Caiet de sarcini pentru achiziția

reinoirii licentei serviciilor SW Subscription & Renewal antivirus Bitdefender GravityZone Business Security, GOV, 24 luni support, 130 computere

Tip: **Achiziția Servicii SW Subscription & Renewal antivirus Bitdefender GravityZone Business Security, GOV, 24 luni support, 130 computere**

Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST, AV-Comparatives, etc.)

Caracteristici generale ale produsului:

Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management:
Protecție stații și servere fizice și virtualizate:

- Windows 10,8.1,7, Vista (SP1), Mac OS X 10.12.x, 10.11.x, 10.10.x ,10.9.x, 10.8.x .
- Windows Server 2003/2008/2008 R2/2012/2012 R2/2016.
- Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Oracle Linux 6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual, Debian 5.0 sau mai recent.
- Sa poata face actualizari automate a consolei de management de catre producatorul solutiei, fara a fi necesara interventia utilizatorului.
- Consola de management sa fie accesibila de oriunde in lume (sa fie bazata pe un serviciu cloud de tip Software-as-a-Service), fara a fi nevoie de setari suplimentare din partea utilizatorului.

Consola de management:

Pachetul de instalare va fi oferit ca un appliance virtual. Aceasta din urma nu va necesita o licență suplimentară pentru sistemul de operare, iar imaginea de tip template va fi posibil de a fi importata în urmatoarele platfomre de virutalizrae: VMware vSphere, Citrix XenServe, Microsoft Hyper-V, Red Hat Enterprise Virtualization, KVM, Oracle VM.

Consola de management va fi oferita cu o baza de date inclusă, non-relațională.
Soluția trebuie să:

- fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri.
- asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web.
- asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management.
- includă un modul load balancer pentru performanța și redundanță
- includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering).
- includă posibilitatea de a fi accesată atât de pe stațiile de lucru cât și de pe dispozitivele mobile (tabletă, smartphone).

Interfata consolei de management va fi in limba romana. Interfata agentului care se instaleaza pe statii de lucru si servere, va fi in limba romana.

Cerințe generale produs:

Soluția trebuie să:

1. includă unul sau mai multe module de update server prin care să asigure actualizarea componentelor și a semnăturilor.
2. permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management.
3. transmită alerte de ne funcționalitate, cu 30 de minute înainte de actualizare.
4. permită vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi si îmbunătățiri, probleme rezolvate, probleme cunoscute
5. afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile).
6. permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus.
7. permită instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management.

Inventarierea rețelei – managementul securității

Produsul trebuie să:

- se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și să importe inventarul acestor platforme.
- permită descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
- permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.
- ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare si adresa IP.
- permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale.
- permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.
- permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus.
- ofere posibilitatea de repornire a mașinilor fizice de la distanță.
- ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui.
- permită configurarea centralizată a clienților antivirus prin intermediul politicilor.
- ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.
- permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.
- Permită crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux si Mac.

Politici:

Produsul trebuie să:

- permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module
- conțină opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.
- permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy.
- poată fi schimbată automat în funcție de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless).

Rapoarte:

Produsul trebuie să:

- Contina rapoarte care prezinta statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate.

- Transmita rapoartele programate catre un numar nelimitat de adrese de email (ne fiind nevoie sa aiba un cont in consola de management).
- Permita vizualizarea rapoartelor curente programate de administrator.
- Permita exportarea rapoartelor in format .pdf si detaliile ca format .csv.

Carantină:

- Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă.
- Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management.

Utilizatori:

- Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite : Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări.
- Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management.
- Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp.

Log-uri:

- Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare.

Actualizari:

Soluția trebuie să:

- permite definirea de locatii de actualizare multiple.
- permite activarea/dezactivarea actualizarilor de produs si semnaturi.
- Ofere posibilitatea ca orice client antivirus să poată fi configurat să ofere update-urile catre alt client antivirus;
- permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, inainte de a fi instalate pe toate statiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizare va include 2 tipuri de actualizari de produs:
  a. Ciclu rapid, gândit pentru un mediu de test in cadrul retelei;
  b. Ciclu lent, gândit pentru restul rețelei (productie, servere critice etc);
- permită stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management.

Protecție stații și servere fizice si virtualizate – caracteristici minime:

Soluția antivirus trebuie să:

- Permite instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).
- Pentru o mai buna protectie a statiilor si serverelor, solutia trebuie sa includa un vaccin anti-ransomware. Acest vaccin va asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
- Vaccinul anti-ransomware trebuie sa primeasca actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware.
- Pentru o mai buna protectie a statiilor si serverelor, solutia trebuie sa includa protectie impotriva atacurilor zero-day de tip exploit avansate (atacuri directionate) bazata pe tehnologii de invatare automata (machine learning).

- Pentru o mai buna protectie a a statiilor si serverelor, solutia trebuie sa includa un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil sa identifice si remedieze in mod automatizat sau manual un numar mare de riscuri existente la nivel de retea sau sistem de operare ce pot afecta functionalitatea si nivelul de securizare al endpoint-ului.

Administrare și instalare remote:

- Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
- Instalarea se va putea face in mai multe moduri:

  a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea;
  b. prin instalarea la distanta, direct din consola de management

  c. trimiterea pe email (oricate adrese) a pachetului de instalare pentru Windows, Linux, Mac.

- Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui client existent in locatiile respective de tip relay pentru a minimiza traficul in WAN.
- In consola vor fi disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc.
- Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere.
- Consola va include o sectiune, „Audit”, unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc.
- Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti.
- Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale).
- Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
- Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu.
- Sa permita selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu.

Caracteristici și funcționalități principale ale modulului antivirus

Produsul trebuie sa permită:

1. Administratorului sa stabileasca actiunea luata de produsul Antimalware la detectarea unei amenintari noi. Astfel administratorul va putea alege intre urmatoarele actiuni:

a. Actiune imiplicita pentru fisiere infectate:

- interzice accesul
- dezinfecteaza
- stergere
- muta fisierele in carantina
- nicio actiune

b. Actiune alternativa pentru fisierele infectate:

- interzice accesul
- dezinfecteaza
- stergere
- muta fisierele in carantina

c. Actiune imiplicita pentru fisierele suspecte:

- interzice accesul

- stergere
- muta fisierele in carantina
- nicio actiune

d. Actiune alternativa pentru fisierele suspecte:

- interzice accesul
- stergere
- muta fisierele in carantina

2. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei,

3. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.
4. Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.
5. Scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB.
6. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP.
7. Configurarea cailor ce urmeaza a fi scanate la cerere.
8. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese.
9. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware.
10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
11. Produsul antimalware sa poata fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala.
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 protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor.
14. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
16. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.
17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.

Firewall:

- sa ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
- modulul să poată fi instalat/dezinstalat la cerere.
- să permită definirea de rețele de încredere pentru mașina destinație.

Carantina:

Produsul trebuie sa permită:

- Trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului.

- Trimiterea continutului carantinei si va putea fi expediat in mod automat, la un interval definit de administrator.
- Stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare.
- Posibilitatea de a restaura un fisier din carantina in locatia lui originala.
- Rescanarea obiectelor dupa fiecare actualizare de semnaturi a modulului de carantina.

Protecția datelor:

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

Controlul conținutului:

Produsul trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

Controlul aplicațiilor:

Pentru administrare și inventariere eficientă produsul trebuie să dețină un modul care va oferi posibilitatea de a:

- efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe.
- regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.
- bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subprocese) după: cale fișier: local, CD-ROM, portabil sau rețea, hash , certificat.

Controlul dispozitivelor:

Produsul trebuie să conțină un modul pentru controlul dispozitivelor care:

- poate fi instalat/dezinstalat conform setărilor stabilite.
- permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage.
- permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.
- permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

Power User:

Produsul trebuie să conțină un modul pentru setări specifice – power user care să:

- poată fi instalat/dezinstalat în funcție de preferința administratorului.
- permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client.
- permită administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User**.**

Actualizare:

Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:

- la nivel de stație în mod silențios (fără avertizări).
- folosind unul sau mai multe servere de actualizare.
- pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare.

Alte cerințe:
Perioada de suport local și menținere de la producător:

1. Pentru soluția ofertată se solicită ca produsul sa fie aliniat la perioada de valabilitate a licentelor existente.
2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local in limba romana din partea partenerului.
3. Partenerul va prezenta autorizarea de la producator pentru produsul livrat;
4. Partenerul va prezenta minim 2 certificate tehnice a persoanelor certificate pe produsul ofertat;

Se va oferi manual de instalare si administrare a produsului ofertat in limba romana,engleza,rusa.

Șef Serviciu TIC Digitally signed by Volcov Veaceslav
Date: 2021.03.25 09:14:47 EET
Reason: MoldSign Signature
Location: Moldova
Veaceslav Volcov