

Anexa 2

Matricea de conformitate conform cerințelor solicitate la caiet de sarcini pentru soluții software DLP

Cerințe tehnice minimale	Cerințe tehnice propuse
1. Integrare cu infrastructura IT 1.1 Soluția trebuie să poată rula cel puțin pe: - Windows 8 și 8.1, 10, Enterprise și Professional, 32-bit and 64-bit - Windows 7 SP1 sau mai recente Enterprise și Business, 32-bit and 64-bit - Windows Server 2008/2008R2 - Windows Server 2012/2012R2 - Windows Server 2016 - OS X Yosemite - OS X Mavericks - OS X Mountain Lion - OS X El Capitan 1.2 Soluția suportă următoarele soluții de tip directory: Microsoft AD și Open LDAP 1.3 Soluția trebuie să ofere funcționalități de instalare la distanță pentru agenții de monitorizare astfel încât la momentul instalării sau upgrade să nu fie necesară restartarea sistemelor. 1.4 Soluția trebuie să ofere suport pentru mediile virtuale incluzând VDI, aceasta însemnând că fiecare politică trebuie să activeze și alerteze pe baza de utilizator. Politicile per user trebuie să se aplice pe sesiuni multiple și să ofere un control și o flexibilitate pe shared terminals sau pe VDI. 1.5 Soluția trebuie să ofere mecanisme de integrare COTS cu soluții consacrate de IRM Right Management cum ar fi Microsoft Right Management Services sau Seclore FileSecure. 2. Politici de Securitate 2.1 Descrieți în detaliu aplicațiile, protocoalele și canalele de I/O pe care soluția le poate folosi. 2.2 Soluția aplică politici bazate pe conținut confidential pentru cel puțin 300 de tipuri de fișiere. 2.3 Soluția trebuie să ofere mecanisme interne de clasificare manuală pentru fișierelor Microsoft Office sau PDF, soluția propusă va folosi un program de ADD-on pentru MS Office și la momentul salvării utilizatorii vor fi direcționați pentru alegerea nivelului de clasificare intern. 2.4 Soluția trebuie să facă clasificarea conținutului chiar dacă acesta este arhivat și trebuie să extragă datele din cel puțin 10 nivele de arhivare. 2.5 Soluția trebuie să suporte detectarea documentelor înregistrate/amprentate și clasificate. Descrieți sursele pe care le poate folosi. 2.6 Soluția trebuie să aibă capacitatea de a proteja datele bazându-se pe punctul lor de origine/creare.	1. Produsul oferit: McAfee Total Protection for Data Loss Prevention Appliance Software: 1.1 Soluția poate rula pe următoarele Sisteme de Operare: - Windows 8 și 8.1, 10, Enterprise și Professional, 32-bit and 64-bit - Windows 7 SP1 sau mai recente Enterprise și Business, 32-bit and 64-bit - Windows Server 2008/2008R2 - Windows Server 2012/2012R2 - Windows Server 2016 - OS X Yosemite - OS X Mavericks - OS X Mountain Lion - OS X El Capitan 1.2 Soluția suportă Microsoft AD și Open LDAP; 1.3 Soluția oferă funcționalități de instalare la distanță pentru agenții de monitorizare astfel încât la momentul instalării sau upgrade nu este necesară restartarea sistemelor; 1.4 Soluția oferă suport pentru mediile virtuale incluzând VDI, fiecare politică activează și alertează pe baza de utilizator. Politicile per user se aplică pe sesiuni multiple și oferă un control și o flexibilitate pe shared terminals sau pe VDI; 1.5 Soluția oferă mecanisme de integrare COTS cu soluții consacrate de IRM Right Management cum este Microsoft Right Management Services sau Seclore FileSecure; 2. Politici de Securitate 2.1 Soluția are capacitatea de a inspecta următoarele protocoale: SMTP*; Telnet; IMAP*; FTP; POP3*; IRC; HTTP; HTTPS; SMB*; LDAP, de asemenea poate analiza traficul care este încapsulat în SOCKS; 2.2 Soluția aplică politici bazate pe conținut confidential pentru cel puțin 300 de tipuri de fișiere; 2.3 Soluția oferă mecanisme interne de clasificare manuală pentru fișierelor Microsoft Office sau PDF, și utilizează un program de ADD-on pentru MS Office și la momentul salvării utilizatorii să direcționează pentru alegerea nivelului de clasificare intern; 2.4 Soluția asigură clasificarea conținutului chiar dacă acesta este arhivat și trebuie să extragă datele din cel puțin 10 nivele de arhivare; 2.5 Soluția suportă detectarea documentelor înregistrate/amprentate și clasificate. Sursele pe care le poate folosi sunt documentele înregistrate; 2.6 Soluția are capacitatea de a proteja datele bazându-se pe punctul lor de origine/creare;

2.7 Solutia trebuie sa ofere mecanisme interne de TAG-are sau etichetare a fisierelor folosind metada fields pentru o categorisire si catuare mai facila si mai rapida. 2.8 Solutia este capabila sa analizeze continut si sa aplice politici, indiferent de limba utilizata. 2.9 Solutia trebuie sa fie capabila sa scaneze si sa gaseasca continut sensibil. 2.10 Agentul trebuie sa aiba capabilitati de analiza de continut si blocare pentru mediile optice. 2.11 Solutia trebuie sa foloseasca mai putin de 5% din procesor in cazul utilizarii intense si gradul de utilizare medie este maxim 2% in timpul functionarii normale. 2.12 Solutia trebuie sa poata proteja informatia confidentiala care poate fi: · scrisa pe USB/optice · trimisa pe mail · uploadata pe web · copiata cu ajutorul clipboardului · printata in fisier sau pe imprimanta · scrisa pe un share in retea · folosita in aplicatiile network – based · aplicatii cloud (DropBox, Google Drive, Box, iCloud, Microsoft OneDrive) 2.13 Solutia trebuie sa poata fi integrate cu o solutie care sa ofere vizibilitate in timp real a amenintarilor pentru prevenirea pierderilor de date. 2.14 Solutia trebuie sa ofere protectie la nive de „Clip board” atat pentru <i>copy</i> sau <i>paste</i> cat si pentru screen capture. 2.15 Solutia trebuie sa permita crearea de politici de securitate pentru dispozitivele USB de tip plug-and-play 2.16 Solutia trebuie sa ofere acelasi nivel de protectie si in Windows SafeMode. 2.17 Solutia trebuie sa fie capabila sa faca analiza de continut local (offline), fara a folosi vreo alta componenta a solutiei. 2.18 Solutia permite auditarea functionalitatii agentului de endpoint. 2.19 Solutia trebuie sa permita dezinstalarea agentului in mod centralizat sau in urma unui mecanism de tipul challenge/response. 2.20 Solutia trebuie sa aiba un mecanism propriu de instalare a agentilor pe statiile de lucru sau alte sisteme. 2.21 Solutia pentru endpoint-uri are capabilitati de clasificare diverse ce nu depind de limbajul folosit: analiza pe termeni/cuvinte cheie, regex-uri si scor de risc, etc. 2.22 Agentul de endpoint trebuie sa fie compatibil, determinat prin testari, cu solutii de antivirus, firewall, criptare backup si antispyware third-party (de ex: Kaspersky, McAfee, Norton, OSCE, Zonelab, GuardianEdge, Credant, Safeguard, Ironkey, Acronis, Spybot, Adaware). 2.23 Agentul de endpoint trebuie sa permita aplicarea politicilor folosind continut inregistrat/ amprentat. 2.24 Solutia trebuie sa permita realizarea unui proces de justificare, in cazul in care utilizatorul transmite continut confidential. 2.25 Optiune de justificare a activitatii folosita de end-user in cadrul procesului de justificare, trebuie sa poata fi validabila sau administrabila.	2.7 Solutia ofera mecanisme interne de TAG-are sau etichetare a fisierelor folosind metadata fields pentru o categorisire si cautare mai facila si mai rapida. 2.8 Solutia este capabila sa analizeze continut si sa aplice politici, indiferent de limba utilizata. 2.9 Solutia este capabila sa scaneze si sa gaseasca continut sensibil. 2.10 Solutia asigura capabilitati de analiza de continut si blocare pentru mediile optice; 2.11 Solutia foloseste mai putin de 5% din procesor in cazul utilizarii intense si gradul de utilizare medie este maxim de 2% in timpul functionarii normale; 2.12 Solutia asigura protejarea informatiei confidentiale, care poate fi: · scrisa pe USB/optice; · trimisa pe mail; · uploadata pe web; · copiata cu ajutorul clipboardului; · printata in fisier sau pe imprimanta; · scrisa pe un share in retea; · folosita in aplicatiile network – based; · aplicatii cloud (DropBox, Google Drive, Box, iCloud, Microsoft OneDrive); 2.13 Solutia asigura posibilitatea de integrare cu o solutie care sa ofere vizibilitate in timp real a amenintarilor pentru prevenirea pierderilor de date; 2.14 Solutia ofera protectie la nive de „Clip board” atat pentru <i>copy</i> sau <i>paste</i> cat si pentru screen capture; 2.15 Solutia permite crearea de politici de securitate pentru dispozitivele USB de tip plug-and-play; 2.16 Solutia ofera acelasi nivel de protectie si in Windows SafeMode. 2.17 Solutia este capabila sa faca analiza de continut local (offline), fara a folosi vreo alta componenta a solutiei; 2.18 Solutia permite auditarea functionalitatii agentului de endpoint; 2.19 Solutia permite dezinstalarea agentului in mod centralizat sau in urma unui mecanism de tipul challenge/response; 2.20 Solutia are un mecanism propriu de instalare a agentilor pe statiile de lucru sau alte sisteme; 2.21 Solutia pentru endpoint-uri are diverse capabilitati de clasificare ce nu depind de limbajul folosit: analiza pe termeni/cuvinte cheie, regex-uri si scor de risc, etc; 2.22 Solutia asigura ca agentul de endpoint sa fie compatibil, cu solutii de antivirus, firewall, criptare backup si antispyware third-party (de ex: Kaspersky, McAfee, Norton, OSCE, Zonelab, GuardianEdge, Credant, Safeguard, Ironkey, Acronis, Spybot, Adaware); 2.23 Solutia asigura ca agentul de endpoint sa permita aplicarea politicilor folosind continut inregistrat/ amprentat; 2.24 Solutia permite realizarea unui proces de justificare, in cazul in care utilizatorul transmite continut confidential; 2.25 Solutia asigura optiunea de justificare a activitatii folosita de end-user in cadrul procesului de justificare si este validabila sau administrabila;
---	---

2.26 Solutia trebuie sa fie capabila sa blocheze dispozitivele mobile sau sa permita doar accesul de tip read-only. 2.27 Solutia trebuie sa poata realiza reguli de protectie care sa aiba ca si criteriu cuvinte-cheie. 2.28 Solutia trebuie sa poata realiza reguli de protectie care sa aiba ca si criteriu expresii regulate. 2.29 Solutia trebuie sa poata realiza reguli de protectie care sa aiba ca si criteriu amprenta (hash-uri). 2.30 Constructia regulilor trebuie sa includa suport pentru logica booleana incluzind AND, OR, sau alte declaratii logice. 2.31 Solutia trebuie sa fie capabila sa aplice urmatoarele actiuni: blocare, monitorizare, notificare utilizator, mentinere evidenta, criptare sau aplicarea de etichete. 2.32 Solutia trebuie sa aiba capabilitatea de a se integra cu soft de criptare 3rd party sau al aceluiasi producator, pentru a realiza aplicarea politicilor de criptare in functie de continut. 2.33 Regulile de protectie de email la nivel de endpoint, trebuie sa permita bypass-ul, folosind un sir de caractere configurabil in subiectul mesajului, mutand detectia la nivelul gateway-ului de email. 2.34 Solutia trebuie sa aiba abilitatea de a identifica fisierele bazandu-se pe conceptul de true file type si nu doar pe extensia fisierele. 2.35 Solutia trebuie sa aiba abilitatea de a face discovery local. De asemenea ea trebuie sa poata contine si o optiune de remediere. 2.36 Solutia trebuie sa fie capabila sa aplice regulie de protectie atat la nivel de grupuri /useri definiti in Active Directory cat si pentru userii locali ai sistemelor. 2.37 Solutia trebuie sa fie capabila sa aplice regulie de control al perifericelor chiar si atunci cand nu este conectat la reseaua companiei, cu posibilitatea de a avea politici diferite in functie de conectivitatea la reseaua companiei 2.38 Solutia are abilitatea de a face discovery in interiorul bazelor de e-mail stocate pe endpoint. 2.39 Solutia trebuie sa permita customizarea notificarilor emise in timpul funtionarii si a ferestrei in care sunt scrise aceste notificari. 2.40 Solutia trebuie sa fie capabila sa identifice nivelul de clasificare a documentelor din marcajele vizuale si sa aplice regulile de protectie pe aceste documente. 2.41 Solutia trebuie sa fie capabila sa protejeze documente nemarcate ce au continut ce provine din documente clasificate cu marcaje vizuale. 2.42 Solutia trebuie sa se integreze nativ cu un produs de clasificarea datelor 2.43 Solutia trebuie sa poata aplica etichete fisierele in functie de originea lor, informatia fiind stocata securizat in Alternate Data Stream pentru a nu putea fi alterata de utilizator 2.44 Solutia trebuie sa fie capabila sa citeasca informatiile de tip META stocate in fisierele Office 2.45 Solutia trebuie sa ofere utilizatorilor posibilitatea de clasificare manuala a documentului la momentul salvarii documentelor MS Office; 2.46 Solutia trebuie sa ofere utilizatorilor capabilitati de clasificare manuala a email-ului la momentul trimterii unui email folosind clientul Outlook office.	2.26 Solutia este capabilă să blocheze dispozitivele mobile sau sa permita doar accesul de tip read-only; 2.27 Solutia realizeaza reguli de protectie care sa aiba ca si criteriu cuvinte-cheie; 2.28 Solutia poate realiza reguli de protectie care sa aiba ca si criteriu expresii regulate; 2.29 Solutia poate realiza reguli de protectie care sa aiba ca si criteriu amprenta (hash-uri); 2.30 Solutia oferă o constructie de reguli care include suport pentru logica booleana incluzind AND, OR, sau alte declaratii. 2.31 Solutia este capabila sa aplice urmatoarele actiuni: blocare, monitorizare, notificare utilizator, mentinere evidenta, criptare sau aplicarea de etichete; 2.32 Solutia este capabilă de a se integra cu soft de criptare 3rd party sau al aceluiasi producator, pentru a realiza aplicarea politicilor de criptare in functie de continut; 2.33 Solutia oferă ca regulile de protectie de email la nivel de endpoint să permită bypass-ul, folosind un sir de caractere configurabil in subiectul mesajului, mutand detectia la nivelul gateway-ului de email; 2.34 Solutia are abilitatea de a identifica fisierele bazandu-se pe conceptul de true file type si nu doar pe extensia fisierele; 2.35 Solutia are abilitatea de a face discovery local si contine si optiune de remediere; 2.36 Solutia este capabilă să aplice regulile de protectie atat la nivel de grupuri /useri definiti in Active Directory cat si pentru userii locali ai sistemelor; 2.37 Solutia este capabilă să aplice regulile de control al perifericelor chiar si atunci cand nu este conectat la reseaua companiei, cu posibilitatea de a avea politici diferite in functie de conectivitatea la reseaua companiei; 2.38 Solutia are abilitatea de a face discovery in interiorul bazelor de e-mail stocate pe endpoint; 2.39 Solutia permite customizarea notificarilor emise in timpul funtionarii si a ferestrei in care sunt scrise aceste notificari; 2.40 Solutia este capabilă să identifice nivelul de clasificare a documentelor din marcajele vizuale si sa aplice regulile de protectie pe aceste documente; 2.41 Solutia este capabilă sa protejeze documente nemarcate ce au continut ce provine din documente clasificate cu marcaje vizuale; 2.42 Solutia oferă integrarea nativa cu un produs de clasificarea datelor; 2.43 Solutia poate aplica etichete fisierele in functie de originea lor, informatia fiind stocata securizat in Alternate Data Stream pentru a nu putea fi alterata de utilizator; 2.44 Solutia este capabilă să citeasca informatiile de tip META stocate in fisierele Office; 2.45 Solutia oferă utilizatorilor posibilitatea de clasificare manuala a documentului la momentul salvării documentelor MS Office; 2.46 Solutia oferă utilizatorilor capabilități de clasificare manuala a email-ului la momentul trimterii unui email folosind clientul Outlook office;
---	--

2.47 Soluția trebuie să ofere politici de securitate out-of-box care pot fi customizate de către utilizator.. 2.48 Soluția trebuie să ofere posibilitatea casificării în timp real pentru a minimiza false positive. 2.49 Soluția trebuie să permită protejarea stațiilor de lucru mobile care sunt/nu sunt conectate la rețea. 3. Consola de administrare 3.1 Consola de administrare trebuie să se poată instala pe unul din următoarele sisteme de operare pe 64 de biți: • Microsoft Windows Sever 2016 • Microsoft Windows Sever 2012 Release 2 (R2) • Microsoft Windows Server 2012 • Windows Server 2008 SP2 Standard, Enterprise, Datacenter • Windows Server 2008 R2 Standard, Enterprise, Datacenter 3.2 Consola permite pe lângă distribuirea componentelor native și împachetarea aplicațiilor de la terți și instalarea acestora pe stațiile de lucru. 3.3 Consola permite atribuirea automată a politicilor pe stații și servere în funcție de specificațiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare) 3.4 Sincronizarea dintre server și client trebuie să se facă dinspre client către server. 3.5 Consola de administrare trebuie să se poată integra cu Active Directory. 3.6 Consola de administrare trebuie să poată fi instalată într-un mediu virtual. 3.7 Consola trebuie să poată fi instalată în mediu Microsoft Cluster. 3.8 Consola de administrare trebuie să folosească Microsoft SQL. 3.9 Consola de administrare permite instalarea unei componente de comunicare în DMZ pentru a putea permite sincronizarea sistemelor prin internet. 3.10 Comunicarea dintre componentele soluției și serverul de administrare trebuie să se facă prin intermediul unui singur agent. 3.11 Soluția trebuie să permită filtrarea evenimentelor ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date să nu se încarce cu informații considerate inutile. 3.12 Soluția trebuie să permită configurare unui mesaj de login. 3.13 Soluția poate folosi un proxy pentru contactarea serverului de actualizare al producătorului. 3.14 Accesul în consola de administrare poate fi făcut pe baza credențialelor din Active Directory. 3.15 Accesul în consola de management poate fi făcut pe baza certificatelor x509. 3.16 Consola de administrare trebuie să permită crearea de roluri în mod granular pentru cei ce o administrează. 3.17 Acțiunile utilizatorilor în consola trebuie să auditeze. 3.18 Consola trebuie să permită construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronică (E-mail).	2.47 Soluția oferă politici de securitate out-of-box care pot fi customizate de către utilizator; 2.48 Soluția oferă posibilitatea casificării în timp real pentru a minimiza false positive; 2.49 Soluția permite protejarea stațiilor de lucru mobile care sunt/nu sunt conectate la rețea. 3. Consola de administrare 3.1 Soluția permite ca consola de administrare să se instaleze pe unul din următoarele sisteme de operare pe 64 de biți: • Microsoft Windows Sever 2016; • Microsoft Windows Sever 2012 Release 2 (R2); • Microsoft Windows Server 2012; • Windows Server 2008 SP2 Standard, Enterprise, Datacenter; • Windows Server 2008 R2 Standard, Enterprise, Datacenter; 3.2 Soluția asigură o consola care permite pe lângă distribuirea componentelor native și împachetarea aplicațiilor de la terți și instalarea acestora pe stațiile de lucru; 3.3 Soluția asigură o consola care permite atribuirea automată a politicilor pe stații și servere în funcție de specificațiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare); 3.4 Soluția permite sincronizarea dintre server și client și se face dinspre client către server; 3.5 Soluția asigură integrarea cu Active Directory a consolei de administrare. 3.6 Soluția permite instalarea consolei de administrare într-un mediu virtual; 3.7 Soluția permite ca consola să fie instalată în mediu Microsoft Cluster; 3.8 Soluția permite ca consola de administrare să folosească Microsoft SQL; 3.9 Soluția asigură ca consola de administrare să permită instalarea unei componente de comunicare în DMZ pentru a putea permite sincronizarea sistemelor prin internet; 3.10 Soluția asigură o comunicare dintre componentele soluției și serverul prin intermediul unui singur agent; 3.11 Soluția permite filtrarea evenimentelor ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date să nu se încarce cu informații considerate inutile; 3.12 Soluția permite configurare unui mesaj de login; 3.13 Soluția asigură posibilitatea folosirii unui proxy pentru contactarea serverului de actualizare al producătorului; 3.14 Soluția permite ca accesul în consola de administrare să fie efectuat pe baza credențialelor din Active Directory; 3.15 Soluția permite ca accesul în consola de administrare să fie efectuat pe baza certificatelor x509; 3.16 Soluția asigură ca consola de administrare să permită crearea de roluri în mod granular pentru cei ce o administrează; 3.17 Soluția permite auditul utilizatorilor în consola; 3.18 Soluția asigură ca consola să permită construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronică (E-mail);
---	--

3.19 Canalul de comunicare dintre serverul de administrare si componentele distribuite pe calculatoare trebuie sa fie criptat. 3.20 Componenta ce asigura canalul de comunicare dintre server si statii de lucru trebuie sa fie valitata din punct de vedere al securitatii. (Ex: FIPS, Common Criteria, Etc.) 3.21 Canalul de comunicare dintre consola si cei ce o acceseaza trebuie sa fie criptat. 3.22 Consola de administrare trebuie sa poata fi accesata de pe orice computer din retea in mod Web securizat utilizand un browser standard (Internet Explorer, Chrome, Firefox), fara necesitatea instalarii de software additional. 3.23 Pentru interfata Web a consolei trebuie sa fie posibil importul unui certificat SSL generat de o autoritate locala, inlocuind astfel pe cel auto-generat. 3.24 Intervalul de sincronizare intre server si componente poate fi modificat. 3.25 Intervalul de transmitere a evenimentelor de pe client catre server poate fi modificat. 3.26 Consola trebuie sa poata detecta prezenta pe retea a sistemelor noi aparute prin intermediul unor senzori. 3.27 Consola trebuie sa foloseasca un propriu index pentru a identifica si actualiza datele despre sistemele care isi schimba proprietati precum nume,ip si configuratie hardware; 3.28 Consola permite automatizarea de sarcini de instalare/dezinstalare a componentelor pe statiile de lucru, de rulare a rapoartelor si de transmiterea de notificari prin mesagerie electronica. 3.29 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. 3.30 Consola trebuie sa se integreze cu sisteme de ticketing externe precum BMC Remedy si HP OpenView. 3.31 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) 3.32 Consola trebuie sa permite aplicarea de politici diferite pentru sisteme pe: • Sisteme individuale • Grupuri de sisteme • Sisteme din AD ce sunt acelasi OU 3.33 Consola trebuie sa stie sa lanseze automat aplicatii externe si sa injecteze parametrii din evenimente. 3.34 Consola permite accesarea logului componentei de sincronizare de pe sisteme in timp real prin intermediul unui serviciu web. 3.35 Consola trebuie sa permita vizualizarea incidentelor de securitate si crearea de cazuri 3.36 Evidentele din incidentele de securitate trebuie stocate criptat pe serverul unde ruleaza consola de management	3.19 Solutia asigură criptarea canalului de comunicare dintre serverul de administrare si componentele distribuite pe calculatoare; 3.20 Soluția oferă componenta validată din punct de vedere al securitatii ce asigura canalul de comunicare dintre server si statii de lucru; 3.21 Solutia asigură criptarea canalului de comunicare dintre consola si cei ce o acceseaza; 3.22 Solutia asigură posibilitatea accesarii consolei de administrare de pe orice computer din retea in mod Web securizat utilizand un browser standard (Internet Explorer, Chrome, Firefox), fara necesitatea instalarii de software additional; 3.23 Solutia oferă importarea unui certificat SSL generat de o autoritate locala pentru interfata Web a consolei; 3.24 Solutia oferă posibilitatea modificarii intervalului de sincronizare intre server si componente; 3.25 Solutia oferă posibilitatea modificarii intervalului de transmitere a evenimentelor de pe client catre server; 3.26 Solutia asigură ca consola să poată detecta prezenta pe retea a sistemelor noi aparute prin intermediul unor senzori; 3.27 Solutia asigură ca consola sa folosească un propriu index pentru a identifica si actualiza datele despre sistemele care isi schimba proprietati precum nume, ip si configuratie hardware; 3.28 Solutia asigură ca consola să permită automatizarea de sarcini de instalare/dezinstalare a componentelor pe statiile de lucru, de rulare a rapoartelor si de transmiterea de notificari prin mesagerie electronica; 3.29 Solutia asigură ca consola să prezinte urmatoarele informatii despre sistemele administrate: numele sistemului, utilizatorul logat, produsele instalate, tipul de system de operare si adresa IP. 3.30 Solutia asigură ca consola să se integreze cu sisteme de ticketing externe precum BMC Remedy si HP OpenView; 3.31 Solutia asigură ca serverul de administrare să fie capabil să declanșeze 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); 3.32 Solutia asigură ca consola să permită aplicarea de politici diferite pentru sisteme pe: • Sisteme individuale; • Grupuri de sisteme; • Sisteme din AD ce sunt acelasi OU; 3.33 Solutia asigură ca consola să efectueze lansarea automată de aplicatii externe si injectarea parametrilor din evenimente; 3.34 Solutia asigură ca consola să permită accesarea logului componentei de sincronizare de pe sisteme in timp real prin intermediul unui serviciu web; 3.35 Solutia asigură ca consola să permită vizualizarea incidentelor de securitate si crearea de cazuri; 3.36 Solutia permite stocarea criptata a evidentelor din incidentele de securitate pe server unde ruleaza consola de management;
--	---

3.37 Consola trebuie sa permita integrarea si altor aplicatii/echipamente de securitate ex. (Antivirus, SandBox, Proxy, Firewall) intr-o consola unica pentru a unifica administrarea acestora. 4. Raportarea 4.1 Consola de administrare poate asigura generarea de rapoarte despre nodurile administrate si despre evenimentele generate de ele. 4.2 Consola trebuie sa permita crearea de noi rapoarte in mod granular cu informatii extrase din evenimente, sau despre sistemele administrate. 4.3 Rapoartele pot fi generate sub forma de tabel, pie chart, buble chart, lista, sumar, sau grafic istoric. 4.4 Rapoartele pot fi exportate in format pdf, csv, html. 4.5 Rapoartele pot fi personalizate cu logo-ul companiei. 4.6 Rapoartele pot fi salvate ca fisiere sau trimise prin e-mail. 4.7 Raportele pot fi exportate intr-un format arhivat pentru conservare de latime de banda si expediate automat pe e-mail unor destinatii presetate. 4.8 Consola permite evaluarea evenimentelor primite de la statiile de lucru si filtrarea lor pentru o mai buna identificare a informatiilor relevante. 4.9 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	3.37 Solutia asigură ca consola să permită integrarea si altor aplicatii/echipamente de securitate ex. (Antivirus, SandBox, Proxy, Firewall) intr-o consola unica pentru a unifica administrarea acestora; 4. Raportarea 4.1 Solutia permite ca consola de administrare să asigure generarea de rapoarte despre nodurile administrate si despre evenimentele generate de ele; 4.2 Solutia asigură ca consola să permită crearea de noi rapoarte in mod granular cu informatii extrase din evenimente, sau despre sistemele administrate; 4.3 Solutia permite generarea rapoartelor sub forma de tabel, pie chart, buble chart, lista, sumar, sau grafic istoric; 4.4 Solutia permite exportarea rapoartelor in format pdf, csv, html; 4.5 Solutia permite personalizarea rapoartelor cu logo-ul companiei; 4.6 Solutia permite salvarea rapoartelor ca fisiere, sau trimise prin e-mail; 4.7 Solutia permite exportarea intr-un format arhivat pentru conservare de latime de banda si expediate automat pe e-mail unor destinatii presetate; 4.8 Solutia asigură ca consola să permită evaluarea evenimentelor primite de la statiile de lucru si filtrarea lor pentru o mai buna identificare a informatiilor relevante; 4.9 Solutia permite 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.
Vendori posibili: McAfee host DLP, TrendMicro DLP, Symantec DLP • Prezența interfeței de administrare, analizarea informațiilor comune cu alte sisteme EndPoint Protection, SIEM, DLP reprezintă necesitatea de importanță înaltă. • Disponibilitatea și poziția produsului în "Gartner Square" reprezintă un avantaj puternic față de alte soluții	• Produsul oferat: McAfee • Produsul oferat oferă posibilitatea de integrare cu alte solutii de EndPoint Protection, SIEM si alte solutii oferite de producatorul McAfee, astfel asigurand o administrare centralizata dintr-o singura consola. • Produsul oferat se regăsește in cadranul de Lideri "Gartner" • In oferta sunt incluse serviciile de instalare, integrare si configurarea soluției.