din grilă intervalele de timp în care doriți să blocați accesul la aplicație. Puteți face clic pe celule individuale sau puteți face clic și trage pentru a acoperi perioade mai lungi de timp. Faceți clic din nou în celulă pentru a inversa selecția.
      - Pentru a începe o nouă selecție, faceți clic pe **Permite tot** sau **Blochează tot**, în funcție de tipul de restricție pe care doriți să îl puneți în aplicare.
      - Faceți clic pe **Save**. Noua regulă va fi adăugată în listă.

Pentru a șterge o regulă din listă, selectați-o și faceți clic pe butonul ⊗ **Ștergere** din partea de sus a tabelului. Pentru a edita o regulă existentă, faceți clic pe aceasta pentru a deschide fereastra de configurare.

Protecție Date

Modulul Protecție Date împiedică divulgarea neautorizată a datelor sensibile pe baza regulilor definite de administrator.

Notă
Această funcție nu este disponibilă pentru macOS.

Puteți crea reguli pentru a proteja orice informații personale sau confidențiale, cum ar fi:

- Informații cu caracter personal ale clientului
- Numele și detalii cheie privind produsele și tehnologiile în dezvoltare
- Informații de contact ale directorilor companiei

Informații protejate care ar putea include nume, numere de telefon, informații privind cardurile de credit și conturile bancare, adrese de e-mail și așa mai departe.

Pe baza regulilor de protecție a datelor pe care le creați, Bitdefender Endpoint Security Tools scanează traficul web și de e-mail de ieșire pentru identificarea șirurilor de caractere specifice (de exemplu, un număr de card de credit). În cazul în care există o potrivire, pagina web respectivă sau mesajul de e-mail este blocat pentru a preveni transmiterea datelor protejate. Utilizatorul este imediat informat cu privire la măsurile luate de Bitdefender Endpoint Security Tools printr-o pagină web sau e-mail de alertă.

Pentru a configura Protecția datelor:

1. Utilizați caseta de selecție pentru a activa protecția datelor.
2. Creați reguli de protecție a datelor pentru toate datele sensibile pe care doriți să le protejați. Pentru a crea o regulă:
   a. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Este afișată o fereastră de configurare.
   b. Introduceți numele cu care regula va fi introdusă în tabelul de reguli. Alegeți un nume sugestiv, astfel încât dvs. sau alt administrator să poată identifica cu ușurință la ce se referă regula.

c. Selectați tipul de date pe care doriți să le protejați.

d. Introduceți datele pe care doriți să le protejați (de exemplu, numărul de telefon al unui director de companie sau numele intern al unui nou produs al companiei care este în lucru). Este aceptată orice combinație de cuvinte, numere sau șiruri de caractere formate din caractere alfanumerice și speciale (cum ar fi @, # sau $).

   Asigurați-vă ca introduceți cel puțin cinci caractere pentru a evita blocarea greșită a unor mesaje și pagini web.

   Important

   Datele furnizate sunt stocate în formă criptată pe stațiile de lucru protejate, dar se pot vizualiza în contul dvs. de Control Center. Pentru mai multă siguranță, nu introduceți toate datele pe care vreți să le protejați. În acest caz, trebuie să debifați opțiunea **Potrivire cuvinte întregi**.

e. Configurați opțiunile de scanare trafic după cum este cazul:

   - **Scanare trafic web (HTTP)** - scanează traficul web (HTTP) și blochează la ieșire toate datele care corespund unei reguli.
   - **Scanare trafic e-mail (SMTP)** - scanează traficul mail (SMTP) și blochează trimiterea mesajelor e-mail care corespund unei reguli.

   Puteți alege să aplicați regula doar dacă datele protejate apar ca șir independent sau ținând cont de majuscule și minuscule.

f. Faceți clic pe **Save**. Noua regulă va fi adăugată în listă.

3. Configurați excepțiile de la regulile de protecție a datelor astfel încât utilizatorii să continue să poată trimite date protejate către site-uri autorizate și beneficiari. Excluderile se pot aplica la nivel global (la toate regulile) sau numai la anumite reguli. Pentru a adăuga o excludere:
   a. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Este afișată o fereastră de configurare.
   b. Introduceți adresa de web sau de e-mail către care utilizatorii sunt autorizați să divulge date protejate.
   c. Selectați tipul de excludere (web sau adresa de e-mail).
   d. Din tabelul **Reguli**, selectați regulile de protecție a datelor la care ar trebui să se aplice această excludere.
   e. Faceți clic pe **Save**. Noua regulă de excludere va fi adăugată în listă.

Notă
În cazul în care un e-mail care conține date blocate este adresat mai multor destinatari, acesta va fi primit de cei pentru care au fost definite excluderi.

Pentru a elimina o regulă sau o excludere din listă, faceți clic pe butonul corespunzător ⊗ **Ștergere** din partea dreaptă a tabelului.

Protecție web

În această pagină, setările sunt organizate în următoarele secțiuni:

- Antiphishing
- Scanare trafic web

Politici computere și mașini virtuale - Protecție rețea - Protecție web

Antiphishing

Protecția antiphishing blochează automat paginile web de phishing cunoscute pentru a împiedica utilizatorii să divulge accidental informații private sau confidențiale unor infractori online. În loc de pagina de web de phishing, în browser este afișată o pagină de avertizare specială de informare a utilizatorului că pagina web solicitată este periculoasă.

Selectați **Antiphishing** pentru a activa protecția antiphishing. Puteți optimiza în continuare Antiphishing prin configurarea următoarelor setări:

- **Protecție împotriva fraudelor**. Selectați această opțiune dacă doriți să extindeți protecția și la alte tipuri de escrocherii în afară de phishing. De exemplu, site-uri care reprezintă companii false, care nu solicită în mod direct informații private, dar în schimb încearcă să pozeze ca afaceri legitime și să obțină profit prin determinarea oamenilor să facă afaceri cu ei.

- **Protecție împotriva tentativelor de phishing**. Păstrați această opțiune selectată pentru a proteja utilizatorii împotriva tentativelor de phishing.

În cazul în care o pagină web legitimă este incorect detectat ca phishing și blocată, o puteți adăuga la lista albă pentru a permite utilizatorilor accesarea acesteia. Este recomandat ca lista să conțină doar site-uri web în care aveți deplină încredere.

Pentru a gestiona excepțiile antiphishing:

1. Accesați setările din categoria **General** și selectați **Excepții globale**.
2. Introduceți adresa de web și faceți clic pe butonul ⊕ **Adăugare**.

   Dacă doriți să excludeți un întreg site, scrieți numele domeniului, cum ar fi `http://www.website.com` și dacă doriți să excludeți doar o pagină web, scrieți adresa web exactă a paginii respective.

   Notă
   Caracterele de înlocuire nu se acceptă în crearea URL-urilor.

3. Pentru a elimina o excepție din listă, faceți clic pe butonul corespunzător ⊗ **Ștergere**.
4. Faceți clic pe **Save**.

Scanare trafic web

E-mailurile primite (POP3) și traficul web sunt scanate în timp real pentru a preveni descărcarea de programe malware pe stația de lucru. E-mailurile trimise (SMTP) sunt scanate pentru a preveni infectarea altor stații de lucru cu programe malware. Scanarea traficului web poate încetini puțin navigarea pe internet, însă aceasta va bloca programele malware provenite de pe internet, inclusiv descărcările ascunse.

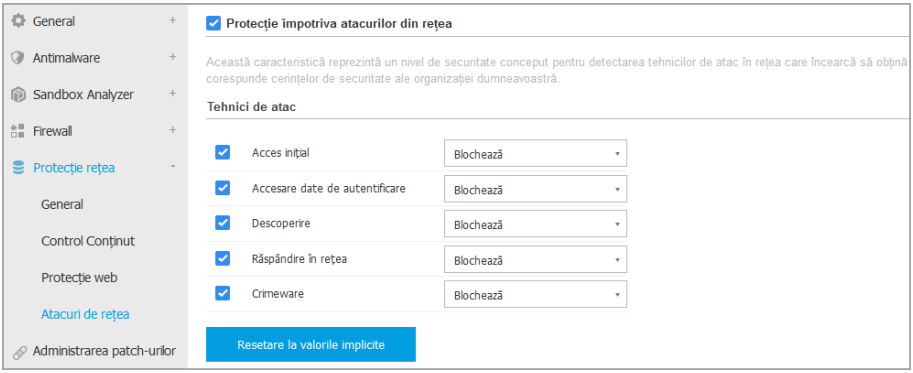
Când un e-mail este găsit infectat, acesta este înlocuit automat cu un e-mail standard de informare a destinatarului cu privire la e-mailul infectat original. În cazul în care o pagină web conține sau distribuie malware, aceasta este blocată în mod automat. În schimb este afișată pagină de avertizare specială pentru informarea utilizatorului că pagina web solicitată este periculoasă.

Deși nu se recomandă, puteți dezactiva scanarea traficului e-mail și web pentru a îmbunătăți performanțele sistemului. Aceasta nu este o amenințare majoră atâta timp cât scanarea la accesarea fișierelor locale rămâne activată.

Notă
Opțiuni **E-mail-uri primite** și **E-mail-uri expediate** nu sunt disponibile pentru macOS.

Atacuri de rețea

Network Attack Defense oferă un nivel de securitate bazat pe o tehnologie Bitdefender care detectează și acționează împotriva atacurilor în rețea concepute pentru obținerea de drepturi de acces pe endpoint-uri folosind anumite tehnici, cum ar fi: atacuri de tip „brute-force”, exploit-uri în rețea sau furt de parole.



Politici computere și mașini virtuale - Protecție rețea - Atacuri în rețea

Pentru a configura Network Attack Defense:

1. Bifați căsuța **Network Attack Defense** pentru a activa modulul.
2. Bifați căsuțele aferente pentru a activa protecția împotriva fiecărei categorii de atacuri în rețea. Tehnicile de atac în rețea sunt grupate în funcție de baza de cunoștințe MITRE ATT&CK după cum urmează:
   - **Acces inițial** - atacatorul obține acces într-o rețea prin diferite metode, inclusiv vulnerabilitățile serverelor web publice. De exemplu, exploit-uri de dezvăluire de date, exploit-uri de injectare SQL, vectori de injectare drive-by download.
   - **Acces la datele de autentificare** - atacatorul fură date de autentificare, cum ar fi nume de utilizator și parole, pentru a obține drepturi de acces la sisteme. De exemplu: atacuri de tip „brute-force”, exploit-uri de autentificare neautorizată, furturi de parole.

- **Descoperire** - odată infiltrat, atacatorul încearcă să obțină informații despre sisteme și rețelele interne înainte de a-și decide următoarele mișcări. De exemplu: exploit-uri de tip „directory traversal”, exploit-uri HTTP de tip „directory traversal”.
- **Răspândire în rețea** - atacatorul explorează rețeaua, adesea prin răspândirea în mai multe sisteme, pentru a găsi ținta principală. Atacatorul poate utiliza anumite instrumente pentru a-și atinge obiectivele. De exemplu: exploit-uri de injectare a comenzilor, exploit-uri Shellshock, exploit-uri cu extensie dublă.
- **Crimeware** - această categorie cuprinde tehnicile concepute pentru automatizarea infracțiunilor cibernetice. De exemplu, tehnicile de crimeware sunt: exploit-uri nucleare, diferite software-uri malware, cum ar fi troienii sau bot-urile.

3. Selectați acțiunile pe care doriți să le întreprindeți împotriva fiecărei categorii de tehnici de atac în rețea dintre următoarele opțiuni:
   a. **Blocare** - Modulul Network Attack Defense oprește tentativele de atac detectate.
   b. **Doar raportare** - Network Attack Defense vă informează cu privire la tentativele de atac detectate, dar nu va încerca să le oprească.

Puteți restabili cu ușurință setările inițiale selectând opțiunea **Revenire la setările implicite** din partea de jos a paginii.

Informațiile referitoare la tentativele de atac în rețea sunt disponibile în raportul de incidente în rețea și în notificarea evenimentului de incidente în rețea.

7.2.7. Administrarea patch-urilor

Notă
Acest modul este disponibil pentru:

- Windows pentru stații de lucru
- Windows pentru servere

Modulul Patch Management vă eliberează de povara actualizării stațiilor de lucru cu cele mai recente patch-uri de software distribuind și instalând automat patch-urile pentru o gamă largă de produse.

Notă
Puteți consulta lista producătorilor și a produselor suportate în acest articol KB.

Această secțiune privind politica include setările pentru instalarea automată a patch-urilor. Mai întâi, veți configura modul în care patch-urile sunt descărcate pe stațiile de lucru și apoi ce patch-uri trebuie instalate și când.

Configurarea setărilor pentru descărcarea patch-urilor

Procesul de distribuire a patch-urilor folosește servere de cache pentru patch-uri pentru a optimiza traficul în rețea. Stațiile de lucru se conectează la aceste servere și descarcă patch-urile prin intermediul rețelei locale. Pentru patch-urile cu grad mare de disponibilitate, se recomandă să folosiți mai multe servere.

Pentru a atribui stațiilor de lucru vizate servere de cache pentru patch-uri:

1. La secțiunea **Setări descărcare patch-uri**, efectuați clic pe câmpul din partea de sus a tabelului. Se afișează lista de servere de cache pentru patch-uri detectate.

   Dacă lista este goală, atunci este necesar să instalați rolul de server de cache pentru patch-uri pe releele din rețeaua dumneavoastră. Pentru informații suplimentare, consultați Ghidul de instalare.

2. Selectați din listă serverul dorit.
3. Faceți clic pe butonul ⊕ **Adăugare**.
4. Repetați pașii anteriori pentru a adăuga mai multe servere, dacă este nevoie.
5. Folosiți săgețile sus și jos din partea dreaptă a tabelului pentru a stabili prioritatea serverelor. Prioritatea scade de sus în josul listei.

   O stație de lucru solicită un patch de la serverele atribuite în ordinea priorităților. Stația de lucru descarcă patch-ul de pe primul server pe care îl găsește. Un server care nu conține un patch solicitat îl va descărca automat de pe site-ul producătorului pentru a-l putea pune la dispoziție la următoarele solicitări.

Pentru a șterge serverele de care nu mai aveți nevoie, efectuați clic pe butonul de ⊖ Ștergere corespunzător din partea dreaptă a tabelului.

Selectați opțiunea **Utilizează site-urile furnizorilor ca locație de fallback pentru descărcarea patch-urilor** pentru a vă asigura că stațiile de lucru primesc patch-urile de software în cazul în care serverele de cache pentru patch-uri sunt indisponibile.

Configurarea scanării patch-urilor și instalarea acestora

GravityZone efectuează configurarea patch-urilor în două faze independente:

1. Evaluare. La transmiterea unei solicitări de pe consola de administrare, stațiile de lucru scanează patch-urile lipsă și generează un raport al acestora.
2. Instalare. Consola trimite către agenți o listă de patch-uri pe care ar trebui să le instalați. Stația de lucru descarcă patch-urile de pe serverul de cache pentru patch-uri și apoi le instalează.

Politica furnizează setările pentru automatizarea acestor procese, parțial sau integral, astfel încât acestea să fie executate periodic pe baza graficului preferat.

Pentru a configura scanarea automată a patch-urilor:

1. Bifați caseta **Scanare automată a patch-urilor**.
2. Folosiți opțiunile de programare pentru a configura recurența scanărilor. Puteți seta scanarea astfel încât să fie executată zilnic sau în anumite zile ale săptămânii, la o anumită oră.
3. Selectați **Scanare inteligentă la instalarea unui nou program/unei noi aplicații** pentru a detecta când este instalată o nouă aplicație pe endpoint și patch-urile disponibile pentru aceasta.

Pentru a configura instalarea automată a patch-urilor:

1. Bifați caseta **Instalează patch-urile automat după scanare**.
2. Selectați ce tipuri de patch-uri doriți să instalați: securitate, altele sau ambele.
3. Utilizați opțiunile de programare pentru a configura când să fie executate sarcinile de instalare. Puteți seta scanarea astfel încât să fie executată imediat după finalizarea scanării patch-urilor, zilnic sau în anumite zile ale săptămânii, la o anumită oră. Vă recomandăm să instalați patch-urile de securitate imediat ce acestea sunt identificate.
4. În mod implicit, toate produsele sunt eligibile pentru aplicarea patch-urilor. Dacă doriți să actualizați automat numai o serie de produse, pe care le considerați esențiale pentru afacerea dumneavoastră, urmați acești pași:
   a. Bifați caseta **Un anumit furnizor și produs**.
   b. Efectuați clic pe câmpul **Producător** din partea de sus a tabelului. Se afișează o listă cu toți producătorii suportați.

c. Parcurgeți lista și selectați un producător pentru produsele pentru care doriți să aplicați patch-urile.

d. Efectuați clic pe câmpul **Produse** din partea de sus a tabelului. Se afișează o listă cu toate produsele producătorului selectat.

e. Selectați toate produsele pentru care doriți să aplicați patch-urile.

f. Faceți clic pe butonul ⊕ **Adăugare**.

g. Repetați pașii anterior pentru restul producătorilor și produselor.

   Dacă ați uitat să adăugați un produs sau doriți să eliminați unul, căutați producătorul în tabel, efectuați dublu clic pe câmpul **Produse** și selectați sau deselectați produsul din listă.

Pentru a elimina din listă un producător cu toate produsele sale, identificați-l în tabel și efectuați clic pe butonul de ⊖ **Ștergere** corespunzător din partea dreaptă a tabelului.

5. Din diverse motive, o stație de lucru poate fi offline atunci când este programată executarea unei instalări de patch. Selectați opțiunea **Dacă este ratată, executați cât mai curând posibil** pentru a instala patch-urile imediat ce stația de lucru este din nou online.

6. Unele patch-uri pot necesita repornirea sistemului pentru finalizarea instalării. Dacă doriți să faceți acest lucru manual, selectați opțiunea **Amânare repornire**.

Important
Pentru ca evaluarea și instalarea să se desfășoare cu succes pe stațiile de lucru Windows, este necesar să vă asigurați că sunt îndeplinite următoarele cerințe:

- **Trusted Root Certification Authorities** stochează certificatul **DigiCert Assured ID Root CA**.
- **Intermediate Certification Authorities** include **DigiCert SHA2 Assured ID Code Signing CA**.
- Endpoint-urile au instalat patch-urile pentru Windows 7 și Windows Server 2008 R2 menționate în acest articol Microsoft: Microsoft Security Advisory 3033929

7.2.8. Application Control

Notă
Acest modul este disponibil pentru:

- Windows pentru stații de lucru
- Windows pentru servere

Modulul Control aplicații adaugă un nivel suplimentar de protecție împotriva tuturor tipurilor de amenințări de tip malware (ransomware, atacuri de tip „zero-day”, exploit-uri ale aplicațiilor terțe, troieni, spyware, rootkit-uri, adware etc.) prin blocarea rulării aplicațiilor și proceselor neautorizate. Modulul Control aplicații reduce suprafața de atac de care pot profita amenințările malware de pe stațiile de lucru și previne instalarea și executarea oricăror aplicații nedorite, nesigure sau periculoase.

Modulul Control aplicații pune în aplicare politici flexibile, care vă permit să includeți aplicații în lista albă și să gestionați drepturile de actualizare.

Application Control

Important

- Pentru a activa modulul **Control aplicații** pentru clienții instalați, executați sarcina **Reconfigurare client**. După instalarea modulului, puteți vizualiza starea acestuia în fereastra**Informații**.
- Modulul Control aplicații afectează modul Utilizator privilegiat după aplicarea actualizărilor. De exemplu, atunci când se actualizează o aplicație inclusă în lista albă, stația de lucru trimite noile informații. GravityZone actualizează regula cu noile valori și retrimite politica.

Trebuie să executați sarcina **Descoperire aplicații** pentru a vizualiza aplicațiile și procesele aflate în curs de execuție în rețeaua dumneavoastră. Pentru mai multe informații, consultați capitolul „Descoperire aplicații” (p. 101). Apoi, puteți defini regulile modulului Control aplicații.

Modulul Control aplicații funcționează în două moduri:

- **Mod de testare**. Modulul Control aplicații doar detectează și raportează aplicațiile în Control Center, lăsându-le să funcționeze ca de obicei. Puteți configura și

testa regulile și politicile dvs. de trecere în lista albă, însă aplicațiile nu vor fi blocate.

- **Mod de producție**. Funcția Control aplicații blochează toate aplicațiile necunoscute. Procesele sistemelor de operare Microsoft și procesele Bitdefender sunt trecut în lista albă implicit. Se va permite executarea aplicațiilor definite și trecute în lista albă. Pentru a actualiza aplicațiile trecute în lista albă, trebuie să definiți programe de actualizare. Acestea sunt procese specifice, care au dreptul de a modifica aplicațiile existente. Pentru mai multe informații, consultați capitolul „Inventar aplicații" (p. 193).

Avertisment

- Pentru a vă asigura că modulul Control aplicații nu restricționează aplicații legitime, trebuie să executați acest modul mai întâi în modul de testare. Astfel, vă puteți asigura că regulile și politicile de trecere pe lista albă sunt definite în mod corespunzător.
- Procesele care sunt deja în curs în momentul trecerii modulului Control aplicații în **Modul de producție** vor fi blocate după următoarea repornire a proceselor.

Pentru a administra drepturile de execuție ale aplicațiilor:

1. Bifați caseta **Control aplicații** pentru a activa acest modul.
2. Utilizați caseta **Executare în Modul de testare** pentru a activa sau dezactiva Modul de testare.

Notă

- În modul de testare, veți primi o notificare în cazul în care modulul Control aplicații blochează o anumită aplicație. Pentru mai multe informații, consultați capitolul „Tipuri de notificări" (p. 535).
- În Zona de notificare se vor afișa notificări de **Aplicații blocate** atunci când sunt detectate noi aplicații și când sunt blocate aplicațiile incluse în lista neagră.

3. Definiți regulile de pornire proces.

Reguli pornire proces

Funcția Control aplicații vă permite să autorizați manual aplicații și procese specifice, în baza codului hash al fișierului executabil, a amprentei certificatului și a căii aplicației. De asemenea, puteți defini excepții pentru reguli.

Notă
Pentru a obține valorile personalizate pentru codul hash al fișierului executabil și amprenta certificatului folosiți„Instrumente Control aplicații” (p. 570)

Tabelul **Reguli pornire proces** vă informează cu privire la regulile existente, oferindu-vă informații importante:

- Prioritatea regulii. Regula cu prioritatea mai mare va fi mai aproape de partea de sus a listei.
- Numele și starea regulii.
- Aplicațiile țintă și drepturi de execuție ale acestora. Ținta reprezintă numărul de condiții ce trebuie îndeplinite pentru ca regula să se aplice, sau numărul de aplicații sau grupuri pentru care se aplică regula.

Pentru a crea o regulă de pornire proces:

1. Faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului pentru a deschide fereastra de configurare.
2. În secțiunea **General**, introduceți un**Nume de regulă**.
3. Bifați caseta **Activat** pentru a activa regula.
4. În secțiunea **Ținte**, specificați destinația regulii:
   - **Procese specifice**, pentru a defini un proces a cărui pornire este permisă sau respinsă. Puteți face autorizarea în funcție de cale, codul hash sau certificat. Condițiile din cadrul regulii sunt potrivite cu ajutorul operatorului logic AND.
     – Pentru a autoriza o aplicație dintr-o cale specifică:
       a. Selectați **Cale** în coloana **Tip**. Specificați calea către obiect. Puteți specifica un nume de cale absolut sau relativ și puteți utiliza caractere wildcard. Simbolul asterisc (*) corespunde oricărui fișier dintr-un director. Un simbol asterisc dublu (**) se potrivește cu toate fișierele și directoarele din directorul definit. Semnul întrebării (?) corespunde

unui singur caracter. De asemenea, puteți adăuga o descriere pentru a ajuta la identificarea procesului.

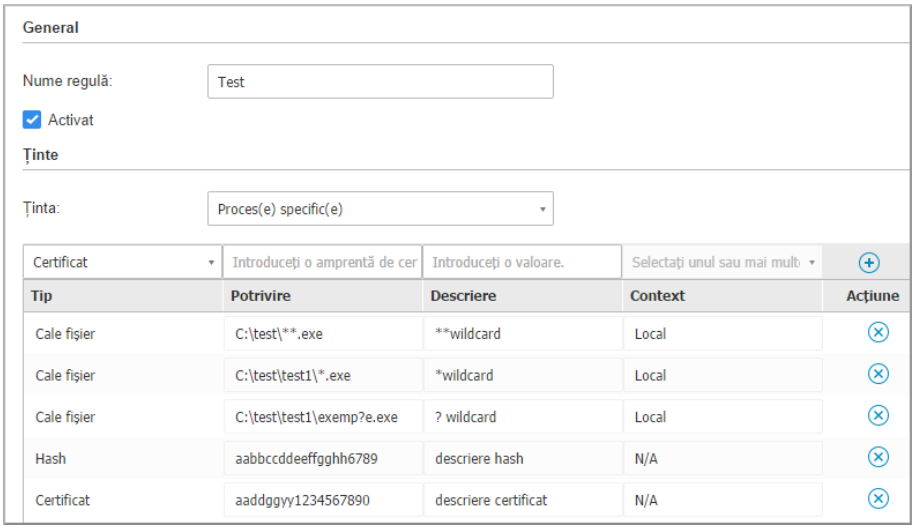
b. Din meniul derulant **Selectați unul sau mai multe contexte** puteți alege între local, CD-ROM, unitate detașabilă și rețea. Puteți bloca o aplicație executată de pe o unitate detașabilă sau puteți permite executarea acesteia dacă aplicația este executată local.

– Pentru a autoriza o aplicație pe baza codului hash, selectați **Hash** din coloana **Tip** și introduceți o valoare hash. De asemenea, puteți adăuga o descriere pentru a ajuta la identificarea procesului.

Important
Pentru a genera valoarea hash, descărcați instrumentul Amprentă. Pentru mai multe informații, consultați capitolul „Instrumente Control aplicații” (p. 570)

– Pentru a efectua autorizarea pe baza certificatului, selectați **Certificat** din coloana **Tip** și introduceți o amprentă de certificat. De asemenea, puteți adăuga o descriere pentru a ajuta la identificarea procesului.

Important
Pentru a obține o amprentă de certificat, descărcați instrumentul Amprentă. Pentru mai multe informații, consultați capitolul „Instrumente Control aplicații” (p. 570)



Reguli privind aplicația

Faceți clic pe ⊕**Adăugare** pentru a adăuga regula.

- **Aplicații sau grupuri inventar**, pentru a adăuga un grup sau o aplicație descoperită în rețeaua dumneavoastră. Puteți vizualiz aplicațiile în curs de execuție în rețeaua dumneavoastră în pagina **Rețea > Inventar aplicații**. Pentru mai multe informații, consultați capitolul „Inventar aplicații” (p. 193).

  Introduceți denumirile aplicațiilor sau grupurilor în câmpul corespunzător, separate prin virgulă. Funcția de completare automată va afișa sugestii pe măsură ce tastați.

5. Bifați caseta **Includere subprocese** pentru a aplica regula la procese subordonate generate.

Avertisment
Atunci când configurați reguli pentru aplicațiile de browser, se recomandă să dezactivați această opțiune pentru a preveni riscurile de securitate.

6. Opțional, puteți defini excepții de la regula de pornire a proceselor. Operațiunea de adăugare este similară celei descrise la pașii anteriori.

7. În secțiunea **Drepturi de acces**, alegeți dacă să permiteți sau să interziceți executarea regulii.
8. Faceți clic pe **Salvare** pentru a aplica modificările.

Pentru a edita o regulă existentă:

1. Faceți clic pe denumirea regulii pentru a deschide fereastra de configurare.
2. Introduceți valorile noi pentru opțiunile pe care doriți să le modificați.
3. Faceți clic pe **Salvare** pentru a aplica modificările.

Pentru a seta prioritatea regulii:

1. Bifați caseta corespunzătoare regulii dorite.
2. Utilizați butoanele de prioritate din partea dreaptă a tabelului:
   - Efectuați clic pe butonul **Sus** pentru a muta mai sus regula selectată.
   - Faceți clic pe butonul **Jos** pentru a o retrograda.

Puteți șterge una sau mai multe reguli simultan. Nu trebuie decât să:

1. Selectați regulile pe care doriți să le ștergeți.
2. Faceți clic pe butonul **Ștergere** din partea de sus a tabelului. Regulile nu mai pot fi recuperate după ce au fost șterse.

7.2.9. Device Control

Notă
Acest modul este disponibil pentru:

- Windows pentru stații de lucru
- Windows pentru servere
- macOS

Modulul de control al dispozitivelor previne, de asemenea, scurgerea de informații confidențiale și infecțiile cu programe periculoase prin intermediul dispozitivelor externe atașate la stațiile de lucru prin aplicarea unor reguli de blocare și a unor excepții folosind politicile de securitate pentru o gamă largă de dispozitive.

Important
Pentru macOS, Controlul dispozitivelor se bazează pe extensia nucleului. Instalarea unei extensii kernel necesită aprobarea utilizatorului pe macOS High Sierra (10.13)

sau mai recent. Sistemul informează utilizatorul că o extensie de sistem de la Bitdefender a fost blocată. O puteți accepta din **Securitate & Confidentialitate** preferinte. Până când utilizatorul acceptă extensia de sistem Bitdefender, acest modul nu va funcționa, iar pe interfața utilizatorului Endpoint Security for Mac se afișa un mesaj de problemă critică pentru care este necesară aprobarea dvs.
Pentru a elimina intervenția utilizatorului, puteți pre-aproba extensia kernel a Bitdefender prin adăugarea ei în lista de excepții utilizând un instrument de administrare a dispozitivelor mobile. Pentru detalii despre extensiile de kernel ale Bitdefender, consultați acest articol din Baza de cunoștințe.

Pentru a folosi modulul Control dispozitiv, trebuie să îl includeți mai întâi în agentul de securitate instalat pe stațiile de lucru țintă și apoi să activați opțiunea **Control dispozitiv** în politica aplicată acestor stații de lucru. Apoi, de fiecare dată când dispozitivul este conectat la o stație de lucru administrată, agentul de securitate va expedia informații referitoare la acest eveniment către Control Center, inclusiv denumirea dispozitivului, clasa, codul și data și ora conectării.

În tabelul de mai jos, regăsiți tipurile de dispozitive acceptate de modulul Control dispozitive pe sistemele Windows și macOS:

Tip dispozitiv	Windows	macOS
Adaptoare Bluetooth	x	x
Dispozitive CD-ROM	x	x
Unități dischetă	x	N/A
IEEE 1284.4	x	
IEEE 1394	x	
Dispozitive de imagine	x	x
Modemuri	x	Administrate din Adaptoare rețea
Unități cu bandă magnetică	x	N/A
Windows portabil	x	x
Porturi COM/LPT	x	LPT pe porturile seriale compatibile
Raid SCSI	x	
Imprimante	x	Compatibil doar cu imprimantele conectate local
Adaptor rețea	x	x (inclusiv dongle-uri Wi-Fi)

Tip dispozitiv	Windows	macOS
Adaptoare de rețea wireless	x	x
Memorie internă	x	
Memorie externă	x	x

Notă

- Pe macOS, dacă se selectează dreptul de acces **Personalizat** pentru o anumită clasă de dispozitive, va fi valabil doar dreptul de acces configurat pentru subcategoria **Altele**.
- Pe Windows și macOS, funcția „Control dispozitive" permite sau respinge complet accesul la adaptorul Bluetooth la nivel de sistem, în funcție de setările politicii de securitate. Nu există posibilitatea de a seta excepții granulare pentru fiecare dispozitiv asociat.

Funcția Control dispozitive permite și administrarea permisiunilor aferente dispozitivului, după cum urmează:

- Definiți regulile permisiunilor
- Definiți excepțiile permisiunilor

Reguli

Secțiunea **Reguli** permite definirea permisiunnilor pentru dispozitivele conectate la stațiile de lucru țintă.

Pentru configurarea permisiunilor pentru tipul de dispozitiv dorit:

1. Mergeți la **Control dispozitive > Reguli**.
2. Faceți clic pe denumirea dispozitivului din tabelul disponibil.
3. Selectați un tip de permisiune dintre opțiunile disponibile. Vă rugăm să rețineți că setul de permisiuni disponibile poate diferi în funcție de tipul de dispozitiv:
   - **Permis**: dispozitivul poate fi folosit pe stația de lucru țintă.
   - **Blocat**: dispozitivul nu poate fi folosit pe stația de lucru țintă. În acest caz, de fiecare dată când dispozitivul este conectat la stația de lucru, agentul de securitate va afișa o informare că dispozitivul a fost blocat.

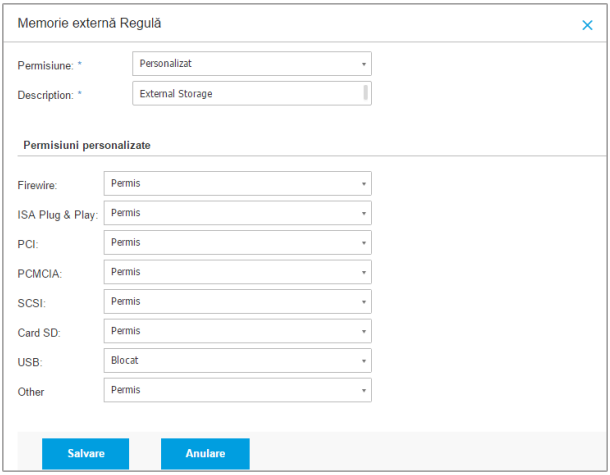
Important

Dispozitivele conectate care au fost blocate anterior nu sunt deblocate automat prin modificarea dreptului de acces la valoarea **Permis**. Utilizatorul

trebuie să repornească sistemul sau să reconecteze dispozitivul pentru a-l putea utiliza.

- **Doar citire**: pe dispozitiv pot fi folosite doar funcțiile de citire.
- **Personalizat**: definiți permisiuni diferite pentru fiecare tip de port de pe același dispozitiv, cum ar fi Firewire, ISA Plug & Play, PCI, PCMCIA, USB, etc. În acest caz, se afișează lista componentelor disponibile pentru dispozitivul selectat și puteți configura permisiunile dorite pentru fiecare calculator.

  De exemplu, pentru Memorie externă, puteți bloca doar USB și permite utilizarea tuturor celorlalte porturi.



Politici referitoare la calculatoare și mașini virtuale - Controlul dispozitivelor - Reguli

Excluderi

După ce ați configurat regulile de permisiuni pentru diferitele tipuri de dispozitive, vă recomandăm să excludeți anumite tipuri de dispozitive sau produse din aceste reguli.

Puteți defini dispozitivele excluse:

- După Cod dispozitiv (sau Cod hardware), pentru desemnarea dispozitivelor individuale pe care doriți să le excludeți.

- După Cod produs (sau PID), pentru a desemna o gamă de dispozitiv realizate de același producător.

Pentru a defini regulile de excludere a dispozitivelor:

1. Mergeți la **Control dispozitive > Excepții**.
2. Activați opțiunea **Excepții**.
3. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului.
4. Selectați metoda pe care doriți să o utilizați pentru adăugarea excepțiilor:
   - **Manual**. În acest caz, trebuie să introduceți codul fiecărui Dispozitiv sau codul Produsului pe care doriți să îl excludeți, cu condiția să aveți la îndemână lista codurilor corespunzătoare:
     a. Selectați tipul de excepții (după Cod produs sau Cod dispozitiv).
     b. În câmpul **Excepții**, introduceți codurile pe care doriți să le excludeți.
     c. În câmpul **Descriere**, introduceți o denumire care să vă ajute să identificați dispozitivul sau gama de dispozitive.
     d. Selectați tipul de permisiune pentru anumite dispozitive (**Permis** or **Blocat**).
     e. Faceți clic pe **Save**.

     Notă
     Puteți să configurați manual excepții cu metacaractere pe baza ID-ului dispozitivului, utilizând sintaxa `wildcards:deviceID`. Folosiți semnul întrebării (?) pentru a înlocui un caracter și asteriscul (*) pentru a înlocui orice număr de caractere din `deviceID`. De exemplu, pentru `wildcards:PCI\VEN_8086*`, toate dispozitivele care conțin string-ul `PCI\VEN_8086` în ID-ul lor vor fi excluse din regula de aplicare a politicii.

   - **Din dispozitivele descoperite**. În acest caz, puteți selecta Codurile dispozitivelor sau Codurile produselor pe care doriți să le excludeți dintr-o listă a tuturor dispozitivelor descoperite în rețeaua dvs. (exclusiv pentru stațiile de lucru administrate):
     a. Selectați tipul de excepții (după Cod produs sau Cod dispozitiv).
     b. În tabelul **Excepții**, selectați codurile pe care doriți să le excludeți:
        – Pentru Codurile dispozitivelor, selectați fiecare dispozitiv pe care doriți să îl excludeți din listă.

– Pentru Codurile produselor, dacă selectați un dispozitiv, veți exclude toate celelalte dispozitive cu același Cod de produs.

c. În câmpul **Descriere**, introduceți o denumire care să vă ajute să identificați dispozitivul sau gama de dispozitive.

d. Selectați tipul de permisiune pentru anumite dispozitive (**Permis** or **Blocat**).

e. Faceți clic pe **Save**.

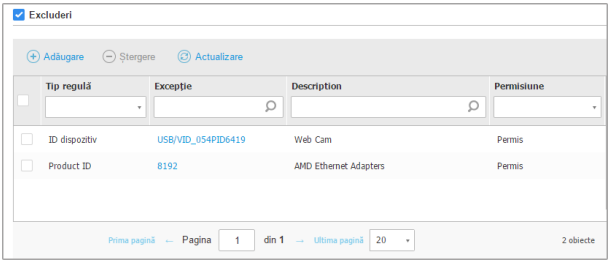
Important

- Dispozitivele conectate deja la stațiile de lucru la instalarea Bitdefender Endpoint Security Tools vor fi descoperite numai după repornirea stațiilor de lucru corespunzătoare.
- Dispozitivele conectate care au fost blocate anterior nu sunt deblocate automat prin setarea unei excepții cu dreptul de acces **Permis**. Utilizatorul trebuie să repornească sistemul sau să reconecteze dispozitivul pentru a-l putea utiliza.

Toate dispozitivele excluse se afișează în tabelul **Excepții**.

Pentru eliminarea unei excepții:

1. Selectați-o din tabel.
2. Faceți clic pe butonul **Ștergere** din partea de sus a tabelului.



Politici referitoare la calculatoare și mașini virtuale - Controlul dispozitivelor - Excepții

7.2.10. Relay

Notă

Acest modul este disponibil pentru:

- Windows pentru stații de lucru

- Windows pentru servere
- Linux

Această secțiune vă permite să definiți setări de comunicare și actualizare pentru stațiile de lucru țintă cărora li s-a alocat rolul de releu.

Setările sunt organizate în următoarele secțiuni:

- Comunicații
- Actualizare

Comunicații

Secțiunea **Comunicare** include preferințele proxy pentru comunicarea între stațiile de lucru releu și componentele GravityZone.

Dacă este necesar, puteți configura independent comunicarea dintre stațiile de lucru releu țintă și Serviciile Cloud Bitdefender/ GravityZone , folosind următoarele setări:

- **Păstrează setările de instalare**, pentru a folosi aceleași setări proxy ca și cele definite în pachetul de instalare.
- **Folosește proxy-ul definit în secțiunea General**, pentru a folosi setările proxy definite în politica curentă, în secțiunea **General > Setări**.
- **Nu folosi**, dacă stațiile de lucru țintă nu comunică cu componentele Bitdefender specifice printr-un proxy.

Actualizare

Această secțiune vă permite să definiți setările de actualizare pentru stațiile de lucru țintă cu rol de releu:

- În secțiunea **Actualizare**, puteți configura următoarele setări:
  - Intervalul de timp la care stațiile de lucru releu verifică dacă sunt disponibile actualizări.
  - Directorul de pe stația de lucru releu pe care se descarcp și sunt oglindite actualizările de produs și de semnătură. Dacă doriți să definiți un anumit director de descărcare, introduceți calea completă în câmpul corespunzător.

Important
Se recomană definirea unui director dedicat pentru produs și actualizările de semnătură. Evitați selectarea unui director cu fișiere de sistem sau personale.

- **Definiți locații personalizate pentru actualizare**. Locația implicită de actualizare pentru agenții releu este serverul local de actualizări GravityZone. Puteți specifica alte locații de actualizare introducând IP-ul sau numele de gazdă locală al unuia sau mai multor servere de actualizare din rețeaua dvs., configurând apoi prioritatea acestora cu ajutorul butoanelor sus/jos care se afișează atunci când poziționați mouse-ul deasupra acestora. Dacă prima locație de actualizare nu este disponibilă, se utilizează următoarea și așa mai departe.

  Pentru a defini o locație personalizată pentru actualizări:

  1. Activați opțiunea **Definire locații personalizate pentru actualizări**.
  2. Introduceți adresa noului server de actualizări în câmpul **Adăugare locație**. Utilizați una dintre aceste sintaxe:
     - `ip_server_actualizări:port`
     - `nume_server_actualizări:port`

     Portul implicit este 7074.
  3. În cazul în care stația de lucru releu comunică cu serverul local de actualizări, printr-un server proxy, selectați **Folosește Proxy**. Vor fi luate în considerare setările proxy definite în secțiunea **General > Setări**.
  4. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului.
  5. Folosiți săgețile ⌃ Sus / ⌄ Jos din coloana **Acțiune** pentru a seta prioritatea locațiilor de actualizare definite. Dacă prima locație de actualizare nu este disponibilă, se verifică următoarea și așa mai departe.

  Pentru a elimina o locație din listă, faceți clic pe butonul corespunzător ⊗ **Ștergere**. Deși puteți elimina adresa implicită a locației de actualizare, acest lucru nu este recomandat.

7.2.11. Protecție Exchange

Notă
Acest modul este disponibil pentru Windows pentru servere.

Security for Exchange include setări cu posibilități extinse de configurare, care protejează serverele Microsoft Exchange Servers contra amenințărilor de tip malware, spam și phishing. Cu Protecția Exchange instalată pe serverul e-mail, puteți filtra mesajele e-mail cu atașamente sau conținut considerat periculos conform politicilor de securitate ale companiei.

Pentru a menține performanțele serverului la niveluri normale, traficul e-mail este procesat de filtrele Security for Exchange în ordinea următoare:

1. Filtrare antispam
2. Controlul conținutului > Filtrarea conținutului
3. Controlul conținutului > Filtrarea atașamentelor
4. Filtrare antimalware

Setările Security for Exchange sunt organizate în următoarele secțiuni:

- General
- Antimalware
- Antispam
- Content Control

General

În această secțiune, puteți crea și administra grupuri de conturi e-mail, defini vârsta articolelor trecute în carantină și interzice anumiți expeditori.

Grupuri de utilizatori

Control Center permite generarea grupurilor de utilizator pentru aplicarea diferitelor politici de scanare și filtrare în diferite categorii de utilizatori. De exemplu, puteți crea politici adecvate pentru departamentul IT, pentru echipa de vânzări sau pentru conducerea companiei.

Grupurile de utilizatori sunt disponibile global, indiferent de politica sau utilizatorul care le-a generat.

Pentru o administrare facilă a grupului, Control Center importă automat grupurile de utilizator din Windows Active Directory.

Pentru a crea un grup de utilizatori:

1. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Se afișează fereastra cu detalii.
2. Introduceți denumirea și descrierea grupurilor și adresele e-mail ale utilizatorilor.

Notă

- Dintr-o listă lungă de adrese e-mail, trebuie să copiați și să inserați lista dintr-un fișier text.
- Elemente de separare acceptate în listă: spațiu, virgulă, punct și virgulă și enter.

3. Faceți clic pe **Save**.

Grupurile personalizate pot fi editate. Faceți clic pe denumirea grupului pentru a deschide fereastra de configurare și puteți modifica detaliile grupului sau edita lista utilizatorilor.

Pentru a elimina un grup personalizat din listă, selectați grupul și faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului.

Notă
Nu puteți edita sau șterge grupurile Active Directory.

Setări

- **Ștergeți fișierele trecute în carantină mai vechi de (zile).** Implicit, fișierele aflate în de mai mult de 30 de zile sunt șterse automat. Dacă doriți să schimbați acest interval, introduceți o valoare diferită în câmpul corespunzător.
- **Lista neagră de conexiuni.** Dacă activați acestă opțiune, Serverul Exchange respinge toate e-mail-urile primite de la expeditorii din lista neagră.

  Pentru generarea unei liste negre:
  1. Faceți clic pe link-ul **Editare articole din lista neagră**.
  2. Introduceți adresele e-mail pe care doriți să le blocați. La modificarea listei, puteți folosi, de asemenea, următoarele metacaractere pentru a defini un întreg domeniu de e-mail sau un model pentru adresele de e-mail:
     - Asterisk (*) înlocuind zero, unul sau mai multe caractere.
     - Semnul întrebării (?), înlocuind un singur caracter.

     De exemplu, dacă introduceți `*@boohouse.com`, toate adresele de e-mail de la `boohouse.com` vor fi blocate.
  3. Faceți clic pe **Save**.

Verificare IP domeniu (Antispoofing)

Folosiți acest filtru pentru a împiedica spammerii să facă spoofing pe adresele de e-mail ale expeditorului, făcând să pară că mesajele e-mail sunt trimise de o

persoană de încredere. Puteți specifica adresele IP autorizate să trimisă mesaje e-mail pentru domeniile dumneavoastră și, dacă este nevoie, pentru alte domenii de e-mail cunoscute. Dacă un mesaj e-mail pare să fie trimis de la un domeniu afișat în listă, însă adresa IP a expeditorului nu corespunde uneia dintre adresele IP specificate, mesajul e-mail este respins.

Avertisment

Nu utilizați acest filtru dacă folosiți o gazdă inteligentă, un serviciu găzduit de filtrare a mesajelor e-mail sau o soluție de filtrare a mesajelor e-mail prin gateway înaintea serverelor dumneavoastră Exchange.

Important

- Acest filtru verifică doar conexiunile de e-mail neautentificate.
- Recomandări de utilizare:
  - Se recomandă să utilizați acest filtru numai pe serverele Exchange care sunt conectate direct la internet. De exemplu, dacă aveți atât servere Edge Transport cât și servere Hub Transport, configurați acest filtru numai pe serverele Edge.
  - Adăugați în lista de domenii toate adresele IP interne care au dreptul de a trimite mesaje e-mail prin intermediul unor conexiuni SMTP neautentificate. Acestea pot include sisteme de notificare automată, echipament de rețea precum imprimante etc.
  - În cadrul unei configurări Exchange folosind Database Availability Groups, adăugați în lista de domenii și adresele IP ale tuturor serverelor Hub Transport și Mailbox.
  - Acționați cu precauție dacă doriți să configurați adrese IP autorizate pentru anumite domenii de e-mail externe, pe care nu le administrați dumneavoastră. Dacă nu reușiți să mențineți la zi lista de adrese IP, mesajele e-mail provenind de la domeniile respective vor fi respinse. Dacă folosiți o copie de siguranță MX, este necesar să adăugați la toate domeniile de e-mail externe configurate adresele IP de la care copia de siguranță MX redirecționează mesajele de e-mail către serverul primar de e-mail.

Pentru a configura filtrul antispoofing, urmați pașii descriși aici:

1. Bifați căsuța **Verificare IP domeniu (Antispoofing)** pentru a activa acest filtru.
2. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Va apărea fereastra de configurare.
3. Introduceți domeniul de e-mail în câmpul corespunzător.

4. Specificați intervalul de adrese IP autorizate pentru a fi utilizate cu domeniul specificat anterior, folosind formatul CIDR (IP/mascărețea).
5. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului. Adresele IP sunt adăugate în tabel.
6. Pentru a șterge un interval IP din listă, faceți clic pe butonul ⊗ **Ștergere** din partea dreaptă a tabelului.
7. Faceți clic pe **Save**. Domeniul este adăugat la filtru.

Pentru a șterge un domeniu de e-mail din filtru, selectați-l din tabelul Antispoofing și faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului.

Antimalware

Modulul Antimalware protejează serverele de e-mail Exchange contra tuturor tipurilor de amenințări malware (viruși, Troieni, spyware, rootkit-uri, adware, etc.), prin detectarea articolelor infectate sau suspectate și încercarea de a le dezinfecta sau de a izola infestarea, conform acțiunilor specificate.

Scanarea antimalware se efectuează la două niveluri:

- Nivel Transport
- Exchange Store

Scanarea nivelului de transport

Bitdefender Endpoint Security Tools se integrează cu agenții de expediere e-mail pentru scanarea întregului trafic e-mail.

În mod implicit, opțiunea de scanare a nivelului de transport este activată. Bitdefender Endpoint Security Tools filtrează traficul prin e-mail și, dacă este cazul, informează utilizatorii cu privire la măsurile luate, prin adăugarea textului în corpul e-mail-ului.

Folosiți caseta de bifare **Filtrare antimalware** pentru a dezactivarea sau reactivarea acestei funcții.

Pentru configurarea textului notificărilor, faceți clic pe link-ul **Setări**. Sunt disponibile următoarele opțiuni:

- **Adăugare subsol la e-mail-urile scanate.** Selectați această casetă de bifare pentru a adăuga o frază în partea de jos a e-mail-urilor scanate. Pentru a modifica textul implicit, introduceți mesajul în caseta de text de mai jos.

- **Text înlocuire.** Pentru e-mail-urile cu atașamente șterse sau trecute în carantină, puteți atașa un fișier de notificare. Pentru a modifica textele implicite de notificare, introduceți mesajul în casetele text corespunzătoare.

Filtrarea antimalware se bazează pe reguli. Fiecare e-mail care ajunge la serverul e-mail este verificat conform regulilor de filtrare antimalware, în funcție de prioritate, până când corespunde unei reguli. Mesajul e-mail este apoi procesat conform opțiunilor specificate de acea regulă.

Administrarea regulilor de filtrare

Puteți vizualiza toate regulile existente în tabel, alături de informațiile referitoare la prioritatea, starea și domeniul de acoperire. Regulile sunt ordonate în funcție de prioritate, prima regulă având cea mai mare prioritate.

Orice politică antimalware are o regulă implicită care devine activă după activarea filtrării antimalware. Ce trebuie să știți despre regula implicită:

- Nu puteți copia, dezactiva sau șterge regula.
- Puteți modifica doar setările și acțiunile de scanare.
- Prioritatea implicită a regulii este întotdeauna cea mai redusă.

Creare reguli

Aveți două alternative pentru crearea regulilor de filtrare:

- Începeți de la setările implicite, urmând pașii de mai jos:
  1. Faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului pentru a deschide fereastra de configurare.
  2. Configurați setările regulii. Pentru detalii referitoare la opțiuni, consultați Opțiunile pentru reguli.
  3. Faceți clic pe **Save**. Regula este prima din tabel.
- Folosiți o clonă a unei reguli personalizate ca șablon, urmând pașii de mai jos:
  1. Selectați regula dorită din tabel.
  2. Faceți clic pe butonul ⊕ **Clonare** din partea de sus a tabelului pentru a deschide fereastra de configurare.
  3. Adaptați opțiunile regulii în funcție de necesități.
  4. Faceți clic pe **Save**. Regula este prima din tabel.

Reguli de editare

Pentru a edita o regulă existentă:

1. Faceți clic pe denumirea regulii pentru a deschide fereastra de configurare.
2. Introduceți valorile noi pentru opțiunile pe care doriți să le modificați.
3. Faceți clic pe **Save**. Modificările intră în vigoare după salvarea politicii.

Configurarea priorității regulii

Pentru a modifica prioritatea unei reguli:

1. Selectați regula pe care doriți să o mutați.
2. Folosiți butoanele **Sus** sau **Jos** din partea de sus a tabelului pentru a mări sau reduce prioritatea regulii.

Ștergerea regulilor

Puteți șterge una sau mai multe reguli personalizate simultan. Nu trebuie decât să:

1. Selectați caseta de bifare regulilor pe care doriți să le ștergeți.
2. Faceți clic pe butonul **Ștergere** din partea de sus a tabelului. Regulile nu mai pot fi recuperate după ce au fost șterse.

Opțiunile regulilor

Sunt disponibile următoarele opțiuni:

- **General.** În această secțiune, trebuie să configurați o denumire pentru regulă. În caz contrar, nu o puteți salva. Selectați caseta de bifare **Activ** dacă doriți ca regula să fie valabilă după ce ați salvat politica.
- **Domeniul de acoperire al regulii.** Puteți limita aplicabilitatea regulii doar la un anumit set de e-mail-uri, prin configurarea următoarelor opțiuni cumulative privind domeniul de acoperire:
  - **Aplicare pentru (direcție).** Selectați direcția traficului e-mail pentru care se aplică regula.
  - **Expeditori.** Puteți decide dacă regula se aplică pentru orice expeditor sau doar pentru anumiți expeditori. Pentru a restrânge domeniul expeditorilor, faceți clic pe butonul **Specific** și selectați grupurile dorite din tabelul din stânga. Vizualizați grupurile selectate în tabelul din dreapta.
  - **Destinatari.** Puteți decide dacă regula se aplică oricărui destinatar sau doar anumitor destinatari. Pentru a restrânge domeniul destinatarilor, faceți clic pe butonul **Specific** și selectați grupurile dorite din tabelul din stânga. Puteți vizualiza grupurile selectate în tabelul din dreapta.

    Regula se aplică dacă oricare dintre destinatari corespunde selecției dvs. Dacă doriți să aplicați regula numai pentru situațiile în care toți destinatarii fac parte din grupurile selectate, alegeți **Corespondență toți destinatarii**.

    Notă
    Adresele din câmpurile **Cc** și **Bcc** sunt, de asemenea, considerate destinatari.

Important
Regulile bazate pe grupurile de utilizatori se aplică numai pentru rolurile Hub Transport și Mailbox.

- **Opțiuni.** Configurați opțiunile de scanare pentru e-mail-urile care corespund regulii:
  - **Tipurile de fișiere scanate.** Folosiți această opțiune pentru a specifica tipurile de fișiere pe care doriți să le scanați. Puteți decide să scanați toate fișierele (indiferent de extensia acestora), exclusiv fișierele de aplicații sau anumite extensii de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor asigură cea mai bună protecție, în timp ce scanarea aplicațiilor este recomandată doar pentru efectuarea unei scanări mai rapide.

    Notă
    Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Tipuri de fișiere de aplicații” (p. 567).

    Dacă doriți să scanați doar fișiere cu anumite extensii, aveți două opțiuni:
    - **Extensii definite de utilizator**, unde trebuie să indicați doar extensiile pe care doriți să le scanați.
    - **Toate fișierele, cu excepția anumitor extensii**, unde trebuie să introduceți doar extensiile pe care nu doriți să le includeți în scanare.
  - **Dimensiunea maximă a atașamentului / cuprinsului e-mail-ului (MB).** Selectați această casetă de bifare pentru a introduce o valoare în câmpul corespunzător, pentru setarea dimensiunii maxime acceptate a fișierului atașat sau a cuprinsului e-mail-ului pe care doriți să îl scanați.
  - **Capacitatea maximă a arhivei (niveluri).** Selectați caseta de bufare și alegeți capacitatea maximă a arhivei din câmpul corespunzător. Cu cât capacitatea este mai redusă, cu atât performanțele sunt mai ridicate, iar nivelul de protecție este mai mic.
  - **Scanare Posibile aplicații nedorite(PUA).** Selectați această casetă de bifare pentru scanarea posibilelor aplicații periculoase sau nedorite, cum ar fi adware, care se pot instala în sisteme fără consimțământul utilizatorului, pot schimba comportamentul diferitelor produse software și reduce performanțele sistemului.
- **Acțiuni.** Puteți specifica diverse acțiuni pentru agentul de securitate pentru a prelua automat fișiere pe baza tipului de detecție.

  Tipul de detecție separă fișierele în trei categorii:

- **Fișiere infectate.** Bitdefender detectează fișierele ca fiind infectate folosind diverse mecanisme avansate, printre care semnăturile malware, învățarea automată și tehnologiile bazate pe inteligență artificială (AI).
- **Fișiere suspecte.** Aceste fișiere sunt detectate ca fiind suspecte de către analiza euristică și alte tehnologii Bitdefender. Acestea asigură o rată mare de detecție, însă utilizatorii trebuie să fie conștienți că există și rezultate fals pozitive (fișiere neinfectate detectate ca fiind suspecte) în unele cazuri.
- **Fișiere care nu pot fi scanate .**Aceste fișiere nu pot fi scanate. Fișierele care nu pot fi scanate includ dar nu se limitează la fișiere protejate cu parolă, criptate sau supra-arhivate.

Pentru fiecare tip de detecție, aveți o acțiune implicită sau principală și o acțiune alternativă, în cazul în care cea principală eșuează. Deși nu se recomandă, puteți modifica aceste acțiuni din meniurile corespunzătoare. Selectați acțiunile care vor fi implementate:

- **Dezinfectare.** Șterge codul malware din fișierele infectate și reconstruiește fișierul original. Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.
- **Respingere / Ștergere e-mail.** Pe serverele cu rol Edge Transport, mesajele e-mail detectate sunt respinse cu un cod de eroare 550 SMTP. În toate celelalte cazuri, mesajul e-mail este șters fără nicio avertizare. Se recomandă să evitați această acțiune.
- **Ștergere fișier.** Șterge atașamentele cu probleme, fără avertizare. Se recomandă să evitați această acțiune.
- **Înlocuire fișier.** Șterge fișierele cu probleme și introduce un fișier text care informează utilizatorul cu privire la măsurile luate.
- **Trecerea fișierelor în carantină.** Mută fișierele detectate în folderul carantină și introduce un fișier text care informează utilizatorul cu privire la măsurile luate. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Puteți administra fișierele în carantină de pe pagina **Carantină**.

Notă

Vă rugăm să rețineți că, în cazul Serverelor Exchange, carantina necesită spațiu suplimentar pe hard-disk, pe partiția pe care este instalat agentul de securitate. Dimensiunea carantinei depinde de numărul de articole stocate și de dimensiunea acestora.

- **Nu se vor lua măsuri.** Nu vor fi luate măsuri cu privire la fișierele detectate. Acește fișiere vor fi doar afișate în jurnalul de scanare. Sarcinile de scanare sunt configurate implicit să ignore fișierele suspecte. Ar putea fi util să modificați sarcina implicită, pentru a trece fișierele suspecte sub carantină.
- În mod implicit, dacă un e-mail corespunde domeniului de aplicare al regulii, acesta este procesat exclusiv în conformitate cu regula, fără a fi verificat cu privire la orice alte reguli rămase. Dacă doriți să continuați să verificați în baza celorlalte reguli, debifați caseta de selectare **Oprire procesare reguli, dacă condițiile regulii sunt îndeplinite**.

Excluderi

Dacă doriți ca un anumit trafic e-mail să fie ignorat de orice regulă de filtrare, puteți defini excluderile din scanare. Pentru a crea o excepție:

1. Extindeți secțiunea **Excepții pentru regulile antimalware**.
2. Faceți clic pe butonul ⊖ **Adăugare** din bara de instrumente a acestei secțiuni, care deschide fereastra de configurare.
3. Configurați setările de excludere. Pentru detalii referitoare la opțiuni, consultați secțiunea Opțiunile pentru reguli.
4. Faceți clic pe **Save**.

Scanarea bazei de date Exchange

Protecția Exchange folosește Exchange Web Services (EWS) din Microsoft pentru a permite scanarea căsuței poștale Exchange și a bazelor de date de foldere publice. Puteți configura modulul antimalware pentru rularea sarcinilor de scanare la cerere în mod regulat pe bazele de date țintă, conform programului specificat.

Notă

- Scanarea la cerere este disponibilă doar pentru Serverele Exchange cu rol de căsuță poștală instalate.
- Vă rugăm să rețineți că scanarea la cerere mărește consumul de resurse și, în funcție de opțiunile de scanare și de numărul de obiecte care trebuie scanate, finalizarea acesteia poate necesita un interval de timp considerabil.

Scanarea la cerere necesită un cont de administrator Exchange (cont de servicii) pentru utilizatorii Exchange și pentru preluarea obiectelor țintă care trebuie scanate din căsuțele poștale ale utilizatorilor și folderele publice. Se recomandă generarea unui cont dedicat în acest scop.

Contul de administrator Exchange trebuie să îndeplinească următoarele cerințe:

- Este membru al grupului Organization Management (Exchange 2016, 2013 și 2010)
- Să fie membru al grupului Exchange Organization Administrators (Exchange 2007)
- Să aibă o căsuță poștală atașată.

Activarea scanării la cerere

1. În secțiunea **Sarcini de scanare**, faceți clic pe link-ul **Adăugare date**.
2. Introduceți numele de utilizator și parola contului de servicii.
3. Dacă e-mail-ul este diferit de numele de utilizator, trebuie să introduceți și adresa e-mail a contului de servicii.
4. Introduceți adresa URL Exchange Web Services (EWS), necesară dacă funcția Exchange Autodiscovery nu este activă.

Notă

- Numele de utilizator trebuie să includă numele de domeniu, cum ar fi `user@domain` sau `domain\user`.
- Nu uitați să actualizați informațiile în Control Center, ori de câte ori s-au modificat.

Administrarea sarcinilor de scanare

Tabelul cu sarcinile de scanare include toate sarcinile programate și oferă informații referitoare la țintele și recurența acestora.

Pentru a crea sarcini de scanare a Bazei de date Exchange:

1. În secțiunea **Sarcini de scanare**, faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului pentru a deschide fereastra de configurare.
2. Configurați setările sarcinii în modul descris în secțiunea următoare.
3. Faceți clic pe **Save**. Sarcina este adăugată în listă și devine valabilă după salvarea politicii.

Sarcinile pot fi editate pe rând, făcânt clic pe denumirea sarcinii.

Pentru a șterge sarcini din listă, selectați-le și faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului.

Setările sarcinii de scanare

Sarcinile au o serie de setări pe care le puteți găsi descrise mai jos:

- **General.** Introduceți o denumire sugestivă pentru sarcină.

Notă
Puteți vizualiza denumirea sarcinii în istoricul Bitdefender Endpoint Security Tools.

- **Programare.** Folosiți opțiunile de programare pentru configurarea calendarului de scanare. Puteți seta ca scanarea să ruleze la fiecare câteva ore, zile sau săptămâni, începând cu o anumită dată și oră. Pentru bazele de date mari, sarcina de scanare poate dura mult și poate afecta performanța serverului. În astfel de cazuri, puteți configura sarcina sa se oprească după un anumit interval de timp.
- **Țintă.** Selectați containerele și obiectele pe care doriți să le scanați. Puteți opta pentru scanarea căsuțelor poștale, a folderelor publice sau a ambelor. În afară de e-mail-uri, puteți opta pentru scanarea altor obiecte, cum ar fi **Contacte**, **Sarcini**, **Programări** și **Articole poștale**. De asemenea, puteți seta următoarele limitări pentru conținutul care urmează să fie scanat:
  – Doar mesajele necitite
  – Doar articolele cu atașamente
  – Doar articolele noi, primite într-un interval de timp specificat

  De exemplu, puteți opta pentru a scana doar e-mail-urile din căsuțele poștale ale utilizatorilor primite în ultimele șapte zile.

  Selectați caseta de bifare **Excepții**, dacă doriți să definiți excepții de scanare. Pentru a crea o excepție, folosiți câmpurile din antetul tabelului, după cum urmează:
  1. Selectați tipul de director din meniu.
  2. În funcție de tipul directorului, specificați obiectele pe care doriți să le excludeți:

Tipul directorului	Formatul obiectului
Mailbox	Adresă e-mail
Folder public	Calea folderului, începând de la rădăcină
Bază de date	Informațiile de identificare ale bazei de date

Notă
Pentru a obține informațiile de identificare ale bazei de date, folosiți comanda shell Exchange:
```
Get-MailboxDatabase | fl name,identity
```

Nu puteți introduce mai multe articole simultan. Dacă aveți mai multe articole de același tip, trebuie să definiți un număr de reguli egal cu numărul de articole.

3. Faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului pentru a salva excepția și a o include în listă.

Pentru a șterge o regulă referitoare la excepții din listă, faceți clic pe butonul ⊖ **Ștergere** corespunzător.

- **Opțiuni.** Configurați opțiunile de scanare pentru e-mail-urile care corespund regulii:
  - **Tipurile de fișiere scanate.** Folosiți această opțiune pentru a specifica tipurile de fișiere pe care doriți să le scanați. Puteți decide să scanați toate fișierele (indiferent de extensia acestora), exclusiv fișierele de aplicații sau anumite extensii de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor asigură cea mai bună protecție, în timp ce scanarea aplicațiilor este recomandată doar pentru efectuarea unei scanări mai rapide.

    Notă
    Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Tipuri de fișiere de aplicații” (p. 567).

    Dacă doriți să scanați doar fișiere cu anumite extensii, aveți două opțiuni:
    - **Extensii definite de utilizator**, unde trebuie să indicați doar extensiile pe care doriți să le scanați.
    - **Toate fișierele, cu excepția anumitor extensii**, unde trebuie să introduceți doar extensiile pe care nu doriți să le includeți în scanare.
  - **Dimensiunea maximă a atașamentului / cuprinsului e-mail-ului (MB).** Selectați această casetă de bifare pentru a introduce o valoare în câmpul corespunzător, pentru setarea dimensiunii maxime acceptate a fișierului atașat sau a cuprinsului e-mail-ului pe care doriți să îl scanați.
  - **Capacitatea maximă a arhivei (niveluri).** Selectați caseta de bufare și alegeți capacitatea maximă a arhivei din câmpul corespunzător. Cu cât capacitatea este mai redusă, cu atât performanțele sunt mai ridicate, iar nivelul de protecție este mai mic.
  - **Scanare Posibile aplicații nedorite(PUA).** Selectați această casetă de bifare pentru scanarea posibilelor aplicații periculoase sau nedorite, cum ar fi adware, care se pot instala în sisteme fără consimțământul utilizatorului, pot schimba comportamentul diferitelor produse software și reduce performanțele sistemului.

- **Acțiuni.** Puteți specifica diverse acțiuni pentru agentul de securitate pentru a prelua automat fișiere pe baza tipului de detecție.

  Tipul de detecție separă fișierele în trei categorii:
  - **Fișiere infectate.** Bitdefender detectează fișierele ca fiind infectate folosind diverse mecanisme avansate, printre care semnăturile malware, învățarea automată și tehnologiile bazate pe inteligență artificială (AI).
  - **Fișiere suspecte.** Aceste fișiere sunt detectate ca fiind suspecte de către analiza euristică și alte tehnologii Bitdefender. Acestea asigură o rată mare de detecție, însă utilizatorii trebuie să fie conștienți că există și rezultate fals pozitive (fișiere neinfectate detectate ca fiind suspecte) în unele cazuri.
  - **Fișiere care nu pot fi scanate .**Aceste fișiere nu pot fi scanate. Fișierele care nu pot fi scanate includ dar nu se limitează la fișiere protejate cu parolă, criptate sau supra-arhivate.

  Pentru fiecare tip de detecție, aveți o acțiune implicită sau principală și o acțiune alternativă, în cazul în care cea principală eșuează. Deși nu se recomandă, puteți modifica aceste acțiuni din meniurile corespunzătoare. Selectați acțiunile care vor fi implementate:
  - **Dezinfectare.** Șterge codul malware din fișierele infectate și reconstruiește fișierul original. Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.
  - **Respingere / Ștergere e-mail.** Mesajul e-mail este șters fără nicio avertizare. Se recomandă să evitați această acțiune.
  - **Ștergere fișier.** Șterge atașamentele cu probleme, fără avertizare. Se recomandă să evitați această acțiune.
  - **Înlocuire fișier.** Șterge fișierele cu probleme și introduce un fișier text care informează utilizatorul cu privire la măsurile luate.
  - **Trecerea fișierelor în carantină.** Mută fișierele detectate în folderul carantină și introduce un fișier text care informează utilizatorul cu privire la măsurile luate. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Puteți administra fișierele în carantină de pe pagina **Carantină**.

  Notă
  Vă rugăm să rețineți că, în cazul Serverelor Exchange, carantina necesită spațiu suplimentar pe hard-disk, pe partiția pe care este instalat agentul de

securitate. Dimensiunea carantinei depinde de numărul și dimensiunea mesajelor e-mail stocate.

- **Nu se vor lua măsuri.** Nu vor fi luate măsuri cu privire la fișierele detectate. Acește fișiere vor fi doar afișate în jurnalul de scanare. Sarcinile de scanare sunt configurate implicit să ignore fișierele suspecte. Ar putea fi util să modificați sarcina implicită, pentru a trece fișierele suspecte sub carantină.
- În mod implicit, dacă un e-mail corespunde domeniului de aplicare al regulii, acesta este procesat exclusiv în conformitate cu regula, fără a fi verificat cu privire la orice alte reguli rămase. Dacă doriți să continuați să verificați în baza celorlalte reguli, debifați caseta de selectare **Oprire procesare reguli, dacă condițiile regulii sunt îndeplinite**.

Antispam

Modulul Antispam oferă protecție pe mai multe niveluri contra mesajelor spam și tentativelor de phishing, folosind o combinație de diferite filtre și motoare pentru a stabili dacă e-mail-urile sunt spam sau nu.

Notă

- Filtrarea antispam este disponibilă pentru:
  - Exchange Server 2016/2013 cu rol Edge Transport sau Mailbox
  - Exchange Server 2010/2007 cu rol Edge Transport sau Hub Transport
- Dacă în organizarea Exchange aveți atât rolul Edge, cât și Hub, se recomandă să activați filtrarea antispam pe server cu rol Edge Transport.

Filtrarea spam este activată automat pentru e-mail-urile primite. Selectați caseta de bifare **Filtrare antispam** pentru dezactivarea sau reactivarea acestei funcții.

Filtrele Antispam

Mesajele e-mail sunt verificate în baza regulilor de filtrare antispam, în funcție de grupurile de expeditori și destinatari, în funcție de prioritate, până când se stabilește corespondența cu o regulă. Mesajele e-mail sunt apoi procesate conform opțiunilor regulii și se iau măsuri cu privire la mesajele spam detectate.

Anumite filtre antispam pot fi configurate și puteți controla dacă le veți folosi sau nu. Mai jos este o listă a filtrelor opționale:

- **Filtru set caractere.** Multe mesaje e-mail spam sunt scrise cu caractere chirilice sau asiatice. Filtrul de caractere detectează astfel de mesaje e-mail și le marchează ca SPAM.
- **Material etichetat ca având conținut sexual explicit.** Mesajele nedorite care conțin materiale cu orientare sexuală trebuie să includă avertismentul SEXUALLY-EXPLICIT: în subiect. Acest filtru detectează mesajele e-mail marcate ca fiind SEXUALLY-EXPLICIT: în subiect și le marchează ca spam.
- **Filtru URL.** Aproape toate mesajele e-mail de tip spam includ link-uri către diferite locații web. În general, aceste locații includ mai multă publicitate și oferă posibilitatea de a efectua achiziții. Uneori, acestea sunt utilizate și pentru phishing.

  Bitdefender păstrează o bază de dată a acestor link-uri. Filtrul URL verifică fiecare link URL dintr-un e-mail în baza de date. Dacă se identifică o corespondență, mesajul e-mail este marcat ca spam.
- **Lista Blackhole în timp real(RBL).** Acesta este un filtru care permite verificarea serverului expeditorului comparativ cu serverele RBL terțe. Filtrul folosește protocolul DNSBL și serverele RBL pentru a filtra mesajele spam pornind de la reputația serverelor e-mail ca și expeditori de mesaje spam.

  Adresa serverului e-mail este preluată din antetul e-mail-ului și i se verifică valabilitatea. Dacă adresa aparține unei clase private (`10.0.0.0`, `172.16.0.0` până la `172.31.0.0` sau `192.168.0.0` oână la `192.168.255.0`), aceasta este ignorată.

  Se efectuează o verificare DNS asupra domeniului `d.c.b.a.rbl.example.com`, unde `d.c.b.a` este adresa IP inversă a serverului și `rbl.example.com` este serverul RBL. Dacă DNS validează domeniul, înseamnă că adresa IP se regăsește în serverul RBL și este prevăzut un anumit scor pentru server. Acest scor variază între 0 și 100, în funcție de nivelul de încredere acordat serverului.

  Interogarea este efectuată pentru fiecare server RBL din listă, iar scorul rezultat pentru fiecare în parte este adăugat scorului intermediar. Dacă scorul a ajuns la 100, nu se mai efectuează interogări.

  Dacă scorul filtrului RBL este 100 sau peste, e-mail-ul este considerat spam și se ia măsura specificată. În caz contrar, se calculează un scor spam pornind de la scorul filtrului RBL, care se adaugă la scorul spam total al e-mail-ului.
- **Filtru euristic.** Dezvoltat de Bitdefender, filtrul Euristic detectează mesajele spam noi și necunoscute. Filtrul este instruit automat pe volume mari de

e-mail-uri de tip spam în Laboratorul antispam Bitdefender. În timpul instruirii, dobândește capacitatea de a distinge între mesajele spam și cele legitime și de a recunoaște mesajele spam noi prin identificarea similarităților, adesea subtile, cu e-mail-urile verificate deja. Acest filtru este destinat îmbunătățirii detecției bazată pe semnătură, menținând numărul de fals pozitive extrem de redus.

- **Bitdefender Interogare Cloud.** Bitdefender menține o bază de date care evoluează constant de "amprente" ale mesajelor e-mail spam din cloud. O interogare care conține amprenta mesajului e-mail este trimisă la serverele in the cloud pentru a verifica din mers dacă mesajul e-mail este de tip spam. Dacă amprenta nu este în baza de date, este verificată prin intermediul altor cercetări recente și, dacă anumite condiții sunt îndeplinite, e-mail-ul poate fi marcat ca fiind spam.

Administrarea regulilor antispam

Puteți vizualiza toate regulile existente în tabel, alături de informațiile referitoare la prioritatea, starea și domeniul de acoperire. Regulile sunt ordonate în funcție de prioritate, prima regulă având cea mai mare prioritate.

Orice politică antispam are o regulă implicită care devine activă după activarea modulului. Ce trebuie să știți despre regula implicită:

- Nu puteți copia, dezactiva sau șterge regula.
- Puteți modifica doar setările și acțiunile de scanare.
- Prioritatea implicită a regulii este întotdeauna cea mai redusă.

Creare reguli

Pentru a crea o regulă:

1. Faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului pentru a deschide fereastra de configurare.
2. Configurați setările regulii. Pentru detalii referitoare la opțiuni, consultați „Opțiunile regulilor” (p. 369).
3. Faceți clic pe **Save**. Regula este prima din tabel.

Reguli de editare

Pentru a edita o regulă existentă:

1. Faceți clic pe denumirea regulii pentru a deschide fereastra de configurare.
2. Introduceți valorile noi pentru opțiunile pe care doriți să le modificați.
3. Faceți clic pe **Save**. Dacă regula este activă, modificările sunt implementate după salvarea politicii.

Configurarea priorității regulii

Pentru a modifica o prioritate a regulii, selectați regula dorită și folosiți săgețile **Sus** și **Jos** din partea de sus a tabelului. Regulile pot fi mutate doar pe rând.

Ștergerea regulilor

Dacă nu doriți să mai folosiți o anumită regulă, selectați-o și faceți clic pe butonul **Ștergere** din partea de sus a tabelului.

Opțiunile regulilor

Sunt disponibile următoarele opțiuni:

- **General.** În această secțiune, trebuie să configurați o denumire pentru regulă. În caz contrar, nu o puteți salva. Selectați caseta de bifare **Activ** dacă doriți ca regula să fie valabilă după ce ați salvat politica.
- **Domeniul de acoperire al regulii.** Puteți limita aplicabilitatea regulii doar la un anumit set de e-mail-uri, prin configurarea următoarelor opțiuni cumulative privind domeniul de acoperire:
  - **Aplicare pentru (direcție).** Selectați direcția traficului e-mail pentru care se aplică regula.
  - **Expeditori.** Puteți decide dacă regula se aplică pentru orice expeditor sau doar pentru anumiți expeditori. Pentru a restrânge domeniul expeditorilor, faceți clic pe butonul **Specific** și selectați grupurile dorite din tabelul din stânga. Vizualizați grupurile selectate în tabelul din dreapta.
  - **Destinatari.** Puteți decide dacă regula se aplică oricărui destinatar sau doar anumitor destinatari. Pentru a restrânge domeniul destinatarilor, faceți clic pe butonul **Specific** și selectați grupurile dorite din tabelul din stânga. Puteți vizualiza grupurile selectate în tabelul din dreapta.

    Regula se aplică dacă oricare dintre destinatari corespunde selecției dvs. Dacă doriți să aplicați regula numai pentru situațiile în care toți destinatarii fac parte din grupurile selectate, alegeți **Corespondență toți destinatarii**.

    Notă
    Adresele din câmpurile **Cc** și **Bcc** sunt, de asemenea, considerate destinatari.

    Important
    Regulile bazate pe grupurile de utilizatori se aplică numai pentru rolurile Hub Transport și Mailbox.

- **Setări.** Faceți clic pe nivelul de securitate care corespunde cel mai bine necesităților dvs. (**Agresiv**, **Normal** sau **Permisiv**). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

  De asemenea, puteți activa diferite filtre. Pentru informații detaliate referitoare la aceste filtre, vă rugăm să consultați „Filtrele Antispam" (p. 366).

  Important
  RBL necesită configurare suplimentară. Puteți configura filtrul după ce ați creat sau modificat regula. Pentru mai multe informații, consultați capitolul „Configurarea Filtrului RBL" (p. 371)

  Pentru conexiunile autentificate puteți alege dacă doriți să săriți peste scanarea antispam sau nu.
- **Acțiuni.** Există o serie de acțiuni pe care le puteți implementa în cazul e-mail-urilor detectate. Fiecare acțiune are, la rândul său, o serie de opțiuni posibile sau acțiuni secundare. Acestea sunt descrise mai jos:

  Acțiuni principale:
  - **Livrare e-mail.** E-mail-ul spam ajunge în căsuțele poștale ale destinatarilor.
  - **Trecere e-mail în carantină.** Mesajul e-mail este criptat și salvat în folderul de carantină din Serverul Exchange, fără a fi livrat destinatarilor. Puteți administra e-mail-urile trecute în carantină de pe pagina **Carantină**.
  - **Redirecționare e-mail către.** E-mail-ul nu este transmis către destinatarii inițiali, ci către o căsuță poștală specificată de dvs. în câmpul corespunzător.
  - **Respingere / Ștergere e-mail.** Pe serverele cu rol Edge Transport, mesajele e-mail detectate sunt respinse cu un cod de eroare 550 SMTP. În toate celelalte cazuri, mesajul e-mail este șters fără nicio avertizare. Se recomandă să evitați această acțiune.

  Acțiuni secundare:
  - **Integrare cu Exchange SCL.** Adaugă un antet e-mail-ului de tip spam, permițând Serverului Exchange sau Microsoft Outlook să ia măsurile care se impun, în funcție de mecanismul Nivelului de încredere spam (SCL).
  - **Marchează subiectul e-mail-ului ca.** Puteți adăuga o etichetă subiectului e-mail-ului pentru a ajuta utilizatorii să filtreze e-mail-urile detectate în clientul e-mail.

- **Adăugare antet e-mail.** Se adaugă un antet e-mail-urilor detectate drept spam. Puteți modifica denumirea și valoarea antetului introducând valorile dorite în câmpurile corespunzătoare. De asemenea, puteți folosi acest antet e-mai pentru a crea alte filtre.
- **Salvare e-mail pe disc.** O copie a mesajului e-mail de tip spam este salvată ca fișier în folderul specificat. Menționați calea absolută a folderului în câmpul corespunzător.

  Notă
  Această opțiune acceptă exclusiv e-mail-urile în format MIME.

- **Arhivare în cont.** O copie a e-mail-ului detectat este transmisă către adresa e-mail specificată. Această acțiune adaugă adresa e-mail specificată în lista Bcc a e-mail-ului.

- În mod implicit, dacă un e-mail corespunde domeniului de aplicare al regulii, acesta este procesat exclusiv în conformitate cu regula, fără a fi verificat cu privire la orice alte reguli rămase. Dacă doriți să continuați să verificați în baza celorlalte reguli, debifați caseta de selectare **Oprire procesare reguli, dacă condițiile regulii sunt îndeplinite**.

Configurarea Filtrului RBL

Dacă doriți să folosiți filtrul RBL, trebuie să furnizați o listă a serverelor RBL.

Pentru configurarea filtrului:

1. Pe pagina **Antispam**, faceți clic pe link-ul **Setări** pentru a deschide fereastra de configurare.
2. Specificați IP-ul serverului DNS pe care doriți să îl interogați și intervalul de timp până la expirarea interogării în câmpurile corespunzătoare. Dacă nu este configurat niciun server DNS, sau dacă serverul DNS server este indisponibil, filtrul RBL va folosi serverele DNS ale sistemului.
3. Pentru fiecare server RBL:
   a. Introduceți numele de gazdă sau adresa IP a serverului și nivelul de încredere atribuit serverului, în câmpurile din antetul tabelului.
   b. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului.
4. Faceți clic pe **Save**.

Configurarea listei albe de expeditori

Pentru expeditorii e-mail cunoscuți, puteți evita consumul inutil de resurse ale serverului, incluzându-i în liste de expeditori de încredere și expeditori care nu sunt

de încredere. Astfel, serverul de e-mail va accepta sau respinge întotdeauna e-mail-urile primite de la acești expeditori. De exemplu, dacă aveți o comunicare intensă prin e-mail cu un parteneri de afaceri și vreți să vă asigurați că primiți toate e-mail-urile, puteți include partenerul în lista albă.

Pentru a realiza o listă albă de expeditori de încredere:

1. Faceți clic pe link-ul **Listă albă** pentru a deschide fereastra de configurare.
2. Selectați caseta de bifare **Lista albă a expeditorilor**.
3. Introduceți adresele e-mail în câmpul corespunzător. La modificarea listei, puteți folosi, de asemenea, următoarele metacaractere pentru a defini un întreg domeniu de e-mail sau un model pentru adresele de e-mail:
   - Asterisk (*) înlocuind zero, unul sau mai multe caractere.
   - Semnul întrebării (?), înlocuind un singur caracter.

   De exemplu, dacă introduceți `*.gov`, toate mesajele e-mail provenind de la domeniul `.gov` vor fi acceptate.
4. Faceți clic pe **Save**.

Notă
Pentru a include în lista neagră expeditori de spam cunoscuți, folosiți opțiunea **Listă neagră de conexiuni** din secțiunea **Protecție Exchange > General > Setări**.

Content Control

Folosiți opțiunea Control conținut pentru a îmbunătăți protecția e-mail, prin filtrarea întregului trafic e-mail care nu corespunde politicilor companiei dvs. (conținut nedorit sau potențial sensibil).

Pentru controlul general al conținutului e-mail, acest modul include două opțiuni de filtrare a mesajelor e-mail:

- Filtrare pe bază de conținut
- Filtrare atașamente

Notă
Filtrarea conținutului și Filtrarea atașamentelor sunt disponibile pentru:

- Exchange Server 2016/2013 cu rol Edge Transport sau Mailbox
- Exchange Server 2010/2007 cu rol Edge Transport sau Hub Transport

Administrarea regulilor de filtrare

Filtrele de control al conținutului se bazează pe reguli. Puteți defini diferite reguli pentru diferiți utilizatori și grupuri de utilizatori. Fiecare e-mail care ajunge la serverul e-mail este verificat conform regulilor de filtrare, în funcție de prioritate, până când corespunde unei reguli. Mesajul e-mail este apoi procesat conform opțiunilor specificate de acea regulă.

Regulile de filtrare a conținutului au prioritate față de regulile de filtrare a atașamentelor.

Regulile de filtrare a conținutului și atașamentelor sunt prezentate în tabelele corespunzătoare ordonate după prioritate, prima regulă având cel mai înalt nivel de prioritate. Pentru fiecare regulă, se furnizează următoarele informații:

- Prioritate
- Nume
- Direcționarea traficului
- Grupuri de expeditori și destinatari

Creare reguli

Aveți două alternative pentru crearea regulilor de filtrare:

- Începeți de la setările implicite, urmând pașii de mai jos:
  1. Faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului pentru a deschide fereastra de configurare.
  2. Configurați setările regulii. Pentru detalii privind opțiunile de filtrare a conținutului și atașamentelor specifice, consultați:
     – Opțiuni referitoare la regulile de filtrare a conținutului
     – Opțiuni privind regulile de filtrare a atașamentelor.
  3. Faceți clic pe **Save**. Regula este prima din tabel.
- Folosiți o clonă a unei reguli personalizate ca șablon, urmând pașii de mai jos:
  1. Selectați regula dorită din tabel.
  2. Faceți clic pe butonul **Clonare** din partea de sus a tabelului pentru a deschide fereastra de configurare.
  3. Adaptați opțiunile regulii la necesitățile dvs.
  4. Faceți clic pe **Save**. Regula este prima din tabel.

Reguli de editare

Pentru a edita o regulă existentă:

1. Faceți clic pe denumirea regulii pentru a deschide fereastra de configurare.
2. Introduceți valorile noi pentru opțiunile pe care doriți să le modificați.

3. Faceți clic pe **Save**. Modificările intră în vigoare după salvarea politicii.

Configurarea priorității regulii

Pentru a modifica prioritatea unei reguli:

1. Selectați regula pe care doriți să o mutați.
2. Folosiți butoanele **Sus** sau **Jos** din partea de sus a tabelului pentru a mări sau reduce prioritatea regulii.

Ștergerea regulilor

Puteți șterge una sau mai multe reguli personalizate. Nu trebuie decât să:

1. Selectați regulile pe care doriți să le ștergeți.
2. Faceți clic pe butonul **Ștergere** din partea de sus a tabelului. Regulile nu mai pot fi recuperate după ce au fost șterse.

Filtrare pe bază de conținut

Filtrarea conținutului vă ajută să filtrați traficul e-mail în funcție de șirurile de caractere definite anterior. Aceste șiruri sunt comparate cu subiectul e-mail-ului sau cu textul din cuprinsul e-mail-ului. Folosind Filtrarea pe bază de conținut, puteți atinge următoarele scopuri:

- Preveniți pătrunderea conținutului e-mail nedorit în căsuțele poștale ale Serverului Exchange.
- Blocați transmiterea de mesaje e-mail cu date confidențiale.
- Arhivați e-mail-urile care îndeplinesc anumite condiții într-un alt cont e-mail sau pe disc. De exemplu, puteți salva mesajele e-mail transmise către adresa de asistență a companiei dvs. într-un folder de pe discul local.

Activarea filtrării conținutului

Dacă doriți să folosiți filtrarea conținutului, bifați caseta **Filtrare conținut**.

Pentru a genera și aministra regulile de filtrare a conținutului, consultați „Administrarea regulilor de filtrare” (p. 373).

Opțiunile regulilor

- **General.** În această secțiune, trebuie să configurați o denumire pentru regulă. În caz contrar, nu o puteți salva. Selectați caseta de bifare **Activ** dacă doriți ca regula să fie valabilă după ce ați salvat politica.
- **Domeniul de acoperire al regulii.** Puteți limita aplicabilitatea regulii doar la un anumit set de e-mail-uri, prin configurarea următoarelor opțiuni cumulative privind domeniul de acoperire:

- **Aplicare pentru (direcție).** Selectați direcția traficului e-mail pentru care se aplică regula.
- **Expeditori.** Puteți decide dacă regula se aplică pentru orice expeditor sau doar pentru anumiți expeditori. Pentru a restrânge domeniul expeditorilor, faceți clic pe butonul **Specific** și selectați grupurile dorite din tabelul din stânga. Vizualizați grupurile selectate în tabelul din dreapta.
- **Destinatari.** Puteți decide dacă regula se aplică oricărui destinatar sau doar anumitor destinatari. Pentru a restrânge domeniul destinatarilor, faceți clic pe butonul **Specific** și selectați grupurile dorite din tabelul din stânga. Puteți vizualiza grupurile selectate în tabelul din dreapta.

  Regula se aplică dacă oricare dintre destinatari corespunde selecției dvs. Dacă doriți să aplicați regula numai pentru situațiile în care toți destinatarii fac parte din grupurile selectate, alegeți **Corespondență toți destinatarii**.

  Notă
  Adresele din câmpurile **Cc** și **Bcc** sunt, de asemenea, considerate destinatari.

  Important
  Regulile bazate pe grupurile de utilizatori se aplică numai pentru rolurile Hub Transport și Mailbox.

- **Setări.** Configurați expresiile pe care doriți să le căutați în e-mail-uri, în modul descris mai jos:
  1. Alegeți partea e-mail-ului pe care doriți să o verificați:
     - Subiectul e-mail-ului, prin bifarea casetei **Filtrare după subiect**. Sunt filtrate toate e-mail-urile al căror subiect conține una dintre expresiile introduse în tabelul corespunzător.
     - Conținutul mesajului, prin bifarea casetei **Filtrare după conținutul mesajului**. Sunt filtrate toate e-mail-urile în cuprinsul cărora se regăsește oricare dintre expresiile definite.
     - Subiectul și cuprinsul e-mail-ului, prin bifarea ambelor căsuțe. Sunt filtrate toate e-mail-urile al căror subiect corespunde oricărei reguli din primul tavel ȘI al căror text cuprinde orice expresii din al doilea tabel. De exemplu:

       Primul tabel conține expresiile: `buletin informativ` și `săptămânal`.
       Al doilea tabel conține expresiile: `cumpărături`, `preţ` și `ofertă`.

       Un e-mail cu subiectul „Newsletter **lunar** de la producătorul dvs. preferat de ceasuri” și cuprinsul „Avem plăcerea de a vă prezenta **oferta** noastră

cea mai recentă, care conține ceasuri senzaționale la prețuri **irezistibile**.” va corespunde regulii și va fi filtrat. Dacă subiectul este „Noutăți de la producătorul dvs. de ceasuri”, mesajul e-mail nu este filtrat.

2. Realizați listele de condiții, folosind câmpurile din antetul tabelului. Pentru fiecare condiție, urmați pașii de mai jos:
   a. Selectați tipul de expresie folosit în căutări. Puteți opta pentru introducerea expresiei exacte din text sau pentru realizarea unor modele de text folosind expresiile obișnuite.

      Notă
      Sintaxa expresiilor obișnuite este validată conform gramaticii ECMAScript.

   b. Introduceți șirul de căutare în câmpul **Expresie**.

      De exemplu:

      i. Expresia `5[1-5]\d{2}([\s\-]?\d{4}){3}` corespunde cardurilor bancare cu numerele care încep cu cincizeci și unu până la cincizeci și cinci, au șaisprezece cifre în grupuri de patru și grupurile pot fi despărțite printr-un spațiu sau o cratimă. Prin urmare, orice e-mail care conține numărul de card într-unul dintre următoarele formate: `5257-4938-3957-3948`, `5257 4938 3957 3948` sau `5257493839573948`, va fi filtrat.

      ii. Această expresie detectează mesajele e-mail conținând cuvintele `loterie`, `numerar` și `premiu`, exact în această ordine:

      ```
      (lottery)((.|\n|\r)*)( cash)((.|\n|\r)*)( prize)
      ```

      Pentru a detecta mesajele e-mail care conțin fiecare dintre cele trei cuvinte indiferent de ordinea acestora, adăugați trei expresii obișnuite cu o topică diferită.

      iii. Această expresie detectează mesajele e-mail care includ trei sau mai multe apariții ale cuvântului `premiu`:

      ```
      (prize)((.|\n|\r)*)( prize)((.|\n|\r)*)( prize)
      ```

   c. Dacă doriți să diferențiați majusculele de minuscule în comparațiile textelor, bifați caseta **În funcție de tipul de caractere**. De exemplu, după

ce ați bifat caseta, `Buletin de informare` nu coincide cu `buletin de informare`.

d. Dacă nu doriți ca expresia să fie inclusă în alte cuvinte, bifați caseta **Întregul cuvânt**. De exemplu, cu caseta de bifare selectată, expresia `Salariul Anei` nu corespunde `Salariul MariAnei`.

e. Faceți clic pe butonul ⊕ **Adăugare** din antetul coloanei **Acțiune** pentru a adăuga condiția în listă.

- **Acțiuni.** Există o serie de acțiunni pe care le puteți implementa în cazul e-mail-urilor. Fiecare acțiune are, la rândul său, o serie de opțiuni posibile sau acțiuni secundare. Acestea sunt descrise mai jos:

  Acțiuni principale:
  - **Livrare e-mail.** E-mail-ul spam detectate în căsuțele poștale ale destinatarilor.
  - **Carantină.** Mesajul e-mail este criptat și salvat în folderul de carantină din Serverul Exchange, fără a fi livrat destinatarilor. Puteți administra e-mail-urile trecute în carantină de pe pagina **Carantină**.
  - **Redirecționare către.** E-mail-ul nu este transmis către destinatarii inițiali, ci către o căsuță poștală specificată de dvs. în câmpul corespunzător.
  - **Respingere / Ștergere e-mail.** Pe serverele cu rol Edge Transport, mesajele e-mail detectate sunt respinse cu un cod de eroare 550 SMTP. În toate celelalte cazuri, mesajul e-mail este șters fără nicio avertizare. Se recomandă să evitați această acțiune.

  Acțiuni secundare:
  - **Marchează subiectul e-mail-ului ca.** Puteți adăuga o etichetă subiectului e-mail-ului detectat pentru a ajuta utilizatorii să filtreze e-mail-urile în clientul e-mail.
  - **Adăugați un antet mesajelor e-mail.**Puteți adăuga un titlu de antet și o valoare pentru antetele e-mail-ului detectat prin introducerea valorilor dorite în câmpurile corespunzătoare.
  - **Salvare mail pe disc.** O copie a mesajului e-mail detectat este salvată ca fișier în folderul specificat de pe Serverul Exchange. Dacă folderul nu există, va fi creat. Trebuie să menționați o cale absolută a folderului în câmpul corespunzător.

  Notă
  Această opțiune acceptă exclusiv e-mail-urile în format MIME.

  - **Arhivare în cont.** O copie a e-mail-ului detectat este transmisă către adresa e-mail specificată. Această acțiune adaugă adresa e-mail specificată în lista Bcc a e-mail-ului.
- Implicit, în momentul în care un e-mail corespunde condițiilor unei reguli, nu mai este verificat cu privire la celelalte reguli. Dacă doriți ca să continue procesarea regulilor, debifați căsuța **Oprire procesare reguli, dacă condițiile regulii sunt îndeplinite**.

Excluderi

Dacă doriți ca traficul e-mail pentru anumiți expeditori sau destinatari să fie livrat fără luarea în considerare a unor reguli de filtrare a conținutului, puteți defini excepțiile de filtrare.

Pentru a crea o excepție:

1. Faceți clic pe link-ul **Excepții** de lângă caseta **Filtrare conținut**. Această acțiune deschide fereastra de configurare.
2. Introduceți adresele e-mail ale expeditorilor și/sau destinatarilor de încredere în câmpurile corespunzătoare. Un e-mail recepționat de la un expeditor de încredere sau adresat unui destinatar de încredere este exclus din filtrare. La modificarea listei, puteți folosi, de asemenea, următoarele metacaractere pentru a defini un întreg domeniu de e-mail sau un model pentru adresele de e-mail:
   - Asterisk (*) înlocuind zero, unul sau mai multe caractere.
   - Semnul întrebării (?), înlocuind un singur caracter.

   De exemplu, dacă introduceți `*.gov`, toate mesajele e-mail provenind de la domeniul `.gov` vor fi acceptate.
3. Pentru e-mail-urile cu mai mulți destinatari, puteți bifa caseta **Excludere e-mail din filtrare doar dacă toți destinatarii sunt de încredere** pentru aplicarea excepțiilor doar dacă toți destinatarii e-mail sunt prezenți în lista destinatarilor de încredere.
4. Faceți clic pe **Save**.

Filtrare atașamente

Modulul Filtrare atașamente oferă caracteristici de filtrare pentru toate atașamentele mesajelor e-mail. Poate detecta atașamentele cu anumite modele de denumiri sau de un anumit tip. Folosind opțiunea de Filtrare a atașamentelor, puteți:

- Blocați posibilele atașamente periculose, cum ar fi fișierele `.vbs` sau `.exe` sau e-mail-urile care le conțin.

- Blocați atașamentele cu denumiri ofensatoare sau e-mail-urile care le conțin.

Activarea Filtrării atașamentelor

Dacă doriți să folosiți filtrarea atașamentelor, bifați caseta **Filtrare atașamente**.

Pentru a genera și aministra regulile de filtrare a atașamentelor, consultați „Administrarea regulilor de filtrare” (p. 373).

Opțiunile regulilor

- **General.** În această secțiune, trebuie să configurați o denumire pentru regulă. În caz contrar, nu o puteți salva. Selectați caseta de bifare **Activ** dacă doriți ca regula să fie valabilă după ce ați salvat politica.
- **Domeniul de acoperire al regulii.** Puteți limita aplicabilitatea regulii doar la un anumit set de e-mail-uri, prin configurarea următoarelor opțiuni cumulative privind domeniul de acoperire:
  - **Aplicare pentru (direcție).** Selectați direcția traficului e-mail pentru care se aplică regula.
  - **Expeditori.** Puteți decide dacă regula se aplică pentru orice expeditor sau doar pentru anumiți expeditori. Pentru a restrânge domeniul expeditorilor, faceți clic pe butonul **Specific** și selectați grupurile dorite din tabelul din stânga. Vizualizați grupurile selectate în tabelul din dreapta.
  - **Destinatari.** Puteți decide dacă regula se aplică oricărui destinatar sau doar anumitor destinatari. Pentru a restrânge domeniul destinatarilor, faceți clic pe butonul **Specific** și selectați grupurile dorite din tabelul din stânga. Puteți vizualiza grupurile selectate în tabelul din dreapta.

    Regula se aplică dacă oricare dintre destinatari corespunde selecției dvs. Dacă doriți să aplicați regula numai pentru situațiile în care toți destinatarii fac parte din grupurile selectate, alegeți **Corespondență toți destinatarii**.

    Notă
    Adresele din câmpurile **Cc** și **Bcc** sunt, de asemenea, considerate destinatari.

    Important
    Regulile bazate pe grupurile de utilizatori se aplică numai pentru rolurile Hub Transport și Mailbox.

- **Setări.** Specificați câmpurile care sunt permise sau respinse în atașamentele e-mail.

  Puteți filtra atașamentele de e-mail după tipul de fișier sau numele fișierului.

Pentru a filtra atașamentele după tipul de fișier, respectați pașii următori:

1. Bifați caseta **Detectare după tipul de conținut**.
2. Selectați opțiunea de detecție care se potrivește cel mai bine nevoilor dumneavoastră:
   - **Numai următoarele categorii**, dacă aveți o listă limitată de categorii de fișiere interzise.
   - **Toate cu excepția categoriilor următoare**, dacă aveți o listă limitată de categorii de fișiere permise.
3. Selectați tipurile de fișiere care vă interesează din lista disponibilă. Pentru detalii cu privire la extensiile fiecărei categorii, consultați „Tipuri de fișiere pentru filtrarea atașamentelor” (p. 568).

   Dacă vă interesează doar un anumit tip de fișiere, bifați caseta **Extensii personalizate** și introduceți lista extensiilor în câmpul corespunzător.
4. Bifați caseta **Activare detecție tip real** pentru a verifica titlurile și a identifica în mod corect tipul de fișier atașat la scanarea extensiilor restricționate. Aceasta înseamnă că o extensie nu poate fi doar redenumită pentru a sări peste politicile de filtrare a atașamentelor.

   Notă
   Detecția tipului real poate necesita numeroase resurse.

Pentru a filtra atașamentele după denumiri, selectați caseta **Detectare după denumirea fișierelor** și introduceți denumirile de fișiere pe care doriți să le filtrați, în câmpul corespunzător. La modificarea listei, puteți folosi și următoarele metacaractere pentru a defini șabloane:

- Asterisk (*) înlocuind zero, unul sau mai multe caractere.
- Semnul întrebării (?), înlocuind un singur caracter.

De exemplu, dacă introduceți `bază de date.*`, vor fi detectate toate fișierele cu denumirea `bază de date`, indiferent de extensie.

Notă
Dacă activați detecțiile atât după tipul de conținut, cât și după denumirea fișierului (fără detecția tipului real), fișierul trebuie să îndeplinească simultan condițiile pentru ambele tipuri de detecție. De exemplu, ați selectat categoria **Multimedia** și ați introdus numele de fișier `test.pdf`. În acest caz, orice e-mail corespunde regulii, deoarece fișierul PDF nu este un fișier multimedia.

Bifați căsuța **Scanare în arhive** pentru a împiedica ascunderea fișierelor blocate în arhive aparent inofensive, evitând astfel regula de filtrare.

Scanarea este recursivă în interiorul arhivelor și merge implicit până la al patrulea nivel de adâncime al arhivelor. Puteți optimiza scanarea după cum este descris în continuare:

1. Bifați căsuța **Adâncimea maximă a arhivei (niveluri)**.
2. Selectați o valoare diferită din meniul corespunzător. Pentru performanțe superioare, alegeți cea mai mică valoare; pentru protecție maximă, alegeți cea mai mare valoare.

Notă
Dacă ați optat pentru scanarea arhivelor, funcția **Scanare în arhive** este dezactivată și sunt scanate toate arhivele.

- **Acțiuni.** Există o serie de acțiuni pe care le puteți implementa pentru fișierele detectate sau pentru e-mail-urile care le conțin. Fiecare acțiune are, la rândul său, o serie de opțiuni posibile sau acțiuni secundare. Acestea sunt descrise mai jos:

  Acțiuni principale:
  - **Înlocuire fișier.** Șterge fișierele detectate și introduce un fișier text care informează utilizatorul cu privire la măsurile luate.

    Pentru configurarea textului notificării:
    1. Faceți clic pe link-ul **Setări** de lângă caseta **Filtrare atașamente**.
    2. Introduceți textul notificării în câmpul corespunzător.
    3. Faceți clic pe **Save**.
  - **Ștergere fișier.** Șterge fișierele atașate fără nicio avertizare. Se recomandă să evitați această acțiune.
  - **Respingere/Ștergere e-mail.** Pe serverele cu rol Edge Transport, e-mail-ul detectat este respins cu un cod de eroare SMTP 550. În toate celelalte cazuri, mesajul e-mail este șters fără nicio avertizare. Se recomandă să evitați această acțiune.
  - **Trecere e-mail în carantină.** Mesajul e-mail este criptat și salvat în folderul de carantină din Serverul Exchange, fără a fi livrat destinatarilor. Puteți administra e-mail-urile trecute în carantină de pe pagina **Carantină**.
  - **Redirecționare e-mail către.** E-mail-ul nu este transmis către destinatarii inițiali, ci către o adresă e-mail specificată de dvs. în câmpul corespunzător.

– **Livrare e-mail.** Permite trecerea e-mail-ului.

Acțiuni secundare:

– **Marchează subiectul e-mail-ului ca.** Puteți adăuga o etichetă subiectului e-mail-ului detectat pentru a ajuta utilizatorii să filtreze e-mail-urile în clientul e-mail.
– **Adăugare antet la mesajele e-mail.**Puteți adăuga un titlu de antet și o valoare pentru antetele e-mail-ului detectat prin introducerea valorilor dorite în câmpurile corespunzătoare.
– **Salvare e-mail pe disc.** O copie a mesajului e-mail detectat este salvată ca fișier în folderul specificat de pe Serverul Exchange. Dacă folderul nu există, va fi creat. Trebuie să menționați o cale absolută a folderului în câmpul corespunzător.

Notă
Această opțiune acceptă exclusiv e-mail-urile în format MIME.

– **Arhivare în cont.** O copie a e-mail-ului detectat este transmisă către adresa e-mail specificată. Această acțiune adaugă adresa e-mail specificată în lista Bcc a e-mail-ului.

- În mod implicit, dacă un e-mail corespunde domeniului de aplicare al regulii, acesta este procesat exclusiv în conformitate cu regula, fără a fi verificat cu privire la orice alte reguli rămase. Dacă doriți să continuați să verificați în baza celorlalte reguli, debifați caseta de selectare **Oprire procesare reguli, dacă condițiile regulii sunt îndeplinite**.

Excluderi

Dacă doriți ca traficul e-mail pentru anumiți expeditori sau destinatari să fie livrat fără luarea în considerare a unor reguli de filtrare a atașamentului, puteți defini excepțiile de filtrare.

Pentru a crea o excepție:

1. Faceți clic pe link-ul **Excepții** de lângă caseta **Filtrare atașamente**. Această acțiune deschide fereastra de configurare.
2. Introduceți adresele e-mail ale expeditorilor și/sau destinatarilor de încredere în câmpurile corespunzătoare. Un e-mail recepționat de la un expeditor de încredere sau adresat unui destinatar de încredere este exclus din filtrare. La modificarea listei, puteți folosi, de asemenea, următoarele metacaractere pentru a defini un întreg domeniu de e-mail sau un model pentru adresele de e-mail:

- Asterisk (*) înlocuind zero, unul sau mai multe caractere.
- Semnul întrebării (?), înlocuind un singur caracter.

De exemplu, dacă introduceți `*.gov`, toate mesajele e-mail provenind de la domeniul `.gov` vor fi acceptate.

3. Pentru e-mail-urile cu mai mulți destinatari, puteți bifa caseta **Excludere e-mail din filtrare doar dacă toți destinatarii sunt de încredere** pentru aplicarea excepțiilor doar dacă toți destinatarii e-mail sunt prezenți în lista destinatarilor de încredere.
4. Faceți clic pe **Save**.

7.2.12. Criptare

Notă
Acest modul este disponibil pentru:

- Windows pentru stații de lucru
- Windows pentru servere
- macOS

Modulul de Criptare administrează criptarea întregului disc pe stațiile de lucru prin influențarea funcției BitLocker pe Windows și FileVault și respectiv a funcției utilitare de linie de comandă diskutil de pe macOS.

Cu această opțiune, GravityZone poate oferi o serie de beneficii importante:

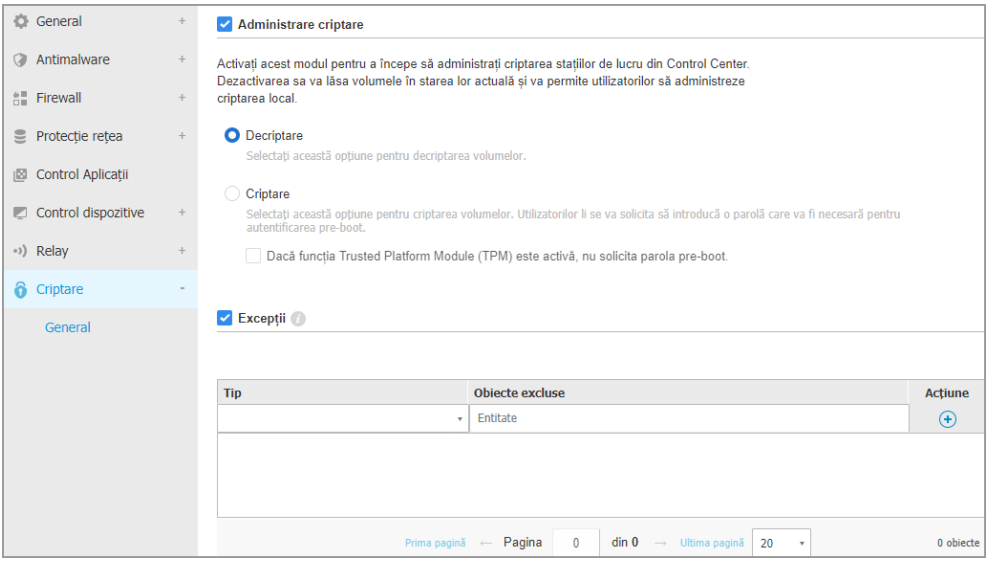
- Datele sunt securizate în cazul pierderii sau furtului dispozitivelor.
- Protecție extinsă pentru cele mai populare platforme de calculatoare din lume, prin utilizarea standardelor recomandate de criptare cu asistență completă din partea Microsoft sau Apple.
- Impact minim asupra performanțelor stațiilor de lucru datorită instrumentelor implicite de criptare.

Modulul de Criptare utilizează următoarele soluții:

- BitLocker versiunea 1.2 și ulterioară, pe stațiile de lucru Windows cu un Modul platformă de încredere (Trusted Platform Module - TPM), pentru volumele boot și non-boot.
- BitLocker versiunea 1.2 și ulterioară, pe stațiile de lucru Windows fără TPM, pentru volumele boot și non-boot.

- FileVault pe stațiile de lucru macOS, pentru volumele boot.
- diskutil pe stațiile de lucru macOS, pentru volumele non-boot.

Pentru a afla care este lista sistemelor de operare acceptate de modulul de Criptare, consultați Ghidul de Instalare GravityZone.



Pagina Criptare

Pentru a începe administrarea criptării stației de lucru din Control Center, bifați căsuța **Administrare criptare**. Atâta timp cât această setare este activată, utilizatorii stațiilor de lucru nu pot administra criptarea local și toate acțiunile lor vor fi anulate sau reluate. Dezactivarea acestei setări va lăsa volumele stației de lucru în starea lor actuală (criptate sau necriptate) și utilizatorii vor putea administra criptarea pe calculatoarele lor.

Pentru a administra procesele de criptare și decriptare, sunt disponibile trei opțiuni:

- **Decriptare** – decriptează volumele și le păstrează decriptate când politica este activă pe stațiile de lucru.
- **Criptare** – criptează volumele și le păstrează criptate când politica este activă pe stațiile de lucru.

În opțiunea Criptare, puteți bifa căsuța **Dacă Modulul platformă de încredere (TPM) este activ, nu solicita parola la criptare**. Această setare furnizează criptare pe stațiile de lucru Windows cu TPM, fără a solicita din partea utilizatorilor o parolă pentru criptare. Pentru detalii, consultați „Criptarea volumelor” (p. 385).

- **Excluderi**

GravityZone acceptă metoda Standardului avansat de criptare (AES) cu chei pe 128 și 256 de biți pe Windows și macOS. Algoritmul actual de criptare utilizat depinde de configurarea fiecărui sistem de operare.

Notă
GravityZone detectează și administrează volumele criptate manual cu BitLocker, FileVault și diskutil. Pentru a începe administrarea acestor volume, agentul de securitate va afișa un mesaj pentru utilizatorii stațiilor de lucru pentru a-și modifica cheile de recuperare. În cazul utilizării altor soluții de criptare, volumele trebuie decriptate înainte de aplicarea unei politici GravityZone.

Criptarea volumelor

Pentru a cripta volume:

1. Bifați căsuța **Administrare criptare**.
2. Selectați opțiunea **Criptare**.

Procesul de criptare începe după ce politica devine activă pe stațiile de lucru, cu unele particularități pe Windows și Mac.

Pe Windows

Agentul de securitate va afișa în mod implicit un mesaj pentru utilizatori pentru ca aceștia să configureze o parolă în vederea începerii criptării. În cazul în care calculatorul dispune de un TPM funcțional, agentul de securitate va notifica utilizatorii să configureze un cod personal de identificare (PIN) pentru a începe criptarea. Utilizatorul trebuie să introducă parola sau codul PIN configurat în această etapă de fiecare dată când pornește stația de lucru, într-un ecran de autentificare înainte de pornire.

Notă
Agentul de securitate vă permite să configurați cerințele legate de complexitatea codului PIN și privilegiile utilizatorilor de a își schimba codul PIN prin intermediul setărilor BitLocker Group Policy (GPO).

Pentru a porni criptarea fără a solicita utilizatorilor stațiilor de lucru să introducă o parolă, bifați caseta **Dacă modulul Trusted Platform Module (TPM) este activ, nu solicita o parolă preliminară pentru pornire**. Această setare este compatibilă cu stațiile de lucru Windows care au TPM și UEFI.

Atunci când caseta **Dacă modulul Trusted Platform Module (TPM) este activ, nu solicita parola preliminară** este activată:

- Pe o stație de lucru necriptată:
  - Procesul de criptare începe fără a necesita o parolă.
  - Ecranul de autentificare pre-boot nu apare la pornirea sistemului.
- Pe o stație de lucru criptată cu parolă:
  - Parola este eliminată.
  - Volumele rămân criptate.
- Pe o stație de lucru criptată sau necriptată, fără funcție TPM sau cu funcție TPM care nu este detectată sau funcțională:
  - Utilizatorului i se solicită să introducă o parolă pentru criptare.
  - Ecranul de autentificare pre-boot apare la pornirea sistemului.

Atunci când caseta **Dacă modulul Trusted Platform Module (TPM) este activ, nu solicita parola preliminară** este dezactivată:

- Utilizatorul trebuie să introducă o parolă pentru criptare.
- Volumele rămân criptate.

Pe Mac

Pentru a începe criptarea pe volumele boot, agentul de securitate va solicita utilizatorilor să introducă datele de autentificare în sistem. Doar utilizatorii care au conturi locale cu drepturi de administrator pot activa criptarea.

Pentru a începe criptarea pe volumele non-boot, agentul de securitate va solicita utilizatorilor să configureze o parolă de criptare. Această parolă va fi solicitată pentru a debloca volumul non-boot la fiecare pornire a calculatorului. În cazul în care calculatorul are mai mult de un volum non-boot, utilizatorii trebuie să configureze o parolă de criptare pentru fiecare dintre acestea.

Decriptarea volumelor

Pentru a decripta volume pe stațiile de lucru:

1. Bifați căsuța **Administrare criptare**.
2. Selectați opțiunea **Decriptare**.

Procesul de decriptare începe după ce politica devine activă pe stațiile de lucru, cu unele particularități pe Windows și Mac.

Pe Windows

Volumele sunt decriptate fără nicio interacțiune a utilizatorilor.

Pe Mac

Pentru volumele boot, utilizatorii trebuie să își introducă datele de autentificare în sistem. În cazul volumelor non-boot, utilizatorii trebuie să introducă parola configurată în timpul procesului de criptare.

În cazul în care utilizatorii stațiilor de lucru își uită parola de criptare, aceștia au nevoie de coduri de recuperare pentru a-și debloca sistemele. Pentru detalii referitoare la extragerea cheilor de recuperare, consultați secțiunea „” (p. 106).

Excluderea partițiilor

Puteți crea o listă de excluderi de la criptare prin adăugarea anumitor partiții de hard-disk, etichete și nume de partiție și tabele de partiții GUID. Pentru stabilirea unei reguli pentru excluderea partițiilor de la criptare:

1. Selectați caseta **Excepții**.
2. Selectați **Tip** și alegeți un tip de unitate din meniul derulant.
3. Introduceți o valoare a unității în câmpul **Obiecte excluse** și țineți cont de următoarele condiții:
   - Pentru o **Partiție hard-disk**, introduceți `D:` sau partiția dumneavoastră urmată de două puncte.
   - Pentru o **Etichetă/Nume** puteți introduce orice etichetă, cum ar fi `Serviciu`.
   - Pentru o partiție **GUID**, introduceți o valoare după cum urmează: `\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\`.
4. Selectați **Adăugare** ⊕ pentru adăugarea excepției pe listă.

Pentru ștergerea unei excepții, alegeți un obiect și selectați **Ștergere** ⊗.

7.2.13. NSX

În această secțiune puteți stabili politica pe care doriți să o utilizați ca profil de securitate NSX. Pentru a face acest lucru:

1. Bifați caseta de selecție **NSX** și configurați-i vizibilitatea și în vSphere Web Client.
2. Introduceți denumirea de identificare a politicii în NSX. Această denumire poate fi diferită de denumirea politicii în GravityZone Control Center. În vSphere va apărea precedată de prefixul `Bitdefender_`. Selectați atent aceastp denumire, deoarece după ce salvați politica nu o veți mai putea edita.

7.2.14. Protecție spațiu de stocare

Notă
Caracteristica de Protecție a spațiului de stocare este disponibilă pentru dispozitivele de stocare atașate la rețea (NAS, Network-Attached Storage) și soluțiile de partajare a fișierelor conforme cu ICAP (Internet Content Adaptation Protocol).

În această secțiune, puteți configura Security Server ca serviciu de scanare pentru dispozitivele NAS și soluțiile de partajare a fișierelor compatibile cu ICAP, precum Nutanix Files și Citrix ShareFile.

Security Server scanează orice fișiere, inclusiv arhive, la solicitarea dispozitivelor de stocare. În funcție de setări, Security Server implementează măsurile adecvate cu privire la orice fișiere infestate, cum ar fi dezinfectarea sau blocarea accesului.

Setările sunt organizate în următoarele secțiuni:

- ICAP
- Excluderi

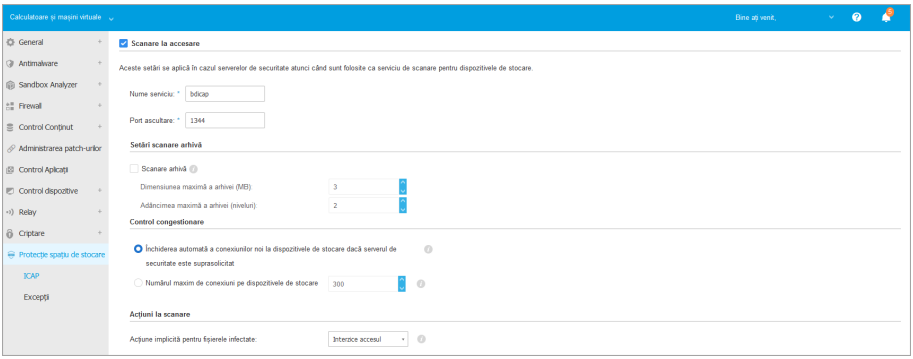
ICAP

Puteți configura următoarele opțiuni pentru Security Server:

- Bifați caseta de selectare **Scanare la acces** pentru a activa modulul de Protecție dispozitive de stocare. Setările necesare pentru comunicarea dintre Security Server și dispozitivele de stocare sunt predefinite după cum urmează:
  - Numele serviciului: `bdicap`.
  - Port ascultare: `1344`.
- În **Setări scanare arhivă**, bifați caseta de selectare **Scanare arhivă** pentru a activa scanarea arhivelor. Configurați dimensiunea și profunzimea maximă a arhivelor care urmează să fie scanate.

Notă
Dacă setați dimensiunea maximă a arhivei pe 0 (zero), Security Server scanează arhivele indiferent de dimensiune.

- În **Control congestie**, selectați metoda preferată de administrare a conexiunilor pe dispozitivele de stocare în cazul suprasolicitării Security Server:
  - **Transferă automat conexiunile pe dispozitivele de stocare dacă Security Server este suprasolicitat**. Dacă un Security Server a atins numărul maxim de conexiuni, dispozitivul de stocare va redirecționa conexiunile în exces către un al doilea Security Server.
  - **Numărul maxim de conexiuni pe dispozitivele de stocare**. Valoarea implicită este configurată la 300 de conexiuni.
- În **Acțiuni scanare**, sunt disponibile următoarele opțiuni:
  - **Blocare acces** – Security Server blochează accesul la fișierele infestate.
  - **Dezinfectare** – Security Server șterge codul malware din fișierele infestate.



Politici - Protejarea dispozitivelor de stocare - ICAP

Excluderi

Dacă doriți ca anumite obiecte să fie excluse din scanare, bifați caseta de selectare **Excluderi**.

Puteți defini excluderile:

- Prin codul hash – identificați fișierul exclus prin codul hash SHA-256.

- Prin metacaractere – identificați fișierele excluse după calea acestora.

Configurarea excluderilor

Pentru a adăuga o excludere:

1. Selectați tipul de excludere din meniu.
2. În funcție de tipul de excludere, specificați obiectul care trebuie exclus, după cum urmează:
   - **Hash** – introduceți codurile SHA-256 separate prin virgulă.
   - **Metacaracter** – specificați un nume de cale absolut sau relativ folosind metacaracterele. Simbolul asterisc (*) corespunde oricărui fișier dintr-un director. Semnul întrebării (?) corespunde unui singur caracter.
3. Adăugați o descriere pentru excludere.
4. Faceți clic pe butonul ⊕ **Adăugare**. Noua regulă de excludere va fi adăugată la listă.

Pentru a elimina o regulă din listă, faceți clic pe butonul ⊗ **Ștergere**.

Importare și exportare de excepții

Dacă intenționați să refolosiți regulile de excludere în mai multe politici, puteți alege să le exportați și să le importați.

Pentru a exporta regulile de excludere:

1. Dați clic pe **Export** în partea de sus a tabelului de excluderi.
2. Salvați fișierul CSV în calculator. În funcție de setările browser-ului, fișierul poate fi descărcat automat sau se poate cere salvarea lui într-o locație implicită.

Fiecare rând din fișierul CSV corespunde unei reguli de excludere, cu câmpurile în următoarea succesiune:

```
<exclusion type>, <object to be excluded>, <description>
```

Acestea sunt valorile disponibile pentru câmpurile CSV:

Tip de excepție:

1, pentru codul hash SHA-256

2, pentru metacaractere

Obiecte ce vor fi excluse:

O valoare hash sau un nume de cale

Descriere

O descriere text pentru a vă ajuta să identificați regula de excludere.

Exemple de reguli de excludere din fișierul CSV:

```
2,*/file.txt,text
2,*/image.jpg,image
1,e4b0c44298fc1c19afbf4c8996fb9227ae41e4649b934ca991b7852b855,hash
```

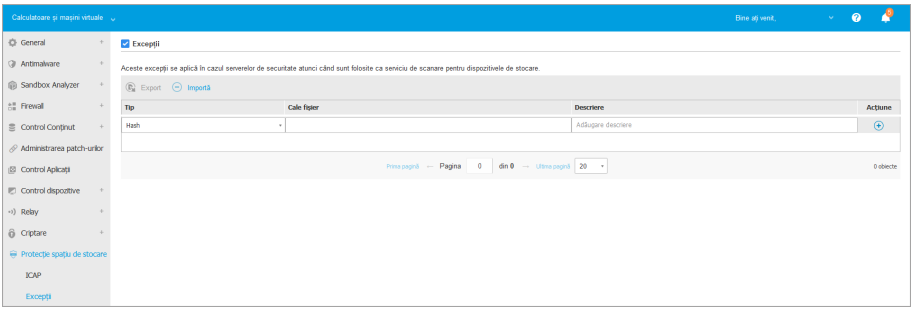
Pentru a importa regulile de excludere:

1. Faceți clic pe **Importă**. Se deschide fereastra **Excepții ale politicii de import**.
2. Faceți clic pe **Adăugare** și apoi selectați fișierul CSV.
3. Faceți clic pe **Save**. Tabelul este completat cu regulile de excludere valabile. Dacă fișierul CSV conține reguli de excludere nevalide, se afișează un mesaj de avertizare cu numerele corespunzătoare ale rândurilor.

Editarea regulilor de excludere

Pentru a edita o regulă de excludere:

1. Faceți clic pe numele acesteia în coloana **Cale** sau pe descriere.
2. Editați regula de excludere.
3. Apăsați `Enter` după ce ați terminat.

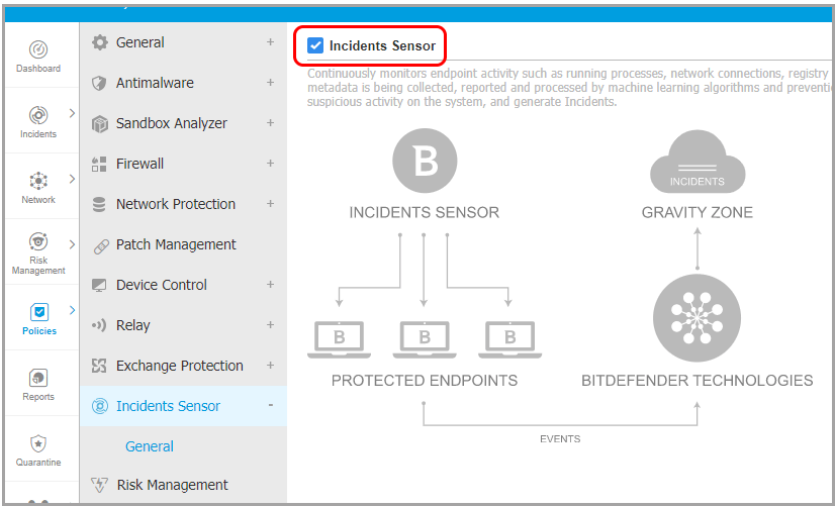


Politici - Protejarea dispozitivelor de stocare - ICAP

7.2.15. Senzor de incidente

Senzorul de incidente monitorizează continuu activitatea la nivel de endpoint, cum ar fi procesele active, conexiunile de rețea, modificările de regiștri și comportamentul utilizatorului. Aceste metadate sunt colectate, raportate și procesate de algoritmi de machine learning și tehnologii de prevenție care detectează activitățile suspecte din sistem și generează incidente.

Bifați caseta Senzor de incidente pentru a activa acest modul.



Senzor de incidente

7.3. Politici pentru dispozitive mobile

Setările politicilor pot fi configurate inițial la crearea politicii. Acestea pot fi ulterior modificate după caz, în orice moment.

Pentru a configura setările unei politici:

1. Mergeți la pagina **Politici**.
2. Selectați **Dispozitive mobile** din selectorul de vederi.
3. Faceți clic pe denumirea politicii. Aceasta va deschide pagina de setări ale politicii.

4. Configurați setările politicii după caz. Setările sunt organizate în următoarele categorii:
   - General
     - Detalii
   - Managementul dispozitivului
     - Securitate
     - Parolă
     - Profiluri

   Puteți selecta categoria de setări folosind meniul din partea stângă a paginii.
5. Faceți clic pe **Salvare** pentru a salva modificările și a le aplica la dispozitivele mobile țintă. Pentru a părăsi pagina de politici fără a salva modificările, faceți clic pe **Anulare**.

7.3.1. General

Categoria **General** conține informații descriptive cu privire la politica selectată.

Detalii

Pagina Details prezintă detalii generale privind politica:

- Nume politică
- Utilizatorul care a creat politica
- Data și ora când a fost creată politica
- Data și ora când a fost modificată politica ultima dată

Puteți redenumi politica introducând noul nume în câmpul corespunzător și făcând clic în câmpul corespunzător. Politicile trebuie să aibă denumiri sugestive, astfel încât dumneavoastră sau un alt administrator să le puteți identifica rapid.

Notă
În mod implicit, numai utilizatorul care a creat politica o poate modifica. Pentru a schimba această setare, deținătorul politicii trebuie să bifeze opțiunea **Permite altor utilizatori să modifice această politică** din pagina **Detalii** a politicii.

7.3.2. Managementul dispozitivului

Setările de gestionare a dispozitivului permit definirea opțiunilor de securitate pentru dispozitivele mobile, blocarea ecranului cu parolă și, în plus, mai multe profiluri pentru fiecare politică de dispozitiv mobil.

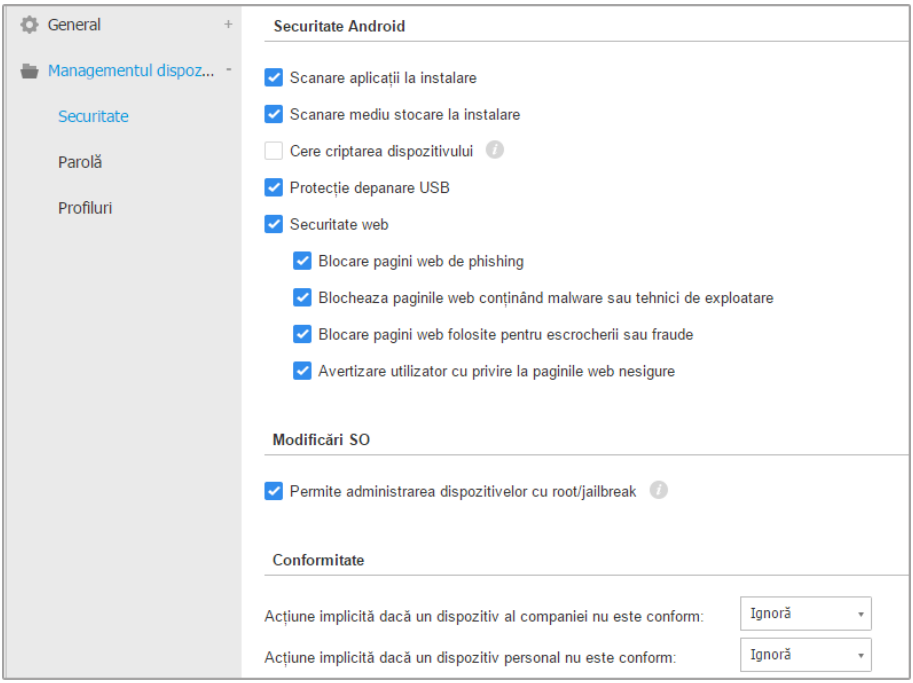
Setările sunt organizate în următoarele secțiuni:

- Securitate
- Parolă
- Profiluri

Securitate

În această secțiune puteți configura diferite setări de securitate pentru dispozitivele mobile, inclusiv scanări antimalware pentru dispozitivele Android, gestionarea dispozitivelor rooted sau jailbroken sau acțiunile care trebuie întreprinse pentru dispozitive non-compatibile.

Important
Scanarea programelor periculoase este efectuată în cloud. Prin urmare, dispozitivul mobil trebuie să aibă acces la Internet.



Politici pentru dispozitive mobile - Setări de securitate

Securitate Android

- Selectați **Scanare aplicații la instalare** dacă doriți să efectuați o scanare atunci când sunt instalate aplicații noi pe dispozitivele mobile gestionate.
- Selectați **Scanare mediu stocare la instalare** dacă doriți să efectuați o scanare de fiecare dată când este montat un dispozitiv de stocare.

Avertisment

În cazul în care este identificat un program periculos, utilizatorului i se este solicitat să-l șteargă. Dacă utilizatorul nu îndepărtează programele periculoase detectate în termen de o oră de la detectare, dispozitivul mobil este declarat neconform fiind aplicată automat acțiunea selectată de neconformitate (Ignorare, Refuzare acces, Blocare, Ștergere sau Deconectare).

- Selectați **Cere criptarea dispozitivului** pentru a solicita utilizatorului să activeze funcția de criptare disponibilă în sistemul de operare Android. Criptarea protejează împotriva accesului neautorizat datele stocate pe dispozitivele Android, inclusiv conturile, setările, aplicațiile descărcate, mediile și alte fișiere. Datele criptate pot fi accesate de pe dispozitive externe numai prin furnizarea parolei de deblocare.

Important

– Criptarea dispozitivului este disponibilă pentru Android 3.0 sau o versiune mai nouă. Nu toate modelele de dispozitive suportă criptare. Verificați fereastra **Detalii dispozitiv mobil** pentru informații suport de criptare.

– Criptare poate afecta performanța dispozitivului.

Avertisment

– Criptarea dispozitivului este ireversibilă și singura modalitate de a reveni la starea necriptată este de a șterge dispozitivul.

– Utilizatorii trebuie să-și salveze datele înainte de a activa criptarea dispozitivului.

– Se interzice utilizatorilor să întrerupă procesul de criptare, altfel își vor pierde o parte sau toate datele.

Dacă activați această opțiune, GravityZone Mobile Client afișează o notificare continuă de informare a utilizatorului în sensul activării criptării. Utilizatorul trebuie să apese butonul **Rezolvat(e)** pentru a trece în ecranul de criptare și a începe procesul. Dacă tehnologia de criptare nu este activată în termen de șapte zile de la notificare, dispozitivul va deveni neconform.

Pentru a activa criptarea pe un dispozitiv Android:

– Bateria trebuie să fie încărcată peste 80%.

– Dispozitivul trebuie să fie conectat până la finalizarea criptării.

– Utilizatorul trebuie să configureze o parolă de deblocare care trebuie să respecte cerințele de complexitate.

Notă

- Dispozitivele Android folosesc aceeași parolă pentru deblocarea ecranului și pentru deblocarea conținutului criptat.

- Criptarea solicită parola, codul PIN sau FACE pentru a debloca dispozitivul, dezactivând celelalte setări de blocare a ecranului.

Procesul de criptare poate dura o oră sau mai mult, timp în care dispozitivul poate reporni de mai multe ori.

Puteți verifica stadiul criptării stocării pentru fiecare dispozitiv mobil în fereastra **Detalii dispozitiv mobil**.

- În modul depanare USB, dispozitivele USB pot fi conectate la calculator printr-un cablu USB, permițând controlul avansat asupra aplicațiilor și sistemelor de operare. În acest caz, securitatea dispoitivelor mobile poate fi în pericol. Activată în mod implicit, opțiunea **Protecție depanare USB** previne utilizarea dispozitivelor în modul depanare USB. Dacă utilizatorul activează depanarea USB, dispozitivul devine automat neconform și se iau măsurile pentru neconformitate. Dacă acțiunea de neconformitate este **Ignoră**, utilizatorul este informat cu privire la setarea nesigură.

  Cu toate acestea, puteți dezactiva această opțiune pentru dispozitivdele mobile care trebuie să lucreze în modul de depanare USB (cum ar fi pentru dezvoltarea și testarea aplicațiilor mobile).

- Selectați **Securitate web** pentru a permite caracteristicile de securitate Web pe dispozitivele Android.

  Securitatea web scanează în cloud fiecare URL accesat, apoi comunică o stare de securitate către GravityZone Mobile Client. Stadiul de securitate URL poate fi: curat, fraudă, malware, phishing sau lipsit de încredere.

  GravityZone Mobile Client poate întreprinde o acțiune specifică pe baza stadiului de securitate al URL:

  – **Blocare pagini web de phishing**. Atunci când utilizatorul încearcă să acceseze un site de phishing, GravityZone Mobile Client blochează URL-ul corespunzător, afișând în schimb o pagină de avertizare.

  – **Blocheaza paginile web conținând malware sau tehnici de exploatare**. Atunci când utilizatorul încearcă să acceseze un site care distribuie malware sau tehnici de exploatare web, GravityZone Mobile Client blochează URL-ul corespunzător, afișând în schimb o pagină de avertizare.

  – **Blocare pagini web folosite pentru escrocherii sau fraude**. Extinde protecția la alte tipuri de escrocherii în afară de phishing (de exemplu conturi escrow false, donații false, amenințări de media sociale și așa mai departe). Atunci

când utilizatorul încearcă să acceseze o pagină web frauduloasă, GravityZone Mobile Client blochează URL-ul corespunzător, afișând în schimb o pagină de avertizare.

– **Avertizare utilizator cu privire la paginile web nesigure**. Atunci când utilizatorul accesează un site web care a fost spart anterior pentru scopuri de tip phishing sau a fost promovat recent prin intermediul e-mailuri spam sau phishing, va fi afișat un mesaj pop-up de avertizare, fără a bloca pagina web.

Important
Funcțiile de Securitate web funcționează numai până la Android 5 și doar cu Chrome și cu browserul Android încorporat.

Modificări SO

Considerat un risc de securitate pentru rețele corporative, dispozitivele rooted sau jailbroken sunt declarate automat neconforme.

- Selectați **Permite administrarea dispozitivelor cu root/jailbreak** dacă doriți să gestionați dispozitivele rooted sau jailbroken din Control Center. Rețineți că, întrucât astfel de dispozitive sunt neconforme în mod implicit, acțiunea de neconformitate selectată le este aplicată în mod automat de îndată ce acestea sunt detectate. Prin urmare, pentru a le putea aplica setările politicii de securitate sau pentru a rula sarcini pe ele, trebuie să setați acțiunea de neconformitate pe Ignoră.
- Dacă debifați căsuța de selecție **Permite administrarea dispozitivelor cu root/jailbreak**, deconectați în mod automat dispozitivele cu root sau jailbreak din rețeaua GravityZone. În acest caz, aplicația GravityZone Mobile Client afișează un mesaj că dispozitivul este compromis prin root/jailbreak. Utilizatorul poate apăsa butonul OK, care redirecționează către ecranul de înregistrare. În momentul în care dispozitivul nu are rooted/jailbreak, sau politica este configurată pentru a permite gestionarea de dispozitive cu root/jailbreak, acesta poate fi reînscris (cu același token pentru dispozitive Android sau cu un nou token pentru dispozitive iOS).

Conformitate

Puteți configura acțiuni specifice care să fie întreprinse în mod automat pe dispozitivele detectate ca neconforme pe baza proprietății dispozitivului (companie sau personal).

Notă
Atunci când se adaugă un nou dispozitiv în Control Center, vi se solicită să specificați proprietatea dispozitivului (companie sau personal). Acest lucru va permite GravityZone să gestioneze dispozitivele mobile personale separat de cele ale companiei.

- Criterii de neconformitate
- Acțiuni de neconformitate

Criterii de neconformitate

Un dispozitiv este declarat neconform în următoarele situații:

- **Dispozitive Android**
  - Dispozitiv cu drept de root activat.
  - GravityZone Mobile Client nu este Administrator dispozitiv.
  - Programul periculos nu este eliminat în decurs de o oră după detectare.
  - Politica nu este îndeplinită:
    - Utilizatorul nu configurează parola de blocare a ecranului în termen de 24 de ore de la prima notificare.
    - Utilizatorul nu modifică parola de blocare a ecranului la ora specificată.
    - Utilizatorul nu activează criptarea dispozitivului în termen de șapte zile de la prima notificare.
    - Modul de depanare USB este activat pe dispozitiv, iar opțiunea politicii de protecție pentru depanarea USB este activată.
- **dispozitive iOS**
  - Dispozitiv compromis prin jailbreak.
  - GravityZone Mobile Client este dezinstalat de pe dispozitivul mobil.
  - Politica nu este îndeplinită:

- Utilizatorul nu configurează parola de blocare a ecranului în termen de 24 de ore de la prima notificare.
- Utilizatorul nu modifică parola de blocare a ecranului la ora specificată.

Acțiune implicită atunci când dispozitivul este neconform

Dacă un dispozitiv este declarat neconform, utilizatorului i se cere să remedieze neconformitatea. Utilizatorul trebuie să facă modificările necesare într-o anumită perioadă de timp, altfel va fi aplicată acțiunea selectată pentru dispozitivul neconform (Ignorare, Interzicere acces, Blocare, Ștergere sau Deconectare).

În orice moment puteți schimba acțiunea pentru dispozitive neconforme în politic. După ce este salvată politica noua acțiune este aplicată la dispozitivele neconforme.

Selectați din meniu corespunzător fiecărui tip de dispozitiv tipul de proprietate care trebuie luate când un dispozitiv este declarat neconform:

- **Ignoră**. Notifică doar utilizatorul că dispozitivul nu este în conformitate cu politica de utilizare a dispozitivului mobil.
- **Interzice accesul**. Blochează accesul dispozitivului la rețelele corporative prin ștergerea setărilor Wi - Fi și VPN, dar păstrând toate celelalte setări definite în politică. Setările blocate sunt restaurate de îndată ce dispozitivul devine compatibil.

  Important
  Când Administrator dispozitiv este dezactivat pentru GravityZone Mobile Client, dispozitivul devine neconform și se aplică automat acțiunea **Interzice accesul**.

- **Blocare**. Blochează imediat ecranul dispozitivului.
  - Pe Android, ecranul este blocat cu o parolă generată de GravityZone numai dacă pe dispozitiv nu este configurată protecția la blocare. Aceasta nu va suprascrie eventualele opțiuni de blocare a ecranului deja configurate, cum ar fi: model, PIN, parolă, amprentă sau blocare inteligentă.
  - Pe dispozitivele iOS, dacă acestea au o parolă pentru blocarea ecranului, parola va fi solicitată pentru deblocare.
- **Ștergere**. Restabilește setările din fabrică ale dispozitivului mobil, ștergând definitiv toate datele utilizatorului.

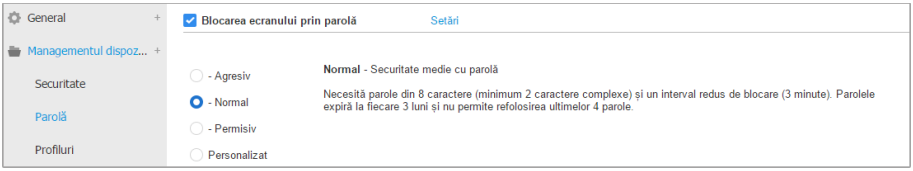
Notă
Curățarea nu șterge acum datele de pe dispozitivele montate (carduri SD).

- **Disociere**. Dispozitivul este imediat eliminat din rețea.

Notă
Pentru a re-înscrie un dispozitiv mobil la care a fost aplicată acțiunea de Deconectare, trebuie să adăugați dispozitivul din nou în Control Center. Dispozitivul trebuie apoi să fie re- inregistrat cu noul token de activare. Înainte de a re-înscrie dispozitivul, asigurați-vă că acele condiții care au dus la deconectarea dispozitivului nu mai există sau modificați setările de politică, pentru a permite gestionarea dispozitivului.

Parolă

În această secțiune puteți alege sa activați caracteristica de blocare a ecranului cu parolă disponibilă în sistemul de operare al dispozitivului mobil.



Politici pentru dispozitive mobile - Setări de protecție cu parolă

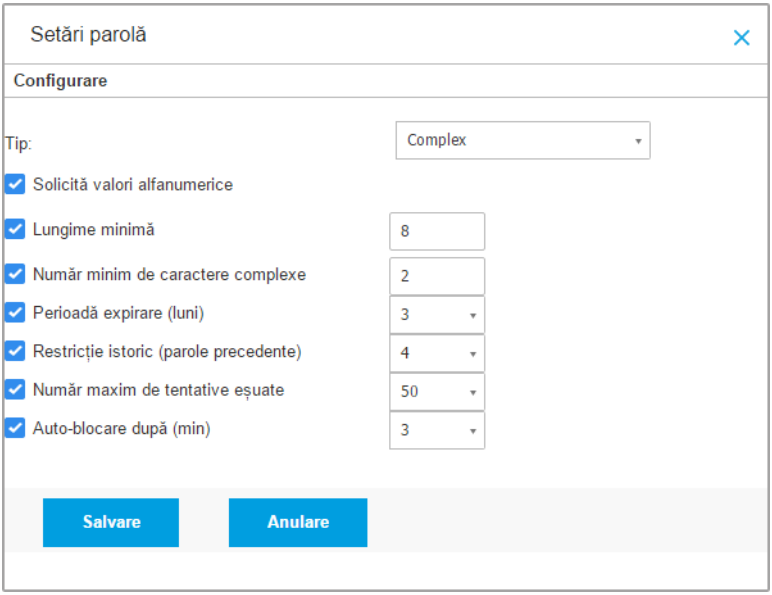
După activarea acestei funcții, o notificare pe ecran solicită utilizatorului să definească o parolă de blocare ecran. Utilizatorul trebuie să introducă o parolă care să respecte criteriile de parolă definite în politică. După stabilirea parolei de către utilizator, sunt șterse toate notificările cu privire la această problemă. La fiecare încercare de a debloca ecranul apare un mesaj care vă solicită să introduceți parola.

Notă
În cazul în care utilizatorul nu a seta o parolă atunci când i s-a solicitat, dispozitivul poate fi utilizat fără o parolă de blocare a ecranului timp de până la 24 de ore după prima notificare. În acest timp, la fiecare 15 minute apare pe ecran un mesaj care solicită utilizatorului să introducă o parolă de blocare a ecranului.

Avertisment
În cazul în care utilizatorul nu setează o parolă în termen de 24 de ore de la prima notificare, dispozitivul mobil devine neconform fiind aplicată acțiunea selectată pentru dispozitive neconforme.

Pentru a configura setările parolei de blocare a ecranului:

1. Selectați caseta de selecție **Blocarea ecranului prin parolă**.
2. Faceți clic pe nivelul de securitate al parolei care corespunde cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.
3. Pentru configurare avansată, selectați nivelul de protecție **Personalizat** și apoi faceți clic pe link-ul **Setări**.



Politici pentru dispozitive mobile - Setări avansate protecție cu parolă

Notă

Pentru a vizualiza cerințele de configurare a parolei de un nivel de securitate predefinit, selectați acest nivel și faceți clic pe link-ul **Setări**. Dacă modificați orice opțiune, nivelul de securitate al parolei se va schimba automat în **Personalizat**.

Opțiuni personalizate.

- **Tip**. Puteți opta pentru o parolă simplă sau complexă. Criterii de complexitate ale parolei sunt definite în sistemul de operare al dispozitivului mobil.
  - Pe dispozitivele Android, parolele complexe trebuie să conțină cel puțin o literă, o cifră sau un caracter special.

    Notă
    Parolele complexe sunt acceptate pe Android 3.0 sau o versiune ulterioară.

  - Pe dispozitivele iOS, parolele complexe nu permit caractere consecutive sau repetate (cum ar fi abcdef, 12345 sau aaaaa, 11111).

  În funcție de opțiunea selectată, atunci când utilizatorul setează parola de blocare a ecranului, sistemul de operare verifică și atenționează utilizatorul în cazul în care nu sunt îndeplinite criteriile necesare.
- **Solicită valori alfanumerice**. Impune ca parola să conțină atât litere cât și numere.
- **Lungime minimă**. Impune ca parola să conțină un număr minim de caractere, pe care le specificați în câmpul corespunzător.
- **Număr minim de caractere complexe**. Impune ca parola să conțină un număr minim de caractere non-alfanumerice (cum ar fi @, # sau $), pe care le specificați în câmpul corespunzător.
- **Perioadă expirare (luni)**. Oblligă utilizatorul să schimbe parola de blocare a ecranului la un interval specificat (în luni). De exemplu, dacă introduceți 3, utilizatorului i se va solicita să schimbe parola de blocare a ecranului la fiecare trei luni.

  Notă
  Pe Android, această caracteristică este acceptată pentru versiunea 3.0 sau o versiune ulterioară.

- **Restricție istoric (parole precedente)**. Selectați sau introduceți o valoare în câmpul corespunzător pentru a specifica numărul ultimelor parole care nu pot fi refolosite. De exemplu, dacă introduceți 4, utilizatorul nu poate reutiliza o parolă care se potrivește cu una dintre ultimele patru parolele folosite.

  Notă
  Pe Android, această caracteristică este acceptată pentru versiunea 3.0 sau o versiune ulterioară.

- **Număr maxim de tentative eșuate**. Specifică de câte ori are utilizatorul dreptul de a introduce o parolă incorectă.

  Notă
  Pe dispozitive iOS, atunci când acest număr este mai mare de 6: după șase tentative eșuate, este necesar un interval de timp, înainte ca utilizatorul să poată introduce din nou parola. Întârzierea de timp crește cu fiecare încercare eșuată.

  Avertisment
  În cazul în care utilizatorul depășește numărul maxim de încercări eșuate de a debloca ecranul, dispozitivul va fi curățat (toate datele și setările vor fi șterse).

- **Auto-blocare după (min)**. Setați perioada de inactivitate (în minute), după care dispozitivul se blochează automat.

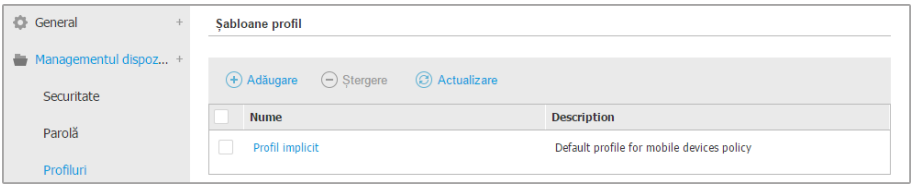
  Notă
  Dispozitivele iOS au o listă predefinită pentru timpul de auto-blocare și nu permit setarea unor valori personalizate. Atunci se atribuie o politică cu o valoare de auto-blocare incompatibilă, dispozitivul activează următoarea perioadă de timp mai restrictivă disponibilă în listă. De exemplu, dacă politica are intervalul de auto-blocare setat la trei minute, dispozitivul se va bloca automat după primele două minute de inactivitate.

Când modificați politica, dacă alegeți un nivel de securitate superior pentru parola de blocare a ecranului, utilizatorii vor fi atenționați să modifice parola conform noilor criterii.

Dacă ștergeți opțiunea **Blocarea ecranului prin parolă**, utilizatorii vor redobândi accesul deplin la setările de blocare a ecranului pe dispozitivul lor mobil. Parola existentă rămâne activă până când utilizatorul decide să o schimbe sau să o elimine.

Profiluri

În această secțiune puteți crea, modifica și șterge profiluri de utilizare pentru dispozitivele mobile. Profilurile de utilizare vă ajută să impuneți setări Wi - Fi și VPN și implementa controlul accesului web pe dispozitivele mobile gestionate.



Politici pentru dispozitive mobile - Modele de profil

Puteți configura unul sau mai multe profiluri, dar numai unul poate fi activ la un moment dat pe un dispozitiv.

- Dacă vă configurați un singur profil, respectivul profil se aplică automat la toate dispozitivele la care este atribuită politica.
- Dacă configurați mai multe profiluri, primul din listă se aplică automat la toate dispozitivele la care este atribuită politica.

Utilizatorii de dispozitive mobile pot vizualiza profilurile atribuite și setările configurate pentru fiecare profil în aplicația GravityZone Mobile Client. Utilizatorii nu pot modifica setările existente într-un profil, dar pot comuta între profiluri, dacă sunt disponibile mai multe.

Notă
Comutarea între profiluri necesită conexiune la Internet.

Pentru a crea un profil nou:

1. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului. Este afișată pagina de configurare a profilului.
2. Configurați setările profilului după cum este nevoie. Pentru informații detaliate, consultați:
   - „Detalii” (p. 406)
   - „Rețele” (p. 406)
   - „Acces Web” (p. 409)

3. Faceți clic pe **Save**. Noul profil este adăugat în listă.

Pentru a șterge unul sau mai multe profiluri, selectați casetele de selectare corespunzătoare și faceți clic pe butonul ⊖ **Ștergere** din partea dreaptă a tabelului.

Pentru a modifica un profil, faceți clic pe numele său, modificați setările după cum este necesar și faceți clic pe **Salvare**.

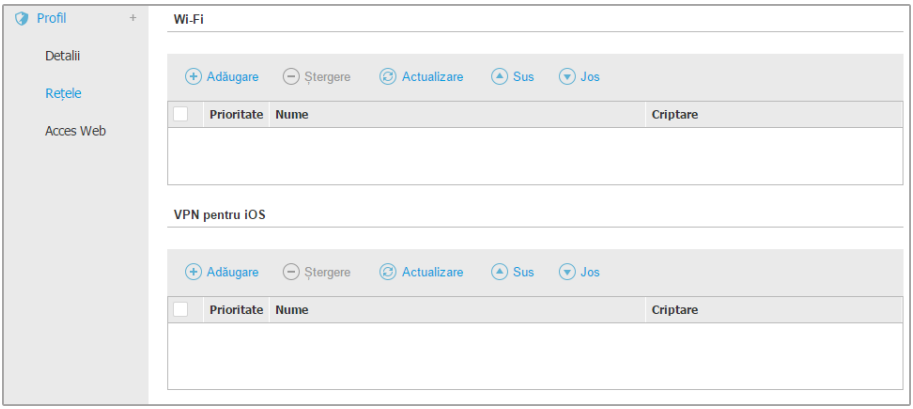
Detalii

Pagina **Detalii** conține informații generale cu privire la profil:

- **Nume**. Introduceți numele dorit pentru profil. Profilurile trebuie să aibă denumiri sugestive, astfel încât dvs. sau alt administrator să le poate identifica rapid.
- **Descriere**. Introduceți o descriere detaliată a profilului. Această opțiune poate ajuta administratorii să identifice cu ușurință un profil din multe altele.

Rețele

În această secțiune puteți specifica setările pentru una sau mai multe rețele Wi - Fi și VPN. Setările VPN sunt disponibile numai pentru dispozitive iOS.



Politici pentru dispozitive mobile - Setările de conexiune rețea ale profilului

Important
Înainte de a defini conexiunile Wi - Fi și VPN, asigurați-vă că aveți toate informațiile necesare la îndemână (parole, setările proxy etc.).

Dispozitivele mobile alocate profilului corespunzător se vor conecta automat la rețeaua definită, când se află în arie. Atunci când sunt create mai multe rețele puteți seta prioritatea, având în vedere faptul că numai o singură rețea poate fi utilizată la un moment dat. Când prima rețea nu este disponibilă, dispozitivul mobil se va conecta la a doua și așa mai departe.

Pentru a configura prioritatea rețelelor:

1. Selectați caseta de selectare a rețelei dorite.
2. Utilizați butoanele de prioritate din partea dreaptă a tabelului:
   - Faceți clic pe **Sus** pentru a promova rețeaua selectată.
   - Faceți clic pe butonul **Jos** pentru a o retrograda.

- **Wi-Fi**

  Puteți adăuga oricâte rețele Wi-Fi necesare. Pentru a adăuga o rețea Wi - Fi:

  1. În secțiunea **Wi-Fi**, faceți clic pe butonul **Adăugare** din partea dreaptă a tabelului. Este afișată o fereastră de configurare.
  2. În secțiunea **General**, puteți configura detaliile conexiunii Wi - Fi:
     - **Nume (SSID)**. Introduceți numele noii rețele Wi - Fi.
     - **Securitate**. Selectați opțiunea corespunzătoare nivelului de securitate al rețelei Wi - Fi:
       - **Niciuna**. Alegeți această opțiune atunci când conexiunea Wi - Fi este publică (nu este necesară acreditare).
       - **WEP**. Alegeți această opțiune pentru a stabili o conexiune Wireless Encryption Protocol (WEP). Introduceți parola necesară pentru acest tip de conexiune în câmpul corespunzător afișat mai jos.
       - **WPA/WPA2 Personal**. Alegeți această opțiune dacă rețeaua Wi - Fi este securizată cu ajutorul Wi-Fi Protected Access (WPA). Introduceți parola necesară pentru acest tip de conexiune în câmpul corespunzător afișat mai jos.
  3. În **TCP/IP** puteți configura setările TCP/IP pentru conexiunea Wi - Fi. Fiecare conexiune Wi - Fi poate folosi IPv4 sau IPv6 sau ambele.
     - **Configurare IPv4**. Dacă doriți să utilizați metoda IPv4, selectați metoda de alocare IP din meniul corespunzător:

DHCP: dacă adresa IP este atribuită automat de un server DHCP. Dacă este necesar, introduceți ID-ul clientului DHCP în câmpul de mai jos.

Dezactivat: selectați această opțiune dacă nu doriți să utilizați protocolul IPv4.

– **Configurare IPv6**. Dacă doriți să utilizați metoda IPv6, selectați metoda de alocare IP din meniul corespunzător:

DHCP: dacă adresa IP este atribuită automat de un server DHCP.

Dezactivat: selectați această opțiune dacă nu doriți să utilizați protocolul IPv6.

– **Servere DNS**. Introduceți adresa a cel puțin un server DNS pentru rețea.

4. La secțiunea **Proxy**, puteți configura setările proxy pentru conexiunea Wi - Fi. Selectați metoda de configurare proxy dorită din meniul **Tip**:
   – **Inactiv**. Alegeți această opțiune dacă rețeaua Wi - Fi nu are setări proxy.
   – **Manual**. Alegeți această opțiune pentru a introduce manual setările proxy. Introduceți numele gazdă al serverului proxy precum și portul pe care-l ascultă pentru conexiuni. Dacă serverul proxy necesită autentificare, selectați caseta de selecție **Authentication** și furnizați numele de utilizator și parola în câmpurile următoare.
   – **Automat**. Alegeți această opțiune pentru a prelua setările proxy dintr-un fișier Proxy Auto-Configuration (PAC), publicat pe rețeaua locală. Introduceți adresa fișierului PAC în câmpul **URL**.
5. Faceți clic pe **Save**. Noua conexiune Wi - Fi este adăugată în listă.

- **VPN pentru iOS**

  Puteți adăuga oricâte reguli este necesar. Pentru a adăuga un VPN:

  1. În secțiunea **VPN for iOS**, faceți clic pe butonul ⊕ **Adăugare** din partea dreaptă a tabelului. Este afișată o fereastră de configurare.
  2. Definiți setările VPN din fereastra **Conexiune VPN**:

     General:

     – **Nume**. Introduceți numele conexiunii VPN.
     – **Criptare**. Protocolul de autentificare disponibil pentru acest tip de conexiune este **IPSec**, care necesită autentificarea utilizatorului prin parolă și mașină de autentificare prin secrete partajate.

- **Server**. Introduceți adresa serverului VPN.
- **Utilizator**. Introduceți numele de utilizator VPN.
- **Parolă**. Introduceți parola VPN.
- **Nume grup**. Introduceți numele grupului.
- **Secret**. Introduceți cheia pre-partajată.

Proxy:

În această secțiune puteți configura setările proxy pentru conexiunea VPN. Selectați metoda de configurare proxy dorită din meniul **Tip**:

- **Inactiv**. Alegeți această opțiune dacă conexiunea VPN nu are setări proxy.
- **Manual**. Această opțiune vă permite să introduceți manual setările proxy.
  - **Server**: introduceți numele gazdei proxy..
  - **Port**: introduceți numărul portului proxy.
  - Dacă serverul proxy necesită autentificare, selectați caseta de selecție **Authentication** și furnizați numele de utilizator și parola în câmpurile următoare.
- **Automat**. Selectați această opțiune pentru a prelua setările proxy dintr-un fișier Proxy Auto-Configuration (PAC), publicat pe rețeaua locală. Introduceți adresa fișierului PAC în câmpul **URL**.

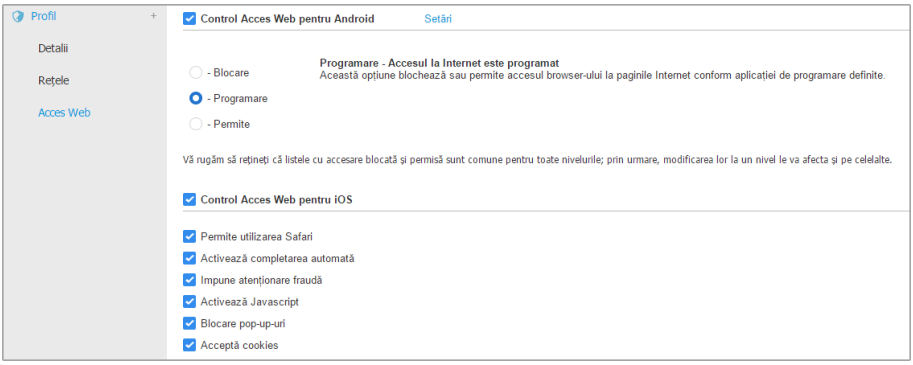
3. Faceți clic pe **Save**. Noua conexiune VPN este adăugată în listă.

Pentru a șterge unul sau mai multe rețele, selectați casetele de selectare corespunzătoare și faceți clic pe butonul ⊖ **Ștergere** din partea dreaptă a tabelului.

Pentru a modifica o rețea, faceți clic pe numele său, modificați setările după cum este necesar și faceți clic pe **Salvare**.

Acces Web

În această secțiune puteți configura controlul accesului web pentru dispozitivele Android și iOS.



Politici pentru dispozitive mobile - Setările de access la internet ale profilului

- **Control Acces Web pentru Android.** Activați această opțiune pentru a filtra accesul web pentru Chrome și browserul Android încorporat. Puteți seta restricții de timp privind accesul web și, de asemenea, puteți permite în mod explicit sau bloca accesul la pagini web specifice. Paginile web blocate de Web Access Control nu sunt afișate în browser. În locul acestora se afișează o pagină web implicită, prin care utilizatorul este informat că pagina web solicitată a fost blocată de Web Access Control.

  Important
  Controlul accesului internet pentru Android funcționează doar până la Android 5 și doar cu Chrome și cu browserul Android încorporat.

  Dispuneți de trei opțiuni de configurare:

  – Selectați **Permite** pentru a acorda întotdeauna acces web.

  – Selectați **Blocare** pentru a bloca întotdeauna accesul web.

  – Selectați **Programare** pentru a permite restricții de timp pentru accesul web la un program detaliat.

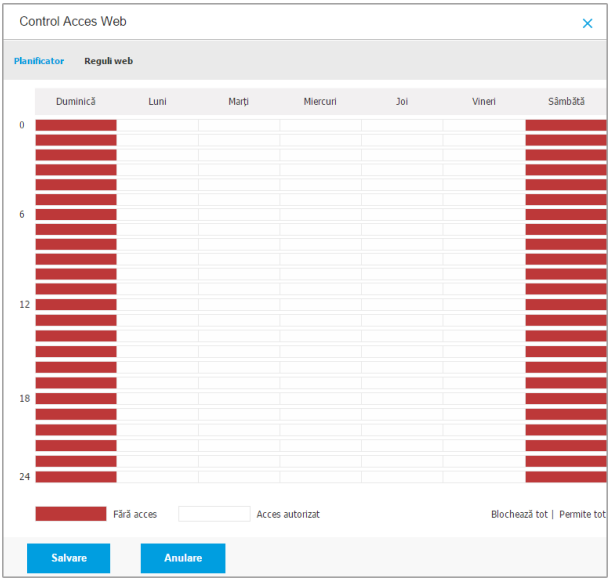
  Indiferent dacă alegeți să permiteți sau să blocați accesul web, puteți defini excepții de la aceste acțiuni pentru toate categoriile de web sau doar pentru adresele de web specifice. Faceți clic pe **Setări** pentru a configura programul dvs. de acces web și excepțiile, după cum urmează:

Planificator

Pentru a restricționa accesul la Internet la anumite ore din zi, pe o bază săptămânală:

1. Selectați din grilă intervalele temporale în care accesul la internet doriți să fie blocat.

   Puteți face clic pe celule individuale sau puteți face clic și trage pentru a acoperi perioade mai lungi de timp. Faceți clic din nou în celulă pentru a inversa selecția.



Politici pentru dispozitive mobile - Planificator pentru accesul la internet

   Pentru a începe o nouă selecție, faceți clic pe **Permite tot** sau **Blochează tot**, în funcție de tipul de restricție pe care doriți să îl puneți în aplicare.

2. Faceți clic pe **Save**.

Reguli web

De asemenea, puteți defini reguli web pentru a bloca în mod explicit sau permite anumite adrese de web, modificând setările Control acces web existente. De exemplu, utilizatorii vor putea accesa o anumită pagină Web și atunci când navigarea pe web este blocată de Control acces web.

Pentru a crea o regulă web:

1. Selectați **Utilizează excepțiile** pentru a permite excepții web.
2. Introduceți adresa pe care doriți să o permiteți sau blocați în câmpul **Adresă Web**.
3. Selectați **Permite** sau**Blochează** din meniul **Permisiune**.
4. Faceți click pe butonul ⊕ **Adăugare** din partea dreaptă a tabelului pentru a adăuga adresa la lista de excepții.
5. Faceți clic pe **Save**.

Pentru a edita o regulă web:

1. Faceți clic pe adresa de web pe care doriți să o editați.
2. Modificați URL-ul existent.
3. Faceți clic pe **Save**.

Pentru a elimina o regulă web:

1. Mutați cursorul pe adresa de web pe care doriți să o eliminați.
2. Faceți clic pe butonul ⊗ **Ștergere**.
3. Faceți clic pe **Save**.

Utilizați metacaractere pentru a defini modele adresei web:

– Asterisc (*) este substitut pentru zero sau mai multe caractere.
– Semn de întrebare (?) este substitut pentru exact un caracter. Puteți folosi mai multe semne de întrebare pentru a defini orice combinație a unui anumit număr de caractere. De exemplu, ??? înlocuiește orice combinație de exact trei caractere.

În tabelul de mai jos, puteți găsi mai multe exemple de sintaxă pentru specificarea adreselor de web.

Sintaxă	Aplicabilitate
`www.example*`	Orice site web sau pagina de web care începe cu `www.example` (indiferent de extensia de domeniu). Regula nu se va aplica la subdomeniile site-ului specificat, cum ar fi `subdomain.example.com`.

Sintaxă	Aplicabilitate
`*example.com`	Orice site care se termină în `example.com`, ininclusiv pagini și subdomenii ale acestora.
`*Şir*`	Orice site web sau pagină web a cărei adresă conține șirul de caractere specificat.
`*.com`	Orice site care are extensia de domeniu `.com` inclusiv paginile și subdomeniile acestora. Utilizați această sintaxă pentru a exclude de la scanare toate domeniile de nivel superior.
`www.example?.com`	Orice adresa de web care începe cu `www.example?.com`, unde ? poate fi înlocuit cu orice caracter unic. Aceste site-uri pot include: `www.example1.com` sau `www.exampleA.com`.

- **Control Acces Web pentru iOS.** Activați această opțiune pentru a gestiona centralizat setările de browser-ului iOS inclus (Safari). Utilizatorii de dispozitive mobile nu vor mai putea schimba setările respective de pe dispozitivul lor.
  - **Permite utilizarea Safari**. Această opțiune vă ajută să controlați utilizarea browser-ului Safari pe dispozitivele mobile. Dezactivarea opțiunii elimină comanda rapidă Safari de pe interfața iOS, prevenind astfel accesul utilizatorilor la Internet prin intermediul Safari.
  - **Activează completarea automată**. Dezactivați această opțiune dacă doriți să preveniți stocarea în browser a formularelor de intrări, care pot include informații sensibile.
  - **Impune atenționare fraudă**. Selectați această opțiune pentru a vă asigura că utilizatorii sunt avertizați atunci când accesează pagini web frauduloase.
  - **Activează Javascript**. Dezactivați această opțiune dacă doriți ca Safari să ignore javascript de pe site-uri.
  - **Blocare pop-up-uri**. Selectați această opțiune pentru a preveni deschiderea automată a ferestrelor de tip pop-up.
  - **Acceptă cookies**. Safari permite în mod implicit fișiere de tip cookie. Dezactivați această opțiune dacă doriți să preveniți ca site-urile să stocheze informații de navigare.

Important
Control acces web pentru iOS nu este compatibil cu iOS 13.

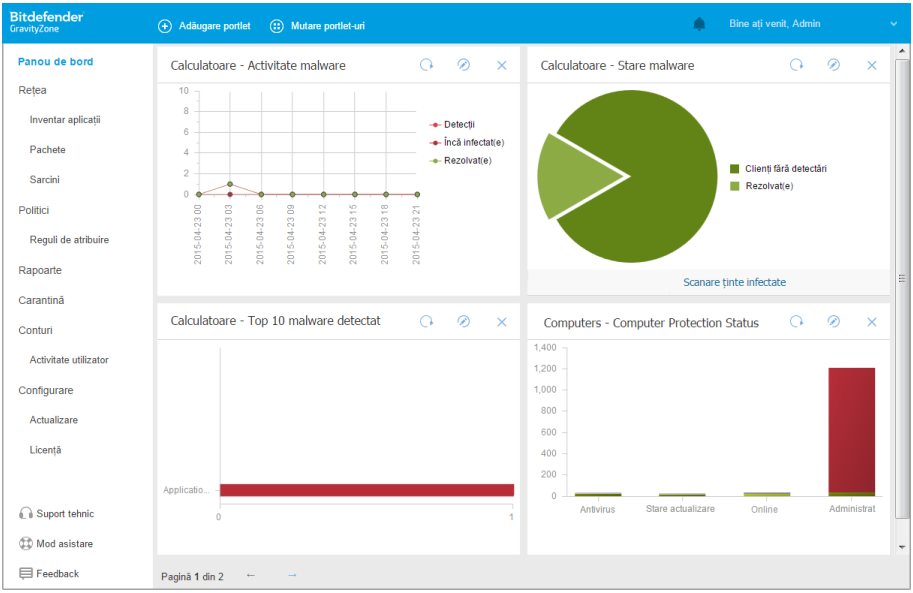
8. PANOUL DE MONITORIZARE

Analiza corespunzătoare a securității rețelei dumneavoastră necesită accesibilitatea și corelarea datelor. Informațiile centralizate privind securitatea vă permit să monitorizați și să garantați conformitatea cu politicile de securitate ale companiei, să identificați rapid problemele și să analizați amenințările și vulnerabilitățile.

8.1. Panou de bord

Panoul de control Control Center reprezintă un mod de afișare personalizabil, ce oferă o vedere de ansamblu rapidă asupra securității tuturor endpoint-urilor și asupra stării rețelei.

Portlet-urile panoului de bord afișează în timp real diferite informații referitoare la securitate, utilizând tabele ușor de citit, permițându-vă astfel să identificați rapid orice probleme care ar putea să vă solicite atenția.



Panoul de bord

Ce trebuie să știți despre portleturi:

- Control Center este livrat cu mai multe portlet-uri predefinite pentru panoul de bord.
- Fiecare portlet al panoului de control include un raport detaliat în fundal, accesibil cu un singur clic pe grafic.
- Există mai multe tipuri de portlet-uri care includ diverse informații despre protecția stațiilor de lucru, cum ar fi starea de actualizare, starea programelor periculoase, activitatea firewall.

  Notă
  În mod implicit, portlet-urile recuperează date pentru ziua curentă și, spre deosebire de rapoarte, nu pot fi setate pentru intervale mai mari de o lună.

- Informațiile afișate prin portlet-uri se referă doar la stațiile de lucru din contul dvs. Puteți personaliza ținta și preferințele fiecărui portlet folosind comanda **Editare portlet**.
- Faceți clic pe intrările de legendă din grafic, atunci când sunt disponibile, pentru a ascunde sau a afișa variabila corespunzătoare pe grafic.
- Portlet-urile sunt afișate în grupuri de câte patru. Utilizați bara de derulare verticală sau săgețile sus și jos pentru a naviga grupurile de portlet-uri.
- Pentru o serie de tipuri de rapoarte, opțiunea de a rula instant anumite sarcini pe stațiile de lucru țintă, fără a trebui să accesați pagina **Rețea** pentru a executa sarcina (de exemplu, scanarea stațiilor de lucru infestate sau actualizarea stațiilor de lucru). Folosiți butonul din partea de jos a portlet-ului pentru a lua măsurile disponibile.

Panoul este ușor de configurat, în funcție de preferințele individuale. Puteți edita setările portlet-ului, adăuga portlet-uri suplimentare, șterge sau rearanja portlet-uri existente.

8.1.1. Reîmprospătarea datelelor de portlet

Pentru a vă asigura că portlet-ul afișează cele mai recente informații, faceți clic pe butonul **Reîmprospătare** din bara de titlu a acestuia.

Pentru a actualiza simultan informațiile tuturor portlet-urilor, faceți clic pe butonul **Reîmprospătare portlet-uri** din partea de sus a panoului de informații.

8.1.2. Editarea setărilor Portlet

Unele dintre portlet-uri oferă informații despre stare, în timp ce altele raportează evenimentele de securitate din ultima perioadă. Puteți verifica și configura perioada

de raportare a unui portlet printr-un clic pe pictograma **Editare portlet** de pe bara cu denumirea sa.

8.1.3. Adăugarea unui portlet nou

Puteți adăuga alte portlet-uri suplimentare pentru a obține informațiile de care aveți nevoie.

Pentru a adăuga un nou portlet:

1. Mergeți la pagina **Panou de bord**.
2. Faceți clic pe butonul **Adăugare portlet** din partea de sus a consolei. Este afișată fereastra de configurare.
3. La secțiunea **Detalii**, configurați detaliile portlet:
   - Tipul stației de lucru (**Calculatoare**, **Mașini virtuale** sau **Dispozitive mobile**)
   - Tip de raport cadru
   - Nume portlet sugestiv
   - Intervalul de timp pentru raportarea evenimentelor

   Pentru mai multe informații cu privire la tipurile de rapoate disponibile, consultați „Tipuri de rapoarte” (p. 475).
4. La secțiunea **Ținte**, selectați obiectele și grupurile de rețea pe care le doriți incluse.
5. Faceți clic pe **Save**.

8.1.4. Ștergerea unui portlet

Puteți elimina cu ușurință orice portlet, făcând clic pe pictograma **Ștergere** de pe bara de titlu. După ce ați eliminat un portlet, nu îl mai puteți recupera. Cu toate acestea, puteți crea un alt portlet cu exact aceleași setări.

8.1.5. Rearanjarea portlet-urilor

Puteți rearanja portlet-urile panou pentru ca acestea să răspundă mai bine nevoilor dvs. Pentru a rearanja portlet-uri:

1. Mergeți la pagina **Panou de bord**.
2. Trageți și inserați fiecare portlet în poziția dorită. Toate celelalte portlet-uri dintre pozițiile noi și cele vechi sunt mutate pentru a le menține ordinea.

Notă
Puteți muta portlet-urile doar în pozițiile ocupate deja.

9. INVESTIGAREA INCIDENTELOR

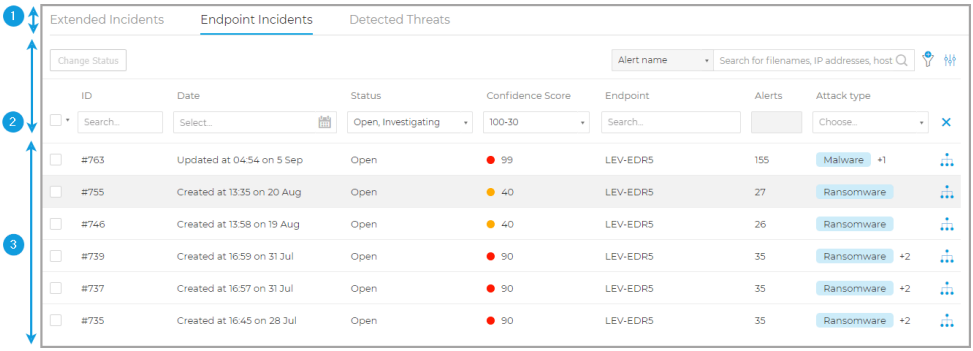
Secțiunea **Incidente** vă ajută să filtrați, să analizați și să întreprindeți acțiuni referitoare la toate evenimentele de securitate detectate de Senzorul de incidente într-un anumit interval de timp.

Secțiunea **Incidente** conține următoarele pagini:

- **Incidente**: permite vizualizarea și investigarea evenimentelor de securitate.
- **Listă blocare**: administrează fișierele blocate implicate în evenimente de securitate.

9.1. Pagina Incidente

Utilizați pagina **Incidente** pentru a filtra și a gestiona evenimentele de securitate.



Vedere de ansamblu asupra paginii de incidente

Notă
Disponibilitatea acestor file poate diferi în funcție de licența inclusă în planul dumneavoastră actual.

Această pagină conține următoarele zone:

1. Bara cu file dintr-o fereastră care include diferite tipuri de incidente:
   - **Amenințări detectate**: afișează toate evenimentele de securitate identificate ca fiind amenințări prin modulele de prevenție GravityZone. Aceste incidente sunt detectate la nivelul endpoint-urilor și sunt remediate prin acțiuni predefinite în politicile de securitate aplicate mediului dumneavoastră.

2. Opțiuni de filtrare pentru personalizarea tabelului dumneavoastră:
   - Selectați butonul **Afișare/Ascundere coloane** pentru a adăuga sau a șterge coloanele de filtrare.

     Pagina se va actualiza automat, încărcând cardurile evenimentelor de securitate cu informații corespunzătoare coloanelor adăugate.
   - Selectați butonul **Afișare/Ascundere filtre** pentru a afișa sau a ascunde bara filtrelor.
   - Selectați butonul **Ștergere filtre** pentru resetarea tuturor filtrelor.
3. Tabelul Incidente afișează o listă a evenimentelor de securitate care se potrivesc filtrelor specificate.

Notă
Această caracteristică nu mai este compatibilă cu Internet Explorer.

Bara Descriere generală

Bara **Descriere generală** listează incidentele deschise, cele mai importante alerte și dispozitivele afectate, printre alte date relevante, pentru a vă oferi o vedere de ansamblu asupra situației generale privind amenințările cu care se confruntă mediul dumneavoastră.

Bara Descriere generală

Notă
Disponibilitatea și conținutul barei **Descriere generală** poate diferi în funcție de licența inclusă în planul dumneavoastră actual.

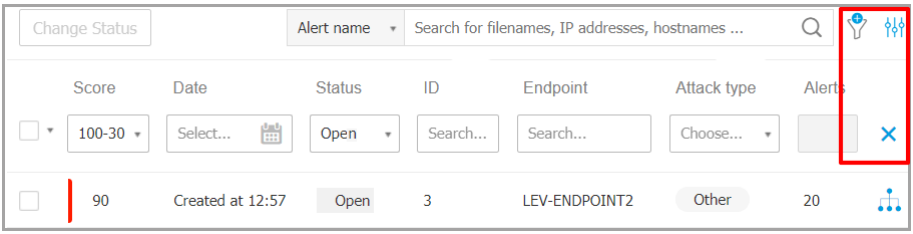
Filtrarea incidentelor din bara Descriere generală

Puteți filtra lista de incidente selectând valorile din bara Descriere generală:

- Dacă selectați o valoare din secțiunea **INCIDENTE DESCHISE**, vor fi afișate doar incidentele care au nivelul de severitate selectat.
- Dacă selectați o valoare din secțiunea **CELE MAI IMPORTANTE ALERTE**, numele alertei va apărea în câmpul de căutare și vor fi afișate doar incidentele în cadrul cărora a fost detectată alerta.
- Dacă selectați o valoare din secțiunea **CELE MAI IMPORTANTE TEHNICI**, numele tehnicii va apărea în câmpul de căutare și vor fi afișate doar incidentele în cadrul cărora a fost detectată tehnica.
- Dacă selectați o valoare din secțiunea **CELE MAI IMPORTANTE DISPOZITIVE AFECTATE**, vor fi afișate doar incidentele care afectează dispozitivul selectat.

9.1.1. Tabelul filtrelor

Pagina **Incidente** vă permite să alegeți incidentele afișate prin personalizarea tabelului filtrelor.



Tabelul filtrelor

- Selectați butonul **Afișare/Ascundere coloane** pentru a adăuga sau a șterge coloanele de filtrare.

  Pagina se va actualiza automat, încărcând cardurile evenimentelor de securitate cu informații corespunzătoare coloanelor adăugate.
- Selectați butonul **Afișare/Ascundere filtre** pentru a afișa sau a ascunde bara filtrelor.
- Selectați butonul **Ștergere filtre** pentru resetarea tuturor filtrelor.

Găsiți detalii privind opțiunile disponibile de filtrare în următorul tabel:

Opțiuni de filtrare	Detalii
Scor	Scorul de încredere este un număr între 100 și 10, indicând cât de periculos este posibil să fie un eveniment de securitate. Cu cât scorul este mai mare, cu atât este mai sigur că evenimentul respectiv este periculos. Pentru a filtra în funcție de scorul de încredere, trageți bara glisantă la valorile alese. Sau puteți utiliza câmpurile numerice de sub bara de glisare. Selectați **OK** pentru confirmarea selecției scorului.
Data	Pentru a filtra în funcție de dată: 1. Selectați pictograma calendar sau câmpul **Date** pentru a deschide pagina de configurare a datelor. 2. Selectați intervalul de timp în care s-a produs incidentul: • Selectați filele **De la** și **Până la** pentru a selecta datele care definesc intervalul de timp. **Notă** Puteți specifica momentul exact pentru data de început și data de final, utilizând câmpurile pentru ore și minute de sub calendar. • De asemenea, puteți selecta un interval predeterminat, raportat la momentul actual. 3. Selectați **OK** pentru a aplica filtrul.
Stare	Filtrați incidentele după starea actuală a acestora, verificând una sau mai multe dintre opțiunile de stare din meniul derulant **Stare**: • **Deschis**: în cazul evenimentelor de securitate care nu au fost investigate • **În curs de investigare**: în cazul evenimentelor de securitate care se află în curs de investigare • **Fals pozitiv**: în cazul evenimentelor de securitate etichetate ca fiind alarme false • **Închis**: în cazul evenimentelor de securitate pentru care investigarea a fost finalizată

Opțiuni de filtrare	Detalii
ID	Micșorați lista incidentelor, căutând un anumit număr ID al evenimentelor de securitate.
Stație de lucru	Micșorați lista incidentelor, căutând un anumit nume de endpoint din rețeaua dumneavoastră administrată.
Tipul de atac	Tipul atacului este o listă dinamică a celor mai comune tipuri de atac, modificându-se pe baza indicatorilor de atac care se găsesc în evenimentele de securitate listate.
Alerte	Coloana **Alerte** afișează numărul de alerte declanșate pentru fiecare incident.
Sistem de operare endpoint	Această opțiune filtrează evenimentele de securitate în funcție de sistemul de operare al endpoint-urilor implicate.

Notă
Opțiunile de filtrare pot diferi în funcție de licența inclusă în planul dumneavoastră actual.

Pentru a căuta mai multe elemente care nu sunt vizibile în tabelul filtrelor, selectați una dintre opțiunile de căutare din meniul derulant **Căutare**:

- **Denumire alertă** - de la 3 la maxim 1000 de caractere.
- **IP endpoint** - maxim 45 de caractere.
- **MD5** - maxim 32 de caractere.
- **SHA256** - maxim 64 de caractere.
- **Denumire nod** - maxim 360 de caractere.
- **Nume de utilizator** - maxim 1000 de caractere.

Pagina va fi actualizată în mod automat, încărcând doar cardurile evenimentelor de securitate care se potrivesc elementului căutat.

9.1.2. Vizualizarea Listei evenimentelor de securitate

Pagina **Incidente** afișează o listă a evenimentelor de securitate care se potrivesc filtrelor selectate.

În mod implicit există 20 de evenimente pe pagină, grupate în funcție de dată. Pagina se va reîncărca automat la intervale regulate de timp, atunci când **Senzorul de incidente** detectează noi evenimente.

Important
Toate evenimentele de securitate mai vechi de 90 de zile sunt șterse automat atât din secțiunea **Amenințări detectate**, cât și din depozitul de evenimente de securitate.

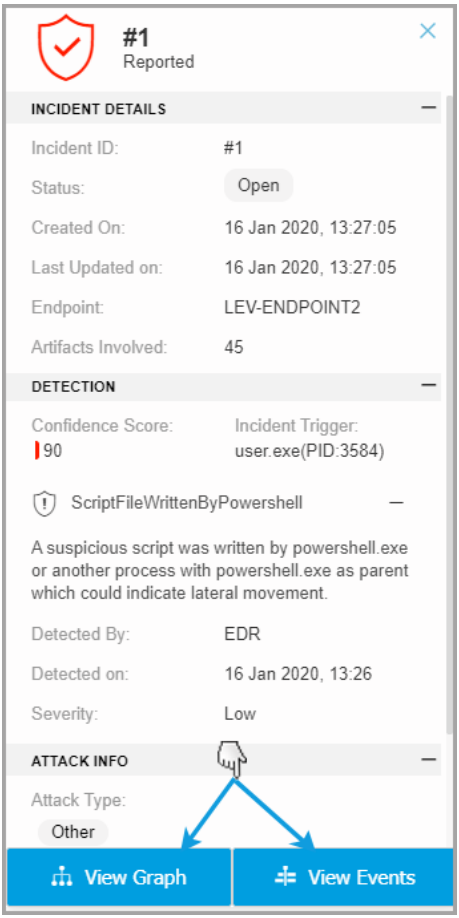
Pentru a naviga în pagină, utilizați tastele săgeată, rotița de derulare sau efectuați clic pe bara de derulare. Modificați numărul de evenimente afișate în partea inferioară a paginii. Puteți alege să afișați maxim 100 de evenimente pe pagină.

Fiecare intrare a evenimentelor de securitate este listată într-un format de card complet, oferind o prezentare generală a fiecărui incident, cu informații bazate pe filtrele selectate.

Notă
Verificați culoarea marginii din partea stângă pentru a evalua rapid nivelul de încredere (scăzut, mediu sau ridicat).

Panoul evenimentelor de securitate

- Dacă faceți clic pe butonul **Vizualizare grafic** asociat unui panou de evenimente de securitate, acesta va fi deschis într-o nouă pagină, unde puteți analiza amănunțit incidentul și întreprinde acțiunile corespunzătoare.
- Dacă selectați cardul evenimentelor de securitate, se va deschide un panou rapid de vizualizare lateral, conținând informații privind incidentul selectat.



Vizualizare rapidă a detaliilor privind incidentele

- Selectați butonul **Vizualizare grafic** pentru a accesa vizualizarea graficului incidentului.
- Selectați butonul **Vizualizare grafic** pentru a accesa cronologia incidentului.

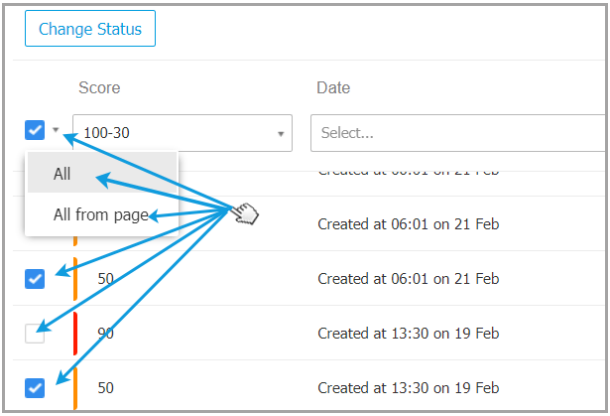
- În cazul în care selectați caseta oricărui card de evenimente de securitate, va fi activat butonul **Modificare stare**, permițându-vă să modificați starea curentă a incidentului.

Modificarea statusului evenimentelor de securitate

Starea de investigație vă ajută să țineți evidența incidentelor deja investigate și marcate ca fiind închise sau fals pozitive, a incidentelor investigate în prezent și care sunt deschise sau a incidentelor noi care urmează să fie analizate.

Puteți alege să modificați statusul unuia sau mai multor evenimente de securitate la un moment dat:

1. Selectați casetele cardurilor evenimentelor de securitate care vor trece printr-o schimbare de stare.

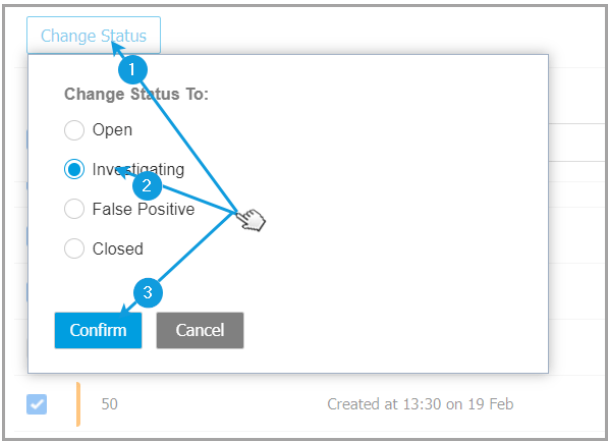


Selectarea cardurilor evenimentelor de securitate

Le puteți selecta individual sau utilizând opțiunile generale de selectare din meniul derulant.

Notă
De asemenea, puteți naviga prin mai multe pagini cu evenimente de securitate în timp ce mențineți selecția.

2. Selectați butonul **Modificare stare** și alegeți opțiunile dorite:

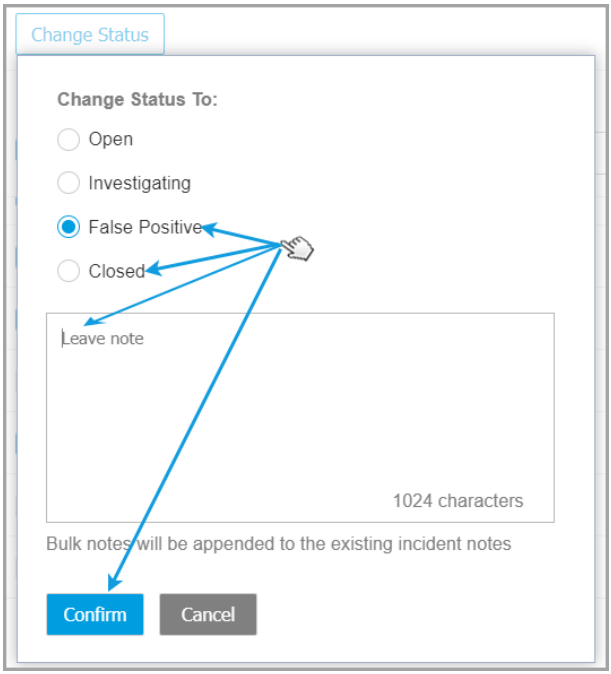


Modificarea statusului evenimentelor de securitate

- **Deschidere** - atunci când un eveniment de securitate nu este încă investigat.
- **În curs de investigare**- atunci când ați început să investigați evenimentul.
- **Fals pozitiv** - dacă ați analizat evenimentul și l-ați identificat ca fals pozitiv.
- **Închis**- atunci când ați finalizat investigarea.

Notă

Se va deschide o casetă la modificarea stării evenimentelor în **Fals pozitiv** sau **Închis**, unde puteți introduce o notă privind motivele pentru modificarea stării evenimentului, pentru a putea fi consultată mai târziu.



Anexarea unei note la evenimentele fals pozitive și închise

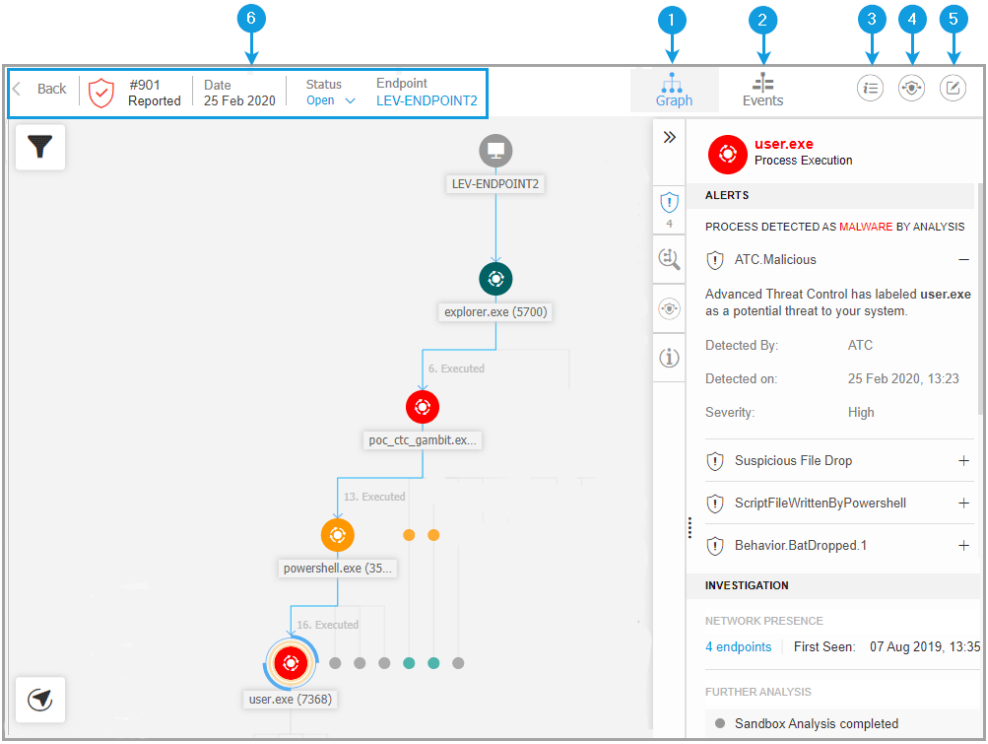
Notă
Nota va fi anexată la cele care deja există în cadrul incidentelor filtrate.

3. Selectați **Confirmare** pentru a aplica opțiunea de modificare a statusului selectat.

9.1.3. Revizuirea unei amenințări detectate

În pagina **Incidente**, identificați evenimentul de securitate pe care doriți să îl analizați și selectați butonul **Vizualizare grafic** pentru a-l afișa într-o pagină nouă.

Fiecare eveniment de securitate are o pagină dedicată care conține informații detaliate despre secvența de evenimente (afișată în grafic ca noduri de evenimente de securitate conectate) care au dus la declanșarea evenimentului și opțiuni de acțiuni de remediere.


6
1
2
3
4
5
Back
#901
Reported
Date
25 Feb 2020
Status
Open
Endpoint
LEV-ENDPOINT2
Graph
Events
LEV-ENDPOINT2
explorer.exe (5700)
6. Executed
poc_ctc_gambit.ex...
13. Executed
powershell.exe (35...
16. Executed
user.exe (7368)
user.exe
Process Execution
ALERTS
PROCESS DETECTED AS MALWARE BY ANALYSIS
ATC.Malicious
Advanced Threat Control has labeled user.exe as a potential threat to your system.
Detected By: ATC
Detected on: 25 Feb 2020, 13:23
Severity: High
Suspicious File Drop
ScriptFileWrittenByPowershell
Behavior.BatDropped.1
INVESTIGATION
NETWORK PRESENCE
4 endpoints
First Seen: 07 Aug 2019, 13:35
FURTHER ANALYSIS
Sandbox Analysis completed

1. Fila Grafic

   Fila Grafic afișează evenimentul de securitate și elementele componente ale acestuia, evidențiind Calea critică a incidentului și afișând detalii despre nodul care a declanșat incidentul în panoul **Detalii nod**.

2. Fila Evenimente

   Fila Evenimente afișează evenimentele și alertele detectate din sistem, care pot fi filtrate, și descrierile aferente.

3. Panou Informații incident

   Acest panou conține secțiuni care pot fi restrânse, cu detalii cum ar fi ID-ul incidentului, statusul curent, marcajul temporal din momentul creării și ultimei actualizări, numărul de elemente implicate, numele declanșatorului și informații referitoare la atac.

4. Panou Remediere

   Acest panou include secțiuni care pot fi restrânse cu acțiuni întreprinse automat de GravityZone și pașii recomandați pe care îi puteți urma pentru a diminua consecințele incidentului.

5. Clipboard note

   La selectarea opțiunii **Note** se deschide un clipboard în care puteți adăuga note despre incidentul curent, pe care le puteți citi când accesați din nou pagina incidentului.

6. Bară de stare incident

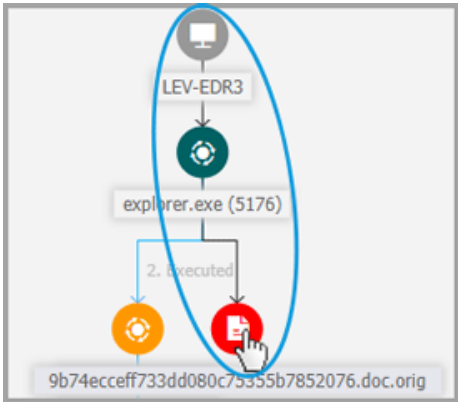
   Bara de stare oferă detalii despre ID-ul incidentului, data și ora la care a fost generat, status, declanșatorul incidentului și endpoint-ul pe care îl afectează. La selectarea opțiunii **Înapoi**, veți reveni în pagina principală de **Incidente**.

Noduri evenimente securitate

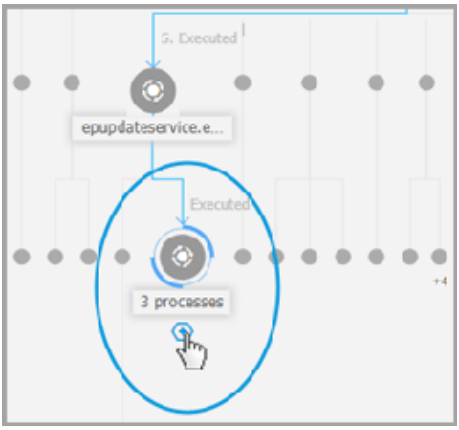
Iată ce trebuie să știți despre nodurile de evenimente de securitate:

- Fiecare nod reprezintă un anumit element implicat în incidentul investigat.
- Toate nodurile care formează calea critică sunt afișate implicit în detaliu atunci când deschideți incidentul, iar celelalte incidente sunt estompate pentru a evita aglomerarea afișajului.

– Dacă plasați cursorul deasupra nodului care nu face parte din calea critică, acesta va fi evidențiat pentru a afișa calea către punctul de origine, fără a întrerupe Calea critică.



- Trei sau mai multe noduri de evenimente cu același tip ce acțiune reproduse dintr-un mod principal sunt grupate într-un nod cluster extensibil.



– Doar nodurile fără elemente subordonate vor fi eliminate din graficul incidentului atunci când nodul cluster este restrâns.

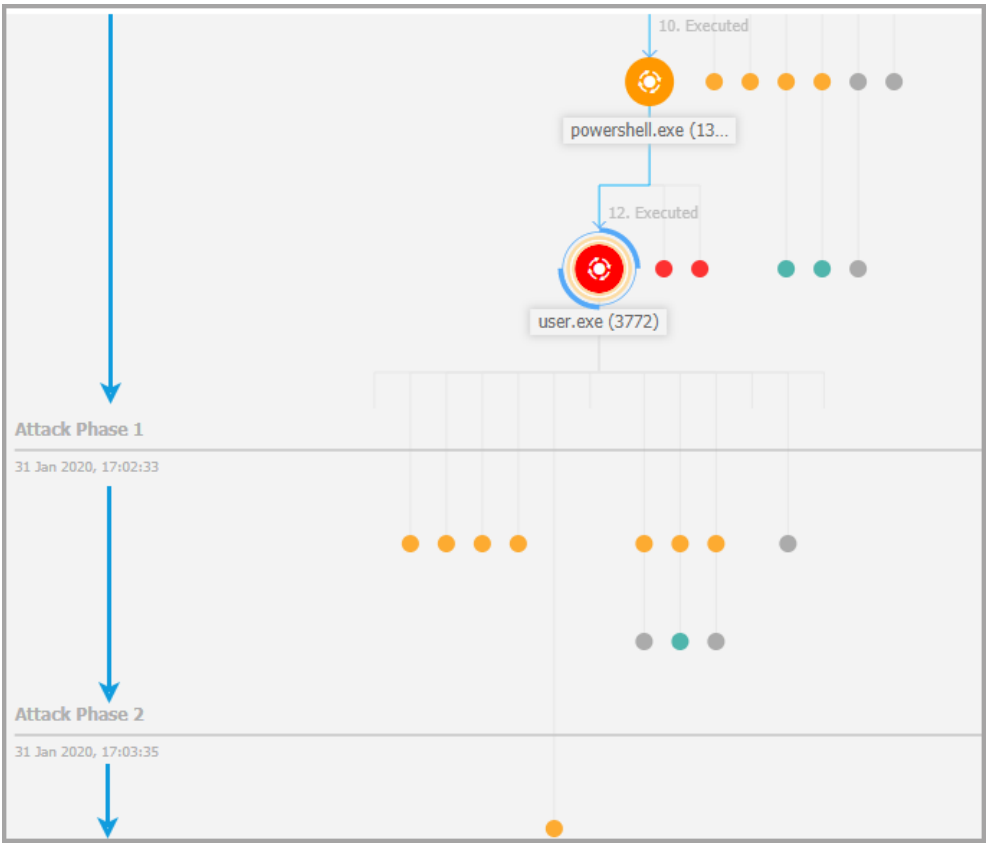
  - Nodurile în care s-a detectat o activitate suspectă nu vor fi adăugate în nodul cluster.
- La selectarea unui nod, vor fi afișate următoarele informații:
  - Calea către nodul endpoint-ului și celelalte elemente implicate vor fi evidențiate cu albastru.
  - Un panou lateral cu secțiuni extensibile, care oferă informații detaliate despre nodul selectat, alerte în cazul în care sunt declanșate detecții, acțiuni disponibile și recomandări. Pentru informații suplimentare, consultați „Detalii nod" (p. 442).
- Nodurile sunt conectate cu săgeți care indică cursul acțiunilor apărute pe endpoint în timpul incidentului. Fiecare rând este etichetat cu numele acțiunii și numărul cronologic.

Pot fi reprezentate ca noduri următoarele elemente ale unui incident:

Tipul de nod	Descriere
Stație de lucru	Afișează detalii despre endpoint și statusul modulului Patch Management.
Domeniu	Afișează informații despre domeniul gazdă și endpoint-urile acestuia.
Proces	Afișează detalii despre rolul procesului în incidentul curent, informații despre fișiere, detalii despre executările proceselor, prezența în rețea și opțiuni de investigație suplimentară.
Fișier	Afișează detalii despre rolul fișierelor în incidentul curent, informații despre fișiere, prezența în rețea și opțiuni de investigație suplimentară.
Regiștri	Afișează informații despre regiștri și detaliile procesului principal.

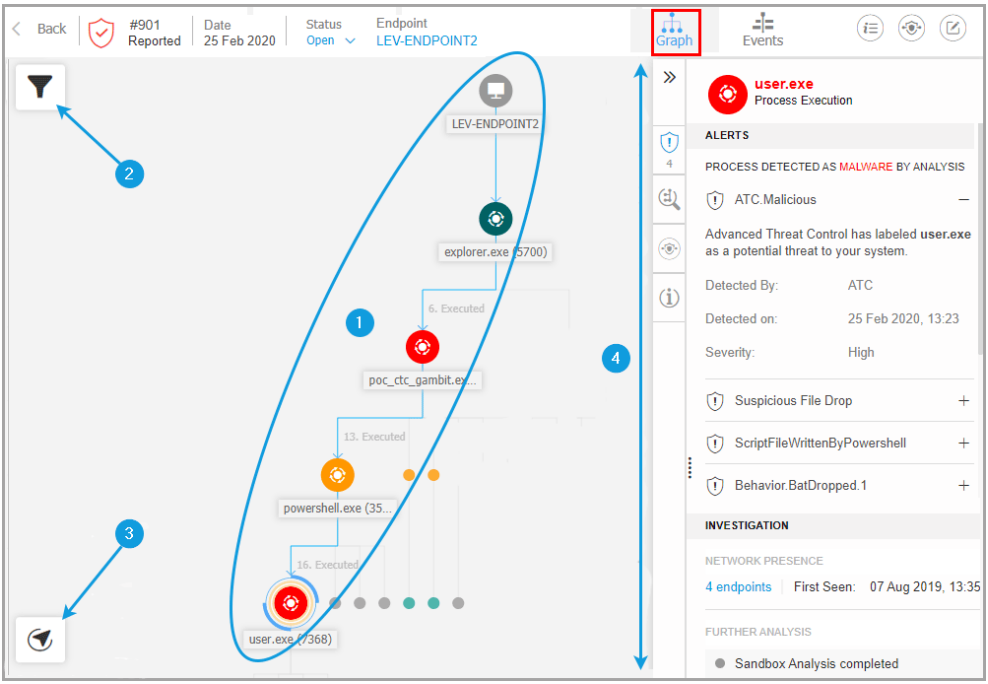
Diagramă

Fila **Grafic** oferă o reprezentare grafică interactivă a incidentului investigat și a contextului acestuia, evidențiind secvența de elemente implicate direct în declanșarea acestuia, cunoscute drept **Cale critică** a incidentului, precum și celelalte elemente implicate, care sunt estompate în mod implicit. În cazul incidentelor complexe care iau amploare în timp, graficul afișează fiecare etapă a atacului.



Atac de test

Fila Grafic include opțiuni de filtrare care permit personalizarea graficului incidentului pentru îmbunătățirea vizualizării, caracteristici de navigare a hărții incidentului și panouri de detalii cu informații suplimentare despre fiecare element.



Fila Grafic

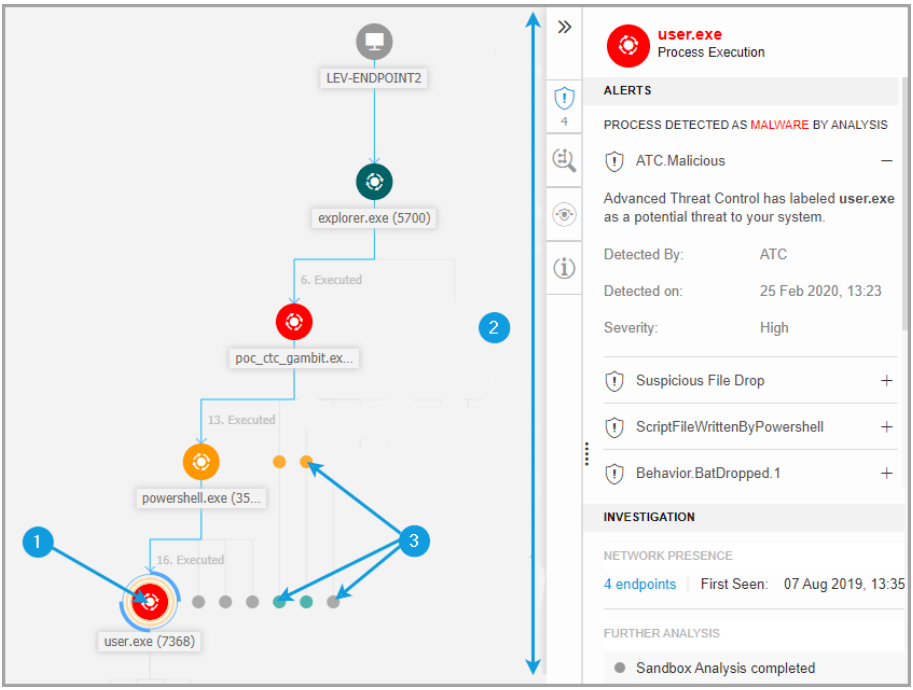
1. Cale critică
2. Meniul Filtre
3. Meniul Navigare
4. Panou detalii nod

Cale critică

Calea critică este o secvență de elemente de securitate conectate care au dus la declanșarea unei alerte, pornind de la punctul de intrare în rețea până la nodul de evenimente care au declanșat incidentul. Calea critică a incidentului este evidențiată implicit în grafic, împreună cu toate nodurile de evenimente care fac parte din aceasta, iar celelalte elemente sunt estompate.

Nodul declanșator se distinge ușor de restul elementelor graficului, fiind înconjurat de caracteristici suplimentare de evidențiere (două cercuri portocalii), iar un panou

de informații aferente este afișat implicit împreună cu graficul incidentului, oferind informații detaliate despre nodul declanșator.



Cale critică

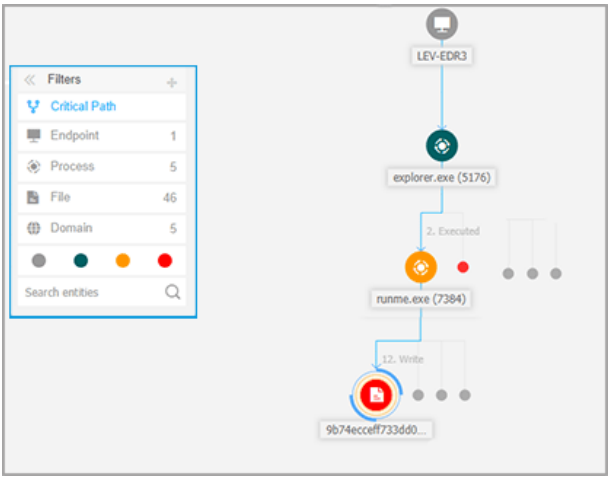
1. Nod declanșator
2. Panou cu detaliile nodurilor, cu informații grupate pe categorii și secțiuni care pot fi restrânse.
3. Noduri estompate implicate în mod indirect în incident

Notă
Dacă selectați un alt element în afară de nodul declanșator, calea critică va fi întreruptă, iar calea către punctul de origine va fi evidențiată, de la nodul selectat până la nodul endpoint-ului.

Filtre

Meniul **Filtre** oferă capabilități de filtrare îmbunătățite, permițând modificarea completă a graficului incidentului prin evidențierea elementelor în funcție de tipul sau relevanța lor ori prin ascunderea acestora pentru a face incidentul mai compact și mai ușor de analizat.

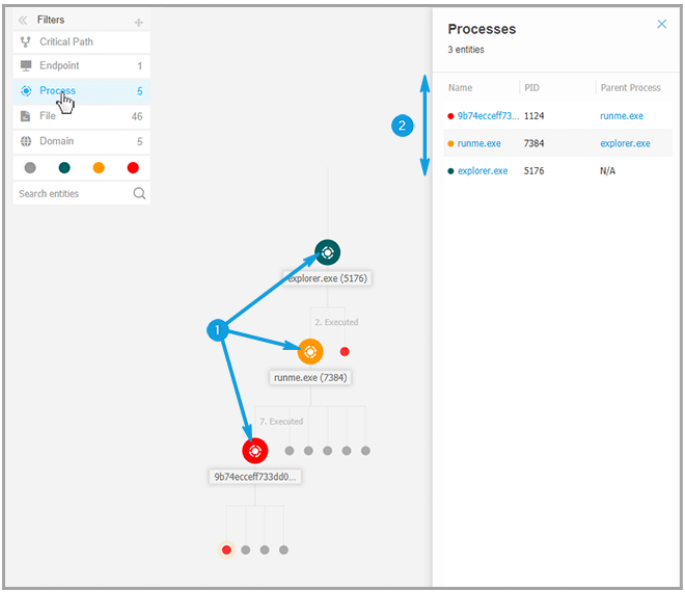
Apăsați și mențineți apăsat pe pictograma **Glisare** pentru a poziționa panoul de Filtre oriunde în interiorul graficului incidentului.



Filtre grafic de incident

Atunci când selectați un filtru pentru tipul de element:

1. Graficul de incident micșorează și evidențiază toate elementele care se încadrează în tipul selectat, în timp ce toate elementele de alte tipuri sunt estompate.
2. Deschide instantaneu un panou cu lista tuturor elementelor evidențiate.



Notă
Selectarea unui element din lista afișată va evidenția elementul respectiv în graficul incidentului și va deschide un panou cu detalii referitoare la acesta.
Nu pot fi aplicate simultan mai multe filtre.

Opțiunile de filtrare includ:

- **Cale critică**: Evidențiază calea critică a incidentului de compromitere.
- **Endpoint**: Evidențiază endpoint-urile afectate de incident.
- **Proces**: Evidențiază toate nodurile de tip proces implicate în incident.
- **Fișier**: Evidențiază toate nodurile de tip fișier implicate în incident.
- **Domeniu**: Evidențiază toate nodurile de tip domeniu implicate în incident.
- **Regiștri**: Evidențiază toate nodurile la nivel de regiștri implicate în incident.

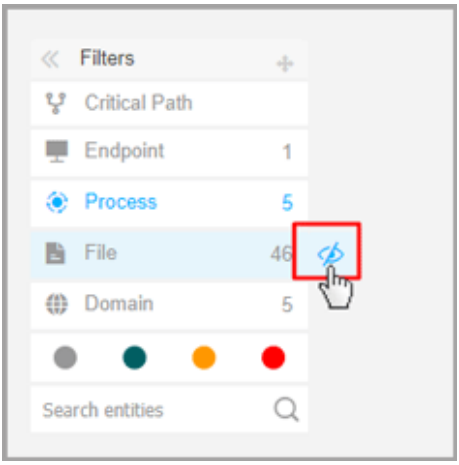
- **Relevanță element**: Puteți filtra elementele și după importanța în cadrul incidentului.
  - **Nod neutru**: Elemente care nu au un impact direct în incidentul de securitate.
  - **Nod important**: Elemente cu rol important în incidentul de securitate.
  - **Nod de origine**: Punctul de intrare a atacului în rețea.
  - **Nod suspect**: Elemente cu comportament suspect, implicate direct în incidentul de securitate.
  - **Nod periculos**: Elemente care au cauzat daune la nivelul rețelei dumneavoastră.

    Notă
    Dacă plasați cursorul deasupra oricărui filtru de culoare, va fi afișat numărul de incidente cu același grad de relevanță implicate în incident.

- **Căutare entități**: Puteți căuta numele sau extensiile de fișier ale componentelor incidentelor în câmpul de căutare, iar rezultatele vor fi afișate în panoul lateral.

Dacă nu este selectat niciun filtru, graficul incidentului va fi resetat la starea implicită, cu endpoint-ul, punctul de origine și elementele declanșatoare evidențiate și celelalte elemente estompate.

De asemenea, puteți ascunde anumite elemente din graficul incidentului făcând clic pe butonul **Afișare/Ascundere**, care va apărea atunci când plasați cursorul deasupra filtrelor de tipul: Fișier, Domeniu și Regiștri.



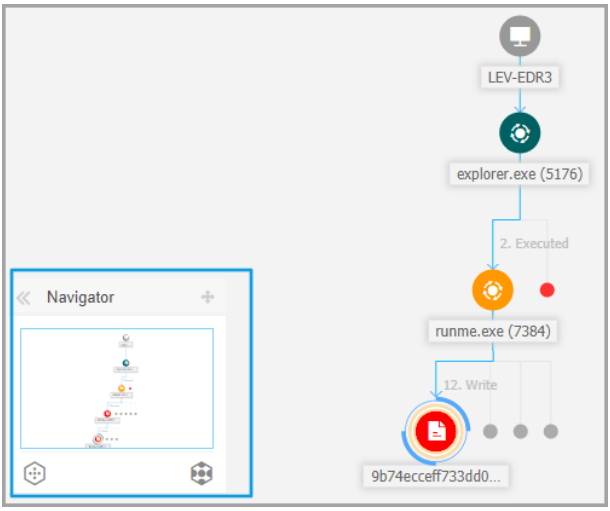
Ascunderea unui element reorganizează graficul incidentului, eliminând toate elementele corespunzătoare chiar dacă acestea sunt micșorate, cu excepția nodului declanșator și nodurilor cu elemente subordonate.

Navigator

Meniul de navigare vă permite să navigați rapid prin graficul incidentului și să explorați toate elementele afișate utilizând mini-harta și diferitele niveluri de vizualizare.

Apăsați și mențineți apăsat pe pictograma ✥ **Glisare** pentru a poziționa panoul de Navigare oriunde în interiorul graficului incidentului.

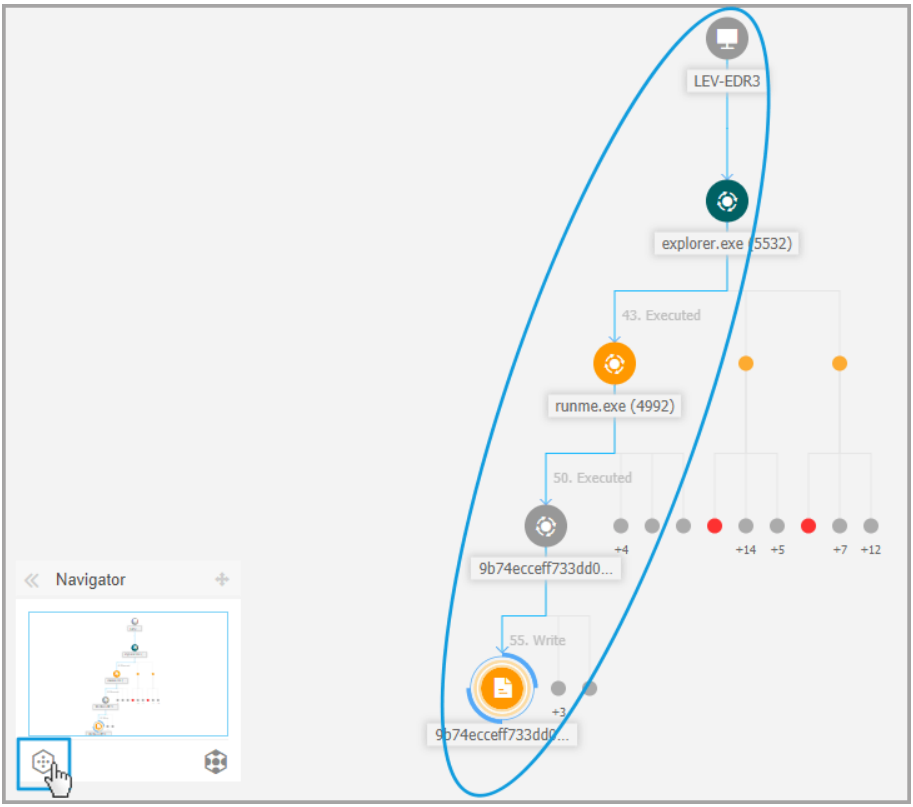
Meniul de navigare este restrâns în mod implicit. Atunci când îl extindeți, meniul va afișa o versiune în miniatură a întregii hărți de incidente și butoane de acțiuni pentru ajustarea nivelului de vizualizare.



Navigator

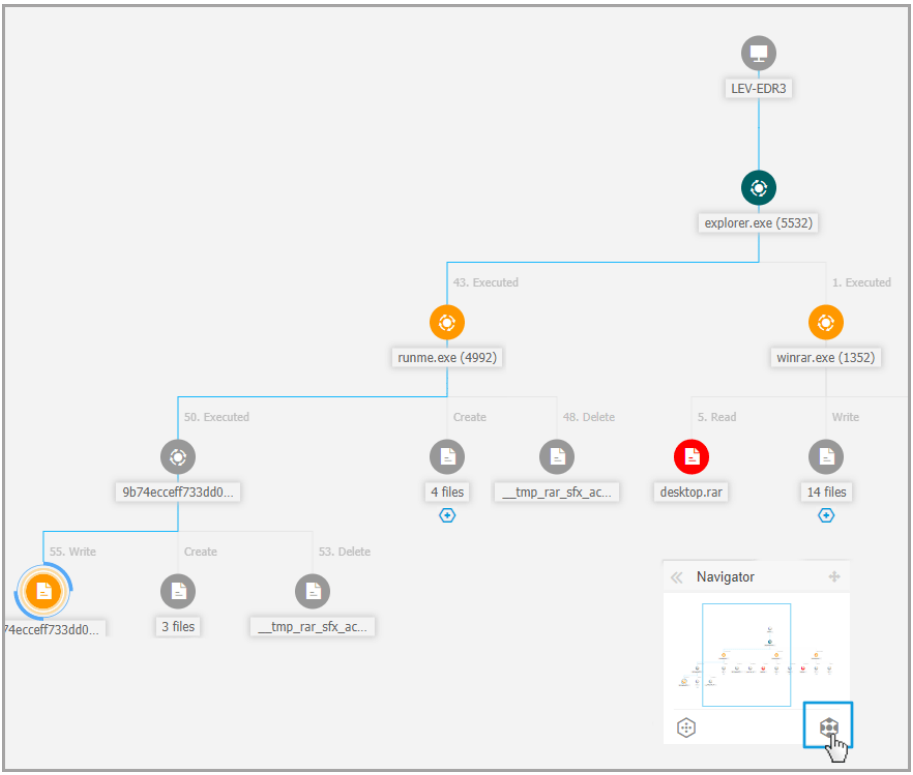
Meniul **Navigare** oferă două butoane de acțiuni pentru ajustarea modului de vizualizare a graficului incidentului: butonul **Mai puține detalii** și butonul **Mai multe detalii**.

Dacă selectați **Mai puține detalii**, graficul va fi resetat la starea implicită, evidențiind doar calea critică a incidentului.



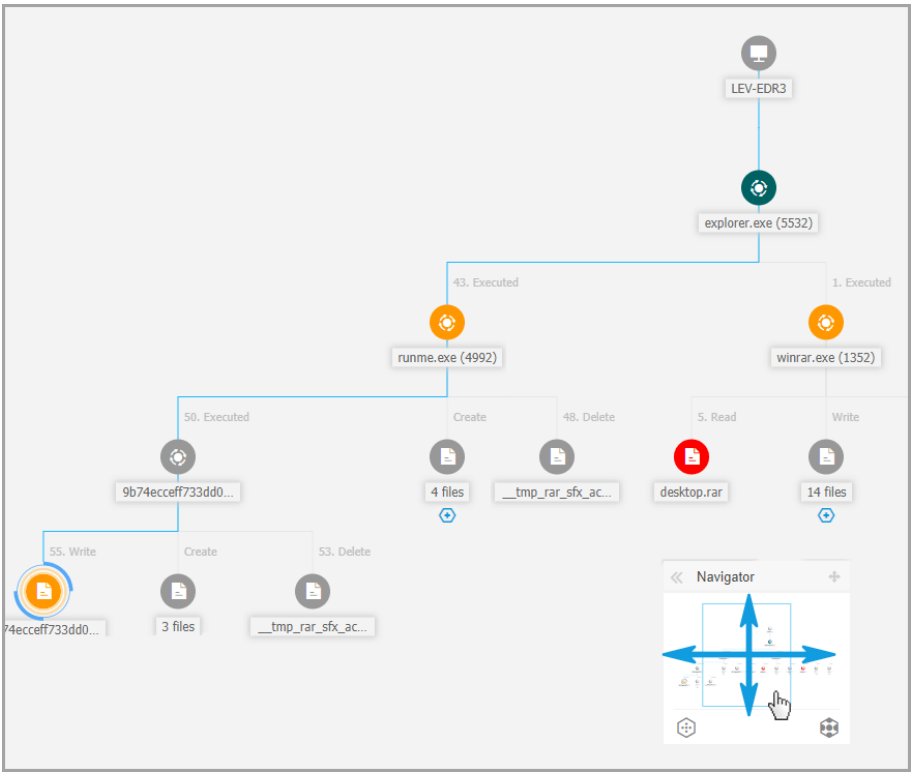
Vizualizare generală

Dacă selectați **Mai multe detalii**, se vor afișa în forma extinsă toate elementele graficului incidentului, evidențiind doar calea critică a incidentului.



Vizualizare mărită

Atunci când incidentul este mărit și toate elementele sunt evidențiate, este posibil ca graficul să se extindă adesea dincolo de limitele ecranului. În acest caz, apăsați și mențineți apăsat pe instrumentul de selectare a hărții din mini-harta de navigare pentru a glisa cu ușurință către zona de pe harta incidentului pe care doriți să o vizualizați, sau trageți simplu harta în direcția pe care doriți să o vizualizați.

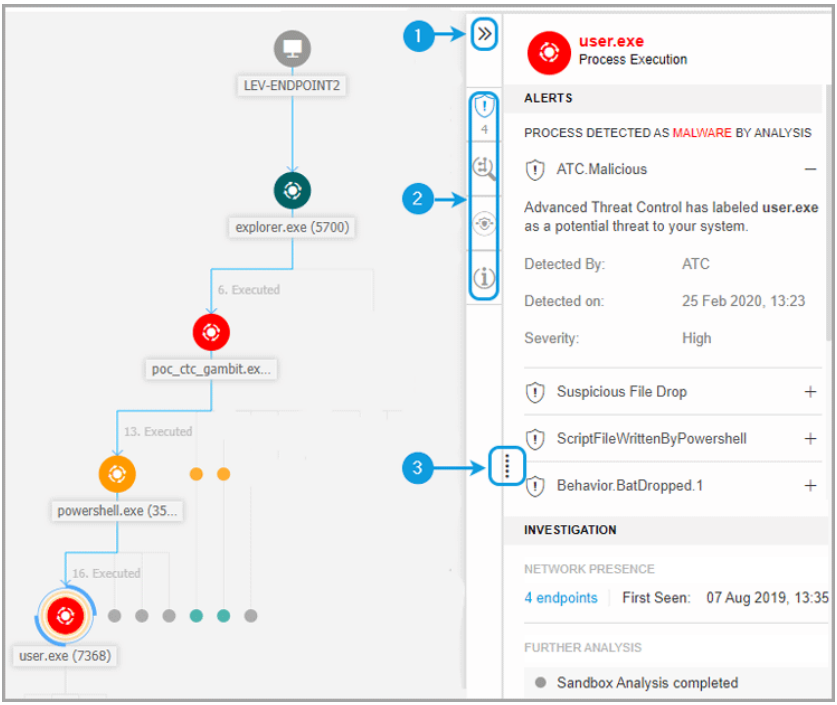


Instrument de selectare hartă în miniatură

Detalii nod

Panoul **Detalii nod** include secțiuni cu informații detaliate despre nodul selectat, inclusiv acțiuni de prevenire și remediere pe care le puteți întreprinde pentru a diminua consecințele incidentului, detalii despre tipul de detecție și alertele detectate în nod, prezența în rețea, detalii despre executarea proceselor, recomandări suplimentare pentru gestionarea evenimentului de securitate sau acțiuni pentru investigarea suplimentară a elementului.

Pentru a vizualiza aceste informații și pentru a putea acționa în interiorul panoului, selectați un nod de pe harta evenimentului de securitate.



Panou detalii nod

1. Puteți restrânge sau extinde panoul **Detalii nod** selectând butonul **Restrângere**.
2. Puteți naviga cu ușurință în pagina cu informațiile afișate în panoul **Detalii nod** selectând pictogramele fiecăreia dintre cele patru categorii principale:
   - **ALERTE**

     Această secțiune afișează una sau mai multe detecții declanșate pe nodul selectat, inclusiv detalii despre tehnologia Bitdefender care a inclus elementul în incident, motivul pentru care a fost declanșată detecția, numele detecției și data la care a fost detectat.
   - **INVESTIGARE**

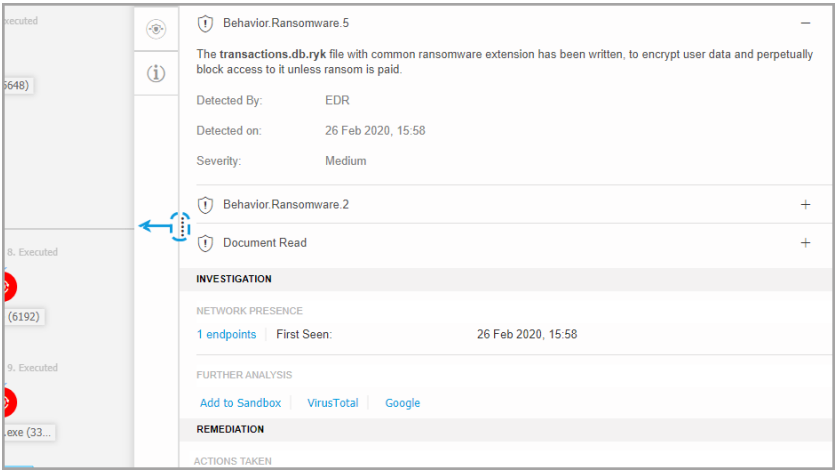
     Această secțiune afișează marcaje temporale pentru detecția inițială și toate endpoint-urile în care a fost identificat acest element.
   - **REMEDIERE**

Această secțiune afișează acțiunile întreprinse automat de GravityZone, acțiuni pe care dumneavoastră le puteți întreprinde imediat pentru a reduce amenințarea, precum și recomandări detaliate pentru fiecare alertă detectată pe nodul selectat, care să vă ajute să remediați incidentul și să creșteți nivelul de securitate al mediului dumneavoastră.

- **INFO**

  Această secțiune afișează informații generale despre fiecare fișier și informații specifice în funcție de tipul nodului selectat.

3. Puteți trage panoul **Detalii nod** spre centrul ecranului pentru a naviga cu ușurință conținutul acestuia.



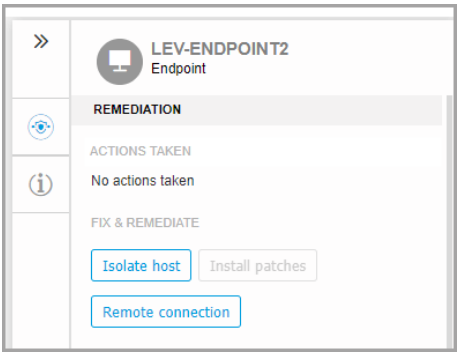
Panou extins

Panou cu detalii pentru nodurile endpoint-ului

Panoul **Detalii nod** pentru endpoint-uri include două categorii:

- **REMEDIERE**

  Afișează informații despre acțiunile întreprinse automat de GravityZone pentru a reduce amenințările și despre acțiunile pe care le puteți întreprinde:



– **Izolare gazdă** -Utilizați această soluție de remediere pentru a izola endpoint-ul de restul rețelei.

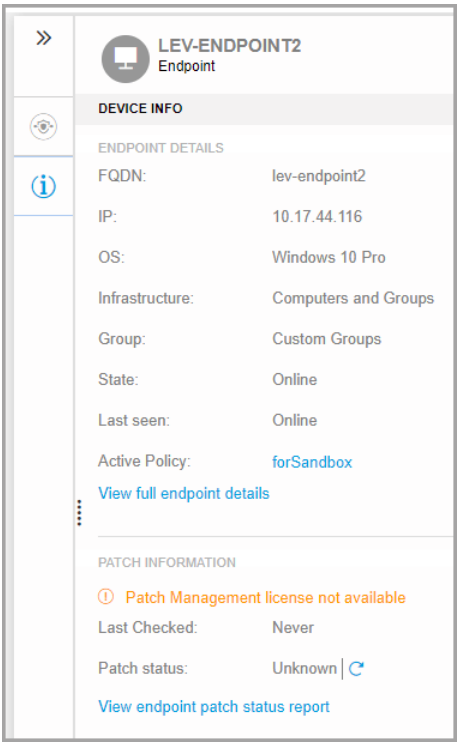
– **Instalare patch-uri** - Utilizați această acțiune pentru a instala un patch de securitate lipsă pe endpoint-ul țintă. Această opțiune este vizibilă numai cu modulul Patch Management, un add-on disponibil cu o cheie de licență separată. Pentru informații suplimentare, consultați secțiunea Instalare patch-uri.

– **Conexiune de la distanță** - Utilizați această acțiune pentru a stabili o conexiune de la distanță cu endpoint-ul implicat în incidentul curent și executa un număr de comenzi shell personalizate direct pe sistemul de operare al acestuia, pentru diminuarea instantanee a consecințelor amenințării sau colectarea de date pentru investigații suplimentare.

  Dacă selectați această opțiune, va fi afișată fereastra Conexiune de la distanță.

- **INFORMAȚII DISPOZITIV**

  Afișează informații despre endpoint-ul afectat, cum ar fi numele endpoint-ului, adresa IP, sistemul de operare, grupul de care aparține, starea, politicile active și un link care deschide o fereastră nouă în care sunt afișate detaliile complete ale endpoint-ului.



De asemenea, vă oferă informații cum ar fi numărul de patch-uri instalate, patch-urile nereușite sau orice patch lipsă, fie el de securitate sau nu. Suplimentar, puteți genera un raport de stare a patch-urilor pentru o stație de lucru. Această secțiune este furnizată la cerere pentru endpoint-ul țintă.

Puteți lua următoarele măsuri în cadrul panoului:

– Vizualizare informații patch pe stația de lucru țintă. Pentru a vizualiza detaliile patch-urilor, selectați **Reîmprospătare** din cadrul acestei secțiunii.

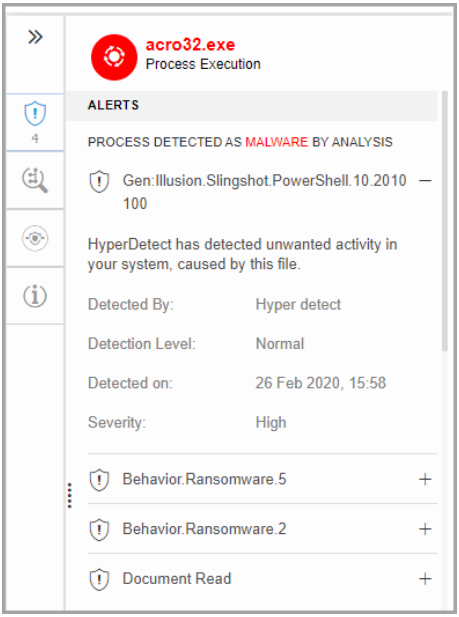
– Vizualizați raportul de stare pentru patch-uri pentru stația de lucru țintă. Pentru a genera raportul, efectuați clic pe **Vizualizare raport stare patch stație de lucru**.

Panou cu detalii pentru nodurile proceselor

Panoul **Detalii nod** pentru nodurile proceselor include patru categorii:

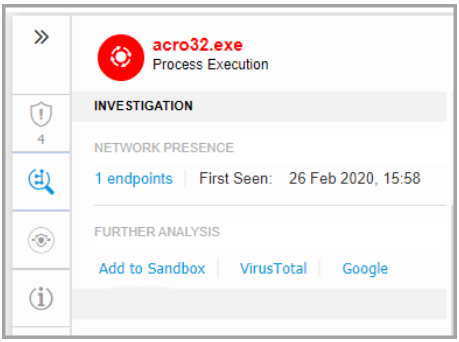
- **ALERTE**

  Afișează una sau mai multe detecții declanșate pe nodul selectat, inclusiv informații despre tehnologia Bitdefender care a inclus acest element în incident, motivul pentru care a fost declanșată detecția, numele detecției și data la care a fost detectată. Descrierea fiecărei alerte respectă cele mai recente standarde MITRE.

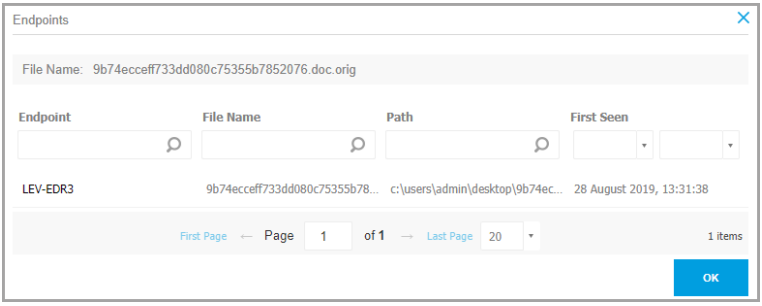


- **INVESTIGARE**

  Afișează marcaje temporale pentru detecția inițială și toate endpoint-urile în care a fost identificat acest element.



Pentru a vizualiza această listă, selectați numărul afișat în câmpul **endpoint-uri** și va apărea o nouă fereastră.

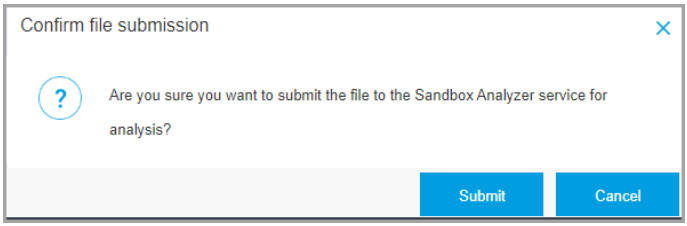


De asemenea, această secțiune oferă o analiză externă prin componentele interne și soluțiile terților.

Următoarele acțiuni sunt disponibile:

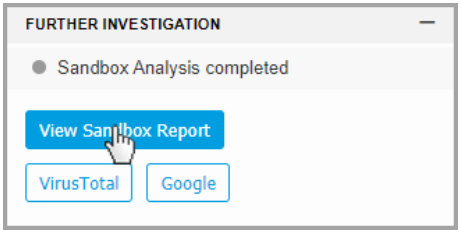
– **Adăugare în Sandbox** - Utilizați această acțiune pentru a genera un raport Sandbox Analyzer.

  Dacă alegeți **Adăugare în Sandbox**, vi se va solicita să confirmați transmiterea fișierului.



După confirmare, sunteți redirecționat automat către ecranul de transmitere.

Atunci când analiza este completă, selectați **Vizualizare raport sandbox** pentru a deschide raportul complet.

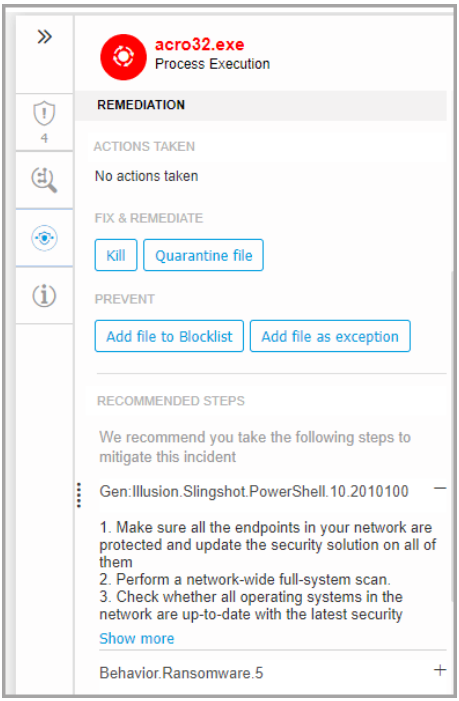


– **VirusTotal** - Utilizați această acțiune pentru a trimite un fișier pentru analiză externă.

– **Google** - Utilizați această acțiune pentru a căuta codul hash a unui fișier.

- **REMEDIERE**

  Afișează informații despre acțiunile întreprinse automat de GravityZone pentru a reduce amenințările și despre acțiunile pe care le puteți întreprinde:



– **Oprire** - Utilizați această acțiune pentru a opri executarea unui proces. Această acțiune creează un proces de distrugere vizibil în bara de execuție a proceselor. `Procesele System32` și cele ale Bitdefender sunt excluse de la această acțiune.

– **Fișier carantină** - Utilizați această acțiune pentru a stoca elementul în cauză și a-l împiedica să-și execute playload-ul. Această acțiune necesită ca modului Firewall să fie instalat pe endpoint-ul țintă.

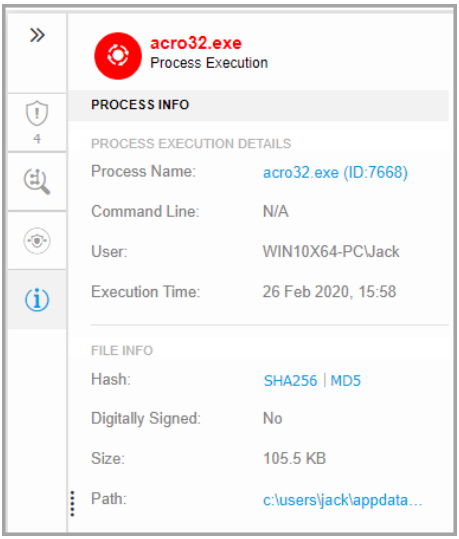
– **Adăugare fișier în lista de blocare** - Gestionați elementele blocate în secțiunea Listă de blocare.

– **Adăugare fișier ca excepție** - Utilizați această acțiune pentru a exclude activitățile legitime dintr-o anumită politică Atunci când alegeți această acțiune, o fereastră de configurare vă va solicita să selectați politica în care doriți să adăugați excepția. Administrați excepția accesând **Politici > Antimalware > Setări**.

De asemenea, această secțiune oferă și recomandări detaliate pentru fiecare alertă detectată pe nodul selectat pentru a vă ajuta să diminuați consecințele incidentului și să creșteți nivelul de securitate al mediului dumneavoastră.

- **INFORMAȚII PROCESE**

  Afișează detalii despre nodul selectat al procesului, inclusiv numele procesului, linia de comandă executată, utilizatorul, momentul executării, originea și calea fișierului, codul hash sau semnătura digitală.



  Puteți copia codul hash în clipboard selectând algoritmii de hashing disponibili în câmpul **Hash** și apoi selectând **Copiere în clipboard** și puteți utiliza această acțiune pentru a adăuga codul hash al unui fișier pe o **Listă de blocare**. Pentru informații suplimentare, consultați secțiunea **Fișiere liste blocare**.

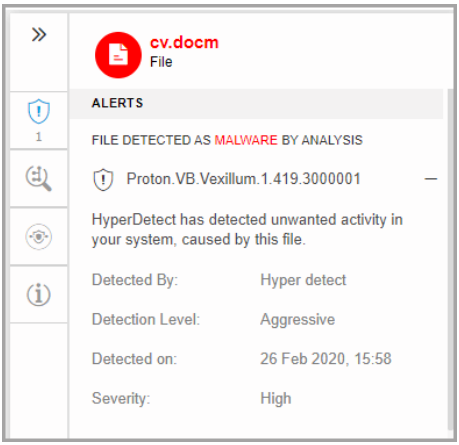
Panou cu detalii pentru nodurile fișierelor

Panoul **Detalii nod** pentru nodurile fișierelor include patru categorii:

- **ALERTE**

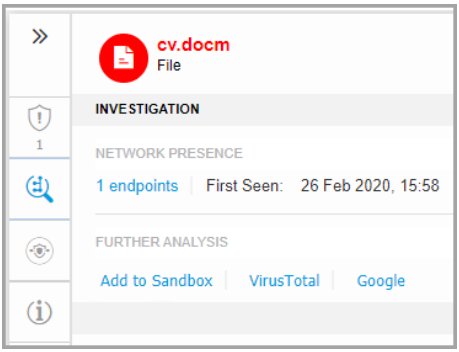
  Afișează una sau mai multe detecții declanșate pe nodul selectat, inclusiv informații despre tehnologia Bitdefender care a inclus acest element în incident, motivul pentru care a fost declanșată detecția, numele detecției și data la care

a fost detectată. Descrierea fiecărei alerte respectă cele mai recente standarde MITRE.

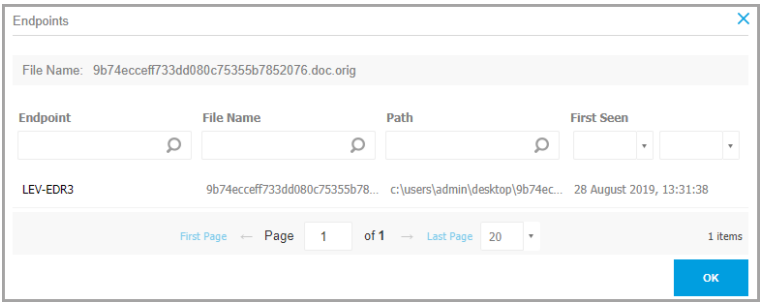


- **INVESTIGARE**

  Afișează marcaje temporale pentru detecția inițială și toate endpoint-urile în care a fost identificat acest element.



Pentru a vizualiza această listă, selectați numărul afișat în câmpul **endpoint-uri** și va apărea o nouă fereastră.

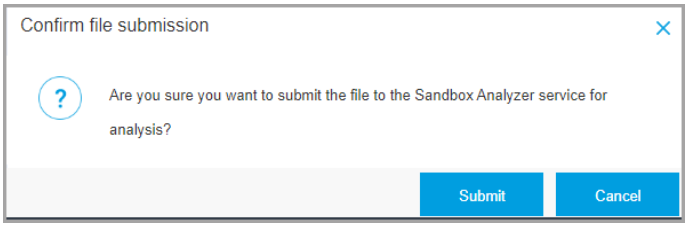


De asemenea, această secțiune oferă o analiză externă prin componentele interne și soluțiile terților.

Următoarele acțiuni sunt disponibile:

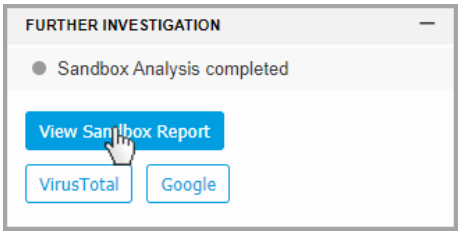
– **Adăugare în Sandbox** - Utilizați această acțiune pentru a genera un raport Sandbox Analyzer.

  Dacă alegeți **Adăugare în Sandbox**, vi se va solicita să confirmați transmiterea fișierului.



  După confirmare, sunteți redirecționat automat către ecranul de transmitere.

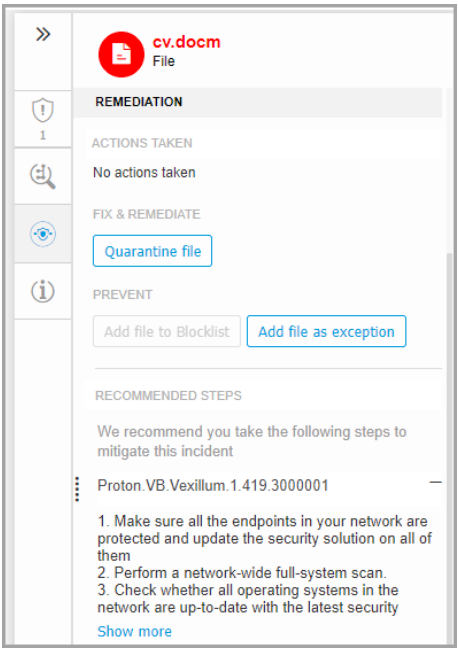
  Atunci când analiza este completă, selectați **Vizualizare raport sandbox** pentru a deschide raportul complet.



  - **VirusTotal** - Utilizați această acțiune pentru a trimite un fișier pentru analiză externă.
  - **Google** - Utilizați această acțiune pentru a căuta codul hash a unui fișier.

- **REMEDIERE**

  Afișează informații despre acțiunile întreprinse automat de GravityZone pentru a reduce amenințările și despre acțiunile pe care le puteți întreprinde:



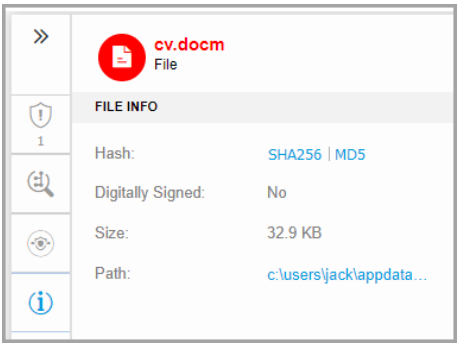
– **Adăugare fișier în lista de blocare** - Gestionați elementele blocate în secțiunea Listă de blocare.

– **Adăugare fișier ca excepție** - Utilizați această acțiune pentru a exclude activitățile legitime dintr-o anumită politică Atunci când alegeți această acțiune, o fereastră de configurare vă va solicita să selectați politica în care doriți să adăugați excepția. Administrați excepția accesând **Politici > Antimalware > Setări**.

De asemenea, această secțiune oferă și recomandări detaliate pentru fiecare alertă detectată pe nodul selectat pentru a vă ajuta să diminuați consecințele incidentului și să creșteți nivelul de securitate al mediului dumneavoastră.

- **INFORMAȚII FIȘIER**

  Afișează detaliile despre nodul selectat al fișierului, inclusiv originea și calea fișierului, codul hash sau semnătura digitală.



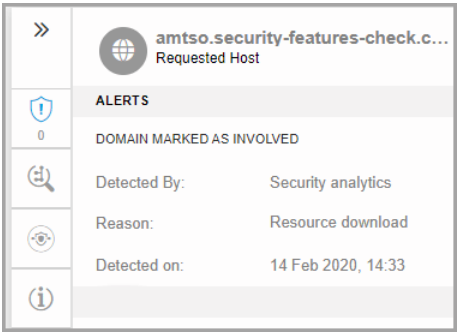
Puteți copia codul hash în clipboard selectând algoritmii de hashing disponibili în câmpul **Hash** și apoi selectând **Copiere în clipboard** și puteți utiliza această acțiune pentru a adăuga codul hash al unui fișier pe o **Listă de blocare**. Pentru informații suplimentare, consultați secțiunea **Fișiere liste blocare**.

Panou cu detalii pentru nodurile domeniilor

Panoul **Detalii nod** pentru nodurile domeniilor include patru categorii:

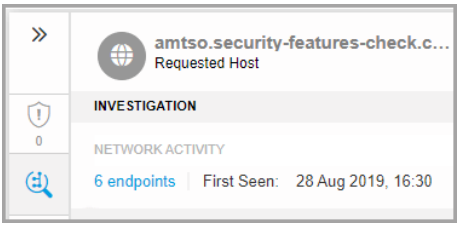
- **ALERTE**

  Afișează gradul de severitate al domeniului, după cum a fost marcat de tehnologia Bitdefender care a inclus acest element în incident, motivul pentru care a fost declanșată detecția și data la care a fost detectat.

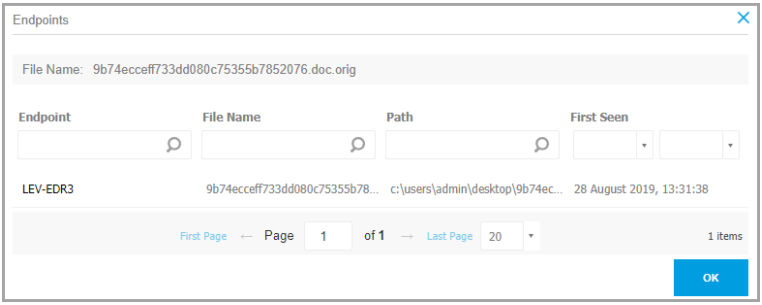


- **INVESTIGARE**

Afișează marcaje temporale pentru detecția inițială și toate endpoint-urile în care a fost identificat acest element.

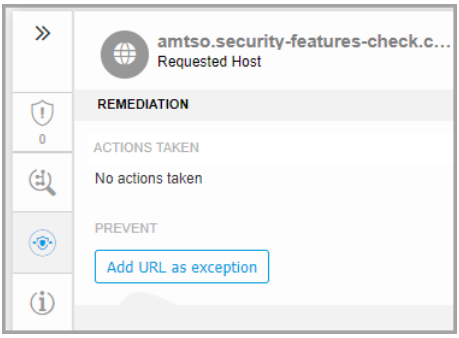


Pentru a vizualiza această listă, selectați numărul afișat în câmpul **endpoint-uri** și va apărea o nouă fereastră.



- **REMEDIERE**

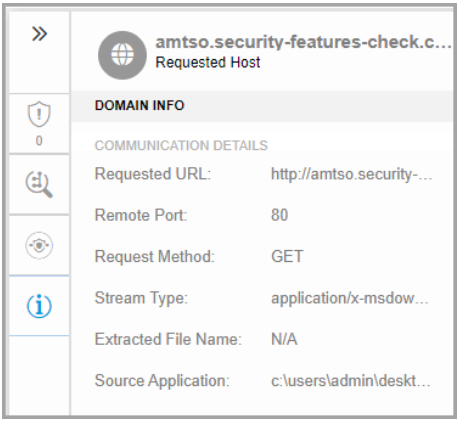
  Afișează informații despre acțiunile întreprinse automat de GravityZone pentru a reduce amenințările și despre acțiunile pe care le puteți întreprinde:



– **Adăugare URL ca excepție** - Utilizați această acțiune pentru a exclude activitățile legitime dintr-o anumită politică. Atunci când alegeți această acțiune, o fereastră de configurare vă va solicita să selectați politica în care doriți să adăugați excepția. Administrați excepția accesând **Politici > Antimalware > Setări**.

- **INFORMAȚII DOMENIU**

  Afișează detalii despre nodul selectat al domeniului, inclusiv URL-ul solicitat, portul utilizat, metoda de solicitare, tipul de flux, numele fișierului extras, aplicația sursă.

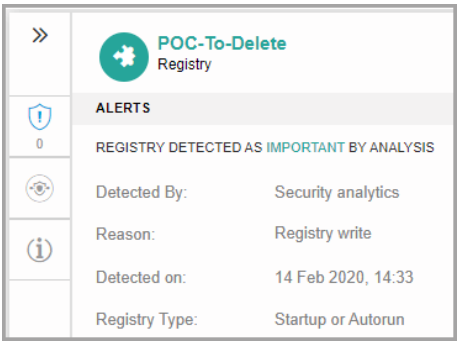


Panou cu detalii pentru nodurile regiștrilor

Panoul **Detalii nod** pentru nodurile regiștrilor include trei categorii:

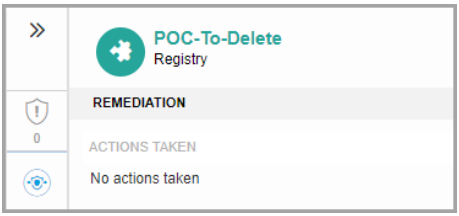
- **ALERTE**

  Afișează gradul de severitate al manipulării registrului, după cum a fost marcat de tehnologia Bitdefender care a inclus acest element în incident, motivul pentru care a fost declanșată detecția, data la care a fost detectat și tipul de registru.



- **REMEDIERE**

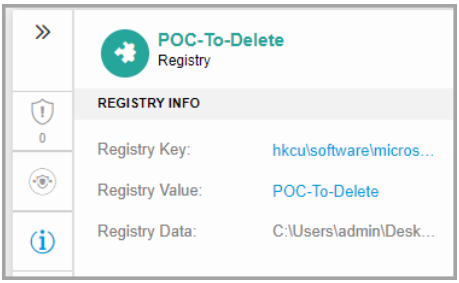
  Afișează informații despre acțiunile întreprinse automat de GravityZone.



  Secțiunea **REMEDIERE** pentru nodurile regiștrilor nu oferă nicio opțiune de acțiune directă a utilizatorului.

- **INFORMAȚII REGIȘTRI**

  Afișează detalii despre nodul selectat al regiștrilor, inclusiv cheia de regiștri, valoarea și datele.

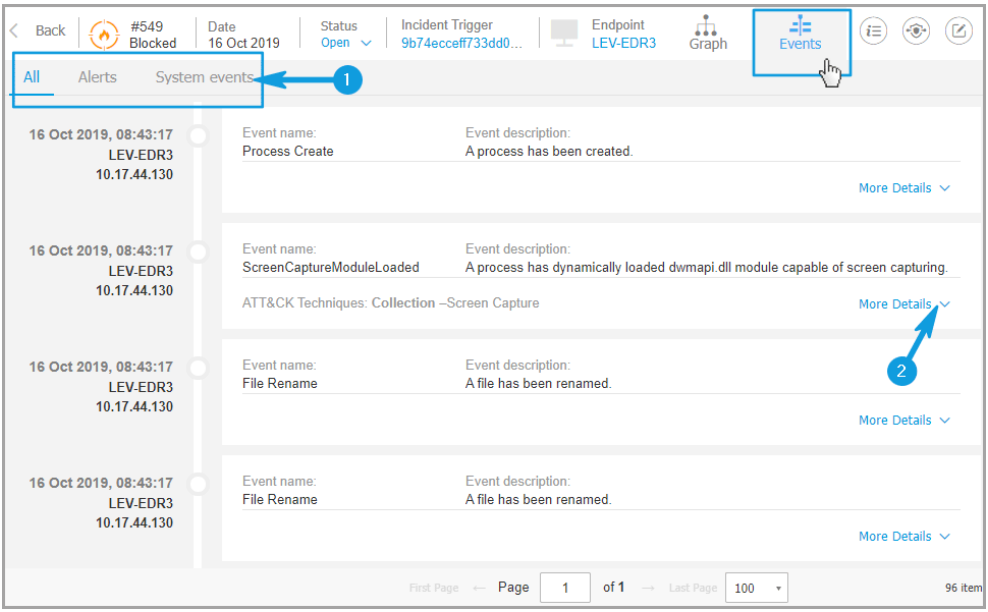


Puteți selecta cheia de regiștri și valoarea și le puteți copia în clipboard, pentru a fi analizate pe viitor.

Evenimente

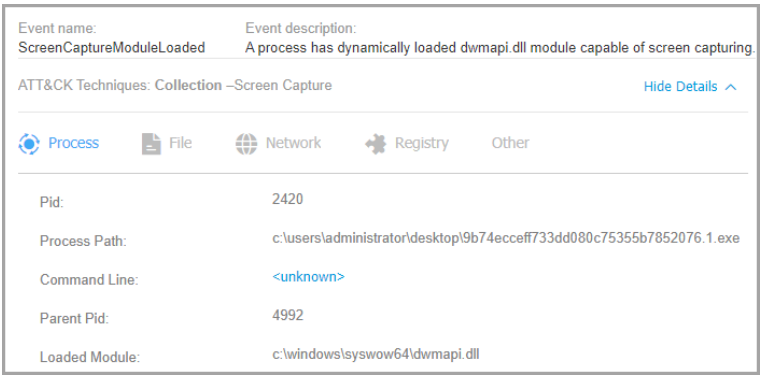
Utilizați fila **Evenimente** pentru a vizualiza modul în care s-a desfășurat secvența de evenimente și cum a dus la declanșarea incidentului investigat în prezent. Această fereastră afișează evenimentele corelate din sistem și alertele detectate de tehnologiile GravityZone, cum ar fi Network Attack Defense, Detecția anomaliilor, Anti-exploit avansat, Interfața de scanare antimalware (AMSI, Antimalware Scan Interface) Windows.

Fiecare eveniment complex dispune de o descriere detaliată care explică ceea ce s-a detectat și ce se poate întâmpla dacă elementul este utilizat în scopuri periculoase, conform ultimelor tehnici și tactici MITRE.



Fila Evenimente

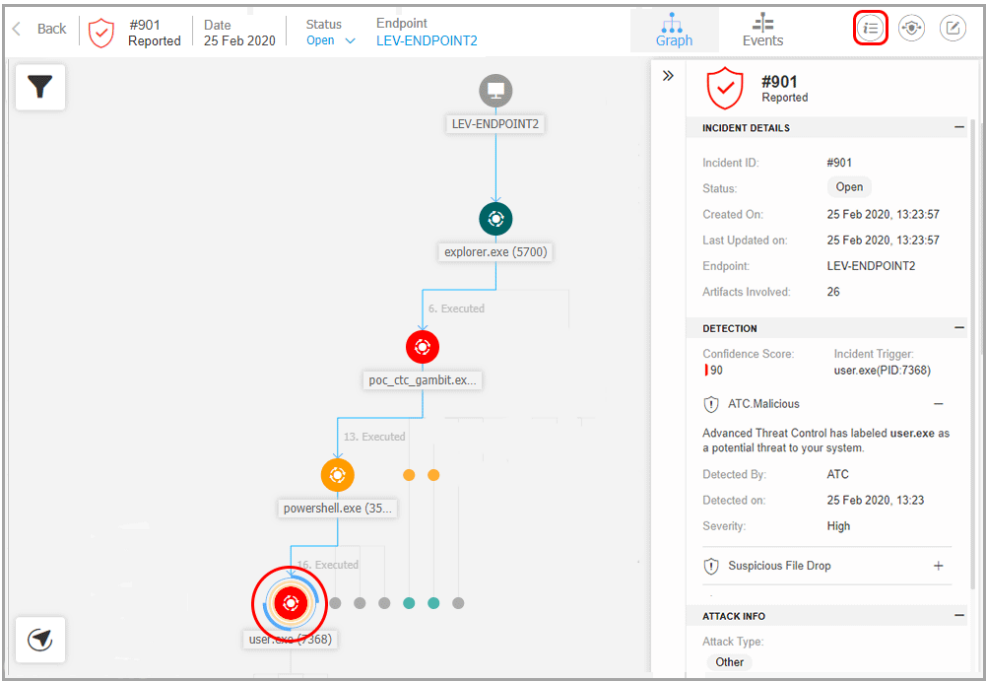
1. Utilizați opțiunile de filtrare pentru a afișa toate evenimentele sau fie doar evenimentele din sistem, fie pe cele complexe (alerte).
2. Selectați opțiunea **Mai multe detalii** pentru a extinde fiecare eveniment și a avea acces la informații suplimentare.



Informații incident

Acest panou conține secțiuni care pot fi restrânse cu detalii cum ar fi ID-ul incidentului, starea curentă, data și ora la care a fost creat și actualizat ultima dată, numărul de elemente implicate, numele și descrierea declanșatorului și informații referitoare la atac.

Din această secțiune puteți accesa incidentul extins, care cuprinde și incidentul de la nivelul endpoint-ului, după caz.

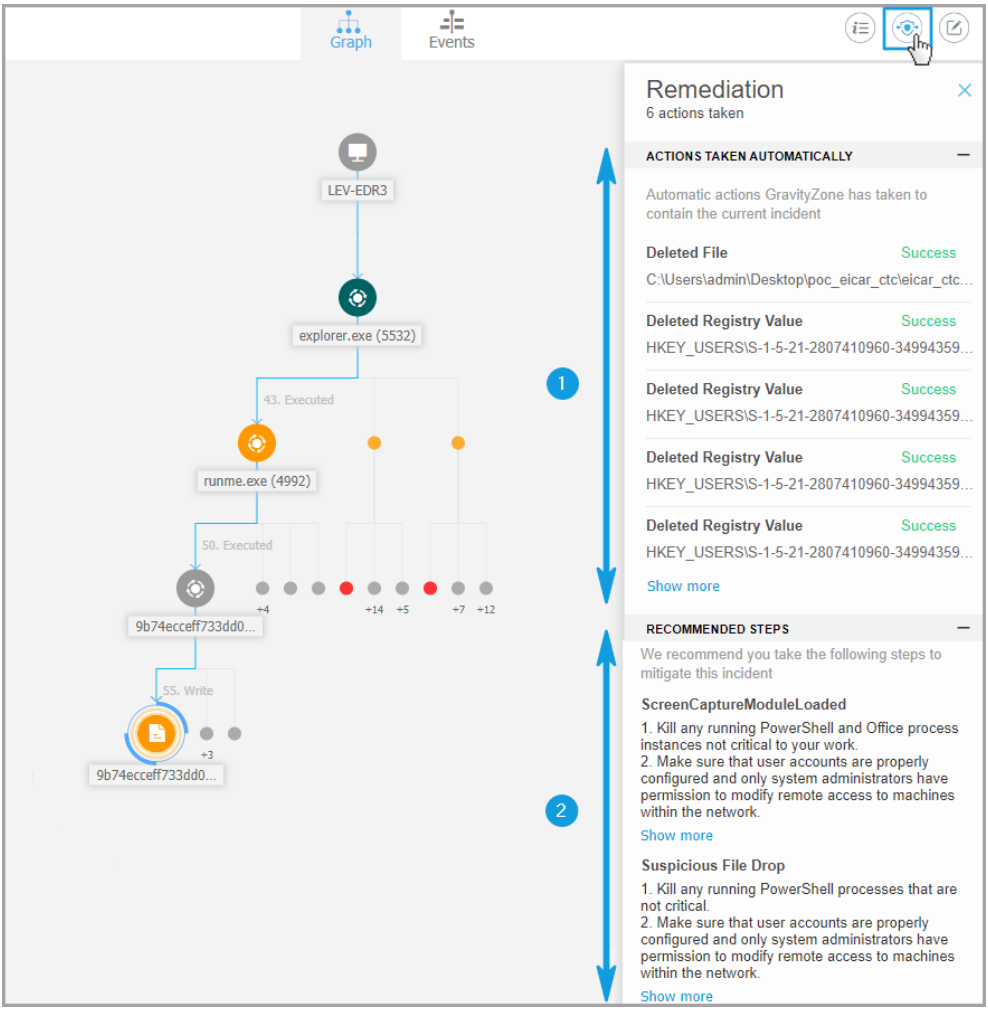


Panou Informații incident

Panoul include, de asemenea, alertele detectate pe elementul care a declanșat incidentul.

Remediere

Panoul **Remediere** vă oferă informații detaliate despre acțiunile de remediere întreprinse automat de GravityZone în cazul atacurilor blocate de tehnologii precum Advanced Threat Control (ATC), HyperDetect, Antimalware, precum și pașii recomandați pe care îi puteți urma pentru a diminua consecințele incidentului și crește nivelul de securitate al sistemului dumneavoastră.



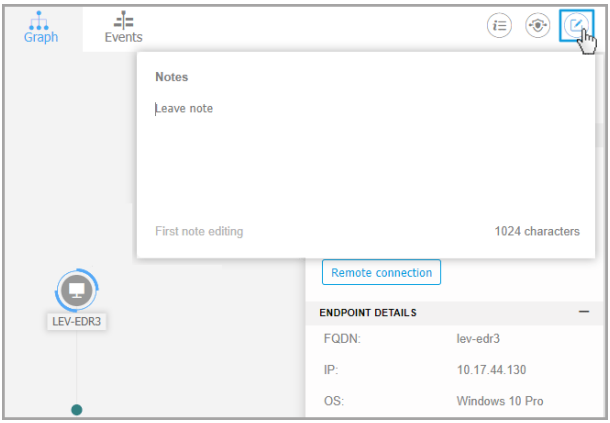
Panou Remediere

1. Acțiuni întreprinse automat de GravityZone.
2. Recomandări pentru continuarea diminuării consecințelor incidentului și sporirea securității.

Notă
Pașii recomandați corespund cu alertele detectate pe nodul care a declanșat incidentul investigat.

Note

Secțiunea **Note** vă permite să adăugați note pentru a urmări modificările recente și simplifica schimbarea responsabilul de incident.

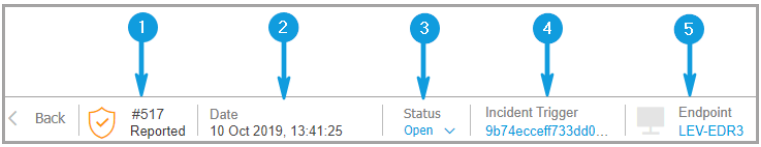


Clipboard note

1. Pentru a introduce un comentariu referitor la evenimentul curent, accesați butonul **Note** pentru a afișa o nouă fereastră.
2. Introduceți mesajul dumneavoastră în această fereastră (maxim 2048 de caractere).

Bară de stare incident

Bara de stare a incidentului oferă tag-uri de evenimente de securitate care vă pot ajuta să detectați informații cheie despre endpoint-urile din rețea implicate.



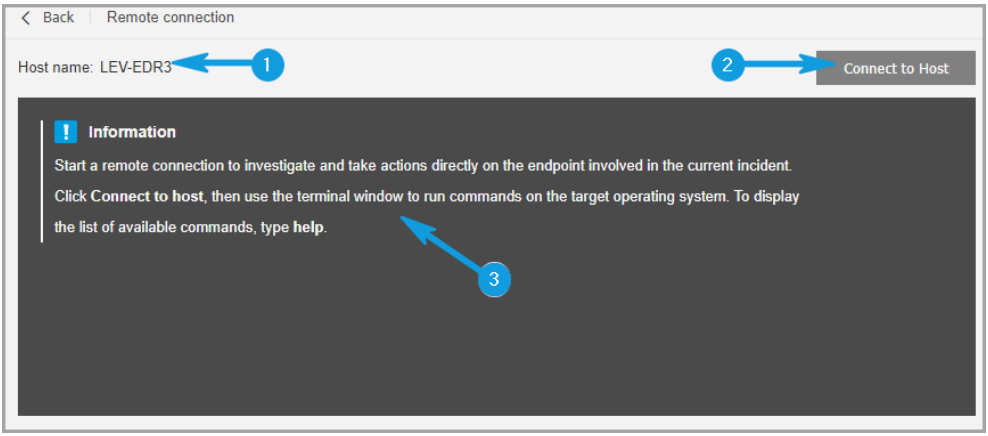
Bară de stare incident

1. ID incident - ID-ul incidentului investigat și dacă este blocat sau doar raportat.
2. Marcaj temporal detecție - data și ora la care incidentul a fost declanșat.
3. Status incident - statusul curent al incidentului.
4. Declanșator incident - numele elementului care a generat incidentul.
5. Endpoint - numele endpoint-ului țintă.

La selectarea opțiunii **Înapoi**, veți reveni în pagina principală **Incidente**.

Conexiune de la distanță

Utilizați această filă pentru a stabili o conexiune de la distanță cu endpoint-ul implicat în incidentul curent și a executa o serie de comenzi shell personalizate direct pe sistemul de operare al acestuia, pentru blocarea instantanee a amenințării sau colectarea de date pentru investigații suplimentare.



Fila Conexiune la distanță

Fila **Conexiune la distanță** include următoarele elemente:

1. Denumirea stației de lucru implicată în evenimentul de securitate actual
2. Butonul care controlează conexiunea la distanță (conectare / deconectare)
3. Fereastra terminal

Cerințe preliminare sesiune terminal

- Versiunea agentului Bitdefender instalat pe stația de lucru acceptă funcția Conexiune la distanță.
- Stația de lucru trebuie pornită și online.
- Stațai de lucru trebuie să aibă sistem de operare Windows.
- GravityZone poate comunica cu stația de lucru.
- Contul dumneavoastră GravityZone trebuie să aibă permisiuni de administrare pentru stația de lucru țintă.

Crearea unei Conexiuni la distanță

Iată cum funcționează o conexiune la distanță:

1. Începeți sesiunea în direct printr-un clic pe butonul **Conectare la gazdă**.

   Starea conexiunii va fi afișată lângă denumirea stației de lucru.

   În cazul în care conexiunea eșuează, va fi afișat un mesaj de eroare în fereastra terminal.

   Notă
   Puteți deschide maxim cinci sesiuni de terminal simultan pe aceeași stație de lucru.

2. O dată conectat, terminalul afișează lista comenzilor disponibile și descrierea acestora. Introduceți comanda dorită în fereastra terminal și apoi apăsați `Enter`.

   Pentru a afla mai multe despre o comandă, tastați `help` urmat de denumirea comenzii (de exemplu, `help ps`).

3. Terminalul afișează rezultatul comenzii, atunci când comanda a fost realizată cu succes.

În cazul în care stația de lucru nu finalizează execuția comenzii, comanda va fi anulată.

Istoricul comenzilor este înregistrat în fereastra terminal. Cu toate acestea, puteți vizualiza comenzile introduse anterior prin apăsarea tastelor săgeată.

4. Pentru a finaliza conexiunea, faceți clic pe butonul **Finalizare sesiune**.

   Sesiunea terminal expiră automat după cinci minute de inactivitate.

   Navigarea în afara filei **Conexiune la distanță** în timp ce sunteți conectat la o stație de lucru va termina de asemenea și sesiunea terminal.

Comenzi sesiune terminal

Comenzile sesiunii terminal EDR sunt comenzi shell personalizate, independente de platformă, care utilizează o sintaxă generică. Puteți găsi în cele ce urmează lista comenzilor disponibile pe care le puteți utiliza pe stațiile de lucru prin intermediul sesiunii terminal:

- `ps`
  - **Descriere**: Afișează informații despre procesele care rulează în acest moment pe stația de lucru țintă, cum ar fi ID de proces (PID), denumire, cale sau utilizare memorie.
  - **Sintaxă**: `ps`
  - **Alias**: `tasklist`
  - **Parametri**: -
- `kill`
  - **Descriere**: Termină un proces sau o aplicație care rulează pe stația de lucru țintă prin PID. Utilizați comanda `ps/tasklist` pentru a obține PID.
  - **Sintaxă**: `kill [PID]`
  - **Alias**: -
  - **Parametri**: `[PID]` - ID-ul unui proces de pe stația de lucru țintă.
- `ls (dir)`
  - **Descriere**: Afișează informații despre toate fișierele și folderele din directorul specificat, cum ar fi denumire, tip, denumire și data modificării. Permite specificarea căii folosind metacaractere. De exemplu:

`C:\Users\admin\Desktop\s*` tot conținutul folderului Desktop care începe cu "s"

`C:\Users\publ??` enumeră tot conținutul de pe calea specificată, cu cel puțin două litere.

- **Sintaxă**: `ls [path]`
- **Alias**: `dir`
- **Parametri**: `[Path]` - calea spre un fișier sau folder de pe stația de lucru țintă.

- `rm (del, delete)`
  - **Descriere**: Șterge fișiere și foldere de pe calea specificată pe stația de lucru țintă.
  - **Sintaxă**: `rm [path]`
  - **Alias**: `del/delete`
  - **Parametri**: `[Path]` - calea spre un fișier sau folder de pe stația de lucru țintă.
- `reg query`
  - **Descriere**: Returnează toate informațiile (denumire, tip și valoare) pentru calea specificată a cheii de regiștri.
  - **Sintaxă**: `reg query [keypath] [/k] [keyname] [/v] [valuename]`
  - **Alias**: -
  - **Parametri**:
    - `keypath`- returnează toate informațiile cheilor de regiștri aferente căii specificate.
    - `/k [keyname]` - filtrează rezultatele aferente cheilor de regiștri în funcție de o denumire specifică a cheii. Puteți filtra rezultatele și cu ajutorul metacaracteror (*, ?) în cazul unei game mai largi de denumiri.
    - `/v [valuename]` - filtrează valorile regiștrilor în funcție de o denumire specifică a valorii. Puteți utiliza de asemenea metacaractere (*, ?) în denumirea valorii pentru a filtra o gamă mai largă de denumiri.

- `reg add`
  - **Descriere**: Adaugă o nouă cheie sau valoare de regiștri. Suprascrie o valoare de regiștri dacă aceasta există deja. La suprascrierea informațiilor de regiștri, este necesar să specificați toți parametrii definiți.
  - **Sintaxă**: `reg add [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`
  - **Alias**: -
  - **Parametri**:
    - `[keyname]` - denumirea cheii de regiștri.
    - `/v [valuename]` - denumirea valorii registrului. Necesită, de asemenea, adăugarea cel puțin a parametrului /d [data].
    - `/t [datatype]` - tipul de date al valorii registrului. Puteți adăuga unul dintre următoarele tipuri de date:

      `REG_SZ, REG_MULTI_SZ, REG_DWORD, REG_BINARY, REG_DWORD_LITTLE_ENDIAN, REG_LINK, REG_FULL_RESOURCE_DESCRIPTOR, REG_EXPAND_SZ`

      În cazul în care nu este specificat, tipul `REG_SZ` este atribuit în mod implicit.

      Când tipul este setat pe `REG_BINARY`, datele de regiștri sunt interpretate ca valori hexadecimale.
- `ştergere registru`
  - **Descriere**: Șterge o cheie de registru sau valorile sale.
  - **Sintaxă**:

    `ştergere [keyname] [/v] [valuename] registru`

    `ştergere [keyname] [/va] reg`
  - **Alias**: -
  - **Parametri**:

    `[keyname]` - șterge cheia de regiștri și toate valorile sale.

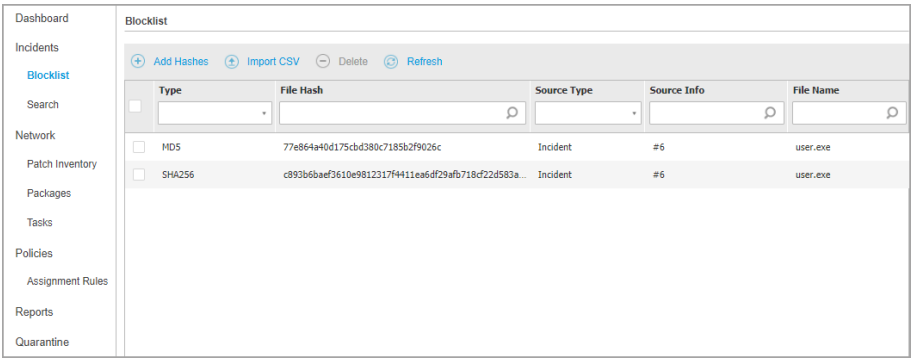
    `/v [valuename]` - șterge valoarea de regiștri specificată.

`/va` - șterge toate valorile cheii specificate de regiștri.

- `cd`
  - **Descriere**: Modifică directorul de lucru în calea specificată. Această comandă necesită, ca parametru, calea către o unitate de disc sau un director de pe endpointul vizat.
  - **Sintaxă**: `cd [path]`
  - **Alias**: -
  - **Parametri**: `[Path]` - calea spre un fișier sau folder de pe stația de lucru țintă.
- `ajutor`
  - **Descriere**: Fără specificarea unui parametru, funcția de ajutor enumeră toate comenzile disponibile împreună cu o scurtă descriere. La introducerea comenzii help, urmată de un parametru, se afișează sintaxa completă a comenzii respective, o scurtă descriere și un exemplu de utilizare.
  - **Sintaxă**: `help [command]`
  - **Alias**: -
  - **Parameteri**: denumire comandă (de exemplu: `cd, kill, ls, ps`)
- `ştergere (cls)`
  - **Descriere**: Șterge feresatra de pe terminal și afișează un mesaj cu directorul de lucru actual.
  - **Sintaxă**: `clear`
  - **Alias**: `cls`
  - **Parametri**: -

9.2. Fișiere în lista de blocare

În pagina **Listă de blocare** puteți vizualiza și administra elementele în funcție de valoarea lor hash. Vizualizați înregistrările de activitate în secțiunea Jurnal activitate utilizator.



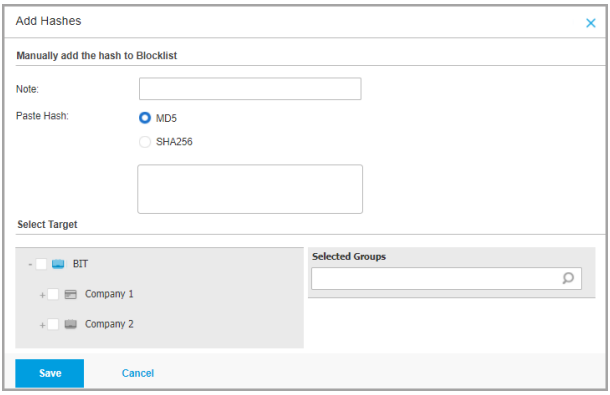
Pagină listă de blocare

Într-un tabel cu date, puteți vizualiza următoarele detalii pentru fiecare element:

- Tip de fișier:
  - MD5
  - SHA256
- Valoare hash fișier
- Tip sursă:
  - Incident
  - Importă
  - Manual
- Informații sursă
- Nume fișier
- Companie

Adăugare valori hash la Lista de blocare existentă:

1. Copiați valoarea hash din **Informații fișier**.
2. Alegeți dintre **MD5** sau **SHA256** și lipiți valoarea în căsuța de mai jos. Adăugați o notă dacă vi se solicită.
3. Faceți clic pe **Save**.



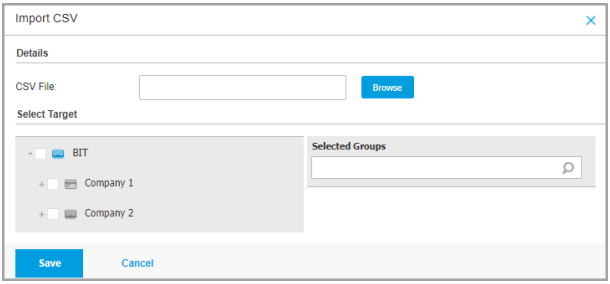
Adăugare fereastră valoare hash

Important

Senzorul de incidente va bloca toate fișierele binare al căror cod hash a fost adăugat într-o **Listă de blocare** de la pornirea unui proces.

Importați înregistrări hash la Lista de blocare existentă. Pentru a importa un fișier CSV:

1. Selectați **Importă fișier CSV**.
2. Căutați fișierul dumneavoastră CSV și efectuați clic pe **Salvare**.



Fereastră Import CSV

De asemenea, puteți importa fișiere CSV de pe dispozitivul dumneavoastră în pagina **Listă de blocare**, dar mai întâi trebuie să vă asigurați că fișierul CSV este valid.

Pentru a crea un fișier CSV valid pentru import, trebuie să introduceți următoarele date în primele trei coloane:

1. Prima coloană a fișierului CSV trebuie să conțină următorul tip de cod hash: fie `md5`, fie `sha256`.
2. Cea de-a doua coloană trebuie să conțină codurile hash hexazecimale aferente.
3. Cea de-a treia coloană poate conține informații de tip text opționale referitoare la coloana **Informații sursă** din pagina **Listă de blocare**.

Notă
Informațiile aferente celorlalte coloane din pagina **Listă de blocare** vor fi completate automat la importarea fișierului CSV.

10. UTILIZAREA RAPOARTELOR

Control Center vă permite să creați și să vizualizați rapoarte centralizate privind starea de securitate a obiectelor de rețea gestionate. Rapoartele pot fi utilizate în mai multe scopuri, cum ar fi:

- Monitorizarea și asigurarea conformității cu politicile de securitate ale organizației.
- Verificarea și evaluarea stării de securitate a rețelei.
- Identificarea problemelor referitoare la securitatea rețelei, a amenințărilor și vulnerabilităților.
- Monitorizarea incidentelor de securitate.
- Oferirea informațiilor ușor de interpretat privind securitatea rețelei către managementul superior.

Sunt disponibile mai multe tipuri de rapoarte diferite, astfel încât să puteți obține cu ușurință informațiile de care aveți nevoie. Informațiile sunt prezentate sub forma unor tabele interactive ușor de consultat, care vă permit să verificați rapid starea de securitate a rețelei și să identificați problemele de securitate.

Rapoartele pot include date din întreaga rețea de obiecte de rețea administrate sau numai din anumite grupuri specifice. Astfel, consultând un singur raport, puteți afla:

- Date statistice referitoare la grupuri sau la toate obiecte de rețea administrate.
- Informații detaliate pentru fiecare obiect din rețea administrat.
- Lista calculatoarelor care îndeplinesc anumite criterii (de exemplu, cele care au protecția contra programelor periculoase dezactivată).

Unele rapoarte permit și soluționarea rapidă a problemelor identificate în rețea. De exemplu, puteți actualiza fără efort toate obiectele din rețeaua țintă direct din raport, fără a trebui să executați o sarcină de actualizare din pagina **Rețea**.

Toate rapoartele programate sunt disponibile în Control Center însă le puteți salva și pe calculator sau transmite prin e-mail.

Formatele disponibile includ Portable Document Format (PDF) și comma-separated values (CSV).

10.1. Tipuri de rapoarte

Sunt disponibile diferite tipuri de rapoarte pentru fiecare tip de stație de lucru:

- Rapoarte referitoare la calculatoare și mașini virtuale

- Rapoarte Exchange
- Rapoarte dispozitive mobile

10.1.1. Rapoarte referitoare la calculatoare și mașini virtuale

Tipurile de rapoarte disponibile pentru mașinile fizice și virtuale sunt următoarele:

Activitate Antiphishing

Vă informează despre starea modulului Antiphishing din Bitdefender Endpoint Security Tools. Puteți vizualiza numărul de site-uri de phishing blocate pe stațiile de lucru selectate și utilizatorul care era autentificat la momentul ultimei detecții. Făcând clic pe link-urile din coloana **Site-uri blocate**, puteți vizualiza și URL-urile site-ului, numărul de blocări și data ultimului eveniment de blocare.

Aplicații blocate

Vă informează despre activitatea următoarelor module: Antimalware, Firewall, Control Conținut, Control Aplicații, Advanced Anti-Exploit, ATC/IDS și HVI. Puteți vedea numărul de aplicații blocate pe stațiile de lucru selectate și utilizatorul care era autentificat la momentul ultimei detecții.

Faceți clic pe numărul asociat unei ținte pentru a vizualiza informații suplimentare privind aplicațiile blocate, numărul de evenimente produse și data și ora ultimei blocări.

În acest raport, puteți instrui rapid modulele de protecție să permită executarea aplicației selectate pe stațiile de lucru țintă:

- Efectuați clic pe butonul **Adăugare excepție** pentru a defini excepțiile din următoarele module: Antimalware, ATC, Control conținut, Firewall și HVI. Se va afișa o fereastră de confirmare, care vă va informa în legătură cu noua regulă care va modifica politica existentă pentru stația de lucru respectivă.
- Efectuați clic pe butonul **Adăugare regulă** pentru a defini o regulă pentru o aplicație sau un proces în Control aplicații. În fereastra de configurare, aplicați regula la o politică existentă. Un mesaj vă va informa cu privire la noua regulă care va modifica politica atribuită stației de lucru respective. De asemenea, raportul va afișa și numărul de tentative de accesare și dacă modulul a fost executat în Modul de testare sau în Modul de producție.

Website-uri blocate

Vă informează despre starea modulului Web Control din Bitdefender Endpoint Security Tools. Pentru fiecare țintă, puteți vizualiza numărul de site-uri blocate.

Făcând clic pe acest număr, puteți vizualiza informații suplimentare, cum ar fi:

- URL-ul și categoria site-ului
- Numărul tentativelor de accesare/site
- Data și ora ultimei accesări, precum și utilizatorul care era autentificat la momentul detecției.
- Motivul blocării, care include accesul programat, detecția de programe periculoase, filtrarea categoriilor și includerea pe o listă neagră.

Protecție Date

Vă informează despre starea modulului Data Protection din Bitdefender Endpoint Security Tools. Puteți vizualiza numărul de mesaje e-mail și site-uri web blocate pe stațiile de lucru selectate, precum și utilizatorul care era autentificat la momentul ultimei detecții.

Activitate de control al dispozitivelor

Vă informează cu privire la evenimentele înregistrate la accesarea stațiilor de lucru prin intermediul dispozitivelor monitorizate. Pentru fiecare stație de lucru, puteți vizualiza numărul de evenimente de acces permise/blocate și needitabile. Dacă s-au înregistrat evenimente, informațiile suplimentare pot fi accesate făcând clic pe cifrele corespunzătoare. Detaliile se referă la:

- Utilizator conectat la mașină
- Tipul și codul dispozitivului
- Producătorul dispozitivului și codul produsului
- Data și ora evenimentului.

Stare criptare stații de lucru

Vă oferă informații cu privire la starea de criptare a stațiilor de lucru. O diagramă circulară prezintă numărul de mașini conforme și, respectiv, neconforme cu setările politicii de criptare.

Un tabel aflat sub diagrama circulară vă oferă detalii precum:

- Nume stație de lucru.
- Full Qualified Domain Name (FQDN).
- IP-ul mașinii.
- Sistemul de operare.

- Conformitate cu politica privind dispozitivele:
  - **Conform** – dacă volumele sunt toate criptate sau decriptate, conform politicii.
  - **Neconform** – dacă starea volumelor nu este în conformitate cu politica atribuită (de exemplu, doar unul din două volume este criptat sau un proces de criptare este în curs pe volumul respectiv).
- Politica privind dispozitivele (**Criptare** sau **Decriptare**).
- Efectuați clic pe numerele din coloana Rezumat volume pentru a vizualiza informații despre volumele fiecărei stații de lucru: ID, nume, starea de criptare (**Criptat** sau **Necriptat**), probleme, tip (**Boot** sau **Non-boot**), dimensiune, ID de recuperare.

Stare module Endpoint Security

Oferă o privire de ansamblu privind sfera de acoperire a modulelor de protecție pentru țintele selectate. În detaliile raportului, puteți vizualiza pentru fiecare stație de lucru țintă ce module sunt active, dezactivate sau neinstalate, precum și motorul de scanare utilizat. Atunci când efectuați clic pe numele stației de lucru, se va afișa fereastra **Informații**, care conține detalii despre stația de lucru și straturile de protecție instalate.

Făcând clic pe butonul **Reconfigurare client**, puteți inițializa o sarcină pentru a modifica setările inițiale ale unuia sau mai multor endpoint-uri selectate. Pentru detalii, consultați Reconfigurare client.

Stare protecție stații de lucru

Vă oferă diverse informații de stare privind stațiile de lucru selectate din rețea.

- Stare protecție antimalware
- Starea de actualizare Bitdefender Endpoint Security Tools
- Starea de activitate a rețelei (online/offline)
- Stadiul managementului

Puteți aplica filtre în funcție de aspectul de securitate și de stare pentru a identifica informațiile pe care le căutați.

Activitate firewall

Vă informează despre starea modulului Firewall din Bitdefender Endpoint Security Tools. Puteți vizualiza numărul de tentative de trafic blocate și porturile

de scanare blocate pe stațiile de lucru selectate, precum și utilizatorul care era autentificat la momentul ultimei detecții.

Activitate HyperDetect

Vă informează despre activitatea modulului HyperDetect al Bitdefender Endpoint Security Tools.

Diagrama din partea superioară a paginii raportului vă arată dinamica tentativelor de atac în perioada specificată și distribuția acestora după tipul de atac. Dacă poziționați mouse-ul deasupra înregistrărilor din legendă, se evidențiază în diagramă tipul de atac asociat. Când efectuați clic pe o înregistrare, se va afișa sau ascunde linia respectivă din diagramă. Când efectuați clic pe orice punct al liniei, datele din tabel se vor filtra în funcție de tipul selectat. De exemplu, dacă efectuați clic pe orice punct de pe linia portocalie, tabelul va afișa doar exploatările.

Detaliile din partea de jos a raportului vă vor ajuta să identificați problemele de acces neautorizat din rețea și să vedeți dacă acestea au fost soluționate. Acestea se referă la:

- Patch-ul fișierului periculos sau URL-ul detectat, în cazul fișierelor infectate. Pentru atacurile fără fișier se furnizează numele fișierului executabil folosit în atac, cu un link la fereastra cu detalii care afișează motivul detectării și string-ul liniei de comandă.
- Stația de lucru unde s-a făcut detecția
- Modulul de protecție care a detectat amenințarea. HyperDetect este un strat suplimentar de module Anti-malware și pentru Controlul conținutului, iar raportul va furniza informații despre unul dintre aceste module, în funcție de tipul detecției.
- Tipul atacului intenționat (atac targhetat, grayware, exploatări, ransomware, fișiere suspecte și trafic pe rețea)
- Starea amenințării
- Nivelul de protecție al modulului la care a fost detectat (Permisiv, Normal, Agresiv)
- De câte ori a fost detectată amenințarea
- Cea mai recentă detectare
- Identificare a atac fără fișier (da sau nu), pentru filtrarea rapidă a detectării unor atacuri fără fișier

Notă
Un fișier poate fi folosit în mai multe tipuri de atac. Astfel, GravityZone îl raportează pentru fiecare tip de atac în care a fost implicat.

Puteți elimina rapid din acest raport rezultatele fals pozitive, adăugând excepții la politicile de securitate alocate. Pentru a face acest lucru:

1. Selectați din tabel numărul de înregistrări de care aveți nevoie.

   Notă
   Detectările de atacuri fără fișier nu pot fi adăugate la lista de excepții deoarece fișierul executabil detectat nu este el însuși un program malware, ci poate fi o amenințare atunci când conține o linie de comandă periculoasă.

2. Efectuați clic pe butonul **Adăugare excepție** în partea de sus a tabelului.
3. În fereastra de configurare selectați politicile la care doriți să adăugați excepțiile și apoi efectuați clic pe **Adăugare**.

   În mod implicit, informațiile aferente fiecărei excepții adăugate sunt trimise la laboratoarele Bitdefender pentru îmbunătățirea capacității de detecție a produselor Bitdefender. Puteți controla această acțiune folosind căsuța **Trimiteți acest feedback la Bitdefender pentru o analiză mai aprofundată**.

Dacă amenințarea a fost detectată de modulul Antimalware, excepția va fi aplicată atât la modul de Scanare la accesare, cât la cel de Scanare la cerere.

Notă
Puteți găsi aceste excepții în următoarele secțiuni ale politicilor selectate: **Antimalware > Setări** pentru fișiere și în **Control conținut > Trafic** pentru URL-uri.

Stare malware

Vă ajută să aflați numărul și identitatea stațiilor de lucru selectate din rețea care au fost afectate de programele periculoase într-un anumit interval de timp și metoda de gestionare a amenințărilor. De asemenea, puteți vedea utilizatorul care era autentificat la momentul ultimei detecții.

Stațiile de lucru sunt grupate pe baza următoarelor criterii:

- Stațiile de lucru pe care nu s-a detectat nimic (nu au fost detectate amenințări malware în perioada de timp specificată)
- Stațiile de lucru cu programe periculoase soluționate (toate fișierele detectate au fost dezinfectate sau mutate cu succes în carantină)

- Stațiile de lucru cu probleme malware neremediate (s-a blocat accesul la unele dintre fișierele detectate)

Pentru fiecare stație de lucru, făcând clic pe link-urile disponibile în coloanele cu rezultatele dezinfectării, puteți vizualiza lista amenințărilor și calea către fișierele afectate.

În acest raport, puteți efectua rapid o Scanare completă pe sistemele țintă care au probleme neremediate efectuând clic pe butonul **Scanare ținte infectate** din bara de instrumente pentru acțiuni de deasupra tabelului cu date.

Incidente în rețea

Vă informează cu privire la activitatea modului Network Attack Defense. Un grafic afișează numărul de tentative de atac detectate într-un anumit interval. Detaliile raportului includ:

- Nume endpoint, adresă IP și FQDN
- Utilizator
- Nume detecție
- Tehnica de atac
- Număr de încercări
- Adresa IP a atacatorului
- Adresa IP și portul targetat
- Ultima dată când atacul a fost blocat

Făcând clic pe butonul **Adăugare excepții** pentru o detecție selectată creează automat o înregistrare în **Excepții globale** din secțiunea **Protecție rețea**.

Stare patch-uri rețea

Verificați starea de actualizare a programelor software instalate în rețeaua dumneavoastră. Raportul dezvăluie următoarele detalii:

- Mașina vizată (denumirea stației de lucru, adresa IP și sistemul de operare).
- Patch-urile de securitate (patch-urile instalate, patch-urile cu erori, patch-urile de securitate și non-securitate care lipsesc).
- Starea și data ultimei modificări pentru stațiile de lucru verificate.

Stare protecție rețea

Oferă informații detaliate cu privire la starea generală de securitate a stațiilor de lucru țintă. De exemplu, puteți vizualiza informații despre:

- Nume, adresă IP și FQDN
- Stare:

  - **Prezintă probleme** - endpoint-ul prezintă vulnerabilități ale protecției (agentul de securitate nu este actualizat, s-au detectat amenințări de securitate etc.)
  - **Nu există probleme** - endpoint-ul este protejat și nu există motive de îngrijorare.
  - **Necunoscut** - endpoint-ul era deconectat atunci când a fost generat raportul.
  - **Neadministrat** - agentul de securitate nu este instalat încă pe endpoint.
- Straturi de protecție disponibile
- Endpoint-uri administrate și neadministrate (agentul de securitate este instalat sau nu)
- Tip și stare licență (coloanele suplimentare aferente licenței sunt ascunse în mod implicit)
- Starea infecției (endpoint-ul este „curat” sau nu)
- Actualizare stare produs și conținut de securitate
- Stare patch de securitate software (patch-uri de securitate sau non-securitate lipsă)

Pentru stațiile de lucru neadministrate, veți vedea starea **Neadministrat** sub alte coloane.

Scanarea la cerere

Oferă informații privind scanările la cerere efectuate pe țintele selectate. O diagramă afișează statisticile pentru scanările finalizate cu succes și cele eșuate. Tabelul de sub diagramă oferă detalii privind tipul de scanare, apariția și ultima scanare finalizată cu succes pentru fiecare stație de lucru.

Conformitate politică

Oferă informații privind politicile de securitate aplicate pe țintele selectate. O diagramă afișează starea politicii. În tabelul de sub diagramă, puteți vedea politica atribuită fiecărei stații de lucru și tipul politicii, precum și data și utilizatorul care a efectuat atribuirea.

Trimiteri eșuate către Sandbox Analyzer

Afișează toate trimiterile eșuate ale unor obiecte trimise de la stațiile de lucru către la Sandbox Analyzer într-o anumită perioadă de timp. O trimitere este considerată eșuată după mai multe încercări de trimitere.

Graficul prezintă variațiile trimiterilor eșuate pentru perioada selectată, în timp ce tabelul cu detaliile raportului vă indică ce fișiere nu au putut fi trimise către Sandbox Analyzer, echipamentul de la care a fost trimis obiectul, data și ora pentru fiecare reîncercare, codul de eroare apărut, descrierea fiecărei încercări eșuate și denumirea companiei.

Rezultate Sandbox Analyzer (Perimat)

Vă furnizează informații detaliate cu privire la fișierele de pe stațiile de lucru țintă, care au fost analizate în sandbox într-un interval de timp specificat. Un grafic cu linii afișează numărul de fișiere analizate, sigure sau periculoase, în timp ce tabelul vă oferă detalii cu privire la fiecare caz.

Puteți genera un raport de tip Rezultat Sandbox Analyzer pentru toate fișierele analizate sau numai pentru cele detectate ca fiind periculoase.

Puteți vizualiza:

- Verdictul analizei ne spune dacă fișierul este sigur, periculos sau necunoscut (**Amenințare detectată** / **Nicio amenințare detectată** / **Fără asistență**). Această coloană apare numai când selectați raportul de afișare a tuturor obiectelor analizate.

  Pentru a vizualiza lista completă a tipurilor și extensiilor de fișiere suportate de către Sandbox Analyzer, consultați „Tipuri și extensii de fișiere acceptate pentru trimitere manuală” (p. 571).
- Tipul de amenințare, cum ar fi adware, rootkit, downloader, exploit, instrument de modificare a fișierului Hosts, instrumente periculoase, furt de parole, ransomware, spam sau troian.
- Data și ora detectării, pe care le puteți filtra în funcție de perioada de raportare.
- Denumirea gazdei sau adresa IP a stației de lucru pe care a fost detectat fișierul.
- Denumirea fișierelor, dacă au fost transmise individual sau numărul de fișiere analizate în cazul unui grup. Efectuați clic pe denumirea fișierului sau pe linkul unui grup pentru a vizualiza detaliile și acțiunile întreprinse.
- Starea acțiunii de remediere pentru fișierele încărcate (**Parțial**, **Eșuat**, **Doar raportat**, **Reușit**).
- Denumirea companiei.
- Mai multe informații despre proprietățile fișierului analizat sunt disponibile efectuând clic pe butonul **Aflați mai multe** din coloana **Rezultat analiză**. Aici puteți vizualiza detalii de securitate și rapoarte detaliate cu privire la comportamentul mostrei.

Sandbox Analyzer surprinde următoarele evenimente comportamentale:

- Scriere / ștergere / mutare / duplicare / înlocuire fișiere în sistem și pe unitățile amovibile.
- Executarea fișierelor nou create.
- Modificări ale sistemului de fișiere.
- Modificări ale aplicațiilor care rulează pe mașina virtuală.
- Modificări ale barei de instrumente și ale meniului de Start din Windows.
- Crearea / terminarea / injectarea proceselor.
- Scrierea / ștergerea cheilor de regiștri.
- Crearea obiectelor mutex.
- Crearea / pornirea / oprirea / modificarea / interogarea / ștergerea serviciilor.
- Modificarea setărilor de securitate ale browser-ului.
- Modificarea setărilor de afișare ale Windows Explorer.
- Adăugarea de fișiere la lista de excepții firewall.
- Modificarea setărilor de rețea.
- Activarea execuției la pornirea sistemului.
- Conectarea la o gazdă la distanță.
- Accesarea anumitor domenii.
- Transferul datelor către și dinspre anumite domenii.
- Accesarea adreselor URL, adreselor IP și a porturilor prin intermediul mai multor protocoale de comunicație.
- Verificarea indicatorilor mediului virtual.
- Verificarea indicatorilor instrumentelor de monitorizare.
- Crearea de capturi de ecran.
- Hook SSDT, IDT, IRP.
- Dump-uri de memorie pentru procese suspecte
- Apelări ale funcțiilor Windows API.
- Inactivitate pentru o anumită perioadă de timp pentru întârzierea execuției.
- Crearea de fișiere cu acțiunile care trebuie executate la anumite intervale de timp.

În fereastra **Rezultat analiză**, efectuați clic pe butonul **Descărcare** pentru a memora pe calculatorul dvs. conținutul Rezumatului de comportament în următoarele formate: XML, HTML, JSON, PDF.

Acest raport va fi disponibil în continuare pentru o perioadă limitată de timp. Vă recomandăm să folosiți înregistrările trimiterilor pentru a aduna informațiile necesare despre mostrele analizate. Înregistrările trimiterilor sunt disponibile în secțiunea **Sandbox Analyzer**, din meniul principal al Control Center.

Verificare de securitate

Oferă informații despre evenimentele de securitate produse pe o țintă selectată. Informațiile se referă la următoarele evenimente:

- Detectare programe periculoase
- Aplicație blocată
- Port de scanare blocat
- Trafic blocat
- Site web blocat
- Blochează dispozitivul
- E-mail blocat
- Proces blocat
- Evenimente HVI
- Evenimente Anti-exploit avansat
- Evenimente Network Attack Defense

Stare Security Server

Vă ajută să evaluați starea serverelor țintă Security Server. Puteți identifica problemele care afectează fiecare Security Server cu ajutorul mai multor indicatori de stare, precum:

- **Stare**: arată starea generală a Security Server.
- **Starea mașinii**: informează ce aplicații Security Server sunt oprite.
- **Starea AV**: arată dacă modulul Antimalware este activat sau dezactivat.
- **Stare actualizare**: arată dacă aplicațiile Security Server sunt actualizate sau actualizările au fost dezactivate.
- **Stare încărcare**: arată nivelul sarcinii de scanare al unui Security Server, după cum este descris în continuare:
  - **Subîncărcat**, atunci când se folosește mai puțin de 5% din capacitatea de scanare.
  - **Normal**, atunci când sarcina de scanare este echilibrată.
  - **Supraîncărcat**, atunci când sarcina de scanare depășește 90% din capacitatea proprie. În acest caz, verificați politicile de securitate. Dacă toate Security Server alocate în cadrul unei politici sunt suprasolicitate, trebuie să adăugați un alt Security Server în listă. În caz contrar, verificați conexiunea la rețea dintre clienți și Security Server care nu prezintă probleme de încărcare.

- **Mașini virtuale protejate HVI**: vă informează cu privire la mașinile virtuale care sunt monitorizate și protejate de modulul HVI.
- **Stare HVI**: arată dacă modulul HVI este activat sau dezactivat. HVI este activat dacă Security Server și pachetul suplimentar sunt instalate pe gazdă.
- **Dispozitive de stocare conectate**: vă informează cu privire la numărul dispozitivelor de stocare compatibile ICAP care sunt conectate la Security Server. Dacă faceți clic pe fiecare număr, se va afișa o listă a dispozitivelor de stocare, cu detalii pentru fiecare: nume, IP, tip, data și ora ultimei conexiuni.
- **Stare scanare dispozitiv stocare**: indică dacă serviciul Security for Storage este activat sau nu.

De asemenea, puteți vedea câți agenți sunt conectați la Security Server. În plus, dacă efectuați clic pe numărul de clienți conectați, se va afișa lista stațiilor de lucru. Aceste stații de lucru pot fi vulnerabile dacă Security Server întâmpină probleme.

Top 10 malware detectat

Vă indică primele 10 amenințări malware detectate într-o anumită perioadă de timp pe stațiile de lucru selectate.

Notă
Tabelul de detalii afișează toate stațiile de lucru care au fost infectate în funcție de primele 10 programe periculoase detectate.

Top 10 stații de lucru infectate

Afișează top 10 a celor mai infectate stații de lucru după numărul total de detecții dintr-o anumită perioadă de timp din stațiile de lucru selectate.

Notă
Tabelul detaliilor afișează toate tipurile de programe periculoase detectate pe primele 10 cele mai infectate stații de lucru.

Stare actualizare

Arată starea de actualizare a agentului de securitate sau Security Server instalat pe țintele selectate. Starea de actualizare se referă la versiunile de produs și conținut de securitate.

Folosind filtrele disponibile, puteți afla cu ușurință ce clienți au efectuat și ce clienți nu au efectuat actualizările în ultimele 24 de ore.

În acest raport, puteți actualiza rapid agenții la cea mai nouă versiune. Pentru a face acest lucru, efectuați clic pe butonul **Actualizare** din Bara de instrumente pentru acțiuni de deasupra tabelului.

Stare upgrade

Ilustrează agenții de securitate instalați pe țintele selectate și dacă este disponibilă o soluție mai recentă.

Pentru stațiile de lucru cu agenți de securitate vechi instalați, puteți instala cel mai recent agent de securitate compatibil, făcând clic pe butonul **Actualizare**.

Notă

Acest raport este disponibil doar dacă s-a efectuat o actualizare a soluției GravityZone.

Stare protecție rețea mașini virtuale

Vă informează asupra gradului de acoperire a protecției Bitdefender din mediul virtualizat. Pentru fiecare dintre mașinile selectate, puteți vizualiza componenta care soluționează problemele de securitate:

- Security Server, pentru configurațiile fără agent în mediile VMware NSX și vShield și pentru HVI
- Un agent de securitate, în orice altă situație

Activitate HVI

Vă informează cu privire la toate atacurile detectate de modulele HVI pe mașinile selectate într-o anumită perioadă de timp.

Raportul include, de asemenea, informații despre data și ora ultimului incident detectat, care a implicat procesul monitorizat, starea finală a acțiunii întreprinse împotriva atacului, utilizatorul în a cărui sesiune a fost pornit procesul și mașina țintă.

În funcție de acțiunea întreprinsă, același proces poate fi raportat de mai multe ori. De exemplu, dacă un proces a fost întrerupt și altădată accesul a fost refuzat, veți vedea două înregistrări în tabelul raportului.

Pentru fiecare proces, atunci când faceți clic pe data ultimei detecții, se va afișa un jurnal separat cu toate incidentele detectate de la momentul pornirii procesului. Jurnalul evidențiază informații importante, cum ar fi tipul și descrierea incidentului, sursa și ținta atacului și acțiunile întreprinse pentru remedierea problemei.

În acest raport, puteți configura modulul de protecție să ignore anumite evenimente, pe care le considerați sigure. Pentru a face acest lucru, efectuați clic pe butonul **Adăugare excepție** din Bara de instrumente pentru acțiuni de deasupra tabelului.

Notă
Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Stare injectare instrumente HVI de la terți

Vă oferă situația detaliată pentru execuția fiecărei injectări pe stațiile de lucru vizate. Informațiile includ:

- Numele stației de lucru.
- Numele instrumentului injectat.
- Adresa IP a stației de lucru.
- Sistemul de operare găzduit.
- Declanșator. Acest lucru poate reprezenta o violare a memoriei, o sarcină la cerere, sau o executare programată.
- Numărul de executări reușite. Un clic pe număr va produce apariția unei ferestre conținând calea jurnalului și marcajul temporal pentru fiecare instrument executat. Un clic pe pictograma din fața căii o copiază pe aceasta pe clipboard.
- Numărul de executări eșuate. Un clic pe număr produce apariția unei ferestre în care puteți vizualiza motivul eșecului și marcajul temporal.
- Ultima injectare reușită.

Injectările sunt grupate după stațiile de lucru vizate. Puteți filtra raportul pentru a vizualiza doar datele referitoare la un anumit instrument, utilizând opțiunile de filtrare din antetul tabelului.

Notă
Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Activitate ransomware

Vă oferă informații privind atacurile ransomware detectate de GravityZone la nivelul endpoint-urilor pe care le administrați și instrumentele necesare pentru a recupera fișierele afectate în timpul atacurilor.

Raportul este disponibil sub formă de pagină în Control Center, fiind diferit de celelalte rapoarte și putând fi accesat direct din meniul principal GravityZone.

Pagina **Activitate ransomware** include un tabel care, pentru fiecare atac ransomware, listează următoarele:

- Numele, adresa IP și FQDN-ul endpoint-ului la nivelul căruia a avut loc atacul
- Compania de care aparține endpoint-ul
- Numele utilizatorului care era conectat în timpul atacului
- Tipul atacului, respectiv local sau de la distanță
- Procesul în cadrul căruia ransomware-ul a rulat, în cazul atacurilor locale, sau adresa IP din care atacul a fost inițiat, în cazul celor de la distanță
- Data și ora detecției
- Numărul fișierelor criptate până la blocarea atacului
- Starea acțiunii de remediere pentru toate fișierele de pe endpoint-ul vizat

Unele detalii sunt ascunse implicit. Apăsați butonul **Afișare/Ascundere coloane** din partea dreaptă sus a paginii pentru configurarea detaliilor pe care doriți să le vedeți în tabel. Dacă sunt multe intrări în tabel, puteți alege să ascundeți filtrele utilizând butonul **Afișare/Ascundere filtre** din partea dreaptă sus a paginii.

Sunt disponibile informații suplimentare dacă selectați numărul pentru fișiere. Puteți vizualiza o listă cu calea completă către fișierele originale și recuperate și cu starea de recuperare a tuturor fișierelor care au fost implicate în atacul ransomware selectat.

Important
Copiile de siguranță sunt disponibile timp de maxim 30 de zile. Țineți seama de data și ora până la care fișierele pot fi recuperate.

Pentru recuperarea fișierelor afectate de atacul ransomware:

1. Selectați atacurile care doriți să fie afișate în tabel.

2. Apăsați butonul**Recuperare fișiere**. Va fi afișată o fereastră de confirmare.

   Se creează o sarcină de recuperare. Puteți verifica starea acesteia în pagina **Sarcini**, la fel ca pentru orice altă sarcină din GravityZone.

Dacă detecțiile sunt rezultatul unor procese legitime, urmați acești pași:

1. Selectați înregistrările din tabel.
2. Apăsați butonul **Adăugare excepție**.
3. În noua fereastră, selectați politicile pentru care va fi aplicată excepția.
4. Efectuează clic pe **Add**.

   Vor fi aplicate toate excepțiile posibile: pentru directoare, procese și adrese IP.

   Le puteți verifica și modifica în secțiunea de politici **Antimalware > Setări > Excepții personalizate**.

Notă
În Activitate ransomware se păstrează înregistrări ale evenimentelor timp de doi ani.

10.1.2. Rapoarte Servere Exchange

Acestea sunt tipurile de rapoarte disponibile pentru Serverele Exchange:

Exchange - Conținut blocat și atașamente

Furnizează informații referitoare la mesajele e-mail sau atașamentele șterse de opțiunea Control conținut de pe serverele selectate, într-un anumit interval de timp. Informațiile includ:

- Adresele e-mail ale expeditorului și ale destinatarilor.

  Dacă e-mail-ul are mai mulți destinatari, în locul adreselor e-mail, raportul afișează numărul destinatarilor, cu un link către o fereastră cu lista adreselor e-mail.
- Subiect e-mail.
- Tip detecție, care indică filtrul de Control al conținutului care a identificat amenințarea.
- Măsura luată cu privire la amenințarea detectată.
- Serverul pe care a fost detectată amenințarea.

Exchange - Atașamente blocate și care nu pot fi scanate

Vă oferă informații despre mesajele e-mail ce conțin atașamente care nu pot fi scanate (supra-arhivate, protejate cu parolă etc.), blocate pe serverele de e-mail Exchange selectate pentru o anumită perioadă de timp. Informațiile se referă la:

- Adresele e-mail ale expeditorului și ale destinatarilor.

  Dacă e-mail-ul este expediat către mai mulți destinatari, în locul adreselor e-mail, raportul afișează numărul destinatarilor, cu un link către o fereastră cu lista adreselor e-mail.

- Subiect e-mail.
- Acțiunile întreprinse pentru ștergerea atașamentelor care nu pot fi scanate:
  - **E-mail șters**, ce indică faptul că întregul e-mail a fost șters.
  - **Atașamente șterse**, un nume generic pentru toate acțiunile de ștergere a atașamentelor din e-mail, cum ar fi ștergerea atașamentului, mutarea în carantină sau înlocuirea acestuia cu o notificare.

  Făcând clic pe link-ul din coloana **Acțiune**, puteți vizualiza detaliile pentru fiecare atașament blocat și acțiunea corespunzătoare întreprinsă.

- Data și ora detecției.
- Serverul pe care a fost detectat mesajul de e-mail.

Exchange - Activitate scanare e-mail

Afișează o statistică a măsurilor luate de modulul de Protecție Exchange într-un anumit interval de timp.

Măsurile sunt grupate după tipul de detecție (program periculos, spam, atașament interzis și conținut interzis) și după server.

Statisticile se referă la următoarele stări ale e-mail-ului:

- **În carantină.** Aceste e-mail-uri sunt mutate în directorul Carantină.
- **Șterse/Respinse.** Aceste e-mail-uri au fost detectate sau respinse de server.
- **Redirecționate.** Aceste e-mail-uri au fost redirecționate către adresa e-mail din politică.
- **Curățate și expediate.** E-mail-uri din care au fost eliminate amenințările și care au fost trecute prin filtre.

Un e-mail este considerat curat dacă toate fișierele atașate identificate au fost dezinfectate, trecute în carantină, șterse sau înlocuite cu text.

- **Modificate și expediate.** Informațiile de scanare au fost incluse în titlurile e-mail-urilor și acestea au fost trecute prin filtre.
- **Expediate fără nicio altă măsură.** Aceste e-mail-uri au fost ignorate de Protecția Exchange și au fost trecute prin filtre.

Exchange - Activitate malware

Furnizează informații referitoare la e-mail-urile cu amenințări de tipul programelor periculoase, detectate pe serverele de mail Exchange selectate, într-un anumit interval de timp. Informațiile se referă la:

- Adresele e-mail ale expeditorului și ale destinatarilor.

  Dacă e-mail-ul este expediat către mai mulți destinatari, în locul adreselor e-mail, raportul afișează numărul destinatarilor, cu un link către o fereastră cu lista adreselor e-mail.
- Subiect e-mail.
- Starea e-mail-ului după scanarea contra programelor periculoase.

  Dacă faceți clic pe link-ul de stare, puteți vedea detalii referitoare la programele periculoase detectate și măsurile luate.
- Data și ora detecției.
- Serverul pe care a fost detectată amenințarea.

Exchange - Top 10 malware detectat

Vă informează cu privire la cele mai des detectate 10 amenințări malware din atașamentele e-mail. Puteți genera două ecrane cu statistici diferite. Un ecran afișează numărul de detecții după destinatarii afectați și celălalt după expeditori.

De exemplu, GravityZone a detectat un e-mail cu un atașament infestat transmis către cinci destinatari.

- În ecranul destinatarilor:
  - Raportul afișează cinci detecții.
  - Detaliile raportului afișează doar destinatarii, nu și expeditorii.
- În ecranul expeditorilor:
  - Raportul afișează o detecție.

– Detaliile raportului afișează doar expeditorul, nu și destinatarii.

Pe lândă expeditor/destinatari și denumirea programului periculos, raportul include și următoarele detalii:

- Tipul de program periculos (virus, spyware, PUA, etc.)
- Serverul pe care a fost detectată amenințarea.
- Măsurile luate de modulul contra programelor periculoase.
- Data și ora ultimei detecții.

Exchange - Top 10 destinatari malware

Afișează cei mai importanți 10 destinatari ai mesajelor e-mail care au fost cei mai vizați de programele periculoase într-un anumit interval de timp.

Detaliile raportului includ o listă completă a programelor periculoase care au afectat acești destinatari, alături de măsurile luate.

Exchange - Top 10 destinatari spam

Vă afișează principalii 10 destinatari e-mail după numărul de mesaje de tip spam sau phishing identificate într-un anumit interval de timp. Raportul furnizează informații și cu privire la acțiunile aplicate respectivelor e-mail-uri.

10.1.3. Rapoarte privind dispozitivele mobile

Notă

Rapoarte privind protecția împotriva malware și rapoarte conexe sunt disponibile numai pentru dispozitivele Android.

Aceasta este lista de tipuri de rapoarte disponibile pentru dispozitivele mobile:

Stare malware

Vă ajută să aflați numărul și identitatea dispozitivelor mobile țintă din rețea care au fost afectate de programele periculoase într-un anumit interval de timp și metoda de gestionare a amenințărilor. Dispozitivele mobile sunt grupate pe baza următoarelor criterii:

- Dispozitive mobile pe care nu s-a detectat nimic (nu au fost detectate amenințări malware în perioada de timp specificată)
- Dispozitivele mobile cu programe periculoase rezolvate (toate fișierele detectate au fost îndepărtate)

- Dispozitive mobile cu malware existent (unele dintre fișierele detectate nu au fost șterse).

Top 10 dispozitive infectate

Arată topul 10 a celor mai infectate dispozitive mobile dintr-o o anumită perioadă de timp din dispozitivele mobile țintă.

Notă

Tabelul detaliilor afișează toate tipurile de programe periculoase detectate pe primele 10 dispozitive mobile cele mai infectate.

Top 10 malware detectat

Vă indică primele 10 amenințări malware detectate într-o anumită perioadă de timp pe dispozitivele mobile țintă.

Notă

Tabelul de detalii afișează toate dispozitivele mobile care au fost infectate în funcție de primele 10 programe periculoase detectate.

Conformitate dispozitiv

Vă informează despre starea de conformitate a dispozitivelor mobile țintă. Puteți vedea numele dispozitivului, starea, sistemul de operare și motivul de neconformitate.

Pentru mai multe informații cu privire la cerințele de conformitate, vă rugăm să consultați „Criterii de neconformitate” (p. 399).

Sicronizare dispozitiv

Vă informează despre starea de sincronizare a dispozitivelor mobile țintă. Puteți vizualiza numele dispozitivului, utilizatorul căruia îi este atribuit, precum și stadiul de sincronizare, sistemul de operare și momentul în care dispozitivul a fost online ultima dată.

Pentru mai multe informații, consultați capitolul „Verificarea Stării Dispozitivelor Mobile” (p. 174).

Website-uri blocate

Vă informează cu privire la numărul de încercări ale dispozitivelor țintă pentru a accesa site-uri care sunt blocate de regulile **Acces Web** într-un anumit interval de timp.

Pentru fiecare dispozitiv cu detecții, faceți clic pe numărul prevăzut în coloana **Website-uri blocate** pentru a vizualiza informații detaliate cu privire la fiecăre pagină web blocată, cum ar fi:

- URL
- Componenta politicii care a efectuat acțiunea
- Număr de tentative blocate
- Ultima dată când a fost blocat site-ul

Pentru mai multe informații despre setările politicii de accesare web, vă rugăm să consultați „Profiluri" (p. 405).

Activitate securitate web

Vă informează cu privire la numărul de încercări ale dispozitivelor mobile țintă de a accesa site-urile cu amenințări de securitate (de tip phishing, fraudă, programe periculoase sau site-uri care nu sunt de încredere), într-un anumit interval de timp. Pentru fiecare dispozitiv cu detecții, faceți clic pe numărul prevăzut în coloana Website-uri blocate pentru a vizualiza informații detaliate cu privire la fiecăre pagină web blocată, cum ar fi:

- URL
- Tip de amenințare (phishing, malware, fraudă, nu este de încredere)
- Număr de tentative blocate
- Ultima dată când a fost blocat site-ul

Securitate Web este componenta de politică care detecteaza și blochează site-urile cu probleme de securitate. Pentru mai multe informații despre setările politicii de securitate web, vă rugăm să consultați „Securitate" (p. 394).

10.2. Crearea rapoartelor

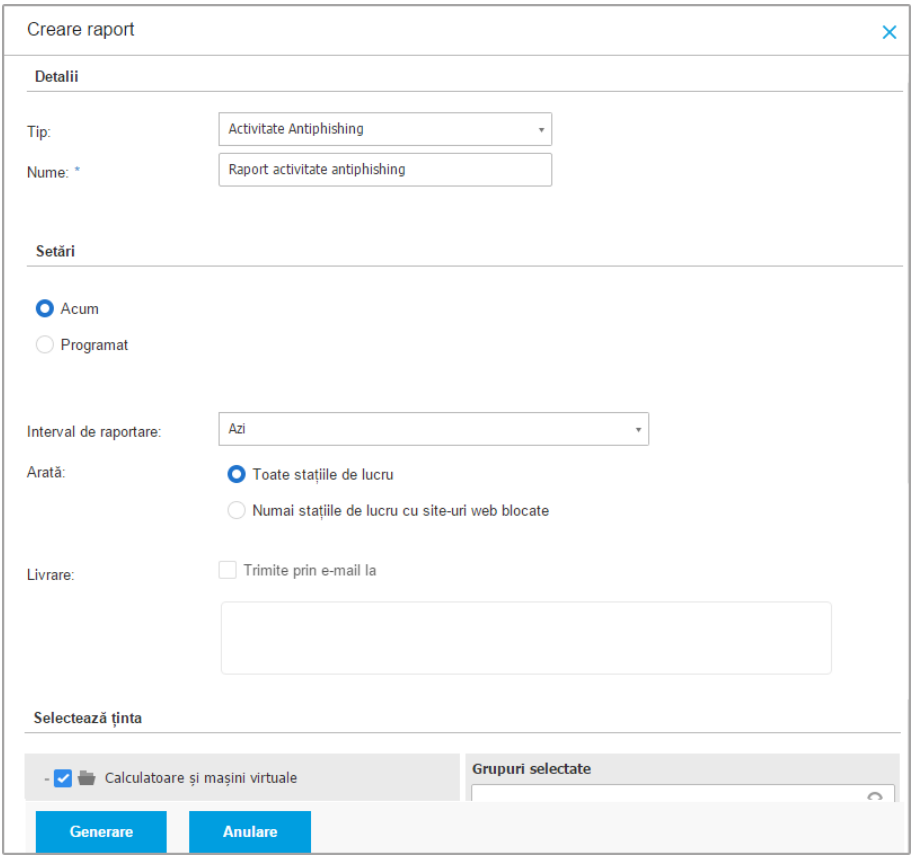
Puteți crea două categorii de rapoarte:

- **Rapoarte instant.** Rapoartele instant sunt afișate în mod automat după ce le generați.
- **Rapoarte programate.** Rapoartele programate pot fi configurate să ruleze periodic, la orele și datele specificate. O listă a tuturor rapoartelor programate se afișează pe pagina **Rapoarte**.

Important
Rapoartele instant sunt șterse automat atunci când închideți pagina de raport. Rapoartele programate sunt salvate și afișate în pagina **Raporate**.

Pentru a crea un raport:

1. Mergeți la pagina **Rapoarte**.
2. Selectați tipul de obiect de rețea din selectorul de vederi.
3. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Este afișată o fereastră de configurare.



Opțiuni pentru rapoartele referitoare la calculatoare și mașini virtuale

4. Selectați tipul dorit de raport din meniu. Pentru mai multe informații, consultați capitolul „Tipuri de rapoarte” (p. 475)
5. Introduceți un nume sugestiv pentru raport. Atunci când alegeți un nume, luați în considerare tipul de raport și, eventual, opțiunile de raportare.
6. Configurați recurența raportului:
   - Selectați **Acum** pentru a crea un raport instant.

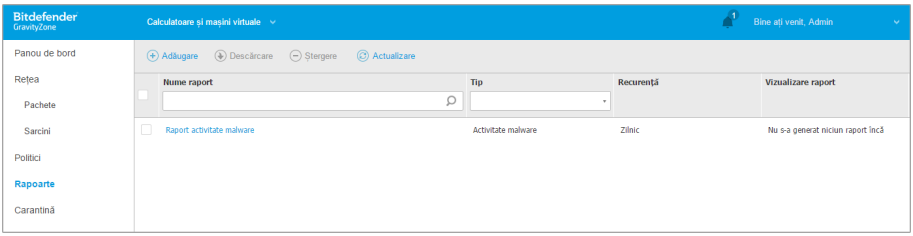
- Selectați **Programat** pentru a configura generarea automată a raportului la intervalul dorit:
  - Orar, la intervalul specificat.
  - Zilnic. În acest caz, puteți să setați și ora de începere (oră și minute).
  - Săptămânal, în zilele specificate ale săptămânii și la ora de începere selectată (oră și minute).
  - Lunar, în fiecare zi specificată a lunii și la ora de începere specificată (oră și minute).

7. Pentru majoritatea tipurilor de rapoarte, trebuie să specificați intervalul temporar la care se referă datele pe care acestea le conțin. Raportul va afișa doar datele din perioada selectată.
8. Mai multe tipuri de rapoarte furnizează opțiuni de filtrare pentru a vă ajuta să identificați mai facil informațiile de care sunteți interesați. Utilizați opțiunile de filtrare din secțiunea **Arată** pentru a obține doar informațiile dorite.

   De exemplu, pentru un raport de **Stare actualizare**, puteți selecta să vizualizați doar lista obiectelor din rețea care nu au fost actualizate sau a celor care necesită repornire pentru finalizarea actualizării.
9. **Livrare**. Pentru a primi prin email un raport programat, bifați căsuța corespunzătoare. Introduceți adresele e-mail dorite în câmpul de mai jos. În mod implicit, e-mailul conține o arhivă cu ambele fișiere de raport (PDF și CSV). Utilizați casetele de bifare din secțiunea **Atașare fișiere** pentru a selecta tipul de fișiere și modul de trimitere al acestora prin e-mail.
10. **Selectare țintă**. Parcurgeți în jos pentru a configura ținta raportului. Selectați unul sau mai multe grupuri de stații de lucru pe care doriți să le includeți în raport.
11. În funcție de recurența selectată, faceți clic pe **Generare** pentru a genera un raport instant sau pe **Salvare** pentru a genera un raport programat.
    - Raportul instant se afișează imediat după ce ați făcut clic pe **Generare**. Intervalul necesar pentru crearea rapoartelor poate diferi în funcție de numărul de obiecte din rețea administrate. Vă rugăm să așteptați pentru a se crea raportul solicitat.
    - Raportul programat se afișează în lista de pe pagina **Rapoarte**. După generarea unei instanțe a raportului, puteți vizualiza raportul făcând clic pe link-ul corespunzător din coloana **Vizualizare raport** de pe pagina **Rapoarte**.

10.3. Vizualizarea și gestionarea rapoartelor programate

Pentru a vizualiza și administra rapoarte programate, mergeți la pagina **Rapoarte**.



Pagina Rapoarte

Toate rapoartele programate se afișează în tabel, alături de informațiile utile referitoare la acestea:

- Denumirea și tipul raportului
- Recurența raportului
- Ultima instanță generată.

Notă
Rapoartele programate sunt disponibile doar pentru utilizatorul care le-a creat.

Pentru a sorta rapoartele pe baza unei anumite coloane, facți clic pe titlul coloanei. Faceți clic pe titlul coloanei din nou pentru a modifica ordinea sortării.

Pentru a găsi ușor ceea ce cauți, utilizați casetele de căutare sau opțiunile de filtrare de sub anteturile de coloană.

Pentru a goli o casetă de căutare, plasați cursorul peste ea și faceți clic pe pictograma × **Ștergere** icon.

Pentru a vă asigura că sunt afișate cele mai recente informații, faceți clic pe butonul **Reîmprospătare** din partea de sus a tabelului.

10.3.1. Vizualizarea rapoartelor

Pentru a vizualiza un raport:

1. Mergeți la pagina **Rapoarte**.

2. Sortați rapoartele după nume, tip sau reapariție pentru a găsi cu ușurință raportul pe care îl căutați.
3. Faceți clic pe link-ul corespunzător în coloana **Vizualizare raport** pentru a afișa raportul. Se afișează cea mai recentă instanță a raportului.

   Pentru a vizualiza toate instanțele unui raport, consultați„Salvarea rapoartelor" (p. 503)

Toate rapoartele cuprind o secțiune rezumat (jumătatea de sus a paginii de raport) și o secțiune de detalii (jumătatea inferioară a paginii de raport).

- Secțiunea rezumat vă oferă date statistice (diagrame și grafice) pentru toate obiectele de rețea țintă, precum și informații generale despre raport, cum ar fi perioada de raportare (dacă este cazul), raportul țintă etc.
- Secțiunea de detalii furnizează informații cu privire la fiecare obiect administrat din rețeaua țintă.

Notă

- Pentru a configura informațiile afișate de diagramă, faceți clic pe intrările de legendă pentru a afișa sau a ascunde datele selectate.
- Faceți clic pe zona grafică (diagramă, gafic) de care sunteți interesat pentru a vedea detaliile aferente din tabel.

10.3.2. Editarea unui raport programat

Notă
Când editați un raport programat, toate actualizările vor fi aplicate începând cu următorul raport. Rapoartele generate anterior nu vor fi afectate de editare.

Pentru a modifica setările unui raport programat:

1. Mergeți la pagina **Rapoarte**.
2. Faceți clic pe numele raportului.
3. Modificați setările raportului după cum este necesar. Puteți modifica următoarele opțiuni:
   - **Nume raport.** Alegeți un nume sugestiv pentru raport care să vă ajute la identificarea cu ușurință la ce se referă. Atunci când alegeți un nume, luați

în considerare tipul de raport și, eventual, opțiunile de raportare. Rapoartele generate de un raport programat sunt denumite după el.

- **Recurența raportului (programul).** Puteți programa ca raportul să fie generat automat orar (după un anumit interval orar), zilnic (la o anumită oră de începere), săptămânal (într-o anumită zi a săptămânii și la o anumită oră de începere) sau lunar (într-o anumită zi a lunii și la o anumită oră de începere). În funcție de programul selectat, raportul va conține numai datele din ultima zi, săptămână sau respectiv lună.
- **Setări**
  - Puteți programa ca raportul să fie generat automat în fiecare oră (în baza unui anumit interval orar), zi (la o anumită oră de începere), săptămână (într-o anumită zi a săptămânii și la o anumită oră de începere) sau lunar (într-o anumită zi a lunii și la o anumită oră de începere). În funcție de programul selectat, raportul va conține numai datele din ultima zi, săptămână sau respectiv lună.
  - Raportul va include date din intervalul de timp selectat. Aveți posibilitatea să modificați intervalul începând cu următorul raport.
  - Cele mai multe tirapoarte asigură opțiuni de filtrare pentru a vă ajuta să identificați mai facil informațiile de care sunteți interesați. Când vizualizați raportul în consolă, vor fi disponibile toate informațiile, indiferent de opțiunile selectate. Însă dacă descărcați raportul sau îl trimiteți prin e-mail, în fișierul PDF vor fi incluse numai rezumatul raportului și informațiile selectate. Detalii cu privire la raport vor fi disponibile doar în format CSV.
  - Puteți alege să primiți raportul prin e-mail.
- **Selectare țintă.** Opțiunea selectată indică tipul țintei curente a raportului (fie grupuri, fie obiecte individuale din rețea). Faceți clic pe link-ul corespunzător pentru a vizualiza raportul țintă curent. Pentru a-l schimba, selectați grupurile sau obiectele de rețea care urmează să fie incluse în raport.

4. Faceți clic pe **Salvare** pentru a aplica modificările.

10.3.3. Ștergerea unui raport programat

Atunci când nu mai aveți nevoie de un raport programat, cel mai bine este să-l ștergeți. Ștergerea unui raport programat va șterge toate instanțele pe care le-a generat în mod automat la acel moment.

Pentru a șterge un raport programat.

1. Mergeți la pagina **Rapoarte**.
2. Selectați raportul pe care doriți să-l ștergeți.
3. Faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului.

10.4. Implementarea măsurilor bazate pe raport

Deși majoritatea rapoartelor evidențiază doar aspecte legate de rețea, unele dintre acestea oferă și o serie de opțiuni pentru rezolvarea problemelor identificate prin apăsarea unui singur buton.

Pentru a rezolva problemele afișate în raport, faceți clic pe butonul corespunzător din Bara de instrumente de acțiuni de deasupra tabelului.

Notă
Pentru efectuarea acestor acțiuni, aveți nevoie de drepturi de **Administrare rețea**.

Opțiunile disponibile pentru fiecare raport sunt:

Aplicații blocate

- **Adăugare excepție**. Adaugă o excepție la politică pentru a împiedica modulele de protecție să blocheze din nou aplicația.
- **Adaugă regulă**. Definește o regulă pentru o aplicație sau un proces în Control aplicații.

Activitate HVI

- **Adăugare excepție**. Adaugă o excepție la politică pentru a împiedica modulul de protecție să raporteze din nou incidentul respectiv.

  Notă
  Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Stare malware

- **Scanare ținte infectate**. Rulează o sarcină de Scanare completă preconfigurată pe țintele care apar ca fiind în continuare infestate.

Stare actualizare

- **Actualizare**. Actualizează clienții țintă la cele mai recente versiuni disponibile.

Stare upgrade

- **Actualizare**. Înlocuiește vechii clienți ai stațiilor de lucru cu ultima generație de produse disponibile.

10.5. Salvarea rapoartelor

În mod implicit, rapoartele programate sunt salvate automat în Control Center.

Dacă aveți nevoie ca rapoartele să fie disponibile mai mult timp, puteți să le salvați pe calculator. Rezumatul raportului va fi disponibil în format PDF, în timp ce detaliile raportului vor fi disponibile doar în format CSV.

Aveți la dispoziție două modalități de salvare a rapoartelor:

- Exportă
- Descărcare

10.5.1. Exportarea rapoartelor

Pentru a exporta raportul în calculator:

1. Alegeți un format și faceți clic pe **Export CSV** sau **Export PDF**.
2. În funcție de setările browser-ului, fișierul poate fi descărcat în mod automat într-o locație de descărcare implicită sau va apărea o fereastră de descărcare unde trebuie să specificați directorul de destinație.

10.5.2. Descărcarea rapoartelor

O arhivă de raport conține atât rezumatul raportului cât și detaliile acestuia.

Pentru a descărca o arhivă de raport:

1. Mergeți la pagina **Rapoarte**.
2. Selectați raportul pe care doriți să-l salvați.

3. Faceți clic pe butonul **Descărcare** și selectați fie **Ultima instanță** tpentru a descărca ultima instanță generată a raportului sau **Arhiva completă** pentru a descărca o arhivă ce conține toate instanțele.

   În funcție de setările browser-ului, fișierul poate fi descărcat în mod automat într-o locație de descărcare implicită sau va apărea o fereastră de descărcare unde trebuie să specificați directorul de destinație.

10.6. Transmiterea prin e-mail a rapoartelor

Puteți trimite rapoarte prin e-mail, folosind următoarele opțiuni:

1. Pentru a trimite raportul pe care îl vizualizați prin e-mail, faceți clic pe butonul **E-mail**. Raportul va fi trimis la adresa de e-mail asociată contului dumneavoastră.
2. Pentru a configura livrarea prin e-mail a rapoartelor programate dorite:
   a. Mergeți la pagina **Rapoarte**.
   b. Faceți clic pe numele raportului dorit.
   c. În **Setări > Livrare**, selectați **Trimite prin e-mail la**.
   d. Introduceți adresa de e-mail dorită în câmpul de mai jos. Puteți adăuga oricâte adrese de e-mail doriți.
   e. Faceți clic pe **Save**.

   Notă
   în fișierul PDF trimis prin e-mail vor fi incluse numai rezumatul raportului și graficul. Detalii cu privire la raport vor fi disponibile în fișierul CSV.

Rapoartele sunt trimise prin email ca arhive de tip ZIP.

10.7. Printarea rapoartelor

Control Center nu acceptă în prezent funcționalitatea de buton de imprimare. Pentru a imprima un raport, trebuie mai întâi să-l salvați pe calculator.

11. CARANTINĂ

Carantina este un director criptat care conține fișiere potențial periculoase, cum ar fi fișierele suspectate că ar fi programe periculoase, infestate cu programe periculoase sau alte fișiere nedorite. Atunci când virușii sau alte tipuri de programe periculoase se află în carantină, sunt inofensivi, pentru că nu pot fi executați sau citiți.

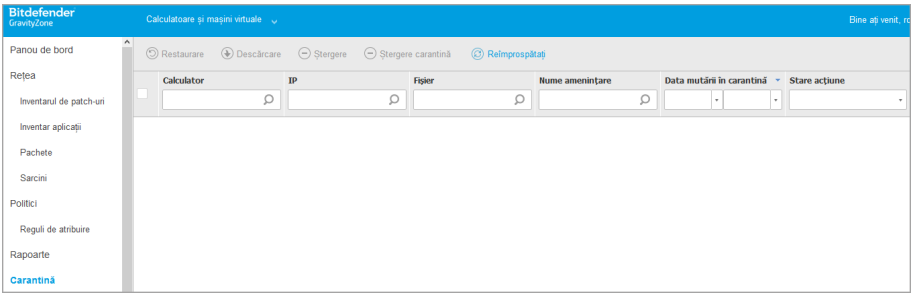
GravityZone trece fișierele în carantină conform politicilor alocate stațiilor de lucru. În mod implicit, fișierele care nu pot fi dezinfestate sunt trecute în carantină.

Carantina este salvată local pe fiecare stație de lucru, cu excepția Serverului VMware vCenter integrat cu vShield Endpoint și cu NSX, unde este salvat pe Security Server.

Important
Funcția Carantină nu este disponibilă pe dispozitivele mobile.

11.1. Explorarea Carantinei

Pagina **Carantină** oferă informații detaliate referitoare la fișierele trecute în carantină de pe toate stațiile de lucru administrate.



Pagina Carantină

Pagina Carantină include două ecrane:

- Calculatoare și mașini virtuale, pentru fișierele detectate direct în sistemul de fișiere al stației de lucru.
- Servere Exchange, pentru e-mail-uri și fișiere atașate la e-mail-uri detectate pe serverele de mail Exchange.

Selectorul de vizualizări din partea de sus a paginii permite comutarea între aceste ecrane.

Informațiile referitoare la fișierele în carantină sunt afișate în tabel. În funcție de numărul de stații de lucru administrate și de nivelul de infestare, tabelul Carantină poate include un număr mai mare de înregistrări. Tabelul poate cuprinde mai multe pagini (în mod implicit, numai 20 de înregistrări sunt afișate pe pagină).

Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului. Pentru a modifica numărul de intrări afișate pe pagină, selectați o opțiune din meniul de lângă butoanele de navigație.

Pentru o mai bună vizibilitate a datelor care vă interesează, puteți folosi casetele de căutare din antetele coloanelor pentru filtrarea datelor afișate. De exemplu, puteți căuta o amenințare specifică detectată în rețea sau pentru un obiect din rețea specific. De asemenea puteți să faceți clic pe antetele de coloană pentru a sorta datele în funcție de o anumită coloană.

Pentru a vă asigura că sunt afișate cele mai recente informații, faceți clic pe butonul **Reîmprospătare** din partea de sus a tabelului. Acest lucru poate fi necesar atunci când petreceți mai mult timp pe pagină.

11.2. Carantină calculatoare și mașini virtuale

Implicit, fișierele aflate în carantină sunt trimise automat către Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender în materie de malware. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia. De asemenea, fișierele în carantină sunt scanate după fiecare actualizare a semnăturii programului periculos. Fișierele curățate sunt mutate automat în locația lor originală. Caracteristicile se referă la fiecare politică de securitate de pe pagina **Politici** și puteți selecta dacă doriți să le mențineți sau să le dezactivați. Pentru mai multe informații, consultați capitolul „Carantină” (p. 287).

11.2.1. Vizualizarea Detaliilor carantinei

Tabelul Carantină include următoarele informații:

- Numele stației de lucru pe care a fost detectată amenințarea.
- Adresa IP a stației de lucru pe care a fost detectată amenințarea.
- Calea către fișierul infectat sau suspect pe stația de lucru pe care a fost detectat.
- Nume dat amenințării de programe periculoase de către cercetătorii de securitate ai Bitdefender.

- Data și Ora la care fișierul a fost izolat în carantină.
- Starea măsurii care trebuie luată asupra fișierului trecut în carantină.

11.2.2. Gestionarea fișierelor aflate în carantină

Comportamentul carantinei este diferit pentru fiecare mediu:

- **Security for Endpoints** stochează fișierele din carantină pe fiecare calculator administrat. Folosind Control Center aveți opțiunea de a șterge sau de a restaura fișierele specifice aflate în carantină.
- **Security for Virtualized Environments (Multi-Platformă)** stochează fișierele din carantină pe fiecare mașină virtuală administrată. Folosind Control Center aveți opțiunea de a șterge sau de a restaura fișierele specifice aflate în carantină.
- **Security for Virtualized Environments (integrat cu VMware vShield Endpoint sau NSX)** stochează fișierele din carantină pe dispozitivul Security Server. Folosind Control Center aveți opțiunea de a șterge fișierele aflate în carantină sau să le descărcați într-o locație aleasă de dumneavoastră.

Restabilirea fișierelor aflate în carantină

În anumite situații, este posibil să fie necesar să recuperați fișierele izolate în carantină, fie în locațiile inițiale, fie într-o locație alternativă. O astfel de situație este când doriți să recuperați fișiere importante stocate într-o arhivă infectată care a fost izolată în carantină.

Notă
Restaurarea fișierelor aflate în carantină este posibilă numai în medii protejate prin Security for Endpoints și Security for Virtualized Environments (Multi - Platformă).

Pentru a restaura unul sau mai multe fișiere aflate în carantină:

1. Mergeți la pagina **Carantină**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi disponibil în partea de sus a paginii.
3. Selectați casetele care corespund fișierelor din carantină pe care doriți să le restabiliți.
4. Faceți clic pe butonul **Repornire** din partea de sus a tabelului.
5. Alegeți locația unde doriți să fie recuperate fișierele selectate (fie locația originală sau o locație anume de pe calculatorul țintă).

   Dacă alegeți să restaurați o locație personalizată, trebuie să introduceți calea absolută în câmpul corespunzător.

6. Selectați **Adaugă automat excepția în politică** pentru a exclude fișierele care urmează să fie restaurate din scanările viitoare. Excluderea sde aplică tuturor politicilor care afectează fișierele selectate, cu excepția politicii implicite, care nu poate fi modificată.
7. Faceți clic pe **Salvare** pentru a solicita acțiunea de recuperare a fișierului. Puteți observa starea în curs în coloana **Acțiune**.
8. Măsura necesară este trimisă către stațiile de lucru țintă imediat sau de îndată ce revin online.

   Puteți vizualiza detaliile referitoare la starea de acțiune pe pagina **Sarcini**. După ce un fișier este recuperat, datele corespunzătoare vor dispărea din tabelul de Carantină.

Descărcarea fișierelor aflate în carantină

În mediile virtualizate VMware integrate cu vSheild Endpoint sau NSX, carantina este salvată pe Security Server. Dacă doriți să examinați sau să recupererați datele din fișierele aflate în carantină, trebuie să le descărcați de pe Security Server folosind Control Center. Fișierele aflate în carantină sunt descărcate ca arhivă ZIP criptată , protejată de o parolă pentru a preveni infectarea accidentală cu programe periculoase.

Pentru a deschide arhiva și a-i extrage conținutul, trebuie să folosiți Instrumentul carantină, o aplicație Bitdefender individuală care nu necesită instalare.

Instrumentul Carantină este disponibil pentru următoarele sisteme de operare:

- Windows 7 sau o versiune mai recentă
- Majoritatea distribuțiilor Linux pe 32 biți cu o interfață grafică cu utilizatorul (GUI).

Notă
Rețineți că Instrumentul de carantină nu are interfață de linie de comandă.

Avertisment
Fiți prudenți atunci când extrageți fișierele din carantină, deoarece acestea pot infecta sistemul. Se recomandă să extrageți și analizați fișierele din carantină pe un sistem de testare sau izolat, de preferință, care rulează pe Linux. Infecțiile cu programe periculoase sunt mai ușor de controlat pe Linux.

Pentru a descărca fișierele din carantină pe calculator:

1. Mergeți la pagina **Carantină**.

2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi disponibil în partea de sus a paginii.
3. Filtrați datele din tabel introducând numebe gazdei sau adresa IP Security Server în câmpul corespunzător din tabel.

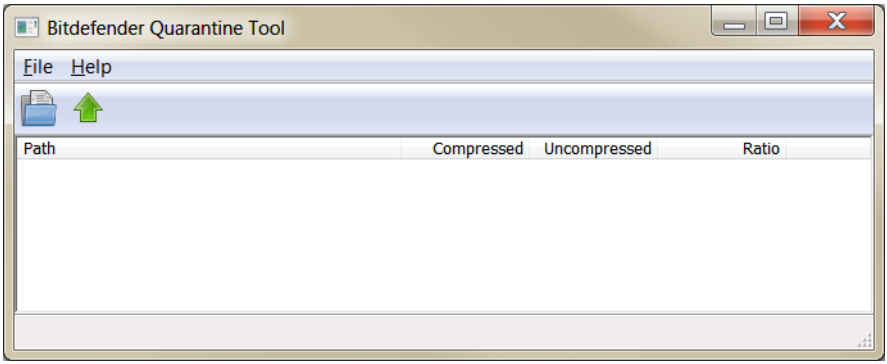
   În cazul în care carantina este mare, pentru a vizualiza fișierele care vă interesează, este posibil să fie necesar să aplicați filtre suplimentare sau să extindeți numărul de fișiere incluse pe pagină.
4. Selectați casetele de bifare corespunzătoare fișierelor pe care doriți să le descărcați.
5. Dați clic pe butonul **Descărcare** din partea de sus a tabelului. În funcție de setările browser-ului, vi se va solicita să salvați fișierele în directorul dorit sau acestea vor fi descărcate autmat în locația implicită de descărcare.

Pentru a accesa fișierele restaurate:

1. Descărcați Instrumentul de carantină corespunzător sistemului dvs. de oeprare de pe pagina **Asistență & Suport tehnic** sau de la următoarea adresă:
   - Quarantine Tool pentru Windows
   - Quarantine Tool pentru Linux

   Notă
   Instrumentul Carantină pentru Linux este arhivat într-un fișier `tar`.

2. Rulați executabilul Instrumentului Carantină.



Instrumentul Carantină

3. În meniul **Fișier**, faceți clic pe **Deschidere** (CTRL+O) sau apăsați butonul **Deschidere** pentru a încărca arhiva în instrument.

   Fișierele sunt organizate în arhivă de mașina virtuală pe care au fost detectați și păstrând calea lor originală.
4. Înainte de extragerea fișierelor arhivate, în cazul în care pe sistem este activată scanarea antimalware la acces , asigurați-vă fie că lați dezactivat sau configurați o excludere de scanare pentru locația în care veți extrage fișierele. În caz contrar, programul antimalware va detecta și va lua măsuri pe fișierele extrase.
5. Selectează fișierele pe care doriți să le extrageți.
6. În meniul **Fișier**, faceți clic pe **Extragere** (CTRL+E) sau apăsați butonul **Extragere**.
7. Selectați directorul de destinație. Fișierele sunt extrase în locația selectată, cu menținerea structurii originale a directorului.

Ștergerea automată a fișierelor din carantină

Implicit, fișierele aflate în carantină de mai mult de 30 de zile sunt șterse automat. Această setare poate fi modificată prin editarea politicii atribuită stațiilor de lucru administrate.

Pentru a schimba intervalul automat de ștergere pentru fișierele aflate în carantină:

1. Mergeți la pagina **Politici**.
2. Găsiți politica atribuită stațiilor de lucru pe care doriți să modificați setările și faceți clic pe numele său.
3. Mergeți la pagina **Antimalware > Setări**.
4. În secțiunea **Carantină**, selectați numărul de zile rămase după care fișierele urmează să fie șterse.
5. Faceți clic pe **Salvare** pentru a aplica modificările.

Ștergerea manuală a fișierelor din carantină

Dacă doriți să ștergeți manual fișierele din carantină, mai întâi trebuie să vă asigurați că fișierele pe care alegeți să le ștergeți, nu sunt necesare.

Un fișier poate fi de fapt program periculos în sine. Dacă cercetarea dumneavoastră va duce la o astfel de situație, puteți căuta în carantină pentru amenințarea specifică și ștergerea ei din carantină.

Pentru a șterge unul sau mai multe fișiere aflate în carantină:

1. Mergeți la pagina **Carantină**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi disponibil în partea de sus a paginii.
3. Selectați casetele care corespund fișierelor din carantină pe care doriți să le ștergeți.
4. Faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

   Puteți observa starea în curs în coloana **Acțiune**.

   Măsura necesară este trimisă către obiectele de rețea țintă imediat sau de îndată ce revin online. După ce un fișier este șters, datele corespunzătoare vor dispărea din tabelul de Carantină.

Golirea Carantinei

Pentru a șterge toate obiectele trecute în carantină:

1. Mergeți la pagina **Carantină**.
2. Selectați **Computere și mașini virtuale** din selectorul de vizualizări.
3. Faceți clic pe butonul **Golire Carantină**.

   Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

Sunt șterse toate datele din tabelul Carantină. Măsura necesară este trimisă către obiectele de rețea țintă imediat sau de îndată ce revin online.

11.3. Carantină Servere Exchange

Carantina Exchange conține e-mail-uri și atașamente. Modulul contra programelor periculoase trece în carantină atașamentele e-mail, iar Filtrarea Antispam, Conținut și Atașamente trece în carantină întregul e-mail.

Notă
Vă rugăm să rețineți că, în cazul Serverelor Exchange, carantina necesită spațiu suplimentar pe hard-disk, pe partiția pe care este instalat agentul de securitate. Dimensiunea carantinei depinde de numărul de articole stocate și de dimensiunea acestora.

11.3.1. Vizualizarea Detaliilor carantinei

Pagina **Carantină** vă oferă informații detaliate referitoare la obiectele trecute în carantină de pe toate Serverele Exchange din organizație. Informațiile sunt disponibile în tabelul Carantină și în fereastra detalii a fiecărui obiect.

Tabelul Carantină include următoarele informații:

- **Subiect.** Subiectul e-mail-ului trecut în carantină.
- **Expeditor.** Adresa e-mail a expeditorului este cea afișată în câmpul **De la** din titlu.
- **Destinatari.** Lista destinatarilor din câmpurile din titlul e-mail-ului **Către** și **Cc**.
- **Destinatari reali.** Lista adreselor e-mail ale utilizatorilor individuali cărora trebuia să le fie transmis e-mail-ul înainte de a fi trecut în carantină.
- **Stare.** Starea obiectului după ce a fost scanat. Starea arată dacă un e-mail este marcat ca fiind spam sau are conținut nedorit, sau dacă un atașament este infectat cu malware, este suspectat ca fiind infectat, nedorit sau nescanabil.
- **Denumire program periculos.** Denumirea alocată amenințării de tip program periculos de cercetătorii de securitate ai Bitdefender.
- **Denumire server.** Denumirea de gazdă a serverului pe care a fost detectată amenințarea.
- **Trecut în carantină în.** Data și ora la care fișierul a fost izolat în carantină.
- **Stare acțiune.** Starea măsurii luate asupra obiectului trecut în carantină. Astfel, puteți vedea rapid dacă o acțiune este încă în curs sau a eșuat.

Notă

- Coloanele **Destinatari reali**, **Denumire program periculos** și **Denumire server** sunt ascunse în ecranul implicit.
- Dacă mai multe atașamente din același e-mail sunt trecute în carantină, tabelul Carantină include o intrare separată pentru fiecare atașament.

Pentru a personaliza detaliile referitoare la carantină afișate în tabel:

1. Faceți clic pe butonul **Coloane** din partea dreaptă a capului de tabel.
2. Selectați coloanele pe care doriți să le vizualizați.

   Pentru a reveni la ecranul coloanelor implicite, faceți clic pe butonul **Resetare**.

Puteți obține informații suplimentare făcând clic pe linkul **Subiect** aferent fiecărui obiect. Se afișează fereastra **Detalii obiect**, care include următoarele informații:

- **Obiect trecut în carantină.** Tipul de obiect trecut în carantină, care poate fi e-mail sau atașament.
- **Trecut în carantină în.** Data și ora la care fișierul a fost izolat în carantină.
- **Stare.** Starea obiectului după ce a fost scanat. Starea arată dacă un e-mail este marcat ca fiind spam sau are conținut nedorit, sau dacă un atașament este infectat cu malware, este suspectat ca fiind infectat, nedorit sau nescanabil.
- **Denumire atașament.** Denumirea de fișier a atașamentului detectat de modulele de Filtrare a programelor periculoase sau atașamentelor.
- **Denumire program periculos.** Denumirea alocată amenințării de tip program periculos de cercetătorii de securitate ai Bitdefender. Aceste informații sunt disponibile numai dacă obiectul era infestat.
- **Punct detecție.** Un obiect este detectat fie la nivelul de transfer, fie într-un mailbox sau director public din Exchange Store.
- **Corespondență regulă.** Regula referitoare la politică identificată drept corespunzătoare amenințării.
- **Server.** Numele de gazdă al serverului pe care a fost detectată amenințarea.
- **IP expeditor.** Adresa IP a expeditorului.
- **Expeditor (De la).** Adresa e-mail a expeditorului este cea afișată în câmpul **De la** din titlu.
- **Destinatari.** Lista destinatarilor din câmpurile din titlul e-mail-ului **Către** și **Cc**.
- **Destinatari reali.** Lista adreselor e-mail ale utilizatorilor individuali cărora trebuia să le fie transmis e-mail-ul înainte de a fi trecut în carantină.
- **Subiect.** Subiectul e-mail-ului trecut în carantină.

Notă
Punctele de suspensie de la finalul textului indică faptul că o parte din text a fost omisă. În acest caz, treceți mausul deasupra textului pentru a-l vedea într-o casetă de instrumente.

11.3.2. Obiecte mutate în carantină

Mesajele e-mail și fișierele mutate în carantină de către modulul de protecție Exchange sunt salvate local pe server ca fișiere criptate. Folosind Control Center, aveți opțiunea de a restabili mesajele e-mail din carantină, precum și de a șterge sau salva orice fișiere sau e-mail-uri mutate în carantină.

Restaurarea e-mail-urilor trecute în carantină

Dacă decideți că un e-mail trecut în carantină nu reprezintă o amenințare, îl puteți elibera din carantină. Folosind Exchange Web Services, modulul de protecție Exchange trimite mesajele e-mail din carantină către toți destinatarii sub formă de atașament la un e-mail de notificare Bitdefender.

Notă
Doar e-mail-urile pot fi restaurate. Pentru a recupera un atașament trecut în carantină, trebuie să îl salvați pe un director local de pe serverul Exchange.

Pentru a restaura unul sau mai multe e-mail-uri:

1. Mergeți la pagina **Carantină**.
2. Selectați **Exchange** din selectorul de vederi disponibil în partea din dreapta sus a paginii.
3. Selectați casetele de bifare, în funcție de e-mail-urile pe care doriți să le recuperați.
4. Faceți clic pe butonul **Repornire** din partea de sus a tabelului. Se va afișa fereastra **Restaurare date de autentificare**.
5. Selectați datele de autentificare ale unui utilizator Exchange autorizat să transmită e-mail-urile care trebuie restaurate. Dacă datele de autentificare pe care intenționați să le folosiți sunt noi, trebuie să le adăugați mai întâi în secțiunea Administrare date de autentificare.

   Pentru a adăuga datele de autentificare necesare:

   a. Introduceți informațiile necesare în câmpurile corespunzătoare din capătul de tabel:
      - Numele de utilizator și parola utilizatorului Exchange.

Notă
Numele de utilizator trebuie să includă numele de domeniu, cum ar fi `user@domain` sau `domain\user`.

- Adresa de e-mail a utilizatorului Exchange, necesară numai atunci când adresa de e-mail este diferită de numele de utilizator.
- Adresa URL Exchange Web Services (EWS), necesară când funcția Exchange Autodiscovery nu funcționează. De obicei, este cazul serverelor Edge Transport într-o zonă DMZ.

b. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului. Noul set de date de autentificare este adăugat la tabel.

6. Faceți clic pe butonul **Restabilire**. Va apărea un mesaj de confirmare.

   Acțiunea solicitată este transmisă imediat serverelor țintă. După restabilirea unui e-mail, acesta este șters din carantină, iar înregistrarea corespunzătoare va dispărea din tabelul Carantină.

   Puteți verifica starea acțiunii de restabilire în oricare dintre aceste locații:

   - Coloana **Stare acțiune** din tabelul Carantină.
   - Pagina **Rețea > Sarcini**.

Salvarea fișierelor trecute în carantină

Dacă doriți să analizați sau să recuperați date din fișierele aflate în carantină, puteți salva fișierele într-un folder local pe serverul Exchange. Bitdefender Endpoint Security Tools decriptează fișierele și le salvează în locația specificată.

Pentru a salva unul sau mai multe fișiere trecute în carantină:

1. Mergeți la pagina **Carantină**.
2. Selectați **Exchange** din selectorul de vederi disponibil în partea din dreapta sus a paginii.
3. Filtrați datele din tabel pentru a vizualiza toate fișierele pe care doriți să le salvați, introducând termenii de căutare în câmpurile de titlu ale coloanelor.
4. Selectați casetele care corespund fișierelor din carantină pe care doriți să le restabiliți.
5. Faceți clic pe butonul **Salvare** din partea de sus a tabelului.

6. Introduceți calea în directorul de destinație de pe Serverul Exchange. Dacă directorul nu este disponibil pe server, va fi creat.

   Important
   Trebuie să excludeți acest director din scanarea de la nivelul sistemului de fișiere. În caz contrar, fișierele vor fi mutate în Carantina pentru calculatoare și mașini virtuale. Pentru mai multe informații, consultați capitolul „Excluderi” (p. 289).

7. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

   Puteți observa starea în curs în coloana **Stare acțiune**. De asemenea, puteți vizualiza starea acțiunii pe pagina **Rețea > Sarcini**.

Ștergerea automată a fișierelor din carantină

Implicit, fișierele aflate în carantină de mai mult de 30 zile sunt șterse automat. Puteți modifica această setare editând politica alocată Serverului Exchange administrat.

Pentru a schimba intervalul automat de ștergere pentru fișierele aflate în carantină:

1. Mergeți la pagina **Politici**.
2. Faceți clic pe denumirea politicii alocate Serverului Exchange care vă interesează.
3. Mergeți la pagina **Protecție Exchange > General**.
4. În secțiunea **Setări**, selectați numărul de zile rămase după care fișierele urmează să fie șterse.
5. Faceți clic pe **Salvare** pentru a aplica modificările.

Ștergerea manuală a fișierelor din carantină

Pentru a șterge unul sau mai multe obiecte trecute în carantină:

1. Mergeți la pagina **Carantină**.
2. Selectați **Exchange** din selectorul de vederi.
3. Selectați casetele de bifare corespunzătoare fișierelor pe care doriți să le ștergeți.
4. Faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

   Puteți observa starea în curs în coloana **Stare acțiune**.

Acțiunea solicitată este transmisă imediat serverelor țintă. După ce un fișier este șters, datele corespunzătoare vor dispărea din tabelul de Carantină.

Golirea Carantinei

Pentru a șterge toate obiectele trecute în carantină:

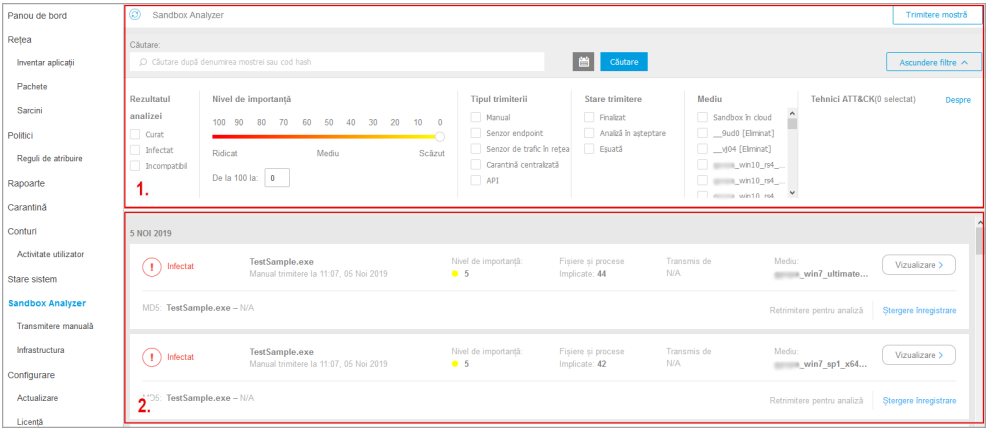
1. Mergeți la pagina **Carantină**.
2. Selectați **Exchange** din selectorul de vizualizări.
3. Faceți clic pe butonul **Golire Carantină**.

   Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

Sunt șterse toate datele din tabelul Carantină. Acțiunea solicitată este transmisă imediat obiectelor țintă din rețea.

12. UTILIZAREA SANDBOX ANALYZER

Pagina **Sandbox Analyzer** oferă o interfață unică pentru vizualizarea, filtrarea și căutarea trimiterilor automate și manuale către mediul sandbox. Pagina **Sandbox Analyzer** constă în următoarele două secțiuni:



Pagina Sandbox Analyzer

1. **Secțiunea de filtrare** vă permite să căutați și să filtrați trimiterile după anumite criterii: nume, cod hash, dată, rezultatul analizei, stare, mediu de detonare și tehnicile MITRE ATT&CK.
2. **Secțiunea de trimiteri** afișează toate fișierele trimise într-un format compact, cu informații detaliate despre fiecare.

În pagina Sandbox Analyzer, puteți face următoarele lucruri:

- Carduri de trimitere a filtrelor
- Vizualizați lista trimiterilor și detaliile analizei
- Retrimiterea mostrelor din secțiunea de trimiteri pentru a fi analizate
- Ștergere carduri trimitere
- Efectuați transmiteri manuale

12.1. Filtrarea înregistrărilor trimiterilor

Iată ce puteți face în secțiunea de filtrare:

- Filtrați fișierele trimise în funcție de anumite criterii. Pagina va încărca automat doar panourile cu evenimente de securitate compatibile cu criteriile selectate.
- Resetați filtrele selectând **Eliminare filtre**.
- Ascundeți secțiunea filtrelor, selectând **Ascundere filtre**. Puteți afișa din nou opțiunile ascunse selectând **Afișare filtre**.

Puteți filtra trimiterile Sandbox Analyzer în funcție de următoarele criterii:

- **Nume mostră și cod hash (MD5)**. Introduceți în fiecare câmp de căutare o parte din nume sau numele complet sau codul hash al mostrei pe care o căutați și apoi selectați opțiunea **Căutare** din partea dreaptă.
- **Data**. Pentru a filtra în funcție de dată:
  1. Accesați pictograma sub formă de calendar pentru a configura intervalul de timp al căutării.
  2. Definiți intervalul. Accesați butoanele **De la** și **Până la** din partea de sus a calendarului pentru a selecta datele care stabilesc intervalul de timp. De asemenea, puteți selecta o perioadă predeterminată din partea dreaptă a listei cu opțiuni, în raport cu momentul prezent (spre exemplu, în ultimele 30 de zile).

     De asemenea, puteți menționa ora și minutul pentru fiecare dată din intervalul de timp, utilizând opțiunile de sub calendar.
  3. Selectați **OK** pentru a aplica filtrul.
- **Rezultat analiză**. Selectați una sau mai multe dintre următoarele opțiuni:
  - **Sigură** – mostra este sigură.
  - **Infectată** – mostra este periculoasă.
  - **Nesuportat** – formatul mostrei nu permite detonarea în Sandbox Analyzer. Pentru a vizualiza lista completă a tipurilor și extensiilor de fișiere suportate de către Sandbox Analyzer, consultați „Tipuri și extensii de fișiere acceptate pentru trimitere manuală” (p. 571).
- **Nivel de importanță**. Valoarea arată cât de periculoasă este o mostră pe o scară de la 100 la 0 (zero). Cu cât scorul este mai mare, cu atât este mai periculoasă

mostra respectivă. Nivelul de importanță se aplică în cazul tuturor mostrelor transmise, inclusiv al mostrelor cu starea **Sigură** sau **Nesuportată**.

- **Tipul de transmitere**. Selectați una sau mai multe dintre următoarele opțiuni:
  - **Manual**. Sandbox Analyzer a primit mostra prin opțiunea **Transmitere manuală**.
  - **Senzor endpoint**. Bitdefender Endpoint Security Tools a trimis mostra către Sandbox Analyzer în baza setărilor politicii.
  - **Senzor trafic rețea**. Senzorul de rețea a trimis mostra către o instanță locală Sandbox Analyzer pe baza setărilor politicii.
  - **Carantină centralizată**. GravityZone a trimis mostra către o instanță locală Sandbox Analyzer pe baza politicilor de rețea.
  - **API**. Mostra a fost trimisă către o instanță locală Sandbox Analyzer utilizând metode API.
  - **Senzor ICAP**. Security Server a trimis mostra către o instanță locală Sandbox Analyzer după scanarea unui server ICAP.
- **Status transmitere**. Selectați una sau mai multe dintre următoarele căsuțe:
  - **Finalizat** – Sandbox Analyzer a livrat rezultatul analizei.
  - **În curs de analiză** – Sandbox Analyzer efectuează detonarea mostrei.
  - **Nereușit** – Sandbox Analyzer nu a putut detona mostra.
- **Mediu**. Aici este o listă a mașinilor virtuale disponibile pentru detonare, inclusiv instanța Sandbox Analyzer găzduită de Bitdefender. Selectați una sau mai multe casete pentru a vedea mostrele care au fost detonate în anumite medii.
- **Tehnicile ATT&CK**. Această opțiune de filtrare integrează cunoștințele de bază MITRE ATT&CK, dacă este cazul. Valorile tehnicilor ATT&CK se modifică în mod dinamic, în funcție de evenimentele de securitate.

  Accesați linkul **Despre** pentru a deschide Matricea ATT&CK într-o nouă filă.

12.2. Vizualizarea detaliilor analizei

Pagina **Sandbox Analyzer** afișează înregistrările trimiterilor pe zile, în ordine cronologică inversă. Panourile transmiterilor includ următoarele date:

- Rezultatul analizei
- Denumirea mostrei

- Tipul trimiterii
- Nivelul de importanță
- Fișiere și procese implicate
- Mediu de detonare
- Valoare hash (MD5)
- Tehnicile ATT&CK
- Statusul transmiterii atunci când un rezultat este indisponibil

Fiecare panou al unei transmiteri include un link către un raport de analiză HTML detaliat, dacă este disponibil. Pentru a deschide raportul, apăsați pe butonul **Vizualizare** din colțul din dreapta al înregistrării.

Raportul HTML oferă numeroase informații organizate pe mai multe niveluri, cu text descriptiv, grafice și capturi de ecran care ilustrează comportamentul mostrei în mediul de detonare. Acestea sunt informațiile pe care le puteți afla dintr-un raport HTML Sandbox Analyzer:

- Informații generale despre mostra analizată, cum ar fi: numele și clasificarea malware-ului, detaliile transmiterii (nume fișier, tipul și dimensiunea, codul hash, ora transmiterii și durata analizei).
- Rezultatele analizei comportamentale, care includ toate evenimentele de securitate surprinse în timpul detonării, organizate în secțiuni. Evenimentele de securitate se referă la următoarele:
  - Scriere / ștergere / mutare / duplicare / înlocuire fișiere în sistem și pe unitățile amovibile.
  - Executarea fișierelor nou create.
  - Modificări ale sistemului de fișiere.
  - Modificări ale aplicațiilor care rulează pe mașina virtuală.
  - Modificări ale barei de instrumente și ale meniului de Start din Windows.
  - Crearea / terminarea / injectarea proceselor.
  - Scrierea / ștergerea cheilor de regiștri.
  - Crearea obiectelor mutex.
  - Crearea / pornirea / oprirea / modificarea / interogarea / ștergerea serviciilor.
  - Modificarea setărilor de securitate ale browser-ului.
  - Modificarea setărilor de afișare ale Windows Explorer.
  - Adăugarea de fișiere la lista de excepții firewall.
  - Modificarea setărilor de rețea.
  - Activarea execuției la pornirea sistemului.
  - Conectarea la o gazdă la distanță.
  - Accesarea anumitor domenii.

- Transferul datelor către și dinspre anumite domenii.
- Accesarea adreselor URL, adreselor IP și a porturilor prin intermediul mai multor protocoale de comunicație.
- Verificarea indicatorilor mediului virtual.
- Verificarea indicatorilor instrumentelor de monitorizare.
- Crearea de capturi de ecran.
- Hook SSDT, IDT, IRP.
- Dump-uri de memorie pentru procese suspecte
- Apelări ale funcțiilor Windows API.
- Inactivitate pentru o anumită perioadă de timp pentru întârzierea execuției.
- Crearea de fișiere cu acțiunile care trebuie executate la anumite intervale de timp.

Important
Rapoartele HTML sunt disponibile doar în limba engleză, indiferent care este limba utilizată pentru GravityZone Control Center.

12.3. Retrimiterea mostrelor

Din secțiunea de trimiteri, puteți retrimite mostrele deja detonate către o instanță locală Sandbox Analyzer, fără a fi nevoie să le încărcați din nou. Puteți face acest lucru pentru mostrele care au fost trimise anterior către instanța locală Sandbox Analyzer prin orice senzor sau metodă, automat, manual sau prin API.

Pentru retrimiterea unei mostre:

1. Selectați **Retrimitere pentru analiză** din secțiunea de trimiteri.
2. În fereastra de configurare, păstrați setările trimiterii anterioare sau modificați-le după cum urmează:
   a. Accesați **Administrare imagini** și selectați imaginea de mașină virtuală pe care doriți să o utilizați pentru detonare.
   b. Accesați **Configurări detonare** și configurați următoarele setări:
      i. **Limită de timp pentru detonarea mostrei (minute)**. Alocați un interval de timp fix pentru finalizarea analizei mostrei. Valoarea implicită este 4 minute, însă uneori analiza poate dura mai mult. La sfârșitul intervalului configurat, Sandbox Analyzer întrerupe analiza și generează un raport pe baza datelor colectate până la acel moment. Dacă este întreruptă, analiza poate conține rezultate imprecise.

ii. **Numărul de reluări permise**. În cazul erorilor neașteptate, Sandbox Analyzer încearcă să detoneze mostra după cum a fost configurat, până la finalizarea analizei. Valoarea implicită este 2. Aceasta înseamnă că Sandbox Analyzer va mai încerca de încă două ori să detoneze mostra în cazul apariției unei erori.

iii. **Pre-filtrare**. Selectați această opțiune pentru a exclude de la detonare mostrele deja analizate.

iv. **Acces la internet în timpul detonării**. În timpul analizei, unele mostre necesită conexiune la internet pentru finalizarea analizei. Pentru a obține cele mai bune rezultate, se recomandă să mențineți activată această opțiune.

c. În secțiunea **Profil detonare**, ajustați nivelul de complexitate al analizei comportamentale, ceea ce va afecta rata de procesare a Sandbox Analyzer. De exemplu, dacă este setat pe **Ridicat**, Sandbox Analyzer ar efectua o analiză mai precisă pentru mai puține mostre decât modul **Mediu** sau **Redus**, în același interval de timp.

3. Selectați **Retrimitere**.

După retrimitere, pagina **Sandbox Analyzer** afișează o nouă trimitere și intervalul de păstrare a datelor aferent mostrei respective se prelungește corespunzător.

Notă
Opțiunea **Retrimitere pentru analiză** este disponibilă pentru mostrele care încă există în spațiul de stocare a datelor Sandbox Analyzer. Asigurați-vă că păstrarea datelor este configurată în pagina **Sandbox Analyzer > Sandbox Manager** a setărilor politicii.

12.4. Ștergerea înregistrărilor trimiterilor

Pentru a șterge înregistrarea unei trimiteri de care nu mai aveți nevoie:

1. Accesați înregistrarea trimiterii pe care doriți să o ștergeți.
2. Selectați opțiunea **Ștergere înregistrare** din stânga.
3. Faceți clic pe **Da** pentru a confirma acțiunea.

Notă
Urmând acești pași, veți șterge doar înregistrarea trimiterii. Informațiile privind trimiterea vor fi în continuare disponibile în raportul **Rezultate Sandbox Analyzer**

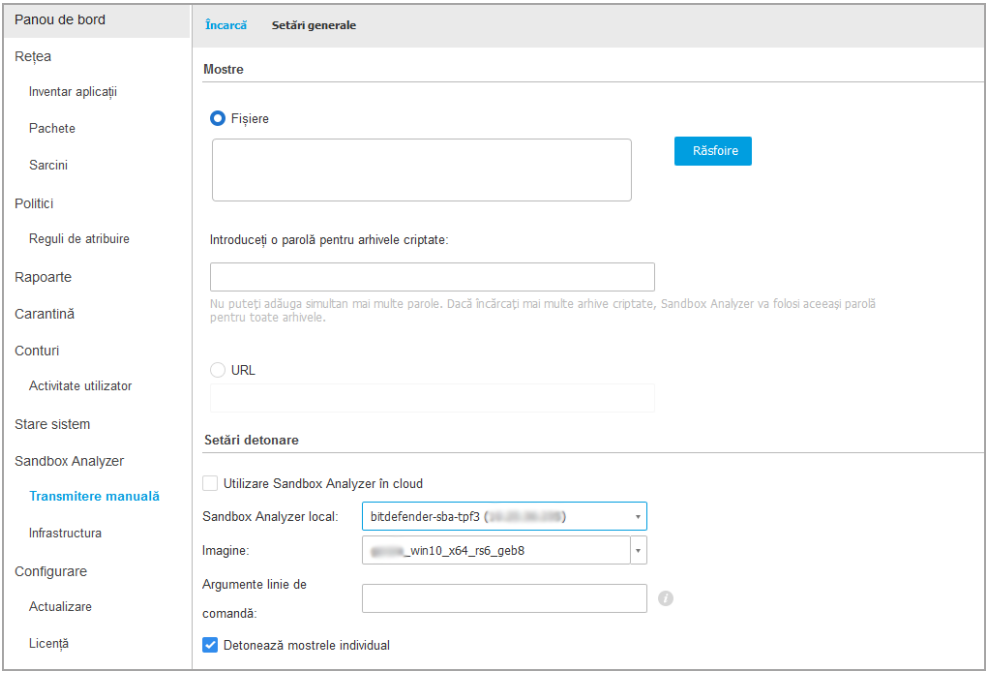
(Perimat). Totuși, acest raport va fi disponibil în continuare numai pentru o perioadă limitată de timp.

12.5. Transmitere manuală

Din fereastra **Sandbox Analyzer > Transmitere manuală**, puteți trimite mostre de obiecte suspecte către Sandbox Analyzer, pentru a stabili dacă reprezintă o amenințare sau dacă fișierele respective sunt inofensive. De asemenea, puteți accesa pagina **Transmiteri manuale** selectând opțiunea **Trimite o mostră** din partea din dreapta sus a secțiunii de filtrare din pagina Sandbox Analyzer.

Notă

Transmiterea manuală către Sandbox Analyzer este compatibilă cu toate browser-ele cerute de Control Center, cu excepția Internet Explorer 9. Pentru a trimite obiecte către Sandbox Analyzer, conectați-vă la Control Center utilizând orice alt browser compatibil, dintre cele menționate la „Conectarea la Control Center" (p. 19).



Sandbox Analyzer > Transmitere manuală

Pentru a trimite mostre către Sandbox Analyzer:

1. În pagina **Încărcare**, în secțiunea **Mostre**, selectați tipul de obiect:
   a. **Fișiere**. Clic pe butonul **Navigare** pentru a selecta obiectele pe care doriți să le trimiteți pentru analiza comportamentală. În cazul arhivelor protejate prin parolă, puteți defini o parolă pentru fiecare sesiune de încărcare într-un câmp dedicat. În timpul procesului de analiză, Sandbox Analyzer aplică parola specificată tuturor arhivelor trimise.
   b. **URL**. Completați câmpul aferent cu orice URL pe care doriți să îl analizați. Puteți trimite doar un URL pe fiecare sesiune.
2. În secțiunea **Setări detonare**, configurați parametri de analiză pentru secțiunea curentă:
   - Instanța Sandbox Analyzer pe care doriți să o utilizați. Puteți selecta fie instanța Cloud, fie instanța Sandbox Analyzer instalată local.

     Dacă alegeți să utilizați o instanță locală Sandbox Analyzer, puteți selecta mai multe mașini virtuale unde să trimiteți mostrele simultan.
   - **Argumente linie de comandă**. Adăugați câte argumente de linie de comandă doriți, separate prin spațiu, pentru a modifica modul de operare al anumitor programe, cum ar fi fișierele executabile. Argumentele în linia de comandă se aplică în cazul tuturor mostrelor transmise în timpul analizei.
   - **Detonare individuală mostre**. Selectați căsuța pentru a analiza individual fișierele grupate.
3. În secțiunea **Profil detonare**, ajustați nivelul de complexitate al analizei comportamentale, ceea ce va afecta rata de procesare a Sandbox Analyzer. De exemplu, dacă este setat pe **Ridicat**, Sandbox Analyzer ar efectua o analiză mai precisă pentru mai puține mostre decât modul **Mediu** sau **Redus**, în același interval de timp.
4. În pagina **Setări generale**, puteți efectua configurări aplicabile pentru toate transmiterile manuale, indiferent de sesiune:
   a. **Limită de timp pentru detonarea mostrei (minute)**. Alocați un interval de timp fix pentru finalizarea analizei mostrei. Valoarea implicită este 4 minute, însă uneori analiza poate dura mai mult. La sfârșitul intervalului configurat, Sandbox Analyzer întrerupe analiza și generează un raport pe baza datelor colectate până la acel moment. Dacă este întreruptă, analiza poate conține rezultate imprecise.

b. **Numărul de reluări permise**. În cazul erorilor neașteptate, Sandbox Analyzer încearcă să detoneze mostra după cum a fost configurat, până la finalizarea analizei. Valoarea implicită este 2. Aceasta înseamnă că Sandbox Analyzer va mai încerca de încă două ori să detoneze mostra în cazul apariției unei erori.

c. **Pre-filtrare**. Selectați această opțiune pentru a exclude de la detonare mostrele deja analizate.

d. **Acces la internet în timpul detonării**. În timpul analizei, unele mostre necesită conexiune la internet pentru finalizarea analizei. Pentru a obține cele mai bune rezultate, se recomandă să mențineți activată această opțiune.

e. Selectați **Salvare** pentru a salva modificările.

5. Reveniți la pagina **Încărcare**.
6. Faceți clic pe **Trimite**. O bară de progres arată starea trimiterii.

   După transmitere, pagina **Sandbox Analyzer** afișează un nou panou. Atunci când analiza se încheie, panoul vă oferă rezultatul și detaliile aferente.

Notă
Pentru a transmite manual mostre către Sandbox Analyzer, trebuie să aveți drepturi de **Administrare rețele**.

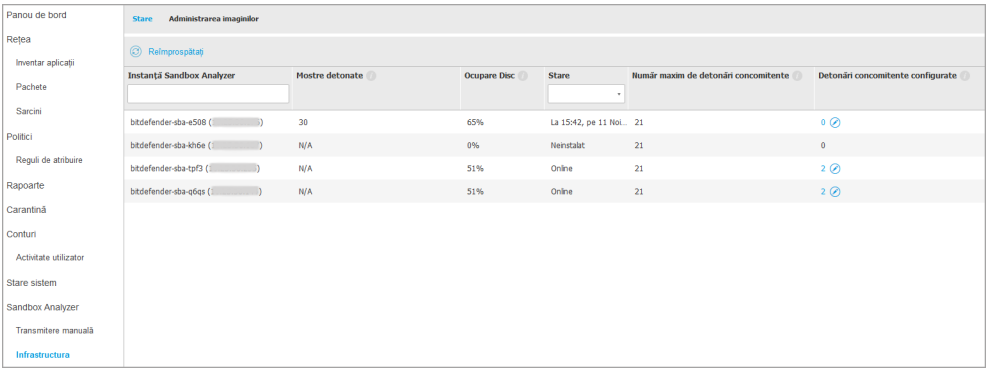
12.6. Administrarea infrastructurii Sandbox Analyzer

În secțiunea **Sandbox Analyzer > Infrastructură**, puteți efectua următoarele acțiuni privind instanța Sandbox Analyzer instalată local:

- Verificarea stării instanței Sandbox Analyzer
- Configurarea detonărilor simultane
- Verificarea stării imaginilor de mașină virtuală
- Configurarea și administrarea imaginilor de mașină virtuală

12.6.1. Verificarea stării Sandbox Analyzer

După instalarea și configurarea Aplicației virtuale Sandbox Analyzer pe hypervisor-ul ESXi, puteți obține informații privind instanța locală Sandbox Analyzer din pagina **Stare**.



Sandbox Analyzer > Infrastructură > Stare

Tabelul vă va oferi următoarele informații:

- **Numele instanței Sandbox Analyzer**. Fiecare nume corespunde unei instanțe Sandbox Analyzer instalată pe un hypervisor ESXi. Puteți instala Sandbox Analyzer pe mai mulți hypervisori ESXi.
- **Mostre detonate**. Valoarea indică numărul de mostre care au fost analizate din momentul primei licențieri a instanței Sandbox Analyzer.
- **Utilizarea unității de disc**. Procentul indică în ce măsură a fost ocupată unitatea de disc de către Sandbox Analyzer pe spațiul de stocare a datelor.
- **Stare**. În această coloană puteți vedea dacă instanța Sandbox Analyzer este online, offline, nu este instalată, instalarea este în derulare sau instalarea a eșuat.
- **Numărul maxim de detonări simultane**. Valoarea reprezintă numărul maxim de mașini virtuale pe care Sandbox Analyzer le poate crea pentru detonarea mostrelor. Într-un moment dat, o mașină virtuală poate efectua o detonare. Numărul mașinilor virtuale este determinat de numărul resurselor de hardware disponibile pe ESXi.
- **Detonări simultane configurate**. Acesta este numărul efectiv de mașini virtuale create pe baza licenței disponibile.
- **Utilizare proxy**. Acționați butonul Pornire/Oprire pentru a activa sau dezactiva comunicarea dintre GravityZone Control Center și instanțele Sandbox Analyzer printr-un server proxy. Pentru configurarea unui server proxy, mergeți

la **Configurare > Proxy** în meniul principal al Control Center. Dacă nu este configurat niciun server proxy, Control Center va ignora această opțiune.

Pentru detalii despre configurarea proxy, consultați **Instalarea protecției> Instalarea și configurarea GravityZone >Configurare setări Control Center > Proxy** în Ghidul de instalare GravityZone.

Notă
Control Center utilizează doar acest proxy pentru a comunica cu instanțele Sandbox Analyzer On-Premises. Pentru a comunica cu instanța din cloud a Sandbox Analyzer, Control Center utilizează serverul proxy configurat în pagina setărilor de politică a Sandbox Analyzer.
Acest server proxy este, de asemenea, diferit de cel configurat în pagina **General > Setări** a setărilor de politică, care asigură comunicarea dintre endpoint-uri și componentele GravityZone.

Puteți căuta și filtra coloanele după numele și starea instanței Sandbox Analyzer. Utilizați butoanele din colțul din dreapta sus al tabelului pentru a reîmprospăta pagina și pentru a afișa și ascunde filtrele și coloanele.

12.6.2. Configurarea detonărilor simultane

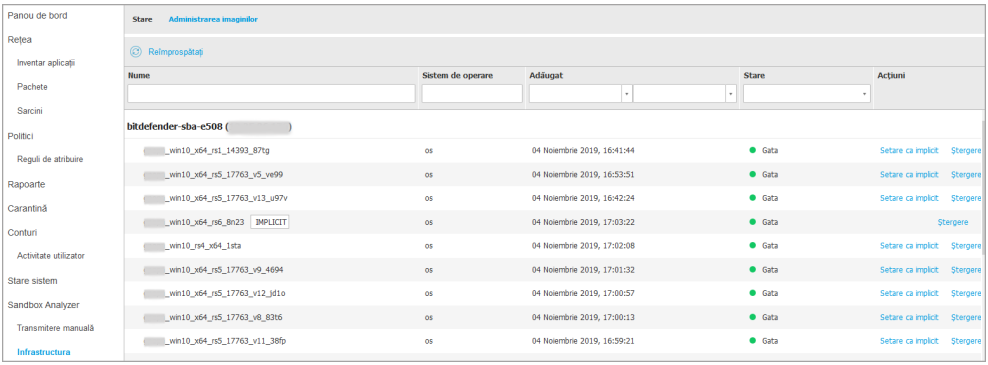
În pagina **Stare**, puteți configura detonările simultane, acestea reprezentând numărul mașinilor virtuale care pot executa și detona mostre simultan pe o instanță Sandbox Analyzer. Numărul de detonări simultane depinde de resursele de hardware și de distribuirea licențelor de utilizator pentru mai multe instanțe Sandbox Analyzer.

Pentru configurarea detonărilor simultane:

1. Selectați numărul sau pictograma **Editare** din coloana **Detonări simultane configurate**.
2. În noua fereastră, specificați în câmpul corespunzător numărul detonărilor simultane pe care doriți să le alocați instanței Sandbox Analyzer.
3. Faceți clic pe **Save**.

12.6.3. Verificarea stării imaginilor de mașină virtuală

Sandbox Analyzer utilizează imagini de mașină virtuală ca medii de detonare pentru efectuarea analizei comportamentale asupra mostrelor trimise. Puteți verifica starea mașinilor virtuale în pagina **Administrare imagini**.



Sandbox Analyzer > Infrastructură > Administrare imagini

Tabelul vă oferă următoarele informații:

- **Numele** imaginilor disponibile de mașină virtuală, așa cum este specificat în consola aplicației Sandbox Analyzer. Mai multe imagini de mașină virtuală sunt grupate în cadrul aceleiași instanțe Sandbox Analyzer.
- **Sistemul de operare**, așa cum este specificat în consola aplicației Sandbox Analyzer.
- Momentul în care a fost adăugată imaginea de mașină virtuală.
- **Stare**. În această coloană puteți afla dacă o imagine de mașină virtuală este nouă și poate fi pregătită pentru detonare, dacă este gata de detonare sau dacă procesul de pregătire a eșuat.
- **Acțiuni**. În această coloană puteți afla cum pot fi utilizate imaginile de mașină virtuală, în funcție de starea acestora: crearea de imagini pentru detonare, definirea lor ca mediu implicit de detonare sau ștergerea acestora.

12.6.4. Configurarea și administrarea imaginilor de mașină virtuală

Crearea mașinilor virtuale de detonare

Pentru detonarea mostrelor utilizând instanța Sandbox Analyzer, este necesar să creați mașini virtuale dedicate. Pagina **Administrare imagini** vă permite să creați mașini virtuale de detonare, în măsura în care ați adăugat în prealabil imagini de mașină virtuală în consola aplicației Sandbox Analyzer.

Notă
Pentru a afla cum puteți adăuga imagini de mașini virtuale în consola aplicației Sandbox Analyzer, consultați capitolul **Instalarea aplicației virtuale Sandbox Analyzer Virtual** din Ghidul de instalare GravityZone.

Pentru crearea mașinilor virtuale de detonare, în coloana **Acțiuni**, selectați opțiunea **Creare imagine** pentru imaginile de mașină virtuală care au starea: **Nou – Necesită creare**. Crearea unei mașini virtuale durează de obicei între 15 și 30 de minute, în funcție de dimensiunea acesteia. La finalizarea procesului de creare, starea mașinii virtuale se modifică în **Pregătit**.

Configurarea unei mașini virtuale implicite

O instanță Sandbox Analyzer poate avea mai multe imagini instalate și configurate ca mașini virtuale de detonare. În cazul trimiterilor automate, Sandbox Analyzer va utiliza prima imagine de mașină virtuală creată pentru detonarea mostrelor.

Puteți modifica acest comportament configurând o imagine de mașină virtuală implicită. Pentru a face acest lucru, selectați opțiunea **Setare ca implicit** pentru imaginea de mașină virtuală preferată.

Ștergerea mașinilor virtuale

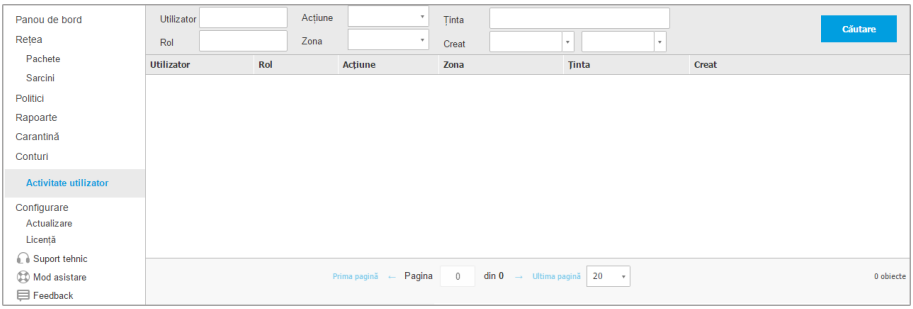
Pentru a șterge o imagine de mașină virtuală din pagina **Administrare imagini**, selectați **Ștergere** în coloana **Acțiuni**. În fereastra de confirmare, selectați **Ștergere imagine**.

13. JURNALUL ACTIVITĂȚII UTILIZATORULUI

Control Center listează toate operațiunile și acțiunile întreprinse de către utilizatori. Lista de activități ale utilizatorului include următoarele evenimente, conform nivelului drepturilor administrative pe care le dețineți:

- Conectarea și deconectarea
- Crearea, editarea, redenumirea și ștergerea rapoartelor
- Adăugarea și eliminarea portlet-urilor din panoul de bord
- Crearea, editarea și ștergerea acreditărilor
- Crearea, modificarea, descărcarea și ștergerea pachetelor de rețea
- Crearea de sarcini de rețea
- Inițierea, încheierea, anularea și oprirea proceselor de depanare pe mașinile afectate
- Crearea, editarea, redenumirea și ștergerea conturilor de utilizator
- Ștergerea sau mutarea stațiilor de lucru între grupuri
- Crearea, mutarea, redenumirea și ștergerea grupurilor
- Ștergerea și restaurarea fișierelor aflate în carantină
- Crearea, editarea și ștergerea conturilor de utilizator
- Crearea, editarea și ștergerea regulilor privind drepturile de acces.
- Crearea, editarea, redenumirea, atribuirea și eliminarea politicilor
- Editarea setărilor de autentificare pentru conturile GravityZone.
- Crearea, editarea, sincronizarea și ștergerea integărilor cu Amazon EC2
- Crearea, editarea, sincronizarea și ștergerea integărilor cu Microsoft Azure EC2
- Actualizarea aplicației GravityZone.

Pentru a examina istoricul activității utilizatorului, mergeți la pagina **Conturi > Activitate utilizator** și selectați tipul de vedere de rețea dorit din selectorul de vederi.



Pagina Activităților utilizatorului

Pentru a afișa evenimentele înregistrate care vă interesează, trebuie să definiți o căutare. Completați câmpurile disponibile cu criteriile de căutare și faceți clic pe butonul **Căutare**. Toate înregistrările care se potrivesc criteriilor dvs. vor fi afișate în tabel.

Coloanele din tabel vă oferă informații utile despre evenimentele din listă:

- Numele de utilizator al persanei care a efectuat acțiunea.
- Rolul utilizatorului.
- Acțiunea care a cauzat evenimentul.
- Tip de obiect de consolă afectat de acțiune.
- Obiect de consolă specific afectat de acțiune.
- Momentul în care a avut loc evenimentul.

Pentru a sorta evenimentele pe baza unei anumite coloane, faceți clic pe titlul coloanei. Faceți clic pe titlul coloanei din nou pentru a inversa ordinea sortării.

Pentru a vizualiza informații detaliate despre un eveniment, selectați-l și verificați secțiunea de sub tabel.

14. UTILIZAREA INSTRUMENTELOR

14.1. Injectare instrumente personalizate cu HVI

Bitdefender HVI vă eliberează de povara remedierii problemelor, culegerii datelor de analiză, sau a executării sarcinilor periodice de întreținere pe mașinile virtuale din mediul dumneavoastră Citrix, permițându-vă să injectați din mers instrumente de la terți în sistemele de operare găzduite. Aceste operații sunt efectuate prin intermediul API-urilor Direct Inspect (nu este necesară conectivitatea TCP/IP) și fără perturbarea beneficiarilor. În acest scop, instrumentele trebuie să fie capabile să ruleze silențios.

GravityZone vă oferă spațiu de 3 GB pentru a vă păstra instrumentele în siguranță și de unde să injectați în interiorul sistemelor de operare găzduite.

Pentru încărcarea kit-urilor de instrumente în GravityZone:

1. Descărcați cea mai recentă versiune a kit-ului instrumentului în computerul dumneavoastră.
2. Arhivați kit-ul într-un fișier ZIP.
3. Conectați-vă la GravityZone Control Center și efectuați clic pe meniul **Instrumente** din colțul de jos stânga al paginii. Se afișează pagina **Centru gestionare instrumente**.
4. Efectuați clic pe butonul de încărcare corespunzător din partea de sus a tabelului, în funcție de sistemul de operare de destinație: **Încărcare instrument Windows** sau **Încărcare instrument Linux**.
5. Dacă instrumentul este pentru Windows, trebuie să selectați și arhitectura de computer aplicabilă din meniul derulant.
6. Localizați fișierul ZIP, selectați-l și efectuați clic pe **Deschidere**.

   Pentru fișierele mari s-ar putea să trebuiască să așteptați câteva minute până la finalizarea descărcării. Când s-a terminat, instrumentul se adaugă în tabel iar bara de progres de deasupra tabelului actualizează informațiile privind spațiul rămas disponibil pentru viitoare încărcări.

Pe lângă numele instrumentului, tabelul mai afișează și alte detalii utile, cum ar fi:

- Sistemul de operare și platforma pe care rulează instrumentul.

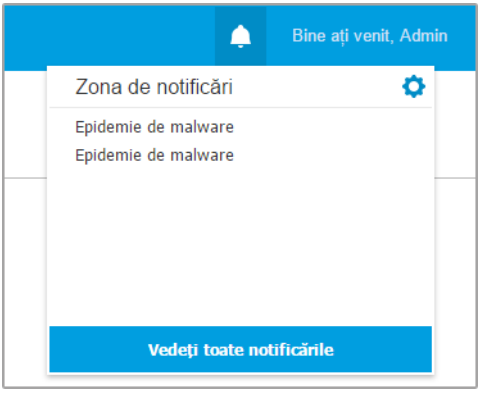
- O scurtă descriere a instrumentului. Puteți modifica acest câmp oricând, dacă doriți.
- Numele utilizatorului care a încărcat instrumentul.
- Stare încărcare. Verificați acest câmp pentru a vă asigura că instrumentul a fost încărcat cu succes.
- Data și ora la care s-a efectuat încărcarea.

Puteți programa prin intermediul politicilor când doriți să fie injectate instrumentele, sau le puteți injecta oricând rulând sarcinile de la pagina **Rețea**.

Când nu mai utilizați instrumentele, selectați-le și efectuați clic pe butonul **Ștergere** din partea de sus a tabelului, pentru a le șterge. Va trebui să confirmați efectuând clic pe **Da**.

15. NOTIFICĂRI

În funcție de evenimentele care ar putea apărea în întreaga rețea, Control Center va afișa diverse notificări pentru a vă informa cu privire la starea de securitate a mediului dumneavoastră. Notificările vor fi afișate în **Zona de notificări**, situată în partea dreaptă a Control Center.



Zona de notificări

Atunci când în rețea sunt detectate evenimente noi, pictograma din colțul din dreapta sus al Control Center indică numărul de evenimente detectate recent. La efectuarea unui clic pe pictogramă se afișează Zona de notificare ce conține lista evenimentelor detectate.

15.1. Tipuri de notificări

Aceasta este lista tipurilor de notificări disponibile:

Epidemie de malware

Această notificare este trimisă utilizatorilor care au cel puțin 5 % din toate obiectele lor de rețea administrate infectate de aceeași program periculos.

Puteți configura pragul pentru epidemia de malware după necesități în fereastra **Setări notificări**. Pentru mai multe informații, consultați capitolul „Configurarea setărilor de notificare” (p. 546).

Amenințările detectate de către HyperDetect nu fac obiectul acestei notificări.

Disponibilitate format syslog: JSON, CEF

Licența expiră

Această notificare este trimisă cu 30, 7 și 1 zi înainte de expirarea licenței.

Pentru a vedea această notificare, este necesar să aveți drepturi de **Gestionare companie**.

Disponibilitate format syslog: JSON, CEF

Limita de utilizare a licenței a fost atinsă

Această notificare este trimisă atunci când au fost utilizate toate licențele disponibile .

Disponibilitate format syslog: JSON, CEF

Limita de utilizare a licenței este pe cale de a fi atinsă

Această notificare este trimisă atunci când au fost folosite 90 % din licențele disponibile.

Pentru a vedea această notificare, este necesar să aveți drepturi de **Gestionare companie**.

Disponibilitate format syslog: JSON, CEF

Limita de utilizare a licenței pentru servere a fost atinsă

Această notificare este trimisă atunci când numărul de servere protejate atinge limita specificată pe cheia dvs. de licență.

Pentru a vedea această notificare, este necesar să aveți drepturi de **Gestionare companie**.

Disponibilitate format syslog: JSON, CEF

Limita de utilizare a licenței pentru servere este pe cale de a fi atinsă

Această notificare este trimisă atunci când au fost folosite 90% din utilizările de licență pentru servere.

Pentru a vedea această notificare, este necesar să aveți drepturi de **Gestionare companie**.

Disponibilitate format syslog: JSON, CEF

Limita de utilizare a licenței Exchange a fost atinsă

Această notificare este trimisă de fiecare dată când numărul de căsuțe de e-mail protejate de pe serverele dvs. Exchange atinge limita maximă prevăzută pentru cheia dvs. de licență.

Pentru a vedea această notificare, este necesar să aveți drepturi de **Gestionare companie**.

Disponibilitate format syslog: JSON, CEF

Date invalide de autentificare utilizator Exchange

Această notificare este trimisă atunci când o sarcină de scanare la cerere nu a putut fi lansată pe serverul Exchange țintă datorită datelor de autentificare utilizator Exchange eronate.

Disponibilitate format syslog: JSON, CEF

Stare upgrade

Această notificare se trimite săptămânal, dacă în rețeaua dvs. se găsesc versiuni vechi ale produsului.

Disponibilitate format syslog: JSON, CEF

Actualizare disponibilă

Această notificare vă informează cu privire la disponibilitatea unei noi actualizări GravityZone, a unui nou pachet sau a unui nou produs.

Disponibilitate format syslog: JSON, CEF

Conexiune Internet

Această notificare este trimisă atunci când se detectează modificări privind conectivitatea la internet de către următoarele procese:

- Validare licență
- Obținerea unei Solicitări de semnare certificat Apple
- Comunicarea cu dispozitivele mobile Apple și Android
- Accesarea contului MyBitdefender

Disponibilitate format syslog: JSON, CEF

Conexiune SMTP

Această notificare se trimite de fiecare dată când GravityZone Bitdefender detectează modificări privind conectivitatea serverului de mail.

Disponibilitate format syslog: JSON, CEF

Utilizatori dispozitive mobile fără adresă e-mail

Această notificare se trimite după adăugarea dispozitivelor mobile la mai mulți utilizatori, atunci când unul sau mai mulți utilizatori selectați nu au o adresă de e-mail specificată pentru contul lor. Scopul acestei notificări este de a vă avertiza că utilizatorii care nu au o adresă de e-mail specificată nu pot înregistra dispozitivele mobile care le sunt atribuite, deoarece detaliile de activare se trimit în mod automat prin e-mail.

Pentru detalii privind adăugarea dispozitivelor mobile pentru mai mulți utilizatori, consultați Ghidul de instalareGravityZone.

Disponibilitate format syslog: JSON, CEF

Backup baza de date

Această notificare vă informează în legătură cu starea unui backup planificat al bazei de date, indiferent dacă acesta este finalizat sau nu cu succes. Dacă backup-ul bazei de date a eșuat, mesajul de notificare va afișa și motivul eșuării.

Pentru detalii privind configurarea copiilor de rezervă ale bazei de date GravityZone, consultați Ghidul de instalare GravityZone.

Disponibilitate format syslog: JSON, CEF

Malware Exchange detectat

Această notificare vă informează atunci când se detectează malware pe un server Exchange din rețeaua dumneavoastră.

Disponibilitate format syslog: JSON, CEF

Anti-Exploit avansat

Această notificare vă informează când modulul Anti-Exploit avansat a detectat o tentativă de exploit în rețeaua dumneavoastră.

Disponibilitate format syslog: JSON, CEF

Eveniment antimalware

Această notificare vă informează atunci când se detectează malware pe o stație de lucru din rețeaua dumneavoastră. Această notificare este creată pentru fiecare detecție de malware, oferind detalii despre endpoint-ul infectat (nume, IP, agent instalat), tipul scanării, malware-ul detectat, versiunea semnăturii, momentul detecției și tipul motorului de scanare.

Disponibilitate format syslog: JSON, CEF

Integrare nesincronizată

Această notificare este transmisă dacă integrarea cu o platformă de virtualizare nu s-a putut sincroniza cu GravityZone. În setările de notificare, puteți selecta integrările în cazul cărora doriți să fiți informat la apariția unei erori. Puteți afla mai multe informații referitoare la starea de sincronizare în detaliile notificării.

Disponibilitate format syslog: JSON, CEF

Eveniment Antiphishing

Această notificare vă informează de fiecare dată când agentul stației de lucru blochează accesul la o pagină de web cunoscută pentru tentative de phishing.

Această notificare vă oferă, de asemenea, detalii precum stația de lucru care a încercat să acceseze site-ul nesigur (nume și IP), agentul instalat sau URL-ul blocat.

Disponibilitate format syslog: JSON, CEF

Eveniment Firewall

Prin această notificare sunteți informat de fiecare dată când modulul firewall al unui agent instalat a blocat scanarea unui port sau accesul la rețea al unei aplicații, în conformitate cu politica aplicată.

Disponibilitate format syslog: JSON, CEF

Eveniment ATC/SDI

Această notificare se trimite de fiecare dată când o aplicație potențial periculoasă este detectată și blocată pe o stație de lucru din rețeaua dumneavoastră. Veți găsi detalii despre tipul, numele și calea aplicației, precum și ID-ul și calea procesului principal și linia de comandă care a inițializat procesul, dacă este cazul.

Disponibilitate format syslog: JSON, CEF

Eveniment Control utilizator

Această notificare se trimite de fiecare dată când activitatea unui utilizator, precum navigarea pe internet sau o aplicație software este blocată de clientul instalat pe stația de lucru în conformitate cu politica aplicată.

Disponibilitate format syslog: JSON, CEF

Eveniment privind protecția datelor

Această notificare se trimite de fiecare dată când traficul de date este blocat pe o stație de lucru conform regulilor de protecție a datelor.

Disponibilitate format syslog: JSON, CEF

Eveniment Module produs

Această notificare se trimite de fiecare dată când un modul de securitate al unui agent instalat este activat sau dezactivat.

Disponibilitate format syslog: JSON, CEF

Eveniment stare Security Server

Acest tip de notificare oferă informații despre modificările de stare ale unui anumit server Security Server instalat în rețeaua dumneavoastră. Modificările de stare ale Security Server se referă la următoarele evenimente: activat /

dezactivat, actualizare produs, actualizare conținut de securitate și repornire necesară.

Disponibilitate format syslog: JSON, CEF

Eveniment Security Server suprasolicitat

Această notificare este transmisă atunci când sarcina de scanare pe un Security Server din rețeaua dumneavoastră depășește pragul definit.

Disponibilitate format syslog: JSON, CEF

Eveniment Înregistrare produs

Această notificare vă informează atunci când starea de înregistrare a unui agent instalat în rețeaua dumneavoastră s-a modificat.

Disponibilitate format syslog: JSON, CEF

Verificare autentificare

Această notificare vă informează atunci când un alt cont GravityZone, în afară de contul dumneavoastră, a fost folosit pentru autentificarea în Control Center folosind un dispozitiv necunoscut.

Disponibilitate format syslog: JSON, CEF

Autentificare de pe un nou dispozitiv

Această notificare vă informează atunci când contul dvs. GravityZone a fost folosit pentru autentificarea în Control Center de la un dispozitiv pe care nu l-ați mai utilizat înainte în acest scop. Notificarea este configurată automat pentru a fi vizibilă atât în Control Center, cât și pe e-mail și puteți doar să o vizualizați.

Disponibilitate format syslog: JSON, CEF

Certificatul expiră la

Această notificare vă informează că expiră un certificat de securitate. Notificarea este trimisă cu 30, șapte și o zi înainte de data expirării.

Disponibilitate format syslog: JSON, CEF

Actualizare GravityZone

Notificarea este transmisă când se efectuează o actualizare GravityZone. În cazul unei erori, actualizarea va rula din nou în 24 de ore.

Disponibilitate format syslog: JSON, CEF

Stare sarcini

Această notificare vă informează fie de fiecare dată când se modifică o stare a unei sarcini, fie numai atunci când se finalizează o sarcină, conform preferințelor dvs.

Disponibilitate format syslog: JSON, CEF

Server de actualizări neactualizat

Această notificare este trimisă atunci când un server de actualizări din rețeaua dvs. are conținutul de securitate neactualizat.

Disponibilitate format syslog: JSON, CEF

Eveniment incidente în rețea

Această notificare este trimisă de fiecare dată când modulul Network Attack Defense detectează o tentativă de atac în rețeaua dumneavoastră. De asemenea, această notificare vă informează dacă tentativa de atac a fost efectuată din afara rețelei sau de pe un endpoint compromis din cadrul rețelei. Alte informații includ date despre endpoint, tehnici de atac, adresa IP a atacatorului și acțiunile întreprinse de modulul Network Attack Defense.

Disponibilitate format syslog: JSON, CEF

Violare de memorie detectată

Această notificare vă informează atunci când HVI detectează un atac ce afectează memoria mașinilor virtuale protejate din mediul Citrix Xen. Notificarea vă oferă informații importante, cum ar fi denumirea și IP-ul mașinii infectate, descrierea incidentului, sursa și ținta atacului, acțiunile întreprinse pentru eliminarea amenințării și timpul de detecție.

Se generează notificări pentru următoarele incidente:

- Tentative de utilizare a unei zone de memorie în mod diferit față de cum era intenționat de hypervisor, prin Tabele de pagini extinse (EPT).
- Tentative ale unor procese de a injecta cod în alte procese.
- Tentative de modificare a adreselor proceselor în tabelele de traducere.
- Tentative de modificare a valorilor Model Specific Registers (MSR).
- Tentative de modificare a conținutului anumitor obiecte tip driver sau a Tabelei de descriptori de întrerupere (IDT).
- Tentative de încărcare a anumitor regiștri de control (CR) cu valori nevalide.

- Tentative de încărcare a anumitor Regiștri de control extins (XCR) cu valori nevalide.
- Tentative de modificare a tabelelor de descriptori globali sau de întrerupere

Notă
Caracteristica HVI poate fi disponibilă pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Disponibilitate format syslog: JSON, CEF

Aplicație nouă în inventarul de aplicații

Această notificare vă informează atunci când modulul Control aplicații detectează o nouă aplicație instalată pe stațiile de lucru monitorizate.

Disponibilitate format syslog: JSON, CEF

Detectare Sandbox Analyzer

Funcția de notificare vă anunță de fiecare dată când Sandbox Analyzer detectează o nouă amenințare în mostrele trimise. Vi se oferă detalii precum numele de gazdă sau adresa IP a endpoint-ului, ora și data detectării, tipul amenințării, calea, numele, dimensiunea fișierelor și acțiunea de remediere întreprinsă pe fiecare dintre acestea.

Notă
Nu veți primi notificări pentru mostrele analizate care sunt sigure. Informațiile cu privire la toate mostrele trimise sunt disponibile în raportul **Rezultate Sandbox Analyzer (scos din uz)** și în secțiunea **Sandbox Analyzer**, din meniul principal al Control Center .

Disponibilitate format syslog: JSON, CEF

Activitate HyperDetect

Această notificare vă informează în momentul în care HyperDetect găsește anti-malware sau evenimente neblocate în rețea. Această notificare se trimite pentru fiecare eveniment HyperDetect și furnizează următoarele detalii:

- Informații privind stația de lucru afectată (nume, IP, agent instalat)
- Tipul și numele programului malware
- Calea fișierului infectat Pentru atacurile fără fișier se furnizează numele fișierului executabil folosit în atac.
- Stadiul infecției

- Codul hash SHA256 al fișierului executabil al programului mlaware
- Tipul atacului intenționat (atac targhetat, grayware, exploatări, ransomware, fișiere suspecte și trafic pe rețea)
- Nivel de detecție (Permisiv, Normal, Agresiv)
- Ora și data detectării

Disponibilitate format syslog: JSON, CEF
Puteți vizualiza detalii cu privire la infecție și investiga problema în continuare generând un raport de **Activitate HyperDetect** chiar din pagina **Notificări**. Pentru a face acest lucru:

1. În Control Center, faceți clic pe **Notificări** pentru a afișa Zona de notificări.
2. Efectuați clic pe linkul **Afișează mai multe** de la sfârșitul notificării pentru a deschide pagina **Notificări**.
3. Efectuați clic pe butonul **Vizualizare raport** din detaliile notificării. Aceasta va deschide fereastra de configurare a raportului.
4. Configurați raportul, dacă este necesar. Pentru mai multe informații, consultați capitolul „Crearea rapoartelor” (p. 495).
5. Faceți clic pe **Generare**.

Notă
Pentru a evita mesajele spam, veți primi cel mult o notificare pe oră.

Integrare nesincronizată

Această notificare vă informează când o integrare întâmpină probleme și nu se mai poate sincroniza. Acest lucru se poate întâmpla din diverse motive, cum ar fi modificarea datelor integrării sau indisponibilitatea temporară a serverului.

Disponibilitate format syslog: JSON, CEF

Problemă legată de absența unui patch

Această notificare apare atunci când de pe stațiile de lucru din rețeaua dumneavoastră lipsesc unul sau mai multe patch-uri disponibile.

GravityZone trimite automat o notificare care conține toate constatările din ultimele 24 de ore până la data notificării.

Puteți vizualiza stațiile de lucru care se află în această situație efectuând clic pe butonul **Vizualizare raport** din detaliile notificării.

În mod implicit, notificarea se referă la patch-urile de securitate, însă o puteți configura pentru a vă informa și în legătură cu patch-urile non-securitate.

Disponibilitate format syslog: JSON, CEF

Incident nou

Această notificare vă informează când este detectat un incident nou. După activare, notificarea va fi generată de fiecare dată când se va afișa un incident nou în secțiunea **Incidente** din Control Center. Evenimentul corespunzător syslog conține o listă a elementele relevante extrase din detaliile incidentului pe care le puteți utiliza pentru îmbogățirea corelațiilor bazate pe Informațiile de securitate și administrarea evenimentelor (SIEM). Pentru mai multe detalii, selectați **Nume incident**.

Disponibilitate format syslog: JSON, CEF

Anti-malware spațiu de stocare

Această notificare este transmisă dacă se detectează programe periculoase pe un dispozitiv de stocare compatibil ICAP. Această notificare este concepută pentru fiecare detecție malware și oferă detalii referitoare la dispozitivul de stocare infestat (nume, IP, tip), programul periculos detectat și ora detecției.

Disponibilitate format syslog: JSON, CEF

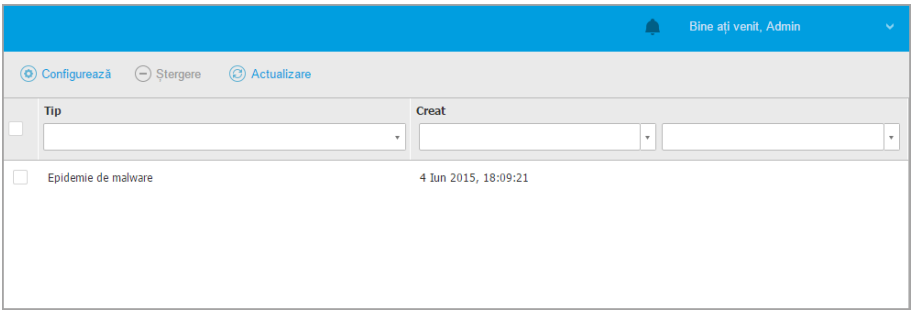
Dispozitive blocate

Această notificare este declanșată când un dispozitiv blocat sau un dispozitiv care are doar drepturi de citire (read-only) se conectează la endpoint. Dacă același dispozitiv se conectează de mai multe ori într-o singură oră, se trimite doar o notificare în acest interval. Dacă dispozitivul se conectează din nou după o oră, se trimite o altă notificare.

Disponibilitate format syslog: JSON, CEF

15.2. Vizualizarea notificărilor

Pentru a vizualiza notificările, faceți clic butonul **Notificări** și apoi faceți clic pe **Vedeți toate notificările**. Este afișat un tabel care conține toate notificările.



Pagina Notificări

În funcție de numărul de notificări, tabelul se poate întinde pe mai multe pagini (implicit, sunt afișate doar 20 intrări pe pagină).

Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului.

Pentru a modifica numărul de intrări afișate pe pagină, selectați o opțiune din meniul de lângă butoanele de navigație.

Dacă există prea multe intrări, puteți utiliza casetele de căutare din antetele de coloană sau meniul de filtrare din partea de sus a tabelului pentru a filtra datele afișate.

- Pentru a filtra notificări, selectați tipul de notificare pe care doriți să-l vizualizați din meniul **Tip**. Opțional, puteți selecta intervalul de timp în care a fost generată notificarea, pentru a reduce numărul de intrări în tabel, mai ales în cazul în care a fost generat un număr mare de notificări.
- Pentru a vedea detaliile de notificare, faceți clic pe numele notificării din tabel. Seccțiunea **Detalii** este afișată în tabelul de mai jos, unde puteți vedea evenimentul care a generat notificarea.

15.3. Ștergerea notificărilor

Pentru a șterge notificări:

1. Faceți clic pe butonul **Notificare** din dreapta barei de mediu și apoi faceți clic pe **Afișează toate notificările**. Este afișat un tabel care conține toate notificările.
2. Selectați notificările pe care doriți să le eliminați.

3. Faceți clic pe butonul ⊖ **Ștergere** din partea de sus a tabelului.

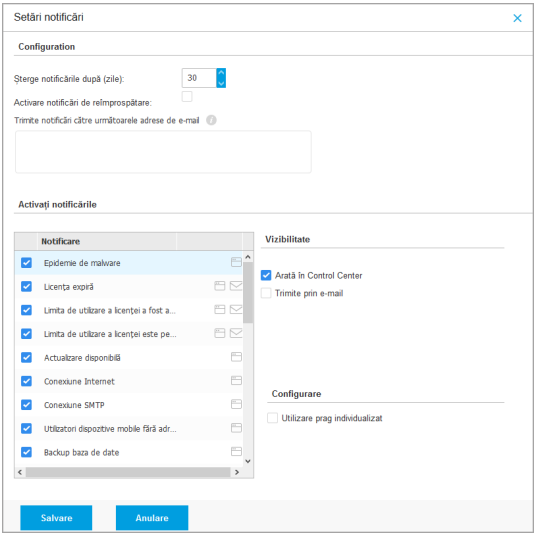
De asemenea, puteți configura notificările care vor fi șterse automat după un anumit număr de zile. Pentru mai multe informații, consultați capitolul „Configurarea setărilor de notificare” (p. 546).

15.4. Configurarea setărilor de notificare

Pentru fiecare utilizator se pot configura tipul de notificări care să fie transmise și adresele de e-mail la care sunt trimise.

Pentru configurarea setărilor de notificare:

1. Faceți clic pe butonul **Notificare** din dreapta barei meniului și apoi pe **Afișează toate notificările**. Este afișat un tabel care conține toate notificările.
2. Faceți clic pe butonul **Configurare** din partea de sus a tabelului. Este afișată fereastra **Setări notificări**.



Setări notificări

Notă
De asemenea, puteți accesa direct fereastra **Setări de notificare** folosind pictograma **Configurare** din colțul din dreapta - sus al ferestrei **Zona de notificare**.

3. În secțiunea **Configurare** puteți defini următoarele setări:
   - Ștergere automată notificări după o anumită perioadă de timp. Setați orice număr dorit între 0 și 365 în câmpul **Ștergere notificări după (zile)**.
   - Bifați caseta **Activare reîmprospătare notificări** dacă doriți ca zona de notificări să se actualizeze automat la fiecare 60 de secunde.
   - În mod suplimentar, puteți trimite notificările prin e-mail către anumiți recipienți. Introduceți adresele e-mail în câmpul dedicat, apăsând tasta `Enter` după fiecare adresă.
4. În secțiunea **Activare notificări** puteți selecta tipul de notificări pe care doriți să le primiți de la GravityZone. De asemenea, puteți configura individual vizibilitatea și opțiunile de transmitere pentru fiecare tip de notificare.

   Selectați din listă tipul de notificare dorit. Pentru mai multe informații, consultați capitolul „Tipuri de notificări” (p. 535). După ce ați selectat un tip de notificare, puteți configura opțiunile specifice (dacă sunt disponibile) în partea din dreapta:

Vizibilitate

- Opțiunea **Afișează în Control Center** indică faptul că acest tip de eveniment se afișează în Control Center, cu ajutorul butonului **Notificări**.
- **Autentificare pe server** specifică faptul că acest tip de eveniment este transmis și către fișierul `syslog`, dacă este configurat un syslog.

  Pentru mai multe informații privind configurarea serverelor syslog, consultați Ghidul de instalare GravityZone.
- **Transmitere prin e-mail** specifică faptul că acest tip de eveniment se transmite, de asemenea, către anumite adrese de e-mail. În acest caz, vi se solicită să introduceți adresele de e-mail în câmpul dedicat, apăsând `Enter` după fiecare adresă.

Configurare

- **Utilizare prag personalizat** - permite definirea unui nivel maxim pentru evenimentele survenite, pornind de la care se transmite notificarea selectată.

  De exemplu, notificarea de Epidemie de malware este transmisă implicit utilizatorilor care au cel puțin 5% din obiectele de rețea administrate infectate cu același malware. Pentru a modifica valoarea pragului de pentru notificarea epidemiei de malware, activați opțiunea **Utilizare prag personalizat** și apoi introduceți valoarea dorită în câmpul **Prag epidemie de malware**.

- Pentru o notificare privind **Copia de rezervă a bazei de date**, puteți decide să fiți informat numai dacă o copie de siguranță a bazei de date a eșuat. Lăsați această opțiune nebifată dacă doriți să fiți informat cu privire la toate evenimentele asociate realizării copiilor de siguranță a bazei de date.

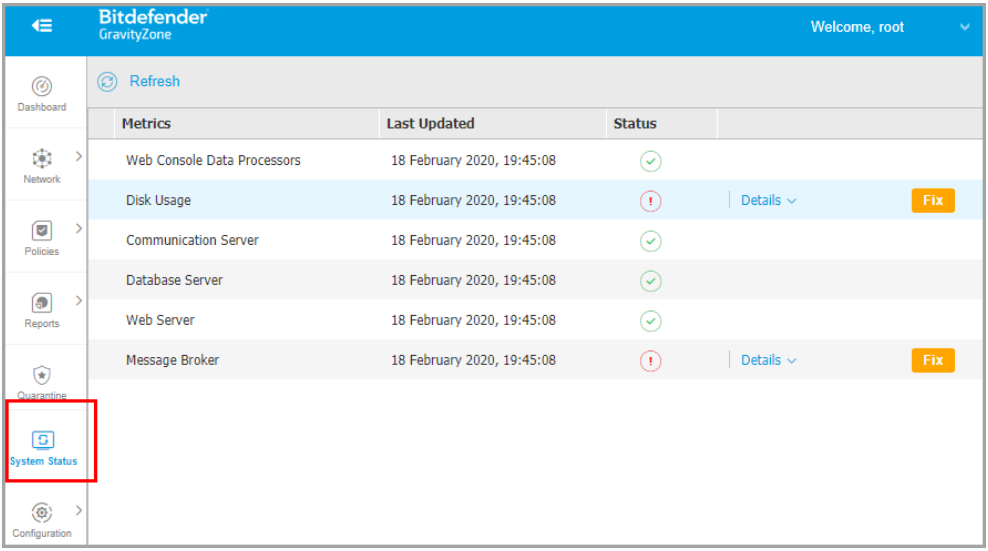
- Pentru **evenimentul de Stare Security Server**, puteți selecta evenimentele Security Server care declanșează acest tip de notificare:
  - **Neactualizat** - vă informează de fiecare dată când un Security Server din rețeaua dvs. nu este la zi.
  - **Oprit** - vă informează de fiecare dată când un Security Server din rețeaua dvs. a fost oprit.
  - **Repornire necesară** - vă informează de fiecare dată când un Security Server din rețeaua dvs. trebuie repornit.

- Pentru **Stare sarcină**, puteți selecta tipul stării care va activa acest tip de notificare:
  - **Orice stare** - vă informează de fiecare dată când o sarcină transmisă din Control Center este efectuată, cu orice stare.
  - **Doar eșuate** - vă informează de fiecare dată când o sarcină transmisă din Control Center eșuează.

5. Faceți clic pe **Save**.

16. STARE SISTEM

Pagina **Stare sistem** afișează informații privind starea instalării GravityZone, fiind astfel mai ușor ca dvs. să vedeți dacă ceva nu merge bine. Pagina afișează indicatori privind sistemul, starea acestora și ultima dată când au fost actualizați, toate aceste informații fiind grupate într-o grilă.



Pagina de stare a sistemului

Coloana **Indicatori** afișează toți indicatorii monitorizați de GravityZone Control Center. Pentru mai multe detalii privind fiecare mesaj despre indicatori și stare, consultați „Instrumente de procesare de date” (p. 573).

Coloana **Ultima actualizare** afișează data și ora ultimei verificări a stării indicatorului.

Coloana **Stare** afișează starea fiecărui indicator: **OK** sau **Atenție**. **Starea** unui indicator este actualizată o dată la fiecare 15 minute sau de fiecare dată când faceți clic pe butonul **Reîmprospătare**.

16.1. Stare OK

Starea OK arată că indicatorul se comportă normal. Nu sunt afișate alte detalii în acest caz.

16.2. Stare Atenție!

Starea Atenție! indică faptul că indicatorul nu rulează în parametri normali.

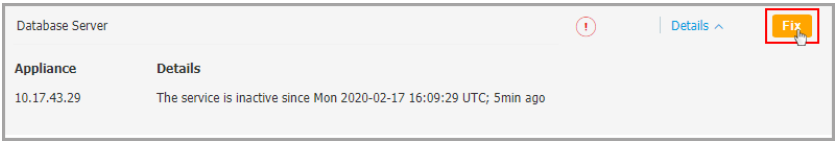
În acest caz este nevoie să investigați mai mult pentru a afla ce s-a întâmplat și pentru a remedia problemele curente:

1. Selectați butonul **Detalii** pentru a vedea informații suplimentare cu privire la indicatorul monitorizat.

Detalii indicatori

- Accesând **Aplicație** puteți găsi adresele IP ale mașinilor afectate.
- Accesând **Detalii** puteți vedea informații despre fiecare indicator.

2. Selectați **Remediere** pentru a remedia indicatorul și GravityZone va avea grijă de tot.



Detalii indicatori

Starea indicatorului va reveni la valoare **OK** după ce a fost remediat.

Notă
Pentru orice alte probleme cu privire la indicator, contactați echipa Enterprise Suport.

16.3. Metrică

Pagina **System Status** conține detalii cu privire la următorii indicatori:

- Instrumente de procesare de date pentru consola web
- Ocupare Disc
- Server de comunicații
- Server de baze de date
- Server web
- Broker mesaje

Instrumente de procesare de date pentru consola web

Acest indicator monitorizează starea instrumentelor de procesare de date care sunt utilizate pentru compilarea datelor afișate în Control Center.

Mesaj stare atenție	Detalii
`Instrumente de procesare care au eşuat în această aplicaţie: <gamă de instrumente de procesare de date> .`	Unul sau mai multe instrumente de procesare de date sunt oprite.
`Aplicaţia virtuală nu funcţionează`	Aplicația virtuală care utilizează servicii ale Consolei web este oprită.

Pentru lista completă a instrumentelor de procesare utilizate de Control Center, consultați „Instrumente de procesare de date” (p. 573).

Ocupare Disc

Acest indicator monitorizează în ce măsură a fost ocupată unitatea de disc de către fiecare aplicație virtuală, cât spațiu liber mai există, dar și spațiul total al unității de disc. Dacă oricare dintre unitățile de disc este utilizată în proporție mai mare de 80%, indicatorul afișează starea ⓘ **Atenție**.

Mesaj stare atenție	Detalii
`Ocuparea spaţiului de pe unitatea de disc (numele unităţii de disc)`	Una sau mai multe unități de disc este utilizată în proporție de 80% din capacitatea maximă.

Mesaj stare atenție	Detalii
Aplicaţia virtuală nu funcţionează	Aplicația virtuală raportată este oprită.

Server de comunicații

Indicatorul monitorizează legătura dintre agenții de securitate instalați pe endpoint-urile dvs. și Serverul de baze de date.

Mesaj stare atenție	Detalii
Serviciul este inactiv de la <timestamp>	Serviciul s-a oprit.

Server de baze de date

Indicatorul monitorizează starea bazei de date GravityZone.

Mesaj stare atenție	Detalii
Serviciul este inactiv de la <timestamp>	Serviciul nu mai rulează pe una dintre aplicații.
Aplicaţia virtuală nu funcţionează	Aplicația virtuală care utilizează Serverul de baze de date este oprită.

Server web

Acest indicator monitorizează starea serverului web care găzduiește GravityZone Control Center.

Mesaj stare atenție	Detalii
Serviciul este inactiv de la <timestamp>	Serverul nu mai rulează pe una dintre aplicații.
Aplicaţia virtuală nu funcţionează	Aplicația virtuală care utilizează acest server este oprită.

Broker mesaje

Acest indicator monitorizează starea serviciului broker mesaje de pe aplicațiile cu rol de Consolă web și Server de comunicare.

Mesaj stare atenție	Detalii
Serviciul broker mesaje nu funcţionează în aceste aplicaţii	Serviciul nu mai rulează pe una dintre aplicații.
Conexiunea la reţea dintre aplicaţii nu a reuşit	Conexiunea dintre două aplicații s-a întrerupt.
Aplicaţia virtuală nu funcţionează	Aplicația virtuală care utilizează acest serviciu este oprită.

17. OBȚINERE AJUTOR

Bitdefender se străduiește să ofere clienților săi un nivel neegalat în ceea ce privește rapiditatea și acuratețea suportului tehnic. Dacă vă confruntați cu o problemă sau dacă aveți orice întrebare cu privire la produsul Bitdefender dvs., mergeți la Centrul de asistență online. Acesta oferă mai multe resurse pe care le puteți folosi pentru a găsi rapid o soluție sau un răspuns. Sau, dacă preferați, puteți contacta echipa de Servicii clienți a Bitdefender. Reprezentanții noștri pentru suport tehnic vă vor răspunde la întrebări la timp și vă vor oferi asistența de care aveți nevoie.

Notă
Puteți afla informații despre serviciile de suport oferite și politica noastră de suport la Centrul de asistență.

17.1. Centrul de asistență Bitdefender

Centrul de asistență Bitdefender este locul unde veți găsi tot ajutorul de care aveți nevoie pentru produsul dumneavoastră Bitdefender.

Puteți utiliza mai multe resurse pentru a găsi rapid o soluție sau un răspuns:

- Articolele din Knowledge Base
- Forum asistență Bitdefender
- Documentație de produs

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare privind securitatea calculatoarelor, produsele și compania Bitdefender.

Articolele din Knowledge Base

Bitdefender Knowledge Base este o bază online de informații despre produsele Bitdefender. Acesta stochează, într-un format ușor accesibil, rapoarte privind rezultatele unor activități continue de asistență tehnică și remediere ale echipelor de asistență și dezvoltare Bitdefender, alături de articole mai generale referitoare la prevenirea virușilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Bitdefender Knowledge Base este deschisă pentru public și putând fi efectuate căutări în mod liber. Prin intermediul informațiilor extinse pe care le conține, putem oferi clienților Bitdefender cunoștințele tehnice și înțelegerea de care au nevoie. Toate solicitările valide pentru informații sau rapoartele de eroare care vin din

partea clienților Bitdefender ajung la Baza de date Bitdefender sub formă de rapoarte de remediere a erorilor, notițe de evitare a erorilor, articole informaționale pentru a completa fișierele de ajutor ale produsului.

Bitdefender Knowledge Base pentru produsele business este disponibilă oricând la adresa http://www.bitdefender.ro/support/business.html.

Forum asistență Bitdefender

Forumul de suport al Bitdefender le oferă utilizatorilor Bitdefender o modalitate facilă de a obține ajutor și de a-i ajuta pe alții. Puteți posta orice probleme sau întrebări legate de produsul dumneavoastră Bitdefender.

Tehnicienii pentru suport tehnic ai Bitdefender monitorizează forumul pentru a verifica noile postări cu scopul de a vă ajuta. De asemenea, puteți obține un răspuns sau o soluție de la un utilizator Bitdefender cu mai multă experiență.

Înainte de a posta problema sau întrebarea, sunteți rugat să verificați în forum existența unui subiect similar sau corelat.

Forumul de suport al Bitdefender este disponibil la https://forum.bitdefender.com, în 5 limbi diferite: engleză, germană, franceză, spaniolă și română. Faceți clic pe link-ul **Protecție Bussiness** pentru a accesa secțiunea dedicată produselor business.

Documentație de produs

Documentația de produs este sursa cea mai completă de informații despre produs.

Cea mai ușoară metodă de a accesa documentația este din pagina **Ajutor și asistență** din Control Center. Efectuați clic pe numele de utilizator din colțul din dreapta sus al consolei, selectați **Ajutor & Asistență** și apoi accesați linkul ghidului care vă interesează. Ghidul se va deschide într-un nou tab în browser.

17.2. Solicitarea de asistență profesională

Puteți solicita asistență prin intermediul Centrului nostru de asistență online. Completați formularul de contact și transmiteți-l.

17.3. Utilizarea Modulului de Suport Tehnic

Modulul de Suport Tehnic GravityZone este conceput pentru a ajuta utilizatorii și pentru a sprijini tehnicienii în obținerea cu ușurință a informațiilor necesare pentru rezolvarea problemelor. Rulați Modulului de Suport Tehnic pe calculatoarele afectate

și trimiteți arhiva rezultată cu informațiile de depanare la reprezentantul de asistență alBitdefender .

17.3.1. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Windows

Se execută Modulul de Suport Tehnic

Pentru a genera jurnalul pe calculatorul afectat, utilizați una din metodele de mai jos:

- Linia de comandă

  Pentru orice probleme cu BEST, instalat pe computer.

- Problemă la instalare

  Pentru situațiile în care BEST nu este instalat pe computer și instalarea eșuează.

Metode liniei de comandă

Utilizând linia de comandă, puteți colecta jurnalele direct de la computerul afectat. Această metodă este utilă în situațiile în care nu aveți acces la GravityZone Control Center sau în care computerul nu comunică cu consola.

1. Deschideți Command Prompt cu privilegii de administrator.
2. Mergeți la folderul de instalare al produsului. Calea implicită este:

   `C:\Program Files\Bitdefender\Endpoint Security`

3. Colectați și salvați jurnalele prin executarea acestei comenzi:

   ```
   Product.Support.Tool.exe collect
   ```

   Jurnalele sunt salvate implicit în `C:\Windows\Temp`.

   Opțional, în cazul în care doriți să salvați jurnalul instrumentului de suport într-o altă locație, utilizați calea opțională:

   ```
   Product.Support.Tool.exe collect [path="<path-to-file>"]
   ```

   Exemplu:

```
Product.Support.Tool.exe collect path="D:\Test"
```

În timpul executării comenzii, veți observa o bară de progres pe ecran. Atunci când procesul s-a încheiat, este afișată denumirea arhivei care conține jurnalele și locația acesteia.

Pentru trimiterea jurnalelor către Bitdefender Enterprise Support accesați `C:\Windows\Temp` sau locația personalizată și căutați fișierul de arhivă denumit `ST_[computername]_[currentdate]`. Atașați arhiva la tichetul de asistență pentru remedierea problemelor.

Problemă la instalare

1. Pentru a descărca Instrumentul de suport BEST, faceți clic aici.
2. Rulați fișierul executabil ca administrator. Va apărea o fereastră.
3. Alegeți o locație în care să salvați arhiva jurnalelor.

   Pe măsură ce jurnalele sunt colectate, vei observa o bară de progres pe ecran. Atunci când procesul s-a încheiat, este afișată denumirea arhivei și locația acesteia.

Pentru trimiterea jurnalelor către Bitdefender Enterprise Support, accesați locația selectată și căutați fișierul de arhivă `ST_[computername]_[currentdate]`. Atașați arhiva la tichetul de asistență pentru remedierea problemelor.

17.3.2. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Linux

Pentru sistemele de operare Linux, Modulul de Suport Tehnic este integrat cu agentul de securitate Bitdefender.

Pentru a colecta informațiile de sistem Linux folosind Modulul de Suport Tehnic, executați următoarea comandă:

```
# /opt/BitDefender/bin/bdconfigure
```

folosind următoarele opțiuni disponibile:

- `--help` pentru afișarea tuturor comenzilor aferente Modulului de Suport Tehnic

- `enablelogs` pentru activarea jurnalelor modulului produs și de comunicare (toate serviciile vor fi repornite automat)
- `disablelogs` pentru dezactivarea jurnalelor modulului produs și de comunicare (toate serviciile vor fi repornite automat)
- `deliverall` pentru a crea:
  - O arhivă cu jurnalele produsului și ale modulului de comunicare, transmisă către directorul `/tmp` în următorul format: `bitdefender_machineName_timeStamp.tar.gz`.

  După ce arhiva a fost creată:

  1. Veți fi întrebat dacă doriți să dezactivați jurnalele. Dacă este necesar, serviciile sunt repornite automat.
  2. Veți fi întrebat dacă doriți să ștergeți jurnalele.
- `deliverall -default` transmite aceleași informații ca și opțiunea anterioară, însă se iau acțiuni implicite asupra jurnalelor, fără ca utilizatorul să fie întrebat (jurnalele sunt dezactivate și șterse).

De asemenea, puteți executa comanda `/bdconfigure` direct din pachetul BEST (kitul complet sau aplicația de descărcare) fără ca produsul să fie instalat.

Pentru a raporta o problemă GravityZone care vă afectează sistemele Linux, urmați pașii de mai jos, folosind opțiunile descrise anterior:

1. Activați jurnalele pentru produs și modulul de comunicare.
2. Încercați să reproduceți problema.
3. Dezactivați jurnalele.
4. Creați arhiva jurnalelor.
5. Deschideți un bilet de asistență prin e-mail folosind formularul disponibil pe pagina de **Suport tehnic** din Control Center, cu o descriere a problemei și jurnalele atașate.

Modulul de Suport Tehnic pentru Linux furnizează următoarele informații:

- Directoarele `etc`, `var/log`, `/var/crash` (dacă este disponibil) și `var/epag` din `/opt/BitDefender`, cu jurnalele și setările Bitdefender

- Fișierul `/var/log/BitDefender/bdinstall.log`, care conține informații referitoare la instalare
- Fișierul `network.txt`, care conține informații privind setările de rețea/conectivitatea mașinii
- Fișierul `product.txt`, care include conținutul tuturor fișierelor `update.txt` din `/opt/BitDefender/var/lib/scan` și o listă recursivă completă a tuturor fișierelor din `/opt/BitDefender`
- Fișierul `system.txt`, care conține informații generale despre sistem (versiune distribuție și kernel, memorie RAM disponibilă și spațiul liber pe hard-disk)
- Fișierul `users.txt`, care conține informații referitoare la utilizator
- Alte informații privind produsul asociat sistemului, cum ar fi conexiunile externe ale proceselor și utilizarea CPU
- Jurnale de sistem

17.3.3. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Mac

La trimiterea unei solicitări către echipa de suport tehnic a Bitdefender, este necesar să furnizați următoarele:

- O descriere detaliată a problemei întâmpinate.
- O captură de ecran (dacă este cazul) care să includă exact mesajul de eroare afișat.
- Jurnalul Modulului de Suport Tehnic.

Pentru a colecta informații despre sistemul Mac folosind Modulul de Suport Tehnic:

1. Descărcați arhiva ZIP conținând Modulul de Suport Tehnic.
2. Extrageți fișierul **BDProfiler.tool** din arhivă.
3. Deschideți o fereastră Terminal.
4. Navigați la locația fișierului **BDProfiler.tool**.

   De exemplu:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. Adăugați drepturi de executare pentru fișierul:

```
chmod +x BDProfiler.tool;
```

6. Executați modulul.

   De exemplu:

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Apăsați D și introduceți parola atunci când vi se solicită să furnizați parola de administrator.

   Așteptați câteva minute până când modulul finalizează generarea jurnalului. Veți găsi fișierul de arhivă rezultat (**Bitdefenderprofile_output.zip**) pe desktop.

17.4. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 18 ani Bitdefender a câștigat o reputație indisputabilă în depășirea așteptărilor clienților și partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

17.4.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro
Centrul de asistență:http://www.bitdefender.ro/support/business.html
Documentație: gravityzone-docs@bitdefender.com
Distribuitori locali:http://www.bitdefender.ro/partners
Programe de Parteneriat: partners@bitdefender.com
Relații Media: pr@bitdefender.com
Subscrieri viruși: virus_submission@bitdefender.com
Subscrieri spam: spam_submission@bitdefender.com
Raportare abuz: abuse@bitdefender.com
Website: http://www.bitdefender.com

17.4.2. Distribuitori locali

Distribuitorii locali Bitdefender sunt pregătiți să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale.

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergeți la http://www.bitdefender.ro/partners.
2. Mergeți la **Localizare partener**.
3. Datele de contact ale distribuitorilor locali Bitdefender ar trebui să se afișeze automat. În caz contrar, selectați țara de reședință pentru a accesa aceste informații.
4. În cazul în care nu găsiți un distribuitor Bitdefender în țara dumneavoastră, nu ezitați să ne contactați prin e-mail la adresa enterprisesales@bitdefender.com.

17.4.3. Filialele Bitdefender

Reprezentanțele Bitdefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și cele generale. Adresele lor precum și modul în care pot fi contactate sunt date mai jos.

Statele Unite ale Americii

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (vânzări&suport tehnic): 1-954-776-6262
Vânzări: sales@bitdefender.com
Web: http://www.bitdefender.com
Centrul de asistență: http://www.bitdefender.com/support/business.html

Franța

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
E-mail: b2b@bitdefender.fr

Site-ul web: http://www.bitdefender.fr
Centrul de asistență: http://www.bitdefender.fr/support/business.html

Spania

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Telefon (birou&vânzări): (+34) 93 218 96 15
Telefon (suport tehnic): (+34) 93 502 69 10
Vânzări: comercial@bitdefender.es
Site-ul web: http://www.bitdefender.es
Centrul de asistență: http://www.bitdefender.es/support/business.html

Germania

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefon (birou&vânzări): +49 (0) 2304 94 51 60
Telefon (suport tehnic): +49 (0) 2304 99 93 004
Vânzări: firmenkunden@bitdefender.de
Site-ul web: http://www.bitdefender.de
Centrul de asistență: http://www.bitdefender.de/support/business.html

Marea Britanie și Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (vânzări&suport tehnic): (+44) 203 695 3415
E-mail: info@bitdefender.co.uk
Vânzări: sales@bitdefender.co.uk
Site-ul web: http://www.bitdefender.co.uk
Centrul de asistență: http://www.bitdefender.co.uk/support/business.html

România

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Telefon (vânzări&suport tehnic): +40 21 2063470
Vânzări: sales@bitdefender.ro
Site-ul web: http://www.bitdefender.ro
Centrul de asistență: http://www.bitdefender.ro/support/business.html

Emiratele Arabe Unite

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (vânzări&suport tehnic): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Vânzări: sales@bitdefender.com
Web: http://www.bitdefender.com
Centrul de asistență: http://www.bitdefender.com/support/business.html

A. Anexe

A.1. Tipuri de fișiere acceptate

Motoarele de scanare antimalware incluse în soluțiile de securitate Bitdefender pot scana toate tipurile de fișiere care ar putea conține amenințări. Lista de mai jos cuprinde cele mai des întâlnite tipuri de fișiere care sunt analizate.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp; xz; z; zip; zl?; zoo

A.2. Tipurile și stările obiectelor de rețea

A.2.1. Tipurile obiectelor de rețea

Fiecare tip de obiect disponibil pe pagina **Rețea** este reprezentat printr-o pictogramă specifică.

Tabelul de mai jos include pictogramele și descrierea tuturor tipurilor de obiecte de rețea disponibile.

Pictogramă	Tip
	Grup rețea
	Calculator
	Computer releu
	Computer server Exchange
	Releu computer server Exchange
	Mașină virtuală
	Releu mașină virtuală
	Model de tip „golden image”
	Server Exchange mașină virtuală
	Releu server Exchange mașină virtuală
	Mașină virtuală cu vShield
	Mașină virtuală releu cu vShield
	Inventar Nutanix
	Nutanix Prism
	Cluster Nutanix
	Inventar VMware
	VMware vCenter
	Centrul de date VMware

Pictogramă	Tip
	Baza de resurse VMware
	Clusterul VMware
	Inventar Citrix
	XenServer
	Xen Pool
	Inventar Amazon EC2
	Integrare Amazon EC2
	Regiune Amazon EC2 / Microsoft Azure
	Zona de disponibilitate Amazon EC2 / Microsoft Azure
	Inventar Microsoft Azure
	Integrare Microsoft Azure
	Security Server
	Security Server cu vShield
	Gazdă fără Security Server
	Gazdă cu Security Server
	VMware vApp
	Utilizator de dispozitiv mobil
	Dispozitiv mobil

A.2.2. Stările obiectelor din rețea

Fiecare obiect din rețea poate avea stări diferite de administrare, securitate, conectivitate și așa mai departe. Tabelul de mai jos include toate pictogramele de stare disponibile și descrierea acestora.

Notă
Tabelul de mai jos include câteva exemple generice de stare. Aceleași stări se pot aplica, individual sau combinat, tuturor tipurilor de obiecte din rețea, cum ar fi grupurile de rețea, calculatoarele și așa mai departe.

Pictogramă	Stare
	Gazdă fără Server de securitate, Deconectată
	Mașină virtuală, Deconectat, Neadministrat
	Mașină virtuală, Conectat, Neadministrat
	Mașină virtuală, Conectat, Administrat
	Mașină virtuală, Conectat, Administrat, Cu probleme
	Mașină virtuală, în curs de repornire
	Mașină virtuală, Suspendat
	Mașină virtuală, Șters

A.3. Tipuri de fișiere de aplicații

Motoarele de scanare antimalware incluse în soluțiile de securitate Bitdefender pot fi configurate să scaneze numai fișiere aplicație (sau program). Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere.

Această categorie conține fișiere cu următoarele extensii:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; iso; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; ps1; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk;

ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.4. Tipuri de fișiere pentru filtrarea atașamentelor

Modulul Control Conținut oferit de Security for Exchange poate filtra atașamentele e-mail în funcție de tipul de fișier. Tipurile disponibile în Control Center includ următoarele extensii de fișiere:

Fișiere executabile

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Imagini

bmp; cal; dcx; drw; ds4; eps; gif; gx2; ico; img; jfif; jpe; jpeg; jpg; pat; pcx; pgm; png; psd; psp; rgb; sdr; sh3; shw; sym; tif; tiff; wpg

Multimedia

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Arhive

7z; ain; arc; arj; bz; bz2; cab; cpio; cru; crush; gz; hap; img; jar; lha; lzh; pak; ppz; rar; rpm; sit; snp; tar; tar.z; tb2; tbz2; tgz; ufa; z; zip; zoo

Foi de calcul

fm3; ods; wk1; wk3; wks; xls; xlsx

Prezentări

odp; pps; ppt; pptx

Documente

doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml

A.5. Variabile de sistem

Unele dintre setările disponibile în consolă necesită specificarea calea pe calculatoarele țintă. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.

Mai jos este lista variabilelor de sistem predefinite:

`%ALLUSERSPROFILE%`

Directorul profilului All Users. Cale obișnuită:

`C:\Documents and Settings\All Users`

`%APPDATA%`

Directorul Application Data a utilizatorului înregistrat. Cale obișnuită:

`C:\Users\{username}\AppData\Roaming`

`%LOCALAPPDATA%`

Fișiere temporare ale aplicațiilor. Cale obișnuită:

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`

Directorul Program Files. O cale tipică este `C:\Program Files`.

`%PROGRAMFILES(X86)%`

Folderul Program Files pentru aplicații pe 32 de biți (pe sistemele pe 64 de biți). Cale obișnuită:

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`

Directorul Common Files. Cale obișnuită:

`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`

Folderul Common Files pentru aplicații pe 32 de biți (pe sistemele pe 64 de biți). Cale obișnuită:

`C:\Program Files (x86)\Common Files`

`%WINDIR%`

Directorul Windows sau SYSROOT. O cale tipică este `C:\Windows`.

`%USERPROFILE%`

Calea către folderul profilului utilizatorului. Cale obișnuită:

`C:\Users\{username}`

Pe sistemele de operare macOS, directorul cu profilul utilizatorului corespunde cu directorul Acasă. Utilizați `$HOME` sau ~ atunci când configurați excepțiile.

A.6. Instrumente Control aplicații

Pentru a seta regulile modulului Control aplicații pe baza codului hash al fișierului executabil sau a amprentei certificatului, trebuie să descărcați următoarele instrumente:

- **Amprentă**, pentru a obține valoarea personalizată a codului hash.
- **Amprentă**, pentru a obține valoarea personalizată a amprentei certificatului.

Amprentă

Efectuați clic aici pentru a descărca fișierul executabil Amprentă sau mergeți la http://download.bitdefender.com/business/tools/ApplicationControl/

Pentru a obține codul hash al aplicației:

1. Deschideți fereastra **Command Prompt**.
2. Navigați către locația instrumentului Amprentă. De exemplu:

```
cd/users/fingerprint.exe
```

3. Pentru a afișa valoarea hash a unei aplicații, executați următoarea comandă:

```
fingerprint <application_full_path>
```

4. Reveniți la Control Center și configurați regula pe baza valorii obținute. Pentru mai multe informații consultați capitolul „Application Control” (p. 339).

Amprentă

Efectuați clic aici pentru a descărca fișierul executabil Amprentă sau mergeți la http://download.bitdefender.com/business/tools/ApplicationControl/

Pentru a obține amprenta certificatului:

1. Executați **Command Prompt** ca Administrator.
2. Navigați către locația instrumentului Amprentă. De exemplu:

```
cd/users/thumbprint.exe
```

3. Pentru a afișa amprenta certificatului, executați următoarea comandă:

```
thumbprint <application_full_path>
```

4. Reveniți la Control Center și configurați regula pe baza valorii obținute. Pentru mai multe informații consultați capitolul „Application Control” (p. 339).

A.7. Obiecte Sandbox Analyzer

A.7.1. Tipuri și extensii de fișiere acceptate pentru trimitere manuală

Următoarele extensii de fișiere sunt acceptate și pot fi detonate manual în Sandbox Analyzer:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, fișiere MZ/PE (executabile), PDF, PEF (executabile), PIF (executabile), RTF, SCR, URL (binar), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer poate detecta tipurile de fișiere menționate mai sus și dacă sunt include în arhive de următoarele tipuri: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, Arhivă comprimată LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolum), ZOO, XZ.

A.7.2. Tipurile de fișiere acceptate de modulul de filtrare preliminară a conținutului la trimiterea automată

Filtrarea preliminară a conținutului va stabili un anumit tip de fișier prin intermediul unei combinații care include conținutul și extensia obiectului. Acest lucru înseamnă că un fișier executabil cu extensia `.tmp` va fi recunoscut ca fiind o aplicație și, dacă este depistat ca fiind suspect, va fi trimis către Sandbox Analyzer.

- Aplicații - fișiere care au formatul PE32, inclusiv, dar fără a se limita la următoarele extensii: `exe`, `dll`, `com`.
- Documente - fișiere cu format de document, inclusiv, dar fără a se limita la următoarele extensii: `xlsx`, `xls`, `ppt`, `doc`, `docx`, `dot`, `chm`, `xlm`, `docm`, `dotm`, `potm`, `potx`, `ppam`, `ppax`, `pps`, `ppsm`, `pptx`, `sldm`, `sldx`, `xlam`, `xlm`, `xltm`, `rtf`, `pdf`.
- Script-uri: `ps`, `wsf`, `ws`, `php`, `py`, `js`, `vb`, `vbs`, `pyc`, `pyo`, `wsc`, `wsh`, `psc1`, `jse`, `vbe`.
- Arhive: `zip`, `jar`, `7z`, `bz`, `bz2`, `tgz` , `msi`, `rar`, `rev`, `z`, `arj`, `iso`, `lha`, `lhz`, `uu`, `uue`, `xxe`, `lzma`, `ace`, `r00`.
- E-mail-uri (memorate în sistemul de fișiere): `eml`, `tnef`.

A.7.3. Excluderi implicite la trimiterea automată

`asc`, `avi`, `bmp`, `gif`, `jpeg`, `jpg`, `mkv`, `mp4`, `pgp`, `png`, `txt`.

A.7.4. Aplicații recomandate pentru mașinile virtuale de detonare

Sandbox Analyzer On-Premises solicită ca anumite aplicații să fie instalate pe mașinile virtuale de detonare, astfel încât acestea să deschidă mostrele trimise.

Aplicații	Tipuri de fișiere
Suita Microsoft Office	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf

Aplicații	Tipuri de fișiere
Windows implicit	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml

A.8. Instrumente de procesare de date

Nume	Detalii
Instrument de trimitere solicitări instrument de procesare	Trimite solicitări ale instrumentelor de procesare mai departe în medii distribuite
Instrument de integrare Hypervision VmWare	Sincronizează inventarul VMWare și alte informații cu GravityZone
Instrument de integrare Hypervisor Citrix	Sincronizează inventarul Xen și alte informații cu GravityZone
Instrument de integrare virtualizare generică	Sincronizează inventarele Nutanix, Amazon EC2 și Azure cu GravityZone
Instrument de integrare NTSA	Sincronizează starea integrării Network Traffic Security Analytics (NTSA) și trimite actualizări de licență către aplicația NTSA
Instrument sincronizare inventar computer Active Directory	Sincronizează inventarul computer Active Directory cu GravityZone
Instrument sincronizare inventar grupuri Active Directory	Sincronizează inventarul grupuri Active Directory cu GravityZone

Nume	Detalii
Instrument sincronizare import utilizatori Active Directory	Sincronizează conturile utilizatorilor Active Directory cu GravityZone (utilizat pentru asocierea dintre conturile AD și conturile GravityZone)
Instrument sincronizare inventar utilizatori Active Directory	Sincronizează inventarul utilizatorilor Active Directory cu GravityZone
Instrument de procesare e-mail	Ierarhizează e-mail-urile pentru a fi trimise din GravityZone
Instrument de procesare rapoarte	Prelucrează rapoarte și portleturi
Instrument de configurare Agent de securitate Windows	Instalează agentul de securitate Bitdefender pe dispozitivele Windows
Instrument de configurare Server de securitate	Instalează Aplicații virtuale de securitate
Manager de licențe	Administrează licențele endpoint-urilor instalate
Instrument de procesare notificări Push pentru mobil	Trimite notificări push către dispozitivele mobile protejate
Instrument de configurare Agent de securitate pentru Linux și macOS	Instalează agentul Bitdefender Enterprise Security for Virtualized Environments (SVE) GravityZone pe dispozitivele Linux și macOS
Instrument de actualizare kit-uri și produse pentru endpoint	Descarcă și publică kit-uri pentru endpoint-uri și actualizări ale produselor Bitdefender
Instrument de actualizare GravityZone	Actualizează automat GravityZone la configurare. Actualizează versiunea Aplicațiilor virtuale GravityZone
Instrument de ștergere pachete	Șterge pachetele de fișiere neutilizate
Instrument de procesare probleme de securitate	Procesează problemele de securitate pentru obiectele din secțiunea Rețea
Instrument de procesare copii de siguranță	Realizează backup-uri pentru baza de date GravityZone
Instrument de procesare notificări	Trimite notificări către utilizatori

Nume	Detalii
Instrument de procesare evenimente de sistem	Gestionează evenimentele din infrastructură (Control aplicații, Sandbox Analyzer, Serenity, SVA) sau integrări (Exchange, Nutanix, NSX)
Instrument de configurare pachet suplimentar HVI	Gestionează instalarea, actualizarea și ștergerea pachetului suplimentar HVI pentru gazdele XEN
Instrument de procesare sarcină repornire HVI	Administrează sarcinile de repornire pe gazdele HVI
Instrument de procesare stare de pornire și stare online	Calculează starea de pornire și de conectivitate a computerelor și mașinilor virtuale
Instrument de procesare ștergere mașini offline	Elimină mașinile offline din rețea
Executarea sarcinilor în fundal	Gestionează și rulează sarcini și procese în fundal

Vocabular

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

Bitdefender dispune de modulul său propriu care realizează actualizarea automată sau manuală.

adware

Aplicația adware este adesea combinată cu o aplicație gazdă care este oferită gratuit dacă utilizatorul acceptă aplicația adware. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere care explică scopul aplicației, nu este comisă nicio infracțiune.

Totuși, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanțele sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licențiere.

Aplicație de descărcare Windows

Este un nume generic pentru un program a cărui funcție principală este descărcarea de conținut pentru activități nedorite sau periculoase.

Arhivă

Un disc, o casetă sau un director care conține fișiere de rezervă.

Un fișier care conține unul sau mai multe fișiere într-un format comprimat.

Atacuri targetate

Atacuri cibernetice care vizează în principal avantaje financiare sau denigrarea reputației. Ținta poate fi un individ, o companie, un software sau un sistem, toate studiate în detaliu înainte de lansarea atacului. Aceste atacuri se derulează pe perioade mai lungi de timp și în etape, folosind mai multe puncte de infiltrare. Sunt observate rar, de cele mai multe ori doar după ce daunele au fost deja făcute.

Backdoor

Reprezintă o breșă de securitate realizată în mod deliberat. Motivația acestor "găuri" nu este întotdeauna malițioasă: unele sisteme de operare, de exemplu, sunt puse în circulație cu conturi privilegiate pentru tehnicienii din service sau de responsabilii cu mentenanța produsului din partea producătorului.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în bara de sarcini Windows (de obicei în partea de jos, lângă ceas) și conține pictograme miniaturale pentru accesul rapid la aplicații de sistem cum ar fi cele legate de fax, imprimantă, modem, volum și altele. Faceți dublu-clic sau clic dreapta cu mouse-ul pe o pictogramă pentru a vizualiza și accesa detaliile și comenzile.

Bootkit

Un bootkit este un program periculos care are capacitatea de a infecta sectoarele de date Master Boot Record (MBR), Volume Boot Record (VBR) sau boot. Bootkit-ul rămâne activ chiar și după repornirea sistemului.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza și încărca pagini de Web.

Cookie

În domeniul Internetului, cookie-urile reprezintă mici fișiere ce conțin informații despre fiecare calculator care pot fi analizate și folosite de către cei care publică reclame pentru a vă urmări interesele și preferințele online. În acest domeniu, tehnologia cookie-urilor este în curs de dezvoltare, iar intenția este de a afișa direct acele anunțuri care corespund intereselor dumneavoastră. Această facilitate are avantaje și dezavantaje pentru mulți deoarece, pe de o parte, este eficientă și pertinentă din moment ce vizualizați doar acele anunțuri despre subiecte care vă interesează. Pe de altă parte, cookie-urile implică de fapt o "monitorizare" și "urmărire" a site-urilor vizitate și a link-urilor accesate. Astfel, în mod logic, părerile sunt împărțite în ceea ce privește confidențialitatea și mulți se simt jigniți de faptul că sunt văzuți ca un simplu "număr SKU" (este vorba de codul de bare de pe spatele ambalajelor care este scanat pe bandă la supermarket). Deși acest punct de vedere poate fi considerat extrem, în anumite cazuri el reprezintă chiar ceea ce se întâmplă în realitate.

Evenimente

O acțiune sau întâmplare detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

Extensie de fișier

Reprezintă porțiunea dintr-un nume de fișier ce urmează după caracterul punct, și care indică tipul de date pe care le stochează fișierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fișiere. De obicei aceasta este formată din una până la trei litere (unele sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: "c" pentru fișierele sursă scrise în limbajul C, "ps" pentru fișiere PostScript sau "txt" pentru fișierele text oarecare.

Fals pozitiv

Apare atunci când un analizator detectează un fișier ca fiind infectat când de fapt acesta nu este infectat.

Fișier de raport

Reprezintă un fișier care listează acțiunile care au avut loc. Bitdefender menține un fișier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fișierelor, numărul de arhive și fișiere scanate, câte fișiere infectate și suspecte au fost găsite.

Fișiere suspecte și trafic în rețea suspect

Fișierele suspecte sunt cele cu reputație îndoielnică. Această caracteristică este dată de numeroși factori, printre care se numără: existența semnăturii digitale, numărul de apariții în rețelele de calculatoare, packerul utilizat etc. Traficul de rețea este considerat suspect dacă se abate de la model. De exemplu, surse nesigure, solicitări de conexiune la porturi neobișnuite, creșterea lățimii de bandă utilizate, timpi aleatorii de conectare etc.

Furtună de scanare antimalware

O utilizare intensivă a resurselor de sistem care intervine atunci când software-ul antivirus scanează simultan mai multe mașini virtuale pe o singura gazdă fizică.

Grayware

O clasă de aplicații software între software legitim și malware. Deși nu sunt la fel de periculoase ca programele malware care afectează integritatea sistemului, comportamentul lor este totuși deranjant, conducând la situații nedorite cum ar fi furtul de date și utilizarea neautorizată, publicitatea nedorită. Cele mai des întâlnite aplicații grayware sunt spyware și adware.

Hoț de parole

Un password stealer colectează date care pot fi nume de conturi și parole asociate. Aceste date de autentificare furate sunt utilizate apoi pentru activități periculoase, precum furtul de cont.

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât și reasamblarea pachetelor IP.

Keylogger

Un keylogger este o aplicație care înregistrează orice tastați.

Keyloggerele nu au o natură periculoasă. Pot fi folosite în scopuri legitime, cum ar fi monitorizarea activității angajaților sau a companiilor subordonate. Cu toate acestea, utilizarea lor de către infractorii cibernetici în scopuri negative este din ce în ce mai răspândită (de exemplu, pentru colectarea informațiilor cu caracter privat, cum ar fi acreditările de înregistrare și codurile numerice personale).

Linie de comandă

Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Malware

Malware este termenul generic pentru software-ul care este proiectat pentru a face rău - o contracție a " malicious software Acesta nu este încă în uz universal, dar popularitatea sa ca un termen general pentru viruși, cai troieni, viermi, și coduri malware mobile este în creștere.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruși noi. Această metodă de scanare nu se bazează pe semnături de viruși

cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuși ocazional poate raporta un cod suspicios în programe normale, generând așa-numitul "fals pozitiv".

Metoda ne-euristică

Această metodă de scanare se bazează pe semnături de viruși cunoscuți. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus și din acest motiv nu generează fals pozitiv.

Phishing

Reprezintă acțiunea de a trimite un e-mail către un utilizator, pretinzând a fi o companie legitimă, în încercarea de a păcăli utilizatorul să furnizeze informații confidențiale ce vor fi folosite la furtul identității. E-mailul îndreaptă utilizatorul către un site Web unde acesta este rugat să actualizeze informații personale, cum ar fi parole și numere de card de credit, de asigurări sociale și de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals și folosit pentru a fura informațiile despre utilizator.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor și tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului, și a altor dispozitive periferice.

În rețelele TCP / IP și UDP acestea reprezintă un punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Programe spion

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la Internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

Ransomware

Un program malware care vă blochează accesul la calculator sau la fișiere și aplicații. Programele ransomware vă solicită să achitați o anumită sumă (răscumpărare) în schimbul unui cod de decriptare care vă permite să redobândiți accesul la calculatoarele sau fișierele dvs.

Rootkit

Un rootkit este un set de unelte soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la unelte recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, loginuri și jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde aplicații malițioase sau prezența intrușilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

Script

Un alt termen pentru fișiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Sector de boot:

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului și altele). În cazul discurilor de startup, sectorul de boot conține un program care încarcă sistemul de operare.

Semnătură malware

Semnăturile malware sunt fragmente de coduri extrase din mostre reale de malware. Acestea sunt utilizate de către programele antivirus pentru a realiza o identificare după model și detectare a programelor malware. Semnăturile sunt utilizate și pentru a elimina codul malware din fișierele infectate.

Baza de date cu semnături malware a Bitdefender reprezintă o colecție de semnături malware actualizate în fiecare oră de către cercetătorii malware ai Bitdefender.

Spam

Termen ce acoperă întreaga gamă a mesajelor electronice nesolicitate (junk). În general, acestea sunt cunoscute sub numele de mesaje electronice nesolicitate.

Straturi de protecție

GravityZone oferă protecție printr-o serie de module și roluri, denumite în mod colectiv straturi de protecție, care sunt împărțite în Protecție pentru endpoint-uri (EPP), sau protecție de bază, și diverse add-on-uri. Protecția pentru endpoint-uri include modulele Antimalware, Advanced Threat Control, Anti-Exploit avansat, Firewall, Control conținut, Controlul dispozitive, Network Attack Defense, Utilizator privilegiat și Releu. Add-on-urile includ straturi de protecție, cum ar fi Security for Exchange și Sandbox Analyzer.

Pentru detalii despre straturile de protecție disponibile în soluția dvs. GravityZone, consultați „Straturi de protecție GravityZone” (p. 2).

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul Internet și care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware și sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât și convenții folosite în conectarea rețelelor și rutării traficului.

Tehnică de exploatare

O exploatare se referă, în general, la orice metodă folosită pentru a câștiga acces neautorizat la calculatoare sau la o vulnerabilitate din securitatea unui sistem care expune un sistem unui atac.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină virușii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruși pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul orașului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.

Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a virușilor se pot și înmulți. Toți virușii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar și un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus și mai periculos este acela care este capabil să se răspândească în rețea și poate să treacă de sistemele de securitate.

Virus de boot

Reprezintă un virus care infectează sectorul de boot al unui disc fix sau al unei dischete. Orice încercare de a face boot de pe o dischetă infectată cu un virus de boot va determina virusul să devină activ în memorie. Din acest moment de fiecare dată când veți realiza boot-area sistemului, virusul va deveni activ în memorie.

Virus de macro

Un tip de virus informatic este acela inclus ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word și Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente și execută aceste macro-uri de fiecare dată când este deschis documentul.

Virus polimorf

Reprezintă un virus care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruși sunt greu de identificat.