09/12/2024
Procurement Committee,
Finance Division,
Disaster Management Centre.

Specification for Next generation Anti-Virus Solution (Business and Enterprise) for Disaster Management Centre

Option -01 For the period of one year

Features	Requirements	Yes/No	Remark
	Product name		
	Version		
	Country of Origin		
	Antivirus		
	Duration (as option 1 & 2)		
Options- I	**For the period of one year (01)**		Forward your quotations separately as on options
Options- 2	**For the period of three years (03)**		

General Specifications	The bidder shall propose the latest Endpoint Protection Solution to secure all Endpoints of DMC including (but not limited to) servers, Desktops, Laptops and Mobile Devices.		
	All features and functionalities complied in the compliance table will be considered as the features & functionalities of the proposed version / edition of the product unless otherwise specifically mentioned under "Remarks" column		
	Provides a Next generation Endpoint security platform thatintegrates and interoperates with other information security systems and tools (existing and future) to improve the overall information security posture.		
	Prevents cyber breaches by preemptively blocking known and unknown ransomware, malware, exploits and zero-day threats.		
	The Proposed Solution must include Next Generation Advanced Endpoint Detection Protection.		
	Must be able to seamlessly integrate within existing systemand practices and without major changes of the infrastructure and IT operations.		
	Provides excellent detection and prevention services without effected to the organization system.		
	Solution should be a Gartner recognized product and continuously participate in Gartner review minimum of three years. (3 years recent or past)		
	The Proposed Solution must support to upgrade of client version seamlessly.		
	The proposed solution must support to distribute requiredsignatures and signature less module updates among the clients in the same network to reduce network inbound traffic & Use download servers directly in case of any communication issue		
	Enables and protects users as they safely perform their daily activities using web-based technologies without becoming a hindrance or negatively affecting user experience with the systems.		
	Product standards & Certifications VB100, ICSA Certified, SE LABS AAA, SC Ratings. ETC		

Functional Requirements	Must be able to prevent the systems from Zero-Day exploits & attacks and not to rely on signature-based. detection and protection methods.		
	Must provide an intuitive white- and blacklisting capability that is auditable and granular that can be applied to an endpoint, group of endpoints or system wide.		
	Must be able to provide protection for diverse digital assets including Microsoft Windows desktops, laptops, servers, and Apple OS based and Linux OS base assets.		
	Hardware Information Visibility - Must be able to View, create &Delivery-Schedule of Inventory Management Reports		
	Inventory Management Report (HW identification, Vendor Details, Accessories)		
	View Network Load (Describe with used MB size with related Process)		
	Provide a consistent, functional, centralized administrativeweb interface that is intuitive and easy to navigate.		
	The solution should be able to automate the endpoint prevention by autonomously reprogramming and re- tuning. itself using threat intelligence gained from behavioralanalysis, URL and machine learning.		
	Doesn't rely on resource intensive detection and protection methods that can adversely affect theperformance of the devices and the system.		
	VDB Update- Should be able centrally deploy with minimumnetwork usage		
Technical Requirements-protection	The solution should provide both real-time and historicalreporting capability that is Intuitive and easy to use.		
	The detected threat information should be communicatedto the system administrators and designated IT staff in real-time. Customizing alerts /notifications based on user's levels		
	The IT staff should be able to configure scheduled customreports in addition to standard reports provided by the vendor. Customizing alerts /notifications based on users' levels		
	Solution's web console should be capable of filtering. events to show only security related data that is relevant. and requires immediate attention. Customizing alerts /notifications based on users levels		
	Provide integrated, remote workflow, that removes or reduces manual staff intervention.		
	Provide protection from file less malware (Memory Scan)		
	Behavioral Detection System monitors system activities &self-defense mechanism for suspicious activities using Multiple technology Such as ML, AI, TI and Rull base.		
	Exploit Block & Botnet protection.		
	Identify and prevent malicious behaviors and malware activities including with new zero-day variants		
	Unified Extensible Firmware interface -Must monitor the integrity of the firmware and notify to user.		
	License – Should provide a Single key for all versions of provided solution.		

	Provide easy and intuitive global search capability thatprovides intuitive drill-down interface to assist in investigation of suspicious activities.		
	Ransomware Protection Module- Detect, Block and preventprocesses that resemble the behavior of ransomware.		
	Prevent uninstall of endpoint protection agent from theInstitute owned devices by end-users who have elevated (high privileged) access on those systems.		
	Able to investigate and mitigate the potentially infected endpoints remotely.		
	Provide extensive, interactive reporting with drill-down capability on captured incidents.		
	Provide extensive, full auditing capabilities for every step of the system workflows		

	IP addresses that have been detected as attack of source address need to block and block connection for a certain period of time and should kept on blacklisted list.		
	solution should support AMSI scanning of PowerShell scripts, scripts executed by Windows Script Host and data. scanned		
	The Proposed Solution must be supporting data Protection Including Document protection without changing the architecture and should be use multiple technologies such as ML, AI, Rulle base but not limited to one technique		
	The proposed solution must be able to force Tamper. protection.		
	The solution should capably Scans for threats on the operating memory of the system, Boot sectors/UEFI(Unified Extensible Firmware interface), Email files, Archives, Self-extracting archives, Runtime packers.		
	The Solution should provide Office documents protection before they are opened, as well as files downloaded automatically by Internet Explorer such as Microsoft ActiveX elements		
	The proposed solution multiple level of remediation levels. Vendor should list the remediation levels.		
	Host isolation should be support for stop spreading malware in case of major attack or data breaching		
	Proposed solution should support with Data encryption on stored data and encryption should be able to manage via central console		
	Cloud-based data, that can identify emerging threats faster than traditional signature-based detection alone		
	The system has Dynamic threat detection without an additional EDR or XDR, the solution should detect new, evolving, and previously unknown threats more quickly.		
	Solution should have reputation analysis for file and URL For known, suspicious, or safe items to determine their risk level.		

Operational requirements	Device Control – Centrally manage and scheduling of device permissions of users		
	Web Control –Should have web filter with URL, category base & centrally manage and scheduling of web access permissions of users.		
	App control- Should have App control functionality to control Start applications, terminate and suspend other process, and other application modification.		
	Endpoint firewall control including with rule creating and customization. Endpoint firewall control should support with Network connection and connection profiles.		
	The vendor is expected to perform knowledge transfer of all necessary operational matters to IT staff to ensure the effectively manage and maintain all ongoing operations of procured solution to keep the assets secure. (For 10 participants)		
Training	Provide manufacturer certified training for Institute employees to be trained to configure, operateand maintain the proposed solution. This formal classroom training must cover all key concepts and be specific to the proposed solution. (For 10 participants)		
Support	Describe if and how you will provide support and the time frame of guaranteed initial responsetime during the acceptance period. Specify whether you will provide on-site support in case of emergency. Supply, Installation and maintenance of all virus guard for DMC requirements		
RFP Response Format	Vendors must address all information specified by this RFP. All questions must be answered completely. Institute reserves the right to verify any information contained in the vendor's RFP response, and to request additional information after the RFP response has been received. Any supplemental information that you provide must be in writing and will become part of your proposal.		