XONTECH

Specificaţii tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloanele 3, 4, 5, 7, iar de către autoritatea contractantă – în coloanele 1,2, 6, 8]

Numărul procedurii de achiziţie:	**ocds-b3wdp1-MD-1602163426198 din 08.10.2020**
Denumirea procedurii de achiziţie:	**Pachete software pentru reţele, internet şi intranet**

Cod CPV	Denumirea bunurilor	Modelul articolului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7	8
48200000-0	Lotul nr. 11: Subscripția pentru Soluția Antivirus	**F-Secure PSB Company Managed Computer Protection Premium for 250 devices, 12 months.**	**Finlanda**	**F-Secure**	Cerințe generale: 1. Soluție de protecție anti- virus real-time care acoperă cel puțin 250 de stații de lucru; 2. Gestionare prin consolă centralizată 3. Sisteme de operare suportate minim: Windows 7, 8, 8.1, 10; MacOS X v. 10.8 si mai sus. 4. Posibilitate de instalare client la distanță	Conform Anexei 1 la formular. Matricea de conformitate	Nu se aplică

					5. Integrare cu LDAP/Active Directory 6. Configurare customizabilă de politici 7. Posibilitatea utilizării wildcards și variabile de cale pentru a specifica fișierele și folderele pe care să le excludă de la scanare 8. Aplicarea centralizată a politicilor pe partea client 9. Gruparea configurabilă a clienților și aplicarea politicilor pe grupe 10. Monitorizare real-time, notificări, rapoarte 11. Inițierea remote a scanării de hosturi (On-Demand) 12. Informație centralizată despre stația de lucru a clienților (sistem de		

					operare, IP, statut, ultima scanare) 13. Posibilitatea generării rapoartelor de scanare sau vulnerabilităților 14. Posibilitate de a introduce remote clientul (endpointul) în ”carantină” 15. Data activării subscripției: 04.02.2021 16. Termenul de valabilitate/ garanție: 36 luni		

Semnat:
Nume: **Irina Vicol**
În calitate de: **Administrator**
Ofertantul: **Xontech Systems SRL**
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.
Data: “26” octombrie 2020

Anexa 1

Matricea de conformitate conform cerințelor solicitate pentru Lotul 11:

Nr. d/o	Denumirea bunurilor solicitate	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant
		Lotul 11	
1.	Lotul nr. 11: Subscripția pentru Soluția Antivirus	Cerințe generale: 1. Soluție de protecție anti- virus real-time care acoperă cel puțin 250 de stații de lucru; 2. Gestionare prin consolă centralizată 3. Sisteme de operare suportate minim: Windows 7, 8, 8.1, 10; MacOS X v. 10.8 si mai sus. 4. Posibilitate de instalare client la distanță 5. Integrare cu LDAP/Active Directory 6. Configurare customizabilă de politici 7. Posibilitatea utilizării wildcards și variabile de cale pentru a specifica fișierele și folderele pe care să le excludă de la scanare 8. Aplicarea centralizată a politicilor pe partea client 9. Gruparea configurabilă a clienților și aplicarea politicilor pe grupe 10. Monitorizare real-time, notificări, rapoarte 11. Inițierea remote a scanării de hosturi (On-Demand) 12. Informație centralizată despre stația de lucru a clienților (sistem de operare, IP, statut, ultima scanare) 13. Posibilitatea generării rapoartelor de scanare sau vulnerabilităților 14. Posibilitate de a introduce remote clientul (endpointul) în ”carantină” 15. Data activării subscripției: 04.02.2021	**F-Secure PSB Company Managed Computer Protection Premium Suite for 250 devices, 12 months.** **1.1. Descriere generală:** - Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protecția a 250 de statii de lucru. • soluția este una bazată pe tehnologia Cloud, care oferă un management centralizat a tuturor stații de lucru; • soluția asigură protecție in timp real, impotriva virusilor (ransomware – crypto) cu scopul prevenirii distrugerii și modificării datelor, amenintarilor spyware, rootkit-urilor, tentativelor de intruziune, spam-urilor si a altor mesaje nedorite. • soluția oferă actualizari automate a versiunilor noi si a hotfix-urilor; • soluția oferă protectie impotriva virusilor si noilor amenintari necunoscute bazată pe analize euristice, de comportament și reputație; • soluția include patch management cu opțiuni pentru excluderi și actualizări manuale si analiza vulnerabilitatilor din retea; • soluția oferă funcționalități de firewall, intrusion prevention si application control;

		16. Termenul de valabilitate/ garanție: 36 luni	• soluția oferă posibilități exacte de activare si dezactivare, de configurare a funcționalităților precum: scanarea antivirus la cerere, firewall gestionat, controlul accesului la Internet, controlul aplicațiilor care să blocheze executarea aplicațiilor și scripturilor conform regulilor create sau definite de administrator, scanarea traficului web, controlul dispozitivelor; • soluția oferă posibilitatea de aplicare a politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale sau utilizatori de AD; • soluția oferă instalare centralizată; • soluția oferă consolă unică de management cu instalare in cloud; • soluția oferă functional Multi-engine anti-malware; • soluția include funcționalul de Patch Management, pentru a asigura actualizarea de software atît de la produsele Microsoft, cît şi pentru alte aplicaţii de la terţi; • soluția oferă funcțional de Firewall ce va permite setarea unor reguli bazate pe actiuni (blocarea sau permiterea) și direcție (intrare sau iesire) pentru controlul și monitorizarea traficului la nivel de endpoint și rețea, astfel furnizând un nivel de securitate suplimentar, aflat deasupra regulilor utilizatorului pentru Windows Firewall şi a altor reguli pentru domenii. • soluția oferă funcțional de Protecție Web: protejarea accesărilor pe site-uri bancare (Control conexiune) care alertează utilizatorii atunci când aceştia au o conexiune securizată către site-uri de operaţiuni bancare online şi către alte site-uri precizate care tratează informaţii sensibile; blocarea site-urilor cunoscute ca fiind dăunătoare (Navigare bazată pe reputaţie); împiedicarea accesului la site-urile nepermise (Controlul conţinutului Web); blocarea accesului la tipurile de conţinut nepermise (Filtrare tipuri de conţinut).;

			• soluția oferă funcțional de Controlul conexiunilor prin securizarea plăților online si afisarea unui pop-up care blocheaza celelalte pagini si imposibilitate accesarii altor decat cea in care se efectueaza tranzactia. • soluția oferă funcțional de scanare în timp real a tuturor obiectelor pe care le accesează utilizatorii finali, pentru depistarea programelor de tip malware și inclusiv să ofere posibilitatea de configurare și efecuare a scanării manuale; • soluția oferă funcțional de scanare a aplicatiilor in cloud; • soluția oferă funcțional de Scanare a semnăturilor; • soluția include funcțional de control a dispozitivelor externe, oferă posibilitatea: de a seta restricţii în privinţa modului în care utilizatorii pot accesa dispozitive USB, precum dispozitive de stocare, camere USB şi imprimante; de a interzcie accesul la orice dispozitiv de stocare USB; de a stopa rularea executabilelor stocate pe astfel de dispozitive; de a seta restricţii pe grupuri de dispozitive; • soluția oferă funcțional de analiză euristică si zero day, de comportament și reputație; • soluția oferă funcțional de Sandbox automatizat inclus – pentru analiza amănunțită prin detonarea fișierilor malițioase sau care nu pot fi protejate in baza de semnătura sau comportament; • soluția oferă funcțional de control al aplicatiilor, prin setarea unor reguli de blocare create ca excluderi pentru a bloca un acces anume și este bazat: - pe actiuni precum permiterea, blocarea, sau permiterea și monitorizarea aplicațiilor; - pe evenimente precum pornire aplicație, încărcare modul, pornire program de instalare, acces la fișiere, pornire aplicație și încărcare modul; - prin stabilirea unor condiții care să poată fi selectate după atribute (cale destinație, nume fișier destinație, reputație

			destinație, versiune fișier destinație, cod hash pentru certificat la destinație.....etc), condiție și valoare, ce vor asigura activarea regulilor de excludere; • soluția oferă funcțional de Management API prin integrarea solutiilor terte precum: SIEM/RMM; **1.2. Administrarea solutiei:** • administrarea soluției se face printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite careva echipamente hardware(servere de management) sau careva software special. • consola de este capabilă de a funcționa pe orice dispozitiv și conține toate funționalitățile sus solicitate; • suportă următorele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; • interfața consolei de administare asigură posibilitatea de funcționare în limbile: romana, rusă si engleză cu capacitatea de a putea fi selectată limba dorită; • administratorul poate permite sau interzice utilizatorului de a activa sau dezactiva caracteristicile de securitate setate; **1.3. Funcționalul de raportare și alerte:** Soluția permite generarea de rapoarte grafice detaliate, saptămînal sau lunar, cu posibilitate de export, inclusiv cu remitere automată către adrese de email specificate, rapoartele cuprind informație despre: - Clasament computere (după infecţii blocate); - Top de infecţii tratate; - Infecţii gestionate; - Starea de protecţie; - Cele mai recente actualizări pentru definiţiile de malware pe computere;

			- Dacă s-au instalat actualizările de securitate; - Soluția permite setarea și configurarea de alerte, declanșarea lor poate fi aplicată pentru următoarele acțiuni: blocat, redenumit, oprit, șters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat şi acţiune suplimentară solicitată de la utilizator, mutat în coşul de gunoi; - Soluția asigură posibilitatea de trimitere a alertelor in momentul declanșării prin email specificat de administrator si permite setarea limbii dorite in care să fie emailul (română, engleză, rusă); Alte detalii suplimentare despre produsul ofertat este in datasheet anexat cu oferta si poate fi accesat pe acest link: https://www.f-secure.com/en/business/solutions/endpoint-security/protection-service-for-business