Annexure - II

Antivirus Technical Specifications and Requirements

1	**General Features**		**Complied (Yes/No)**
1.1	The solution offered should be based on an enterprise class, purpose built, well established proven product(s) having unified agent for all the required features.		
1.2	In case of cloud, the solution should be deployed on MeitY empaneled data center in India.		
1.3	The solution should support and be deployable on host operating systems of virtual machines like vmware/ hyper-V/ HCI and VDI.		
2	**Endpoint Protection**		
2.1	Malware Protection	The solution must protect against all kinds of viruses, Trojans, worms and any other forms of exploits by blocking files (executable/malicious) in real-time.	
2.1.1		The solution should be capable of detecting malware by scanning multi levels of compressed files.	
2.1.2		The solution should be able to detect malware/virus in the files packed using real-time compression algorithms as executable files.	
2.1.3		The solution must protect the endpoints on the network using stateful inspection.	
2.1.4		The solution shall also protect against other malwares such as Spyware, adware, dialers, joke programs, remote Access and hacking tools, which can be used with malicious intent	
2.1.5		The solution shall detect and block access to phishing sites.	
2.1.6		The solution shall be able to scan only those file types which are potential virus carriers (based on true file type).	
2.1.7		The solution should be able to do on-access scan and heuristic (behavioral) scan of the files.	
2.1.8		The solution should be able to detect suspicious network traffic. It shall allow blocking of all traffic from the originating suspicious endpoint.	
2.1.9		The solution must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.	
2.1.10		The solution should have tamper protection against malware/virus that attempt to disable security measures.	
2.2	Web Reputation	The solution shall provide detection and blocking of Command and control (C&C) traffic and prevent access of malicious and suspicious websites.	
2.3	Browser Exploit Protection	The solution should identify the web browser exploits and prevent the exploits from being used to compromise the web browser.	
2.4	Outbreak Prevention	The solution must provide outbreak prevention to limit/deny access to the affected endpoints in case there is an outbreak	
2.4.1		The solution should have a manual outbreak prevention feature that allows administrators to limit/deny access to the affected endpoints in case there is an outbreak	

2.5	Machine Learning	The solution should detect emerging unknown security threats using machine learning, which do not have any signatures	
2.5.1		The solution should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.	
2.6	Sandbox Solution	The solution shall have on-prem / cloud based sandboxing feature so that suspicious objects can be submitted for detailed analysis.	
2.6.1		Before downloading any files on file-system, the endpoint should monitor, scan and analyze the file. If the file is found to be suspicious, it should be forwarded to the sandbox for detailed analysis and emulation. If found potentially malicious, the sandbox shall share the threat intelligence with endpoint security for quarantining/blocking the malicious file across the enterprise. The reports of sandboxing shall be made available to BHEL admin.	
2.6.2		The solution should have the ability to analyze and detect malware in common file formats including (but not limited to) the following types: · Compressed archives – Zip, Rar · Common Text document Formats: MS Word formats (doc, docx), pdf · Common Spreadsheet formats: MS Excel formats (xls, xlsx) · Presentation formats: MS PowerPoint formats (ppt, pptx). · Common Executable Formats: exe, dll, jar	
2.6.3		Solution should support zero trust policy for files downloaded from untrusted sources on web. Solution shall quarantine suspicious files.	
2.7	Application Control	The solution should provide application whitelisting. The solution should be able to create user defined whitelist.	
2.7.1		The solution should provide file reputation and global usage details to allow cross checking of known good/bad files.	
2.7.2		The solution should log and block any changes / tampering of whitelisted applications / codes, like DLL's, System files, registry etc.	
2.8	Behavioral Monitoring	The solution shall protect against unauthorized encryption (ransomware) or modification and provide detailed information of the attempted attack.	
2.8.1		The solution shall protect against fileless malware and shall utilize behavioral techniques to detect malware based on the behavior of the file.	
2.8.2		The solution shall be able to detect and block process execution chains. It should be able to detect when a malicious application tries to execute a trusted application.	
2.9	Data Exfiltration Detection	The solution should be able to scan any file downloaded via network or email on the system. If any malicious file, link, attachment is detected the same should be blocked and cleaned to prevent spread of the infection across the network or data exfiltration from the system.	

2.9.1		The solution should have capability of anti-bot and block the command and control communication from endpoint	
2.10	Actions and Alerts	The solution should have the capability to repair, quarantine, block, delete or process kill on detection of malware / Suspicious activity.	
2.10.1		Damage rollback - The solution should allow removal of detected malicious file, affected registry entries and any new files dropped by malware.	
2.10.2		User Alerting - The solution shall provide alerts to users in case of any security incident along with a course of action, in case of any failure to clean	
3	**Device Control**		
3.1		The solution should automatically scan external devices (CDs/DVDs, USB devices) as soon as they are accessed from an endpoint (PC, Server, Laptop).	
3.2		The solution should automatically allow standard USB Keyboards, USB Printers, USB Scanners, USB webcams and USB mouse (Human interface devices)	
3.3		The solution should allow blocking of physical devices on USB such as removable storage devices, Bluetooth, Wi-Fi network cards, and other plug and play devices.	
3.4		The solution shall provide management of plug and play devices and allow restrictions on their usage to Monitor, Block or make the device Read-Only along with the option of providing exceptions	
3.5		The solution shall allow classification of USB devices as allowed / not allowed USB devices. The solution shall allow exclusion of allowed USB devices by using their vendor ID, product ID or serial number	
3.6		The solution shall provide logs of the device control feature to detect attempts of connecting not-allowed devices	
3.7		The solution should prevent data loss via USB	
4	**Endpoint Detection and Response (EDR)**		
4.1		The solution should provide context-aware endpoint detection and response (EDR). Custom detection, intelligence, controls, recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack.	
4.2		The solution should be able to perform threat sweep based on the threat feeds (IP Address, Files, URLs, Domain)	
4.3		The solution shall perform sweep across endpoints using user-defined search criteria like User Name, File - Name, File - Hash, IP address, Hostname.	
4.4		The solution should be able to perform the root cause analysis of an incident.	
4.5		The solution should be able to search and analyze data regarding critical breach or potential attack.	
4.6		The solution should provide the advance response capabilities like Kill process, Isolate device, Block process.	

4.7		The solution shall allow using of domains, file-hashes, etc. for root cause analysis and shall also allow blocking of the files/file-hashes/domains/URLs identified by the root cause analysis.	
5	**Support for Legacy OS**		
5.1		The solution should support legacy OS like Windows 7 SP1/8.1/Windows Server 2008 R2, etc., during contract period.	
5.2		The agent for legacy OS should be light weight and should not affect the performance of the devices.	
5.3		The solution should provide the capability to create firewall rules, to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.	
5.4		The solution should provide intrusion detection and prevention, file system and admin lockdown of infected endpoints.	
5.5		The solution should provide application whitelisting. The solution should be able to create user defined whitelist.	
5.6		The solution should be able to do on-access scan and heuristic (behavioral) scan of the files.	
5.7		The solution shall provide detection and blocking of Command and control (C&C) traffic and prevent access of malicious and suspicious websites.	
5.8		The solution should identify the web browser exploits and prevent the exploits from being used to compromise the web browser.	
5.9		The solution should provide machine learning to detect emerging unknown security threats, which do not have any signatures	
5.10		The solution should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.	
5.11		The solution should allow blocking of physical devices on USB such as removable storage devices, Bluetooth, Wi-Fi network cards, and other plug and play devices.	
5.12		In case legacy OS support is not available on cloud-based solution, then in that case an on-prem solution should be provided for legacy OS only along with necessary update server, management server, etc.	
6	**Solution Architecture and Management**		
6.1		The solution should have a central server deployed on cloud / on-prem with high availability for getting the updates from the OEM. The updates shall flow from the central server to the endpoints through internet/MPLS.	
6.2		In case of cloud solution, an on-prem intermediary server will be required at BHEL Hyderabad DC for users who are not having direct internet access. The vendor shall provide the necessary server hardware, OS and any other required softwares.	

6.3		The solution should be managed from a single centralized console and should provide integrated management for endpoint security solution. It should be able to deploy, manage, and update agents and policies from one management platform.	
6.4		The solution shall provide the enterprise-wide visibility of the status of all the deployed components from a central dashboard. The dashboard shall provide a summarized view to analyze top threats & summary of malware traffic or any other threats	
6.5		The solution should provide a central view of threat detections, logs, threat intelligence for endpoints.	
6.6		The solution shall have provision to centrally manage the scan schedule and frequency for endpoints. The solution must support logical grouping of various endpoints into separate groups with separate AV policies. Endpoints should have an option to postpone the scan.	
6.7		The OEM should have a 24/7 security service update and should support real time updates of the system on release.	
6.8		The solution must have the flexibility to roll back/overwrite the Virus Pattern and Virus Scan Engine if required via the web/management console.	
6.9	Incremental Updates	The solution should allow for incremental update of definitions to reduce the network traffic.	
6.10	Roaming Clients	The solution should provide a mechanism for updates of roaming devices or clients which are not connected to corporate network.	
6.10.1		When the PC is connected to network after a long period, the endpoint agent should get updated by itself once it is connected to the network.	
6.11		The solution should be able to do full scan of files / folders with a choice of specifying directories and file extensions not to be scanned.	
6.12		Host user (normal/admin) should not be able to uninstall/remove the endpoint security agent.	
6.13		The solution shall provide hierarchical grouping of machines and policy deployment	
6.14		The solution should support IPv6.	
6.15		The solution shall provide detection of endpoints that do not have the agent installed either directly or through integration with Active Directory.	
6.16		The solution must have readymade policies including –	
		a) To make all removable drives read only,	
		b) To block program from running from removable drives	
		c) Protect clients files and registry keys	
		d) Block modifications to host files	
6.17		Endpoint Platforms should support Windows 10 and later releases and Windows Server 2012 and later during contract period.	
6.18	Agent Installation	Should be able to deploy the endpoint agent using the following mechanisms:	

		a) Client Packager (Executable & Microsoft Installer (MSI) Package Format)	
		b) Web install page or through the Web Console of the management station.	
		c) Login Script Setup	
		d) Remote installation	
		e) From a disk/ghost image.	
		f) Inbuilt capability or through AD or through system management software. All the client components should be installed using the single client package.	
6.19	Role Based Administration	Central management console should support role-based access control	
6.19.1		The solution shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges for different components	
6.20	Log Management	The solution shall be able to receive logs from the managed components & endpoints and store them centrally for a period of 90 days on cloud/on-prem. In case of any limitations on cloud storage, then cloud storage should be provided for minimum 30 days and for the remaining days, on prem storage at BHEL Hyderabad DC to be provided by the vendor. The vendor shall supply the necessary hardware and software for on-prem storage of logs. In total 90 days' log backup shall be available on either cloud or on prem. The solution shall also provide the functionality to integrate these events with SIEM. The vendor shall also demonstrate log restoration.	
6.20.1		The endpoint client should store event data generated while it is disconnected from the corporate network and forwards it on reconnection	
6.21	Endpoint Quarantine	The solution shall have provision of restricting network access to an infected endpoint as per administrator requirement	
7	**Reporting**		
7.1	The solution should support report customization and allow viewing directly using a web browser and/or as a dashboard using the same management console for the endpoints.		
7.2	The solution should support at least the following formats for exporting data: CSV/Excel, Acrobat PDF		
7.3	The solution must be able to send notifications whenever it detects a security risk on any endpoint or during a security risk outbreak, via E-mail or SNMP trap		
7.4	The solution should have a feature that notifies administrators about security risk or virus outbreaks. This should be configurable on number and type of occurrences of new risks or viruses or logs and the time period within which they must occur to trigger the notification on any computer, on a single computer, or on distinct computers.		

7.5	Solution should be able to generate downloadable reports from existing and customizable templates.	
7.6	The solution shall provide the feature to send the reports via E-mail on fixed time intervals or event driven basis.	
7.7	The solution should provide the customizable/standard reports group/Unit wise	
7.8	The solution should be able to generate a report of clients which should include fields	
	a. Username in computer	
	b. Hostname	
	c. Network parameters	
	d. Definition update in client	
	e. Client status Online/Offline	
	f. Client version/ Agent version	
	g. Outdated/ Unmanaged endpoints	