



Office of the Chief Engineer
Area Load Dispatch Centre, Ambazari, MSETCL,
8th mile, P.O.Wadi, Amravati Road, Nagpur- 440023.
Phone No. (07104) 220611/221242 Website: www.mahatransco.in
Email: progit8100@mahatransco.in / itadmin8100@mahatransco.in
Mobile No: 8554993681/ 8983086816



E-6653

Date: 03.09.2026

E-Enquiry

To,

Subject:- Enquiry for Supply, Installation and Commissioning of 50 cloud-based Antivirus Software Client Licenses and 3 cloud-based Antivirus Software Server Licenses, along with an EDR/XDR solution for period of 3 (three) years at ALDC Ambazari, Nagpur

Dear Sir/Madam,

Please quote your lowest rates in the prescribed form i.e. Schedule 'A' duly filled & stamped/signed (on company letterhead) with the rates written in words & figures for Supply, Installation and Commissioning of 50 cloud-based Antivirus Software Client Licenses and 3 cloud-based Antivirus Software Server Licenses, along with an EDR/XDR solution for period of 3 (three) years at ALDC Ambazari, Nagpur, subject to terms and conditions stipulated below.

The quotation may please be submitted in a sealed envelope and superscribed with **"Supply, Installation and Commissioning of 50 cloud-based Antivirus Software Client Licenses and 3 cloud-based Antivirus Software Server Licenses, along with an EDR/XDR solution for period of 3 (three) years at ALDC Ambazari, Nagpur"** at Office of the Chief Engineer, Area Load Dispatch Centre Ambazari MSETCL, 8th mile, Po. Wadi, Amravati Road, Nagpur- 440023. So as reach this office on before **09.09.2026 upto 05:00 pm**. In case of hand delivery, the quotation should be handed over to the Receipt Clerk in the GAD Section of this office.

Contact Person:

- 1) Mr. Baliram Chavhan, Programmer (IT)
Mobile No. 8554993681, Email Id – progit8100@mahatransco.in
- 2) Mr. Gajanan Mirashe, Assistant Programmer (IT)
Mobile No. 8983086816, Email Id – itadmin8100@mahatransco.in

Terms and Conditions

- 1) **Scope of Work:** The bidder shall provide 50 cloud-based Antivirus Software Client Licenses and 3 cloud-based Antivirus Software Server Licenses, along with an EDR/XDR solution for the required number of endpoints as specified in the Schedule A of this enquiry.
For detailed scope of work please refer annexure 1 of this enquiry.
- 2) **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.
- 3) **Taxes:** - The rates quoted should be inclusive of all 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.

- 4) **Documents:** PAN Card/ Valid GST Certificate/Data Sheet shown in Annexure-1 with seal and sign.
- 5) **Delivery Period:** The material should be Supply, Installation & Commissioning to the consignee within 60 (Sixty) days from the date of receipt of order. Testing will be completed by MSETCL within 15 days after successful commissioning.
- 6) **Destination for Supply:** The 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.
- 7) **Penalty for late delivery:** If the complete tendered/e-enquired materials is not supplied within stipulated time limit, penalty at the rate 1/2% (Half Percent) per delayed week or part thereof 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 & SD in this case will be forfeited to company.
- 8) The Competent authority reserves the right to reject any enquiry which does not confirm to any of the enquiry conditions.
- 9) **Security Deposit:** - The successful bidder will have to pay Security Deposit @ 10% of order value of contract within 7 days from the receipt of the purchase order. The Security Deposit shall be paid in the form of BG/DD/NEFT/RTGS (In favor of Area Load Dispatch Centre ALDC Ambazari, Nagpur). If the bidder pays security deposit by BG the validity period of BG should be such as to cover complete warranty period. Security Deposit is payable at 10% of the amount of order subject to the deduction if any as per the terms of the contract. The SD will be returned after the completion of complete warranty period of material or 12 months whichever is later after successful completion of order. No interest will be paid on this Security Deposit while refunding Security Deposit. In the event of unsatisfactory performance of the contract or non-compliance of Works this amount will be forfeited.
- 10) **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.
- 11) **Packing:** The material shall be packed suitably for Rail/Road worthy packing as per standard practice.
- 12) Compensation under labor laws if any, during contract period will be on your account.
- 13) **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.
- 14) **Transit Insurance:** Transit Insurance will be borne by contractor.
- 15) **Termination of contract:** In case you fail to carry out the work as per terms and conditions of this enquiry document, 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.
- 16) **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

- 17) For any loss to the company's property during execution of work, the tenderer/vendor will be liable to pay the equivalent compensation as per the recommendation of concerned engineer
- 18) 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.
- 19) **Acceptance of Quotation:** The Company does not bind to accept the lowest or any quotations neither will any reasons be assigned for rejection of any enquiry. It is also not binding on the company to disclose any analysis report of enquiry.
- 20) If any dispute arises, the decision of the undersigned is final and binding on you.
- 21) Partial delivery of any task related to development or server administration will not be accepted by the MSETCL. Payment will not be made for partially executed work.
- 22) No extra charges for Engineer visit etc. will be paid; it should be arranged by vendor agency only.
- 23) The disputes / arbitration etc. if any, against this contract will be subject to the jurisdiction of the Nagpur Court.
- 24) **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 upto 5 Lakhs + 0.3% for amount above 5 Lakhs) of the stamp papers as per MSETCL rules and regulation shall be borne by suppliers.
- 25) **Non-Disclosure Agreement:** - The contractor shall strictly abide by the non-disclosure commitments related to all kinds of information, documents, security particulars etc. in respect of ALDC office premises and details of its functioning and other confidential information related to the establishment, to which the contractor and/or his deployed manpower shall have access to during the course of work. Contractor will have to sign non-disclosure agreement with MSETCL in the prescribed format within 7 days from the date of receipt of work order.

Thanking You.

Encl: Schedule-A/ Annexure-1(A/B/C/D)

Yours Faithfully,

S/d
**Superintending Engineer
Area Load Despatch Centre
Ambazari MSETCL Nagpur**

Copy to: - The Manager (F&A) ALDC, Ambazari, Nagpur.

<< On Bidder's Company Letterhead >>

SCHEDULE - 'A'

Subject:- Enquiry for Supply, Installation and Commissioning of 50 cloud-based Antivirus Software Client Licenses and 3 cloud-based Antivirus Software Server Licenses, along with an EDR/XDR solution for period of 3 (three) years at ALDC Ambazari, Nagpur

Sr. No.	Particular's	Quantity	Rate Per Unit (In Rs.)	GST Rate Per Unit @18% (In Rs.)	Total Price Including GST (In Rs.)
A	B	C	D	E	F = (D+E)*C
1	50 cloud-based Antivirus Software Client Licenses	50			
2	3 cloud-based Antivirus Software Server Licenses	3			
Total Amount (In Rs.)					
Amount In Words -					

OEM Details	
Product Name	
Edition & Licensing Model	
License/Subscription Validity	3 (Three) years from the date of successful installation and commissioning

SIGNATURE & SEAL OF THE BIDDER

Annexure 1(A)

Subject:- Enquiry for Supply, Installation and Commissioning of 50 cloud-based Antivirus Software Client Licenses and 3 cloud-based Antivirus Software Server Licenses, along with an EDR/XDR solution for period of 3 (three) years at ALDC Ambazari, Nagpur

Scope of Work

- The bidder shall Supply, Install and Commission of 50 cloud-based Antivirus Software Client Licenses and 3 cloud-based Antivirus Software Server Licenses, along with an EDR/XDR solution for period of 3 (three) years at ALDC Ambazari, Nagpur.
- The proposed solution shall provide centralized cloud-based management through a secure web console for deployment, monitoring, policy management, reporting, and incident response.
- The solution shall provide comprehensive protection against malware, ransomware, viruses, spyware, phishing, fileless attacks, and other advanced cyber threats.
- The XDR solution shall support real-time threat detection, automated response, threat investigation, and remediation capabilities.

Annexure 1(B)

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 against browser-based attacks, script-based attacks, command-shell abuse, malicious SMB traffic, unauthorized remote administration activities (including PsExec), Windows Management Instrumentation (WMI)-based attacks, and lateral movement techniques originating from devices within 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/ Security incident investigation and case-management 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	Solution shall provide device control capabilities including allow/block policies for removable devices, monitoring of files copied to removable media, restriction of unsigned or untrusted executable files from removable devices, automated threat scanning upon device insertion, and customizable detection and response policies.
8	Threat Detection Features	Solution shall provide advanced threat detection capabilities including detection of kernel-level attacks, memory-based attacks, behavioural analysis, forensic data collection, historical and real-time threat hunting, customizable investigation queries, telemetry correlation, on-demand endpoint data collection, monitoring of active processes and network connections, and visibility into startup applications and their reputation status.
9	Threat Remediation Features	Solution shall provide automated remediation and containment capabilities to reduce security risks. The solution shall support detection, containment, and remediation of memory-based attacks, in-memory malware, and advanced threats through endpoint monitoring and response mechanisms.
10	File Level Actions Features	Solution shall support file-level response actions including block, quarantine, allow, collect, and restore operations for investigation and remediation purposes.
11	System Level Actions	Solution shall support endpoint response actions including device isolation, on-demand malware scanning, collection of investigation artifacts, process termination, service management, and removal or disabling of malicious components during incident response.
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	Expert-assisted threat analysis and incident response capability	Solution should provide targeted attack notifications and access to on-demand expert threat analysis, incident response assistance, and security advisory services, either included or available as an optional subscription-based service.
14	Hosting Environment/Deployment Option for Console	Solution shall provide a centrally managed cloud-based console for administration, monitoring, reporting, and policy management.

Annexure-1 (C)

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 Centralized 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 virtualized environment
8	Solution must have virtualization support Esxi & Hyper V
9	Solution must have off board malware protection to a centralized 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	The solution shall provide centralized security event logging and shall support integration with standard operating-system event logging mechanisms and/or SIEM platforms.
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	The solution shall provide Host Intrusion Prevention System (HIPS) or equivalent behavior-based prevention capabilities to protect against unknown, zero-day and fileless threats.
20	Anti-Virus Software must have the capability to clean, Quarantine or delete Viruses
21	The solution shall provide pre-execution and/or behavioral analysis capabilities to detect and prevent malicious code before execution wherever technically applicable.

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 crypto guard or similar.
28	Solution should have Real-time cloud-assisted threat intelligence and file reputation analysis
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 i.e. 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 feature to set devices to "Read Only", "Add Exceptions" and "Block" Black listing and whitelisting of the devices.
32	USB mass storage device Blocking and Exceptions 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 privilege to log a support case from the management dashboard
36	The solution shall provide Root Cause Analysis (RCA) and an attack timeline/attack chain showing the sequence of events associated with detected threats.
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	The solution shall support integration with network security devices/firewalls through standard APIs, connectors, Syslog, or equivalent mechanisms for sharing relevant endpoint security and threat information.
41	Solution must automatically identify 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	The solution shall provide secure remote response capabilities, including remote command execution/terminal functionality for authorized administrators, subject to configurable access controls and audit logging.
50	EDR Solution must have predefined live discover queries for threat hunting and IT operations. These queries should be fully customizable.
51	Solution must store threat telemetry data for at least 90 days on disk and 30 days on cloud repository
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	The proposed XDR solution should have established industry recognition for its endpoint and/or extended detection and response capabilities from reputed independent industry analyst/research organizations such as Gartner, Forrester, IDC, or equivalent, during the recent years.
55	The proposed XDR solution shall have demonstrated a minimum protection accuracy of 99% or equivalent in the latest available SE Labs independent security testing report applicable to Endpoint Detection and Response (EDR)/XDR solutions, published within the preceding three years from the date of tender submission.

Annexure-1 (D)
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	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 train 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: • Memory Protection: Protection against exploitation of memory corruption and buffer-overflow vulnerabilities, including enforcement of appropriate memory-execution and memory-randomization protections. • Address Space Protection: Protection against attacks that attempt to predict or manipulate memory addresses through techniques such as address-space manipulation and randomization bypass. • Null Pointer / Invalid Memory Access Protection: Prevention of exploitation techniques involving null-pointer dereferencing or execution through invalid memory locations. • Heap Exploitation Protection: Detection and prevention of heap-based exploitation techniques, including heap spraying and manipulation of memory allocation. • Stack Exploitation Protection: Protection against stack-based attacks, including stack manipulation, unauthorized execution from stack memory and related memory-corruption techniques. • Return-Oriented Programming Protection: Detection and prevention of attacks that abuse legitimate code sequences or control-flow mechanisms to execute malicious instructions. • Exception Handler Protection: Protection against exploitation or manipulation of operating-system and application exception-handling mechanisms.

- API and System Function Protection: Protection against attempts to abuse, manipulate or bypass application programming interfaces and system functions for malicious code execution.
- Dynamic Library Protection: Prevention of unauthorized or malicious loading of dynamic-link libraries, including DLL injection, DLL side-loading and library hijacking techniques.
- Reflective and Memory-Based Code Injection Protection: Detection and prevention of malicious code or libraries being loaded directly into the memory of legitimate processes.
- Shellcode Protection: Detection and prevention of malicious shellcode execution, including encoded, obfuscated, fragmented or dynamically generated shellcode.
- Script and Browser-Based Exploitation Protection: Protection against exploitation of scripting engines, browsers and script interpreters to execute unauthorized or malicious code.
- 32-bit/64-bit Execution Boundary Protection: Protection against exploitation techniques that attempt to improperly transition between different execution modes or bypass operating-system security controls.
- System Call and Security-Control Bypass Protection: Detection and prevention of attempts to bypass endpoint security monitoring or security controls through direct or abnormal system calls.
- Process Manipulation Protection: Protection against process hollowing, process injection, process impersonation and other techniques that use legitimate processes to conceal or execute malicious code.
- Application and Library Hijacking Protection: Protection against attacks that manipulate application loading mechanisms or library search paths to execute unauthorized code.
- Trusted Application Abuse Protection: The solution shall detect and prevent malicious use of legitimate and trusted applications, including office applications, scripting engines, system utilities and other applications to execute unauthorized commands or code.
- Application Behavior Protection: The solution shall be capable of identifying and blocking malicious activities initiated by otherwise legitimate applications, including unauthorized execution of scripts, command interpreters, system-management interfaces or modification of critical system resources.
- Script Interpreter Abuse Protection: The solution shall protect against exploitation of scripting and runtime environments to execute malicious code or launch unauthorized executables.
- Signed/Trusted Binary Abuse Protection: The solution shall detect and prevent abuse of legitimate or digitally signed system utilities to execute remote, unauthorized or malicious scripts and code.
- In-Memory Attack Protection: The solution shall detect and prevent in-memory exploitation techniques, including execution of malicious payloads without requiring the creation of a conventional executable file on disk.
- Credential and Security-Tool Bypass Protection: The solution shall provide protection against exploitation techniques intended to bypass endpoint security controls, access protected memory or manipulate security-sensitive operating-system components.
- File-System and Encryption Mechanism Protection: The solution shall provide protection against exploitation or abuse of operating-system file-system and encryption mechanisms for unauthorized access, modification or execution.
- Operating-System Component Protection: The solution shall provide protection against exploitation of vulnerable operating-system components and services, including components used for text input, scripting, application execution and system management.
- Security Control Bypass Protection: The solution shall detect and prevent attempts to circumvent endpoint security mechanisms through manipulation of operating-system components, application interfaces, memory structures, execution mechanisms or security hooks.

	- Zero-Day and Emerging Exploit Protection: The solution shall provide behavior-based and/or exploit-mitigation protection against previously unknown exploitation techniques and newly emerging attack methods, wherever technically supported. - Exploit Detection and Response: On detection of an exploitation attempt, the solution shall be capable of blocking, terminating, isolating or otherwise mitigating the malicious activity and shall generate appropriate security alerts and forensic information for further investigation. - Policy-Based Configuration: Exploit prevention and mitigation controls shall be centrally configurable through the management console and shall support application/device/group-specific policies wherever technically supported. - Audit and Reporting: The solution shall maintain logs and reports for exploit-prevention events, including affected endpoint, application/process, detection time, attack technique where identifiable, action taken and relevant investigation information.
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	Command-and-Control (C2) Traffic Detection: 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. - Upon detection of unauthorized or malicious file-encryption activity, the solution shall be capable of preventing further malicious modifications and restoring affected files to their pre-attack state, wherever technically feasible. - The solution shall maintain sufficient forensic information to identify the source, execution chain, affected files and propagation/activity associated with a ransomware incident. - The solution shall provide appropriate protection against ransomware and other destructive malware targeting the master boot record, boot process, disk contents or other critical system components. - 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.
	Incident Investigation Log shall allow administrators to add and maintain notes related to the security incident.
	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 will be identified in the chain, but any events executed by the process identified as the beacon event will also be shown.
28	Advanced System Cleaning: 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. The solution shall detect and remediate mechanisms used by malicious software to maintain persistence across system reboots. 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	Centralized Security Data Repository The solution shall provide centralized collection and querying of security telemetry from managed endpoints and integrated security solutions, including the ability to perform investigations using previously collected data when endpoints are offline. Must be able to run security queries on all managed devices, even if they are offline Must be able to query data from either: Connected endpoints with locally retained security telemetry for the required retention period. Must be able to schedule queries. Must be able to query security data from multiple products, including endpoint, network, email and other integrated security solutions. 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 within the available security telemetry retention period for unusual activity on a missing or destroyed device. Threat Hunting Extend investigations using previously collected security telemetry without requiring a device to be brought back online. Use threat-prevention and intrusion-prevention detections from network security devices to investigate suspicious hosts. Compare email header information, file hashes (e.g., SHA-256), 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

	The solution shall provide an on-demand threat intelligence capability to submit suspicious files for further analysis by the vendor's threat research or malware analysis service. The solution shall provide a summary of machine-learning or automated analysis performed on submitted suspicious files, including relevant indicators and analysis results. The solution shall provide a detailed analysis report for submitted suspicious files, including sufficient information to assist administrators in determining whether the file is malicious, potentially unwanted, or benign.
32	Endpoint Isolation: Must have an option to 'manually isolate' protected endpoints from the network while investigating a threat case. <i>Must have an option to 'automatically isolate' compromised endpoints from the network.</i>
33	Forensic Data Export: Must have an option to generate a forensic data snapshot of malicious or suspicious activity that occurred on a protected endpoint. Must be able to convert or export the generated forensic data snapshot into a structured format that supports advanced querying and analysis, such as SQLite, JSON, or equivalent machine-readable formats. Must have an option to enable auditing of Windows authentication events, allowing the forensic data collection to include relevant information regarding user logon and authentication activities. Must have the capability to export or securely transfer the collected forensic data to an administrator-designated storage location, including an S3-compatible object storage repository.
34	Endpoint Security Query and Investigation: Must provide security analysts and IT administrators the ability to run custom security queries to obtain information from managed endpoints and servers. Must support querying of the current running state, configuration and relevant security information of devices using SQL or an equivalent query mechanism. Must be able to quickly identify IT operations issues, maintain IT hygiene and investigate suspicious activity using custom security queries. Must have the capability to use relevant information obtained from one query as input for subsequent or related queries, enabling efficient investigation and analysis. Must support powerful, out-of-the-box and customizable security queries that can search current and historical endpoint data retained for the required period. 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
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.

SIGNATURE & SEAL OF THE BIDDER