SUPPLY OF ENTERPRISE ANTIVIRUS SOFTWARE (CLIENT SERVER) WITH ENDPOINT DETECTION AND RESPONSE (EDR)

Details of Endpoints:

Sr.No.	Endpoint Description	Quantity
1.	Enterprise Antivirus Endpoint with a Server License for a period of 3 years.	300 Nos.

SERVICE / DELIVERABLES DESCRIPTION:

The Antivirus software solution need to be installed on to a dedicated server and

1. Configuration of Centralized/ Main Antivirus Server console at IIPS.
2. Creation of Policies, Implementation, Configuration and Testing which includes configuration of scheduled scanning/ implementation of device control mechanism/ configuration of email alerts and reporting.
3. Installation of Antivirus Agents in all End-Points.
4. Uninstallation of existing/ Old Antivirus Agents from the End-Points
5. All tasks, encompassing server configuration and client installation, must be completed within the designated timeframe of 15 working days.
6. Submit commissioning report after completion of work.
7. Vendor must deliver trainings on Endpoint Detection and Response service (EDR) solution by request. Trainings must be at least of two distinct types – one for deploying, administering and maintaining solutions, another – for operating the solution from analyst perspective.
8. Technology Review and Planning Meeting twice a Year: a.] Once in a year thorough audit of Antivirus solution and its policies b.] Necessary patch deployments (if any/required)
9. Vendor must deliver Incident Response services and managed Threat Hunting services, if needed.
10. Maintenance services during the period of Contract (i.e. 3 years) should be provided by vendor without any additional cost (apart from support cost, if any) which includes upgrades, updates, patches and regular virus signature updates etc.
11. During the contract period, the vendor must depute qualified maintenance engineer whenever required.
12. The POC will be conducted the bidder needs to demonstrate compliance of the proposed solution to mandatory technical requirements as mentioned in this BID document.

Compliance Criteria and Required Documentation

Sr. No.	Criteria	Compliance (Yes/No)	Proof to be Submitted
1.	The vendor should be the original Equipment manufacturer (OEM) or authorized highest efficiency partner of OEM		Documentary proof to be submitted of OEM or Documentary proof of authorized Highest efficiency partner letter issued by OEM authorizing partner for valid period of Quotation
2.	Vendor Must have back support relation with the OEM's whose products are proposed by the vendor to IIPS		Manufacturer's authorization Form/Letter must be submitted along with the bid.
3.	Experience in providing 'cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program for ICT (Information and Communications Technology) systems' during the last 05 (Seven) years		Certification/Undertaking letter from OEM is to be submitted clearly mentioning the details and projects where Solution is implemented and providing support
4.	The proposed EDR solution should have been implemented by the bidder / OEM / authorized channel partner of OEM / in at least two Commercial Banks / higher education institutions (HEIs) like IIT, IIM, TISS, TIFR, SNDT, NIFT etc. / Govt. Organizations in India in the last 5 years, out of which one implementation should be on minimum 250 endpoints (in a single deployment).		Copy of Purchase Orders / Completion Certificate
5.	The Vendor preferable office setup in Mumbai/Navi Mumbai/Pune, Maharashtra.		List of support Centers in Mumbai/Navi Mumbai/Pune to be provided
6.	The Vendor shall not quote for the products, whose end of sale/ End of support has been declared by the OEM and the certificate assuring the same has to be submitted with product having minimum support life 5 years from date of purchase		Vendor to provide the following documents: 1) Certificate from the OEM assuring that the proposed Solution has not reach end-of-life and end-of-support. 2) Authorization letter of the OEM stating the product has the most recent/stable version of the operating system that is to be

Sr. No.	Criteria	Compliance (Yes/No)	Proof to be Submitted
			installed at the site. 3) Authorization letter of the manufacturer stating the product has the most recent/stable hardware device that is to be installed at the site for all the Solution.
7.	The product will cover technical support from the vendor and back to back OEM support, software updates, OS upgrades, version upgrades, troubleshooting, TAC support from the OEM, new signature for security Solution and all relevant updates for all to ensure that the most updated security risk library is available at any given point in time.		Certification/Undertaking letter from OEM
8.	The bidder must have following valid Certifications: • ISO 27001:2013 certified		Relevant ISO Certificate
9.	Bidder to submit MAF (Manufacturer Authorization Certificate) from OEM with tender reference number		MAF from OEM to be submitted.
10.	Data Sheet(s) of the product offered in the bid are to be uploaded along with the bid documents. IIPS can match and verify the Data Sheet with the product specifications offered. In case of any unexplained mismatch of technical parameters, the bid is liable for rejection.		Product data sheet created released by OEM

TECHNICAL SPECIFICATIONS OF REQUIRED ANTIVIRUS

OEM and bidder ensure that EDR solution and related modules supports listed Technical specifications and they will make sure that they will configure the solution in such a way that IIPS will check all the listed technical features and used in IIPS Network architecture. Any non-compliance to below mentioned Technical specifications may lead to rejection of bid.

Sr.No.	Description	Compliant Yes or No	Comments
1.	**Architecture and design**		
1.1	Antivirus product must support and compatible with the below operating systems: a) Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise. b) Windows 10 Home / Professional / Education / Enterprise 32-bit / 64-bit [20H1 (version 2004) ,19H2 (version 1909), 19H2 (version 1909), RS6 (version 1903), RS5 (version 1809), RS4 (version 1803), RS3 (version 1703) etc.] c) Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit) d) Windows 8.1.1 Professional / Enterprise 32-bit / 64-bit e) Windows Server 2008 R2 Foundation / Standard / Enterprise 64-bit f) Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit) g) Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit) h) Windows Server 2016 Essentials / Standard / Datacenter 64-bit i) Windows Server 2019 Essentials / Standard / Datacenter 64-bit j) Microsoft Windows Server 2022 Standard / Data Center / Essentials k) Linux Platform - 64 Bit/32 Bit including major distributions such as Ubuntu, Debian, CentOS, Fedora, and RHEL. l) Compatible with macOS 11.0 and later, supporting Intel and Apple Silicon (M1, M2, M3) (M1, M2, M3 chipsets) through native or Rosetta 2 translation.		
1.2.	Solution must support all supported versions of Operating Systems and should continue support for a minimum period of 12 months after the OS version is end of sale/life.		

1.3.	Hardware platform where the solution is installed should be flexible for any upgrade include network interfaces, RAM and CPU.		
2.	**Integration**		
2.1	The solution must Integrate with Active Directory for automatic Agent to Group Mappings and policy association.		
2.2	Active Directory should not require an agent to be installed on domain controllers for integration to work.		
2.3	The proposed solution should be able to perform threat sweeping based on the threat feeds (Files, URLs) or from intelligence received from the integrated on-premises sandbox solution.		
2.4	The solution must support integration with Managed Detection and Response service(EDR).		
2.5	The proposed solution should have the capability to allow integration with 3rd party solutions via API.		
2.6	The solution must support integration with threat intelligence portal, which contains and displays information about the reputation of files and URLs.		
2.7	The proposed solution should be have the capability to integrate with either or both cloud and on-premise identity access management (iAM) system for user authentication and access control.		
2.8	The solution should support integration with cloud reputation service.		
2.9	The proposed solution should support the cloud deployment of the Endpoint Security Server and allow High Availability (HA) configuration for Site Servers.		
3.	**Centralized Policy Management and Analytics**		
3.1	The solution should provide a unified, web-based console with multi-site support, role-based access, multi-factor authentication, customizable policies, and centralized auditing, all accessible from any authorized machine without additional software installation.		
3.2	The solution must support central management and analytics through on-prem Web console and cloud management console. (Incident related data, System status and health check data, Settings, etc).		

3.3	The system must support creating user groups, assigning policies, synchronizing endpoints, importing/exporting groups and policies, integrating with Active Directory, and enforcing policies across servers.		
3.4	Prevents potential damage from unwanted or unknown applications (executables, DLLs, OLE, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files) also Should have dynamic policies that still allow users to install valid applications based on reputation-based variables like the prevalence, regional usage, and maturity of the application.		
3.5	Ordinary Users should not be able to modify Anti Virus settings except for those in special groups as deemed necessary by the Administrators.		
3.6	The proposed solution should support configuring policies, retrieving status and reports, installing/uninstalling Endpoint Security Clients, and ensuring compatibility with Windows, Mac, and Linux endpoints, even when clients are outside the corporate network in a roaming configuration.		
3.7	The proposed solution should support flexible client software deployment (e.g., via MSI packages, web pages, login scripts, disk images, Active Directory), allow admin-only uninstallation, provide password-protected packages, send installation/uninstallation notifications, remove third-party antivirus software, and repair endpoint agents on demand.		
3.8	The tool should support dynamic policy assignment, real-time policy updates, predefined exclusions, easy false positive handling, and multi-level exclusions (account, group, process) for devices.		
3.9	The tool should control USB and Bluetooth devices with granular policies, support Mac, Linux, and Windows, identify unpatched 3rd party software vulnerabilities, and provide a software inventory.		
3.10	Solution should be capable of identifying the following devices: Windows, Linux, Mac.		
3.11	Must have the capability to identify source of infection i.e. from where the infection has originated in the network.		
3.12	Must have the capability to restore a file from quarantine if the file is deemed safe.		

4.	**Unified Endpoint Protection and Detection**		
4.1	Solution should provide Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) capabilities available in a single agent without requiring multiple software packages to be installed. Beside this all the other security features of the solution i.e. Firewall, HIPS, threat- intel, Device Control, Application Control, DLP, real-time analysis & threat hunting must be available via a single agent.		
4.2	The product should stream EDR data in real-time to own internal data lake for Threat Hunting purposes.		
4.3	Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware.		
4.4	Proposed solution should provide Recommended and Aggressive scanning capability of vulnerability protection addressing vulnerability issues and protection agains suspicious network activities.		
4.5	Solution should have ability to trigger/schedule on-demand scans (from console and/or endpoint) to look for malware, or ensure a threat has been remediated.		
4.6	Proposed solution should defends endpoints against malware, ransomware, malicious scripts also support Pre-execution and runtime machine learning to detect and mitigate threats along with File reputation - Variant protection - Census check - Web reputation having True file type scan along with proactive outbreak prevention and Command & Control call back detection supporting IPv4 and IPv6 environments.		
4.7	Solution should provide outbreak prevention with capability to limit/deny access to shared folders, block vulnerable ports, deny write access to files and folders, deny access to executable compressed files and creating mutual exclusion handling on malware processes/files.		
4.8	Should have anti malware protection and cleanup capability.		
4.9	Must have the capability to scan plug and play USB storage drives as soon as they are connected.		
4.10	Must have the capability to terminate virus program threads in memory, repair registry, remove any malicious OS processes created by trojans.		

4.11	Must have capability to disconnect endpoint from the network in case if virus/suspicious file is active in memory.		
4.12	Must have the capability to exclude file types/extensions and folders from real-time scanning.		
4.13	Must have provision to send Email Notification with list of unprotected systems in the network.		
4.14	The proposed solution should support email security it must block spam, malware, malicious attachments, and vulnerabilities, support trusted email client configurations, and scan encrypted emails over SSL/TLS.		
4.15	The proposed solution should block safe mode access, optimize endpoints, manage remote workforce, analyze files in a sandbox, and enable BitLocker encryption on Windows.		
4.16	The solution should offer context-aware, AI/ML-driven protection across Windows, MacOS, and Linux, detecting and responding to known/unknown threats with offline capabilities and prevention against malware, exploits, and unwanted programs.		
4.17	The solution should support threat sweeping, MITRE detection, advanced responses, IOC ingestion, risk-based actions, remote shell logging, alerts, process quarantine, ransomware backup, network quarantine, automated responses, and issue status management.		
4.18	The proposed solution should enable advanced alert investigation, query-based searches, saved queries, log retention, root cause analysis, risk filtering, attack visualization, and detailed threat hunting.		
4.19	Allows ingestion of custom threat feeds and Indicators of Attack (IoA) for better detection and response strategies.		
5.	**Indicators of Compromise**		
5.1	The proposed solution should allow to perform sweeps identifying indicators of compromise (IoC).		
5.2	The proposed solution should support automatic sweeping tasks based on curated intelligence and manual sweeping tasks against custom intelligence to search the environment for IoCs.		
5.3	The proposed solution should allow the Administrator/Analyst to manually add IoCs such as		

	File Hashes SHA-1, IP Addresses, Domains, and URL's as part of the custom intelligence.		
5.4	The suggested solution must support auto generation of threat indicators of Compromise (IoC) after detection occurs with ability to apply response action.		
6.	**Data Loss Prevention**		
6.1	The proposed solution should monitor, control, and report data transfers across various channels, including devices, networks, emails, cloud services, and social media, support custom rules, exemptions, and file classifications, detect confidential data via OCR, and use RegEx for DLP monitoring with differentiated report and block actions.		
6.2	The proposed solution should provide data loss prevention with pre-defined compliance templates (HIPAA, PCI-DSS, GLBA) and customizable policies using regular expressions, keywords, and dictionaries, offering visibility and control over data on ports, devices, and actions like copy-paste and print screen.		
6.3	The proposed solution should offers granular international identifiers for identifying specific data, allows custom creation, and provides visibility and control over sensitive information in motion across various protocols and applications, while continuously monitoring data at rest, in use, and in motion to prevent data loss.		
6.4	Should empowers IT to restrict the use of USB drives, USB attached mobile devices, CD/DVD writers, cloud storage, and other removable media with granular device control and DLP policies and ability to Detects and reacts to improper data use based on keywords, regular expressions, and file attributes having granular device control with the following control actions: Read only, Read and write, Read, write and execute.		
6.5	The proposed solution should be capable of detecting, monitoring, reporting, and controlling the flow of confidential data across storage drives, clipboards, file-sharing applications, cloud services, social media, and various file types, with support for custom-defined keywords or phrases.		

6.6	The proposed solution shall adhere to industry standards like HIPAA, PCI DSS, GDPR etc.		
7.	**Administration & Reporting**		
7.1	The Solution should have capability to report all known vulnerabilities in programs installed on an endpoint, along with export option.		
7.2	The solution must have a unified policies, centralized reporting and tasks execution within a Single-console for centralized management – on-prem or cloud based.		
7.3	The solution must support generating and exporting graphical/tabular reports, automatic purging of old reports, logging management server activities, scheduling report distribution, generating Host Integrity reports, providing notifications (email/SMS) for critical events, sending update status notifications, sending Endpoint Reports to SIEM, and aggregating data in Multi-Site configurations.		
7.4	The Endpoint Security Solution must manage endpoints from a central console, with all components deployed on-premise and no endpoint data shared in the public cloud.		