Clause in RFP

Sr No.	Clause in RFP	Clarifications/ Changes made
1.	**[A] Important Dates:** Last Date of Submission of RFP Response (Closing Date) 03:00 PM on 04-04-2022 Eligibility and Technical Bid Opening Date 03:30 PM on 04-04-2022	**[A] Important Dates:** Last Date of Submission of RFP Response (Closing Date) **03:00 PM on 18-04-2022** Eligibility and Technical Bid Opening Date **03:30 PM on 18-04-2022**
2	**Annexure 02 - Evaluation Terms** **Eligibility cum Technical Bid** **B. Financial** The OSD must have registered average annual turnover of Rs. 100 Crores or above (from Indian Operations only) during the last three completed financial years – 2018-19, 2019-20 and 2020-21* (Not inclusive of the turnover of associate companies) The OSD must be net profit (after tax) making entity (from Indian operations only) continuously for the last three completed financial years – 2018-19, 2019-20 and 2020-21	**Annexure 02 - Evaluation Terms** **Eligibility cum Technical Bid** **B. Financial** The OSD must have registered average annual turnover of Rs. 100 Crores or above ~~**(from Indian Operations only)**~~ during the last three completed financial years – 2018-19, 2019-20 and 2020-21* (Not inclusive of the turnover of associate companies) The OSD must be net profit (after tax) making entity ~~**(from Indian operations only)**~~ continuously for the last three completed financial years – 2018-19, 2019-20 and 2020-21
8	**Annexure 02 - Evaluation Terms** **B. Technical Bid Evaluation** Number of implementations carried out (in the last 3 years starting from date of RFP) ** For each Implementation 3 marks -- Maximum 15 Marks	**Annexure 02 - Evaluation Terms** **B. Technical Bid Evaluation** Number of implementations carried out (in the last 3 years starting from date of RFP) ** For each Implementation **5 marks** -- Maximum 15 Marks
9	**Annexure 02 - Evaluation Terms** **Eligibility cum Technical Bid** **C. Experience and Support Infrastructure** The proposed OSD's server security solution should be successfully implemented in minimum two organization across 1,000 servers for each organization in Commercial Banks / Financial Institutions / Govt. Organizations in India in last 3 years (as on RFP date)	**Annexure 02 - Evaluation Terms** **Eligibility cum Technical Bid** **C. Experience and Support Infrastructure** The proposed OSD's server security solution should be successfully implemented in minimum two organization across **600** servers for each organization in Commercial Banks / Financial Institutions / Govt. Organizations in India in last 3 years (as on RFP date)

Sr No.	Clause in RFP	Clarifications/ Changes made
11	**Anexure 10 | Letter of Undertaking from OEM** We …… (Name of the OSD / OEM) who are established and reputable manufacturers / developers of …… having factories at ……, …… and …… do hereby authorize M/s …… (who is the Bidder submitting its bid pursuant to the Request for Proposal issued by the Bank) to submit a Bid and negotiate and conclude a contract with you for supply of ……	**Anexure 10 | Letter of Undertaking from OEM** We …… (Name of the OSD / OEM) who are established and reputable manufacturers / developers of …… having **development centers** at ……, …… and …… do hereby authorize M/s …… (who is the Bidder submitting its bid pursuant to the Request for Proposal issued by the Bank) to submit a Bid and negotiate and conclude a contract with you for supply of ……
	Annexure 02 - Evaluation Terms Eligibility cum Technical Bid **D. Others** Bidder must ensure that the proposed security solution to be supplied will not be End of Life/ Sale in next 3 years and End of Support in next 5 years	**Annexure 02 - Evaluation Terms Eligibility cum Technical Bid** **D. Others** Bidder must ensure that the proposed security solution to be supplied will not be ~~**End of Life/ Sale in next 3 years and**~~ End of Support in next 5 years.

All other Terms & Conditions are same as per our RFP No. BCC:IT:PROC:114:08 dated 07-03-2022 for Supply, Implementation and Maintenance of Server Security Solution for a period of 5 Years

Addendum to following Annexures

1. Annexure 12 – Project Details Scope of Work
2. Annexure 14 – Masked Commercial Bid
3. Annexure 15 – Commercial Bid

Annexure 12 – Project Details Scope of Work

1. Project Scope

Bank will award the contract to the successful bidder and the bidder should Supply, Implementation and Maintenance of Server Security Solution for a period of 5 Years as per the scope briefed in this RFP.

The Bidder shall perform the following tasks as per Bank requirement and satisfaction as per this RFP, but not limited to:

a) Supply, Implementation and Maintenance of Server Security Solution

b) Acceptance Testing

c) Certification from OEM

d) Training/Handholding

e) Handover to Bank/Managed Service Provider (MSP) with full functionality and technical knowledge transfer to Bank & MSP

f) Completion Schedule, Warranty, AMC and Service Support of Supply, Implementation and Maintenance of Server Security Solution for a period of 5 Years through MSP as part of Warranty and Annual Maintenance Contract

Description of the envisaged scope is enumerated as part of this Annexure however the Bank reserves its right to change the scope of work considering the size and variety of the requirements and the changing business conditions.

Considering the enormity of the assignment, any service which forms a part of the Project Scope that is not explicitly mentioned in scope of work as excluded would form part of this RFP, and the Bidder is expected to provide the same at no additional cost to the Bank. The Bidder needs to consider and envisage all services that would be required in the Scope and ensure the same is delivered to the Bank. The Bank will not accept any plea of the Bidder at a later date for omission of services on the pretext that the same was not explicitly mentioned in the RFP.

2. Requirement Background

Traditional perimeter-based security models severely lacked the capability to extend unit level protection to data center workloads to keep up with the dynamic threat landscape. To get sufficient visibility into east-west traffic, malware makes its way into the data center, there is little control to block and isolate the attack inside the data center. Additionally, manual security configuration and vulnerability patching remains biggest areas of exposure for corporations as hackers are quick to exploit any holes they can find. And the dynamic nature of today's data centers makes keeping up with basic security even more difficult as workloads are spun up and down and security policies have to be moved or reconfigured with the workloads. As more and more workloads transition from physical infrastructure to the private cloud, the software-defined data center is demanding opportunity for security and automation.

The objective is to implement a robust enterprise-wide server security solution providing a broad range of threat defense techniques to address the evolving threat landscape and compliance guidelines that helps bank to identify, detect and secure the server infrastructure from current and future cyber-attacks and subsequently enhance the operational efficiency & security posture of the bank.

3. Brief Scope of Work

The solution should be deployed in banks DC/DR setup and should strictly not be cloud based. The solution shall provide a centralized architecture with a single agent to deliver the licensed security modules. Additionally, the agent installation and configuration changes shall not require reboot of the protected servers for operational efficiency. The solution should support the most widely used server OS platforms which includes Microsoft Windows and non-Windows platform like Linux (Red Hat, Suse, Rocky, Alma, Ubuntu, Cent OS, Oracle, Debian), Solaris, AIX, ~~**HP-Unix**~~, Atalla Key Block, ESXi, Guardian, OVF etc. The solution shall have provision to provide protection against the vulnerabilities exploited by the threat actors. The solution should be managed from a centralized management console and provide capability to monitor, report and configuration related task of the solution for the protected target servers.

The SOW includes (but not limited to) the overview of tasks to establish protection that is best suited for banks environment, sane is mentioned here:

- Operating system (OS) and databases licenses for the solution deployment will be provided by the bank whereas availability of necessary licensed security modules of the proposed server security solution to be provided by bidder.
- Sizing of solution to be done on the basis of server count and feature requirements as stated by the bank, an UAT is suggested to test and validate the solution functionality.
- The solution should be designed in such a way that it covers the current and future scalability as stated in the solution requirement.
- All the patches/versions/upgrades/ should be applied as and when released by the OEM.
- Compatibility of server OS platforms to be verified as per the OEM's official documentation portal.
- Software packages to be offered should be legally valid, licensed and latest version along with the complete set of manuals along with the media.
- OEM will share their generalized APIs with the Bank so that existing as well as future solutions can be integrated without any additional cost to the bank.
- Solution to be deployed and configured as per the best recommendation practices provided by the OEM.
- Solution deployment to be done required feature functionality, performance on a few selective server's during the install phase before rolling out into production. The full testing will be based on the mutually agreed criteria.
- Any performance issue observed during deployment/implementation or new feature requests shall be treated as a regular incident and will be subject to OEM's support review and assistance.

4. Implementation scope of bidder

This section of document describes the overall work that has to be done in regards to the deployment and implementation of server security solution in the bank's environment.

- The selected bidder shall be required to understand the proposed solution and based on requirements specified in the RFP and it's understanding, shall propose and submit the approach document explaining in detail the solution architecture (physical and logical), its integration with the other solutions of the Bank, management & monitoring of the solution, and project plan with timelines.

- The Bidder has to develop the project plan, get it approved by the Bank and then implement the project based on timelines agreed.
- The solution's architecture deployment & configurations done at the Bank should be vetted by OEM before sign-Off from Bank. In solution design the security best practices should be taken care of by design team.
- The bidder shall commence the implementation of the solution only after the acceptance of the proposal by the Bank.
- The Bidder shall be responsible for preparation and updating (periodically or as and when there are considerable changes) of all the documents pertaining to the solution including (but not limited to) the following:
  - ✓ Logical and physical architecture of the solution
  - ✓ Low & High-Level Design
  - ✓ Standard Operating Procedure (SOP) for various activities pertaining to the management and configuration of the Solution
  - ✓ User and Administrator Guide/manual
  - ✓ Installation & Configuration Documents
  - ✓ Administrative guide / manuals of all proposed solution
- All the above documents (soft copy or hard copy) should be provided by the bidder, vetted by the bank, suggestions incorporated by bidder and then provided to the Bank.
- The Bidder shall ensure that during various phases of implementation of the solution and during the contract period, the performance, security, etc. of the existing setup/network shall not be compromised.
- Bidder would be responsible for all technical support to maintain the required uptime. Initial installation, configuration and integration should be done by the Bidder. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required onsite support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support.
- The bidder will maintain enough provisions of additional manpower for managing the absence of any resources due to whatsoever reasons. (Like company policy, work-hour limitations, leave, sickness, recess, interval, training, etc.).
- The bidder should arrange OEM audit post deployment and submit report after the completion of deployment by the bidder and co-ordinate with OEM to assist in fixing any gaps in the deployment found out during the audit.

5. Implementation steps

Following are the procedural steps to be followed for the planning the implementation and maximize the overall solution efficacy:

- Based on the approved solution design & architecture ensure that the necessary prerequisites like network access, rights & permissions and environmental data (like server inventory, point of contact etc.) are ready with required approvals (if any).
- Plan and install the solution components and perform the necessary configuration as per the recommended best practices.
- Validate the security modules are licensed as per the requirement and verify compatible platforms and supported features as per the OEM's official documentation portal.

- Check and confirm for existence of any non-compatible software's like AV, uninstall them if required.
- Finalize the deployment methodology of the agents like manual, script based etc. Confirm and validate the agent connectivity and its activation status with management console.
- Perform the mutually agreed use cases, monitor the console dashboard / events to verify the enabled security modules working status.
- Fine tune the configuration if required based on the results achieved in above step
- UAT sign-off from the bank for selective servers.
- Plan the production roll out in banks environment which includes activities like inventory list, compatibility, downtime if required etc.
- Perform any additional integration task (ex. with SIEM) if required by the bank.
- Generate / Schedule reports as per the bank's requirement.

6. Functional and Technical scoring sheet

Functional & technical scoring will be evaluated on following criteria as part of technical evaluation. **Bank reserve the right to conduct the onsite POC of proposed solution as a part of technical evaluation in UAT/Live environment. Bank Team may ask to demonstrate all or specific capabilities as per compliance sheet. Bidder/OEM have to arrange POC & License of proposed solution. If Bidder/OEM fails to demonstrate such features, Bank may technically disqualify such Bidder/OEM.**

- Requirement available as part of solution (RA) – 2 Marks
- Requirement will be provided as customization (RC) – 1.5 Marks
- Requirement is feasible and to be developed (RD) – 1 Mark

Total Marking will proportionate to 50 marks and accordingly bidders "Product Demo" marks will be calculated

S. No.	General Requirement	Marking as per RA/ RC/ RD	Bidders Remarks
1	The proposed server security solution should consolidate multiple security controls including anti-malware, stateful Inspection firewall, ~~**Deep Packet Inspection with HIPS**~~, Integrity Monitoring, Application Control, ~~**and Log inspection features**~~ to ensure optimal security and compliance for critical servers.		
2	The proposed server security solution must support multiple platforms of server operating systems i.e. Windows **&** Non Windows **both** (i.e. Linux RedHat, Suse, ~~**Rocky, Alma,**~~ Ubuntu, CentOS, Oracle, Debian, ~~**Amazon Cloud**~~ , Solaris, AIX, **VMware/ESX** etc)		
3	All feature modules i.e. Anti-malware, HIPS, Firewall, Application control, FIM, Log correlation, ~~**C&C**~~ **threat** prevention must be delivered in single unified agent managed through a web based centralized management console.		

4	The solution should offer protection for physical as well as virtual instances.		
5	The proposed solution must support Anti-malware, HIPS, Integrity Monitoring, Host Firewall **etc** for the below mentioned server operating system: ✓ Microsoft Windows Server **2012 & above ~~2008 & 2008 R2, 2012 & 2012 R2, 2016, 2019, 2022~~** ✓ RHEL 6 **& above~~,7,8~~** ✓ CentOS 6 **& above~~,7,8~~** ✓ **~~Alma Linux 8~~** ✓ **~~Rocky Linux 8~~** ✓ Ubuntu 16 **& above~~,18,20~~** ✓ Debian 8 **& above~~, 9,10~~** ✓ Oracle Linux 6 **& above~~,7,8~~** ✓ SUSE Linux 12 **& above~~,15~~** ✓ Solaris 10 **& above~~,11.0, 11.1,11.2,11.3,11.4~~** ✓ AIX 6.1 **& above~~, 7.1, 7.2~~** ✓ **~~HP-Unix all versions~~**		
6	The proposed solution installation of agent should not require a restart of the server. Also, any changes in policy and configuration should not require server restart/reboot.		
7	The proposed solution should support new Linux kernels as & when they are released.		
~~8~~	**~~Bank reserve the right to conduct the onsite POC of proposed solution as a part of technical evaluation in UAT/Live environment. Bank Team may ask to demonstrate all or specific capabilities as per compliance sheet. Bidder/OEM have to arrange POC & License of proposed solution. If Bidder/OEM fails to demonstrate such features, Bank may technically disqualify such Bidder/OEM.~~**		
Host Based Firewall			
9	The solution should support stateful inspection firewalling functionality.		
~~10~~	**~~The solution should have ability to run internal port scan on individual servers to know the open ports and will help administrator create rules.~~**		
11	The solution should have Security Profiles **which** allows Firewall rules to be configured for groups of systems, or individual systems.		
12	The solution should provide policy inheritance exception capabilities.		

13	The solution should provision inclusion of packet data on event trigger for forensic purposes.		
14	The firewall shall be bidirectional for controlling both inbound and outbound traffic.		
15	The firewall shall have the capability to define different rules to different network interfaces.		
16	The firewall rules should filter traffic based on source and destination IP address, port, MAC address, direction etc.		
~~**17**~~	~~**Firewall should detect reconnaissance activities such as port scans without any firewall rules.**~~		
18	Firewall rules should be able to support different actions for rules like Allow, Bypass, Deny, Force allow, Log Only.		
19	The firewall should be able to detect protocol violations of standard protocols.		
Host Based IPS			
20	The proposed solution should support Deep Packet Inspection (HIPS/IDS) **or equivalent solution.**		
21	Deep packet Inspection **or equivalent solution** should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.		
22	Deep Packet Inspection **or equivalent solution** should support virtual patching of both known and unknown vulnerabilities until the next scheduled maintenance window.		
23	Deep Packet Inspection **or equivalent solution** should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities).		
24	Deep Packet Inspection **or equivalent solution** should have pre-built rules to provide broad protection and low-level insight, for servers. For operating systems and applications, the rules limit variations of traffic, limiting the ability of attackers to exploit possible attack vectors. Generic rules are also used to protect web applications (commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting.		
25	Deep packet inspection **or equivalent solution** should have signatures to control based on application traffic. These rules provide increased visibility into & control over the applications that are		

	accessing the network. These rules will be used to identify malicious software accessing the network.		
~~**26**~~	~~**Virtual Patching should be achieved by using a high-performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.**~~		
27	Solution should provide ability to automate rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (eg. Selecting rules, configuring policies, updating policies, etc)		
28	Solution should support creation of customized DPI rules **or equivalent solution** if required.		
~~**29**~~	~~**Solution should have capability to provide recommendation for removing assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.**~~		
~~**30**~~	~~**The proposed solution should allow imposing HTTP Header length restrictions.**~~		
31	The proposed solution shall have the capability to inspect and block attacks that happen over SSL.		
32	The proposed solution should allow or block resources that are allowed to be transmitted over http or https connections.		
33	Detailed events data to provide valuable information, including the source of the attack, the time and what the potential intruder was attempting to exploit, shall be logged.		
34	Solution should be capable of blocking and detecting of IPv6 attacks.		
35	Solution should offer protection for virtual, physical, ~~**cloud and**~~ Docker container environments.		
36	Solution should work in Tap/detect only mode and prevent mode.		
37	Solution should support automatic and manual tagging of events.		
38	Solution should provision inclusion of packet data on event trigger for forensic purposes.		
39	The solution should support CVE cross referencing **or signature less protection for known and un-known vulnerabilities** when applicable.		
40	The proposed solution shall protect against fragmented attacks		
41	The proposed solution should allow to block based on thresholds		
~~**42**~~	~~**The solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all**~~		

	~~**Windows/ Non Windows (i.e. Linux RedHat, Suse, Rocky, Alma, Ubuntu, CentOS, Oracle, Debian, Amazon Cloud , Solaris, AIX etc) servers use the same base security profile allowing further fine tuning if required. Rules should be auto-Provisioned based on Server Posture. De-provisioning of rules should also be automatic if the vulnerability no longer exists.**~~		
Integrity Monitoring			
43	Integrity Monitoring module should be capable of monitoring critical operating system and application elements like files, directories, and registry keys and values, installed software, processes, listening ports, and running services to detect suspicious behaviour such as modifications or changes in ownership or permissions.		
44	The solution should be able to monitor system Services, installed programs and running Processes for any changes.		
45	The solution should support creation of baseline to identify the original secure state of the monitored server to be compared against changes.		
46	The solution should have extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc).		
47	The solution should be able to track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored.		
48	The solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.		
49	The solution should have automated recommendation **or equivalent technology** for ~~**of**~~ integrity rules to be applied as per Server OS and can be scheduled for assignment/un-assignment when not required.		
50	The solution should have by default Rules acting at Indicators of Attacks detecting suspicious/malicious activities.		
51	In the event of unauthorized file change, the proposed solution shall report reason, who made the change, how they made it and precisely when they did so.		
52	The solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Windows/ Non Windows ~~**(i.e. Linux RedHat, Suse, Rocky, Alma, Ubuntu, CentOS,**~~		

	~~Oracle, Debian, Amazon Cloud , Solaris, AIX etc)~~ servers use the same base security profile allowing further fine tuning if required. Rules should be auto-Provisioned based on Server Posture.		
53	The solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.		
54	The solution should support the following: • Multiple groups of hosts with identical parameters • Regex or similar rules to define what to monitor • Any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc) • Ability to apply a host template based on a regex of the hostname • Ability to exclude some monitoring parameters if they are not required • Ability to generate E Mail and SNMP alerts in case of any changes • Creation/Import of custom rules.		
55	The solution must support real time as well as schedule integrity monitoring based on operating system.		
Anti-malware			
56	Anti-malware should support Real Time, Manual and Schedule scan.		
57	The solution should have flexibility to configure different real time and schedule scan times for different servers.		
58	The solution should support excluding certain file, directories, file extensions from scanning (real-time/schedule).		
59	The solution should use a combination of cloud-based threat intelligence combined with traditional endpoint security technologies.		
60	The solution should support True File Type Detection, File extension checking.		
61	The solution should support heuristic technology blocking files containing real-time compressed executable code.		
62	The proposed solution should be able to detect and prevent the advanced threats which come through executable files, PDF files, Flash files, RTF files and and/or other objects using Machine learning		
63	The proposed solution should be able to perform behaviour analysis for advanced threat prevention		

64	The solution should have its own threat intelligence portal for further investigation, understanding and remediation an attack.		
65	The solution deployment should cause limited interruption to the current network environment.		
66	The solution should have Highly Accurate machine learning analysis, document exploit prevention to address known/Unknown threats. Additionally, allows ability to specify custom actions for behaviour Monitoring and Machine Learning.		
67	The solution should have ransomware Protection in Behaviour Monitoring.		
68	The solution should have feature to try & backup ransomware encrypted files and restoring the same as well.		
Log Analysis and Co-relation			
69	The solution should have a Log Inspection module **or equivalent technology** which provides the ability to collect and analyze operating system, databases and applications logs for security events.		
70	The solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow creation of custom ~~**log inspection**~~ rules ~~**as well**~~.		
71	The solution must have an option of automatic recommendation of rules for log analysis module as per the OS platform and can be scheduled for automatic assignment/un-assignment of rules when not required.		
~~**72**~~	~~**The solution should have Security Profiles allowing Log Inspection rules to be configured for groups of systems, or individual systems. eg. All Windows/Non Windows (i.e. Linux RedHat, Suse, Rocky, Alma, Ubuntu, CentOS, Oracle, Debian, Amazon Cloud , Solaris, AIX etc) servers use the same base security profile allowing further fine tuning if required.**~~		
73	The solution should have ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving.		
~~**74**~~	~~**Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.**~~		
75	Customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered on a match.		
~~**76**~~	~~**Ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.**~~		

77	The solution must support decoders for parsing the log files being monitored.		
Application Control			
78	The solution should allow administrators to control what has changed on the server compared to initial state.		
79	The solution should have ability to scan for an inventory of installed software & create an initial local ruleset.		
80	Change or new software should be identified based on File name, path, time stamp, permission, file contents etc.		
81	The solution must have ability to enable maintenance mode during updates or upgrades for predefined time period.		
82	The solution should have option to allow to install new software or update by setting up maintenance mode.		
83	Logging of all software changes except when the module is in maintenance mode.		
~~84~~	~~Should support Windows & Non Windows (i.e. Linux RedHat, Suse, Rocky, Alma, Ubuntu, CentOS, Oracle, Debian, Amazon Cloud , Solaris, AIX etc) operating systems.~~		
85	Should have the ability to enforce either Block or Allow unrecognized software.		
86	The solution must support lockdown mode: No software is allowed to be installed except what is detected during agent installation.		
87	The solution must support global blocking on the basis of Hashes and create blacklist for the environment.		
Command & Control Prevention			
88	The solution must be able to block all communication to Command & control centre.		
89	The solution must be able to identify communication over HTTP/HTTPS protocols and commonly used Http ports.		
90	The solution must provide by default security levels i.e. High, Medium & low so that it eases the operational effort and The solution must have an option of assessment mode only so that URLs are not blocked but logged.		
91	The solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list of allowed/blocked URL's.		
Management and Reporting Features			
92	The proposed solution should be managed from a single centralized web-based management console.		

93	The management server of proposed solution should support both Windows and Non Windows ~~**(i.e. Linux RedHat, Suse, Rocky, Alma, Ubuntu, CentOS, Oracle, Debian, Amazon Cloud , Solaris, AIX etc)**~~ operating system.		
94	The management server should support Active Passive high availability configuration for DC/DR setup.		
95	The management console must support API integration to automate the operational tasks to increase the productivity and improving the security services.		
96	The management console provides the ability to create deployment scripts to ease the task of the security agent deployment.		
97	The management console should allow to define bypass rules to ignore scanning traffic from known VA scanners like Qualys or Nessus.		
98	In case of any module is expired or about to expire the console should automatically show alerts on the dashboard.		
99	The solution shall allow to do all configurations from the central management console like enabling/disabling agents, selecting and applying new policies, creating custom policies, reports etc.		
100	Once the policies are deployed, the agents should continue to enforce the policies whether the management server is available or not.		
101	Agent installation methods should support manual local installation, packaging with third party software distribution systems and distribution through Active Directory.		
102	Any policy updates pushed to the agent should not require to stop the agent, or to restart the system		
103	The solution should be able to automate discovery of new agents that are installed on any servers.		
104	The solution shall have the capability to disable the agents temporarily from the Central Management console & such action should be logged.		
105	The solution shall allow to do all configurations from the central management console including, but not limited to enabling/disabling agents, selecting and applying new policies, creating custom policies, reports etc.		
106	The solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the solution and who can do what within the application.		
107	Should support integration with Microsoft Active directory.		

108	The solution should allow grouping into smart folders based on specific criteria like OS, policy etc. for easy manageability.		
109	The solution should support the logging of events to a non-proprietary, industry-class database such as MS-SQL, Oracle, Postgres.		
110	The solution shall allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.		
111	The solution should support forwarding of alerts through SNMP and E Mail.		
112	The solution should be able to generate detailed and summary reports.		
113	The solution shall allow scheduling and E Mail delivery of reports.		
114	The solution shall have a customizable dashboard that allows different users to view based on their requirement.		
115	The solution should support Web Services if it is required to export data out to other custom reporting solutions.		
116	The solution shall allow creation of custom lists, such as IP Lists, MAC lists etc. that can be used in the policies that are created.		
117	Administrators should be able to selectively rollback rules applied to agents.		
118	The solution should have an override feature which would remove all the applied policies and bring the client back to default policies.		
119	The solution should maintain full audit trail of administrator's activity.		
120	The solution shall allow updates to happen over the internet, or shall allow updates to be manually imported in the central management system and then distributed to the agents. Additionally, the solution must also have an option of defining machine to be Updater relay only.		
121	Solution should have API level integration with public cloud service ~~**providers (e.g. AWS, Azure & vCloud Air etc.)**~~ from the management console.		

SERVICE LEVELS AND UPTIME GUARANTEE

For details, please refer to Annexure that provides the service levels for the Solution.

DELIVERY

All the Services / Resource(s) should be delivered within -02- months from the date of purchase order. Any deliverable has not been supplied or not operational on account of which the implementation is delayed, will be deemed/treated as non-delivery thereby excluding the Bank from all payment obligations under the terms of this contract.

Bidder will have to pay late delivery charges to Bank of Baroda @ 1% of Total Contract Value inclusive of all taxes, duties, levies etc., per week or part thereof, for late implementation beyond due date of implementation, to a maximum of 5% of total contract value. If delay exceeds beyond two weeks from due date of delivery, Bank of Baroda reserves the right to cancel the entire order.

The bidder must strictly adhere to the delivery dates or lead times identified in their proposal and as agreed by the Bank. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to the Bank, may constitute a material breach of the Bidder's performance. In the event that the Bank is forced to cancel an awarded contract (relative to this tender document) due to the Bidder's inability to meet the established delivery dates or any other reasons attributing to the bidder then that bidder will be responsible for any re-procurement costs suffered by the Bank. The liability in such an event could be limited to the differential excess amount spent by the Bank for procuring similar deliverables and services.

ANNUAL TECHNICAL SUPPORT (ATS)

ATS services needs to be provided by the successful bidder for all in-scope applications. Successful bidder needs to ensure following services as a part of ATS but not limited to:

- Product upgrades & enhancements
- Maintenance releases
- Statutory and Regulatory Updates
- Patches & bug fixes
- Updates/Upgrades/New releases/New versions need to be notified to the Bank about the same and need to be covered as part of AMC / ATS. Upgrades would include product releases to incorporate technological changes, consolidating all bug fixes, consolidating all enhancement requests made by the Bank.
- Review on yearly basis for version upgrade of in scope applications and report to bank such details in advance along with plan for version upgrade. Intimate the bank for various technology upgrades released by OEM's along with feasibility & impact analysis. Also propose migration plan for technology upgrade due to OEM releases.
- Planning and implementing version up-gradation, migration, testing of the application. In case bank engaging OEM directly for version upgrade, then the successful bidder is required to carry out Program Management Responsibilities to ensure end to end completion of the activities. Post version upgrade, successful bidder is required to manage & support the application along with the IT hardware.
- Develop / customization of in scope applications as per regulatory / statutory requirement.
- Mandates from various interchanges / information security/ enhancement / any other requirement.
- Patch management, release update and upgrade of in scope applications during the contract period, all update or upgrade needs to be done with concurrence of the Bank. The successful bidder to ensure that necessary due diligence in carried out for pre-testing before releasing to UAT (User Acceptance Test).

Technical Support Team should be well trained to effectively handle queries raised by the User. Bank will provide the Service Desk tool for call logging and SLA management.

The bidder should provide an indicative list of reports call login periodically. for example: volume of calls / per day, resolution % per day etc which come out of the box.

The technical bid should cover the support structure available for the administrators and Bank users. A brief write up to be included with regard to how the vendor proposes to address the training needs at multiple levels within the Bank. The bids should inter alia cover the time period for which they would be made available.

The price payable to the Vendor shall be inclusive of carrying out any modifications changes / upgrades to the application and other software or equipment that is required to be made in order to comply with any statutory or regulatory requirements or any industry-wide changes arising during the subsistence of the contract / agreement, and the Bank shall not pay any additional cost for the same. The Vendor needs to provide with the details about all such items considered in the RFP.

Annexure 14–Masked Commercial Bid

S. No.	Description	Total Qty	One Time Cost (OTC) (Rs.)	Year 1	Year 2	Year 3	Year 4	Year 5	Total Cost (Rs.)
1	Enterprise License Cost*	**3,550**	0.00						0.00
2	Implementation Cost	-	0.00						0.00
3	ATS (Annual Technical Support including upgradation)	-		0.00	0.00	0.00	0.00	0.00	0.00
4	Onsite Support Cost**	-		0.00	0.00	0.00	0.00	0.00	0.00
Grand Total (Rs.)									0.00

- *Enterprise License would mean - License for Bank Branches in India & International territories, RRBs, Subsidiaries and associates both domestic & international
- **Onsite Support for the solution will be 24x7 for 5 years and charges to be provided based on the manpower efforts in 3 shifts per day. The Bank has discretion to avail onsite support services and number of support engineers at person day cost given as and when required by the Bank. However, for the TCO purpose 3 person day (3 shift x 1 person) x 365 for each year will be considered. (e.g. In case Bank requires only one person then the cost considered for that person will be Onsite Support Cost provided by the bidder in their commercial divided by 3)

We abide by following terms and conditions

a. For each of the above items provided the vendor is required to provide the cost for every line item where the vendor has considered the cost in BOM.
b. The vendor needs to clearly indicate if there are any recurring costs included in the above bid and quantify the same. In the absence of this, the vendor would need to provide the same without any charge. Vendor should make no changes to the quantity.
c. If the cost for any line item is indicated as zero then it will be assumed by the Bank that the said item is provided to the Bank without any cost.
d. All Deliverables to be supplied as per RFP requirements provided in the tender

e. The Service Charges need to include all services and other requirement as mentioned in the RFP

f. The vendor has to make sure all the arithmetical calculations are accurate. Bank will not be held responsible for any incorrect calculations however for the purpose of calculation Bank will take the corrected figures / cost.

g. All prices to be in Indian Rupee (INR) only.

h. Prices quoted by the Vendor should be inclusive of all taxes, duties, levies etc. except GST which will be paid extra at actuals. The Vendor is expected to provide the GST amount and GST percentage in both the commercial and masked bids (without amounts being submitted in the technical response). There will be no price escalation for during the contract period and any extension thereof. Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected

i. Unit wise implementation must be provided by vendor. These prices would be considered for the calculation of TCO (Total Cost of Ownership). The Bank has discretion to avail any of these optional functionalities as per Bank's requirement during the contract period.

j. All Quoted Commercial Values should comprise of values only upto 2 decimal places. Bank for evaluation purpose will consider values only upto 2 decimal places for all calculations & ignore all figures beyond 2 decimal places.

Authorized Signatory
Name:
Designation:
Vendor's Corporate Name

Annexure 15–Commercial Bid

S. No.	Description	Total Qty	One Time Cost (OTC) (Rs.)	Year 1	Year 2	Year 3	Year 4	Year 5	Total Cost (Rs.)
1	Enterprise License Cost*	**3,550**	0.00	X	X	X	X	X	0.00
2	Implementation Cost	-	0.00	X	X	X	X	X	0.00
3	ATS (Annual Technical Support including upgradation)	-	X	0.00	0.00	0.00	0.00	0.00	0.00
4	Onsite Support Cost**	-	X	0.00	0.00	0.00	0.00	0.00	0.00
Grand Total (Rs.)									0.00

- *Enterprise License would mean - License for Bank Branches in India & International territories, RRBs, Subsidiaries and associates both domestic & international
- **Onsite Support for the solution will be 24x7 for 5 years and charges to be provided based on the manpower efforts in 3 shifts per day. The Bank has discretion to avail onsite support services and number of support engineers at person day cost given as and when required by the Bank. However, for the TCO purpose 3 person day (3 shift x 1 person) x 365 for each year will be considered. (e.g. In case Bank requires only one person then the cost considered for that person will be Onsite Support Cost provided by the bidder in their commercial divided by 3)

We abide by following terms and conditions

k. For each of the above items provided the vendor is required to provide the cost for every line item where the vendor has considered the cost in BOM.

l. The vendor needs to clearly indicate if there are any recurring costs included in the above bid and quantify the same. In the absence of this, the vendor would need to provide the same without any charge. Vendor should make no changes to the quantity.

m. If the cost for any line item is indicated as zero then it will be assumed by the Bank that the said item is provided to the Bank without any cost.

n. All Deliverables to be supplied as per RFP requirements provided in the tender

o. The Service Charges need to include all services and other requirement as mentioned in the RFP

p. The vendor has to make sure all the arithmetical calculations are accurate. Bank will not be held responsible for any incorrect calculations however for the purpose of calculation Bank will take the corrected figures / cost.

q. All prices to be in Indian Rupee (INR) only.

r. Prices quoted by the Vendor should be inclusive of all taxes, duties, levies etc. except GST which will be paid extra at actuals. The Vendor is expected to provide the GST amount and GST percentage in both the commercial and masked bids (without amounts being submitted in the technical response). There will be no price escalation for during the contract period and any extension thereof. Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected

s. Unit wise implementation must be provided by vendor. These prices would be considered for the calculation of TCO (Total Cost of Ownership). The Bank has discretion to avail any of these optional functionalities as per Bank's requirement during the contract period.

t. All Quoted Commercial Values should comprise of values only upto 2 decimal places. Bank for evaluation purpose will consider values only upto 2 decimal places for all calculations & ignore all figures beyond 2 decimal places.

Authorized Signatory
Name:
Designation:
Vendor's Corporate Name