Caietul de sarcini

Licențe produs program antivirus
pentru asigurarea protecției infrastructurii TIC a ASP - reînnoirea subscripției licențelor programului antivirus Bitdefender GravityZone
Cloud Business Security pentru asigurarea protecției infrastructurii TIC a ASP

CARACTERISTICI GENERALE ALE PRODUSULUI

Produsul („soluția") reprezintă o platformă integrată pentru managementul securității, gândită ca o soluție modulara. Produsul conține următoarele module:

A. O consola de management care asigura funcționalități de administrare.
B. Protecție antimalware pentru stații fizice, laptop-uri și servere.

A. CONSOLA DE MANAGEMENT

1. Cerințe generale:

1. Interfața consolei de management va fi în limba română.
2. Interfața clientului de securitate, care se instalează pe stații și servere, va fi in limba română.
3. Manualul de instalare a produsului va fi în limba română.
4. Manualul de administrare a produsului va fi în limba română.
5. Soluția va permite activarea/dezactivarea actualizărilor de produs/semnături.
6. Actualizări automate a consolei de management făcute de către producătorul soluției, fără a fi necesara intervenția utilizatorului.
7. Notificările – prezente în interfața, notificările necitite sunt evidențiate, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile).
8. Consola de management este accesibila de oriunde în lume (este bazată pe un serviciu cloud de tip Software-as-a-Service), fără a fi nevoie de setări suplimentare din partea utilizatorului.
9. Consola de management este accesibila atât de pe stații de lucru cât și de pe dispozitive mobile (smartphone, tableta).

2. Panou de monitorizare și raportare (Dashboard):

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație este considerată neactualizată).
2. Panoul central conține rapoarte pentru toate modulele suportate.
3. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea.

3. Inventarierea rețelei – managementul securității:

1. Soluția se va integra cu domeniul Active Directory și va putea importa inventarul.
2. Se permite descoperirea stațiilor stații fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.

3. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicată, ultima dată când s-a conectat (online și/sau offline) și FQDN.
4. Soluția va permite crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac.
5. Soluția va permite instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale.
6. Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.
7. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanță pentru clientul antimalware.
8. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanță.
9. Soluția va oferi informații detaliate despre fiecare task și se fișează daca task-ul s-a finalizat sau nu cu succes.
10. Soluția va permite configurarea centralizată a clienților antimalware prin intermediul politicilor
11. Se vor oferi în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.

4. Politici:

1. Soluția va permite configurarea setărilor antimalware prin intermediul politicilor din consola de management.
2. Politica va conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.
3. Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale.
4. Politica sa poate fi schimbată automat în funcție de:
   a. IP sau clasa de IP al stației
   b. Gateway-ul alocat
   c. DNS serverul alocat
   d. WINS serverul alocat
   e. Sufix DNS pentru conexiunea dhcp
   f. Clientul este/nu este în accesași rețea cu infrastructura de management (stația de lucru poate soluționa implicit numele gazdei)
   g. Tipul rețelei (lan, wireless)

5. Rapoarte:

1. Soluția va conține rapoarte care prezintă statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie sa aibă un cont în consola de management).
3. Soluția va permite vizualizarea rapoartelor curente programate de administrator.
4. Soluția va permite exportarea rapoartelor în format pdf și detaliile ca format csv.

6. Carantina:

1. Soluția va permite restaurarea fișierelor carantinate în locația originală sau într-o cale configurabilă cu opțiunea de excludere automată a fișierului restaurat.
2. Carantina va fi locală, pe fiecare stație administrată și va fi administrată, fie local, fie din consola de management.

7. Utilizatori:

1. Administrarea se va putea face pe bază de roluri.
2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat.
   a. Administrator companie: administrează arhitectura consolei de management;
   b. Administrator rețea: administrează serviciile de securitate;
   c. Reporter: monitorizează și generează rapoarte.
3. Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management.
4. Se va permite configurarea detaliata a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.
5. Se va permite deconectarea automata a oricărui tip de utilizator după un anumit timp pentru o protecție sporita a datelor afișate în consola de administrare. Acest interval se poate personaliza de administratorul soluției.

8. Log-uri:

1. Înregistrarea acțiunilor utilizatorilor.
2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator.
3. Se va permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune.

9. Actualizare:

1. Se permite definirea de locații de actualizare multiple.
2. Se permite activarea/dezactivarea actualizărilor de produs și semnături.
3. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus.
4. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, soluția include 2 tipuri de actualizări de produs:
   a. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei.
   b. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc).
5. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management

B. PROTECTIE STATII SI SERVERE FIZICE

1. Caracteristici generale minimale și eliminatorii:

1. Pentru reducerea la minim a consumului de resurse, soluția antimalware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției antimalware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall).

2. Pentru o mai buna protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare.
3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.
4. Pentru o mai buna protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazata pe tehnologii de învățare automata (machine learning).
5. Pentru o mai buna protecție a stațiilor și serverelor, soluția include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil să identifice și remedieze în mod automatizat sau manual un număr mare de riscuri existente la nivel de rețea sau sistem de operare ce pot afecta funcționalitatea și nivelul de securizare al endpoint-ului

2. Cerințe de sistem:

- Sisteme de operare pentru stații de lucru: **Windows11, Windows 10, Windows 8/8.1, Windows 7, Mac OS Monterey 12.x, macOS BIG SUR 11.x, macOS Catalina 10.15, Mac OS X Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12),**
- Sisteme de operare embedded: **Windows 10 IOT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7**
- Sisteme de operare pentru servere: **Windows Server 2022, Windows Server 2019, Windows Server 2019 CORE, Windows Server 2016 , Windows Server 2016 (Core), Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, , Windows Server 2008 R2,**
- Sisteme de operare Linux: Red Hat Enterprise Linux 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Exnterprise15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 31 sau mai recent, AWS Bottlerocket 2020.03, Amazon Linux v2, Google COS Milestones 77,81,85, Azure Mariner 2, AlmaLinux 8,9.x, Rocky Linux 8.x, Cloud Linux 7,8.x, Pardus 21, Linux Mint 20.3, Miracle 8.4.

3. Administrare și instalare remote:

1. Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea se va putea face în mai multe moduri:
   a. prin descărcarea directă a pachetului pe stația pe care se va face instalarea;
   b. prin instalarea la distanță, direct din consola de management;
   c. trimiterea pe email (indicând adrese) a pachetului de instalare pentru Windows, Linux, Mac.
3. Instalarea clienților la distanță în alte locații decât cele în care este instalată consola de management se va face prin intermediul unui client existent în locațiile respective de tip relay pentru a minimiza traficul în WAN.
4. În consolă vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc.

5. Din consolă se va putea trimite o singura politică pentru configurarea integrală a clientului de pe stații/servere.
6. Consola va include o secțiune, „Audit", unde se vor menționa toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc.
7. Posibilitatea creări unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cât și pentru cele pe 64 de biți.
8. Posibilitatea creări unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale).
9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
10. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu.
11. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu.

4. Caracteristici și funcționalități principale ale modulului antimalware:

1. Soluția permite administratorului să stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul va putea alege intre următoarele acțiuni:
    1. Acțiune implicită pentru fișiere infectate:
        i. interzice accesul
        ii. dezinfectează
        iii. ștergere
        iv. muta fișierele în carantină
        v. nicio acțiune
    2. Acțiune alternativă pentru fișierele infectate:
        i. interzice accesul
        ii. dezinfectează
        iii. ștergere
        iv. mută fișierele în carantină
    3. Acțiune implicită pentru fișierele suspecte:
        i. interzice accesul
        ii. ștergere
        iii. mută fișierele în carantină
        iv. nicio acțiune
    4. Acțiune alternativă pentru fișierele suspecte:
        i. interzice accesul
        ii. ștergere
        iii. mută fișierele în carantină
2. Scanarea automată în timp real va putea fi setată să nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definită de administratorul soluției,
3. Definirea până la 16 nivele de profunzime pentru scanarea în arhive.
4. Scanarea euristica comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de viruși necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.
5. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). De asemenea, se va putea anula scanarea în cazul în care sunt detectate unități care au informații stocate mai mult de « x » MB.
6. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP.
7. Configurarea căilor ce urmează a fi scanate la cerere.

8. Clienții antimalware pentru Workstation să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese.
9. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware.
10. Posibilitatea de configura scanările programate să se execute cu prioritate redusă.
11. Produsul antimalware poate fi configurat să folosească scanarea în clod, și parțial scanarea locală.
12. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:
    - Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local.
    - Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
13. Pentru o protecție sporita, soluția antimalware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor.
14. Pentru o protecție sporită, soluția antimalware trebuie să poată scana paginile HTTP.
15. Pentru o mai buna gestionare a antimalware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecție la dezinstalare.
16. Pentru siguranța utilizatorului, clientul va include un modul de antiphishing.
17. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată.

5. Anti-Exploit-Avansat:

1. Posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive.
2. Depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare.
3. Protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem" cum ar fi browserele, aplicațiile de tip Office sau Reader, procesele critice aferente sistemelor de operare.

6. Firewall:

1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.
3. Posibilitatea de a defini rețele de încredere pentru mașina destinată.
4. Abilitatea de a detecta scanarea de porturi.
5. Posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide).
6. Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune.

7. Carantina:

1. Produsul antimalware să permită trimiterea automata a fișierelor din carantină către laboratoarele antimalware ale producătorului.
2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator.
3. Produsul antimalware să permită ștergerea automata a fișierelor carantinate mai vechi de o anumita perioadă, pentru a nu încarcă inutil spațiul de stocare.
4. Posibilitatea de a restaura un fișier din carantină în locația lui originală.
5. Modulul de carantină va permite rescanarea obiectelor după fiecare actualizare de semnături.

8. Protecția datelor:

1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

9. Controlul conținutului:

1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu următoarele particularități:
   a. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini.
   b. Permite blocarea accesului la Internet pe intervale orare.
   c. Permite blocarea paginilor de internet care conțin anumite cuvinte cheie.
   d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
   e. Permite blocarea accesului la anumite aplicații definite de administrator;
   f. Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violență, pornografie etc).

10. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.
2. Modulul va permite controlul următoarelor tipuri de dispozitive:
   a. Bluetooth Devices
   b. CDROM Devices
   c. Floppy Disk Drives
   d. Security Policies 153
   e. IEEE 1284.4
   f. IEEE 1394
   g. Imaging Devices
   h. Modems
   i. Tape Drives
   j. Windows Portable
   k. COM/LPT Ports
   l. SCSI Raid
   m. Printers
   n. Network Adapters
   o. Wireless Network Adapters
   p. Internal and External Storage
3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.
4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

11. Power User:

1. Modulul poate fi instalat/dezinstalat în funcție de preferință administratorului.
2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa și modifica setările clientului antimalware dintr-o consola disponibilă local pe mașina client.

3. Modificările efectuate din modulul Power User vor fi active local, pe mașina pe care s-au făcut respectivele modificări.
4. Administratorul va putea suprascrie din consolă setările aplicate de utilizatorii Power User.

12. Actualizare:

1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare).
2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are și rol de server de actualizare.