# Cerinţele funcţionale pentru Endpoint Protection

## 1.1 Antivirus, Antispyware, Desktop Firewall si Prevenirea Intruziunilor

| | |
|---|---|
| Solutia trebuie sa asigure protectie pentru statii de lucru si servere cu urmatoarele sisteme de operare:<br>- Windows 10 Versiunile 1507, 1511, 1607, 1703<br>- Windows 10 IoT Enterprise<br>- Windows 8.1, Update 1, August 2014 update rollup<br>- Windows 8 (Win NT 6.2) Editions: Basic / Pro / Enterprise<br>- Windows 7 (Home Premium / Professional / Ultimate / Enterprise)<br>- Windows Vista<br>- Windows Vista Business/Ultimate for Embedded Systems<br>- Windows 7 Professional/Ultimate for Embedded Systems<br>- Windows Server 2016 Editions: Datacenter / Essentials / Standard installed in „Server with Desktop Experience” mode<br>- Windows Server 2012 Release 2 (R2) , R2 Update 1, R2 August 2014 update<br>- Windows Server 2008, HyperV, Standard, Datacenter, Enterprise, Foundation, Web, HPC<br>- VMware ESX, ESXi<br>- Citrix XenApp 5.0, 5.6, 6.0, 6.5, 7.5, 7.6<br>- Citrix Xen Guest<br>- MAC OS X 10.7 sau mai nou | |
| Solutia trebuie sa ofere protectie pe sisteme de operare pe 32/64 de biti. | |
| Solutia trebuie sa ofere protectie pentru statii de lucru si servere cu roluri precum Windows Active Directory Domain Controller, Microsoft SQL server, Microsoft Exchange Server, fara a le impacta in mod negative. | |
| Solutia nu poate fi oprita de utilizator chiar daca acesta are dreptul de administrator local. | |
| Solutia trebuie sa ofere protectie pentru registrii sistemului de operare prin aplicarea de politici ce restrictioneaza efectuarea de modificari. De asemenea, trebuie sa poata scana registrii de programe malitioase instalate. | |
| Solutia trebuie sa efectueze scanari On Access si On Demand. | |
| Solutia trebuie sa vina cu o unealta de monitorizare a consumului de resurse ce genereaza rapoarte pe baza carora se pot face optimizari. | |
| Solutia trebuie sa permita optimizarea consumului de resurse prin configurarea de politici de scanare diferite in functie de aplicatii. | |
| Solutia trebuie sa permita alocarea dinamica a resurselor pe endpoint, pentru optimizarea performantei. | |
| Solutia trebuie sa prezinte un mecanism propriu de instalare a agentilor pe statiile de lucru sau alte sisteme. | |
| Solutia trebuie sa poata detecta virusi pe email daca se utilizeaza clientii de mail Microsoft Outlook sau Lotus Notes Client. | |
| Solutia trebuie sa fie capabila sa detecteze scripturi malitioase pe pagini web. | |

Digitally signed by Şarco Vasile
Date: 2018.11.28 18:57:57 EET
Reason: MoldSign Signature
Location: Moldova

| | |
|---|---|
| Solutia ofera protectie pentru masinile virtuale ce ruleaza pe statii. | |
| Solutia trebuie sa foloseasca un singur motor de scanare a antivirusului de statie, pentru a nu se incarca suplimentar memoria sistemelor de calcul | |
| Agentul unic sa poata fi instalat in mod silentios, fara alertarea utilizatorului | |
| Actualizarile sa fie instalate in mod silentios, fara alertarea utilizatorului | |
| Clientii antivirus pentru workstation trebuie sa contina optiunea de pauza si reluare a scanarilor | |
| Solutia poate bloca accesul la directoare partajate pentru a bloca raspandirea codului malitios. | |
| Solutia are capacitatea de a detecta si de a curata cod malitios. | |
| Solutia trebuie sa poata detecta aplicatii malitioase precum Spyware, Adware, Dialers, Password Crackers, Jokes, Key Loggers si altele. De asemenea permite administratorului sa defineasca propriile aplicatii considerate malitioase. | |
| Solutia are capacitate de scanare euristica si poate detecta fisiere infectate pentru care nu exista semnatura in baza de date. | |
| Solutia poate proteja impotriva:<br>- Rularii de aplicatii din directorul TEMP al sistemului de operare<br>- Conexiunilor IRC, TFTP, FTP, SMTP cu exceptia aplicatiilor cunoscute si permise<br>- Inregistrarii automata a programelor ca servicii<br>- Modificarii/crearii de executabile, extensii, procese si setari | |
| Solutia trebuie sa ofere posibilitatea blocarii comunicatiilor aplicatiilor pe retea, Inbound/Outbound, pe porturi ce se pot specifica. | |
| Solutia poate detecta codul malitios din fisierele transferate prin software de genul Instant Messaging. | |
| Solutia trebuie, atunci cand detecteaza cod mailtios, sa permita actiunile de prevenire a accesului la fisier, de curatare si de stergere a fisierului. | |
| Solutia trebuie sa poata scana la cerere:<br>- Memoria sistemelor<br>- Procesele ce ruleaza<br>- Partitiile locale<br>- Dispozitivele atasate de stocare date<br>- Directoare din retea<br>- Registrii | |
| Solutia trebuie sa ofere functionalitatea de intoarcere la baza de date de semnaturi de virusi anterioara. | |
| Solutia trebuie sa utilizeze un mecanism de caching pentru fisierele deja scanate ce nu au suferit modificari. | |
| Solutia permite modificarea consumului de resurse pentru scanarile la cerere pentru a nu impacta performantele sistemelor. | |
| Solutia trebuie sa fie capabila sa identifice daca un laptop lucreaza pe baterie si sa amane scanarea la cerere. | |
| Solutia trebuie sa aibe mecanisme de protectie ce nu permit utilizatorului sau aplicatiilor malitioase sa intervina asupra fisierelor/proceselor/cheilor de registrii ale acesteia. | |
| Solutia trebuie sa permita carantinarea fisierelor infectate si sa ofere posibilitatea restaurarii acestora direct din consola de administrare, fara a fi nevoie sa se intervina asupra sistemului. | |

| | |
|---|---|
| Actualizarea semnaturilor trebuie sa se faca incremental pentru a evita incarcarea retelei. | |
| Solutia trebuie sa permita actualizarea semnaturilor offline (prin pachet de actualizare executabil), din serverul de administrare, direct de la producator, din director partajat de retea, din ftp si din pagina web prin HTTP. | |
| Actualizarea trebuie sa permita definirea unui interval de timp in care sistemele vor incepe aleator sa descarce noile semnaturi pentru a evita supraincarcarea retelei. | |
| Solutia trebuie sa fie recunoscuta de sistemele de operare Microsoft Windows in Security Center. | |
| Solutia trebuie sa poata scana si detecta cod malitios in arhive. | |
| Solutia trebuie sa ofere protectie impotriva programelor de tip Mass Mailer | |
| Solutia trebui sa detecteze codul malitios inainte de executie. | |
| Solutia trebuie sa permita configurarea unei politici de identificarea a aplicatiilor de tipul P2P. | |

## 1.2 Controlul dispozitivelor periferice

| | |
|---|---|
| Componenta trebuie sa poata rula cel putin pe:<br>- Microsoft Windows Vista (32-bit)<br>- Microsoft Windows 7 (32/64-bit)<br>- Microsoft Windows 8 (32/64-bit)<br>- Microsoft Windows 8.1 (32/64-bit)<br>- Microsoft Windows 10 (32/64-bit)<br>- Microsoft Windows 10 TH2 (32/64-bit)<br>- Microsoft Windows 10 RS1 (32/64-bit)<br>- Microsoft Windows 10 RS2 (32/64-bit)<br>- Microsoft Windows 2008 (32/64-bit)<br>- Microsoft Windows 2008 R2 (32/64-bit)<br>- Microsoft Windows 2012 (64-bit)<br>- Microsoft Windows 2012 R2 (64-bit)<br>- OS X 10.9 sau mai nou<br>- Citrix XenApp 6.0/6.5/7.5/7.6/7.9<br>- Citrix XenDesktop 5.5/5.6/7.0/7.1/7.5/7.6/7.8<br>- VMware View 4.6/5.0/5.1/5.2/5.3/6.0/6.2<br>- VMware Hyper-V 6.3.9600 | |
| Solutia trebuie sa poata colecta informatii din Microsoft Active Directory. | |
| Solutia trebuie sa prezinte un mecanism propriu de instalare a agentilor pe statiile de lucru sau alte sisteme. | |
| Solutia trebuie sa permita creare de poltici in mod granular de permitere/blocare a dispozitivelor periferice pe baza informatiilor precum:<br>- ID Producator<br>- ID Model Dispozitiv Periferic<br>- Tipul de dispozitiv<br>- Clasa dispozitivului detectat de sistemul de operare | |

| | |
|---|---|
| - BUS Conectare (USB, S-ATA, ETC.)<br>- Numele Dispozitivului<br>- Tipul sistemului de fisiere (NTFS/FAT/FAT32)<br>- Numele Volumului/Partitiei (In cazul dispozitivelor de stocare date) | |
| Solutia trebuie sa poata lua urmatoarele actiuni la conectarea unui dispozitiv periferic:<br>- Blocare: Sa nu permita instalarea acestuia<br>- Monitorizare: Sa genereze un eveniment ce contine detalii despre dispozitiv<br>- Fortare mod utilizare ReadOnly: In cazul dispozitivelor de stocare date, acestea se vor utiliza doar pentru citirea datelor de pe ele | |
| Solutia trebuie sa poata preveni executarea de cod si aplicatii direct de pe dispozitive externe. De asemenea, trebuie sa vina si cu un mecanism de marcare a aplicatiilor permise. | |
| Solutia trebuie sa permita aplicarea de politici diferite in functie de locatia utilizatorlui. Ex: Sa nu poata conecta imprimante atunci cand nu se afla in perimetrul retelei, dar cand revine in retea sa le poata utiliza fara sa necesite actiuni suplimentare din partea utilizatorului. | |
| Solutia trebuie sa ofere un mecanism de justificare a unor actiuni care contravin cu politica de securitate a datelor. | |
| Solutia trebuie sa permita construirea unei liste de dispozitive permise si corelarea acestei liste la utilizatori/grupuri de utilizatori din Active Directory, astfel incat acestia sa poata utiliza dispozitivele indiferent de calculatorul la care se afla. | |
| Solutia trebuie sa permita alertarea administratorului atunci cand sunt copiate informatii pe dispozitive externe de stocare date. | |
| Solutia trebuie sa permita filtrarea fisierelor ce sunt copiate pe dispozitive externe de stocare date dupa extensie si/sau tip de fisier. Tipul de fisier trebuie identificat indiferent de extensia acestuia. (Ex: Blocarea copierii fisierelor Microsoft Office Word, Adobe Reader PDF) | |
| Solutia nu poate fi oprita de utilizator chiar daca acesta are dreptul de administrator local. | |
| Solutia trebuie sa permita crearea unei reguli de shadowing (duplicare) a fisierelor copiate pe dispozitive externe atunci cand anumite criteria sunt indeplinite (Ex: Un anumit utilizator, grup de utilizatori, tipul fisierului, extensia fisierului). Duplicatul fisierului trebuie sa poata fi accesat numai de cei ce au acest drept in consola de administrare. | |

## 1.3 Filtrarea Web pentru endpoint-uri

| | |
|---|---|
| Solutia trebuie sa permita crearea de seturi multiple de politici diferite si asignarea lor atit catre noduri individuale cat si catre grupuri de noduri. | |
| Solutia trebuie sa prezinte rapoarte predefinite care sa contina cel putin:<br>- Top 100 site-uri blocate<br>- Top Sites Grouped by Content<br>- Visit Log<br>- Download log<br>De asemenea solutia trebuie sa permita customizarea rapoartelor | |
| Solutia trebuie sa pemita blocarea site-urilor de phising. | |
| Solutia trebuie sa permita blocarea paginilor de phising din site-uri autorizate sau continute in mesaje email | |
| Solutia trebuie sa poata bloca descarcarile de fisiere malitioase | |
| Solutia trebuie sa poata bloca site-urile malitioase si cele care genereaza spam | |
| Solutia trebuie sa ofere acelasi nivel de protectie si daca endpoint-ul nu este conectat in reteaua companiei | |
| Solutia trebuie sa genereze raport cu privire la site-urile pe care utilizatorii incerca sa le acceseze | |

| | |
|---|---|
| Solutia trebuie sa permita controlul accesului la site-uri bazat pe un indice de siguranta, tipul de continut pe care il au si numele de URL sau de domeniu. | |
| Solutia trebuie sa poata bloca bazandu-se atit pe continut cat si pe reputatia site-ului accesat | |
| Solutia trebuie sa suporte urmatoarele browsere, prin instalarea unui plugin:<br>- Microsoft Internet Explorer 11<br>- Google Chrome - versiunea curenta<br>- Mozilla Firefox - versiunea curenta<br>- Mozilla Firefox ESR (Extended support release) – versiunea curenta si anterioare | |

## 1.4 Consola de administrare

| | |
|---|---|
| Consola de administrare trebuie sa se poata instala pe unul din urmatoarele sisteme de operare:<br>• Windows Server 2008 R2 64 bit<br>• Windows Server 2008 64-bit<br>• Windows Server 2012<br>• Windows Server 2012 R2<br>• Windows Server 2016 | |
| Consola trebuie sa dispuna de o unealta de verificare a prerechizitelor necesare pentru a instala versiuni actualizate ale produselor. | |
| Consola trebuie sa contina o unealta de diagnosticare si remediere automata a problemelor | |
| Solutia trebuie sa dispuna de o unealta care sa permita colectarea automata a logurilor si a altor informatii necesare pentru deschiderea unui caz de suport. | |
| Consola permite pe langa distribuirea componentelor native si impachetarea aplicatiilor de la terti si instalarea acestora pe statiile de lucru. | |
| Instalarea si administrarea componentelor antivirus, web control, threat detection, firewall, prevenire a intruziunilor, de control al dispozitivelor externe, de control al aplicatiilor, de DLP si etichetare si clasificare si criptare trebuie sa se faca dintr-o singura consola. | |
| Consola permite atribuirea automata a politicilor pe statii si servere in functie de specificatiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare) | |
| Sincronizarea dintre server si client trebuie sa se faca dinspre client catre server. | |
| Consola de administrare trebuie sa se poata integra cu Active Directory. | |
| Consola de administrare trebuie sa poata fi instalata intr-un mediu virtual. | |
| Consola trebuie sa poate fi instalata in mediu Microsoft Cluster de tip activ/pasiv. | |
| Consola de administrare foloseste Microsoft SQL. | |
| Consola de administrare permite instalarea unei component de comunicare in DMZ pentru sincronizarea sistemelor prin internet. | |
| Comunicarea din component si serverul de administrare trebuie sa se faca prin intermediul unui singur agent. | |
| Componentele de antivirus, firewall, web control, prevenire a intruziunilor si control al dispozitivelor externe trebuie sa poata rula sub o singura iconita in Tray Bar pentru a permite usor identificarea acestora. | |

| | |
|---|---|
| Solutia trebuie sa permita filtrarea evenimentelor ce sunt generate de componentele aflate pe statiile de lucru astfel incat baza de date sa nu se incarce cu informatii considerate inutile. | |
| Solutia trebuie sa permita configurare unui mesaj de login. | |
| Solutia poate folosi un proxy pentru contactarea serverului de actualizare al producatorului. | |
| Accestul in consola de administrare poate fi facut pe baza credentialelor din Active Directory. | |
| Accesul in consola de management poate fi facut pe baza certificatelor x509. | |
| Consola de administrare trebuie sa permita creare de roluri in mod granular pentru cei ce o administreaza. | |
| Actiunile utilizatorilor in consola trebuiesc audidate. | |
| Consola trebuie sa permita construirea unei liste de contacte in vederea folosirii acestora pentru notificari prin mesagerie electronica (E-mail). | |
| Canalul de comunicatie dintre serverul de administrare si componentele distribuite pe calculatoare trebuie sa fie criptat. | |
| Componenta ce asigura canalul de comunicatie dintre server si statii de lucru trebuie sa fie valitata din punct de vedere al securitatii. (Ex: FIPS, Common Criteria, Etc.) | |
| Canalul de comunicatie dintre consola si cei ce o acceseaza trebuie sa fie criptat. | |
| Consola de administrare trebuie sa poata fi accesata de pe orice computer din retea in mod securizat, fara necesitatea instalarii de software aditional. | |
| Daca serverul de administrare este accesat prin intermediul unei interfete web trebuie sa fie posibil importul unui certificat ssl generat de o autoritate locala, inlocuind astfel pe cel auto-generat. | |
| Intervalul de sincronizare intre server si componente poate fi modificat. | |
| Intervalul de transmitere a evenimentelor de pe client catre server poate fi modificat. | |
| Consola trebuie sa poata detecta prezenta pe retea a sistemelor noi aparaute prin intermediul unor senzori. | |
| Consola trebuie sa foloseasca un propriu index pentru a identifica si actualize datele despre sistemele care isi schimba proprietati precum nume,ip si configuratie hardware; | |
| Consola permite automatizarea de sarcini de instalare/dezinstalare a componentelor pe statiile de lucru, de rulare a rapoartelor si de transmiterea de notificari de prin mesagerie electronica. | |
| Consola trebuie sa prezinte cel putin urmatoarele informatii despre sistemele administrate : numele sistemului, utilizatorul logat, produsele instalate, tipul de system de operare si adresa IP . | |
| Consola trebuie sa se integreze cu sisteme de ticketing extern precum BMC Remedy si HP OpenView. | |
| Serverul de administrare trebuie sa fie capabil sa declanseze actiuni automate atunci cand anumite conditii sunt indeplinite (Ex: Generarea unui eveniment pe server, pe o statie de lucru, detectarea unui nou sistem pe retea) | |
| Consola trebuie sa permite aplicarea de politici diferite pentru sisteme pe:<br>- Sisteme individuale<br>- Grupuri de sisteme<br>- Sisteme din AD ce sunt acelasi OU | |
| Consola trebuie sa stie sa lanseze automat aplicatii externe si sa injecteze parametrii din evenimente. | |
| Consola permite accesarea logului componentei de sincronizare de pe sisteme in timp real prin intermediul unui serviciu web. | |
| Consola trebuie sa poata fi instalata pe o masina fizica sau virtuala cu urmatoarele caracateristici fizice minime: | |

| | |
|---|---|
| - Sistem de operare: Server Windows 2016, Server Windows 2012 Release 2 (R2), Server Windows 2012, Server Windows 2008 cu SP2 64-bit (Standard, Enterprise sau Datacenter), Server Windows 2008 R2 64-bit (Standard, Enterprise, or Datacenter)<br>- Server virtual: VMware ESX/ESXi 5.x sau mai recent, Citrix XenServer 6.0, Citrix XenServer 5.5 Update 2, Windows Server 2012 Hyper-V, Windows Server 2008 R2 Hyper-V sau mai noi<br>- Baza de date: Server SQL 2016, Server SQL 2016 Express, Server SQL 2014, Server SQL 2014 Express, Server SQL 2012 Express, Server SQL 2012, Server SQL 2008 with SP1/SP2/R2 Standard, Enterprise, Workgroup, Express<br>- Cerinte hardware minimale:<br>o memorie RAM 8GB<br>o spatiu pe Hard Disk: 20 GB pentru aplicatie, 100 Gb pentru baza de date<br>o Procesor: Intel Premium D 64-bit sau mai recent, cu frecventa de 2,66GHz sau mai mare<br>o Placa de retea: 100Mb sau mai mult | |

## 1.5 Raportarea

| | |
|---|---|
| Consola de administrare poate asigura generarea de rapoarte despre nodurile administrate si despre evenimentele generate de ele. | |
| Consola trebuie sa permita crearea de noi rapoarte in mod granular cu informatii extrase din evenimente, sau despre sistemele administrate. | |
| Rapoartele pot if generate sub forma de tabel, pie chart, buble chart, lista, sumar, line chart sau grafic istoric. | |
| Rapoartele pot fi exportate in format pdf, csv, html. | |
| Rapoartele pot fi personalizate cu logo-ul companiei. | |
| Rapoartele pot fi salvate ca fisiere sau trimise prin e-mail. | |
| Raportele pot fi exportate intr-un format arhivat pentru conservare de latime de banda si expediate automat pe e-mail unor destinatii presetate. | |
| Solutia trebuie sa permita agregarea evenimentelor generate de componenta de prevenire a intruziunilor pe categorii precum: nume sistem, ip soursa atacator, ip destinatie atac, nume amenintare, categorie amenintare, factor de risc, gruprare logica in consola. | |
| Consola permite evaluarea evenimentelor primite flitrarea evenimentelor primite de la statiile de lucru pentru o mai buna identificare a informatiilor relevante. | |
| Se pot genera rapoarte utilizand:<br>- Logul de audit administrativ<br>- Detalii despre sitemele administrate (Detalii de configurare, hardware, utilizator)<br>- Evenimente de la siteme<br>- Informatii despre politicile si sarcinilie aplicate sistemelor<br>- Informatii furnizate de senzori | |
| Solutia ofertata va avea licenta perpetua si va include subscriptiile pe o durata de 1 an la serviciile de actualizari de software si semnaturi. Solutia va beneficia de suport tehnic al producatorului pentru o perioada de 1 an. | |
| | |
| | |

| | |
|---|---|
| • **Prezenţa interfeței de administrare, analizarea informațiilor comune cu alte sisteme EndPoint Protection, SIEM, DLP reprezintă un avantaj important în comparație cu alte soluții.**<br>• **Disponibilitatea și poziția produsului în "Gartner Square" reprezintă un avantaj puternic față de alte soluții.** | |