Anexa nr.1

Specifiția tehnică pentru software antivirus.

№	Requirement	Compliance (Yes/No)	Comment
System requirements			
1.	**The proposed solution must support the operating systems below:** • Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later • Windows 8 Professional / Enterprise • Windows 8.1 Professional / Enterprise • Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise • Windows 11 **Servers** • Windows Small Business Server 2011 Essentials / Standard (64-bit) • Windows MultiPoint Server 2011 (64-bit) • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later • Windows Server 2012 Foundation / Essentials / Standard / Datacenter • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter • Windows Server 2016 Essentials / Standard / Datacenter • Windows Server 2019 Essentials / Standard / Datacenter • Windows Server 2022 **Microsoft Terminal Servers** • Microsoft Remote Desktop Services based on Windows Server 2008 R2 SP1 • Microsoft Remote Desktop Services based on Windows Server 2012 • Microsoft Remote Desktop Services based on Windows Server 2012 R2 • Microsoft Remote Desktop Services based on Windows Server 2016 • Microsoft Remote Desktop Services based on Windows Server 2019 **32-bit Linux operating systems:** • CentOS 6.7 and later • Debian GNU / Linux 9.4 and later • Debian GNU / Linux 10.1 and later • Linux Mint 19 and later • Mageia 4 • Red Hat Enterprise Linux 6.7 and later • ALT Education 9 • ALT Workstation 9 • ALT Server 9 **64-bit Linux operating systems:** • AlterOS 7.5 and later • Amazon Linux 2 • Astra Linux Common Edition (operational update 2.12). • Astra Linux Special Edition RUSB.10015-01 (operational update 1.5) • Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) • Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6) • CentOS 6.7 and later • CentOS 7.2 and later • CentOS 8.0 and later • Debian GNU / Linux 9.4 and later • Debian GNU / Linux 10.1 and later • EulerOS V2.0SP2 2.2.17		

	• EulerOS V2.0SP5 2.5.6 • Linux Mint 19 and later • Linux Mint 20.1 and later • openSUSE Leap 15.0 and later • Oracle Linux 7.3 and later • Oracle Linux 8.0 and later • Pardus OS 19.1 • Red Hat Enterprise Linux 6.7 and later • Red Hat Enterprise Linux 7.2 and later • Red Hat Enterprise Linux 8.0 and later • SUSE Linux Enterprise Server 12 SP5 and later • SUSE Linux Enterprise Server 15 and later • Ubuntu 18.04 LTS and later • Ubuntu 20.04 LTS • ALT Education 9 • ALT Workstation 9 • ALT Server 9 • GosLinux 7.2 • Red OS 7.3 **MAC OS operating systems:** • macOS 10.14 – 12		
2.	The proposed solution must support the following virtual platforms: • VMware Workstation 16.1.1 Pro • VMware ESXi 7.0 Update 2a • Microsoft Hyper-V Server 2019 • Citrix Virtual Apps and Desktops 7 2103 • Citrix Provisioning 2012 • Citrix Hypervisor 8.2 LTSR		
3.	The proposed solution must support protection of the latest Operating Systems versions across all platforms (Windows, Linux, MacOS, iOS, Android).		
Functional requirements			
2.1	**Functional requirements: Antivirus**		
	The proposed solution must be able to detect following types of threat: • 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.		
	The proposed solution must support Anti-malware Scan Interface (AMSI).		
	The proposed solution must have the ability to integrate with Windows Defender Security Center.		
	The proposed solution must support Windows Linux subsystem.		
	The proposed solution must provide next gen protection technologies. For example: • protection against file-less threats • provision of multi-layered Machine Learning (ML) based protection and behavioral analysis during different stages of the kill-chain		
	The proposed solution must provide Memory Scanning for Windows workstations.		
	The proposed solution must provide Kernel Memory Scanning for Linux workstations.		
	The proposed solution must provide the ability to switch to cloud mode for threat protection, decreasing RAM and hard disk drive usage for resource-limited machines.		
	The proposed solution must have dedicated components to monitor, detect and block activities on Windows, Linux and Windows servers, and endpoints, to protect against remote encryption attacks.		
	The proposed solution must include signatureless components to detect threats even without frequent updates. Protection must be powered by Static ML for pre-execution and Dynamic ML for post-execution stages of the kill-chain on endpoints and in the cloud for Windows servers and workstations.		
	The proposed solution must provide behavioral analysis based on ML.		

	The proposed solution must provide the ability to integrate with the vendor's own Endpoint Detection and Response (EDR) and Anti-APT solutions, for active threat hunting and automated incident response.		
	The proposed solution must support integration with a standalone/independent automated threat detection and prevention sandbox solution that does not depend on the vendor's EDR and /or Anti-APT solution.		
	The proposed solution must include the ability to configure and manage firewall settings built into the Windows Server and Linux operating systems, through its management console.		
	The proposed solution must provide Application and Device Controls for Windows workstations.		
	The proposed solution's protection for servers and workstations must include a dedicated component for protection against ransomware/cryptor virus activity on shared resources.		
	The proposed solution must, on detecting ransomware/cryptor-like activity, automatically block the attacking computer for a specified interval and list information about the attacking computer IP and timestamp, and the threat type.		
	The proposed solution must provide a pre-defined list of scan exclusions for Microsoft applications and services.		
	The proposed solution should support the installation of endpoint protection on servers without the need to restart.		
	The proposed solution must enable the following for endpoints: • 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 on connection with system • The ability to detect and block untrusted hosts on detection of encryption-like activities on server shared resources.		
	The proposed solution should be password-protected to prevent the AV process being halted/killed and for self-protection, regardless of the user authorization level on the system.		
	The proposed solution must have both local and global reputation databases.		
	The proposed solution must be able to scan HTTPS, HTTP and FTP traffic against viruses and spyware, or any other malware.		
	The proposed solution must include a personal firewall capable, as an absolute minimum, of: • Blocking network activates of applications based on their categorization. • Blocking/allowing specific packets, protocols, IP addresses, ports and traffic direction. • The automatic and manual addition of network subnets, and modification of network activity permissions.		
	The proposed solution must prevent the connection of reprogrammed USB devices emulating keyboards, and enable control of the use of onscreen keyboards for authorization.		
	The proposed solution must be able to block network attacks and report the source of the infection.		
	The proposed solution must have local storage on endpoints to keep copies of files that have been deleted or modified during disinfection. These files must be stored in a specific format that ensures they cannot pose any threat.		
	The proposed solution must have a proactive approach to preventing malware from exploiting existing vulnerabilities on servers and workstations.		
	The proposed solution must support AM-PPL (Anti-Malware Protected Process Light) technology for protection against malicious actions.		

	The proposed solution must include protection against attacks that exploit vulnerabilities in the ARP protocol in order to spoof the device MAC address.		
	The proposed solution must provide Anti-Bridging functionality for Windows workstations to prevent unauthorized bridges to the internal network that bypass perimeter protection tools. Administrators should be able to ban the establishment of simultaneous wired, Wi-Fi, and modem connections.		
	The proposed solution must include a dedicated component for scanning encrypted connections.		
	The proposed solution must be able to decrypt and scan network traffic transmitted over encrypted connections supported by the following protocols; SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3.		
	The proposed solution must have the ability to automatically exclude web resources when a scan error occurs while performing an encrypted connection scan. This exclusion must be unique to the host and must not be shared with other endpoints.		
	The proposed solution must include functionality to remotely wipe data on the endpoint (for workstations).		
	The proposed solution must have following remote data wipe functionalities: • In silent mode • On hard drives and removable drives • For all user accounts on the computer		
	The proposed solution's remote data wipe functionality must support the following modes: • Immediate data deletion • Postponed data deletion		
	The proposed solution's remote data wipe functionality must support the following data deletion methods: • Delete by using the operating resources - files are deleted but are not sent to the recycle bin • Delete completely, without recovery - making data practically impossible to restore after deletion		
	The proposed solution must include functionality to automatically delete the data if there is no connection to the endpoint management server.		
	The proposed solution must support signature-based detection in addition to cloud-assisted and heuristics.		
	The proposed solution should have the ability to raise an alert on, clean, and delete a detected threat.		
	The proposed solution should have the ability to accelerate scanning tasks, skipping those objects that have not changed since the previous scan.		
	The proposed solution should have the ability to prioritize custom and on-demand scanning tasks for Linux workstations.		
	The proposed solution must allow the administrator to exclude specified files/ folders/applications/digital certificates from being scanned, either on-access (real-time protection) or during on-demand scans.		
	The proposed solution should include the functionality to isolate infected computers.		
	The proposed solution must automatically scan removable drives for malware when they are attached to any endpoint. Scan control should be based on drive size.		
	The proposed solution must be able to block the use of USB storage devices or allow access only to permitted devices, and allow read/write access only by domain users, to reduce data theft and enforce lock policies.		
	The proposed solution must be able to differentiate between USB storage devices, printers, mobiles and other peripherals.		
	The proposed solution must be able to log file operations (Write and Delete) on USB storage devices. This should not require any additional license or component to be installed on the endpoint.		
	The proposed solution must have ability to block the execution of any executable from the USB storage device.		
	The proposed solution must have ability to block/allow user access to web resources based on websites, content type, user and time of day.		
	The proposed solution must have a specific detection category to block website banners.		

	The proposed solution must provide the ability to configure Wi-Fi networks based on Network Name, Authentication Type, Encryption Type, so these can later be used to block or allow the Wi-Fi connections.		
	The proposed solution must support user-based policies for Device, Web and Application Control.		
	The proposed solution should specifically allow the blocking of the following devices: • Bluetooth • Mobile devices • External modems • CD/DVDs • Cameras and Scanners • MTPs • And the transfer of data to mobile devices		
	The proposed solution should feature cloud integration, to provide the fastest possible updates on malware and potential threats.		
	The proposed solution must have ability to manage user access rights for Read and Write operations on CDs/DVDs, removable storage devices and MTP devices.		
	The proposed solution must feature firewall filtering by local address, physical interface, and packet Time-To-Live (TTL).		
	The proposed solution must allow the administrator to monitor the application's use of custom/random ports after it has launched.		
	The proposed solution must support the blocking of prohibited (Deny-List) applications from being launched on the endpoint, and the blocking of all applications other than those included in Allow-Lists.		
	The proposed solution must have a cloud-integrated Application Control component for immediate access to the latest updates on application ratings and categories.		
	The proposed solution must offer protection to files executed in Windows Server containers.		
	The proposed solution must include traffic malware filtering, web link verification and web-resource control based on cloud categories.		
	The proposed solution Web Control/Restriction component must include a Cryptocurrencies and Mining category. It must also include predefined regional legal restrictions to comply with Belgian and Japanese Law.		
	The proposed solution must have the ability to allow applications based on their digital signature certificates, MD5, SHA256, META Data, File Path, and pre-defined security categories.		
	The proposed solution must have controls for the download of DLL and Drivers.		
	The proposed solution must support the control of scripts from PowerShell.		
	The proposed solution must support Test Mode with report generation on the launch of blocked applications.		
	The proposed solution must have the ability to restrict application activities within the system according to the trust level assigned to the application, and to limit the rights of applications to access certain resources, including system and user files "HIPS functionality".		
	The proposed solution must have the ability to control system/user application access to audio and video recording devices.		
	The proposed solution must provide a facility to check applications listed in each cloud-based category.		
	The proposed solution must have ability to integrate with a vendor-specific Advanced Threat Protection system.		
	The proposed solution must have ability to automatically regulate the activity of programs running, including access to the file system and registry as well as interaction with other programs.		
	The proposed solution must have the ability to automatically delete Application Control rules if an application is not launched during a specified interval. The interval must be configurable.		
	The proposed solution must have ability to automatically categorize applications launched prior to endpoint protection installation.		
	The proposed solution must have endpoint mail threat protection with: • Attachment filter and the ability to rename attachments. • Scanning of mail messages when receiving, reading and sending.		

	The proposed solution must have the ability to scan multiple redirects, shortened URLs, hijacked URLs, and time-based delays.		
	The proposed solution must enable the user of the computer to perform a check on a file's reputation from the File Context menu.		
	The proposed solution must include the scanning of all scripts, including those developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.), launched when the user works on the computer, including the internet.		
	The proposed solution must provide protection against as yet unknown malware based of the analysis of their behavior and examination of changes in the system register, together with a strong remediation engine to automatically restore any system changes made by the malware.		
	The proposed solution must provide 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.		
	The proposed solution must include IPv6 protocol support.		
	The proposed solution must offer scanning of critical sections of the computer as a standalone task.		
	The proposed solution must incorporate Application Self-Protection technology: • protecting against unauthorized the remote management of an application service. • protecting access to application parameters by setting a password. • preventing the disabling of protection by malware, criminals or amateur users.		
	The proposed solution must offer the ability to choose which threat protection components to install.		
	The proposed solution must include the antivirus checking and disinfection of files that have been packed using programs like PKLITE, LZEXE, DIET, EXEPACK, etc.		
	The proposed solution must include the anti-malware checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files.		
	The proposed solution must protect against as yet unknown malware belonging to registered families, based on heuristic analysis.		
	The proposed solution must include multiple ways to notify the administrator about important events which have taken place (mail notification, audible announcement, pop-up window, log entry).		
	The proposed solution must allow the administrator to create a single installer with the required configuration, for use by non-IT literate users.		
2.	**Functional requirements: Detection**		
	The suggested solution must supplement verdict information from Endpoint Protection solution with system artefacts about the detection.		
	The suggested solution must support auto generation of threat indicators (IoC) after detection occurs with ability to apply response action.		
	The solution must have the capability to force run IoC scan across all endpoints with installed EP applications.		
	The suggested solution must support IoC scanning run according to a scheduler.		
	The suggested solution must support import of third-party IoC in OpenIoC format for its use in network scanning.		
	The suggested solution must support scanning using auto generated, uploaded or external (third-party) set of IoCs to detect earlier undetected threats.		
	The suggested solution must support exporting of IoC generated by the solution to a file in OpenIoC format.		
	Functional requirements: Visibility		
	The suggested solution must generate detailed alert card related to the detected threat on the endpoints.		
	An alert card must include at least the following information about detected threat: - Threat development chain graph (kill chain). - Information about the device on which the threat is detected (name, IP address, MAC address, user list, operating system).		

	- General information about the detection, including detection mode. - Registry changes associated with the detection. - History of the file presence on the device. Response actions performed by the application.		
	Threat development chain (kill chain) graph must provide visual information about the objects involved in the alert, for example, about key processes on the device, network connections, libraries, registry, etc.		
	An alert card must present detailed view on system artefacts and alert-related data for root cause analysis: - Process spawning - Network connections - Registry changes - Downloading object Dropped objects, etc.		
	Functional requirements: Response		
	The suggested solution must support 'Single-click" response form management console		
	The suggested solution must support at least the following response actions that an administrator can perform when threats are detected:		
	Prevent object execution		
	o EDR solution must support both modes: records to the events about attempts to launch objects or open documents that meet the criteria of the Execution prevention, but *does not block* launch or opening these objects. blocks launch of the objects or opening the documents that meet criteria of the Execution prevention rules.		
	EDR solution must support blocking objects by hash (MD5 or SHA256) or by path pattern.		
	EDR solution must support blocking executables, scripts and documents		
	EDR solution must support notification user about prevention option		
	Host isolation.		
	EDR solution must provide means of isolating machine from the rest of the network in case of security incident, while preserving controlled communication with agents' administration and management server.		
	EDR solution must support creating custom host isolation rules (i.e. adding particular network resources to exclusion e.g. DNS or selecting predefined profiles)		
	EDR solution must support manual bringing host back online from isolation.		
	Delete object from host or group of hosts.		
	Get (download) file from a host or group of hosts.		
	Terminate a process on the device.		
	Quarantine an object		
	The suggested solution must support object recovery from quarantine.		
	Run system scan		
	Remote program / process / command execution		
	Start IoC scan for a group of hosts.		
	The suggested solution must support 'Single-click" response form management console		
Centralized administration, monitoring and update software requirements			
	The proposed solution must enable the installation of anti-malware software from a single distribution package.		
	The proposed solution must have customizable installation profiles depending on the number of protected nodes.		
	The proposed solution must support IPv6 addresses.		
	The proposed solution must support two-step verification (authentication).		
	The proposed solution must have ability to read information from Active Directory to obtain data about computer accounts in the organization.		
	The proposed solution must include a built-in web console for the management of the endpoints, which should not require any additional installation.		
	The proposed solution's web management console should be straightforward to use and must support touch screen devices.		

	The proposed solution must automatically distribute computer accounts by management group if new computers appear on the network. It must provide the ability to set the transfer rules according IP address, type of the operating system and location in Organizational Units of Active Directory.		
	The proposed solution must provide for the centralized installation, update and removal of anti-malware software, together with centralized configuration, administration, and the viewing of reports and statistical information about its operation.		
	The proposed solution must feature the centralized removal (manual and automatic) of incompatible applications from the administration center.		
	The proposed solution must provide flexible methods for anti-malware agent installation: RPC, GPO, an administration agent for remote installation and the option to create a standalone installation package for local installation.		
	The proposed solution must enable the remote installation of anti-malware software with the latest anti-malware databases.		
	The proposed solution must feature the automatic update of anti-malware software and anti-malware databases.		
	The proposed solution must have automatic search facilities for vulnerabilities in applications and in the operating system on protected machines.		
	The proposed solution must enable the management of a component prohibiting the installation and/or running of programs.		
	The proposed solution must enable the management of a component controlling work with external I/O devices.		
	The proposed solution must enable the management of a component controlling user activity on the internet.		
	The proposed solution must allow for the testing of downloaded updates by means of the centralized administration software prior to distributing them to client machines, and the delivery of updates to user workplaces immediately after receiving them.		
	The proposed solution must be able to automatically deploy protection to virtual infrastructures based on VMware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization platform or hypervisor.		
	The proposed solution must enable the creation of a hierarchy of administration servers at an arbitrary level and the ability to centrally managing the entire hierarchy from the upper level.		
	The proposed solution must support Managed Services Mode for administration servers, so that logically isolated administration server instances can be set up for different users and user groups.		
	The proposed solution must give access to the anti-malware security vendor's cloud services via the administration server.		
	The proposed solution must include the automatic distribution of licenses on client computers.		
	The proposed solution must be able to perform inventories of software and hardware installed on user computers.		
	The proposed solution must have a notification mechanism to inform users about events in the installed anti-malware software and settings, and to distribute notifications about events via email.		
	The proposed solution must enable the centralized installation of third-party applications on all or selected computers.		
	The proposed solution must have the ability to specify any computer in the organization as a center for relaying updates and installation packages, in order to reduce the network load on the main administration server system.		
	The proposed solution must have the ability to specify any computer in the organization as a center for forwarding anti-malware agent events from the selected group of client computers to the centralized administration server, in order to reduce the network load on the main administration server system.		
	The proposed solution must be able to generate graphical reports for anti-malware software events, and data about the hardware and software inventory, licensing, etc.		
	The proposed solution must be able to export of reports to PDF and XML files.		

	The proposed solution must provide the centralized administration of backup storages and quarantine on all network resources where the anti-malware software is installed.		
	The proposed solution must provide the creation of internal accounts to authenticate administrators on the administration server.		
	The proposed solution must provide the creation of an administration system backup copy with the help of integrated administration system tools.		
	The proposed solution must support Windows Failover Cluster.		
	The proposed solution must have a built-in clustering feature.		
	The proposed solution must include some form of system to control virus epidemics.		
	The proposed solution must include Role Based Access Control (RBAC), and this must allow restrictions to be replicated throughout the management servers in the hierarchy.		
	The proposed solution's management server must include pre-defined security roles for the Auditor, Supervisor and Security Officer.		
	The proposed solution must have ability manage mobile devices through remote commands.		
	The proposed solution must have ability to delete downloaded updates.		
	The proposed solution must enable Administration Server updates to be managed from the application interface.		
	The proposed solution must provide the ability to select an update agent for client computers based on analysis of the network.		
	The proposed solution must clearly show information about the distribution of vulnerabilities across managed computers.		
	The proposed solution's management server interface must support the Arabic language.		
	The proposed solution's management server must maintain a revision history of the policies, tasks, packages, management groups created, so that modifications to a particular policy/task can be reviewed.		
	The proposed solution's management server must have functionality to create multiple profiles within a protection policy with different protection settings that can be simultaneously active on a single/multiple devices based on the following activation rules: • Device status • Tags • Active directory • Device owners • Hardware		
	The proposed solution must support following notification delivery channels: • Email • Syslog • SMS • SIEM		
	The proposed solution must have the ability to define an IP address range, in order to limit client traffic towards the management server based on time and speed.		
	The proposed solution must have the ability to perform inventory on scripts and .dll files.		

	The proposed solution must have the ability to tag/mark computers based on:
	• Network Attributes
	  o Name
	  o Domain and/or Domain Suffix
	  o IP address
	  o IP address to management server
	• Location in Active Directory
	  o Organizational Unit
	  o Group
	• Operating System
	  o Type and Version
	  o Architecture
	  o Service Pack number
	• Virtual Architecture
	• Application registry		

	○ Application name ○ Application version ○ Manufacturer		
	The proposed solution must have the ability to create/define settings based on a computer's location in the network, rather than the group to which it belongs in the management server.		
	The proposed solution must have the functionality to add a unidirectional connection mediator between the management server and the endpoint connecting over the internet/public network.		
	The proposed solution must allow the administrator to define restricted settings in policy/profile settings, so that a virus scan task can be triggered automatically when a certain number of viruses are detected over defined amount of time. The values for the number of viruses and timescale must be configurable.		
	The proposed solution must have a customizable dashboard generating and displaying real time statistics for endpoints.		
	The proposed solution must allow the administrator to customize reports.		
	The proposed solution must have the functionality to detect non-persistent virtual machines and automatically delete them and their related data from the management server when powered off.		
	The proposed solution must enable the administrator to set a period of time after which a computer not connected to the management server, and its related data are automatically deleted from the server.		
	The proposed solution must allow the administrator to create categories/groups of application based on: • Application Name • Application Path • Application Metadata • Application Digital certificate • Vendor pre-defined application categories • SHA • Reference computers to allow/deny their execution on endpoints.		
	The proposed solution must allow the administrator to define different status change conditions for groups of endpoints in the management server.		
	The proposed solution must allow the administrator to add custom/3rd party endpoint management tools into the management server.		
	The proposed solution must have a built-in feature/module to remotely collect the data needed for troubleshooting from the endpoints, without requiring physical access.		
	The proposed solution must allow the administrator to create a Connection Tunnel between a remote client device and the management server if the port used for connection to the management server is not available on the device.		
	Suggest solution must have built-in functionality to remotely connect to the endpoint using Windows Desktop Sharing Technology. In addition, the solution must be able to maintain the auditing of administrator actions during the session.		
	The proposed solution must have a feature to create a structure of administration groups using the Groups hierarchy, based on the following data: • structures of Windows domains and workgroups • structures of Active Directory groups • contents of a text file created by the administrator manually		
	The proposed solution must be able to retrieve information about the equipment detected during a network poll. The resulting inventory should cover all equipment connected to the organization's network. Information about the equipment should update after each new network poll. The list of detected equipment should cover the following: • devices • mobile devices • network devices • virtual devices • OEM components • computer peripherals • connected devices		

	• VoIP phones • network repositories The administrator must be able to add new devices to the equipment list manually or edit information about equipment that already exists on the network. 'Device is Written Off' functionality must be available, so that such devices are not displayed in the equipment list.		
	The proposed solution must incorporate a single distribution/relay agent to support at least 10,000 endpoints for the delivery of protection, updates, patches, and installation packages to remote sites.		
	The proposed solution must incorporate a single distribution/relay agent to relay/transfer or proxy threat reputation requests from endpoints to the management server.		
	The proposed solution must support the download of differential files rather than full update packages.		
	The proposed solution must support OPEN API, and include guidelines for integration with 3rd party external systems.		
	The proposed solution must include a built-in tool to perform remote diagnostics and collect troubleshooting logs without requiring physical access to the computer.		
	The proposed solution must include Role Based Access Control (RBAC) with customizable predefined roles.		
	The proposed solution's master/primary/parent management server must be able to relay updates and cloud reputation services.		
	The proposed solution's reports must include information about each threat and the technology that detected it.		
	The proposed solution report must include details about which endpoint protection components are, or are not, installed on client devices, regardless of the protection profile applied/existing for these devices.		
	The proposed solution's primary management server must be able to retrieve detailed information reporting on the health status etc. of managed endpoints from the secondary management servers.		
	The proposed solution must include the option for the customer to either deploy an on-premises management console, or use the vendor-provided cloud-based management console.		
	The proposed solution must be able to integrate with the vendor's cloud-based management console for endpoint management at no additional cost.		
	The proposed solution must enable swift migration from the on-premises management console to the vendor cloud-based management console.		
	The proposed solution must include support for cloud-based deployment via: • Amazon Web Services • Microsoft Azure		
	The proposed solution must provide anti-malware database update mechanisms including: • Multiple ways of updating, including global communication channels over the HTTPS protocol, shared resource at local network and removable media. • Verification of the integrity and authenticity of updates by means of an electronic digital signature.		
	The proposed solution must support Single Sign On (SSO) using NTLM and Kerberos.		
	Administration & Reporting EDR		
	The suggested solution must support secure communication between management console and endpoints with EDR agent		
	The suggested solution must support management of EDR agent through command line interface		
	Suggested solution must have inbuilt feature/module to collect the data required for troubleshooting, without require a physical access to the endpoint.		
	EDR application must have self-defence mechanism to prevent modifying its files/system components entries etc.		
	The solution must allow the creation of accounts with different roles used to administer the solution, just monitor the alerts, or review changes		

	The solution should be able to send email notifications when certain types of security alerts are generated.		
	Requirements for the solution documentation. A documentation for EDR software, including administration tools, should include at least online help for Administrators		
	Suport local de la Ofertant; Lucrările de instalare, configurare, punerea în funcţiune a soluţiei şi asigurarea suportului la definirea/configurarea politicilor iniţiale Training Beneficiarului - min. 3 persoane; Furnizarea documentaţiei de instalare, (passport system şi sistemul de administrare; Configurare, restabilire a serviciului oferit + Training + documentaţia, trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă; Servicii de intervenţie în mod continuu 24h/zi – 7zile/săptămână pentru alerte cibernetice ce conţin următoarele activităţi: - Efectuarea interogări de bază pentru a aduna informaţii suplimentare legate de incidentul de securitate - Echipa de support local se va conecta la consola de management a acestuia şi va actualiza progresul / rezolvarea incidentelor de Securitate - Echipa de support local va investiga evenimentele de securitate şi va escalada la nivelul 2 de intervenţie - Echipa de support local va asigura gestionarea şi prioritizarea alertelor, gestionarea răspunsurilor la incidente şi escaladarea acestora - Echipa de support local va asista personalul superior al utilizatorilor finali în probleme de securitate, daca va fi necesar. - Echipa de support local va valida atacurile, evalua impactul, recomandă contramăsurile şi va lucra în implementarea soluţiei de mitigare şi răspuns. - Echipa de support local va emite recomandări de ajustare a produsului/ tehnologiei de securitate către IS Posta Moldovei - Echipa de support local va colabora cu părţile interesate ale Clientului pentru a asigura rezolvarea în timp util a problemelor de securitate ridicate şi critice - Echipa de support localva prioritiza şi gestiona escaladarea incidentelor validate catre IS Posta Moldovei Autorizarea de la producător - Manufacture Authorization Letter.		

Şef Direcţiei Tehnologii Informaţionale **Victor TVERDOHLEB**

Administrator interimar **Roman COJUHARI**