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 2, 6, 8]

Numărul procedurii de achiziţie: **ocds-b3wdp1-MD-1595939704756 din 28 iulie 2020.**
Denumirea procedurii de achiziţie: Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate.(Specificațiile tehnice confor caietului de sarcini)

Nr. d/o	Cod CPV	Denumirea bunurilor	Modelul articolului	Ţara de origine	Producătorul	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
1	48761000-0	Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate	**F-Secure PSB Company Managed Computer Protection Premium Suite for 195 devices, 12 months.** **F-Secure PSB Company Managed Server Protection Premium Suite for 5 devices, 12 months**	**Finlanda**	**F-Secure Corporation**	**1. Cerințele tehnice funcționale minim solicitate:** - Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protecția a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate. - Soluția trebuie sa asigure protecție si management centralizat pentru statii de lucru, servere și dispozitive mobile cu următoarele sisteme de operare: *Stații de lucru*: - Microsoft Windows 7 Service Pack 1; 8.1; 10; (all 32-bit and 64-bit editions); - macOS 10.12, 10.13, 10.14; *Servere*: - Microsoft® Windows Server 2008 R2; 2012; 2012 Essentials; 2012 R2; 2012 R2 Essentials; 2012 R2 Foundation; 2016 Standard;	**1.Cerinte tehnice functionale ofertate:** - Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protecția a 195 de statii de lucru fizice/virtualizate si 5 servere fizice/virtualizate. - Soluția asigura protecție si management centralizat pentru statii de lucru, servere și dispozitive mobile cu următoarele sisteme de operare: *Stații de lucru*: - Microsoft Windows 7 Service Pack 1; 8.1; 10; (all 32-bit and 64-bit editions - macOS 10.12, 10.13, 10.14; *Servere* • Microsoft® Windows Server 2008 R2; 2012; 2012 Essentials; 2012 R2; 2012 R2 Essentials; 2012 R2 Foundation; 2016 Standard; 2016	

						2016 Essentials; 2016 Datacenter: 2016 Core; 2019 Standard; 2019 Essentials; 2019 Datacenter; 2019 Core; CentOS, Debian, Oracle Linux, RHCK and UEK, RUEL, SUSE Linux Enterprise Servei 11 SP3, SP4, Ubuntu, etc. *Dispozitive Mobile*: Android 4.03 and later; iOS 9.x and later • soluția ofertată trebuie să fie una bazată pe tehnologia Cloud, care să ofere un management centralizat a tuturor dispozitivelor: stații de lucru, servere și dispozitive mobile; • soluția trebuie sa asigure proiecție in timp real, impolriva virușilor (ransomware - crypto) cu scopul prevenirii distrugerii și modificării datelor, amenințărilor spyware, rootkit-urilor, tentativelor de intruziune, spam-urilor si a altor mesaje nedorite. • soluția trebuie să ofere actualizări automate a versiunilor noi si a botfix-urilor; • soluția trebuie să ofere protecție impotriva virușilor si noilor amenințări necunoscute care să fie bazată pe analize euristice, de comportament si reputatie; • soluția trebuie să includă patch management cu opțiuni pentru excluderi și actualizări manuale si analiza vulnerabilităților din rețea; - soluția trebuie să ofere funcționalități de firewall, intrusion prevention, application control si sanbox pentru analiza traficului de tip ransomware si detonarea acestuia; - soluția trebuie să asigure criptarea automată prin VPN, a întregului trafic realizat dintre dispozitivele mobile, permițând utilizarea în	Essentials; 2016 Datacenter; 2016 Core; 2019 Standard; 2019 Essentials; 2019 Datacenter; 2019 Core; CentOS, Debian, Oracle Linux, RHCK and UEK, RHEL, SUSE Linux Enterprise Server 11 SP3, SP4, Ubuntu, etc. *Dispozitive Mobile*: Android 4.03 and later; iOS 9.x and later • soluția este una bazată pe tehnologia Cloud, care oferă un management centralizat a tuturor dispozitivelor: stații de lucru, servere și dispozitive mobile; • 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 care să fie 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; • soluția ofera posibilitatea pentru criptarea automată prin VPN, a întregului trafic realizat dintre dispozitivele mobile, permițând utilizarea în condiții de	

						condiții de siguranță a Wi-Fi public și rețelelor mobile; - soluția trebuie să ofere 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 traficulu web, controlul dispozitivelor; - soluția trebuie să ofere posibilitatea de aplicare a politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale sau utilizatori de AD; - soluția trebuie să ofere instalare centralizată a stațiilor de lucru si terminalelor mobile; - soluția trebuie să ofere consolă unică de management cu instalare in cloud; - soluția trebuie să ofere funcțional Multi-engine anti-malware; - soluția trebuie să includă funcționalul de Patch Management, pdntru a asigura actualizarea de software atît de la produsele Microsoft, cit și pentru alte aplicații de la terți; - soluția trebuie să ofere funcțional de Firewall ce va permite setarea unor reguli bazate pe acțiuni (blocarea sau permiterea) și direcție(intrare sau ieșire) pentru controlul și monitorizarea traficului la nivel de endpoint și rețea, care sa furnizeze un nivel de securitate suplimentar, aflat deasupra regulilor utilizatorului pentru Windows	siguranță a Wi-Fi public și rețelelor mobile; • 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 și a altor reguli pentru domenii.	

						Firewall și a altor reguli pentru domenii. - soluția trebuie să ofere funcțional de Protecție Web: protejarea accesărilor pe site-uri bancare (Control conexiune) care să alerteze utilizatorii atunci când aceștia au o conexiune securizată către site-uri de operațiuni bancare online și către alte site-uri precizate care tratează informații sensibile; blocarea site-urilor cunoscute ca fiind dăunătoare (Navigare bazată pe reputație); împiedicarea accesului la site-urile nepermise (Controlul conținutului Web); blocarea accesului la tipurile de conținut nepennise (Filtrare tipuri de conținut).; - soluția trebuie să ofere funcțional de Controlul conexiunilor prin securizarea plăților online si afișarea unui pop-up care blocoeaza celelalte pagini si imposibilitate accesării altor decât cea in care se efectuează tranzacția. - soluția trebuie să ofere 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 trebuie să ofere funcțional de scanare a aplicațiilor in cloud; - soluția trebuie să ofere funcțional de Scanare a semnăturilor; - soluția trebuie să includă funcțional de control a dispozitivelor externe, să ofere posibilitatea: de a seta restricții în privința modului în care utilizatorii pot accesa dispozitive	• 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 și 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	

						USB, precum dispozitive de stocare, camere USB și imprimante; de a interzcie accesul la orice dispozitiv de stocare USB; de a stopa rularea executabilelor stocate pe astfel de dispozitive; de a seta restricții pe grupuri de dispozitive; - soluția trebuie să ofere funcțional de analiză euristică si zero day, de comportament și reputație; - soluția trebuie să ofere 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 trebuie să ofere funcțional de control al aplicațiilor, prin setarea unor reguli de blocare create ca excluderi pentru a bloca un acces anume și să fie bazate: • pe acțiuni 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 trebuie să ofere funcțional de Management API prin integrarea soluțiilor terte precum: SIEM/RMM;	dispozitive USB, precum dispozitive de stocare, camere USB și 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;	

						1.1 Cerințele tehnice vis-a-vis de administrarea soluției: - administrarea soluției ofertate este necesara să se faca printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite careva echiapmente hardware(servere de management) sau careva software special. - consola de administrare trebuie să fie capabilă de a funcționa pe orice dispozitiv și să conțină toate funționalitățile sus solicitate; - să supone următorele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; - interfața consolei de administare trebuie să asigure posibilitatea de funcționare în limbile: romana, rusă si engleză obligatoriu, cu capacitatea de a putea fi selectată limba dorită, în scopul unei administrări mai ușoare de către administratori; - administratorul trebuie să poată permite sau interzice utilizatorului de a activa sau dezactiva caracteristicile de securitate setate; **1.2. Cerințe vis-a-vis de funcționalul de raportare și alerte:** - Soluția trebuie să permită generarea de rapoarte grafice detaliate, saptâmînal sau lunar, cu posibilitate de export minimum in format (csv), inclusiv cu remitere automată către adrese de email specificate, rapoartele trebuie să cuprindă minim informație despre: • Clasament computere (după infecții blocate); • Top de infecții tratate; • Infecții gestionate; • Starea de protecție;	**1.1. Cerintele tehnice vis-a-vis de 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 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; **1.2. Cerințe vis-a-vis de funcționalul de raportare și alerte:** - Soluția permite generarea de rapoarte grafice detaliate, saptămînal sau lunar, cu posibilitate de export minimum in format (csv), inclusiv cu remitere automată către adrese de email specificate, rapoartele cuprind informație despre: • Clasament computere (după infecții blocate); • Top de infecții tratate; • Infecții gestionate; • Starea de protecție;	

						• Cele mai recente actualizări pentru definițiile de malware pe computere; • Dacă s-au instalat actualizările de securitate; - Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru minim următoarele acțiuni: blocat, redenumit, oprit, șters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat și acțiune suplimentară solicitată de la utilizator, mutat în coșul de gunoi; - Soluția trebuie să asigure posibilitatea de trimitere a alertelor in momentul declanșării prin email specificat de administrator si sa permită setarea limbii dorire in care să fie emailul (minim română, engleză, rusă); **1.3. Alte cerințe obligatorii:** - Pentru soluția ofertată se solicită a fi 12 luni suport local și de la producător. - Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului. - Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comerciala. - Ofertantul va avea minim o persoana certificata in calitate de auditor intem pentru sistemul de management al securității informaționale conform ISO 27001:2013;	• Cele mai recente actualizări pentru definițiile 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 și acțiune suplimentară solicitată de la utilizator, mutat în coșul 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); **1.3. Alte cerințe obligatorii:** - Pentru soluția ofertată se oferă 12 luni suport local de la Xontech Systems și de 12 luni de la producător. - Producătorul oferă suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului Xontech Systems. - Lucrările de instalare, configurare, punerea în funcțiune a soluției vor fi executate de Xontech Systems, conform ofertei comerciale. - Persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013 , certificatul este atasat cu oferta;	

						- Soluția trebuie sa se regaseasca in Gartner in ultimii 3 ani de zile si sa ocupe locuri de top in testele internaționale “AV-TEST”	- Solutia ‚F-Secure’ se regaseste in Gartner in ultimii 3 ani si ocupa locuri de top in testele internationale „AV-TEST”	
		TOTAL						

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: “28” iulie 2020

Digitally signed by Vicol Irina
Date: 2020.07.30 17:14:53 EEST
Reason: MoldSign Signature
Location: Moldova