MAHARASHTRA STATE ELECTRICITY TRANSMISSION COMPANY LTD

AREA LOAD DESPATCH CENTRE AMBAZARI, NAGPUR

[IT DEPARTMENT]

Office of the Superintending Engineer
Area Load Dispatch Centre, Ambazari,
MSETCL, 8th mile, P.O.Wadi,
Amravati Road, Nagpur- 440023.

Phone No, (07104) 220611/221242
Fax: - (07104) 220275
Website: www.mahatransco.in
Email: ap8100it@mahatransco.in
Mobile No. 8554993681

SE/ALDC/IT/2023-24/ENQ-01/336 **Date: - 22.08.2023**

To,

Sub: - Supply installation and commissioning of 30 Client Antivirus Software License & 2 Server Antivirus Software License along with EDR/XDR for period of three years at ALDC Ambazari, Nagpur.

Dear Sir/Mam,

Please quote your lowest rates for Supply installation and commissioning of 30 Client Antivirus Software License & 2 Server Antivirus Software License along with EDR/XDR for period of three years at ALDC Ambazari, Nagpur **as per details mentioned in annexure A&B,** subject to following terms and conditions stipulated below. The quotation may please be submitted in a sealed envelope super scribed **"Quotation for Supply installation and commissioning of 30 Client Antivirus Software License & 2 Server Antivirus Software License along with EDR/XDR for period of three years at ALDC Ambazari Nagpur"** At Office of the Superintending Engineer Area Load Dispatch Centre, Ambazari, MSETCL, 8th mile, P.O.Wadi, Amravati Road, Nagpur- 440023. So as reach this office on before 28.08.2023 upto 06:00 pm. In case of hand delivery, quotation should be handed over to the receipt clerk of this office.

Sr. No	Particulars	Antivirus Product Should be mentioned by Vendor	Qty	Rates per qty to be quoted by vendor
1	Server Antivirus License Technical Specification as per Annexure-A&B(1)		2	
2	Client Antivirus license Technical Specification as per Annexure-A&B(2)		30	

Terms and Conditions

1) **Rates**: - The rates quoted should stand firm for two months, otherwise & variation in the rates should be quoted. Rates should include general packing and forwarding charges.
2) **Taxes: - The rates quoted should be inclusive of al taxes otherwise extra taxes applicable if any should be clearly mentioned in quotation. Income Tax & any tax applicable will be deducted from your bills as per rules.**

3) **Documents: -** Submit documents such as PAN and GST along with your quotation.

4) **General: -** The undersigned reserves the right to reject any or all the quotations without assigning any reason.

5) **Destination for Supply:** The complete material should be supplied at the "Office of the Superintending Engineer, Area Load Despatch centre, Ambazari, 8th mile, Amravati Road, Opp. Ordnance Factory 2nd gate, P.O. Wadi, Nagpur" during working hours 10:00 Hrs. to 18:00 Hrs. on any working day.

6) **Delivery Period**: The Supply, installation and commissioning of complete material shall be effected to the consignee within 20 (Twenty) days from the date of receipt of order.

7) **Terms of payments:** 100% payment will be made to you within 45 days after supply, installation, Commissioning and testing of complete material as per specifications, after submission of invoice bill, delivery challan & guarantee certificate to this office. However, release of payment may depend on availability of funds.

8) **Penalty** If the complete material is not supplied and commissioned within stipulated time limit, penalty at the rate 1/2% (Half Percent) per delayed week will be recovered from your bill subject to 10% maximum of work order value. In case failing of supply goods from your side, the balance goods will be purchased from other agency & difference in cost will be recovered from your bill.

9) Material supplied shall be strictly as per Annexures-A&B. substitute material/compatible material/material with difference in specification shall not be accepted.

10) If the materials are not approved/ received in good condition, the same shall have to be replaced in part or in whole as per case.

11) **Guarantee/Warranty:** The material offered shall be covered by guarantee/warranty under proper use for faulty material or workmanship. During the period of guarantee/warranty you will replace free of cost material found defective.

12) **Packing:** The material shall be packed suitably for Rail/Road worthy packing as per standard practice.

13) Compensation under labor laws if any, during contract period will be on your account.

14) **Accident:** If any accident occurs to your skilled or unskilled labor, compensation if any, is to be paid by tenderer only. MSETCL will not be responsible for any accident (fatal or non-fatal) or injury to the personnel of the agency or any financial implication arising there from.

15) **Transit Insurance:** Transit Insurance will be borne by contractor.

16) **Termination of contract**: In case you fail to carry out the work as per above terms and conditions, the MSETCL shall exercise its discretionary powers to cancel the contract by giving one-month notice. The decision of MSETCL will be final and in such case Security Deposit will be forfeited.

17) **Consignee for supply**

The consignee is as below or his authorized representative:

Superintending Engineer, Area Load Despatch centre, Ambazari, 8th mile, Amravati

Road, Opp. Ordnance Factory 2nd gate, P.O. Wadi, Nagpur – 440023

18) For any loss to the company's property during execution of work, the tenderer will be liable to pay the equivalent compensation as per the recommendation of concerned engineer

19) Apart from above points, all the terms and conditions published by MSEB in booklet "Tender and Contract of Works" are applicable to this order also.

20) **Agreement:** As per rules of MSETCL & Erstwhile MSEB you (proprietor of the firm) will have to enter into an agreement with the company for the above works as early as possible and within 10 days from date of receipt of the purchase order and until such agreement is executed with the company, the company shall not be liable to pay nor you shall be entitled to claim any amount due for payment, if any under this contract. The cost ₹500 of the stamp pa pers as per MSETCL rules and regulation shall be borne by suppliers.

Yours Faithfully,

s/d
Superintending Engineer
Area Load Despatch Centre
Ambazari, MSETCL, Nagpur

Annexure-A
Features of the Antivirus Software License

Sr. No	Features	Details
1	Threat Prevention Features	Application Exploitation - Protection from exploitation of specific application, Credential Theft Protection, Prevent privilege escalation, Prevent process hollowing attacks, Protect from Encrypting File System attacks, Protection from malicious webpages, Protection from malicious IP and domains, HIPS/Exploit Prevention - Application Control – Threat Intelligence, Web Content Filtering based on Category like Gaming, Social Networking, Hacking, Criminal Activity, Violence
2	Network Protection Features	Protection across browsers, scripts, shells ,Protection from malicious SMB, Psexec, WMI injections from other devices in the network
3	Malware Protection (AV) Features	Blended Threats/Malware Protection, Automated Malware and Threat Removal, Web Filtering, Suspicious email attachments scanning, Enhanced remediation capabilities, Global Threat Intelligence with Reputation Source configuration capability, Advanced Protection against fileless attack methods., Memory Protection, Root cause analysis/Threat cases for the malware incidents, Advance machine learning and AI based malware protection, Application startup Control, Detect low reputation downloads
4	Automatic Investigation Features	Automatic AI-Guided Intelligent alert correlation and analysis with no manual intervention, Recommendations on threat mitigations for approvals like kill process, Machine isolation etc., Suspicious event detection and prioritization, Reduced time to mitigate, automatically gather, summarize and visualize evidence, different views for different users
5	Reducing Attack Surface Features	Block all applications from creating child processes, Block execution of potentially obfuscated scripts, Block Win32 API calls from Office macro, Block applications from creating executable content, Block the theft of passwords and hash information from memory, registry, or hard disk, Block against loading .DLL files from untrusted folders, Block applications from injecting code into other processes, Block JavaScript or VBScript from launching downloaded executable content, Block executable content from email client and webmail, Block executable files from running unless they meet a prevalence, age, or trusted list criterion, Use advanced protection against ransomware., Block credential stealing from the Windows local security authority subsystem (lsass.exe).,Block process creations originating from PSExec and WMI commands., Block untrusted and unsigned processes that run from USB., Block applications from creating child processes., Block Adobe Reader from creating child processes., Block persistence through WMI event subscription
6	Potentially Malicious Applications Features	Advertisement Software, Bundling Software, Evasion Software, Torrent software, Crypto mining software, Marketing software, Poor industry reputation, Web Content Filtering
7	Device Control Features	Block Specific Devices, Allow specific devices, Monitor files written to USB devices, Disallow execution of Unsigned/Untrusted files from USB, Custom detection and

		response of device control, Automatic Threat detection on USB mount
8	Threat Detection Features	Comprehensive detection of Advanced Kernel Exploitation and In Memory Attack - Kernel sensors, Pre-written SQL queries for IT operations, Interception of API and Hypercalls, Solution should have the ability to create Forensic Snapshots and perform detailed analysis on demand, Threat analysis/correlation of 3 months data., Historical Search, Real time search, On demand data collection to capture active processes and network connections, Lists applications in the startup section of the registry and their reputation scores
9	Threat Remediation Features	Automatically applies surgical remediation & containment steps to reduce risk., Ability to remediate completely in memory attacks - due to our presence in Kernel.
10	File Level Actions Features	Block, Quarantine, Allow, Collect, Restore
11	System Level Actions	Isolate Machine, Run AV, Collect Investigation Package, Kill Process, Stop Service, De-register Dlls
12	Advanced Threat Hunting Features	Hunting for IOCs and IOAs., Shows a process tree of currently running processes, Lists the activity history of a process, Hunt for specific Application behaviors like process creations etc., Hunt for User behavior like web browsing, Application usage, file creation., Hunt for registry creation and modifications., Hunt for Logon events and activities., Hunt for command lines and PowerShell activities., Hunt for Network info and events .
13	Threat Experts Features	Targeted attack notification.,Collaborate with experts, on demand (Paid service).
14	Hosting Environment/Deployment Option for Console	Cloud

Annexure-B (1)

Technical Specification of Antivirus Software License for Server

Sr. No	Specifications
1	The antivirus solution should provide enhanced dedicated antivirus protection for servers of all the attacks originating from places inside/outside of the network due to virus and/or other malicious programming code.
2	The antivirus solution Should have a Centralized Management Console with off-premise (cloud managed) model.
3	The OEM must have its own proprietary scan engine
4	The antivirus solution Should Support Multi-Platform operating system (Windows, Linux) and the same should be managed from a single Centralised Management console
5	The antivirus solution Should have single, Configurable Installation with centralized configuration & policy management.
6	Antivirus should support integration with Active directory for directory structure of computers for better management
7	Solution must Prevent update storms and Scan Storms for virtualised environment
8	Solution must have virtualization support Esxi & Hyper V
9	Solution must have off board malware protection to a centralised security virtual machine
10	Solution must have the File Integrity Monitoring module for windows 2012 & above.
11	Solution must offer default monitored locations for File integrity monitoring for Files/registry

	entries for Windows Server platforms
12	Solution should have feature of Monitoring events & storing on a local server with option to send them to the Windows Event Viewer
13	Solution must support Malicious Traffic Detection to monitor non-browser based traffic for any Command & Control (C&C) Servers connection.
14	Administrator should have flexibility to schedule Scan and update Antivirus Agents from central Server.
15	Solution must provide integrated EDR features on Windows Server and Linux
16	Antivirus should be able to capture Viruses, Trojans, Worms, Spyware and Malware, Adware and PUA from single agent.
17	Solution should have Data control that enables you to monitor and control the transfer of files from computers to storage devices and applications connected to the internet.
18	Solution should support Data Protection Policy to monitor data copied or shared through external mediums and internet browsers.
19	Anti Virus Should have Host Intrusion Prevention System (HIPS) technology which works in 4 Layers to provide zero day protection without the need for updates (Unknown Virus Detection & Repair),
20	Anti-Virus Software must have the capability to clean, Qurantine or delete Viruses
21	Solution should have use pre-execution analysis to detect threats without letting the code run, avoiding the risk of partial infection and damage
22	Administrator Should be able to add files, folders or extensions to an exclude list so that they are not scanned on access.
23	Should enable automatic submissions of unknown/suspected virus samples to vendor and automatic response/delivery of the cure.
24	Administrator should be able to lock down all anti-virus configurations at the server & User should be prevented from being able to uninstall the anti-virus software.
25	Solution must have the Server Lockdown facility to lock the state of server to protect its integrity.
26	Antivirus should provide centralized event logging to locate and cure virus problems.
27	Solution must protect against ransomware running locally or remotely using cryptoguard.
28	Solution should have Live protection with Web Reputation
29	Solution Application control should also have the capability to restrict the usage and block the applications even if they are installed on category basis ie. Whitelisting & Blacklisting of the applications
30	Antivirus solution should have integrated Data Loss Prevention module with pre-defined templates.
31	Antivirus solution should have integrated DEVICE control module with a features to set devices to "Read Only", "Add Exceptions" and " Block" Black listing and whitelisting of the devices.
32	USB mass storage device Blocking and Exeptions with Vendor and Model (Device ID)
33	Integrated HIPS for Easy of Management and Protection
34	OEM Should have 24x7x365 toll free Global Technical Support
35	Solution must have the privilige to log a support case from the management dashboard
36	Solution must show root cause on console with complete attack chain for malware/ ransomware detection
37	Solution must have the Anti exploit technology on signature less basis so that it protects against browser, plugin, or Java-based exploit kits even if your servers are not fully patched
38	solution must be powered by Deep Learning Neural Network technology for zero day malware protection
39	Solution must have the Root Cause Analysis that provides the who, what, when, where, and how of a given attack, allowing IT the ability to constantly improve upon their security posture
40	Solution should have capability that if installed with same OEM firewall, it shares server health status with network firewall
41	Solution must automatically identifies and stops unwanted encryption attempts as well as

	system-crippling MBR attacks
42	Solution must have Anti-Hacker Capabilities that protects against the most persistent hacking attempts and prevents pervasive, real-time hacking techniques such as credential harvesting, lateral movement, and code-caving
43	Solution should have AMSI Protection (with enhanced scan for script-based threats)
44	Solution should support Malicious Traffic Detection (MTD) to known command and control centers
45	Solution should be able to provide attack chain (RCA) on management console in case if a malware detection. It should also provide SHA256 for the detection
46	Solution must have capability to Search for potential threats on devices using file names, SHA-256 file hashes, IP addresses, domains or command lines.
47	Solution should offer pre-defined administration roles to divide up security tasks according to the administrators' responsibility level.
48	Solutions must have the privilege to isolate device manually from the network.
49	EDR Solution must provide functionality of Remote Terminal to get command line access to remotely take remeadtion actions
50	EDR Solution must have predefined live discover queries for threat hunting and IT operations. These quiries should be fully customizable.
51	Solution must store threat telemetry data for at least 90 days on disk and 30 days on cloud data lake
52	Solution must have option to schedule threat hunting queries
53	Solution must allow usage of same server license on physical, virtual or cloud hosted servers
54	Proposed Solution should be in 'Leaders' quadrant of the gartners Magic Quadrant for Endpoint protection platform for the last 5 or more years
55	Proposed Solution should have secured minimum 99% protection accuracy in latest SE Labs report for 2021

Annexure-B (2)
Technical Specification of Antivirus Software License for Client

Sr. No	Specifications
1	**Integrated Management** Must have a unified console for managing multiple products such as Advanced Endpoint Protection, Email Gateway, Server Security, Mobile Control etc.
	All settings for these products MUST be configured from a Central Dashboard without the need to access additional consoles.
2	**Multi-Platform Management**
	Windows, Mac must be managed from one management console.
3	**Updating Bandwidth Consumption**
	Updating of endpoints should have the ability to set pre-configured available bandwidth used for both software updating and threat definition updates(e.g., 64, 128, 256Kbps, etc.)
	Must have the option to set up a local cache updating server within the on-premise network environment to minimize large software engine update.
	Must have an Update Management Policy that contains the configuration of update schedules on managed endpoints.
4	**Deployment Options**
	Deploying the endpoint agent must support the following methodology:
	1) Email setup link
	2) via AD Startup/Shutdown script
	3) AD Login script

	4) SCCM
	5) Include the endpoint agent installation to a gold image
5	**SIEM Integration**
	Must have the capability to extract events and alerts information from the Cloud Dashboard to a local SIEM.
6	**API for Endpoint Management**
	Must have APIs offered as RESTful HTTP endpoints over the public internet.
	APIs must have the capability to query tenants, enumerate and manage endpoints and servers, and query alerts and manage them programmatically.
7	**Role Management**
	Must have the capability to allow the separation of estate management to different administrator login.
	Must provide admins the capability to assign predefined administrative roles to users who need access to the Admin Console.
	Must be able to create custom roles and assign the products and access needed.
8	**Microsoft AD Synchronization**
	Must have the capability to only allow outbound synchronization of Users/Groups from the local Active Directory servers to the Cloud Dashboard for policy management.
9	**Policies**
	Selected policies should be able to be applied to either users or devices.
	Policies must have the capability to be disabled automatically based on a scheduled time and date.
10	**Enhanced Tamper Protection**
	Must have the capability to prevent local administrative users or malicious processes from disabling the endpoint protection.
	Must have the capability to prevent the following actions on the endpoint protection solution:
	1) Stopping services from the Services UI
	2) Kill services from the Task Manager UI
	3) Change Service Configuration from the Services UI
	4) Stop Services/edit service configuration from the command line
	5) Uninstall
	6) Reinstall
	7) Kill processes from the Task Manager UI (desired)
	8) Delete or modify protected files or folders
	9) Delete or modify protected registry keys
	Must be able to export Tamper Protection passwords in CSV or PDF formats.
11	**Threat Protection**
	Must protect against multiple threats, both known and unknown, and provide a trusted and integrated approach to threat management at the endpoint.
	Must protect endpoint systems against viruses, spyware, Trojans, rootkits, and worms on workstations and laptops regardless of their nature or the concealment mechanisms used.
	Must protect against threats related to executable files, as well as document files containing active elements such as macros or scripts. It must protect against exploits resulting from discovery (whether published or not) of security flaws in systems or software.
	Must have the capability to 'lookup' files in real-time to verify if they are malicious. This feature checks suspicious files against the latest malware in the vendor's Threat Intelligence

	database in the cloud.
	Must have the capability to do real-time scanning of local files and network shares the moment the user tries to access them. Access must be denied unless the file is healthy.
	Must have the capability to do real-time scanning of end-users Internet Access. It must monitor and classify the Internet websites according to their level of risk, and make this technology available to endpoint systems. A site known to host malicious code or phishing sites must be proactively blocked by the solution to prevent any risk of infection or attack against a flaw of the browser used. The solution must carry out checks against a database of compromised websites that are constantly being updated with new sites identified per day.
	Must protect managed systems from malicious websites in real-time, whether end-users work within the company or outside the company's secure network - at home or through public Wi-Fi. All browsers on the market must be supported (Internet Explorer, Firefox, Safari, Opera, Chrome, etc.)
12	**Anti-rootkit Detection**
	Must identify a rootkit when reviewing an element without overloading the endpoint system. Rootkits must be proactively detected.
13	**Suspicious Behavior Detection**
	Must be able to protect against unidentified viruses and suspicious behavior.
	Must have both pre-execution behavior analysis and runtime behavior analysis.
	Must be able to identify and block malicious programs before execution.
	Must be able to dynamically analyze the behavior of programs running on the system and detect then block activity that appears to be malicious. This may include changes to the registry that could allow a virus to run automatically when the computer is restarted.
	Must provide protection against buffer overflow attacks
14	**Scanning**
	Must provide a scheduled scanner to run depending on the selected frequency or by manually triggering through Windows Explorer to scan the specified directories (local, remote or removable), with analysis parameters used, which may be different from the ones selected for real-time protection.
	Must have the capability to scan archives such as zip, cab, etc. which can be enabled via policy settings.
15	**Advanced Deep Learning mechanism**
	The system shall be light speed scanning; within 20 milliseconds, the model shall able to extract millions of features from a file, conduct deep analysis, and determine if a file is benign or malicious. This entire process happens before the file executes.
	Must be able to prevent both known and never-seen-before malware, likewise must be able to block malware before it executes.
	Must protect the system even with offline and will not rely on signatures.
	Must classify files as malicious, potentially unwanted apps (PUA) or benign. Deep learning must also focus on Windows portable executables.
	Able to perform new Zero days threat scanning offline (without internet).
	Must be Smarter - should be able to process data through multiple analysis layers, each layer making the model considerably more powerful.
	Must be scalable - should be able to process significantly more input, can accurately predict threats while continuing to stay up-to-date.
	Must Lighter - model footprint shall be incredibly small, less than 20MB on the endpoint, with almost zero impact on performance.
	The deep learning model shall be trail and evaluate models end-to-end using advanced developed packages like Keras, Tensorflow, and Scikit-learn.
16	**Exploit Prevention/Mitigation must detect and stop the following known exploits:**

	1) Enforcement of Data Execution Protection (DEP) Prevents abuse of buffer overflows
	2) Mandatory Address Space Layout Randomization (ASLR) Prevents predictable code locations
	3)Bottom-up ASLR Improved code location randomization
	4) Null Page (Null Dereference Protection) Stops exploits that jump via page 0
	5) Heap Spray Allocation Reserving or pre-allocating commonly used memory addresses, so they cannot be used to house payloads.
	6) Dynamic Heap Spray Stops attacks that spray suspicious sequences on the heap
	7) Stack Pivot Stops abuse of the stack pointer
	8) Stack Exec (MemProt) Stops attacker's code on the stack
	9) Stack-based ROP Mitigations (Caller) Stops standard Return-Oriented Programming attacks
	10) Branch-based ROP Mitigations (Hardware Augmented) Stops advanced Return-Oriented Programming attacks
	11) Structured Exception Handler Overwrite Protection (SEHOP) Stops abuse of the exception handler
	12) Import Address Table Access Filtering (IAF) (Hardware Augmented) Stops attackers that lookup API addresses in the IAT
	13) LoadLibrary API calls Prevents loading of libraries from UNC paths
	14) Reflective DLL Injection Prevents loading of a library from memory into a host process
	15) Shellcode monitoring Detecting the adversarial deployment of shellcode involves multiple techniques to address things like fragmented shellcode, encrypted payloads, and null free encoding
	16) VBScript God Mode Have the ability to detect the manipulating of the safe mode flag on VBScript in the web browser
	17) WoW64 Must have the ability to prohibit the program code from directly switching from 32-bit to 64-bit mode (e.g., using ROP) while still enabling the WoW64 layer to perform this transition.
	18) Syscall Stops attackers that attempt to bypass security hooks
	19) Hollow Process Protection Stops attacks that use legitimate processes to hide hostile code
	20) DLL Hijacking Gives priority to system libraries for downloaded applications
	21) Application Lockdown Will automatically terminate a protected application based on its behavior; for example, when an office application is leveraged to launch PowerShell, access the WMI, run a macro to install arbitrary code or manipulate critical system areas; the solution must block the malicious action – even when the attack doesn't spawn a child process.
	22) Java Lockdown Prevents attacks that abuse Java to launch Windows executables
	23) Squiblydoo AppLocker Bypass Prevents regsvr32 from running remote scripts and code
	24) CVE-2013-5331 & CVE-2014-4113 via Metasploit In-memory payloads: Meterpreter & Mimikatz
	25)Dynamic Shellcode Protection Detects and blocks behavior of stagers
	26)EFS Guard Protection against Encrypting File System attacks
	26) CTF Guard Protects against a vulnerability in the "CTF" Windows component
	26) ApiSetGuard Prevents applications from side-loading a malicious DLL posing as an ApiSet Stub DLL
17	**Advanced Exploit Mitigation**
	Must be able to protect against a range of exploits or "active adversary" threats such as the following:
	1) Credential Theft Theft of passwords and hash information from memory, registry, or hard disk.
	2) APC Violation Attacks using Application Procedure Calls (APC) to run malicious codes.
	3) Privilege Escalation Attacks escalating a low-privilege process to higher privileges to access systems.
	4) Code Cave Utilisation Malicious code that's been inserted into another, legitimate application.

	5) Application Verifier Exploits Attacks that exploit the application verifier in order to run unauthorized software at startup.
18	**Malicious Traffic Detection (MTD)**
	Must be able to detect communications between endpoint computers and command and control servers involved in a botnet or other malware attacks.
19	**Intrusion Prevention System (IPS)**
	Must be able to prevent malicious network traffic with packet inspection (IPS).
	Must be able to scan traffic at the lowest level and block threats before harming the operating system or applications.
20	**Anti-Ransomware Protection**
	Must have the ability for the encrypted files to be rolled back to a pre-encrypted state.
	Both Anti-Exploit and Ransomware protection does not need to have a Cloud Lookup to perform the detection.
	When the Anti-crypto function suspects that certain behavior is not in keeping with its intended process, the Data Recorder starts caching data while the said behavior is closely reviewed to identify if the application is legitimate or if the activity is warranted. The maximum size of the data recorder is 100MB, and the Anti-crypto function caches files under 75MB.
	The anti-crypto function shall look back at all the malicious file modifications made by that process and restores them to their original location.
	Should a ransomware infection managed to get in, detailed historical tracking of where the infection originated and how it propagated will be reported courtesy of the Threat Cases (RCA).
	Must be able to protect from ransomware that encrypts the master boot record and from attacks that wipe the hard disk.
21	**AMSI Protection**
	Must be able to protect against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI).
	Must be able to scan code forwarded via AMSI before it runs, and the applications used to run the code are notified of threats. If a threat is detected, an event is logged.
22	**Data Loss Prevention (DLP)**
	Must be able to monitor and restrict the transfer of files containing sensitive data.
	Must have the capability to create custom DLP policies or policies from templates.
	Must have DLP policy templates that cover standard data protection for different regions.
23	**Peripheral Control**
	Must have the capability to control and restrict removable mass storage devices (USB sticks, CD Rom, USB external hard drives, iPods, MP3 players, etc.), as well as connection devices (Wi-Fi, Bluetooth, Infrared, Modems, etc.).
	Must have the capability to add device exemptions either by Model ID or Instance ID.
24	**Application Control**
	Must have the capability to limit the applications needed for specific user groups.
	Must be able to detect and block application categories that may not be suitable for use in an enterprise environment.
	Must have application categories for commonly used applications.
25	**Web Control**
	Must be able to block risky downloads, protect against data loss, prevent users from accessing

	web sites that are inappropriate for work, and generate logs of blocked visited sites.
	Must have security options to configure access to ads, uncategorized sites, or dangerous downloads.
	Must provide the administrator the ability to define "acceptable web usage" settings (defined by categories) in order to control the sites on which users are allowed to visit. Admin must have control access to websites that have been identified and classified in their own categories.
	Must have a data loss protection option that allows the administrator to control access to web-based email and file downloads, with choices of blocking the data, allowing data sharing, or customizing this choice.
26	**Windows Firewall Policy**
	Must be able to monitor and configure Windows Firewall on managed computers and servers using a Windows Firewall policy.
	Must be able to apply the Windows Firewall policy to individual devices (computers or servers) or groups of devices.
27	**Root Cause Analysis**
	Must have the capability to identify what happened, where a breach originated, what files were impacted, and provides guidance on how to strengthen an organization's security posture
	Must be able to record chain of events that occurred after an infection has been detected, enabling you to determine the origin of the infection, any resulting damage to assets, potentially exposed data, and the chain of events leading up to the halting of the infection.
	Shall provide a summary of the event: What the exploit was discovered, where the beacon event occurred (an asset), when it occurred, how the infection succeeded. Eg. "Outlook.exe."
	Shall provide recommendations to address the problem: Things to look for post-attack. Eg. Aside from files being restored from encrypted ones, check browser settings to ensure no vulnerabilities were created as a result of the infections.
	Activity Record allows administrators to add notes to the case. All case-related notes will be listed in this column.
	There are also buttons to enable the admin to modify the status of the case (New, In Progress, Closed) and to set priority (Low, Medium, High). When closing, the administrator can add notes and is also required to confirm (via checkboxes) that remediation steps were taken: analyzed impact on files/assets and relevant environmental improvements were implemented.
	Shall provide a tabular view of everything affected during the attack. Items can be filtered based on type — e.g., files, processes, registry keys. The administrator can view information about each item, e.g., Filename (victim file or malware agent), process ID, start/stop timestamp of the event.
	Shall indicate the beginning of the root cause, charting out the series of events resulting from the attack as a collection of nodes. Each node contains specific information about files, processes, registry keys, etc. involved at that stage. The beacon event (marked with a blue dot) will be identified in the chain, but any events executed by the process identified as the beacon event will also be shown.
28	**Advance System Clean**
	Must have the capability to trigger a deep clean upon any active detection from exploit or ransomware detection.
	The next-gen endpoint shall provide advanced Clean detection of malware by looking for the following:
	A. Files
	flagged as bad
	File has been downloaded from the internet
	Author's name/version information is missing from file properties, i.e., Impersonating a common windows system file. Reboot survivability is vigorously protected.
	Un-common file extension used.
	Contains PE structure anomalies and suggestions of obfuscation

	B. Processes
	Listening for incoming connections
	Missing source executable file
	No UI elements
	Address Space Layout Randomization (ASLR) has been removed from the system.
29	**Data Lake**
	Must be able to run security queries on all managed devices, even if they are offline
	Must be able to query data from either:
	Endpoints that are currently connected (90 days of data stored on the device)
	The Data Lake in the cloud (30 days of cloud storage)
	Must be able to schedule queries.
	Must be able to query security data from multiple Sophos products, including Sophos Firewall and Sophos Email, as well as Intercept X. Example use cases include:
	IT Operations
	Identify unmanaged, guest, and IoT devices
	Why is the office network connection slow? Which application is causing it?
	Look back 30 days for unusual activity on a missing or destroyed device
	Threat Hunting
	Extend investigations to 30 days without bringing a device back online
	Use ATP and IPS detections from the firewall to investigate suspect hosts
	Compare email header information, SHAs, and other IoCs to identify malicious traffic to a domain
30	**Block Applications**
	Must have an option to immediately detect and remove potentially malicious Portable Executable (PE) files from protected computers in the environment.
	Must have an option to block applications using their SHA-256 hash.
31	**On-demand Threat Intelligence**
	Must have an option to 'request intelligence' on suspicious files, which will upload the file to our malware research team for further analysis.
	Must be able to provide a report summary of the machine learning analysis of a suspicious file.
	Must be able to provide a summary report with a more in-depth analysis of a suspicious file to help you decide if it's malicious or clean.
32	**Endpoint Isolation**
	Must have an option to 'manually isolate' protected endpoints from the network while investigating a threat case.
	Must have an option to 'automatically isolate' compromised endpoints from the network.
33	**Forensic Data Export**
	Must have an option to generate a Forensic Snapshot of a malicious activity that occurred on a protected endpoint.
	Must be able to convert the generated Forensic Snapshot into a format where advanced queries can be run, such as SQLite or JSON file format.
	Must have an option to enable audit of Windows Authentication events, which allows Forensic Snapshots to contain more information on logon events.
	Must have the capability to upload the forensic snapshot to an AWS S3 bucket.
34	**Live Query**
	Must provide security analysts, and IT admins the ability to run SQL queries to answer almost

	any question they can think of across their endpoints and servers.
	Must be based on Osquery that allows administrators to understand the current running state of a device.
	Must be able to quickly discover IT operations issues to maintain IT hygiene and ask detailed questions to hunt down suspicious activity via SQL queries.
	Must have the capability to Pivot Queries that allows admins to select a significant piece of data in query results and use it as the basis for a new query.
	Must use powerful, out-of-the-box, fully-customizable SQL queries that can quickly search up to 90 days of current and historical on-disk data. Example use cases include:
	IT Operations
	Why is a machine running slowly? Is it pending a reboot?
	Which devices have known vulnerabilities, unknown services, or unauthorized browser extensions?
	Are there programs running that should be removed?
	Is remote sharing enabled? Are unencrypted SSH keys on the device? Are guest accounts enabled?
	Does the device have a copy of a particular file?
	Threat Hunting
	What processes are trying to make a network connection on non-standard ports?
	List detected IoCs mapped to the MITRE ATT&CK framework
	Show processes that have recently modified files or registry keys
	Search details about PowerShell executions
	Identify processes disguised as services.exe
35	**Remote Access**
	Must provide a command-line interface that can remotely access devices in order to perform a further investigation or take appropriate action.
	Must provide admins the capability to remotely connect to managed devices and get access to a command-line interface to perform actions such as:
	Reboot a device pending updates
	Terminate suspicious processes
	Browse the file system
	Edit configuration files
	Remote Access option must only be available to Admin accounts using Multi-Factor Authentication (MFA).
	Must have control over which specific admin accounts have Remote Access capability.
	Remote access sessions must be included in Audit Logs (when it started, ended or if the connection was lost)
	Must be available on Windows, Mac, and Linux operating systems.