

Matricea de conformitate conform cerințelor solicitate la caiet de sarcini pentru Soluții software de tip EPP

Cerintele tehnice minime	Cerintele tehnice propuse
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: - Windows 10 Versiunile 1507, 1511, 1607, 1703 - Windows 10 IoT Enterprise - Windows 8.1, Update 1, August 2014 update rollup - Windows 8 (Win NT 6.2) Editions: Basic / Pro / Enterprise - Windows 7 (Home Premium / Professional / Ultimate / Enterprise) - Windows Vista - Windows Vista Business/Ultimate for Embedded Systems - Windows 7 Professional/Ultimate for Embedded Systems - Windows Server 2016 Editions: Datacenter / Essentials / Standard installed in „Server with Desktop Experience” mode - Windows Server 2012 Release 2 (R2) , R2 Update 1, R2 August 2014 update - Windows Server 2008, HyperV, Standard, Datacenter, Enterprise, Foundation, Web, HPC - VMware ESX, ESXi - Citrix XenApp 5.0, 5.6, 6.0, 6.5, 7.5, 7.6 - Citrix Xen Guest - MAC OS X 10.7 sau mai nou	1.1 Produsul oferat: McAfee Complete Endpoint Threat Protection Solutia oferata asigura protectie pentru statii de lucru si servere cu urmatoarele sisteme de operare: - Windows 10 Versiunile 1507, 1511, 1607, 1703 - Windows 10 IoT Enterprise - Windows 8.1, Update 1, August 2014 update rollup - Windows 8 (Win NT 6.2) Editions: Basic / Pro / Enterprise - Windows 7 (Home Premium / Professional / Ultimate / Enterprise) - Windows Vista - Windows Vista Business/Ultimate for Embedded Systems - Windows 7 Professional/Ultimate for Embedded Systems - Windows Server 2016 Editions: Datacenter / Essentials / Standard installed in „Server with Desktop Experience” mode - Windows Server 2012 Release 2 (R2) , R2 Update 1, R2 August 2014 update - Windows Server 2008, HyperV, Standard, Datacenter, Enterprise, Foundation, Web, HPC - VMware ESX, ESXi - Citrix XenApp 5.0, 5.6, 6.0, 6.5, 7.5, 7.6 - Citrix Xen Guest - MAC OS X 10.7 sau mai nou
Solutia trebuie sa ofere protectie pe sisteme de operare pe 32/64 de biti.	Solutia asigură 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 asigură 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 oferă disponibilitatea dezactivarii solutiei de Endpoint Security la statie inclusiv si cu 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 oferă 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 efectuează scanarea 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 are capacitatea 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 permite 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 permite 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 prezinta 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 asigură detectarea de 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.	Solutia este capabila sa detecteze scripturi malitioase pe pagini web.
Solutia ofera protectie pentru masinile virtuale ce ruleaza pe statii.	Solutia asigură 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	Solutia utilizează 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	Solutia oferă agentul unic care poate fi instalat in mod silentios, fara alertarea utilizatorului.
Actualizarile sa fie instalate in mod silentios, fara alertarea utilizatorului	Solutia asigură instalarea actualizarii in mod silentios, fara alertarea utilizatorului
Clientii antivirus pentru workstation trebuie sa contina optiunea de pauza si reluare a scanarilor	Solutia oferă ca clientii antivirus pentru workstation să contină optiunea de pauza si reluare a scanarilor
Solutia poate bloca accesul la directoare partajate pentru a bloca raspandirea codului malitios.	Solutia oferă blocarea accseului la directoare partajate pentru a bloca raspandirea codului malitios.
Solutia are capacitatea de a detecta si de a curata cod malitios.	Solutia deține 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 oferă posibilitatea de a 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 deține capacitate de scanare euristica si poate detecta fisiere infectate pentru care nu exista semnatura in baza de date.
Solutia poate proteja impotriva: - Rularii de aplicatii din directorul TEMP al sistemului de operare - Conexiunilor IRC, TFTP, FTP, SMTP cu exceptia aplicatiilor cunoscute si permise - Inregistrarii automata a programelor ca servicii - Modificarii/crearii de executabile, extensii, procese si setari	Solutia asigură protecție impotriva : - Rularii de aplicatii din directorul TEMP al sistemului de operare - Conexiunilor IRC, TFTP, FTP, SMTP cu exceptia aplicatiilor cunoscute si permise - Inregistrarii automata a programelor ca servicii - 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 oferă 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 are posibilitatea de a 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 permite actiunile de prevenire a accesului la fisier, de curatare si de stergere a fisierului cind se detecteaza cod malitios.
Solutia trebuie sa poata scana la cerere: - Memoria sistemelor - Procesele ce ruleaza - Partitiile locale - Dispozitivele atasate de stocare date - Directoare din retea - Registrii	Solutia oferă scanarea la cerere : - Memoria sistemelor - Procesele ce ruleaza - Partitiile locale - Dispozitivele atasate de stocare date - Directoare din retea - Registrii
Solutia trebuie sa ofere functionalitatea de intoarcere la baza de date de semnături de virusi anterioara.	Solutia oferă functionalitatea de intoarcere la baza de date de semnături de virusi anterioara.
Solutia trebuie sa utilizeze un mecanism de caching pentru fisierele deja scanate ce nu au suferit modificari.	Solutia utilizează 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 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 este 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 fisielerelor/proceselor/cheilor de registrii ale acesteia.	Solutia contine mecanisme de protectie ce nu permit utilizatorului sau aplicatiilor malitioase sa intervina asupra fisielerelor/proceselor/cheilor de registrii ale acesteia.
Solutia trebuie sa permita carantinarea fisielerelor infectate si sa ofere posibilitatea restaurarii acestora direct din consola de administrare, fara a fi nevoie sa se intervina asupra sistemului.	Solutia permite carantinarea fisielerelor 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 permite actualizarea semnaturilor 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.	Solutia permite 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 semnături pentru a evita supraincercarea retelei.	Solutia asigură ca actualizarea să permită definirea unui interval de timp in care sistemele vor incepe aleator sa descarce noile semnături pentru a evita supraincercarea retelei.
Solutia trebuie sa fie recunoscuta de sistemele de operare Microsoft Windows in Security Center.	Solutia este recunoscuta de sistemele de operare Microsoft Windows in Security Center.
Solutia trebuie sa poata scana si detecta cod malitios in arhive.	Solutia poate scana si detecta cod malitios in arhive

Solutia trebuie sa ofere protectie impotriva programelor de tip Mass Mailer	Solutia oferă protecție împotriva programelor de tip Mass Mailer
Solutia trebui sa detecteze codul malitios inainte de executie.	Solutia detecteaza codul malitios inainte de executie.
Solutia trebuie sa permita configurarea unei politici de identificarea a aplicatiilor de tipul P2P.	Solutia permite configurarea unei politici de identificarea a aplicatiilor de tipul P2P.
Solutia trebuie sa poata scana si detecta programe malitioase in timp real.	Solutia poate scana si detecta programe malitioase in timp real.
Solutia trebuie sa utilizeze mecanisme de analizează a fisierelor, aplicatiilor și a decide ce să facă pe baza reputației, regulilor și pragurilor de reputație.	Solutia permite utilizarea mecanismelor de analiza a fisierelor, aplicatiilor și poate decide ce să facă pe baza reputației, regulilor și pragurilor de reputație.
Solutia trebuie sa ofere capacitatea de a ști care sunt sistemele sau dispozitivele compromise și modul în care amenințarea se răspândesc.	Solutia oferă capacitatea de a ști care sunt sistemele sau dispozitivele compromise și modul în care amenințarea se răspândesc.
Solutia trebuie sa ofere o tehnologie de detectare în timp real bazată pe comportament si care monitorizeaza activitatile unei aplicatii iar in caz ca depisteaza un cod malitios să îl blocheaze imediat.	Solutia oferă o tehnologie de detectare în timp real bazată pe comportament si care monitorizeaza activitatile unei aplicatii iar in caz ca depisteaza un cod malitios să îl blocheaze imediat.
Solutia trebuie sa ofere un mecanism care inspectează fișierele și activitățile suspecte pe un sistem și detectează codul malitios pe baza de machine-learning.	Solutia oferă un mecanism care inspectează fișierele și activitățile suspecte pe un sistem și detectează codul malitios pe baza de machine-learning.

1.2 Controlul dispozitivelor periferice

Componenta trebuie sa poata rula cel putin pe: - Microsoft Windows Vista (32-bit) - Microsoft Windows 7 (32/64-bit) - Microsoft Windows 8 (32/64-bit) - Microsoft Windows 8.1 (32/64-bit) - Microsoft Windows 10 (32/64-bit) - Microsoft Windows 10 TH2 (32/64-bit) - Microsoft Windows 10 RS1 (32/64-bit) - Microsoft Windows 10 RS2 (32/64-bit) - Microsoft Windows 2008 (32/64-bit) - Microsoft Windows 2008 R2 (32/64-bit) - Microsoft Windows 2012 (64-bit) - Microsoft Windows 2012 R2 (64-bit) - OS X 10.9 sau mai nou - Citrix XenApp 6.0/6.5/7.5/7.6/7.9 - Citrix XenDesktop 5.5/5.6/7.0/7.1/7.5/7.6/7.8 - VMware View 4.6/5.0/5.1/5.2/5.3/6.0/6.2 - VMware Hyper-V 6.3.9600	Solutia asigură ca componenta să ruleze pe urmatoarele platforme : - Microsoft Windows Vista (32-bit) - Microsoft Windows 7 (32/64-bit) - Microsoft Windows 8 (32/64-bit) - Microsoft Windows 8.1 (32/64-bit) - Microsoft Windows 10 (32/64-bit) - Microsoft Windows 10 TH2 (32/64-bit) - Microsoft Windows 10 RS1 (32/64-bit) - Microsoft Windows 10 RS2 (32/64-bit) - Microsoft Windows 2008 (32/64-bit) - Microsoft Windows 2008 R2 (32/64-bit) - Microsoft Windows 2012 (64-bit) - Microsoft Windows 2012 R2 (64-bit) - OS X 10.9 sau mai nou - Citrix XenApp 6.0/6.5/7.5/7.6/7.9 - Citrix XenDesktop 5.5/5.6/7.0/7.1/7.5/7.6/7.8 - VMware View 4.6/5.0/5.1/5.2/5.3/6.0/6.2 - VMware Hyper-V 6.3.9600
Solutia trebuie sa poata colecta informatii din Microsoft Active Directory.	Solutia asigură colectarea informatiilor din Microsoft Active Directory.
Solutia trebuie sa prezinte un mecanism propriu de instalare a agentilor pe statiile de lucru sau alte sisteme.	Solutia prezinta un mecanism propriu de instalare a agentilor pe statiile de lucru sau alte sisteme.

Solutia trebuie sa permita creare de politici in mod granular de permitere/blocare a dispozitivelor periferice pe baza informatiilor precum: - ID Producator - ID Model Dispozitiv Periferic - Tipul de dispozitiv - Clasa dispozitivului detectat de sistemul de operare - BUS Conectare (USB, S-ATA, ETC.) - Numele Dispozitivului - Tipul sistemului de fisiere (NTFS/FAT/FAT32) - Numele Volumului/Partitiei (In cazul dispozitivelor de stocare date)	Solutia permite creare de politici in mod granular de permitere/blocare a dispozitivelor periferice pe baza informatiilor precum: - ID Producator - ID Model Dispozitiv Periferic - Tipul de dispozitiv - Clasa dispozitivului detectat de sistemul de operare - BUS Conectare (USB, S-ATA, ETC.) - Numele Dispozitivului - Tipul sistemului de fisiere (NTFS/FAT/FAT32) - Numele Volumului/Partitiei (In cazul dispozitivelor de stocare date)
Solutia trebuie sa poata lua urmatoarele actiuni la conectarea unui dispozitiv periferic: - Blocare: Sa nu permita instalarea acestuia - Monitorizare: Sa genereze un eveniment ce contine detalii despre dispozitiv - Fortare mod utilizare ReadOnly: In cazul dispozitivelor de stocare date, acestea se vor utiliza doar pentru citirea datelor de pe ele	Solutia permite gestionarea urmatoarelor actiuni la conectarea unui dispozitiv periferic: - Blocare: Sa nu permita instalarea acestuia; - Monitorizare: Sa genereze un eveniment ce contine detalii despre dispozitiv; - 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 are capacitatea de a preveni executarea de cod si aplicatii direct de pe dispozitive externe. De asemenea, vine si cu un mecanism de marcare a aplicatiilor permise.
Solutia trebuie sa permita aplicarea de politici diferite in functie de locatia utilizatorului. 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 permite aplicarea diferitor politici in functie de locatia utilizatorului.
Solutia trebuie sa ofere un mecanism de justificare a unor actiuni care contravin cu politica de securitate a datelor.	Solutia oferă 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 permite construirea unei liste de dispozitive permise si corelarea acestei liste la utilizatori/grupuri de utilizatori din Active Directory, astfel incat acestia pot 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 permite 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 permite 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 are capacitatea de a stabili restrictii la dezactivarea solutiei pe statie inclusiv si cu drepturi 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.	Solutia permite 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 poate 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 permite 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: - Top 100 site-uri blocate - Top Sites Grouped by Content - Visit Log - Download log De asemenea solutia trebuie sa permita customizarea rapoartelor	Solutia permite prezentarea rapoartelor predefinite care contine: - Top 100 site-uri blocate - Top Sites Grouped by Content - Visit Log - Download log Solutia permite customizarea rapoartelor.
Solutia trebuie sa permita blocarea site-urilor de phishing.	Solutia permite blocarea site-urilor de phishing.
Solutia trebuie sa permita blocarea paginilor de phishing din site-uri autorizate sau continute in mesaje email	Solutia permite blocarea paginilor de phishing din site-uri autorizate sau continute in mesaje email.
Solutia trebuie sa poata bloca descarcarile de fisiere malitioase	Solutia poate bloca descarcarile de fisiere malitioase.
Solutia trebuie sa poata bloca site-urile malitioase si cele care genereaza spam	Solutia poate 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 retea companiei	Solutia oferă acelasi nivel de protectie si daca endpoint-ul nu este conectat in retea companiei.
Solutia trebuie sa genereze raport cu privire la site-urile pe care utilizatorii incerca sa le acceseze	Solutia generează 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 permite 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 poate bloca bazandu-se atit pe continut cat si pe reputatia site-ului accesat.
Solutia trebuie sa suporte urmatoarele browsere, prin instalarea unui plugin: - Microsoft Internet Explorer 11 - Google Chrome - versiunea curenta - Mozilla Firefox - versiunea curenta - Mozilla Firefox ESR (Extended support release) – versiunea curenta si anterioare	Solutia suportă urmatoarele browsere, prin instalarea unui plugin: - Microsoft Internet Explorer 11 - Google Chrome - versiunea curenta - Mozilla Firefox - versiunea curenta - 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: • Windows Server 2008 R2 64 bit • Windows Server 2008 64-bit • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016	Solutia se instaleaza pe unul din urmatoarele sisteme de operare: - Windows Server 2008 R2 64 bit - Windows Server 2008 64-bit - Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2016
Consola trebuie sa dispuna de o unealta de verificare a prerechizitelor necesare pentru a instala versiuni actualizate ale produselor.	Solutia oferă o consola care dispune 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 oferă o consola care contine 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.	Solutia dispune de o unealta care permite 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.	Solutia oferă o consolă care 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.	Solutia permite ca 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 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)	Solutia oferă o consolă care 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.	Solutia permite ca sincronizarea dintre server si client sa se faca dinspre client catre server.
Consola de administrare trebuie sa se poata integra cu Active Directory.	Solutia permite integrarea consolei de administrare cu Active Directory.
Consola de administrare trebuie sa poata fi instalata intr-un mediu virtual.	Solutia permite instalarea consolei de administrare intr-un mediu virtualizat.
Consola trebuie sa poata fi instalata in mediu Microsoft Cluster de tip activ/pasiv.	Solutia permite instalarea consolei de administrare in mediu Microsoft Cluster de tip activ/pasiv.
Consola de administrare foloseste Microsoft SQL.	Solutia este implementată cu Microsoft SQL.
Consola de administrare permite instalarea unei component de comunicare in DMZ pentru sincronizarea sistemelor prin internet.	Solutia oferă instalarea unei componente 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.	Solutia oferă ca comunicarea din component si serverul de administrare 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 oferă rularea componentelor de antivirus, firewall, web control, prevenire a intruziunilor si control al dispozitivelor externe 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 permite 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 permite configurarea unui mesaj de login.
Solutia poate folosi un proxy pentru contactarea serverului de actualizare al producatorului.	Solutia permite folosirea unui proxy pentru contactarea serverului de actualizare al producatorului.
Accesul in consola de administrare poate fi facut pe baza credentialelor din Active Directory.	Solutia permite accesul in consola de administrare pe baza credentialelor din Active Directory.
Accesul in consola de management poate fi facut pe baza certificatelor x509.	Solutia permite accesul in consola de administrare pe baza certificatelor x509.
Consola de administrare trebuie sa permita creare de roluri in mod granular pentru cei ce o administreaza.	Solutia asigură ca consola de administrare să permită creare de roluri in mod granular pentru cei ce o administreaza.
Actiunile utilizatorilor in consola trebuiesc auditate.	Solutia permite auditul actiunilor utilizatorilor in consola.
Consola trebuie sa permita construirea unei liste de contacte in vederea folosirii acestora pentru notificari prin mesagerie electronica (E-mail).	Solutia permite 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.	Solutia asigură criptarea canalul de comunicatie dintre serverul de administrare si componentele distribuite pe calculatoare
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.)	Solutia oferă validarea din punct de vedere al securitatii a componentei ce asigură canalul dintre server si statii de lucru.
Canalul de comunicatie dintre consola si cei ce o acceseaza trebuie sa fie criptat.	Solutia oferă criptarea canalul de comunicatie dintre consola si cei ce o acceseaza.
Consola de administrare trebuie sa poata fi accesata de pe orice computer din retea in mod securizat, fara necesitatea instalarii de software aditional.	Solutia oferă ca consola de administrare să poată fi accesată 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.	Solutia oferă posibilitatea importului unui certificat ssl generat de o autoritate locala, inlocuind astfel pe cel auto-generat.
Intervalul de sincronizare intre server si componente poate fi modificat.	Solutia oferă posibilitatea de a modifica intervalul de sincronizare intre server si componente.
Intervalul de transmitere a evenimentelor de pe client catre server poate fi modificat.	Solutia oferă posibilitatea de a modifica intervalul de transmitere a evenimentelor de pe client catre server.
Consola trebuie sa poata detecta prezenta pe retea a sistemelor noi aparate prin intermediul unor senzori.	Solutia oferă ca consola să poată detecta prezența pe retea a sistemelor noi aparate 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;	Solutia oferă o consola care folosaste 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.	Solutia oferă o consola care 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 .	Solutia o consolă care permite prezentarea 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.	Solutia oferă o consola care sa integreaza 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)	Solutia oferă serverul de administrare care este 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: - Sisteme individuale - Grupuri de sisteme - Sisteme din AD ce sunt acelasi OU	Solutia oferă o consola care permite aplicarea de politici diferite pentru sisteme pe: - - Sisteme individuale - Grupuri de sisteme - Sisteme din AD ce sunt acelasi OU
Consola trebuie sa stie sa lanseze automat aplicatii externe si sa injecteze parametrii din evenimente.	Solutia oferă o consola care 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.	Solutia oferă o consola care 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 caracteristici 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) - 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 - 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 - Cerinte hardware minime: - o memorie RAM 8GB - o spatiu pe Hard Disk: 20 GB pentru aplicatie, 100 Gb pentru baza de date	Solutia oferă o consola care se instaleaza pe o masina fizica sau virtuala cu urmatoarele caracteristici 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) - 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 - 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 - Cerinte hardware minime: • memorie RAM 8GB • spatiu pe Hard Disk: 20 GB pentru aplicatie, 100 Gb pentru baza de date • Procesor: Intel Premium D 64-bit sau mai recent, cu frecventa de 2,66GHz sau mai mare

○ Procesor: Intel Premium D 64-bit sau mai recent, cu frecventa de 2,66GHz sau mai mare ○ Placa de retea: 100Mb sau mai mult	● 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.	Solutia oferă o consola care 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.	Solutia oferă o consola care permite crearea rapoartelor in mod granular cu informatii extrase din evenimente, sau despre sistemele administrate.
Rapoartele pot fi generate sub forma de tabel, pie chart, bubble chart, lista, sumar, line chart sau grafic istoric.	Solutia oferă generarea rapoartelor sub forma de tabel, pie chart, bubble chart, lista, sumar, line chart sau grafic istoric.
Rapoartele pot fi exportate in format pdf, csv, html.	Solutia oferă exportarea rapoartelor in format pdf, csv, html.
Rapoartele pot fi personalizate cu logo-ul companiei.	Solutia oferă personalizarea rapoartelor cu logo-ul companiei.
Rapoartele pot fi salvate ca fisiere sau trimise prin e-mail.	Solutia oferă salvarea rapoartelor 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 oferă exportarea rapoartelor 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 sursa atacator, ip destinatie atac, nume amenintare, categorie amenintare, factor de risc, grupare logica in consola.	Solutia permite agregarea evenimentelor generate de componenta de prevenire a intruziunilor pe categorii precum: nume sistem, ip sursa atacator, ip destinatie atac, nume amenintare, categorie amenintare, factor de risc, grupare logica in consola.
Consola permite evaluarea evenimentelor primite filtrarea evenimentelor primite de la statiile de lucru pentru o mai buna identificare a informatiilor relevante.	Solutia oferă o consola ce permite evaluarea evenimentelor primite filtrarea evenimentelor primite de la statiile de lucru pentru o mai buna identificare a informatiilor relevante.
Se pot genera rapoarte utilizand: - Logul de audit administrativ - Detalii despre sistemele administrate (Detalii de configurare, hardware, utilizator) - Evenimente de la sisteme - Informatii despre politicile si sarcinile aplicate sistemelor - Informatii furnizate de senzori	Solutia oferă generarea rapoartelor utilizand: - Logul de audit administrativ; - Detalii despre sistemele administrate (Detalii de configurare, hardware, utilizator); - Evenimente de la sisteme; - Informatii despre politicile si sarcinile aplicate sistemelor; - 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 semnături. Solutia va beneficia de suport tehnic al producatorului pentru o perioada de 1 an.	Solutia se va livra cu licenta perpetua si include subscriptiile pe o durata de 1 an la serviciile de actualizari de software si semnături. Solutia ofertata va beneficia de suport tehnic al producatorului pentru o perioada de 1 an.
Prezența interfeței și instrumentariului de administrare, analiza informațiilor comune cu alte sisteme EndPoint Protection, SIEM, DLP este obligatoriu.	● Produsul ofertat oferă posibilitatea de integrare cu alte solutii de DLP, SIEM si alte solutii oferite de producatorul McAfee, astfel asigurand o administrare centralizata dintr-o singura consola.

Disponibilitatea și poziția produsului în "Gartner Square" reprezintă un avantaj puternic față de alte soluții.	• Produsul oferit se regăsește în cadranul de Lideri "Gartner" În oferta sunt incluse serviciile de instalare, integrare și configurarea soluției.
--	---