Bitdefender

GravityZone

GHID SECURITY ANALYST

Bitdefender GravityZone
Ghid Security Analyst

Publicat 2021.01.13

Digitally signed by Celonenco Vitalie
Date: 2021.04.09 10:49:50 EEST
Reason: MoldSign Signature
Location: Moldova

Termeni legali

Cuprins

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)**

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 catalogheză 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

Soluția GravityZone include următoarele componente:

- Consola web (Control Center)
- Security Server
- Pachet suplimentar HVI
- Agenți de securitate

3.1. 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.

3.2. 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.

3.3. 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)

3.3.1. 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).

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
- 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.

3.3.2. 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

3.3.3. 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.

3.3.4. 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.

3.4. 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 Bitdefender pot fi configurate și administrate prin platforma de administrare 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

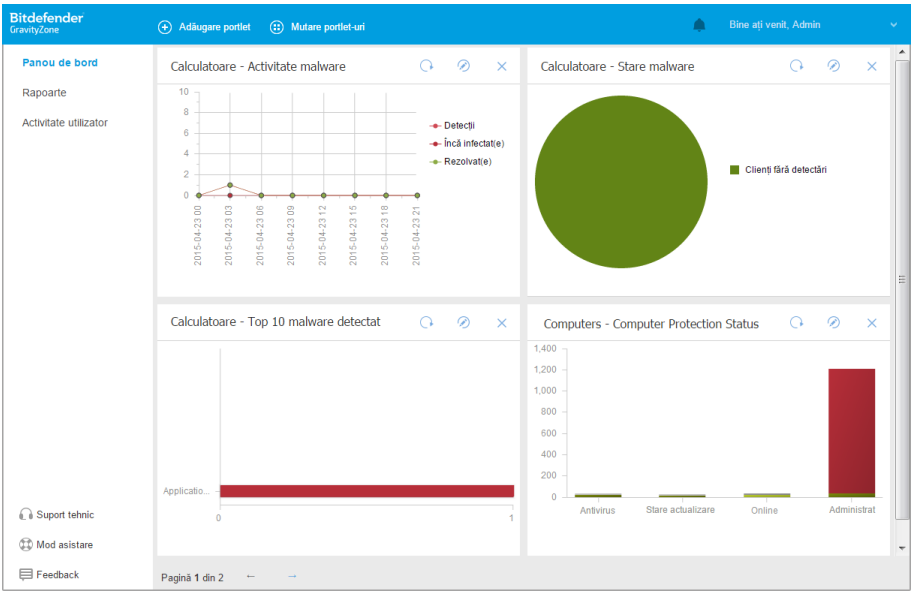
Avertisment
Control Center nu va funcționa/nu se va afișa corespunzător în Internet Explorer 9+ cu funcția Compatibility View activată, care este echivalentă cu utilizarea unei versiuni de browser incompatibile.

Pentru conectarea la Control Center:

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

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 zona superioară pentru a naviga prin consolă.



Panoul de bord

Analistii de securitate pot accesa următoarele secțiuni din bara de meniu:

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

Rapoarte
Obțineți rapoarte de securitate referitoare la clienții administrați.

Activitate utilizator
Verificați jurnalul activității utilizatorului.

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.
- **Ajutor & Asistență**. Efectuați clic pe această opțiune pentru ajutor și informații de asistență.

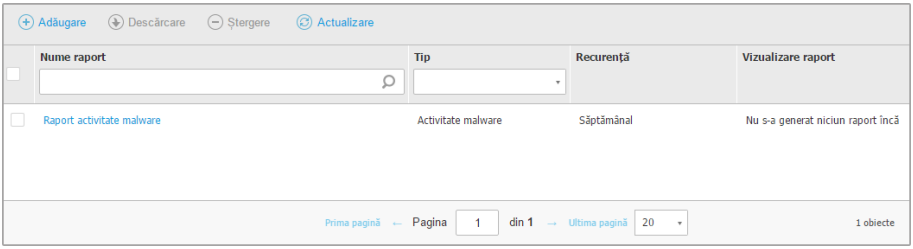
- **Trimiteți feedback**. Efectuați clic pe această opțiune pentru a afișa un formular care vă permite să modificați și să trimiteți mesaje de feedback cu privire la experiența dumneavoastră cu GravityZone.
- **Deconectare**. Faceți clic pe această opțiune pentru a ieși din contul dumneavoastră.

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

- Pictograma **Modului Ajutor**, care activează o funcție de ajutor, afișând casete de indicații deasupra elementelor Control Center. Veți afla cu ușurință informații utile referitoare la funcțiile Control Center.
- Pictograma **Notificări**, asigură un acces ușor la mesajele de notificare și la pagina **Notificări**.

4.2.1. 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

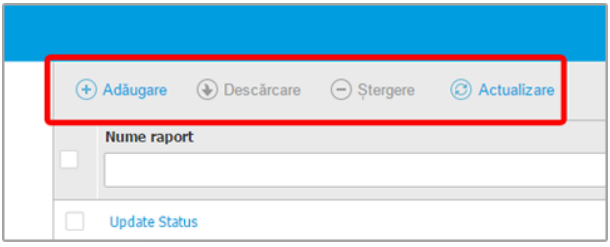
Pentru a vă asigura că în consolă se afișează cele mai recente informații, faceți clic pe butonul **Reîmprospătare** din colțul de sus al tabelului.

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

4.2.2. 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:

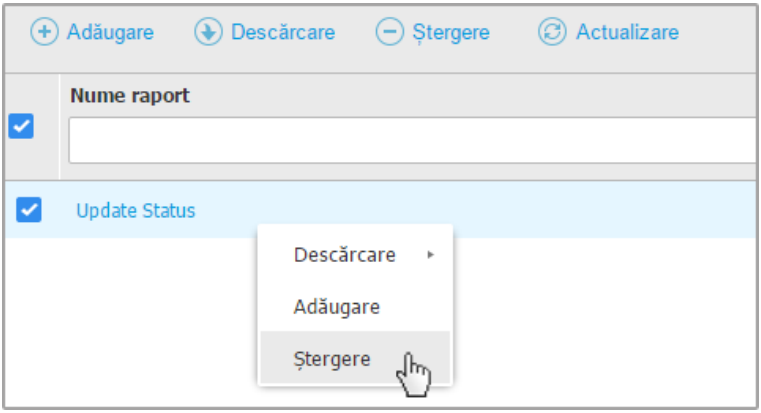
- Crearea unui nou raport.
- Descărcați un raport programat.
- Ștergerea unui raport programat.



Pagina de Rapoarte - Bara de instrumente pentru acțiuni

4.2.3. 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.



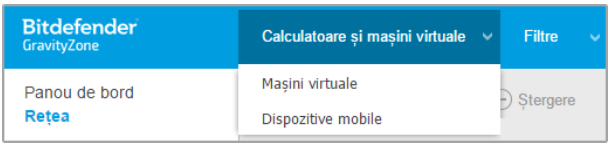
Pagina de Rapoarte - Meniu contextual

4.2.4. 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. 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.

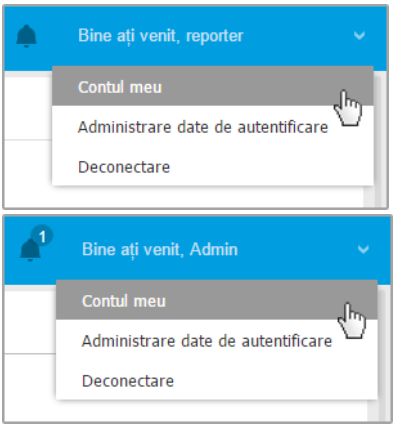
Pentru a modifica parola de autentificare:

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.

4.4. 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.

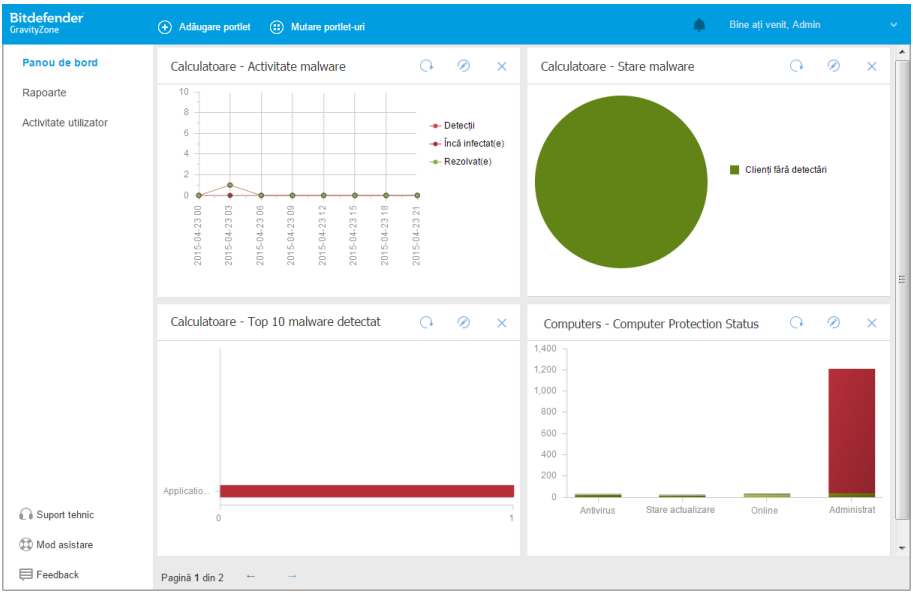
5. PANOUL DE MONITORIZARE

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.

5.1. 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.

5.1.1. 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.

5.1.2. 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.

5.1.3. 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. 36).
4. La secțiunea **Ținte**, selectați obiectele și grupurile de rețea pe care le doriți incluse.
5. Faceți clic pe **Save**.

5.1.4. 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.

5.1.5. Rearanjarea portlet-urilor

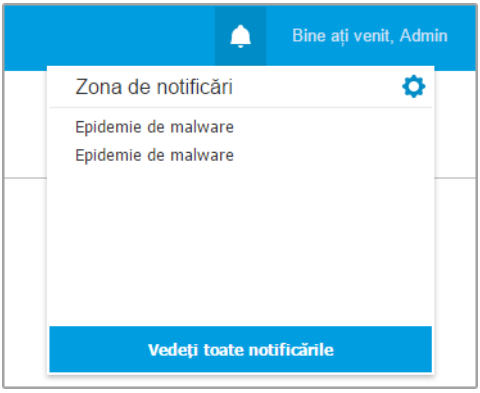
Puteți rearanja portlet-urile panou pentru ca acestea să răspundă mai bine nevoilor dvs. Pentru a rearanja portlet-uri:

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.

6. 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.

6.1. 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. 32).

Amenințările detectate de către HyperDetect nu fac obiectul acestei notificări.

Anti-Exploit avansat

Această notificare vă informează când modulul Anti-Exploit avansat a detectat o tentativă de exploit în rețeaua dumneavoastră.

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.

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.

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

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. 56).
5. Faceți clic pe **Generare**.

Notă
Pentru a evita mesajele spam, veți primi cel mult o notificare pe oră.

Problemă legată de absența unui patch

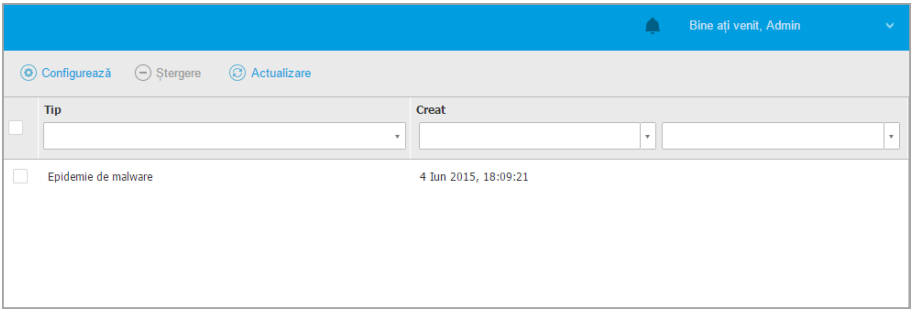
Această notificare apare atunci când de pe stațiile de lucru din rețeaua dumneavoastră lipsesc unul sau mai multe patch-uri disponibile.

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.

6.2. 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. Secțiunea **Detalii** este afișată în tabelul de mai jos, unde puteți vedea evenimentul care a generat notificarea.

6.3. 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.

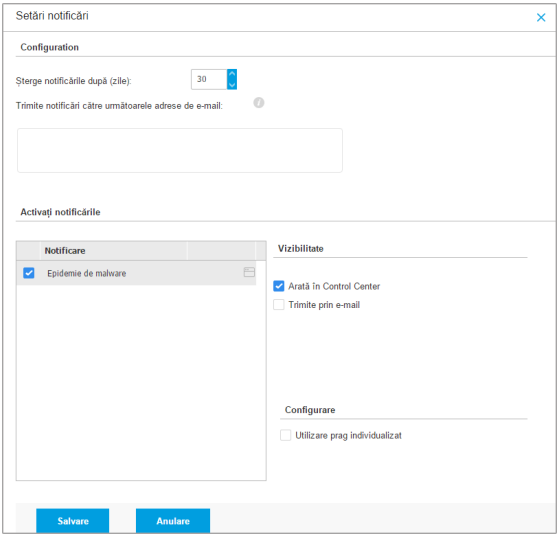
De asemenea, puteți configura notificările care vor fi șterse automat după un anumit număr de zile. Pentru mai multe informații, consultați capitolul „Configurarea setărilor de notificare” (p. 32).

6.4. 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:
   -
   - 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. 29). 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.
- **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 **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**.

7. 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).

7.1. 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

7.1.1. 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.

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. 68).
- 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.

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.

7.1.2. 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 lângă 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.

7.1.3. 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.

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.

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

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.

7.2. Crearea rapoartelor

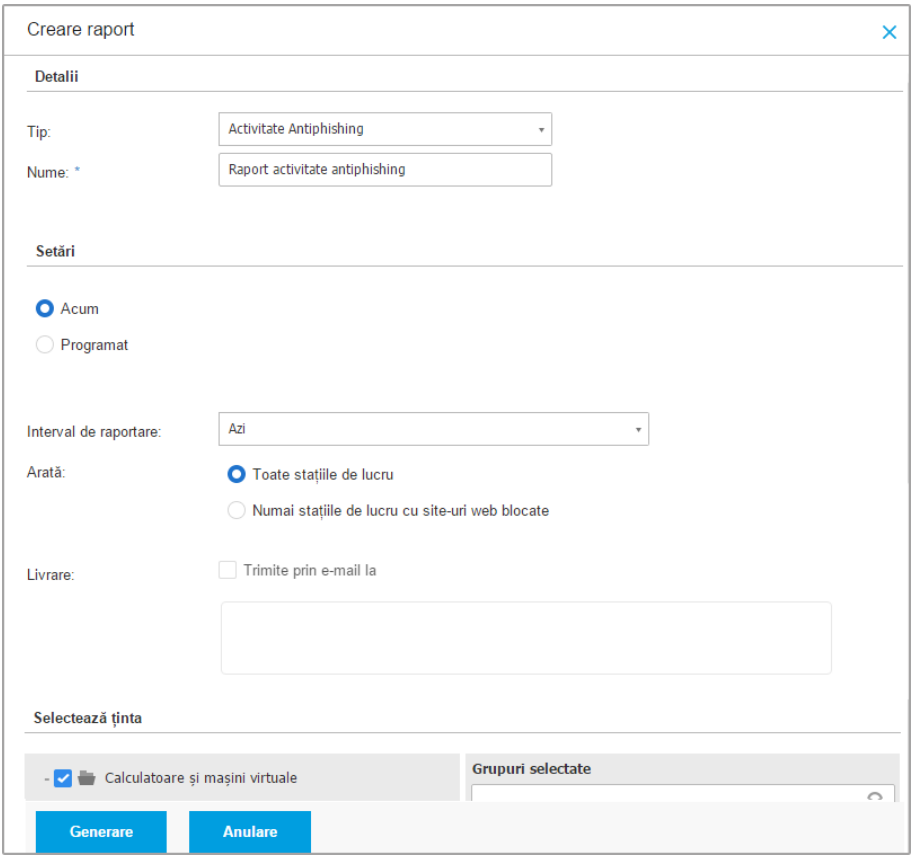
Puteți crea două categorii de rapoarte:

- **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. 36)
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**.

7.3. 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.

7.3.1. 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. 62)

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.

7.3.2. 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.

7.3.3. 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.

7.4. 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

7.4.1. 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.

7.4.2. 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.

7.5. 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.

7.6. Printarea rapoartelor

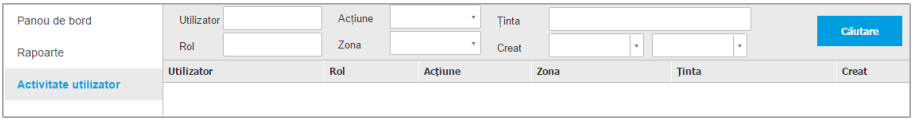
Control Center nu acceptă în prezent funcționalitatea de buton de imprimare. Pentru a imprima un raport, trebuie mai întâi să-l salvați pe calculator.

8. 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
- Inițierea, încheierea, anularea și oprirea proceselor de depanare pe mașinile afectate
- Editarea setărilor de autentificare pentru conturile GravityZone.

Pentru a examina istoricul activității utilizatorului, mergeți la pagina **Activitate utilizator** și selectați vizualizarea de rețea dorită din selectorul de vizualizări.



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.

9. OBȚINERE AJUTOR

Pentru orice probleme sau întrebări legate de GravityZone, contactați un administrator.

9.1. 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.

A. Anexe

A.1. Obiecte Sandbox Analyzer

A.1.1. 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, fişiere 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.1.2. 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.1.3. Excluderi implicite la trimiterea automată

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt`.

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.