Sl.No.	Feature description	Comply (Y/N)	Proof of compliance with page numbers
1	Sheet1 OEM should be present in gartner's "Leaders" quardent atleast 3 times in last 5 years For endpoint security		
2	Wave for Endpoint security		
3	GDPR Compliance		
4	The proposed enterprise endpoint security solution should be of a client server architecture and provide enhanced protection for all desktops, laptops & servers in the network against malware,Viruses, spyware, worms, ransomware		
5	Automatic update of EPS server should happen from OEM server and EPS clients should get Updates from EPS server		
6	Version upgrades and updates of virus definitions should happen automatically across all servers And clients without downtime.		
7	Should conserve network bandwidth, wan bandwidth while updating clients with all policies		
8	Solution should support multiple client installation methods like remote installation, email based Installation, url based installation, network share based installation		
9	Heuristic scanning and behavioural protection for web browsers, documents & programs should be available.		
10	Proposed solution should automatically uninstall existing antivirus product and install new product		
11	Should have options to scan rootkit, vulnerability, tracking cookies		
12	Should have the ability to exclude specific files and directories from scanning		
13	User should not be able to tamper the end point security agent – uninstall or change the Security settings		
14	Detailed report with fields such as date, time, username, IP		
15	Global quarantine mechanism with restore function & should be able to manage data purging		
16	Web reputation, Application Control, Device Control to be present by default and not by means of ADD ON		
17	Advanced malware and ransomware protection: Defends endpoints—on or off the corporate Network—against malware, Trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like crypto malware and file less malware.		
18	Automatic detection and response against an ever-growing variety of threats, Including file less and ransomware		

19	Using a blend of advanced threat protection techniques to eliminate Security gaps across any user activity and any endpoint. It constantly learns, adapts, and automatically shares threat Intelligence across your environment		
20	Endpoint solution should have capability of AV, HIPS, Firewall, Application control, Device control, integrated DLP with pre-execution and post-execution machine learning feature In unified single Agent		
21	Detection and response capabilities: Advanced detection and response capabilities are included With the solution.		
22	The industry's most timely virtual patching: Vulnerability Protection virtually patches known and Unknown vulnerabilities, giving you instant protection, before a patch is available or deployable.		
23	Centralized visibility and control: multiple capabilities Antimalware, Application control, Vulnerability protection, Device control, Firewall, DLP can be managed through a single console To provide central visibility and control across all functions		
24	Infuses high-fidelity machine learning with other advanced detection techniques for the broadest Protection against ransomware and advanced attacks.		
25	Blends signature-less techniques, including high-fidelity machine learning, behavioural analysis, variant protection, census check, application control, exploit prevention, and good file check with Other techniques like file reputation, web reputation, and command and control (C&C) blocking.		
26	Advanced ransomware protection monitors for suspicious file encryption activities at the endpoint, Terminates malicious activities, and even recovers lost files if necessary		
27	Support different agent operating system like Windows 7, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Linux , MAC & Latest Versions		
28	High-fidelity machine learning (pre-execution and runtime)		
29	Behavioural analysis (against scripts, injection, ransomware, memory and browser attacks)		
30	File reputation - Variant protection - Census check - Web reputation		
31	Exploit prevention (host firewall, exploit protection)		
32	Command and control (C&C) blocking - Device control- Good file check		
33	Should have Integrated spyware protection and clean-up		
34	Should have the capability to assign a client the privilege to act as a update agent for rest of the Agents in the network		
35	Safeguards endpoint mail boxes by scanning incoming POP3 email and Outlook folders for Threats		

37	Should be able to detect files packed using real-time compression algorithms as executable files.		
38	Solution should have AV, HIPS, Application control, DLP. All features must be available in Single agent.		
39	Delivers the most-timely vulnerability protection in the industry across a variety of endpoints		
40	Stop zero-day threats immediately on your physical and virtual desktops and laptops—on and Off the network		
41	Blocks known and unknown vulnerability exploits before patches are deployed		
42	Should have protection from Document Exploits		
43	Protects endpoints with minimal impact on network throughput, performance, or user productivity.		
44	Filters forbidden network traffic and ensures allowed traffic through stateful inspection		
45	Blocks all known exploits with intrusion prevention signatures		
46	Shield operating system and common applications from known and unknown attacks.		
47	Solution should allow to enhance your defences against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints. With a combination of Flexible dynamic policies, whitelisting and blacklisting capabilities.		
48	Solution should Prevent potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files)		
49	Solution should provide global and local real-time threat intelligence based on good file Reputation data correlated across a global network		
50	Solution should Categorize the applications and provides regular updates to simplify administration		
51	Should use intelligent and 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.		
52	Should uses application name, path, regular expression, or certificate for basic application Whitelisting and blacklisting.		
53	Features system lockdown to harden end-user systems by preventing new applications from Being executed		
54	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		
55	Detects and reacts to improper data use based on keywords, regular expressions, and file attributes		
56	Should have granular device control with the following control actions: Read only, Read and write, Read, write and execute		

57	Provides regional specific templates and data protection options, helping customers comply with Data protection guidelines such as GDPR, PCI/DSS, HIPAA, GLBA, SB-1386 and US PII		
58	Includes a granular list of truly international identifiers to identify specific data by patterns,Formulas, positioning, and more. Identifiers can also be created from scratch		
59	Web traffic protection with ability to scan objects delivered to end user computer via HTTP and FTP protocols, including possibilities to perform heuristic analysis and define Trusted sites excluded from the scan.		
60	Detection and block access to phishing links.		
61	Network monitor with ability to set up per application network rules for certain protocols (TCP, UDP) and ports.		
62	Reduced scan time by omitting scan of unchanged objects since last scan.		
63	Recovery after infection by removing all malware related artifacts, including System files, registry and hence to prevent possible OS faults and crashes.		
64	Notify administrator about important events related to antivirus protection by mail, sound, pop-up window and log record. Simple Network Management Protocol (SNMP) support.		
65	Ability to discover unprotected computers within corporate network by IP, hostname, Domain name and subnet mask.		
66	Mobile device management via iOS MDM.		
67	Reports export into PDF, XML, HTML & excel or equiavalent format		
68	Periodic update by schedule.		
69	Ability to update application modules and antivirus bases from different sources and by various Means, including network and local data sources.		
70	User/administrator guide		
71	Documentation should explain in details the process of antivirus software deployment,Configuration and usage.		
72	Antivirus software should have context help.		
73	Technical support provided by certified professional from ISV side or its partners via Telephone, mail and web channels and resident engineer		
74	ISV web site of antivirus software should have appropriate sections related to the Given antivirus software, including support knowledge bases and community forum.		

CHAIRMAN
Computer Centre
I.I.T. Madras
Chennai - 600 036