

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
1	TECHINICAL	8	Point 4	Bidder shall have minimum five years experience in supplying ANTIVIRUS in any utility / reputed organisations in India. Bidder shall submit documentary evidence of order copies and performance certificate	The Bidder / OEM shall have a minimum of five (5) years' experience in supplying antivirus solutions to utilities or other reputed organizations in India. •Documentary evidence in the form of order copies and performance certificates shall be submitted in support of this requirement by the Bidder / OEM.	Tender conditions shall prevail
2	Technical	8	Point 5	Bidder must have record of successfully supplied minimum 5000 no of ANTIVIRUS License each in the last 3 years. Max of 2 Orders copies for above along with customer's reference shall be submitted with the bid. Documentary evidence to be submitted. PO and Tax Invoice (without rates) to be submitted by Bidder as an evidence to support the above.	The Bidder / OEM must demonstrate a record of having successfully supplied a minimum of 5,000 antivirus licenses in total during the last three (3) years. • A maximum of two (2) order copies, along with customer references, shall be submitted with the bid. • Documentary evidence, including Purchase Orders (POs) and Tax Invoices (without rates), shall be provided by the Bidder / OEM to substantiate compliance with this requirement.	Tender conditions shall prevail
3	Technical Qualification Criteria - Point 5		Point 5	Bidder must have record of successfully supplied minimum 5000 no of ANTIVIRUS License each in the last 3 years. Max of 2 Orders copies for above along with customer's reference shall be submitted with the bid.	Kindly confirm if 2 PO of 5000 AV license each is required.	combined 2 PO covering 5000 AV can be submitted for each Year
4	Bill of Quantity			Antivirus +EDR on premise model	This is an Antivirus RFP and EDR is add On. Kindly confirm for how many Endpoints needs to cover with EDR solution.	All end points
5	Scope of Work - Service and Deliverables		Point 2	Uninstallation of existing/ Old Antivirus Agents from the End- Points	THIS should not be the sole responsibility of bidder. Either BSES/Trend Micro must support while doing the unistallation.	This will be done in coordination
6	Scope of Work - Solution			Single product solution (Agent & Management Console) for End Points and Server	Kindly confirm if bidder needs to provide the hardware required for Management Console	NO
7	Technical Qualification Criteria		4	Bidder shall have minimum five years experience in supplying ANTIVIRUS in any utility / reputed organisations in India. - Bidder shall submit documentary evidence of order copies and performance certificate.	Request to add the start-up organizations and start-up exemption for the experience	
8	Technical Qualification Criteria		5	Bidder must have record of successfully supplied minimum 5000 no of ANTIVIRUS License each in the last 3 years. Max of 2 Orders copies for above along with customer's reference shall be submitted with the bid. - Documentary evidence to be submitted. PO and Tax Invoice (without rates) to be submitted by Bidder as an evidence to support the above	Also the all relevant experience should consider from OEM / Bidder - That is : OEM/ Bidder Must have supplied at least 5000 antivirus licenses in last 3 years (max 2 orders).	Tender conditions shall prevail
9	Technical Qualification criteria	8	8	The OEM vendor should be leaders quadrant of Gartner for last 3 years and should be able to provide update to clients/end points from on premise server.	Removal of this clause will ensure fair competition, transparency, and better value for public funds.	
10	Technical	43	3	The Propose Solution should support NetApp ONTAP (ONTAP system hosting the CIFS/SMB Shares) integration with Antivirus solution using ONTAP Antivirus Connector.	Our solution does not support it , as Net app storage have different antivirus product Net App have inbuilt antivirus solutions please suggest we can quote without this complainece if it not affect the whole solution	Tender conditions shall prevail
11	Technical		Antivirus +EDR on premise model	Antivirus +EDR	Most of the OEMs have cloud based solution and this requirement restricts them to participate.	*Management console should be same for all end points. Agents can be different *Bidder SI can bid for separate solution for Netapp and for other end points *Not compatible OS needs to be mentioned same will be discussed during technical evaluation

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
12	Technical		SCOPE	The "Total solution" will include Supply and Installation of Enterprise Anti-Virus Software with EDR License on 3525 nodes. Solution must support: 1. PC: Windows 10/11 and later, 2. Servers Windows Ver 2012/2016/2019 and later, Linux 6.5/7 and later, and MacOS Laptops. 3. Storage - NetApp ONTAP integration with Antivirus - 200 TB	The "Total solution" will include Supply and Installation of Enterprise Anti-Virus Software with EDR License on 3525 nodes. Solution must support: 1. PC: Windows 10/11 and later, 2. Servers Windows Ver 2012/2016/2019 and later, Linux recent distributions and later, and MacOS Laptops. The solution can have separate licenses for Client and servers.	Tender conditions shall prevail
13	Technical		ASSET COUNT	PC/Laptop: 3400 Server: 125		
14	Technical		OS	PC: Windows: 10, 11 Server: Windows 2012, 2016, 2019 Linux: 6.5. 7 Mac NetApp Storage :	PC: Windows: 10, 11 Server: Windows 2012, 2016, 2019 Linux: Recent distributions & Mac	Tender conditions shall prevail
15	Technical		License and Support	3 Years from Go live (Contract Period)		ok
16	Technical		Agent	Solution should be able to run on PC running on 4GB RAM and 1 GB free HDD space	Solution should be able to run on PC running on 4GB RAM and 8 GB free HDD space	*Management console should be same for all end points.Agents can be different
17	Technical		Solution	Single product solution (Agent & Management Console) for End Points and Server.	Single product solution (Agent & Management Console)	*Management console should be same for all end points.Agents can be different
18	Technical		Deployment	2 Months from LOI/PO		Tender conditions shall prevail
19	Technical		Service and Deliverables	1.Installation of Antivirus Agents in all End-Points (Laptop/Desktop/Servers)		Tender conditions shall prevail
20	Technical			2.Uninstallation of existing/ Old Antivirus Agents from the End-Points		Tender conditions shall prevail
21	Technical			3. Configuration of Centralized/ Main Antivirus Server Console		Tender conditions shall prevail
22	Technical			4. Creation of Policies, Implementation, Configuration and Testing which includes configuration of scheduled scanning/ implementation of device control mechanism/ configuration of email alerts and reporting		Tender conditions shall prevail
23	Technical			5.Training of the New Antivirus Solution deployed along with implementation document and manual		Tender conditions shall prevail
24	Technical			6.Technology Review and Planning Meeting twice a Year:		Tender conditions shall prevail
25	Technical			a. Once in a year thorough audit of Antivirus solution with EDR and its policies		Tender conditions shall prevail
26	Technical			b. Necessary patch deployments (if any/required and released by OEM with in 1 month of release)		Tender conditions shall prevail
27	Technical			7.The "Total solution" will include Supply and Installation of		Tender conditions shall prevail
28	Technical			Enterprise Anti-Virus Software License on 3400 +125 nodes for		Tender conditions shall prevail
29	Technical		server. Nodes consist of Windows/10/11 and later, Windows		Tender conditions shall prevail	
30	Technical		Servers 2012/2016/2019 and later, Linux Servers and MacOS		Tender conditions shall prevail	
31	Technical		Laptops.		Tender conditions shall prevail	
32	Technical		8.Installation of console and onboarding of clients on console,Group update provider configuration at major locations to provide update to clients.Update provider at locations should take update from central update provider which should be on premise		Tender conditions shall prevail	
33	Technical		9.The bidder must proactively inform about potential security threats/vulnerabilities, new global security threats/ zero day attacks in circulation and suggest suitable counter measures to safeguard BRPL's IT assets / data.		Tender conditions shall prevail	
34	Technical		10.The bidder shall ensure that faults and failures intimated by BRPL as above are set right within 24 hours of being informed of the same.Also in case of server crash rebuilding and reinstallation of solution will be in bidders scope		Tender conditions shall prevail	

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
35	Technical			11.The bidder shall provide maintenance services during the period of 3 years. During license period, the bidder shall provide upgrades, updates, patches and regular virus signature updates, etc. without any additional cost. During the contract period, the bidder must depute qualified maintenance engineer whenever required.		Tender conditions shall prevail
36	Technical		S. No	General Requirement		
37	Technical		1	The proposed solution should be able to offer Endpoint Protection, Device Control –Solution to provide on premise update for 3400 endpoints and 125 servers. Clients need not to have internet access and can take update from on premise server and remote location update providers created at each site		Tender conditions shall prevail
38	Technical		2	Endpoint Protection functionality should be available for Windows, and Linux based OS platforms. Including Laptop, Desktop and Servers. Should support Desktop OS-Windows 10 and 11 and any other OS released by Microsoft during contract period Should support Servers OS - Windows 2012, 2016, 2019 , Linux: 6.5. 7 & later, Ubuntu, CentOS and Solaris	Endpoint Protection functionality should be available for Windows, MacOS, and Linux based OS platforms. Including Laptop, Desktop and Servers. Should support Desktop OS-Windows 10 and 11 and any other OS released by Microsoft during contract period Should support Servers OS - Windows 2012, 2016, 2019 , Linux: Recent distributions like Ubuntu, CentOS & later	*Bidder SI can bid for separate solution for Netapp and for other end points
39	Technical		3	The Propose Solution should support NetApp ONTAP (ONTAP system hosting the CIFS/SMB Shares) integration with Antivirus solution using ONTAP Antivirus Connector.	Remove this point to make the specs generic.	ok
40	Technical		4	The proposed solution agent should be light weight and should be able to facilitate the proposed functionality with minimum system requirement of 4GB RAM, 2.2GHZ CPU & 1Gb free HDD space	The proposed solution agent should be light weight and should be able to facilitate the proposed functionality with minimum system requirement of 4GB RAM, 2.2GHZ CPU & 8Gb free HDD space	ok
41	Technical		5	Bidder should be an authorized partner of OEM, Manufacturer Authorization Form (MAF) from OEM should be provided stating that bidder is an authorized partner of OEM and authorized to participate in this tender and in case the bidder is not able to perform obligations as per contract during the contract period, contracted services will be provided by OEM within the stipulated time.		Tender conditions shall prevail
42	Technical			Threat Prevention		
43	Technical		1	Heuristic virus scan: Should Scan files and identifies infections based on behavioral characteristic of viruses		Tender conditions shall prevail
44	Technical		2	On-access virus scan :Should Scan files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses		Tender conditions shall prevail
45	Technical		3	Scan target drives: Should specify directories and file types to scan & it should include the target areas such as; Memory for rootkits Running process Registry Temp folder Recycle Bin Compressed MIME -encode files		Tender conditions shall prevail
46	Technical		4	Scan exclusions: Should specify directories and file extensions not to be scanned		Tender conditions shall prevail
47	Technical		5	Should have Configurable Scanning. Should have the ability to control the percentage of CPU resources dedicated to a scan process	Should have Configurable Scanning. Should have the ability to minimize impact on system resources during scan process	ok
48	Technical		6	Treatment options: Should Enable choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete.		Tender conditions shall prevail
49	Technical		7	Intelligent quick scan: Should Check the most common areas of the file system and registry for traces of spyware		Tender conditions shall prevail
50	Technical		8	Should support unique real time update based on over the web cloud technology to provide real time signatures for dynamic and latest threats to reduce the dependency on Daily Signature updates.		Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
51	Technical		9	Should have a different protection level in cloud based intelligence. This includes Very Low, Low, Medium, High and Very High.	Should have adjustable protection levels in cloud based intelligence.	As per RFP also we need to have option to create package with specific feature only
52	Technical		10	Full-system scan: Should Scans local file folders and specific file types		Tender conditions shall prevail
53	Technical		11	Should be able to lock down all anti-virus configurations on the system		Tender conditions shall prevail
54	Technical		12	User should be prevented from being able to uninstall the anti-virus software.		Tender conditions shall prevail
55	Technical		13	Must be able to totally protect from spyware, adware, Trojans, key loggers, P2P Threats, Hackers tools, DDOS Attack Agents, in real time	Must be able to totally protect from spyware, adware, Trojans, key loggers, P2P Threats, Hackers tools in real time	OK
56	Technical		14	Should have centralized management and reporting capabilities to deliver reports like top Spywares, by category, by infected machines, by risk priority etc		Tender conditions shall prevail
57	Technical		15	Real time Active protection on memory, process termination / file removal of pests in active memory		Tender conditions shall prevail
58	Technical		16	The proposed solution should have an ability to create custom expert rule to prevent sophisticated attacks. The custom rule configuration should have coverage for syntax to protect files, protect process, product registry, buffer overflow, illegal API use, protect services.		Tender conditions shall prevail
59	Technical		17	Should have centralized update/download mechanism which should be able to download details of latest Spywares and push the same across all the desktops		Tender conditions shall prevail
60	Technical		18	The solution must be able to auto-quarantine or auto-delete spyware or adware without end-user interaction. The administrator should be able to restore an endpoint back from quarantine using central management.		Tender conditions shall prevail
61	Technical		19	The administrator should have option to rescana a quarantined endpoint to make sure that the infection has been removed.		Tender conditions shall prevail
62	Technical		20	Browser Security : Should Support Internet Explorer ,Mozilla Firefox and Chrome		Tender conditions shall prevail
63	Technical		21	Proposed solution should have integrated URL categorization feature		Tender conditions shall prevail
64	Technical		22	Proposed solution should categories URLs for threats like – Spywares, Trojans, Spam, Adware etc		Tender conditions shall prevail
65	Technical		23	Solution URL category module should provide end user detail threat information about the site		Tender conditions shall prevail
66	Technical		24	Should be able to update definitions & scan engine on the fly, without a need for reboot or stopping of services on servers.		Tender conditions shall prevail
67	Technical		25	The solution should be able to determine file-execution decisions with rule-based logic based on endpoint context (file, process, and environmental attributes) blended with collective threat intelligence.		Tender conditions shall prevail
68	Technical		26	The proposed solution should be able to map the global intelligence from their own cloud with the local intelligence collected from endpoint solution proposed.		Tender conditions shall prevail
69	Technical		27	The proposed endpoint protection solution should be able to integrate with third party feeds such as Virus Total in the same endpoint management console.	The proposed endpoint protection solution should have inbuilt threat intelligence feeds.	OK
70	Technical		28	The proposed endpoint protection solution should be able to import threat reputation of files through file hashes into the central endpoint protection management solution.	The proposed endpoint protection solution should have inbuilt threat intelligence feeds.	OK
71	Technical		29	The proposed endpoint solution should be able to automatically prevent the execution of even unknown executable files even if the endpoint does not have the latest signatures and without heuristics or behavioral patterns.		
72	Technical		30	Should not block just on file hashes but on certificate bases also such that only trusted certificates are allowed to execute.		Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
73	Technical		31	The solution should provide an Integrated firewall which should use reputation scores based on vendors global threat intelligence to protect endpoints from botnets, DDoS, APTs, and suspicious web connections.	The solution should protect endpoints from botnets, APTs	OK
74	Technical		32	The proposed solution should provide an option for the administrator to pick and choose the protection modules they want for their endpoints based on their system type and environment.		Tender conditions shall prevail
75	Technical		33	The solution should have an integrated endpoint-assisted security installation (EASI) installer to offer an accelerated and simplified deployment process.	The solution should have simplified deployment processes for endpoints.	OK
76	Technical		34	The proposed endpoint security solution should be able to undertake pre-execution analysis for unknown malware while performing Static file feature extraction (for example file type, import hash, entry point, resources, strings, packer & compiler details, compile time, API's, section names etc.)		Tender conditions shall prevail
77	Technical		35	The proposed endpoint security solution should be able to undertake Post-execution analysis for unknown malware while performing Behavioral features and Memory analysis (for example behavioral sequence, process tree, file system, registry events, network communication events, mutex, strings from memory etc.)		Tender conditions shall prevail
78	Technical		36	The proposed endpoint security solution should Extract static file feature for classification by using an machine learning model that resides on endpoint and the Static feature based detection should not require cloud lookups.		Tender conditions shall prevail
79	Technical		37	The solution should be able to inspects all data that flows between the client system and the network. It should compare the network data with the known network-based attacks		Tender conditions shall prevail
80	Technical		38	It should support desktop firewall capabilities to directly block unwanted traffic		Tender conditions shall prevail
81	Technical		39	HIPS solution should provide facility to create different policy for different network connectivity like – LAN, DHCP.		Solution should provide facility to create User defined agent with specific feature and rest features disabled
82	Technical		40	Solution should provide facility to create User defined signatures	Solution should provide facility to create custom rules/policies for threat detection	we need to have option to create package with specific feature only and also there should be offline package of current signature for instant scanning
83	Technical		41	Solution should prevent buffer overflow, illegal API use, and network exploits.		
84	Technical		42	The solution should intercept and scan Javascripts and VBScripts before they are executed. The solution should also be able to create URL exclusion for certain in-house/known sites from this scan process.		Tender conditions shall prevail
85	Technical		43	The proposed solution should have system rollback feature in case system is compromised with the advanced malware attack. Rollback remediation should monitors the behavior of unknown processes and backs up changes that they make to the system. If a monitored process exhibits malicious behavior, enhanced remediation stops the process, its children, and ancestors, and rolls back the changes that it made, restoring the system as close as possible to its original state before the process ran.	The proposed solution should have ransomware rollback feature to restore files encrypted by ransomware attacks.	As per RFP and also there should be feaure to have ransomware rollback feature to restore files encrypted by ransomware attacks.
86	Technical			Device Control for Desktops/Laptops/Servers/Storage		
87	Technical		1	The solution should potentially block the end point system from loading physical devices such as removable storage devices, Bluetooth, Wi-Fi, and other plug and play devices based on device classes and device definitions are used to define device rules		Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
88	Technical		2	It should support device management and should allow you to Monitor, Block or make the device Read-Only along with the option of providing exceptions		Tender conditions shall prevail
89	Technical		3	It should support for detecting attempts to copy confidential data to removable storage devices (e.g. USB drives, floppy, CD/DVD, etc.).		Tender conditions shall prevail
90	Technical		4	It should support for blocking Windows native CD writing and other CD writing software. The block must inform the user that the action is being blocked.		Tender conditions shall prevail
91	Technical		5	It should support for customizable notification "pop-up" messages		Tender conditions shall prevail
92	Technical		6	It should be able to control the access of USB devices by using their vendor ID, product ID or serial number, along with time based USB access.	It should be able to control the access of USB devices by using their model or instance ID.	ok
93	Technical		7	The solution installation, policy management and reporting should be handled by an integrated endpoint agent on the client.		Tender conditions shall prevail
94	Technical		8	The solution should provide near real-time event monitor allowing you to see events as they happen, view details (user, machine, rules triggered, etc), and even access evidence files as the events happen in your environment.		Tender conditions shall prevail
95	Technical		9	It should support ability to restrict access to company approved devices, but also if necessary to permit exclusions to this requirement. Exception and/or exclusions can be designed to accommodate different devices or different groups of users		Tender conditions shall prevail
96	Technical		10	It should provide the functionality of logging and audit-trail capabilities		Tender conditions shall prevail
97	Technical			Management Platform		
98	Technical		1	Should have a Centralized Management Console for managing Antivirus, Antispyware, device control		Tender conditions shall prevail
99	Technical		2	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.	The solution should be managed from a single centralized console and should provide integrated management for endpoint security solution. It should be able to manage, and update agents and policies from one management platform.	Tender conditions shall prevail
100	Technical		3	It should support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subset of machines or a particular site	It should support hierarchical grouping of machines and policy deployment.	Tender conditions shall prevail
101	Technical		4	Central management console should provide actionable reports and customized Reports as per requirement for Audit and internal reporting purpose		Tender conditions shall prevail
102	Technical		5	Central management console should support granular role based access control		Tender conditions shall prevail
103	Technical		6	Should ensure security policy enforcement by integrating and centralizing installation, deployment, management & updating	Remove this point to make the specs generic.	Tender conditions shall prevail
104	Technical		7	Centralized management server should be able to automatically report about the new unprotected systems. Also it should have centralized management tagging mechanism to identify the system with no agent and to run automated agent deployment task if system found as unmanaged.	Remove this point to make the specs generic.	ok for removal
105	Technical		8	Solution should provide for custom reports and queries along with role-based access providing different levels of dash-boarding and relevant reports to users.		Tender conditions shall prevail
106	Technical		9	Solutions should provide near real-time event monitor allowing you to see events as they happen, view details (user, machine, rules triggered, etc), and even access evidence files as the events happen in your environment.		Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
107	Technical		10	The proposed management server deployment mechanism should have dedicated components as distributed repository for bandwidth management.	This will only be applicable in case the management solution is deployed on premise.	We will be needing Update provider on premise so that endpoints can take update from on premise update provider without internet. Console can be on cloud. There should be option to configure pushing updates as per our schedule and option to save bandwidth
108	Technical		11	Solutions should support report customization and allow viewing directly using a web browser and also as a dashboard using the same management console for the endpoints.		Tender conditions shall prevail
109	Technical		12	Solution should supports the following formats for exporting data: CSV, HTML, XML, Acrobat PDF,		Tender conditions shall prevail
110	Technical		13	Solution should support ability to restrict access to company approved devices, but also if necessary to permit exclusions to this requirement. Exception and/or exclusions can be designed to accommodate different devices or different groups of users		Tender conditions shall prevail
111	Technical		14	Solution should provide the functionality of events being viewed, filtered, and sorted in the Management console, allowing security officers or administrators to view events and respond quickly. If applicable, suspicious content is attached as evidence to the event.		Tender conditions shall prevail
112	Technical		15	Solution should provide the functionality of logging and audit-trail capabilities.		Tender conditions shall prevail
113	Technical		16	Solution should provide the capability to log administrative activities in the Management console. Administrative activities that are logged in the Management console include, changes to policies, deployment of policies, agent override activities, agent termination, and agent uninstall key generation.		Tender conditions shall prevail
114	Technical			Premium Support		Tender conditions shall prevail
115	Technical		1	The solution should be proposed with 24x7 email and telephonic support with the standard licensing. The same should be certified by OEM with relevant documents.		Tender conditions shall prevail
116	Technical		2	The OEM should provide a utility to collect product and system information to assist Support in diagnosing issues		Tender conditions shall prevail
117	Technical		3	Product upgrades should be easily be downloadable from the OEM Official Website		Tender conditions shall prevail
118	Technical		4	The OEM should provide a service which delivers the latest OEM product information by email — patch and upgrade notification; and critical alerts that require immediate attention.		Tender conditions shall prevail
119	Technical		5	During warranty period the software must be covered with necessary minor or major upgrades (Software support and upgrade-Major i.e. Version and minor too)		Tender conditions shall prevail
120	Technical		6	The bidder/OEM must ensure that their team is available on a high-priority basis to promptly resolve any cybersecurity attack on BRPL throughout the contract period. The bidder shall provide 24/7 support and immediate incident response to mitigate threats and minimize operational disruptions		Tender conditions shall prevail
121	Technical		7	All points covered under Scope of Work ,section Service and Deliverables		Tender conditions shall prevail
122	Technical			INTEGRATION		Tender conditions shall prevail
123	Technical		1	Solution should support end point protection and device control (SOAR for Outgoing Control)	Solution should support endpoint protection and device control with automated response capabilities.	ok
124	Technical		2	Solution should have file integrity monitoring		Solution needs to be on premise. Distribution agents should be on premise and all agents should be able to take update from on premise distributionserver/agent and internet is not required by agents for taking update. Console can be on cloud

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
125	Technical		3	Proposed solution should be capable of deployable on a virtual appliance using Enterprise hypervisor solutions	Proposed solution should be capable of on-premise/cloud-based management with agents deployable on virtual machines using Enterprise hypervisor solutions.	Update provider should be on premise and should be able to be installed on virtual machine so that endpoints can take update from on premise update provider without internet. Console can be on cloud. There should be option to configure pushing updates as per our schedule
126	Technical		4	Solution must be able to auto-quarantine or auto-delete spyware, Malware, Adware. The administrator should be able to restore an endpoint back from quarantine using central management.		Tender conditions shall prevail
127	Technical		5	Solutions should provide near real-time event monitor of events with, view details (user, machine, rules triggered, etc), and even access evidence files as the events.		Tender conditions shall prevail
128	Technical		6	The solution must have Integration with SIEM and other security solution for log collection through API integration		Tender conditions shall prevail
129	Technical		SCOPE	The "Total solution" will include Supply and Installation of Enterprise Anti-Virus Software with EDR License on 3525 nodes. Solution must support: 1. PC: Windows 10/11 and later, 2. Servers Windows Ver 2012/2016/2019 and later, Linux 6.5/7 and later, and MacOS Laptops. 3. Storage - NetApp ONTAP integration with Antivirus - 200 TB		Tender conditions shall prevail
130	Technical		ASSET COUNT	PC/Laptop: 3400 Server: 125		Tender conditions shall prevail
131	Technical		OS	PC: Windows: 10, 11 Server: Windows 2012, 2016, 2019 Linux: 6.5. 7 Mac NetApp Storage :		Tender conditions shall prevail
132	Technical		License and Support	3 Years from Go live (Contract Period)		Tender conditions shall prevail
133	Technical		Agent	Solution should be able to run on PC running on 4GB RAM and 1 GB free HDD space	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/release-notes/system-requirements-for-v53308029-d69e1453.html	The proposed solution agent should be light weight and should be able to facilitate the proposed functionality with minimum system requirement of 4GB RAM, 2.2GHZ CPU & 8Gb free HDD space
134	Technical		Solution	Single product solution (Agent & Management Console) for End Points and Server.		Tender conditions shall prevail
135	Technical		Deployment	2 Months from LOI/PO		Tender conditions shall prevail
136	Technical		Service and Deliverables	1. Installation of Antivirus Agents in all End-Points (Laptop/Desktop/Servers)		Tender conditions shall prevail
137	Technical			2. Uninstallation of existing/ Old Antivirus Agents from the End-Points		Tender conditions shall prevail
138	Technical			3. Configuration of Centralized/ Main Antivirus Server Console		Tender conditions shall prevail
139	Technical			4. Creation of Policies, Implementation, Configuration and		Tender conditions shall prevail
140	Technical			Testing which includes		Tender conditions shall prevail
141	Technical			configuration of scheduled scanning/ implementation of device		Tender conditions shall prevail
142	Technical			control mechanism/		Tender conditions shall prevail
143	Technical		configuration of email alerts and reporting		Tender conditions shall prevail	
144	Technical		5. Training of the New Antivirus Solution deployed along with		Tender conditions shall prevail	
145	Technical		implementation document		Tender conditions shall prevail	
146	Technical		and manual		Tender conditions shall prevail	

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
147	Technical			6.Technology Review and Planning Meeting twice a Year:		Tender conditions shall prevail
148	Technical			a. Once in a year thorough audit of Antivirus solution with EDR		Tender conditions shall prevail
149	Technical			and its policies		Tender conditions shall prevail
150	Technical			b. Necessary patch deployments (if any/required and released by		Tender conditions shall prevail
151	Technical			OEM with in 1 month of release)		Tender conditions shall prevail
152	Technical			7.The "Total solution" will include Supply and Installation of		Tender conditions shall prevail
153	Technical			Enterprise Anti-Virus Software License on 3400 +125 nodes for		Tender conditions shall prevail
154	Technical			server. Nodes consist of Windows/10/11 and later, Windows		Tender conditions shall prevail
155	Technical			Servers 2012/2016/2019 and later, Linux Servers and MacOS		Tender conditions shall prevail
156	Technical			Laptops.		Tender conditions shall prevail
157	Technical			8.Installation of console and onboarding of clients on		Tender conditions shall prevail
158	Technical			console,Group update provider configuration at major locations		Tender conditions shall prevail
159	Technical			to provide update to clients.Update provider at locations should		Tender conditions shall prevail
160	Technical			take update from central update provider which should be on		Tender conditions shall prevail
161	Technical			premise		Tender conditions shall prevail
162	Technical			9.The bidder must proactively inform about potential security		Tender conditions shall prevail
163	Technical			threats/vulnerabilities, new global security threats/ zero day		Tender conditions shall prevail
164	Technical			attacks in circulation and suggest suitable counter measures to		Tender conditions shall prevail
165	Technical			safeguard BRPL's IT assets / data.		Tender conditions shall prevail
166	Technical			10.The bidder shall ensure that faults and failures intimated by		Tender conditions shall prevail
167	Technical			BRPL as above are set right within 24 hours of being informed of		Tender conditions shall prevail
168	Technical			the same.Also in case of server crash rebuilding and		Tender conditions shall prevail
169	Technical			reinstallation of solution will be in bidders scope		Tender conditions shall prevail
170	Technical			11.The bidder shall provide maintenance services during the		Tender conditions shall prevail
171	Technical			period of 3 years. During license period, the bidder shall provide		Tender conditions shall prevail
172	Technical			upgrades, updates, patches and regular virus signature updates,		Tender conditions shall prevail
173	Technical			etc. without any additional cost. During the contract period, the		Tender conditions shall prevail
174	Technical			bidder must depute qualified maintenance engineer whenever		Tender conditions shall prevail
175	Technical			required.		Tender conditions shall prevail
176	Technical		S. No	General Requirement		
177	Technical		1	The proposed solution should be able to offer Endpoint Protection, Device Control –Solution to provide on premise update for 3400 endpoints and 125 servers. Clients need not to have internet access and can take update from on premise server and remote location update providers created at each site	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/how-to-update-content-and-definitions-on-the-client-v38539566-d79e6/choose-a-distribution-method-to-update-content-on-v107363096-d79e384.html	as per RFP

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
178	Technical		2	Endpoint Protection functionality should be available for Windows, and Linux based OS platforms. Including Laptop, Desktop and Servers. Should support Desktop OS-Windows 10 and 11 and any other OS released by Microsoft during contract period Should support Servers OS - Windows 2012, 2016, 2019, Linux: 6.5. 7 & later, Ubuntu, CentOS and Solaris	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/release-notes/system-requirements-for-v53308029-d69e1453.html	as per RFP,rest can be discussed during technical evaluation
179	Technical		3	The Propose Solution should support NetApp ONTAP (ONTAP system hosting the CIFS/SMB Shares) integration with Antivirus solution using ONTAP Antivirus Connector.	This is covered under Symantec Protection Engine https://docs.netapp.com/us-en/ontap/antivirus/vscan-partner-solutions.html#:~:text=Creating%20your%20file...,and%20mediate%20any%20affected%20files.	Bidder SI can bid for separate solution for Netapp and for other end points
180	Technical		4	The proposed solution agent should be light weight and should be able to facilitate the proposed functionality with minimum system requirement of 4GB RAM, 2.2GHZ CPU & 1Gb free HDD space	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/release-notes/system-requirements-for-v53308029-d69e1453.html	The proposed solution agent should be light weight and should be able to facilitate the proposed functionality with minimum system requirement of 4GB RAM, 2.2GHZ CPU & 8Gb free HDD space
181	Technical		5	Bidder should be an authorized partner of OEM, Manufacturer Authorization Form (MAF) from OEM should be provided stating that bidder is an authorized partner of OEM and authorized to participate in this tender and in case the bidder is not able to perform obligations as per contract during the contract period, contracted services will be provided by OEM within the stipulated time.		Tender Conditions remain unchanged
182	Technical			Threat Prevention		
183	Technical		1	Heuristic virus scan: Should Scan files and identifies infections based on behavioral characteristic of viruses	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-sonar-v40139626-d47e6/about-sonar-v44010692-d47e487.html#:~:text=Last%20Updated%20April%2016%2C%202025.monitor%20them%20for%20suspicious%20activity.	as per RFP,rest can be discussed during technical evaluation
184	Technical		2	On-access virus scan :Should Scan files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/preventing-and-handling-virus-and-spyware-attacks-v40739565-d49e172/managing-scans-on-client-computers-v40739504-d49e6/about-the-types-of-auto-protect-v41324382-d49e2589.html#:~:text=Last%20Updated%20April%2016%2C%202025.when%20Auto%2DProtect%20is%20Enabled.	Tender conditions shall prevail
185	Technical		3	Scan target drives: Should specify directories and file types to scan & it should include the target areas such as; Memory for rootkits Running process Registry Temp folder Recycle Bin Compressed MIME -encode files	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/hardening-windows-clients-against-memory-tampering-v123149922-d3859e12879/memory-exploit-mitigation-techniques-v114221375-d53e13441.html	Tender conditions shall prevail
186	Technical		4	Scan exclusions: Should specify directories and file extensions not to be scanned	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-exceptions-in-v36686987-d51e6/creating-exceptions-for-virus-and-spyware-scans-v39814459-d51e102/excluding-a-file-or-a-folder-from-scans-v39818564-d51e811.html	Tender conditions shall prevail
187	Technical		5	Should have Configurable Scanning. Should have the ability to control the percentage of CPU resources dedicated to a scan process	https://knowledge.broadcom.com/external/article/151599/client-scan-performance-tuning-options.html#:~:text=Best%20Scan%20Performance%20E2%80%93%20Symantec%20Endpoint,the%20other%20processes%20goes%20down.	Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
188	Technical		6	Treatment options: Should Enable choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/customizing-the-virus-and-spyware-scans-that-run-o-v43098005-d49e1253/changing-the-action-that-takes-when-it-makes-a-det-v42955926-d49e3203.html	Tender conditions shall prevail
189	Technical		7	Intelligent quick scan: Should Check the most common areas of the file system and registry for traces of spyware	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/preventing-and-handling-virus-and-spyware-attacks-v40739565-d49e172/managing-scans-on-client-computers-v40739504-d49e6/about-the-types-of-scans-and-real-time-protection-v41160104-d49e2232.html	Tender conditions shall prevail
190	Technical		8	Should support unique real time update based on over the web cloud technology to provide real time signatures for dynamic and latest threats to reduce the dependency on Daily Signature updates.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-sonar-v40139626-d47e6/about-sonar-v44010692-d47e487.html	Tender conditions shall prevail
191	Technical		9	Should have a different protection level in cloud based intelligence. This includes Very Low, Low, Medium, High and Very High.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/About-Incidents/understanding-the-severity-and-priority-levels-of-incidents.html	Tender conditions shall prevail
192	Technical		10	Full-system scan: Should Scans local file folders and specific file types	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/symantec-endpoint-protection-client-for-windows-help/managing-scans-on-your-computer-v19072109-d49e5983.html	Tender conditions shall prevail
193	Technical		11	Should be able to lock down all anti-virus configurations on the system	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/about-application-control-system-lockdown-and-devi-v36534292-d45e176/configuring-system-lockdown-v35628639-d45e1550.html	Tender conditions shall prevail
194	Technical		12	User should be prevented from being able to uninstall the anti-virus software.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/managing-groups-clients-and-administrators/managing-client-computers-v55115300-d19e131/preventing-users-from-disabling-protection-on-clie-v9510980-d19e3226.html	Tender conditions shall prevail
195	Technical		13	Must be able to totally protect from spyware, adware, Trojans, key loggers, P2P Threats, Hackers tools, DDOS Attack Agents, in real time	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/what-is-v45096464-d43e1648/how-symantec-endpoint-protection-technologies-prot-v97539434-d43e1669.html#:~:text=and%20unknown%20threats-,Symantec%20Endpoint%20Protection,exfiltration%2C%20and%20remediation%20and%20inoculation.	OK
196	Technical		14	Should have centralized management and reporting capabilities to deliver reports like top Spywares, by category, by infected machines, by risk priority etc	https://knowledge.broadcom.com/external/article/178847	Tender conditions shall prevail
197	Technical		15	Real time Active protection on memory, process termination / file removal of pests in active memory	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/sescloud/Protection/managing-memory-exploit-mitigation-mem-policies-v123103490-d4155e23348.html	Tender conditions shall prevail
198	Technical		16	The proposed solution should have an ability to create custom expert rule to prevent sophisticated attacks. The custom rule configuration should have coverage for syntax to protect files, protect process, product registry, buffer overflow, illegal API use, protect services.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/what-is-v45096464-d43e1648/how-symantec-endpoint-protection-technologies-prot-v97539434-d43e1669.html	Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
199	Technical		17	Should have centralized update/download mechanism which should be able to download details of latest Spywares and push the same across all the desktops	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/symantec-endpoint-protection-client-for-mac-help/updating-virus-definitions-intrusion-prevention-de-v40556228-d35e585.html	Tender conditions shall prevail
200	Technical		18	The solution must be able to auto-quarantine or auto-delete spyware or adware without end-user interaction. The administrator should be able to restore an endpoint back from quarantine using central management.	https://knowledge.broadcom.com/external/article/151677/managed-quarantined-files-with-endpoint.html	Tender conditions shall prevail
201	Technical		19	The administrator should have option to rescan a quarantined endpoint to make sure that the infection has been removed.	https://knowledge.broadcom.com/external/article/151677/managed-quarantined-files-with-endpoint.html	Tender conditions shall prevail
202	Technical		20	Browser Security : Should Support Internet Explorer ,Mozilla Firefox and Chrome	https://knowledge.broadcom.com/external/article/155401/supported-browsers-for-browser-intrusion.html	Tender conditions shall prevail
203	Technical		21	Proposed solution should have integrated URL categorization feature	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-intrusion-prevention-v36820771-d53e8657/Integrating-browser-extensions-with-Symantec-Endpoint-Protection.html	Tender conditions shall prevail
204	Technical		22	Proposed solution should categories URLs for threats like – Spywares, Trojans, Spam, Adware etc	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-intrusion-prevention-v36820771-d53e8657.html	Tender conditions shall prevail
205	Technical		23	Solution URL category module should provide end user detail threat information about the site	https://knowledge.broadcom.com/external/article/176256/using-symsubmit-for-symantec-and-carbon.html	Tender conditions shall prevail
206	Technical		24	Should be able to update definitions & scan engine on the fly, without a need for reboot or stopping of services on servers.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/how-to-update-content-and-definitions-on-the-client-v38539566-d79e6.html	Tender conditions shall prevail
207	Technical		25	The solution should be able to determine file-execution decisions with rule-based logic based on endpoint context (file, process, and environmental attributes) blended with collective threat intelligence.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/ru10-gs-adaptive-protection/Adaptive-Protection.html	Tender conditions shall prevail
208	Technical		26	The proposed solution should be able to map the global intelligence from their own cloud with the local intelligence collected from endpoint solution proposed.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/preventing-and-handling-virus-and-spyware-attacks-v40739565-d49e172/how-uses-symantec-insight-to-make-decisions-about-v45204303-d49e3040.html#:~:text=By%20default%2C%20a%20client%20computer,submissions%20for%20reputation%20detections%20enabled.	Tender conditions shall prevail
209	Technical		27	The proposed endpoint protection solution should be able to integrate with third party feeds such as Virus Total in the same endpoint management console.	Virus Total can be used as reference but cannot be integrated hence we request you to remove this clause.	ok for removal
210	Technical		28	The proposed endpoint protection solution should be able to import threat reputation of files through file hashes into the central endpoint protection management solution.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/exceptions-v8093021-d51e2316/file-access-exception.html	Tender conditions shall prevail
211	Technical		29	The proposed endpoint solution should be able to automatically prevent the execution of even unknown executable files even if the endpoint does not have the latest signatures and without heuristics or behavioral patterns.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-sonar-v40139626-d47e6/about-sonar-v44010692-d47e487.html#:~:text=Behavioral%20analysis%20uses%20heuristics%20to,More%20information	Tender conditions shall prevail
212	Technical		30	Should not block just on file hashes but on certificate bases also such that only trusted certificates are allowed to execute.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Using-Adaptive-Protection/behavioral-application-isolation-policy-settings-v135293970-d4155e40071.html	Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
213	Technical		31	The solution should provide an Integrated firewall which should use reputation scores based on vendors global threat intelligence to protect endpoints from botnets, DDoS, APTs, and suspicious web connections.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-intrusion-prevention-v36820771-d53e8657.html#v36820771	Tender conditions shall prevail
214	Technical		32	The proposed solution should provide an option for the administrator to pick and choose the protection modules they want for their endpoints based on their system type and environment.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Policies-and-Policy-Groups/creating-and-applying-policy-groups-v123653692-d4155e12595.html	Tender conditions shall prevail
215	Technical		33	The solution should have an integrated endpoint-assisted security installation (EASI) installer to offer an accelerated and simplified deployment process.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Managing-a-custom-installation/preparing-for-client-installation-v16742985-d21e7/choosing-a-method-to-install-the-client-using-the-v17080435-d21e721.html	Tender conditions shall prevail
216	Technical		34	The proposed endpoint security solution should be able to undertake pre-execution analysis for unknown malware while performing Static file feature extraction (for example file type, import hash, entry point, resources, strings, packer & compiler details, compile time, API's, section names etc.)		Tender conditions shall prevail
217	Technical		35	The proposed endpoint security solution should be able to undertake Post-execution analysis for unknown malware while performing Behavioral features and Memory analysis (for example behavioral sequence, process tree, file system, registry events, network communication events, mutex, strings from memory etc.)		Tender Conditions remain unchanged
218	Technical		36	The proposed endpoint security solution should Extract static file feature for classification by using an machine learning model that resides on endpoint and the Static feature based detection should not require cloud lookups.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/preventing-and-handling-virus-and-spyware-attacks-v40739565-d49e172/how-does-use-advanced-machine-learning-v120625733-d47e275.html#:~:text=The%20advanced%20machine%20learning%20(AML,Insight%20lookups%20for%20threat%20detection,	Tender conditions shall prevail
219	Technical		37	The solution should be able to inspects all data that flows between the client system and the network. It should compare the network data with the known network-based attacks	https://knowledge.broadcom.com/external/article/155064/endpoint-protection-network-threat-prote.html#:~:text=Virus%20and%20Spyware%20threat%20protection,meet%20the%20specified%20security%20criteria.&text=Firewall%20policies%20consist%20of%20one,Stealth%20Settings	Tender conditions shall prevail
220	Technical		38	It should support desktop firewall capabilities to directly block unwanted traffic	https://knowledge.broadcom.com/external/article/155064/endpoint-protection-network-threat-prote.html#:~:text=Virus%20and%20Spyware%20threat%20protection,meet%20the%20specified%20security%20criteria.&text=Firewall%20policies%20consist%20of%20one,Stealth%20Settings	Tender conditions shall prevail
221	Technical		39	HIPS solution should provide facility to create different policy for different network connectivity like – LAN, DHCP.	https://knowledge.broadcom.com/external/article/178049/location-awareness-best-practices-for-en.html	Tender conditions shall prevail
222	Technical		40	Solution should provide facility to create User defined signatures	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-intrusion-prevention-v36820771-d53e8657/managing-custom-intrusion-prevention-signatures-v37711224-d53e8845/creating-a-custom-ips-library-v38553637-d53e9900.html	Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
223	Technical		41	Solution should prevent buffer overflow, illegal API use, and network exploits.	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/hardening-windows-clients-against-memory-tampering-v123149922-d3859e12879/memory-exploit-mitigation-techniques-v114221375-d53e13441.html#:~:text=The%20HeapSpray%20technique%20reserves%20the.host%20name%20might%20be%20different.	Tender conditions shall prevail
224	Technical		42	The solution should intercept and scan Javascripts and VBScripts before they are executed. The solution should also be able to create URL exclusion for certain in-house/known sites from this scan process.		Tender conditions shall prevail
225	Technical		43	The proposed solution should have system rollback feature in case system is compromised with the advanced malware attack. Rollback remediation should monitor the behavior of unknown processes and backs up changes that they make to the system. If a monitored process exhibits malicious behavior, enhanced remediation stops the process, its children, and ancestors, and rolls back the changes that it made, restoring the system as close as possible to its original state before the process ran.	Rollback feature is not available. Symantec predominantly focus on pre-breach technologies rather post-breach.	Tender conditions shall prevail
226	Technical			Device Control for Desktops/Laptops/Servers/Storage		This is required
227	Technical		1	The solution should potentially block the end point system from loading physical devices such as removable storage devices, Bluetooth, Wi-Fi, and other plug and play devices based on device classes and device definitions are used to define device rules		Tender conditions shall prevail
228	Technical		2	It should support device management and should allow you to Monitor, Block or make the device Read-Only along with the option of providing exceptions		Tender conditions shall prevail
229	Technical		3	It should support for detecting attempts to copy confidential data to removable storage devices (e.g. USB drives, floppy, CD/DVD, etc.).	Symantec DLP holds capability.	ok for removal
230	Technical		4	It should support for blocking Windows native CD writing and other CD writing software. The block must inform the user that the action is being blocked.		ok for removal
231	Technical		5	It should support for customizable notification "pop-up" messages		Tender conditions shall prevail
232	Technical		6	It should be able to control the access of USB devices by using their vendor ID, product ID or serial number, along with time based USB access.		Tender conditions shall prevail
233	Technical		7	The solution installation, policy management and reporting should be handled by an integrated endpoint agent on the client.		Tender conditions shall prevail
234	Technical		8	The solution should provide near real-time event monitor allowing you to see events as they happen, view details (user, machine, rules triggered, etc), and even access evidence files as the events happen in your environment.		Tender conditions shall prevail
235	Technical		9	It should support ability to restrict access to company approved devices, but also if necessary to permit exclusions to this requirement. Exception and/or exclusions can be designed to accommodate different devices or different groups of users		Tender conditions shall prevail
236	Technical		10	It should provide the functionality of logging and audit-trail capabilities		Tender conditions shall prevail
237	Technical			Management Platform		Tender conditions shall prevail
238	Technical		1	Should have a Centralized Management Console for managing Antivirus, Antispyware, device control		Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
239	Technical		2	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.		Tender conditions shall prevail
240	Technical		3	It should support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet of machines or a particular site		Tender conditions shall prevail
241	Technical		4	Central management console should provide actionable reports and customized Reports as per requirement for Audit and internal reporting purpose		Tender conditions shall prevail
242	Technical		5	Central management console should support granular role based access control	https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/managing-groups-clients-and-administrators/managing-administrator-accounts-v17364367-d1e6/about-administrator-accounts-and-access-rights-v9542187-d1e204.html	Tender conditions shall prevail
243	Technical		6	Should ensure security policy enforcement by integrating and centralizing installation, deployment, management & updating		Tender conditions shall prevail
244	Technical		7	Centralized management server should be able to automatically report about the new unprotected systems. Also it should have centralized management tagging mechanism to identify the system with no agent and to run automated agent deployment task if system found as unmanaged.		Tender conditions shall prevail
245	Technical		8	Solution should provide for custom reports and queries along with role-based access providing different levels of dash-boarding and relevant reports to users.	Reports in dashboard is not available. Customer can export reports and work on dashboard view using 3rd party tool.	Tender conditions shall prevail
246	Technical		9	Solutions should provide near real-time event monitor allowing you to see events as they happen, view details (user, machine, rules triggered, etc), and even access evidence files as the events happen in your environment.		This is required
247	Technical		10	The proposed management server deployment mechanism should have dedicated components as distributed repository for bandwidth management.		Tender conditions shall prevail
248	Technical		11	Solutions should support report customization and allow viewing directly using a web browser and also as a dashboard using the same management console for the endpoints.		Tender conditions shall prevail
249	Technical		12	Solution should supports the following formats for exporting data: CSV, HTML, XML, Acrobat PDF,		Tender conditions shall prevail
250	Technical		13	Solution should support ability to restrict access to company approved devices, but also if necessary to permit exclusions to this requirement. Exception and/or exclusions can be designed to accommodate different devices or different groups of users		Tender conditions shall prevail
251	Technical		14	Solution should provide the functionality of events being viewed, filtered, and sorted in the Management console, allowing security officers or administrators to view events and respond quickly. If applicable, suspicious content is attached as evidence to the event.		Tender conditions shall prevail
252	Technical		15	Solution should provide the functionality of logging and audit-trail capabilities.		Tender conditions shall prevail
253	Technical		16	Solution should provide the capability to log administrative activities in the Management console. Administrative activities that are logged in the Management console include, changes to policies, deployment of policies, agent override activities, agent termination, and agent uninstall key generation.		Tender conditions shall prevail
254	Technical			Premium Support		Tender conditions shall prevail
255	Technical		1	The solution should be proposed with 24x7 email and telephonic support with the standard licensing. The same should be certified by OEM with relevant documents.		Tender conditions shall prevail

PROCUREMENT OF ANTIVIRUS IN BRPL

PRE BID QUERIES

S.NO	Query Type Technical / Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL Replies
256	Technical		2	The OEM should provide a utility to collect product and system information to assist Support in diagnosing issues		Tender conditions shall prevail
257	Technical		3	Product upgrades should be easily be downloadable from the OEM Official Website		Tender conditions shall prevail
258	Technical		4	The OEM should provide a service which delivers the latest OEM product information by email — patch and upgrade notification; and critical alerts that require immediate attention.		Tender conditions shall prevail
259	Technical		5	During warranty period the software must be covered with necessary minor or major upgrades (Software support and upgrade-Major i.e. Version and minor too)		Tender conditions shall prevail
260	Technical		6	The bidder/OEM must ensure that their team is available on a high-priority basis to promptly resolve any cybersecurity attack on BRPL throughout the contract period. The bidder shall provide 24/7 support and immediate incident response to mitigate threats and minimize operational disruptions		Tender conditions shall prevail
261	Technical		7	All points covered under Scope of Work ,section Service and Deliverables		Tender conditions shall prevail
262	Technical			INTEGRATION		Tender conditions shall prevail
263	Technical		1	Solution should support end point protection and device control (SOAR for Outgoing Control)		Tender conditions shall prevail
264	Technical		2	Solution should have file integrity monitoring	Symantec DCS holds capability.	Tender conditions shall prevail
265	Technical		3	Proposed solution should be capable of deployable on a virtual appliance using Enterprise hypervisor solutions		This is required
266	Technical		4	Solution must be able to auto-quarantine or auto-delete spyware, Malware, Adware. The administrator should be able to restore an endpoint back from quarantine using central management.		Tender conditions shall prevail
267	Technical		5	Solutions should provide near real-time event monitor of events with, view details (user, machine, rules triggered, etc), and even access evidence files as the events.		Tender conditions shall prevail
268	Technical		6	The solution must have Integration with SIEM and other security solution for log collection through API integration		Tender conditions shall prevail