Anexa nr. 1 la Anunțul de participare privind achiziționarea prelungirii licențelor sistemului de protecție și securitate cibernetică, tip Antivirus

Specificațiile tehnice minime pentru sistemul de protecție și securitate cibernetică, de tip Antivirus

Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST) și să fie prezent în mențiunile Gartner. Satisfacerea necesităților minime va constitui în total: **390 licențe** (340 licențe (workstation PC) și 50 licențe (VDI/VS/Server), în scopul managementului centralizat al dispozitivelor.

Licențele oferite trebuie sa prelungească licențele existente pentru produsul Bitdefender Gravity Zone Elite, pe un termen de 12 luni.

Caracteristici generale ale produsului:

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

1. Protecție stații și servere fizice și virtualizate:
   - Windows 10,8.1,7
   - Windows Server 2003/2008/2008/2019 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.
2. Protecție și securitate de tip „sandboxing" pentru serverele si stațiile de lucru;
3. Controlul dispozitivelor, controlul accesului la Internet, filtrarea traficului prin modul de tip firewall pentru mașinile fizice și virtuale
4. Protecție și securitate pentru serverele email Microsoft Exchange.

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 următoarele platforme de virtualizare: 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:

1. Fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri.
2. Asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web.
3. Asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management.
4. Includă un modul load balancer pentru performanța și redundanță
5. Includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering).

6. Includă posibilitatea de a fi accesată atât de pe stațiile de lucru cât și de pe dispozitivele mobile (tabletă, smartphone).

Interfața consolei de management va fi in limba romana. Interfața agentului care se instalează pe stații 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 SNMP pentru raportarea statusului mașinilor din cadrul componentei de management.
8. Permită crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocata local, pe un server FTP sau în rețea

Inventarierea rețelei – managementul securității

Produsul trebuie să:

1. Se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și să importe inventarul acestor platforme.
2. Permită descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
3. Permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.
4. ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare si adresa IP.
5. Permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale.
6. Permită selectarea modulelor componente atunci când se creează pachetul clientului care se Instalează pe mașinile fizice/virtuale.
7. Permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus.
8. Ofere posibilitatea de repornire a mașinilor fizice de la distanță.
9. Ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui.
10. Permită configurarea centralizată a clienților antivirus prin intermediul politicilor.
11. 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.
12. Permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.
13. Permită crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descarcă pachetele pentru protecția stațiilor si serverelor pe care rulează sistemul de operare Windows, Linux si Mac.

Politici:

Produsul trebuie să:

1. Permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module
2. 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.
3. Permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy.
4. 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).

Monitorizare și raportare:

Produsul trebuie să:

1. Permită setarea de opțiuni specifice pentru afișarea rapoartelor existente.
2. Dețină un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate.
3. Conțină rapoarte care prezinta statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
4. Trimită rapoarte către un număr nelimitat de adrese de email.
5. Permită vizualizarea rapoartelor curente programate de administrator.
6. Permită exportarea rapoartelor în format .pdf si detaliile ca format .csv.
7. Includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.
8. Ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor.
9. Ofere interogări legate de evenimente precum: calculatorul ținta pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc)
10. Ofere interogări de evenimente Exchange precum: direcția traficului e-mail, evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate), măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau plasarea în carantină a fișierului, ștergerea sau respingerea e-mail-ului)

Carantină:

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

Utilizatori:

1. 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.
2. Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management.
3. Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp.

Log-uri:

1. 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:

1. Permită definirea de locații de actualizare multiple.
2. Permită activarea/dezactivarea actualizărilor de produs si semnături.
3. Ofere posibilitatea ca orice client antivirus să poată fi configurat să ofere update-urile către alt client antivirus;
4. Permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile si serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare va include 2 tipuri de actualizări de produs:

- Ciclu rapid, gândit pentru un mediu de test in cadrul rețelei;
- Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc);

5. Permită stabilirea zonelor de test si critice din cadrul rețelei prin intermediul politicilor din consola de management.

Protecție stații și servere fizice si virtualizate – caracteristici minime:

Soluția antivirus trebuie să:

1. Permită instalarea personalizată a modulelor,
2. includă un vaccin anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar daca sunt infectate și blocarea procesului de criptare.
3. Includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).
4. Includă module avansate de securitate, proiectate special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție, pentru protecție împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware cu posibilitatea de stabilire a nivelului de protecție dorit: permisiv, normal, agresiv cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare.
5. Includă un sandbox în cloud-ul producătorului, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate” pentru o analiză în profunzime.
6. Includă două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranța. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranța: ștergere sau permutare în carantină;

7. Modulul de Sandbox va include si posibilitatea de trimitere manuala a fișierelor in Sandbox-ul din cloud-ul producătorului. Astfel, daca administratorul suspectează un fișier ca fiind maliții, îl poate trimite manual in Sandbox pentru a fi „detonat" si a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica daca vor fi „detonate" individual sau toate in același timp. Acest modul va poate suporta „detonarea" următoarelor tipuri de fișiere: 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, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Aceste fișiere menționate anterior, vor putea fi detectate corect chiar daca sunt incluse in arhive de tipul: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

Administrare și instalare remote:

1. Pachetele de instalare trebuie să fie configurabile cu modulele necesare: firewall, content control, device control, power user.
2. Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management. Instalarea se va putea face in mai multe moduri:
   - prin descărcarea directa a pachetului pe stația pe care se va face instalarea;
   - prin instalarea la distanta, direct din consola de management
   - remiterea pe email (oricâte adrese) a pachetului de instalare pentru Windows, Linux.
3. Consola trebuie să includă o secțiune, „Audit", unde se vor păstra toate acțiunile întreprinse de administratori și utilizatori ai consolei, cu informații detaliate: logare, editare, creare, delogare, permutare etc.
4. Produsul trebuie să ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
5. Produsul trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domen.
6. Produsul va oferi posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange;

Caracteristici și funcționalități principale ale modulului antivirus

Produsul trebuie sa permită:

1. Stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:
2. Implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune.
3. Alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină.
4. Acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune.
5. Acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină.
6. Scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de « x » MB, definirea nivelelor de profunzime pentru scanarea în arhive.

7. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansata încă.
8. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc).
9. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP.
10. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.
11. Configurarea căilor ce urmează a fi scanate la cerere.
12. 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.
13. Setarea priorităților scanărilor programate.
14. Configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware
15. Administratorului să personalizeze și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată în Cloud-ul privat, scanare centralizată cu fallback* pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid.
16. Setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor.
17. Scanarea paginilor web.
18. Setarea a unei parole pentru protecția la dezinstalare.
19. Modul de antiphishing.
20. Protecție în timp real pe mașinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalată.
21. Instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale.

Firewall:

1. Să ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2. Modulul să poată fi instalat/dezinstalat la cerere.
3. Să permită definirea de rețele de încredere pentru mașina destinație.

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 aplicaţiilor:

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

1. Efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe.
2. Regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.

3. 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:

1. Poate fi instalat/dezinstalat conform setărilor stabilite.
2. 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.
3. Permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.
4. 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:

1. Poată fi instalat/dezinstalat în funcție de preferința administratorului.
2. 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.
3. Permită administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User**.**

Actualizare:

Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:

1. La nivel de stație în mod silențios (fără avertizări).
2. Folosind unul sau mai multe servere de actualizare.
3. Pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare.

Alte cerințe specifice:

Perioada de suport local și menținere de la producător:

1. Pentru soluția oferită, se solicită a fi oferit și suport local și de menținere de la producător pentru perioada de 12 luni;
2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local în limba româna sau rusă din partea partenerului;
3. Se va oferi (la solicitare) manual de instalare si administrare a produsului ofertat in limba romana si engleza.
4. Compania învingătoare trebuie să prezinte până la semnarea contractului pachetul antivirus (consolă de management, etc) pentru a verifica în practică dacă produsul dat corespunde cerințelor cerute;
5. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în oferta.

Digitally signed by Muntean Vadim
Date: 2022.04.18 15:45:56 EEST
Reason: MoldSign Signature
Location: Moldova

Director adjunct,
Președintele Grupului
de lucru pentru achiziții: _____ Vadim MUNTEAN