Specification for Next generation Anti-Virus Solution (Business and Enterprise) - for Disaster Management Center – Endpoint License Renewal

Features	Requirements	Yes/No	Remark
	Product name		
	Version		
	Country of Origin		
	Antivirus		

1. General Specifications			
1.1	The Proposed Solution must include Next Generation Advanced Endpoint Detection Protection.		
1.2	Provides a Next Generation Endpoint security platform that integrates and interoperates with other information security systems and tools (existing and future) to improve the overall information security posture.		
1.3	Prevents cyber breaches by preemptively blocking known and unknown ransomware, malware, exploits, and zero-day threats.		
1.4	The solution must enable and protect users as they safely perform their daily activities using web-based technologies, without causing any hindrance or negatively impacting the user experience.		
1.5	It should seamlessly integrate with existing systems and practices, requiring no major changes to the infrastructure or IT operations.		
1.6	The solution must provide excellent detection and prevention capabilities without affecting organizational systems.		
1.7	It should be recognized by Gartner and maintain active participation in Gartner reviews continuously for the last 3 years.		
1.8	The proposed solution must support seamless client version upgrades.Centralized management console shall support Multi-Factor Authentication (MFA) for administrative access. (To prevent unauthorized access to the management console even if an administrator's password is compromised.)		
1.9	Additionally, it must support the distribution of required signature and signature-less module updates among clients within the same network to minimize inbound network traffic.		
2. Functional Requirements			
2.1	Solution must be able to prevent the systems from Zero-Day exploits & attacks and not rely on virus definition updates.		

2.2	Product Standards & Certifications: VB100, ICSA Certified, SE LABS AAA, SC Ratings, etc.		
2.3	A track record of successfully defending enterprise endpoint systems against sophisticated threats such as ransomware.		
2.4	The organization's centralized, multi-site operations must consider the broad workforce of Information Technology Services, which has a range of skill sets and responsibilities.		
2.5	It must have an easy-to-use, auditable, granular white- and blacklisting capability that may be applied to a single endpoint, a collection of endpoints, or the entire system.		
2.6	Hardware Information Visibility: Inventory management reports must be seen, created, and delivered according to a schedule.		
2.7	It must be able to safeguard a variety of digital assets, such as servers, laptops, and desktops running Microsoft Windows, as well as assets running Linux and Apple operating systems.		
2.8	To notify IT personnel of questionable behaviors that could endanger security, a configurable email notification feature must be provided.		
2.9	Does not rely on resource-intensive detection and protection techniques that may negatively impact system and device performance.		
2.10	Management of everyday chores. Using threat knowledge from machine learning, behavioral analysis, and reputation, the solution should be able to automatically reprogram and fine-tune itself to prevent endpoint threats.		
2.11	Provide a centralized administration web interface that is easy to use, consistent, and functional.		
2.12	View Network Load (explain the consumed MB size and associated process).		
2.13	All capabilities of the proposed solution must be delivered through a single endpoint agent that cannot consume more than 15% of the resources of the installed device at its peak. To ensure that each IT staff member is granted only the permissions required for their role, thereby preventing unnecessary administrative access		
2.14	The solution's agent should have a minimum footprint and performance impact on the endpoints (should not noticeably impact the end user's computing experience during scanning or continuous protection).		
2.15	The vendor should provide 24x7 product support over multiple remote tools as well as traditional channels such as email and phone support.		

2.16	The vendor is expected to provide timely support for project planning, deployment, and problem resolution for the proposed solution.		
2.17	The vendor is expected to perform knowledge transfer of all necessary operational matters to IT staff to ensure they can effectively manage and maintain all ongoing operations of the procured solution.		
3. Technical Requirements			
3.1	Agent applications should protect: Windows 10 and 11 OS versions (32 & 64-bit), including all service pack variations.		
	Windows Server 2012 R2 and above.		
	Apple OS-based and Linux OS-based assets.		
3.2	License – Should provide a single key for all versions of the provided solution.		
3.3	Should be able to perform license management, including assigning licenses to specific sites and assigning administrative users to a specific site, so they can only manage licenses assigned to that site.		
3.4	The false positive threat identification should be less than 0.1%.		
3.5	The endpoint protection agent should not cause performance degradation on systems.		
3.6	The solution's agent must be easy to deploy, re-deploy, and manage through its life cycle. (GPO/SCCM Deployment, Remote Deployment).		
3.7	The solution should provide both real-time and historical reporting capabilities that are intuitive and easy to use.		
3.8	Only relevant information should be presented to the authorized console user (security trimmed) based on the user's role in the system. Console administrator(s) should have ultimate access to the system and all its components.		
3.9	The detected threat information should be communicated to system administrators and designated IT staff in real-time.		
3.10	Real-time threat statistics should be displayed in graphic and numerical forms for IT team investigations.		
3.11	The system should have an open reporting architecture that is easy to share and export to other systems.		
3.12	The solution should provide the capability to generate status reports for the monitored endpoints on a predefined schedule.		
3.13	The management system should be able to email the scheduled reports.		
3.14	The solution should provide holistic and historic reporting of the protected endpoints (through real-time, ad-hoc, and for a specific time).		
3.15	VDB Update – Should be able to centrally deploy with minimum network usage.		
3.16	The administration console should be available to any authorized IT staff on any device and at any time.		
3.17	The IT staff should be able to configure scheduled custom reports in addition to standard reports provided by the vendor.		
3.18	Solution's web console should be capable of filtering events to show only security-related data that is relevant and requires immediate attention.		

3.19	The centralized management console should facilitate granular new agent deployment and control of remote workstations.		
3.20	Provide real-time visibility of the system's drivers, network connections, applications, and DLL files in detail, along with the risk and reputation levels associated with each component.		
4.Additional Protection Features			
4.1	Solution to interoperate with Active Directory through ADFS to provide access to system functions in addition to the console's own local security database.		
4.2	Device Control – Centrally manage and schedule device permissions of users.		
4.3	Web Control – Should have a web filter with URL and category-based control; centrally manage and schedule web access permissions of users.		
4.4	App Control – Should have App control functionality to control/start applications, terminate and suspend other processes, and perform other application modifications.		
4.5	Provide an integrated, remote workflow that removes or reduces manual staff intervention.		
4.6	Able to replace the existing endpoint solution without any consequence or loss of capability.		
4.7	Protect from fileless malware (Memory Scan).		
4.8	Behavioral Detection System monitors system activities & self-defense mechanism for suspicious activities using multiple technologies such as ML, AI, TI, and Rule-based.		
4.9	Exploit Block & Botnet protection.		
4.10	DNA detection – Identify and prevent malicious behaviors and malware activities.		
4.11	UEFI Scanner – Unified Extensible Firmware Interface: Must monitor the integrity of the firmware and notify the user.		
4.12	Provide an easy and intuitive global search capability that provides an intuitive drill-down interface to assist in the investigation of suspicious activities.		
4.13	Ransomware Protection Module – Detect, block, and prevent processes that resemble the behavior of ransomware.		
4.14	Prevent uninstall of endpoint protection agent from Institute-owned devices by end-users who have elevated (highly privileged) access on those systems.		
4.15	Able to uninstall the endpoint agent from installed systems through the management console.		
4.16	Able to investigate and mitigate potentially infected endpoints remotely.		
4.17	Provide extensive, interactive reporting with drill-down capability on captured incidents.		
4.18	Provide extensive, full auditing capabilities for every step of the system workflows.		
4.19	IP addresses that have been detected as an attack source need to be blocked for a certain period and kept on a blacklisted list.		
4.20	Solution should support AMSI scanning of PowerShell scripts, scripts executed by Windows Script Host, and other scanned data.		
4.21	The Proposed Solution must support data protection, including document protection, without changing the architecture; should use		

	multiple technologies such as ML, AI, and Rule-based, but not limited to one technique.		
4.22	The proposed solution must be able to enforce Tamper protection.		
4.23	The solution should capably scan for threats in the operating memory of the system, boot sectors/UEFI, email files, archives, self-extracting archives, and runtime packers.		
4.24	The solution should provide Office document protection before they are opened, as well as files downloaded automatically by Internet Explorer, such as Microsoft ActiveX elements.		
4.25	The proposed solution should support multiple levels of remediation. The vendor should list the remediation levels.		
4.26	Host isolation should be supported to stop the spread of malware in case of a major attack or data breach.		
4.27	The proposed solution should provide continuous security posture assessment with risk-based scoring for endpoints and systems.		
4.28	The solution should provide real-time visibility of organizational security, including exposed assets, domains, IP addresses, and credentials.		
4.29	The solution should be capable of identifying and prioritizing security vulnerabilities based on severity and exploitability.		
4.30	The solution should provide a third-party or vendor security posture to evaluate external risk exposure.		
4.31	The solution should maintain historical tracking of security posture improvements and degradations over time. endpoint vulnerability assessment with risk-based remediation recommendations.		
4.32	The solution should provide actionable remediation recommendations to improve overall security posture and reduce risk.		
4.33	The solution should integrate global threat intelligence to enhance detection accuracy and contextual awareness.		
4.34	Provide the historical information security posture of the organization.		
4.35	Solution should support automatic network-level isolation if any unauthorized network profile is connected. Optionally, it is better if the solution is able to disable access to the network layer.		
5. Operational requirements			
5.1	Device Control – Centrally manage and scheduling of device permissions of users		
5.2	Web Control –Should have web filter with URL, categorybase & centrally manage and scheduling of web access permissions of users.		
5.3	App control- Should have App control functionality to control Start applications, terminate and suspend other process, and other application modification.		
5.4	Endpoint firewall control including with rule creating and customization. Endpoint firewall control should support with Network connection and connection profiles.		
5.5	The vendor is expected to perform knowledge transfer of all necessary operational matter to IT staff to ensure the effectively manage and maintain all ongoing operations of procured solution to keep the assets secure.		
6.Training and Support			
6.1	Provide manufacturer-certified training for Institute employees to be trained to configure, operate, and maintain the proposed solution		

6.2	This formal classroom training must cover all key concepts and be specific to the proposed solution.		
7. Support			
6.1	Describe if and how you will provide support and the time frame of guaranteed initial response time during the acceptance period.		
6.2	Specify whether you will provide on-site support in case of emergency.		
6.3	Supply, Installation and maintenance of all virus guard for DMC requirements		
7. Bidder Experience Requirement			
7.1	The bidder shall have a minimum of three (03) years of proven experience in selling, supplying, implementing, and supporting the offered brand of the proposed Next Generation Antivirus/Endpoint Security solution. The bidder shall provide documentary evidence, such as manufacturer authorization letters, purchase orders, contracts, completion certificates, customer references, or other relevant documents, to demonstrate compliance with this requirement.		
8. RFP Response Format			
8.1	Vendors must address all information specified in this Request for Proposal (RFP). All questions shall be answered fully, accurately, and comprehensively. Vendors are required to provide appropriate documentary evidence and supporting documentation for all statements, claims, qualifications, certifications, experience, technical capabilities, and compliance declarations made in their proposal. Failure to provide sufficient supporting evidence may result in the proposal being considered incomplete or non-responsive. The Institute reserves the right to verify any information contained in the vendor's RFP response, validate the authenticity of the supporting documentation, and request additional information, clarifications, or documentary evidence after the proposal has been received. Any supplemental information or documentation provided in response to such requests must be submitted in writing within the specified timeframe and shall form an integral part of the vendor's proposal.		