

Specificații 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,]

Numărul procedurii de achiziție: ocds-b3wdp1-MD-1669023732449 din 21.11.2022						
Denumirea procedurii de achiziție: Pachete software antivirus						
Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standard e de referință
1	2	3	4	5	6	7
Pachete software antivirus, subscripție pentru 3 ani	1. WithSecure Elements EPP for Computers Premium, Company Managed License for 3 years Governmental – 96 licențe 2. WithSecure Elements EPP for Servers Premium, Company Managed License for 3 years Governmental – 4 licențe	Finlanda	WithSecure	Conform caietului de sarcini	Conform Anexei la formular. Matricea de conformitate	

Semnat:

Nume: **Irina Vicol**

În calitate de: **Administrator**

Ofertantul: **Xontech Systems SRL**

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

Matricea de conformitate conform Conform Anexei 1 solicitate in SIA RSAP

Nr. d/o	Denumirea bunurilor solicitate	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant
1.	Pachete software antivirus, subscripție pentru 3 ani	Soluție de protecție si securitate antivirus pentru protectia infrastructurii: Se solicita achizitia solutiei de securitate corporativa in cadrul institutiei: - pentru 96 statii de lucru fizice si virtualizate; - pentru 4 servere fizice si virtualizate; Solutia de securitate ofertata trebuie sa se regaseasca in Gartner in ultimii 4 ani de zile si sa ocupe locuri de top in testele internationale "AV-TEST" cel putin 8 ani la rind. In cazul in care ofertantul doreste sa ofere un produs alternativ decat cel existent, acesta trebuie sa intruneasca minim cerintele de mai sus, echivalent solutiei instalate deja in cadrul institutiei: 1.1.Cerintele tehnice functionale minim solicitate fata de solutia antivirus pentru protectia statiilor de lucru si a serverelor: Solutia trebuie sa asigure protectie si management centralizat pentru statii de lucru, servere și dispozitive mobile care sa acopere urmatoarele sisteme de operare:	Se oferă Soluția de protecție si securitate antivirus WithSecure Elements EPP Premium pentru protectia infrastructurii: Se oferă soluție de securitate corporativa WITHSECURE care este o platforma integrata pentru managementul securității endpoint-urilor, gândita ca o soluție modulara și scalabila, bazată pe tehnologia Cloud, pentru a minimiza resursele locale.: - pentru 96 statii de lucru fizice si virtualizate; - pentru 4 servere fizice si virtualizate; Solutia de securitate ofertata se regaseste in Gartner in ultimii 4 ani de zile si ocupa locuri de top in testele internationale "AV-TEST" cel putin 8 ani la rind. 1.1.Specificații tehnice functionale oferate pentru solutia antivirus pentru protectia statiilor de lucru si a serverelor: Solutia aigura protectie si management centralizat pentru statii de lucru, servere și dispozitive mobile care acoperă urmatoarele sisteme de operare, licentierea fiind separata dar cu managementul dintr-o singura interfata:

	Stații de lucru: - Microsoft Windows 7 Service Pack 1; 8.1; 10 ,11; (all 32-bit and 64-bit editions); - macOS 10.12, 10.13, 10.14, 11, 12; Servere: - Microsoft® Windows Server 2008 R2 - Microsoft® Small Business Server 2011, Standard edition - Microsoft® Small Business Server 2011, Essentials - Microsoft® Windows Server 2012 - Microsoft® Windows Server 2012 Essentials - Microsoft® Windows Server 2012 R2 - Microsoft® Windows Server 2012 R2 Essentials - Microsoft® Windows Server 2012 R2 Foundation - Microsoft® Windows Server 2016 Standard - Microsoft® Windows Server 2016 Essentials - Microsoft® Windows Server 2016 Datacenter - Microsoft® Windows Server 2016 Core - Microsoft® Windows Server 2019 Standard - Microsoft® Windows Server 2019 Essentials - Microsoft® Windows Server 2019 Datacenter - Microsoft® Windows Server 2019 Core - Microsoft Windows Server 2022 Standard - Microsoft Windows Server 2022 Essentials - Microsoft Windows Server 2022 Datacenter - Microsoft Windows Server 2022 Core Servere Terminale:	Stații de lucru: - Microsoft Windows 7 Service Pack 1; 8.1; 10 ,11; (all 32-bit and 64-bit editions); - macOS 10.12, 10.13, 10.14, 11, 12; Servere: - Microsoft® Windows Server 2008 R2 - Microsoft® Small Business Server 2011, Standard edition - Microsoft® Small Business Server 2011, Essentials - Microsoft® Windows Server 2012 - Microsoft® Windows Server 2012 Essentials - Microsoft® Windows Server 2012 R2 - Microsoft® Windows Server 2012 R2 Essentials - Microsoft® Windows Server 2012 R2 Foundation - Microsoft® Windows Server 2016 Standard - Microsoft® Windows Server 2016 Essentials - Microsoft® Windows Server 2016 Datacenter - Microsoft® Windows Server 2016 Core - Microsoft® Windows Server 2019 Standard - Microsoft® Windows Server 2019 Essentials - Microsoft® Windows Server 2019 Datacenter - Microsoft® Windows Server 2019 Core - Microsoft Windows Server 2022 Standard - Microsoft Windows Server 2022 Essentials - Microsoft Windows Server 2022 Datacenter - Microsoft Windows Server 2022 Core Servere Terminale:
--	---	---

		- Microsoft Windows Terminal/RDP Services (on the above mentioned Windows Server platforms) - Citrix® XenApp 5.0 - Citrix® XenApp 6.0 - Citrix® XenApp 6.5 - Citrix® XenApp 7.5, 7.6, 7.14, 7.15 - Citrix® Virtual Apps and Desktops 2009 Linux: - AlmaLinux 8 - Amazon Linux 2 - CentOS 7 (7.3 or newer) - CentOS 8 - CentOS Stream 8 - Debian 9 - Debian 10 - Debian 11 (with no SELinux enabled) - Oracle Linux 7 - Oracle Linux 8 - RHEL 7 (7.3 or newer) - RHEL 8 - SUSE Linux Enterprise Server 12 - SUSE Linux Enterprise Server 15 - Ubuntu 16.04 - Ubuntu 18.04 - Ubuntu 20.04 Dispozitive Mobile:	- Microsoft Windows Terminal/RDP Services (on the above mentioned Windows Server platforms) - Citrix® XenApp 5.0 - Citrix® XenApp 6.0 - Citrix® XenApp 6.5 - Citrix® XenApp 7.5, 7.6, 7.14, 7.15 - Citrix® Virtual Apps and Desktops 2009 Linux: - AlmaLinux 8 - Amazon Linux 2 - CentOS 7 (7.3 or newer) - CentOS 8 - CentOS Stream 8 - Debian 9 - Debian 10 - Debian 11 (with no SELinux enabled) - Oracle Linux 7 - Oracle Linux 8 - RHEL 7 (7.3 or newer) - RHEL 8 - SUSE Linux Enterprise Server 12 - SUSE Linux Enterprise Server 15 - Ubuntu 16.04 - Ubuntu 18.04 - Ubuntu 20.04 Dispozitive Mobile:
--	--	--	--

		- Android 7.0 (Nougat) sau mai sus; iOS 12.1 sau mai sus, iPadOS 13 sau mai sus, care sa ofere browsing protection separat securizat, mobile VPN pentru protecția personală, protecție malware cel puțin pentru Android. ○ Solutia trebuie sa ofere urmatoarele functionalitati - soluția oferată 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 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 trebuie să ofere actualizari automate a versiunilor noi si a hotfix-urilor; - soluția trebuie să ofere protectie impotriva virusilor si noilor amenintari necunoscute care să fie bazată pe analize euristice, de comportament și reputație; - soluția trebuie să includă patch management cu opțiuni pentru excluderi și actualizări manuale; - Solutia trebuie sa ofere statistica pentru urmatoarele: top patch-uri instalate, severitatea patch-urilor, top vendori dupa cantitatea actualizarilor. - Solutia trebuie sa ofere posibilitatea de a crea politici de securitate ce vor fi distribuite la discreția administratorului. - Solutia trebuie sa ofere posibilitatea de a compara una sau mai multe politici de securitate. - Solutia trebuie sa ofere posibilitatea de a stabili politica implicita pentru calculatoare , servere , dispozitive mobile , linux , macOS.	- Android 7.0 (Nougat) sau mai sus; iOS 12.1 sau mai sus, iPadOS 13 sau mai sus, care sa ofere browsing protection separat securizat, mobile VPN pentru protecția personală, protecție malware cel puțin pentru Android. ○ Solutia ofera urmatoarele functionalitati - soluția oferată este bazată pe tehnologia Cloud, care ofera un management centralizat a tuturor dispozitivelor: stații de lucru, servere și dispozitive mobile; - soluția asigura 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 ofera actualizari automate a versiunilor noi si a hotfix-urilor; - soluția ofera 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; - Solutia ofera statistica pentru urmatoarele: top patch-uri instalate, severitatea patch-urilor, top vendori dupa cantitatea actualizarilor. - Solutia ofera posibilitatea de a crea politici de securitate ce vor fi distribuite la discreția administratorului. - Solutia ofera posibilitatea de a compara una sau mai multe politici de securitate. - Solutia ofera posibilitatea de a stabili politica implicita pentru calculatoare , servere , dispozitive mobile , linux , macOS.
--	--	---	---

		- soluția trebuie să ofere funcționalități de firewall, intrusion prevention, application control si sandbox 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 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 traficului web, controlul dispozitivelor; - soluția trebuie să ofere posibilitatea de a scana calculatoarele din Active Directory, ce nu sunt protejate de agentul de securitate. - Solutia trebuie sa ofere posibilitatea de a descarca agentul de securitate in format de tip .msi pentru ulterioara implementare in AD. - Solutia trebuie sa ofere posibilitatea de a transmite invitatie pe email, pentru descarcarea agentului de securitate cu licenta integrata; - soluția trebuie să ofere instalare centralizată a stațiilor de lucru si terminalelor mobile; - solutia trebuie sa ofere posibilitatea de a activa pentru utilizatori dubla autentificare. - soluția trebuie să ofere functional Multi-engine anti-malware;	- soluția ofera funcționalități de firewall, intrusion prevention, application control si sandbox pentru analiza traficului de tip ransomware si detonarea acestuia; - soluția ofera posibilitatea de a asigura criptarea automată prin VPN, a întregului trafic realizat dintre dispozitivele mobile, permițând utilizarea în condiții de siguranță a Wi-Fi public și rețelelor mobile, prin achiziționarea licenței aditionale pentru dispozitivele mobile, care la moment nu sunt solicitate in cadrul licitatiei. - soluția ofera 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 ofera posibilitatea de a scana calculatoarele din Active Directory, ce nu sunt protejate de agentul de securitate. - Solutia ofera posibilitatea de a descarca agentul de securitate in format de tip .msi pentru ulterioara implementare in AD. - Solutia ofera posibilitatea de a transmite invitatie pe email, pentru descarcarea agentului de securitate cu licenta integrata; - soluția ofera instalare centralizată a stațiilor de lucru si terminalelor mobile(terminalele mobile se licentiaza separat, la moment nu sunt solicitate in cadrul licitatiei); - solutia ofera posibilitatea de a activa pentru utilizatori dubla autentificare. - soluția ofera functional Multi-engine anti-malware;
--	--	--	--

		- soluția trebuie să includă funcționalul de Patch Management, pentru a asigura actualizarea de software atât de la produsele Microsoft, cât și pentru alte aplicații de la terți; - soluția trebuie să ofere posibilitatea vizualizării istoriilor instalărilor a aplicațiilor sau actualizărilor învechite minim conținând următoarele date: timpul instalării, vendor, aplicație, versiunea instalată, versiunea anterioară instalată, numele calculatorului, statutul instalării, criticitatea actualizării, CVE ID, Bulletin ID. Posibilitatea filtrării după: categorii de actualizări, perioada, statut, tipul de platformă. Posibilitatea de a exporta informația în CSV fisier. - 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 să furnizeze un nivel de securitate suplimentar, aflat deasupra regulilor utilizatorului pentru Windows 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 nepermise (Filtrare tipuri de conținut).; - soluția trebuie să ofere funcțional de Controlul conexiunilor prin securizarea plăților online și afișarea unui pop-up care blochează celelalte pagini și imposibilitate accesării altor decât cea în care se efectuează tranzacția, posibilitatea de a bloca conexiunile de la distanță (cu posibilitatea de a adăuga în	- soluția include funcționalul de Patch Management, pentru a asigura actualizarea de software atât de la produsele Microsoft, cât și pentru alte aplicații de la terți; - soluția oferă posibilitatea vizualizării istoriilor instalărilor a aplicațiilor sau actualizărilor învechite minim conținând următoarele date: timpul instalării, vendor, aplicație, versiunea instalată, versiunea anterioară instalată, numele calculatorului, statutul instalării, criticitatea actualizării, CVE ID, Bulletin ID. Posibilitatea filtrării după: categorii de actualizări, perioada, statut, tipul de platformă. Posibilitatea de a exporta informația în CSV fisier. - soluția oferă 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 să furnizeze un nivel de securitate suplimentar, aflat deasupra regulilor utilizatorului pentru Windows Firewall și a altor reguli pentru domenii. - soluția oferă 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 nepermise (Filtrare tipuri de conținut).; - soluția oferă funcțional de Controlul conexiunilor prin securizarea plăților online și afișarea unui pop-up care blochează celelalte pagini și imposibilitate accesării altor decât cea în care se efectuează tranzacția, posibilitatea de a bloca conexiunile de la distanță (cu posibilitatea de a adăuga
--	--	--	--

		excludere dupa IP) , blocarea liniei de comanda si a instrumentelor de scriptare - Solutia 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 efeculare a scanării manuale; - Solutia trebuie să ofere funcțional de scanare a aplicatiilor in cloud; - Solutia trebuie să ofere funcțional de Scanare a semnăturilor; - Solutia trebuie sa ofere posibilitatea de a expedia invitatii pentru instalarea agentului de securitate minim in limba romana , rusa , engleza si cu posibilitatea de a importa mai multe cutii postale printr-un fisier de tip CSV. Vizualizarea invitatiiilor expediate/expirate si posibilitatea de a reaminti utilizatorul printr-un email de a instala solutia de protectie. - solutia trebuie sa ofere posibilitatea de a importa/exporta politica de securitate si blocarea modificarilor in politica. - Solutia trebuie sa ofere posibilitatea de a seta scanarea programata (zilnic , saptaminal , lunar) - Solutia trebuie sa ofere posibilitatea de a scana fisierele de tip ZIP , RAR... - Solutia trebuie sa ofere posibilitatea de a scana fisierele de tip mailbox PST , OST... - Solutia trebuie sa permita activarea/dezactivarea modulelor de securitate, bazata de locatia identificata a dispozitivului dupa urmatoarele criterii: DNS server ip address , DHCP server ip address , default gateway ip address, wins ip address. - Solutia trebuie sa ofere procese automatizate precum: scanare rapidă pentru malware , scanare programată pentru malware , restart forțat , oprire forțată , hibernare , instalarea actualizarilor	in excludere dupa IP) , blocarea liniei de comanda si a instrumentelor de scriptare - Solutia ofera 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 efeculare a scanării manuale; - Solutia ofera funcțional de scanare a aplicatiilor in cloud; - Solutia ofera funcțional de Scanare a semnăturilor; - Solutia ofera posibilitatea de a expedia invitatii pentru instalarea agentului de securitate minim in limba romana , rusa , engleza si cu posibilitatea de a importa mai multe cutii postale printr-un fisier de tip CSV. Vizualizarea invitatiiilor expediate/expirate si posibilitatea de a reaminti utilizatorul printr-un email de a instala solutia de protectie. - solutia ofera posibilitatea de a importa/exporta politica de securitate si blocarea modificarilor in politica. - Solutia ofera posibilitatea de a seta scanarea programata (zilnic , saptaminal , lunar) - Solutia ofera posibilitatea de a scana fisierele de tip ZIP , RAR... - Solutia ofera posibilitatea de a scana fisierele de tip mailbox PST , OST... - Solutia permite activarea/dezactivarea modulelor de securitate, bazata de locatia identificata a dispozitivului dupa urmatoarele criterii: DNS server ip address , DHCP server ip address , default gateway ip address, wins ip address. - Solutia ofera procese automatizate precum: scanare rapidă pentru malware , scanare programată pentru malware , restart forțat , oprire forțată , hibernare , instalarea
--	--	---	---

		de securitate critică și importantă , instalarea tuturor actualizărilor. - Solutia trebuie să includă funcțional de control a dispozitivelor externe, să ofere posibilitatea: de a seta restricții în privința modului în care utilizatorii pot accesa următoarele dispozitive: USB Mass Storage Devices , Bluetooth Devices , IrDA Devices , IEEE 1394 Host Bus Controllers , Imaging Devices (cameras and scanners) , Smart Card Readers , COM & LPT ports , Modems , Floppy drives , Windows CE ActiveSync devices , DVD/CD-ROM drives , Wireless devices , Imprimante; de a interzice 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; - Solutia 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 în baza de semnătura sau comportament; - Solutia 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	actualizărilor de securitate critică și importantă , instalarea tuturor actualizărilor. - Solutia include funcțional de control a dispozitivelor externe, să ofere posibilitatea: de a seta restricții în privința modului în care utilizatorii pot accesa următoarele dispozitive: USB Mass Storage Devices , Bluetooth Devices , IrDA Devices , IEEE 1394 Host Bus Controllers , Imaging Devices (cameras and scanners) , Smart Card Readers , COM & LPT ports , Modems , Floppy drives , Windows CE ActiveSync devices , DVD/CD-ROM drives , Wireless devices , Imprimante; de a interzice 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; - Solutia ofera funcțional de analiză euristică si zero day, de comportament și reputație; - soluția ofera funcțional de Sandbox automatizat inclus – pentru analiza amănunțită prin detonarea fișierilor malițioase sau care nu pot fi protejate în baza de semnătura sau comportament; - Solutia ofera 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
--	--	---	---

		certificat la destinație, etc), condiție și valoare, ce vor asigura activarea regulilor de excludere; - Solutia trebuie să ofere funcțional de Management API prin integrarea soluțiilor terțe precum: SIEM/RMM; - Solutia trebuie să ofere posibilitatea de dezinstalare a agentului de securitate de la distanță; - Solutia trebuie să ofere posibilitatea de a transmite un mesaj informativ pe stațiile distanțe; - Solutia trebuie să ofere posibilitatea de izolare a stațiilor de la distanță; - Solutia trebuie să ofere posibilitatea de a șterge din carantina fișierelor malicioase identificate, restabilirea fișierelor malicioase la locația originală, excluderea fișierului după calea deplină, excluderea fișierului după SHA1; - Solutia trebuie să ofere posibilitatea de a descărca evenimentele de securitate în format (JSON); 1.2. Cerințele tehnice vis-a-vis de administrarea soluției antivirus: - administrarea soluției oferite este necesară să se facă printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite creva echipamente 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 funcționalitățile sus solicitate; - posibilitatea administrării centralizate, prin intermediul unei singure console, a următoarelor medii și funcționalități: stații de lucru fizice și virtualizate, servere fizice și virtualizate, dispozitivelor mobile pe Android și iOS, iPadOS, căsuțelor poștale pe Exchange sau office 365, scanarea vulnerabilităților web și a infrastructurii IT (interne și externe), scanarea dispozitivelor la anomalii, investigarea lor în detaliu și stoparea scurgerilor de date;	pentru certificat la destinație, etc), condiție și valoare, ce vor asigura activarea regulilor de excludere; - Solutia oferă funcțional de Management API prin integrarea soluțiilor terțe precum: SIEM/RMM; - Solutia oferă posibilitatea de dezinstalare a agentului de securitate de la distanță; - Solutia oferă posibilitatea de a transmite un mesaj informativ pe stațiile distanțe; - Solutia oferă posibilitatea de izolare a stațiilor de la distanță; - Solutia oferă posibilitatea de a șterge din carantina fișierelor malicioase identificate, restabilirea fișierelor malicioase la locația originală, excluderea fișierului după calea deplină, excluderea fișierului după SHA1; - Solutia oferă posibilitatea de a descărca evenimentele de securitate în format (JSON); 1.2. Cerințele tehnice vis-a-vis de administrarea soluției antivirus: - administrarea soluției oferite se face printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite creva echipamente hardware (servere de management) sau careva software special. - consola de administrare este capabilă de a funcționa pe orice dispozitiv și conține toate funcționalitățile sus solicitate; - oferă posibilitatea administrării centralizate, prin intermediul unei singure console, a următoarelor medii și funcționalități: stații de lucru fizice și virtualizate, servere fizice și virtualizate, dispozitivelor mobile pe Android și iOS, iPadOS, căsuțelor poștale pe Exchange sau office 365, scanarea vulnerabilităților web și a infrastructurii IT (interne și externe), scanarea dispozitivelor la anomalii, investigarea lor în detaliu și stoparea scurgerilor de date;
--	--	--	---

	- să suporte următoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; - interfața consolei a clientului 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; 1.3. Cerințe vis-a-vis de funcționalul de raportare și alerte a soluției antivirus: - Soluția trebuie să permită generarea de rapoarte grafice detaliate, săptămînal 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: • 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 si ulterior expediata catre o cutie postala sau mai multe. - Soluția, prin intermediul direct al experților producătorului, trebuie să ofere consultanță și expertiză în materie de securitate cibernetică și să fie disponibili ca serviciu prin intermediul funcției de produs încorporat în consolă sub SLA cu un minim de 2 ore și acces la ei 24/7/365.	- suportă următoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; - interfața consolei a clientului trebuie asigură posibilitatea de funcționare în limbile: romana, rusă si engleză, cu capacitatea de a putea fi selectată limba dorită, în scopul unei administrări mai ușoare de către administratori; - administratorul poate permite sau interzice utilizatorului de a activa sau dezactiva caracteristicile de securitate setate; 1.3. Funcționalul de raportare și alerte a soluției antivirus oferate: - Soluția permite generarea de rapoarte grafice detaliate, săptămînal 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: • 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 permite 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 si ulterior expediata catre o cutie postala sau mai multe. - Soluția, prin intermediul direct al experților producătorului, ofera consultanță și expertiză în materie de securitate cibernetică și este disponibil ca serviciu prin intermediul funcției de produs încorporat în consolă sub SLA cu un minim de 2 ore și acces la ei 24/7/365.
--	---	---

	- Soluția va oferi un serviciu avansat de căutare și răspuns la amenințări prin intermediul consolei, accesând inclusiv la direct suportul producătorului. 1.4. Cerințele tehnice functionale minim solicitate fata de solutia de scanare a vulnerabilitatilor a infrastructurii interne, externe si web: - Produsul oferit va trebui să poată fi extins prin achiziția ulterioară a unei soluții de antivirus, de la același producător pentru a exista o integrare nativă a soluției. Cu posibilitatea de a accesa dintr-o singură interfață fie soluția de antivirus fie soluția de scanare a vulnerabilităților. - Platforma trebuie să fie capabilă să identifice atât amenințările interne cât și pe cele externe și să raporteze riscurile si reglementările conform minim PCI, GDPR. - Soluția trebuie să asigure scanarea vulnerabilităților pentru echipamente din rețea, aplicațiilor web, site-urilor interne sau externe. - Soluția oferită trebuie să fie una bazată pe tehnologia Cloud, care să ofere o vizibilitate a vulnerabilităților într-un mod centralizat pentru toate tipurile de dispozitive conectate în rețea și care pot comunica, de exemplu: stații de lucru, servere, servere virtuale, site-uri, switch-uri, routere, aplicațiilor web, etc; - Soluția va oferi posibilitatea de a identifica toate echipamentele conectate la rețea, la fel va fi posibil de a verifica tipul de echipament, după caz: sistemul de operare instalat, IP-ul și MAC adresa, a cărui domeniu se atribuie, vulnerabilitățile depistate, software-ul instalat pe echipament, spațiu disponibil, tipul procesor, tip de Bios. - Soluția va permite planificarea activităților după data/ora/an și de rulat scanarea vulnerabilităților pentru fiecare echipament in parte.	- Soluția ofera un serviciu avansat de căutare și răspuns la amenințări prin intermediul consolei, accesând inclusiv la direct suportul producătorului. 1.4 Specificații tehnice functionale oferitate fata de solutia de scanare a vulnerabilitatilor a infrastructurii interne, externe si web pentru (WithSecure Elements Vulnerability Management): - Produsul propus va putea fi extins prin achizitia ulterioara si este de la același producător și exista o integrare nativă cu soluția Antivirus oferită mai sus. Cu posibilitatea de a fi accesată dintr-o singură interfață fie soluția de antivirus fie soluția de scanare a vulnerabilităților. Se licențiază per Ip/Host, la achizitionarea ulterioara va apărea in consola si acest acest functional solicitat. - Platforma este capabilă să identifice atât amenințările interne cât și pe cele externe și să raporteze riscurile si reglementările conform minim PCI, GDPR. - Soluția asigura scanarea vulnerabilităților pentru echipamente din rețea, aplicațiilor web, site-urilor interne sau externe. - Soluția oferită este una bazată pe tehnologia Cloud, care ofera o vizibilitate a vulnerabilităților într-un mod centralizat pentru toate tipurile de dispozitive conectate în rețea și care pot comunica, de exemplu: stații de lucru, servere, servere virtuale, site-uri, switch-uri, routere, aplicațiilor web, etc; - Soluția ofera posibilitatea de a identifica toate echipamentele conectate la rețea, la fel va fi posibil de a verifica tipul de echipament, după caz: sistemul de operare instalat, IP-ul și MAC adresa, a cărui domeniu se atribuie, vulnerabilitățile depistate, software-ul instalat pe echipament, spațiu disponibil, tipul procesor, tip de Bios. - Soluția permite planificarea activităților după data/ora/an și de rulat scanarea vulnerabilităților pentru fiecare echipament in parte.
--	---	---

	- Soluția va pune la dispoziție un instrument care poate fi instalat pe o mașină virtuală sau pe un calculator în rețeaua pe care se dorește o scanare al vulnerabilităților sau pentru colectarea datelor echipamentelor aflate în rețea. - Soluția trebuie să permită adăugarea unui grup de scanare în care se va indica minim: Numele grupului și persoana responsabilă, descrierea succintă a grupului. - Posibilitatea de scanare prin alegerea unui șablon prestabilit care va propune de a scana sistemul după minim următoarele modele: • TCP 0-65535 , UDP 0-1024 • Badlock detection • Bash Shellshock detection • GHOST detection • Hearbeat detection • Limited TCP 0-30000, no UDP • PCI scan • Scan full TCP/UDP port range • Scan top-100 ports • Scan top-1000 ports • SSL/TLS maturity scanning - Modul de scanare să poată fi setat după: oră, repetări zilnice, săptămânale, lunare, trimestriale, etc. - Soluția trebuie să ofere funcțional de Management API prin integrarea soluțiilor terțe; - Soluția trebuie să ofere posibilitatea de setare a unui logo care trebuie să se afișeze în consola de administrare și în rapoartele de vulnerabilități exportate. - Soluția va dispune de posibilitatea de autentificare prin doi factori cu ajutorul unor soluții bazate pe TOTP (Time-based One Time Password) ca: • Google Authenticator, • Microsoft Authenticator, • Sau altele care suportă acest algoritm.	- Soluția pune la dispoziție un instrument care poate fi instalat pe o mașină virtuală sau pe un calculator în rețeaua pe care se dorește o scanare al vulnerabilităților sau pentru colectarea datelor echipamentelor aflate în rețea. - Soluția permite adăugarea unui grup de scanare în care se va indica minim: Numele grupului și persoana responsabilă, descrierea succintă a grupului. - Oferă posibilitatea de scanare prin alegerea unui șablon prestabilit care va propune de a scana sistemul după minim următoarele modele: • TCP 0-65535 , UDP 0-1024 • Badlock detection • Bash Shellshock detection • GHOST detection • Hearbeat detection • Limited TCP 0-30000, no UDP • PCI scan • Scan full TCP/UDP port range • Scan top-100 ports • Scan top-1000 ports • SSL/TLS maturity scanning - Modul de scanare va putea fi setat după: oră, repetări zilnice, săptămânale, lunare, trimestriale, etc. - Soluția oferă funcțional de Management API prin integrarea soluțiilor terțe; - Soluția oferă posibilitatea de setare a unui logo care se va afișa în consola de administrare și în rapoartele de vulnerabilități exportate. - Soluția dispune de posibilitatea de autentificare prin doi factori cu ajutorul unor soluții bazate pe TOTP (Time-based One Time Password) ca: • Google Authenticator, • Microsoft Authenticator, • Sau altele care suportă acest algoritm.
--	--	---

	- Administrarea soluției este necesară să se facă printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite careva echipamente hardware (servere de management) sau careva software speciale. - Soluția propusă trebuie să poată genera un raport pe segmente din rețea pe care se dorește. Și va fi posibil de a selecta ce fel de vulnerabilități să fie afișate în raport, sortate după severitatea lor. - Soluția propusă trebuie să pună la dispoziție posibilitatea de a asigura remedierea unei vulnerabilități către un user / administrator creat în platforma de administrare. - Asignarea unui task va fi posibil prin crearea unui ticket astfel se va indica unele date ca : denumire task, descrierea succintă, perioada până când să fie executat, prioritatea, o perioadă estimată pentru remediere, etc. - Soluția trebuie să dispună de capacitatea de a automatiza unele procese de lucru ca: - Închiderea și redeschiderea automată a tichetelor; - Să transmită notificări tuturor participanților la expirarea taskului; - Până la expirarea termenului limită pentru executarea taskului, soluția va notifica toți participanții. - Consola de administrare trebuie să suporte următoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; - Interfața consolei de administrare trebuie să asigure posibilitatea de funcționare cel puțin în limba engleză obligatoriu. - Soluția va permite accesul altor useri cu drepturi de: administrator, doar vizualizare sau colegi de echipă. - Soluția va putea afișa toată informația referitor la licența instalată, jurnal de evenimente, modificările aplicate de către user-ul care are accesul la portal. - În consola de administrare trebuie să se regăsească acces la manuale, ghiduri de instalare, ghidul de utilizare, etc, informații referitor la schimbările și actualizările soluției, comunitate, portal pentru suport cu posibilitatea de a solicita ajutor de la producător.	- Soluția se administrează printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite careva echipamente hardware (servere de management) sau careva software speciale. - Soluția propusă poate genera un raport pe segmente din rețea pe care se dorește. Și va fi posibil de a selecta ce fel de vulnerabilități să fie afișate în raport, sortate după severitatea lor. - Soluția propusă pune la dispoziție posibilitatea de a asigura remedierea unei vulnerabilități către un user / administrator creat în platforma de administrare. - Asignarea unui task este posibil prin crearea unui ticket astfel se va indica unele date ca : denumire task, descrierea succintă, perioada până când să fie executat, prioritatea, o perioadă estimată pentru remediere, etc. - Soluția dispune de capacitatea de a automatiza unele procese de lucru ca: - Închiderea și redeschiderea automată a tichetelor; - Să transmită notificări tuturor participanților la expirarea taskului; - Până la expirarea termenului limită pentru executarea taskului, soluția va notifica toți participanții. - Consola de administrare suportă următoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; - Interfața consolei de administrare asigură posibilitatea de funcționare în limba engleză. - Soluția permite accesul altor useri cu drepturi de: administrator, doar vizualizare sau colegi de echipă. - Soluția poate afișa toată informația referitor la licența instalată, jurnal de evenimente, modificările aplicate de către user-ul care are accesul la portal. - În consola de administrare se regăsește acces la manuale, ghiduri de instalare, ghidul de utilizare, etc, informații referitor la schimbările și actualizările soluției, comunitate, portal pentru suport cu posibilitatea de a solicita ajutor de la producător.
--	--	---

	- Soluția trebuie să asigure lipsa actualizărilor de software și patch-uri care sunt afișate în consola de administrare cu ID-uri CVE și link către baza de date de vulnerabilitate și expunere comună (CVE) pentru informații suplimentare despre detaliile și criticitatea vulnerabilității - Soluția trebuie să ofere o modalitate de a executa scanări autentificate pe sistemele țintă - Soluția trebuie să ofere scanările de descoperire trebuie să fie nelimitate pe parcursul perioadei de licență. - Soluția trebuie să ofere activarea accesului către date prin configurarea cheilor API - Soluția trebuie să fie personalizabilă pentru scanări, performanță, șabloane și rapoarte. 1.4.1 Cerințe față de funcționalul de raportare și alerte a sistemului de scanare a vulnerabilitatilor: - Soluția trebuie să permită generarea de rapoarte grafice detaliate, cu posibilitate de export minim în format (docx.xml,xlsx), inclusiv cu remitere către adrese de email specificate. Posibilitatea de a configura o frecvență pentru crearea rapoartelor după (zi, săptămâna, luna, ora), rapoartele trebuie să cuprindă minim informație despre: • Vulnerabilitățile descoperite clasificate după severitate: informativ, severitate minimă, severitate medie, și severitate înaltă. • Notarea severității vulnerabilităților se va face pe notă de la 1 la 10 • Raportul va afișa descrierea pentru fiecare vulnerabilitate în parte cu unele referințe. • Recomandările propuse pentru remedierea vulnerabilității depistate.	- Soluția asigură lipsa actualizărilor de software și patch-uri care sunt afișate în consola de administrare cu ID-uri CVE și link către baza de date de vulnerabilitate și expunere comună (CVE) pentru informații suplimentare despre detaliile și criticitatea vulnerabilității - Soluția oferă o modalitate de a executa scanări autentificate pe sistemele țintă - Soluția trebuie să ofere scanările de descoperire trebuie să fie nelimitate pe parcursul perioadei de licență. - Soluția trebuie să ofere activarea accesului către date prin configurarea cheilor API - Soluția este personalizabilă pentru scanări, performanță, șabloane și rapoarte. 1.4.1 Specificații oferite față de funcționalul de raportare și alerte a sistemului de scanare a vulnerabilitatilor: - Soluția permite generarea de rapoarte grafice detaliate, cu posibilitate de export minim în format (docx.xml,xlsx), inclusiv cu remitere către adrese de email specificate. Posibilitatea de a configura o frecvență pentru crearea rapoartelor după (zi, săptămâna, luna, ora), rapoartele trebuie să cuprindă minim informație despre: • Vulnerabilitățile descoperite clasificate după severitate: informativ, severitate minimă, severitate medie, și severitate înaltă. • Notarea severității vulnerabilităților se va face pe notă de la 1 la 10 • Raportul va afișa descrierea pentru fiecare vulnerabilitate în parte cu unele referințe. • Recomandările propuse pentru remedierea vulnerabilității depistate.
--	---	---

	• Crearea unei statistici grafice în dependență de vulnerabilitățile depistate • Top vulnerabilități depistate. - Soluția trebuie să permită crearea unor widgeturi care pot fi editate, clonate sau șterse cu afișarea lor pe pagină în mod dinamic. La fel, widgeturi de bord pot fi create în forma de minimă de: tabel, plăcinta, histograma, etc. - Tablourile de bord trebuie să conțină informații ca: vulnerabilitățile depistate care vor fi grupate după severitate/data/luna/cantitatea depistată. Cele mai grave vulnerabilități. Scanările active, scanările care sunt planificate, ultimele dispozitive scanate. - Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru minim următoarele acțiuni: când începe un proces de scanare, finalizarea procesului de scanare, la crearea și asignarea unui task către un utilizator existent. Alte cerințe obligatorii: 1. Pentru soluția oferită se solicită a fi 36 luni suport local și de la producător. 2. Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului. Necesare de prezentat timpii de reacție oferită. 3. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comercială. 4. Prezentarea a minim 2 certificate tehnice pe soluțiile propuse. 5. Ofertantul va prezenta copia Certificatului ISO 27001:2013 și Certificatului ISO 9001:2015 - confirmat cu aplicarea semnăturii electronice;	• Crearea unei statistici grafice în dependență de vulnerabilitățile depistate • Top vulnerabilități depistate. - Soluția permite crearea unor widgeturi care pot fi editate, clonate sau șterse cu afișarea lor pe pagină în mod dinamic. La fel, widgeturi de bord pot fi create în forma de minimă de: tabel, plăcinta, histograma, etc. - Tablourile de bord conțin informații ca: vulnerabilitățile depistate care vor fi grupate după severitate/data/luna/cantitatea depistată. Cele mai grave vulnerabilități. Scanările active, scanările care sunt planificate, ultimele dispozitive scanate. - Soluția permite setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru minim următoarele acțiuni: când începe un proces de scanare, finalizarea procesului de scanare, la crearea și asignarea unui task către un utilizator existent. Alte cerințe obligatorii: 1. Pentru soluția oferită se oferă 36 luni suport local și de la producător. 2. Producătorul oferă suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului. Timpii de reacție menționați în documentul XONTECH SYSTEMS Service Centru anexat cu oferta. 3. Lucrările de instalare, configurare, punerea în funcțiune a soluției vor fi executate de Xontech Systems, iar costul acestora sunt incluse în oferta comercială. 4. Atasat cu oferta sunt certificatele tehnice pe soluțiile propuse. 5. Atasat cu oferta sunt anexate copia Certificatului ISO 27001:2013 și Certificatului ISO 9001:2015 - confirmat cu aplicarea semnăturii electronice;
--	---	---

		6. Ofertantul va prezenta Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul oferat. 7. Ofertantul va prezenta Autorizarea de la producător pentru licitatie la care participa ofertantul. 8. Ofertantul va prezenta minim 3 referințe și 3 recomandări de implementare pe piața locală a soluției oferate.	6. Atasat cu oferta este Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul oferat. 7. Atasat cu oferta este Autorizarea de la producător pentru licitatie la care participam. 8. La solicitare se va prezenta 3 referințe și 3 recomandări de implementare pe piața locală a soluției oferate.
--	--	---	---