Anexa nr. 22
la Documentația standard nr.115
din "15" septembrie 2021

Specificaţii tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Procedura de achiziție: nr. ocds-b3wdp1-MD-170835439440014 din 19.02.2024
Obiectul achiziției: Servicii de prevenire a pierderilor de date (DLP)

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard de referinţă
1	2	3	4	5	6	7
Servicii de prevenire a pierderilor de date				Conform cerințelor solicitate în caietul de sarcini (Anexa nr. 1) pentru soluția de software DLP (Soluția de prevenire a pierderilor de date Data Loss Prevention DLP)	**Solutia ofertată DLP (Data Loss Prevention) Trellix Data Security Endpoint Protection Suite Subscription License sau Perpetual License** **I. Integrare cu infrastructura IT**	-

					1. Soluția ruleaza: 1.1 Windows 10 1803 sau mai noi Enterprise si Professional, 32-bit si 64-bit si Windows 11 64 bit 1.2 Windows Server 2012, 2012 R2, 2016, 2019, 2022 1.3 Windows 8 si 8.1 sau mai recente, Enterprise si Professional, 32-bit si 64-bit 1.4 Windows 7 SP1 sau mai recente Enterprise si Business, 32-bit and 64-bit 1.5 macOS Mojave, Catalina, Big Sur, Monterey. 1.6 Linux Ubuntu, CentOS 2. Soluția suportă următorul tip directory: Microsoft AD si Open LDAP 3. Soluția ofer[funcționalități de instalare și deservire de la distanță pentru agenții de monitorizare. 4. Soluția oferă suport pentru mediile virtuale: • VMware ESXi, • ProxMox. 5. Politicile se aplică la nivel de user sau stație pe sesiuni multiple. 6. Solutia este capabilă sa tina evidenta unui numar de peste 500 de milioane de semnaturi ale fisierelor clasificate pe un singur server si posibilitatea de a instala un numar nelimitat de repositoare 7. Solutia alică politici bazate pe continut confidential pentru un numar nelimitat de tipuri de fisiere 8. Solutia face clasificarea continutului chiar daca acesta este arhivat si trebuie de	

					asemenea sa suporte “nesting” (ex: arhiva zip in interiorul unei alte arhive zip) **II. Politici de Securitate** 1. Soluția are capacitatea de a inspecta următoarele protocoale: • SMTP, • Telnet, • IMAP, • FTP, • POP3, • IRC, • HTTP, • HTTPS, • SMB, • WSD, • TCP/IP, • LDAP, de asemenea poate analiza traficul care este încapsulat în SOCKS; 2. Soluția suportă detectarea documentelor înregistrate/amprentate și clasificate. 3. Soluția are capabilitatea de a proteja datele bazându-se pe punctul lor de origine/creare. - Solutia este capabilă de a atribui in mod automat taguri fisierelor clasificate. Aceste taguri trebuie sa fie utilizabile de aplicatii third-party si alte aplicatii DLP 4. Solutia este capabila sa analizeze continut si sa aplice politici, indiferent de limba utilizata. (Română, Rusă, Engleză, Franceză, etc) 5. Soluția este capabila să scaneze și să găsească conținut sensibil.	

					- Agentul are capabilitati de analiza de continut si blocare pentru mediile optice. - Solutia foloseşte mai putin de 5% din procesor in cazul utilizarii intense si gradul de utilizare medie este maxim 2% in timpul functionarii normale. 6. Soluția poate proteja informația confidențiala care poate fi: • scrisă pe unități USB, CD/DVD, • trimisă pe mail, • upload-ată, • copiată cu ajutorul clipboard-ului, • printată în fișier sau pe imprimantă, • scrisă pe resursele partajate în rețea, • aplicații cloud (DropBox, Google Drive, Box, iCloud, Microsoft OneDrive). • folosita in aplicatiile network – based • Copiata prin comanda de printscreen 7. Soluția oferă vizibilitate în timp real a amenințărilor pentru prevenirea pierderilor de date. 8. Soluția oferă protecție la nivel de „Clip board" atât pentru copy sau paste cât și pentru screen capture. 9. Soluția trebuie să permită crearea de politici de securitate pentru dispozitivele USB de tip plug-and-play. 10. Soluția oferă același nivel de protecție și în regim OS Safe-Mode. 11. Soluția este capabilă să facă analiză de conținut local (offline), fără a utiliza vreo altă componentă a soluției.	

					12. Soluția permite auditarea funcționalității agentului de endpoint. - Solutia trebuie permite dezinstalrea agentului in mod centralizat sau in urma unui challenge/response. 13. Soluția are un mecanism propriu de instalare a agenților pe stațiile de lucru sau alte sisteme. - 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. 14. Agentul de endpoint este compatibil, cu soluții de antivirus, firewall și antispyware third-party (de ex: Bitdefender, Kaspersky, McAfee, Norton, OSCE, Zonelab, GuardianEdge, Credant, Safeguard, Ironkey, Acronis, Spybot, Adaware, etc.). - Agentul de endpoint permite aplicarea politicilor folosind continut inregistrat/ amprentat. 15. Soluția permite realizarea unui proces de justificare, în cazul în care utilizatorul transmite conținut confidențial. 16. Opțiunea de justificare a activității folosită de end-user în cadrul procesului de justificare, poate fi validabilă sau administrabilă. - Solutia permite utilizatorilor sa devina “stakeholderi” pe un caz/eveniment, ori din initiativa acestora ori asignata de administrator 17. Solutia este capabila sa blocheze dispozitivele mobile sau sa permita accessul al ele doar de tip read-only sau sa permita	

					doar incarcarea dispozitivelor mobile nu si accesarea acestora. - Solutia poate realiza reguli de protectie care sa aiba ca si criteriu cuvinte-cheie. - Solutia poate realiza reguli de protectie care sa aiba ca si criteriu regex-uri. 18. Soluția poate aplica reguli de protecție care să aibă ca criteriu cuvinte-cheie, expresii regulate și amprentă (hash-uri). - Solutia poate realiza reguli de protectie care sa aiba ca si criteriu reguli de proximitate intre alte doua reguli (de tip keyword, dictionar sau regex). 19. Construcția regulilor include suport pentru logica booleana incluzând AND, OR, sau alte declarații logice. 20. Solutia este capabila sa aplice urmatoarele actiuni: blocare, monitorizare, notificare utilizator, mentinere evidenta, criptare sau aplicarea de etichete. - Solutia permite setarea unui threshold astfel incat o regula sa nu fie activata decat dupa gasirea unui anumit numar de matchuri. 21. Soluția are abilitatea de a identifica fișierele bazându-se pe conceptul de true file type și nu doar pe extensia fișierelor. 22. Soluția are posibilitatea rulării autonome a agentului pe endpoint în baza politicilor inițial aplicate. - Solutia are capabilitatea de a se integra cu soft de criptare 3rd party, pentru a realiza aplicarea politicilor de criptare in functie de continut.	

					- Solutia dispune de cel putin 70 de reguli de validare pentru definitiile bazate pe expresii regulate, inclusiv pentru definitia de IDNP. - Solutia permite “whitelist-area” de continut, dispozitive, procese si utilizatori/grupuri de utilizatori din regulile de protectie - Solutia permite salvarea continutului ce a declansat o regula de protectia ca “evidence”. Aceste date salvate sunt recunoscute in instanta ca fiind dovezi valide. - Solutia are abilitatea de a identifica fisierele bazandu-se pe conceptul de true file type si nu doar pe extensia fisierelor. - Solutia dispune de integrare nativa cu serviciu de tip CASB pentru aplicarea acelorasi reguli de protectie DLP si pe resurse manipulate in cloud - Solutia are abilitatea de a face discovery local. De asemenea ea trebuie sa poata contine si o optiune de remediere. 23. Soluția este capabilă să aplice reguli de protecție atât la nivel de grupuri /user-i definiți în Active Directory cât și pentru user-ii locali ai sistemelor. 24. Soluția este capabilă să aplice reguli de control al perifericelor chiar și atunci când nu este conectat la rețeaua companiei, cu posibilitatea de a avea politici diferite în funcție de conectivitatea la rețeaua companiei.	

					25. Soluția are abilitatea de a face discovery în interiorul bazelor de e-mail stocate pe endpoint. 26. Soluția permite customizarea notificărilor emise în timpul funcționării și a ferestrei în care sunt scrise aceste notificări. 27. Soluția este capabilă să identifice nivelul de clasificare a documentelor din marcajele vizuale și să aplice regulile de protecție pe aceste documente. 28. Soluția este capabilă să protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale. 29. Soluția are opțiunea de clasificare a datelor sau integrarea cu alte produse de clasificare a datelor. 30. Soluția poate aplica etichete fișierelor în funcție de originea lor, informația fiind stocată securizat pentru a nu putea fi alterată de utilizator. 31. Soluția este capabilă să citească informațiile de tip META stocate în fișierele Office. 32. Soluția oferă utilizatorilor capabilități de clasificare manuala a email-ului la momentul trimiterii unui e-mail folosind clientul Outlook office. 33. Soluția oferă politici de securitate out-of-box care pot fi constumizate de către utilizator. 34. Soluția oferă posibilitatea clasificării în timp real pentru a minimiza false pozitive.	

					35. Soluția permite protejarea stațiilor de lucru mobile care sunt/nu sunt conectate la rețea. 36. Solutia este capabilă să comunice cu alte componente de retea prin protocol Open DXL pentru blocarea incercarilor de exfiltrare de date din cadrul infrastructurii. 37. Solutia permite clasificarea manuala a fisierelor, intr-un mod granular asignat pe grupuri, OU-uri sau useri de AD 38. Solutia permite managementul incidentelor si cazurilor in mod granular si sa permita asignarea de useri ePO pe acestea 39. Solutia permite obfuscarea campurilor sensibile ale incidentelor raportate, in functie de utilizator si setul de permisiuni al acestuia 40. Solutia pune la dispozitie un utilitar de tip “wizard” pentru ghidarea administratorului in crearea politicilor initiale DLP 41. Solutia suportă solutii terte de clasificare a datelor, precum Boldon James, Titus si Azure Information Protection 42. Solutia permite exportul si importul politicilor, clasificarilor si regulilor create 43. Solutia dispune de o unealta de testare a clasificarilor in consola, pentru a permite testarea match-urilor fara a fi necesara schimbarea politicilor DLP si actualizarea acestora pe clienti 44. Solutia dispune de ghidaj pentru troubleshooting in cadrul interfetei de administrare a acesteia	

					45. Solutia poate scana in fundal email-urile trimise din Outlook, pentru a nu impacta exeperienta utilizatorilor in mod negativ 46. Solutia poate adăuga atribute costumizabile in cadrul incidentelor DLP, precum managerul utilizatorului, regiunea utilizatorului, ID, etc 47. Solutia suportă utilizare de Rest API pentru extragerea evenimentelor de DLP si a detaliilor atribuite acestora. **III. Consola de administrare** 1. Consola poate fi instalată pe unul din următoarele sisteme de operare pe 64 de biți: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 Release 2 (R2) • Microsoft Windows Server 2012 • Windows Server 2008 SP2 Standard, Enterprise, Datacenter • Windows Server 2008 R2 Standard, Enterprise, Datacenter 2. Soluția permite instalarea/dezinstalarea agentului în mod centralizat. 3. Consola permite pe lângă distribuirea componentelor native și împachetarea aplicațiilor de la terți și instalarea acestora pe stațiile de lucru. 4. 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).	

					- Sincronizarea dintre server si client se face atat dinspre client catre server, cat si invers. 5. Consola de administrare poate fi integrată cu Active Directory. 6. Consola de administrare poate fi instalată într-un mediu virtual. 7. Consola de administrare utilizează bază de date freeware sau licența soluției să cuprindă și licența bazei de date utilizate. 8. Consola de administrare permite instalarea unei componente de comunicare în DMZ pentru a putea permite sincronizarea sistemelor prin internet. - Comunicarea cu serverul de administrare se poate face prin intermediul unui singur agent. - 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 permite configurare unui mesaj de login. - Solutia poate folosi un proxy pentru contactarea serverului de actualizare al producatorului. 9. Acces-ul în consola de administrare poate fi făcut pe baza credențialelor din Active Directory. Accesul in consola de management treebuie se poate face pe baza certificatelor x509. 10. Consola de administrare permite crearea de roluri în mod granular pentru cei ce o administrează.	

					11. Toate acțiunile utilizatorilor în consola de administrare sunt auditate. 12. Consola permite construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronica (E-mail). 13. Canalul de comunicație dintre serverul de administrare si componentele distribuite pe calculatoare este criptat. 14. Componența ce asigură canalul de comunicație dintre server și stații de lucru este validată din punct de vedere al securității. (Ex: FIPS, Common Criteria, Etc.) 15. Canalul de comunicație dintre consola și cei ce o accesează trebuie este criptat. 16. Consola de administrare este accesată de pe orice computer din rețea în mod Web securizat utilizând un browser standard (Internet Explorer, Chrome, Firefox), fără necesitatea instalării de software adițional. - Consola de administrare poate 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 este 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. 17. Intervalul de transmitere a evenimentelor de pe client către server poate fi modificat.	

					18. Consola detectează prezenta pe rețea a sistemelor noi apărute prin intermediul unor senzori. 19. Consola folosește un propriu index pentru a identifica și actualiza datele despre sistemele care își schimbă proprietăți precum nume, IP și configurații hardware; 20. Consola permite automatizarea de sarcini de instalare/dezinstalare a componentelor pe stațiile de lucru, de rulare a rapoartelor și de transmiterea de notificări prin mesagerie electronica. 21. Consola prezintă cel puțin următoarele informații despre sistemele administrate: numele sistemului, utilizatorul logat, produsele instalate, tipul de system de operare și adresa IP. De asemenea consola se integrează cu sisteme de ticketing extern precum BMC Remedy si HP OpenView. 22. Serverul de administrare este capabil să declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (Ex: Generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem în rețea). 23. Consola permite aplicarea de politici diferite pentru sisteme pe: • Sisteme individuale, • Grupuri de sisteme, • Sisteme din AD ce sunt același OU.	

					24. Consola știe să lanseze automat aplicații externe și să injecteze parametrii din evenimente. 25. Consola permite accesarea log-ului componentei de sincronizare de pe sisteme în timp real prin intermediul unui serviciu web. 26. Consola permite vizualizarea incidentelor de securitate și crearea de cazuri. 27. Consola permite integrarea și altor aplicații/echipamente de securitate ex. (Antivirus, SandBox, Proxy, Firewall) într-o consola unica pentru a unifica administrarea acestora. 28. Consola are capabilitati de diagnoza si sa ofere recomandari si solutii pentru problemele detectate 29. Consola suportă autentificare in regim Single Sign On (SSO) print utilizarea unei solutii de IDP 30. Consola dispune de posibilitatea de a necesita aprobare din partea managerului pentru schimbarile politicilor si task-urilor din cadrul solutiei. **IV. Raportarea** 1. Consola de administrare asigură generarea de rapoarte despre nodurile administrate și despre evenimentele generate de ele. 2. Consola permite crearea de noi rapoarte în mod granular cu informații extrase din	

					evenimente, sau despre sistemele administrate. 3. Rapoartele sunt generate sub forma de tabel, lista, sumar, sau grafic istoric. 4. Rapoartele pot fi exportate în format pdf, csv, html. Rapoartele pot fi personalizate cu logo-ul companiei. 5. Rapoartele pot fi salvate ca fișiere sau trimise prin e-mail. 6. Rapoartele pot fi exportate într-un format arhivat și expediate automat pe e-mail unor destinații presetate. 7. Consola permite să evalueze evenimentele primite de la stațiile de lucru și filtrarea lor pentru o mai buna identificare a informațiilor relevante. 8. Pot fi generate rapoarte utilizând: • Log-ul de audit administrativ, • Detalii despre sistemele administrate (detalii de configurare, hardware, utilizator), • Evenimente de sisteme, • Informații despre politicile și sarcinile aplicate sistemelor, • Informații furnizate de senzori. **V. Solicitări suplimentare** 1. Oferta comercială este pentru 100 stații de lucru. 2. Dispunem de oficiu de suport local, iar timpul de suport să fie 8/24 ore și 5/7 zile. 3. Oferta comercială include și serviciile de instalare și configurare.	

					4. Compania RSD este partener oficial al companiei Trellix. 5. Prezentăm CV-ul la doi specialiști tehnici angajati ai RSD-ului, certificati pe solutiile Trellix. 6. La solicitarea suntem pregătiți pentru a prezenta funcționalitățile produsului instalat, pe o platformă de testare, înainte de scurgerea timpului de anunțare a învingătorului. 7. Oferta comercială conține costul utilizării soluției pentru un an calendaristic (subscriptie) și nelimitat (Perpetual) 8. În dependență tipul licenței achiziționate (anuală sau pentru totdeauna), suportul este inclus în oferta comercială.	

Numele, Prenumele: Vitalie Bîrsan
În calitate de: Administrator
Ofertantul: ICS Reliable Solutions Distributor S.R.L.
Adresa: str. Alexandru cel Bun 85, MD-2012, mun Chisinau, Republica Moldova

Digitally signed by Bîrsan Vitalie
Date: 2024.02.26 11:07:50 EET
Reason: MoldSign Signature
Location: Moldova

Semnat:_____