

Specificații tehnice (F4.1)

Numărul procedurii de achiziție: LD nr. ocds-b3wdp1-MD-1607607781096 din 30 decembrie 2020, ora 16:00

Denumirea achiziției: Servicii DLP

Cod CPV	Denumirea serviciilor	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5
Lotul nr. 1: Servicii de prelungire a protecției datelor confidențiale la stațiile de lucru (modulul Endpoint) stații PC, All-in-One, note-bokuri				
4820000-0	Servicii de prelungire a protecției datelor confidențiale	La nivel de puncte finale (stații de lucru, baze de date, noduri de rețea): - identificarea automatizată, monitorizarea, blocarea și criptarea datelor confidențiale indiferent de amplasarea sau utilizarea lor; - procesarea și recunoașterea următoarelor tipuri de fișiere: a. Microsoft Office™ inclusiv Office 2013 și 2016 (ex.: Microsoft Word, Excel, PowerPoint, Outlook, Acces, Power Point, RTF, Wordpad, Text, etc.); b. fișiere grafice, de exemplu: Visio, PDF, TIFF, etc...; c. fișiere arhivate/comprimate, protejarea datelor de amenințările provenite în interiorul rețelei ca rezultat al transmiterii mesajelor instantanee și e-mail-urilor, publicarea informației pe pagini web, imprimarea și	Denumire soluției oferite - Licență McAfee Complete Data Protection Advancs 1yr BZ (P+) de tip perpetual cu mentenanță activă pentru 280 devices La nivel de puncte finale (stații de lucru, baze de date, noduri de rețea): - identificarea automatizată, monitorizarea, blocarea și criptarea datelor confidențiale indiferent de amplasarea sau utilizarea lor; - procesarea și recunoașterea următoarelor tipuri de fișiere: a. Microsoft Office™ inclusiv Office 2013 și 2016 (ex.: Microsoft Word, Excel, PowerPoint, Outlook, Acces, Power Point, RTF, Wordpad, Text, etc.); b. fișiere grafice, de exemplu: Visio, PDF, TIFF, etc...; c. fișiere arhivate/comprimate, protejarea datelor de amenințările provenite în interiorul rețelei	



	copierea documentelor pe suporturi mobile (USB, CD, DVD §.a.);	transmiterii mesajelor instantanee și e-mail-urilor, publicarea informației pe pagini web, imprimarea și copierea documentelor pe suporturi mobile (USB, CD, DVD §.a.);	
	– blocarea surselor de scurgere a informației confidențiale, precum și transmiterii prin intermediul aplicațiilor de schimb a fișierelor; – etichetarea documentelor conform provenienței acestora, astfel asigurând securizarea informației confidențiale care se copie pe suporturi mobile, prin aplicații web, aplicații de rețea și resurse partajate în rețea; – verificarea stațiilor de lucru pentru identificarea informațiilor confidențiale pe hard disk-uri și în mesajelor electronice din arhivele poștei electronice; – categorizarea dispozitivelor de stocare a datelor după identificatorul produsului, identificatorul producătorului, numărul de serie, clasa dispozitivului și denumirea acestuia; – criptarea sau blocarea informației încărcate pe suport amovibil, în dependență de conținutul informației; – protejarea accesului la fișierele aflate pe suporturi amovibile; – colectarea informației importante și critice cu privire la folosirea dispozitivelor (expeditor, destinatar, ștampila de timp și de date, utilizate în calitate de dovezi).	– blocarea surselor de scurgere a informației confidențiale, precum și transmiterii prin intermediul aplicațiilor de schimb a fișierelor; – etichetarea documentelor conform provenienței acestora, astfel asigurând securizarea informației confidențiale care se copie pe suporturi mobile, prin aplicații web, aplicații de rețea și resurse partajate în rețea; – verificarea stațiilor de lucru pentru identificarea informațiilor confidențiale pe hard disk-uri și în mesajelor electronice din arhivele poștei electronice; – categorizarea dispozitivelor de stocare a datelor după identificatorul produsului, identificatorul producătorului, numărul de serie, clasa dispozitivului și denumirea acestuia; – criptarea sau blocarea informației încărcate pe suport amovibil, în dependență de conținutul informației; – protejarea accesului la fișierele aflate pe suporturi amovibile; – colectarea informației importante și critice cu privire la folosirea dispozitivelor (expeditor,	



La nivel de puncte finale (stații de lucru, baze de date, noduri de rețea): – identificarea automatizată, monitorizarea, blocarea și criptarea datelor confidențiale indiferent de amplasarea sau utilizarea lor; procesarea și recunoașterea următoarelor tipuri de fișiere:	La nivel de puncte finale (stații de lucru, baze de date, noduri de rețea): – identificarea automatizată, monitorizarea, blocarea și criptarea datelor confidențiale indiferent de amplasarea sau utilizarea lor; procesarea și recunoașterea următoarelor tipuri de fișiere:
a. Microsoft Office™ inclusiv Office 2013 și 2016 (ex.: Microsoft Word, Excel, PowerPoint, Outlook, Acces, Power Point, RTF, Wordpad, Text, etc.); b. Fișiere grafice, de exemplu: Visio, PDF, TIFF, etc....; c. Fișiere arhivate/comprimate: protejarea datelor de amenințările provenite în interiorul rețelei ca rezultat al transmiterii mesajelor instantanee și e-mail-urilor, publicarea informației pe pagini web, imprimarea și copierea documentelor pe suporturi mobile (USB, CD, DVD ș.a.);	a. Microsoft Office™ inclusiv Office 2013 și 2016 (ex.: Microsoft Word, Excel, PowerPoint, Outlook, Acces, Power Point, RTF, Wordpad, Text, etc.); b. Fișiere grafice, de exemplu: Visio, PDF, TIFF, etc....; c. Fișiere arhivate/comprimate: protejarea datelor de amenințările provenite în interiorul rețelei ca rezultat al transmiterii mesajelor instantanee și e-mail-urilor, publicarea informației pe pagini web, imprimarea și copierea documentelor pe suporturi mobile (USB, CD, DVD ș.a.);
– blocarea surselor de scurgere a informației confidențiale, precum și transmiterii prin intermediul aplicațiilor de schimb a fișierelor; – etichetarea documentelor conform provenienței acestora, astfel asigurând securizarea informației confidențiale care se copie pe suporturi mobile, prin aplicații web, aplicații de rețea și resurse partajate în rețea; – verificarea stațiilor de lucru pentru identificarea informațiilor confidențiale pe hard disk-uri și în	destinatar, ștampila de timp și de date, utilizate în calitate de dovezi). La nivel de puncte finale (stații de lucru, baze de date, noduri de rețea): – identificarea automatizată, monitorizarea, blocarea și criptarea datelor confidențiale indiferent de amplasarea sau utilizarea lor; procesarea și recunoașterea următoarelor tipuri de fișiere: a. Microsoft Office™ inclusiv Office 2013 și 2016 (ex.: Microsoft Word, Excel, PowerPoint, Outlook, Acces, Power Point, RTF, Wordpad, Text, etc.); b. Fișiere grafice, de exemplu: Visio, PDF, TIFF, etc....; c. Fișiere arhivate/comprimate: protejarea datelor de amenințările provenite în interiorul rețelei ca rezultat al transmiterii mesajelor instantanee și e-mail-urilor, publicarea informației pe pagini web, imprimarea și copierea documentelor pe suporturi mobile (USB, CD, DVD ș.a.); – blocarea surselor de scurgere a informației confidențiale, precum și transmiterii prin intermediul aplicațiilor de schimb a fișierelor; – etichetarea documentelor conform provenienței acestora, astfel asigurând securizarea informației confidențiale care se copie pe suporturi mobile, prin aplicații web, aplicații de rețea și resurse partajate în rețea;



		mesajelor electronice din arhivele poștei electronice; - categorizarea dispozitivelor de stocare a datelor după identificatorul produsului, identificatorul producătorului, numărul de serie, clasa dispozitivului și denumirea acestuia; - criptarea sau blocarea informației încărcate pe suport amovibil, în dependență de conținutul informației; - protejarea accesului la fișierele aflate pe suporturi amovibili; - colectarea informației importante și critice cu privire la folosirea dispozitivelor (expeditor, destinatar, ștampila de timp și de date, utilizate în calitate de dovezi). Platforma sistemului DLP trebuie să asigure următoarele: - posibilitatea integrării cu sistemele de operare Windows licențiate cu toate versiunile actuale existente pe piață; - posibilitatea integrării centralizate a altor module de securitate (filtrare web, controlaplicații, antivirus, criptare, firewall, gestionare riscuri, ș.a.); - funcțional complex și scalabilitate avansată; suport adecvat (operativ) din partea vendorului și transparență în dezvoltareaprodusului prin publicarea periodică a "problemelor cunoscute". În cadrul prestării Serviciului DLP se vor asigura următoarele lucrări:	- verificarea stațiilor de lucru pentru identificarea informațiilor confidențiale pe hard disk-uri și în mesajelor electronice din arhivele poștei electronice; - categorizarea dispozitivelor de stocare a datelor după identificatorul produsului, identificatorul producătorului, numărul de serie, clasa dispozitivului și denumirea acestuia; - criptarea sau blocarea informației încărcate pe suport amovibil, în dependență de conținutul informației; - protejarea accesului la fișierele aflate pe suporturi amovibili; - colectarea informației importante și critice cu privire la folosirea dispozitivelor (expeditor, destinatar, ștampila de timp și de date, utilizate în calitate de dovezi). Platforma sistemului DLP asigură următoarele: - posibilitatea integrării cu sistemele de operare Windows licențiate cu toate versiunile actuale existente pe piață; - posibilitatea integrării centralizate a altor module de securitate (filtrare web, controlaplicații, antivirus, criptare, firewall, gestionare riscuri, ș.a.); - funcțional complex și scalabilitate avansată; suport adecvat (operativ) din partea vendorului și transparență în dezvoltareaprodusului prin publicarea periodică a "problemelor cunoscute".
--	--	--	--



		- asigurarea funcționalității serviciului, cu prezentarea lunară a rapoartelor de documentare a conformității nivelurilor de funcționalitate ale serviciului. - asigurarea condițiilor pentru conectarea la sistemul DLP a 280 stații de lucru, precum și suportul necesar la conectarea acestora 8/24 (ore) și 5/7 (zile). - asigurarea securității serviciului și înregistrărilor din cadrul serviciului. suportul tehnic, în conformitate cu termenii și condițiile speciale pentru prestarea serviciului, anexate la contractul de bază. - instalarea update-urilor necesare (după testarea preventivă a acestora); - back-up-ul lunar al înregistrărilor și păstrarea acestor copii de rezervă pentru o perioadă minimă de 12 luni.	transparență în dezvoltarea produsului prin publicarea periodică a "problemelor cunoscute". În cadrul prestării Serviciului DLP vom asigura următoarele lucrări: - asigurarea funcționalității serviciului, cu prezentarea lunară a rapoartelor de documentare a conformității nivelurilor de funcționalitate ale serviciului. - asigurarea condițiilor pentru conectarea la sistemul DLP a 280 stații de lucru, precum și suportul necesar la conectarea acestora 8/24 (ore) și 5/7 (zile). - asigurarea securității serviciului și înregistrărilor din cadrul serviciului. suportul tehnic, în conformitate cu termenii și condițiile speciale pentru prestarea serviciului, anexate la contractul de bază. - instalarea update-urilor necesare (după testarea preventivă a acestora); - back-up-ul lunar al înregistrărilor și păstrarea acestor copii de rezervă pentru o perioadă minimă de 12 luni.	
--	--	--	--	--

Semnat:

Numele, Prenumele: Ovidiu Vincenzo Creangă

În calitate de: Administrator

Ofertantului: Reliable Solutions Distributor

Adresa: str. Alexandru cel Bun 85, MD-2012, mun Chisinau, Republica Moldova.

