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,]

Numărul procedurii de achiziţie:	**ocds-b3wdp1-MD-1646123927520 din 01.03.2022**
Denumirea procedurii de achiziţie:	**Licență Antivirus pentru anul 2022**

Denumirea bunurilor/serviciilor	**Denumirea modelului bunului/serviciului**	**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
Bunuri/servicii						
Lotul 1: Antivirus						
Antivirus	**F-Secure Elements EPP for Computers Premium, Company Managed for 1 year Governmental**	**Finlanda**	**F-Secure**	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.
Data:

Digitally signed by Vicol Irina
Date: 2022.03.04 11:21:03 EET
Reason: MoldSign Signature
Location: Moldova

Anexa

Matricea de conformitate conform caietului de sarcini 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.	Antivirus	**Specificații tehnice** Software antivirus pentru protecția stațiilor de lucru (PC, NoteBook, tabletă) împotriva virușilor, troienilor, spyware, rootkit-uri, adware și amenințări necunoscute. **Suggested solution must support below operating systems:** • Windows Desktop OS: 7, 8, 8.1, 10, 11. • Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022. • macOS 10.14 – 12 **Suggested solution must support the following virtual infrastructure:** • VMware ESXi 6.5 hypervisor, …, VMware ESXi 7.0 hypervisor (with the latest updates). • Windows Server 2008 R2 SP1, …, Windows Server 2019 (in full mode or in Server Core mode). **Functional requirements (Endpoint)**	**F-Secure Elements EPP for Computers Premium, Company Managed for 1 year** **Specificații tehnice ofertate** Software antivirus pentru protecția stațiilor de lucru (PC, NoteBook, tabletă) împotriva virușilor, troienilor, spyware, rootkit-uri, adware și amenințări necunoscute. **Solution support below operating systems:** • Windows Desktop OS: 7, 8, 8.1, 10, 11. • Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022. • macOS 10.14 – 12 **Solution support the following virtual infrastructure:** • VMware ESXi 6.5 hypervisor, …, VMware ESXi 7.0 hypervisor (with the latest updates). • Windows Server 2008 R2 SP1, …, Windows Server 2019 (in full mode or in Server Core mode). **Functional requirements (Endpoint)**

		• Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-day vulnerabilities and other malicious and unwanted software. • Suggested solution must provide next gen protection technologies for example, protection against file-less threats, provides multi-layered machine learning to offer protection and behavioral analysis during different stages of kill chain. • Suggested solution must provide Memory Scanning for windows workstations. • Suggested solution must provide ability to switch to a cloud mode for threat protection, while decreasing RAM and Hard disk drives usage for resource-limited machines. • Suggested solution must have dedicated components to monitor, detect and block activities on Windows, Linux and Windows Server and endpoints, to protect against remote encryption attacks. • Suggested solution must provide behavioral analysis based on machine learning. • Suggested solution must provide integration with same vendors Endpoint Detection and Response “EDR”, SandBox, Anti-APT solution, for active hunting for threats, and incident response automation. • Suggested solution must include following components in a single agent installed on the endpoint:	• Support detecting viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-day vulnerabilities and other malicious and unwanted software. • Solution provide next gen protection technologies for example, protection against file-less threats, provides multi-layered machine learning to offer protection and behavioral analysis during different stages of kill chain. • Solution provide Memory Scanning for windows workstations. • Solution provide ability to switch to a cloud mode for threat protection, while decreasing RAM and Hard disk drives usage for resource-limited machines. • Solution provide dedicated components to monitor, detect and block activities on Windows, Linux and Windows Server and endpoints, to protect against remote encryption attacks. • Solution provide behavioral analysis based on machine learning. • Solution provide integration with same vendors Endpoint Detection and Response “EDR”, SandBox, Anti-APT solution, for active hunting for threats, and incident response automation. • Solution include following components in a single agent installed on the endpoint:

		○ Application, Web and Device control ○ Anomaly detection ○ HIPS and Firewall ○ Patch management ○ Encryption • Suggest solution must include Application launch/start control for the windows server operating system. • Suggested solution must provide application and device control for Windows servers and workstations. • Suggested solution should support installation endpoint protection on Servers without restart. • Suggested endpoint solution must allow the following: ○ Manual scanning ○ On access scanning ○ On demand scanning ○ Compressed File Scanning ○ Scan Individual file, Folder and drive ○ Script blocking and scanning ○ Registry guard ○ Buffer Overflow Protection ○ Background/idle scanning ○ Removable drive scanning upon connection with system ○ Ability to detect untrusted hosts and block upon detection of encryption like activities on the server shared resources	○ Application, Web and Device control ○ Anomaly detection ○ HIPS and Firewall ○ Patch management ○ Encryption • Solution include Application launch/start control for the windows server operating system. • Solution provide application and device control for Windows servers and workstations. • Solution provide support installation endpoint protection on Servers without restart. • Solution allow the following: ○ Manual scanning ○ On access scanning ○ On demand scanning ○ Compressed File Scanning ○ Scan Individual file, Folder and drive ○ Script blocking and scanning ○ Registry guard ○ Buffer Overflow Protection ○ Background/idle scanning ○ Removable drive scanning upon connection with system ○ Ability to detect untrusted hosts and block upon detection of encryption like activities on the server shared resources

		• Suggested endpoint solution should be protected with a password to prevent stopping/killing the AV process and for self-protection regardless of user authorization level on the system. • Suggested solution must have local and global reputation. • Suggested solution that can decrypt and scan network traffic transmitted over encrypted connections support following protocols: SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3. Scans both HTTPS, HTTP and FTP traffic against viruses and spyware or any other malware. • Suggested solution must prevent connection of reprogrammed USB devices that emulate keyboards and also allows to control the use of on-screen keyboard for authorization. • Solution must be able to block network attacks and report source of infection. • Suggested solution must have local storage on endpoints to keep copies of files that have been deleted or modified during disinfection, those files must be stored in a special format that do not impose any threat. • Suggest solution must allow administrator to exclude specified files / folders / Application / By Digital Certificate from being scanned either in the on-access scan (real-time protection) or during on-demand scans.	• Solution provide a protected with a password to prevent stopping/killing the AV process and for self-protection regardless of user authorization level on the system. • Solution provide local and global reputation. • Solution can decrypt and scan network traffic transmitted over encrypted connections support following protocols: SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3. Scans both HTTPS, HTTP and FTP traffic against viruses and spyware or any other malware. • Solution prevent connection of reprogrammed USB devices that emulate keyboards and also allows to control the use of on-screen keyboard for authorization. • Solution are able to block network attacks and report source of infection. • Solution provide local storage on endpoints to keep copies of files that have been deleted or modified during disinfection, those files must be stored in a special format that do not impose any threat. • Solution allow administrator to exclude specified files / folders / Application / By Digital Certificate from being scanned either in the on-access scan (real-time protection) or during on-demand scans.

		• Automatically scans removable drives for malware upon insertion to any endpoint. Scan should be controlled based on drive size. • Suggested solution must be able to block the usage of USB storage devices or only allow access to allowed devices and allow read/write access by domain users to reduce data theft and enforce lock policies. • Suggested solution must be able to differentiate among USB storage devices, printers, mobiles and other peripherals. • Suggested solution must be able to log the file operations (Write and delete) on USB storage devices. Stated functionality does not require any additional license or component to installed on the endpoint. • Suggested solution must have Ability to block/allow user access to web resources based on websites, content type, special detected category, user and time of day. • Suggested solution should allow blocking following devices: Bluetooth, Mobile devices, External modems, CD/DVDs, Transferring data to mobile device, Camera and Scanners, MTP. • Suggest solution must allow administrator to enlist and monitor the application that use custom/random ports when launched. • Suggested solution must support blocking forbidden applications from being launched on endpoints. Also, it	• Automatically scans removable drives for malware upon insertion to any endpoint. • Solution are able to block the usage of USB storage devices or only allow access to allowed devices and allow read/write access by domain users to reduce data theft and enforce lock policies. • Solution are able to differentiate among USB storage devices, printers, mobiles and other peripherals. • Solution are able to log the file operations (Write and delete) on USB storage devices. Stated functionality does not require any additional license or component to installed on the endpoint. • Solution provide ability to block/allow user access to web resources based on websites, content type, special detected category. • Solution allow blocking following devices: Bluetooth, Mobile devices, External modems, CD/DVDs, Transferring data to mobile device, Camera and Scanners, MTP, Printers, IEEE 1394 Host Bus Controllers, IrDA Devices, Floppy drives, Wireless devices, COM & LPT ports. • Solution allow administrator to enlist and monitor the application when launched. • Solution support blocking forbidden applications from being launched on endpoints. Also, it support blocking all applications except allowed ones.

		must support blocking all applications except allowed ones. • Suggested solution must have cloud-integrated application control component to get latest updates on applications' rating and categories. • Suggested solution must have ability to allow application based on the digital signature certificate, MD5, SHA256, META Data, File Path, Pre-defined security categories. • Suggested solution must support control of scripts from PowerShell. • Suggested solution must have ability that restrict application activities within the system according to the trust level assigned to the application and limits the rights of applications to access certain resources, including system and user files "HIPS functionality". • Suggested solution must have endpoint mail threat protection with: o Attachment filter and ability to rename attachments o Scan of mail messages when receiving, reading and sending • Protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type, including wireless networks.	• Solution have cloud-integrated application control component to get latest updates on applications' rating and categories. • Solution have ability to allow application based on the digital signature certificate, MD5, SHA256, META Data, File Path, Pre-defined security categories. • Solution support control of scripts from PowerShell. • Solution have ability that restrict application activities within the system according to the trust level assigned to the application and limits the rights of applications to access certain resources, including system and user files "HIPS functionality". • Solution have endpoint mail threat protection with: o Attachment filter and ability to rename attachments o Scan of mail messages when receiving, reading and sending • Protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type, including wireless networks.

		• Availability of multiple ways to notify administrator about important events that have taken place (mail notification, audible announcement, pop-up window, log entry). • Suggested solution must allow the administrator to create a single installer with required configuration to non-IT literate users. **Cerințe tehnice specifice** **Browsere acceptate** ***Browsere care acceptă funcționalitatea completă a programului:*** • Microsoft Internet Explorer versiunile 8.0, 9.0, 10.0, 11.0 și ulterioare*. o Internet Explorer 8.0 - 11.0 în stilul noii interfețe Windows nu este acceptat. Windows 10 nu acceptă instalarea automată a extensiilor de browser. • Microsoft Edge (suportul este limitat). • Mozilla Firefox versiunile 52.x–65.x și versiuni ulterioare*. • Mozilla Firefox ESR 52.x-65.x și o versiune ulterioară*. • Google Chrome versiunile 48.x-68.x și versiuni ulterioare*. • Yandex.Browser 18.3.1–19.0.3 și versiuni ulterioare* (limitat). ***Browsere care acceptă instalarea antivirusului:*** • Microsoft Internet Explorer versiunile 8.0, 9.0, 10.0, 11.0 și ulterioare*. • Internet Explorer 8.0-11.0 cu noul stil de interfață Windows nu este acceptat.	• Availability of multiple ways to notify administrator about important events that have taken place (mail notification, audible announcement, pop-up window, log entry). • Solution allow the administrator to create a single installer with required configuration to non-IT literate users. **Cerințe tehnice specifice ofertate** **Browsere acceptate** ***Browsere care acceptă funcționalitatea completă a programului:*** • Microsoft Edge • Mozilla Firefox • Google Chrome ***Browsere care acceptă instalarea antivirusului:*** • Microsoft Edge • Mozilla Firefox • Google Chrome

		• Mozilla Firefox versiunile 52.x–65.x și versiuni ulterioare*. • Mozilla Firefox ESR 52.x-60.x și o versiune ulterioară*. • Google Chrome versiunile 48.x–72.x și versiuni ulterioare*.	
		Browsere care acceptă tastatura pe ecran și Verificarea conexiunii securizate: • Microsoft Internet Explorer 8.0, 9.0, 10.0, 11.0 și versiuni ulterioare, dar lucrul cu versiuni mai noi de browser este posibil, dar nu este pe deplin garantat. • Internet Explorer 8.0-11.0 cu noul stil de interfață Windows nu este acceptat. • Microsoft Edge (suportul este limitat). • Mozilla Firefox versiunile 52.x–65.x și versiuni ulterioare. • Mozilla Firefox ESR 52.x-60.5 și versiuni ulterioare. • Google Chrome 48.x–68.x și versiuni ulterioare.	***Browsere care acceptă tastatura pe ecran și Verificarea conexiunii securizate:*** • Microsoft Edge • Mozilla Firefox • Google Chrome
		Versiuni acceptate de Microsoft Office Outlook Componenta Mail Anti-Virus este compatibilă cu: • Microsoft Office Outlook 2003. • Microsoft Office Outlook 2007. • Microsoft Office Outlook 2010. • Microsoft Office Outlook 2013. • Microsoft Office Outlook 2016. • Microsoft Office Outlook 2019.	**Versiuni acceptate de Microsoft Office Outlook Componenta Mail Anti-Virus este compatibilă cu:** • Microsoft Office Outlook 2003. • Microsoft Office Outlook 2007. • Microsoft Office Outlook 2010. • Microsoft Office Outlook 2013. • Microsoft Office Outlook 2016. • Microsoft Office Outlook 2019.
		Cerințe pentru Computer • Procesor 1 GHz sau mai mare • 1 GB RAM (32 biți) sau • 2 GB RAM (64 biți)	**Cerințe pentru Computer** • Procesor 1 GHz sau mai mare • 1 GB RAM (32 biți) sau • 2 GB RAM (64 biți)

		• Conexiune la internet pentru activarea și actualizarea bazelor de date antivirus	• Conexiune la internet pentru activarea și actualizarea bazelor de date antivirus
		Cerințe pentru Computer Mac • Mac OS X 10.5, 10.6 sau 10.7 • 512 MB RAM • 270 MB de spațiu liber pe hard disk (în funcție de dimensiunea bazelor de date antivirus) • Conexiune la internet pentru activarea și actualizarea bazelor de date antivirus	**Cerințe pentru Computer Mac** • Mac OS X 10.5, 10.6 sau 10.7 • 512 MB RAM • 270 MB de spațiu liber pe hard disk (în funcție de dimensiunea bazelor de date antivirus) • Conexiune la internet pentru activarea și actualizarea bazelor de date antivirus
		Cerințe pentru tablete • Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10. • Procesor Intel Celeron 1,66 GHz sau mai mare. • 1024 MB de memorie RAM liberă. • Conexiune la internet pentru activarea și actualizarea bazelor de date antivirus	**Cerințe pentru tablete** • Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10. • Procesor Intel Celeron 1,66 GHz sau mai mare. • 1024 MB de memorie RAM liberă. • Conexiune la internet pentru activarea și actualizarea bazelor de date antivirus
		Cerințe hardware pentru laptopuri • Procesor: Intel Atom 1,6 GHz • 1024 MB de memorie RAM liberă. • Ecran de min. 10,1 inchi cu o rezoluție de 1024x600 sau mai mare. • Conexiune la internet pentru activarea și actualizarea bazelor de date antivirus	**Cerințe hardware pentru laptopuri** • Procesor: Intel Atom 1,6 GHz • 1024 MB de memorie RAM liberă. • Ecran de min. 10,1 inch cu o rezoluție de 1024x600 sau mai mare. • Conexiune la internet pentru activarea și actualizarea bazelor de date antivirus