Cerinţele funcţionale faţa de DLP solution

DLP - Protecția pierderilor de date

1. Integrare cu infrastructura IT

1.1 Solutia trebuie sa poata rula cel putin pe:

- Windows 8 si 8.1, 10 , Enterprise si Professional, 32-bit and 64-bit
- Windows 7 SP1 sau mai recente Enterprise si 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 Solutia suporta urmatoarele solutii de tip directory: Microsoft AD si Open LDAP

1.3 Solutia trebuie sa ofere functionalitati de instalare la distanta pentru agentii de monitorizare astfel incat la momentul instalarii sau upgrade sa nu fie necesara restartarea sistemelor.

1.4 Solutia trebuie sa ofere suport pentru mediile virtuale incluzand VDI, aceasta insemnand ca fiecare politica trebuie sa activeze si alerteze pe baza de utilizator. Politicile per user trebuie sa sa se aplice pe sesiuni multiple si sa ofere un control si o flexibilitate pe shared terminals sau pe VDI.

1.5 Solutia trebuie sa ofere mecanisme de integrare COTS cu solutii consacrate de IRM Righ Management cum ar fi Microsoft Right Management Services sau Seclore FileSecure.

2. Politici de Securitate

2.1 Descrieti in detaliu aplicatiile, protocoalele si canalele de I/O pe care solutia le poate folosi.

2.2 Solutia aplica politici bazate pe continut confidential pentru cel putin 300 de tipuri de fisiere.

2.3 Solutia trebuie sa ofere mecanisme interne de clasificare manuala pentru fiserelor Microsoft Office sau PDF, solutia propusa va folosi un program de ADD-on pentru MS Office si la momentul salvarii utilizatorii vor fi directionati pentru alegerea nivelului de clasificare intern.

2.4 Solutia trebuie sa faca clasificarea continutului chiar daca acesta este arhivat si trebuie sa extraga datele din cel putin 10 nivele de arhivare.

2.5 Solutia trebuie sa suporte detectarea documentelor inregistrate/amprentate si clasificate. Descrieti sursele pe care le poate folosi.

2.6 Solutia trebuie sa aiba capabilitatea de a proteja datele bazandu-se pe punctul lor de origine/creare.

2.7 Solutia trebuie sa ofere mecanisme interne de TAG-are sau etichetare a fiserelor 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 la amenintarilor pentru prevenirea pierderilor de date.

Digitally signed by Şarco Vasile
Date: 2018.11.29 09:24:16 EET
Reason: MoldSign Signature
Location: Moldova

2.14 Solutia trebuie sa ofere protectie la nive de „Clip board” atat pentru *copy* sau *paste* cat si pentru screen capture.
2.15 Solutia trebuie sa permita crearea de politici de securiteate pentru dispositivele 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 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.
2.26 Solutia trebuie sa fie capabila sa blocheze dispozitivele mobile sau sa permita doar accessul 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 fisierelor.
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 reteaua companiei, cu posibilitatea de a avea politici diferite in functie de conectivitatea la reteaua 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 fisierelor 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.
2.47 Solutia trebuie sa ofere politici de securitate out-of-box care pot fi constumizate de catre utilizator..
2.48 Solutia trebuie sa ofere posibilitatea casificarii in timp real pentru a minimiza false positive.
2.49 Solutia trebuie sa permita protejarea statiilor de lucru mobile care sunt/nu sunt conectate la retea.

3. Consola de administrare

3.1 Consola de administrare trebuie sa se poata instala pe unul din urmatoarele sisteme de operare pe 64 de biti:

- 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 langa distribuirea componentelor native si impachetarea aplicatiilor de la terti si instalarea acestora pe statiile de lucru.
3.3 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)
3.4 Sincronizarea dintre server si client trebuie sa se faca dinspre client catre server.
3.5 Consola de administrare trebuie sa se poata integra cu Active Directory.
3.6 Consola de administrare trebuie sa poata fi instalata intr-un mediu virtual.
3.7 Consola trebuie sa poate fi instalata in mediu Microsoft Cluster.
3.8 Consola de administrare trebuie sa foloseasca Microsoft SQL.
3.9 Consola de administrare permite instalarea unei componente de comunicare in DMZ pentru a putea permite sincronizarea sistemelor prin internet.
3.10 Comunicarea dintre componentele solutiei si serverul de administrare trebuie sa se faca prin intermediul unui singur agent.
3.11 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.
3.12 Solutia trebuie sa permita configurare unui mesaj de login.
3.13 Solutia poate folosi un proxy pentru contactarea serverului de actualizare al producatorului.
3.14 Accestul in consola de administrare poate fi facut pe baza credentialelor din Active Directory.
3.15 Accesul in consola de management poate fi facut pe baza certificatelor x509.
3.16 Consola de administrare trebuie sa permita creare de roluri in mod granular pentru cei ce o administreaza.
3.17 Actiunile utilizatorilor in consola trebuiesc audidate.
3.18 Consola trebuie sa permita construirea unei liste de contacte in vederea folosirii acestora pentru notificari prin mesagerie electronica (E-mail).
3.19 Canalul de comunicatie dintre serverul de administrare si componentele distribuite pe calculatoare trebuie sa fie criptat.
3.20 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.)
3.21 Canalul de comunicatie 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 aditional.
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
3.37 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 sitemele administrate (Detalii de configurare, hardware, utilizator)
- Evenimente de la siteme
- Informatii despre politicile si sarcinilie aplicate sistemelor
- Informatii furnizate de senzori

Vendori posibili: McAfee host DLP, TrendMicro DLP, Symantec DLP

-
- **Prezenţa interfeței de administrare, analizarea informațiilor comune cu alte sisteme EndPoint Protection, SIEM, DLP reprezintă necesitatea de importanţa înaltă.**

- **Disponibilitatea și poziția produsului în "Gartner Square" reprezintă un avantaj puternic față de alte soluții.**