Annxure - 1 - Technical and Product License Details

Category	Description	Vendor Response	
		Compliance	Vendor Comment
Advanced Endpoint Protection			
General	Provide advanced automated threat detection and response against variety of advanced malware threats, including fileless attack, cryptomining and ransomware		
	Provide flexible on-premises deployment options		
	Able to provide in a single agent the following features: Data Loss Prevention (DLP), Virtual Patching, Application Control, Device Access Control etc.		
	Provide both Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) features in a single agent		
	Perform threat investigation through integrated EDR		
	Must have a visualized root cause analysis (RCA) report		
	Able to integrate with customer's SIEM solution		
	Allow third-party programs to integrate with the solution through an Application Programming Interface (API)		
	Must have a host-based intrusion prevention system (HIPS) to virtually patch known and unknown vulnerabilities before a patch is available or deployable.		
	Provide in-house Managed Detection and Response (MDR) service option		
	Able to submit suspicious files, IPs and URLs through on-premises or cloud sandbox environment		

	Able to support agent installation on Windows and MAC OS as well as Virtual Desktop environment		
	Easy agent deplyment using various supported procedures (e.g. web install, login script, agent installer package, windows remote install, client disk, Microsoft System Center Configuration Manager, etc.)		
	Solution must be able to integrate seamlessly to Next-Generation IPS (NGIPS) solution to close endpoint and network-level security gap		
	Must be able to present a holistic security solution that provided endpoint protection, and central visibility across the threat landscape.		
	Provide single, centralized management console for most efficient management of all protection components in the ever changing threat landscape.		
	Solution must provide central management functions in terms of logs, threat intelligence, status of managed products / devices, and deployment of applications.		
	Solution must provide central management functions of threat intelligence which can be shared with managed products / devices		
	Solution must provide central management functions of logs collected from managed products / devices		
	Solution must provide granular log search filters for users to define their own search criteria		
	Solution should be able to centrally manage and deploy product updates including patches, hotfixes, and firmware upgrade to all managed products/devices.		

Central Management	Solution should be able to provide a central view of threat detections for managed products / devices		
	Solution should have a tree view, or equivalent view, of all managed products/ devices including product/device name, IP address, connection status, application versions, etc.		
	Solution must be able to provide license management for all enabled features and add-ons of managed products/ devices.		
	Solution should be able to provide a configuration or policy replication mechanism for managed products / devices.		
	Solution should provide role-based access control for administration, investigation as well as operation purposes		
	Solution must provide audit log function for historical view of user activities		
	Solution should be able to generate downloadable reports from existing and customizable templates		
	Supports SSL- based encryption for secure browser access		
	Able to support Multi-factor Authentication (MFA)		
	Solution must be able to remove (reset) malware changes in the windows registry, remove dropped file(s) and terminates running malicious processes.		
	Able to perform different scan Actions based on varios malware types (Trojan/ Worm, Joke, Hoax, Virus, etc.)		

Malware Protection	Solution shall have behavior monitoring capability to detect malicious program behavior that is common to exploit attacks		
	Able to detect and remove Spyware and Adware even after it is installed and running on the computer.		
	Shall provide continuous malware protection and able to perform updates regardless of whether the client is connected to the management server.		
	Shall provide continuous malware protection regardless of whether the endpoint is connected to the Internet.		
	Solution must be able to block access to malicious websites and URLs with accurate and comprehensive rating algorithm		
	Must be able to support approved (whitelist) and blocked (blacklist) URLs list		
	Must be able to block connection attempts to command and control (C&C) servers		
	Must be able to support approved (whitelist) and blocked (blacklist) IP list		
	Able to protect computer against unauthorized encryption and modification		
	Able to block processes commonly associated with ransomware		
	Able to automatically back up and restore file changed by ransomware		
	Must have behavior monitoring capability to constantly monitors endpoints for unusual modifications to the operating system, work-related documents or on installed application.		

	The proposed solution should offer capabilities to submit suspicious payloads to sandbox, automatically or without user intervention, for advanced malware detection.		
	Solution must be able to prevent access to malicious files with accurate and comprehensive algorithm matching the MD5 checksum hash value powered by threat intelligence		
	Must be able to support scan exclusion for approved (whitelisting) file, file extension and directory		
	Solution must have machine learning technology which provides multi-layer protection for pre-execution and on execution (runtime) of malware		
	Able to block attempts to terminate processes and services associated with the vendor's agent		
	Able to block attempts to modify, delete, or add new registries associated with vendor's agent		
	Shall support automated virus outbreak prevention with the following capabilities:		
	Able to prevent other programs or users from uninstalling, modifying or deleting vendor's files		
	Solution shall shield endpoints from network exploitable vulnerabilities targetting endpoint OS		
	Shall reduce risk exposure due to missing patches		
	The proposed solution is able to provide virtual patching functionality without additional agent footprint or 3rd party integration		

Virtual Patching	Solution shall provide the customer with performance and security priority option that suits their security requirement and environment.		
	The proposed solution must allow the customer to choose the profile between perfromance & security and vice versa		
	Shall be able to block against known & unknown vulnerability exploits		
Data Loss Prevention	The proposed solution is able to provide DLP functionality without additional agent footprint or 3rd party integration		
	The integrated DLP provides protection customer's data, which includes the following functions: • Protects private data - on or off network • Advanced device control capability protects against data leaks via USB drives and other media • Covers the broadest range of devices, applications, and file types • Aids compliance with greater visibility and enforcement. Eg. GDPR, PCI/DSS, PII, GLBA, HIPAA, PDPA, ISMS, etc • The integrated DLP will be able to support the same policy across varies security solution like Web/Mail gateway, Exchage, Endpoints, etc.		
	Must support user justification option when violating the DLP policies		
	Must have customizable DLP templates, option to import and export data identifiers, and add DLP expression		

	Must be able to integrate with endpoint encryption solution to automatically encrypt protected data at rest and in motion		
Device Access Control	Configuration for Device Access Control must be done centrally from the management console		
	Able to display notification message on client computer when violation happens		
	Able to log Device Control violation		
	Allow adding of trusted devices		
	Must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The Devices that are able to be restricted must include the following: - USB Storage Devices (Also able to disable autorun) - Network Shares - CD/DVD		
Host-based Firewall	Centrally managed firewall policies		
	Able to detect & block Network viruses/worms		
	Able to centrally update network virus patterns		
	Able to define different firewall policies for online/offline client		
	Supports stateful inspection		
	Able to generate firewall logs when violation happens		

	Able to display Firewall Violation Notification for client users		
	Able to modify the content of the notification message		
	Able to isolate endpoint when outbreak prevention is invoked		
Application Control	Able to block malicious software from running using customizable lockdown, whitelisting, and blacklisting policies		
	The proposed solution is able to provide application control functionality without additional agent footprint or 3rd party integration		
	Able to manually (by the administrator or security officer) or automatically (via sandbox report) block the tagged suspicious applications.		
	The proposed solution should support SHA1 & SHA2 Hash values to be imported and block/allow the same from executing		
	Must be able to correlate data from millions of application events to identify threats and maintain an up-to-date database of validated applications		
Supported Platform	Must support Virtual Desktop on the following platforms: - VMware vCenter™ (VMware View™) - Citrix™ XenServer™ (Citrix XenDesktop™) - Microsoft Hyper-V™ Server		
	The vendor shall have 30 year's experience in enterprise data security and cybersecurity solutions		
	The vendor is in partnership with international police organization that helps other law-enforcement agencies capture cyber criminals		

Vendor	The vendor is highly recognized and named a leader by Gartner, Forrester and consistently perform in AV-TEST, NSS Labs etc.		
	The vendor garnered consistent high score from real-world protection based from independent testing labs		
	The vendor offers comprehensive product lines from hybrid cloud, endpoint, and network security solutions geared towards layered security approach		
	The vendor shall provide technical product documentation and other related information to the customer		
	The vendor shall provide 24x7 Phone and Email Support		