S. No.	Relevant Clause of the RFP2	Query	Bank's Response
1	Annexure XVIII – Solution Compliance Statement - The proposed solution should have mechanism to host local relay server to communicate with cloud for telemetry push and updates, etc.	We understand that it's essential to have a mechanism in place to communicate with the cloud for telemetry push and updates, etc. However, this approach can conveniently be achieved either directly or via deploying a proxy server or via deploying local network relay server that endpoint can reach. Thus, we humbly request you to please amend the clause as below for making it vendor neutral and allowing a fair OEM participation: "The proposed solution should have mechanism to deploy a local network relay and proxy system to communicate with cloud for telemetry push and updates, etc."	Please be guided by RFP
2	Annexure XVIII – Solution Compliance Statement - Proposed solution should have IPv4 and IPv6 support	We humby request you to amend this clause as below for a wider OEM participation as it seems to be favouring a particular OEM: "Proposed solution should have IPv4 or IPv6 support."	Please be guided by RFP
3	Annexure XVIII – Solution Compliance Statement - The proposed solution provider (OEM) must be an active participant in the MITRE ATT&CK evaluations.	As this point is favouring a particular OEM(s) as it talks about being an active participant in the MITRE ATT&CK evaluations which only some leading global OEMs are doing. Therefore, we request you to please modify this point as below for allowing a maximum OEM participation: "The proposed solution provider (OEM) must be able to deeply integrate and map to the MITRE ATT&CK Farmework, including TTP-based detection, incident metrics, and threat categorization using ATT&CK techniques."	Kindly refer corrigendum
4	Annexure XVIII – Solution Compliance Statement - The proposed solution should offer API access to all management functionalities and data. The APIs must be well-documented, readily available at no additional cost, and should not require any extra applications or hardware. The solution should also support the ability to execute APIs directly on console data without limitations, enabling quick and efficient access.	We humbly request you to please amend the clause as below to allow maximum vendor particpation: "The proposed solution must provide API access to all major management functionalities and data within the XDR platform. These APIs should be well-documented and included as part of the standard offering at no additional cost, with endpoint access available over HTTPS through the OEM's XDR cloud console. No extra hardware or separate application installations should be required for API use, and the solution should support direct, real-time execution of API queries on console data to enable fast, efficient integration and automation."	Please be guided by RFP
5	- The proposed solution should offer an intuitive, easy-to-navigate console. It must enforce protection across Windows, macOS, and Linux using a single unified policy, without the need to create separate policies for each operating system.	This clause seems to be restrictive in nature as it speaks about having a single unified agent delivering and pushing policies from console across different OS platforms, viz. WIndows, MacOS, and Linux. This sort of capability is provided by only a handful of OEMs, thus, limiting a wider OEM participation. So, we request you to please neutralize this point as below: "The proposed solution should offer an intuitive, easy-to-navigate console for centralized security management. It must enforce protection across Windows, macOS, and Linux endpoints through unified policy management, allowing administrators to create and deploy consistent security policies from a single platform, while accommodating necessary operating system-specific controls or configurations as required."	Kindly refer corrigendum

6	Annexure XVIII – Solution Compliance Statement - The proposed solution must allow temporary disabling of the endpoint agent through the management console for troubleshooting or testing purposes.	This clause seems to be favouring a specific OEM(s) here and is restrictive in nature, thus, limiting other OEMs to participate fairly. Hence, we humbly request you to please modify this clause as below: "The proposed solution must allow administrators to remotely manage endpoint agent operations—including granular control of protection modules and policies—for troubleshooting or testing purposes, via the security management console."	Please be guided by RFP
7	- Solution should have feasbility to secure the uninstalltion of antivirus client by user without a password. This password should be unique for every machine/group of machine and should be visible only to admin of the the Management console.	We understand that it's crucial to have a password requirement feature for preventing users to uninstall the software solution client from user endpoints and devices, however, keeping a unique password for each machine/OU/group by the console admin seems to be OEMs specific and is therefore limiting more OEMs from participation. Hence, we humbly request you to please amend this clause as below and make it vendor neutral: "Solution should have feasbility to secure the uninstallation of antivirus client without a password to prevent end users from uninstalling it without entering an administrator-defined password. This password should be accessible only to authorized administrators through the Management console."	Please be guided by RFP
8	- In case a machine is deleted from management console, solution should still provide functionality to uninstall the EDR client from console.	This clause seems to be favouring a particular OEM(s) and is therefore restrictive in nature for other OEMs participation. Thus, we request you to please modify the clause as below for more vendor participation: "The solution must provide the ability to remotely uninstall the EDR client from the management console for endpoints that are still present and managed within the console, including those that are offline but have not yet been deleted. Remote uninstallation for endpoints removed from the console is not supported."	Please be guided by RFP
9	Annexure XVIII – Solution Compliance Statement - The proposed solution shall protect endpoints against the exploitation of known and unknown vulnerabilities in Operating Systems and other applications. Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployed.	The term "virtual patch" used here seems to be favouring a specific OEM(s) and is therefore restriciting a wider OEM participation in the bid. So, to allow a maximum and fair vendor participation, we humbly request you to please modify the clause as below: "The proposed solution must protect endpoints against the exploitation of both known and unknown (zero-day) vulnerabilities in operating systems and applications. The solution should provide vulnerability protection that leverages virtual patching and/or exploit prevention technologies, enabling immediate risk mitigation—even before official software patches are available or deployed—while also supporting traditional patch management for long-term remediations."	Kindly refer corrigendum
10	Annexure XVIII – Solution Compliance Statement - Response & Remediation Capabilities - The proposed solution must display the confidence level assigned to each machine learning–based detection, indicating the likelihood or predictiveness of the identified threat.	We understand that this requirement is essential to have in a EDR solution, though, explicity mentioning of "confidence level or score" here seems to be aligning some specific OEM(s) and therefore making the clause compliance to be restrictive in nature for other OEMs to qualify and comply. Hence, we sincerely request you to please modify the clause as below: "The proposed solution must leverage machine learning–based detection to prioritize, triage, and enrich alerts with contextual information—enabling analysts to assess the risk or severity of identified threats—even if specific confidence levels or likelihood scores are not enumerated for each detection."	Please be guided by RFP

11	- The proposed solution should have the capability to undo all operating system changes and perform necessary corrective actions. It should also be able to reverse any system-level modifications related to the attack, such as registry edits and configuration changes.	This clause seems to favouring some particular OEM(s) as mentioning about "OS level changes" in the clause clearly indicates that only the leading OEM(s) would be able to provide this requirement. Therefore, the scope for allowing more and a fair OEM participation is getting limited here. Thus, we humbly request you to please modify the clause as below to keep it vendor neutral: “The proposed solution should be capable of performing corrective actions and automatically remediating system-level changes made by attacks, including restoration of critical registry entries and security settings, rollback of security agent-related changes, and repair of commonly modified configurations.”	Please be guided by RFP
12	- The proposed solution should provide granular control over telemetry for all endpoints, including the ability to define which data is exported.	As per our understanding, we acknowledge that is important to have a granular control over the telemetry for endpoint data, etc. However, in a generic scenario, the platform of the said solution requirement must be designed in such a way that it automatically collects and exports only the most relevant and security-critical endpoint data needed for detection, investigation, and compliance—minimizing information overload and ensuring operational efficiency. In addition, only the leading vendors here are able to deliver such a fine-grained control feature but then that will cause resource contention leading to performance impact, potential system instability, so and so forth affecting the overall UX (user experience) of the delivered solution. Meaning, only the necessary telemetry should be exported minimizing complexities for administrators. Hence, we sincerely request you to kindly modify this clause as below for allowing a maximum OEM participation and give them a fair chance: "The proposed solution should provide centralized, policy-based control over the export of security telemetry and reports for all endpoints, allowing administrators to select which categories of data or modules are exported as required for compliance, investigation, or operational needs."	Please be guided by RFP
13	Annexure XVIII – Solution Compliance Statement - Policy & Installation - Solution should have the option to provide dynamic policy assignment based on device attributes.	As per our understanding, this clause seems to be favouring some specific OEM(s) and thus restrictive and limiting a wider OEM participation. Therefore, to make it vendor neutral and fair, we humbly request you to please modify the clause as per below consideration: "The solution should enable administrators to assign and manage security policies for groups or individual endpoints based on device attributes or logical grouping, ensuring appropriate policy application as operational needs change."	Please be guided by RFP

14	- The solution must support automatic placement of devices into designated device groups.	Per our understanding and knowledge, for the said solution requirement, automatic placement of devices into designated device groups is not essential because manual or administrator-controlled grouping ensures deliberate, auditable, and secure policy assignment. In most organizations, device roles and attributes are stable; manual or bulk-assisted assignment prevents unintended policy exposure or misclassification that could result from attribute errors or frequent changes. This approach maximizes operational control, reduces misconfiguration risk, and supports regulatory and audit requirements without adding unnecessary management complexity. Also, for this reason, the clause seems to be aligning with some particular OEM(s) solution here and making the restrictive in nature for more vendor participation. Thus, we sincerely request you to kindly modify the clause as per below suggestion: "The solution should support straightforward assignment and management of devices into designated groups, allowing administrators to efficiently organize endpoints for policy application and operational needs."	Kindly refer corrigendum
15	Annexure XVIII – Solution Compliance Statement - Data Loss Prevention - Proposed solution should have data loss prevention capability with pre-defined DLP templates for HIPAA, PCI-DSS etc. And should have capability to create policies on basis of regular expression, key word and dictionary having visibility and control of data that's being transferred to USB ports, CDs, DVDs, removable disks, cloud storage, email clients, FTP, IM applications, P2P applications and webmails.	We understand that DLP feature is essential in having control over an enterprise's confidential and sensitive data and information in terms of monitoring, blocking, allowing, etc. via different data transfer channels. However, in this clause, employing pre-defined DLP templates for creating DLP policies for HIPAA, PCI-DSS, etc. compliances seem to be in favour a specific OEM(s) and thus making it restrictive in nature for other OEMs to participate. So, to make the clause vendor neutral, we sincerely request and suggest you to modify the clause as below: "The proposed solution should deliver data loss prevention capabilities, including the ability to create policies using regular expressions, keywords, and custom dictionaries. It should provide visibility and control of data transfers over vectors such as USB, CDs, DVDs, removable disks, cloud storage, email clients, FTP, instant messaging, peer-to-peer applications, and webmail. The solution should support templates or guidance for regulatory compliance use cases and allow customization to accommodate evolving business and regulatory needs."	Please be guided by RFP

16	- Solution should allow to discover and monitor the confidential information with capability block, notify the agent user and user justification of the data with real-time view of endpoint status and broad coverage of communication systems including email clients, webmail, IM, P2P, FTP, Skype, Windows File Share, ActiveSync, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS and SMTP and applications like System and application channels: Cloud storage services, Data recorders (CD/DVD)	As per our understanding, specific DLP policies in vendor solutions are capable enough to discover and monitor confidential information with different monitoring capabilties and reporting or notifying the same to the administrator in the form of, say, an email / SMS notifications / console reports, etc. However, a DLP policy providing detailed justification of the monitored data with real-time view of endpoint status and broad coverage of communication systems seems to be in favour of some leading OEM(s) only, therefore, making the overall clause confined to them. For a fair and allowing a wider OEM participation here, we humbly request you to please modify the clause as per below suggestion: "The solution should enable discovery, monitoring, and protection of confidential information, with the capability to block or allow transfers and notify users or administrators in real time. It should provide visibility into endpoint status and support broad coverage of communication and storage channels, including email clients, webmail, instant messaging, peer-to-peer applications, FTP, Windows File Share, ActiveSync, SaaS/cloud applications, USB and removable storage, CDs/DVDs, and common networking protocols such as HTTP/HTTPS and SMTP."	Please be guided by RFP
17	- Solution should provide outbreak prevention with capability to limit/deny access to shared folders, block vulnerable ports, deny write access to files and folders, deny access to executable compressed files and creating mutual exclusion handling on malware processes/files.	Per our understanding, this clause is favouring a particular OEM(s) and it limiting other OEMs from a fair participation in this bid. Therefore, we sincerely request you to kindly nueutralize the point and modify it for allowing maximum vendor participation: "The solution should provide outbreak prevention capabilities, including the ability to restrict or control access to shared folders, block specified ports, limit write access to files and folders, restrict execution of compressed files containing executables, and support policy-based handling of processes or files identified as threats."	Please be guided by RFP
18	Annexure XVIII – Solution Compliance Statement - Extended Detection & Response (XDR) - The proposed solution must enable security analysts to query both EDR and third-party logs—such as Microsoft Office 365, Firewalls, and others—using natural language for intuitive and efficient investigations.	This clause seems to be favouring only the leading specific OEM(s) by mentioning NLQ (Natural Language Query) of 3rd-party logs ingestion and integration in the clause as only those vendors will be able to provide such a functionality embedded into their solution. But, it is a fact that once the data is onboarded onto the required solution platform, it is not really necessary to run natural language searches directly against external tools. Moreover, most customer investigations and analytic workflows rely on centralized, correlated data already ingested and normalized by the required solution platform. For the above mentioned reasons, we humbly request you to please modify the clause as per below suggestion and allow a wider OEM participation: "The solution should enable security analysts to perform intuitive investigations across endpoint and integrated third-party security data by supporting natural language queries within a unified platform, delivering rapid access to incident, alert, and log information from connected sources such as EDR, email, firewall, and cloud applications."	Please be guided by RFP

19	GeM RFP @ Page no. 01, - Exemption for Turnover is mentioned only Partially,	We request from the competent authorities to give Exemptions for Start-ups companies for experience also, A Indian govt. initiative that offers support, or funding to promote the growth of the start-up ecosystem and to facilitate the success of individual start-ups in India. As per the RFP asked, experiences in EDR/XDR/EPP is very critical for start-ups companies during his initial phase however scope define in the RFP will be catered by start-ups by its own technical professionals.Therfore we request for exemption in experiences also for this RFP so that an start-up can also participate	Please be guided by RFP
20	5.1 Statement of Work : - (Vii) - Vendor will integrate the deployed solution with existing SIEM and other reporting solution as per Bank's requirement.	Syslog (CEF and LEEF) and RESTful API integration is supported.	Syslog and API are supported
21	(XIII) Solution must have features for hybrid implementation (on premises centralised EDR deployment for endpoints & servers and cloud deployment for EDR dashboard/ management reports/AV patching for devices out of Bank's LAN network) and architecture, ease of deployment, minimal impact on network performance while doing data collection and communication across the network. -	We can provide an on-premises service gateway for communication between internal machines and the centralized console, while cloud-based or internet-connected machines can directly communicate with the cloud. This approach enables seamless management of both internal and external machines, ensuring centralized administration of all devices, including endpoints and servers	Please be guided by RFP
22	EMD and Experience Clause -	Request to provide full exemption from EMD and Past Experience criteria for MSME bidders.	Please be guided by RFP
23	5.4 Monitoring and Control : - (A) The solution must support File Integrity Monitoring (FIM). -	FIM is generally required for server workloads where compliances are required.	Please be guided by RFP
24	(B) The solution must have built-in vulnerability assessment -	Request to modify as below: Solution should be able to automatically assess the system vulnerabilities, virtually patch it and provide recommended rules against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor also should provide recommendation for automatic removal of assigned rules if a vulnerability or software no longer exists to optimize the policy - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.	Please be guided by RFP

25	(C) The solution must provide the means to conduct Inventory Management. -	EDR is not an inventory management soltuion however it possess tha capability to provide endpoitn inventory where EDR agent has nbeen deployed. **Request to modify this point for broader OEM participation and competitive bid.** The solution must provide Endpoint Inventory and provide an option to export data in csv/xls format.	Kindly refer corrigendum
26	5.5 EDR infrastructure capabilities : - (C) The solution must provide the means to conduct Inventory Management. -	Since this is a hybrid setup with a mix of LAN and internet users. We request you to please modify this pointer as below:	Kindly refer corrigendum
27	5.6 EDR Operations : - (F) Block access to the program settings for end users. -	These are not relevant to EDR functionality and can instead be achieved through Active Directory policy implementation. Requesting you to please delete this clause.	Kindly refer corrigendum
28	Request to add the following advance threat protection capabilities for endpoint and servers -	Vulnerability protection network engine should provide configurable option of Inline and Tap mode deployment along with advance logging policy option including bypass, normal, verbose mode, stateful, normalization, frag and verifier suppression etc.	Please be guided by RFP
29	Request to add the following advance threat protection capabilities for endpoint and servers	Proposed solution should have capability to use application name, path, regular expression, or certificate for basic application whitelisting and blacklisting containing broad coverage of pre-categorized applications that can be easily selected from application catalog (with regular updates) having features roll-your-own application whitelisting and blacklisting for in-house and unlisted applications ensuring that patches/updates associated with whitelisted applications can be installed.	Please be guided by RFP
30	Request to add the following advance threat protection capabilities for endpoint and servers	Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per Frost & Sullivan Reports and should be in Leader Quadrant as per Gartner Magic Quadrant of EPP category from last 5 consecutive years and OEM must have contributed at least 40 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publically available.	Please be guided by RFP
31	Request to add the following advance threat protection capabilities for endpoint and servers	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) also should provide recommendation for automatic removing of 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.	Please be guided by RFP

32	Request to add the following advance threat protection capabilities for endpoint and servers	Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behaviour, such as modifications, or changes in ownership or permissions also should be able to monitor System Services, Installed Programs and Running Processes for any changes also extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.).	Please be guided by RFP
33	Request to add the following advance threat protection capabilities for endpoint and servers	Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/unassigment of rules when not required also support decoders for parsing the log files being monitored also have customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered on a match also ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.	Please be guided by RFP
34	Request to add the following advance threat protection capabilities for endpoint and servers	The proposed solution should support Deep Packet Inspection (HIPS/IDS) and should support creation of customized DPI rules if required supporting virtual patching capabilities for both known and unknown vulnerabilities until the next scheduled maintenance window also virtual Patching should be achieved by using a high-performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.	Please be guided by RFP
35	Request to add the following advance threat protection capabilities for endpoint and servers	Solution must support CPU usage performance control during scanning - Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer i.e. High, Medium and low.	Please be guided by RFP
36	Number of years of experience of the bidder in implementation / support of EDR/MDR/XDR/EPP Solutions a. > 5 years - 20 Marks b. ≥ 4 to <=5 Years - 15 Marks c. ≥ 2 to <=3 Years - 10 Marks -	Number of years of experience of the bidder in implementation / support of EDR/MDR/XDR/EPP/ NGFW/NDR/DDoS Solutions a. > 5 years - 20 Marks b. ≥ 4 to <=5 Years - 15 Marks c. ≥ 2 to <=3 Years - 10 Marks **Note:** XDR/MDR were not available before 5 years so we request to add NGFW/NDR/DDoS along with EDR to allow bidder to acheive maximum qualifying marks. This will allow more participant of interested bidder hence more competition	Please be guided by RFP

37	Total number of implementations/supports of EDR/MDR/XDR/EPP solutions by bidder. (Only Work Completion Certificate (upto last 10 years) will be considered for award of points) - Max Marks - 20 a. ≥ 6 Implementations in Govt. Sector/PSU/PSBs/FIs/Corporate* in India - 20 Marks b. ≥ 4 to ≤5 Implementations in Govt. Sector / PSU/PSBs/FIs/Corporate* in India - 15 Marks c. ≥ 2 to ≤3 Implementations in Govt. Sector / PSU/PSBs/FIs/Corporate* in India - 10 Marks -	Total number of implementations/supports of EDR/MDR/XDR/EPP/NGFW/NDR/DDoS solutions by bidder. (Only Work Completion Certificate (upto last 10 years) will be considered for award of points) - Max Marks - 20 a. ≥ 6 Implementations in Govt. Sector/PSU/PSBs/FIs/Corporate* in India - 20 Marks b. ≥ 4 to ≤5 Implementations in Govt. Sector / PSU/PSBs/FIs/Corporate* in India - 15 Marks c. ≥ 2 to ≤3 Implementations in Govt. Sector / PSU/PSBs/FIs/Corporate* in India - 10 Marks Note: We request to add NGFW/NDR/DDoS along with EDR/MDR/XDR/EPP solutions to allow bidder to acheive maximum qualifying marks. This will allow more participant of interested bidder hence more competition.	Please be guided by RFP
38	Statement of Work -		
39	The solution must have built-in vulnerability assessment -	Request to modify as below: Solution should be able to automatically assess the system vulnerabilities, virtually patch it and provide recommended rules against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor also should provide recommendation for automatic removal of assigned rules if a vulnerability or software no longer exists to optimize the policy - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.	Please be guided by RFP
40	5.5. c) EDR infrastructure capabilities - The solution must support automated distribution on endpoints or servers added to the environment following the initial deployment.	Since this is a hybrid setup with a mix of LAN and internet users. We request you to please modify this pointer as below: The solution must support centralized dsitributon and installation of agents on endpoints or servers leveraging GPO or app deployment tools.	Please be guided by RFP
41	- Request to add the following advance threat protection capabilities for endpoint and servers	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) also should provide recommendation for automatic removing of 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.	Please be guided by RFP
42	- Request to add the following advance threat protection capabilities for endpoint and servers	Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behaviour, such as modifications, or changes in ownership or permissions also should be able to monitor System Services, Installed Programs and Running Processes for any changes also extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.).	Please be guided by RFP
43	5.1 (i) -	Please confirm the number and addresses of NHB locations where the EDR solution is to be deployed. Are remote branches included?	List of all regional offices is mentioned at bank's website
44	5.1 (ii) -	Does “ICT infrastructure” include network devices, mobile endpoints, or only desktops, laptops, and servers?	It includes all servers, desktops and laptops with scope of future expansion.
45	5.1 (ii) -	Kindly confirm whether the 800 endpoints include virtual machines, BYOD devices, or future expansion endpoints.	It includes all servers, desktops and laptops with scope of future expansion.
46	5.1 (v) -	Please share details of the existing EDR solution (vendor, architecture, endpoint coverage) to assess migration complexity.	Bank is using Sophos EDR
47	5.1 (vii) -	Please specify the SIEM solution currently in use. Are APIs or connectors available for integration?	Bank is using Elastic SIEM

48	5.1 (xii) -	Please clarify the process for deploying OEM updates during the contract period. Will testing and rollback mechanisms be required?	Please by guided by RFP
49	5.1 (xiv) -	How many users are expected to be trained, and what is the preferred mode (online/offline/hybrid)?	Training can be provided to approx. 10 users in any mode.
50	5.3 (c) -	Is the sandboxing capability expected to be cloud-based or on-premises?	Please by guided by RFP
51	5.4 (a) -	Please clarify whether the FIM capability should include real-time monitoring of system files, configuration files, and registry changes across all supported operating systems.	Please by guided by RFP
52	5.4 (b) -	Kindly confirm whether the built-in vulnerability assessment should include periodic scanning, CVE mapping, and prioritization of vulnerabilities. Is there a requirement to integrate with external patch management or ticketing systems?	Please by guided by RFP
53	5.4 (c) -	Is the inventory expected to include real-time status of endpoint agents (e.g., online/offline, last sync time, version)? Should it support tagging or grouping of assets based on location or department?	Please by guided by RFP
54	5.4 (e) -	What is the “sufficient period” for log retention? Is there a minimum duration mandated by NHB?	Please by guided by RFP
55	5.5 (i) -	Please clarify how offline endpoints are expected to receive updates and policy changes.	Please by guided by RFP
56	5.5 (a, b, c) -	Is there a preferred method for distributing installation centrally (e.g., via Active Directory, SCCM, or custom scripts)?	Bank is using Endpoint Central soution.
57	5.6 (o) -	The RFP mandates that the OEM’s data center must be located in India. Given that most leading EDR solutions are cloud-based and operate on globally distributed infrastructure, please clarify whether: a) The requirement applies only to data residency for customer data, or b) The entire backend infrastructure (including threat intelligence, telemetry processing, and management console) must be hosted within India.	Please by guided by RFP
58	3 - The entire endpoint software should be a single agent software deployed with all features and functions of NGAV, HIPS, EDR, Threat Hunting, Application Control, Device Control, Vulnerability Protection, Integrated DLP, Firewall, and Device Control and does not require any agent or software update to enable or disable these modules.	The RFP mentions inclusion of Host Intrusion Prevention System (HIPS), Vulnerability Protection, and Data Loss Prevention (DLP) as part of the EDR solution requirements. As per industry standards, EDR solutions are primarily focused on endpoint threat detection, response, and forensic visibility. HIPS and vulnerability management are generally part of Endpoint Protection Platforms (EPP), while DLP is a separate data security and compliance control. Including these within the EDR scope may	Please by guided by RFP

59	17 - The endpoint agent must support on-demand & scheduled scans, initiated either from the management console or directly from the endpoint, to detect malware or verify that a threat has been successfully remediated.	We request clarification on the requirement stating "The endpoint agent must support on-demand & scheduled scans, initiated either from the management console or directly from the endpoint, to detect malware or verify that a threat has been successfully remediated." Restricting scheduled scans to initiation only from the management console and not allowing flexibility through APIs appears to favor specific OEM architectures and may unintentionally prohibit participation from vendors who offer equivalent or superior functionality via API-driven orchestration. Modern EDR and endpoint security solutions increasingly adopt API-first designs to provide automation, scalability, and integration with broader security ecosystems, while still enabling scan initiation and validation. We therefore seek confirmation whether API-based scheduled scan initiation will be considered compliant, in order to ensure fair competition and alignment with current industry practices. Hence seek modification in the clause as -> "**The endpoint agent must support on-**	Please by guided by RFP
60	28 - The proposed solution shall protect endpoints against the exploitation of known and unknown vulnerabilities in Operating Systems and other applications. Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployed.	We seek clarification on the requirement stating, "The proposed solution shall protect endpoints against the exploitation of known and unknown vulnerabilities in Operating Systems and other applications. Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployed." While vulnerability management and virtual patching are valuable security capabilities, they are traditionally addressed by specialized Vulnerability Management solutions, not by Endpoint Detection and Response (EDR). EDR's core purpose is to detect, investigate, and respond to endpoint threats rather than perform vulnerability shielding. Making vulnerability protection a mandatory part of EDR significantly narrows vendor participation, as it excludes EDR-focused solutions aligned with industry standards, thereby limiting competition and potentially driving up costs. We request the requirement be relaxed or decoupled from EDR to ensure broader participation and alignment with standard EDR	Please by guided by RFP

61	39 - Solution should be APT ready capable of submitting SO (Suspicious Objects) to the sandbox solution for analysis without additional license on Endpoint.	We seek clarification on the requirement for a mandatory sandbox capability within the EDR solution for handling APTs and unknown threats. SentinelOne EDR natively addresses such threats using its patented behavioral AI and autonomous detection engines that analyze and correlate processes in real time on the endpoint, eliminating the dependency on external sandboxing for zero-day or fileless attacks. Unlike traditional sandboxing, which introduces latency and requires detonation environments, SentinelOne's on-device AI provides instant protection and automated remediation without cloud reliance, ensuring faster response and lower operational overhead. Making sandbox capability a compulsory criterion may unnecessarily restrict solutions that use advanced AI-driven approaches instead of sandboxing, thereby limiting participation**. Kindly confirm if sandbox functionality may be considered optional rather than mandatory for EDR.**	Please by guided by RFP
62	Annexure XVIII – Solution Compliance Statement -63 - Solution must have the application control lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office.Also there should be option to request for addition of applications not present	Category-based application blocking is not part of the standard scope of an Endpoint Detection and Response (EDR) solution, which is designed for advanced threat detection, investigation, and response. Such functionality falls under endpoint protection or application control solutions and is offered only by a limited set of vendors. Mandating	Please by guided by RFP
63	Annexure XVIII – Solution Compliance Statement -67 - The proposed solution shall allow usage of authorized USB devices by users and blocking of unauthorized USB devices. The solution shall allow exclusion of authorized USB devices by using their Vendor ID, Product ID or Serial number.	The specification appears to emphasize configuration of USB devices on a per-user basis rather than per-device, which aligns with the proprietary approach of only certain OEMs and restricts broader vendor participation. Industry-standard device control features typically manage USB authorization at the device level through Vendor ID, Product ID, or Serial number without binding the control to individual user profiles. To ensure maximum vendor participation and maintain fairness, we request modification of this requirement to allow USB control at the device level, independent of user-specific configurations -> " **The proposed solution shall allow usage of authorized USB devices by users/devices and blocking of unauthorized USB devices. The solution shall allow exclusion of authorized USB devices by using their Vendor ID, Product ID or Serial number."**	Kindly refer corrigendum

64	Annexure XVIII – Solution Compliance Statement -71 - Solution should have privilege to define the time based policies	While time-based policies may be useful in certain access control or productivity management tools, they are not a standard or core capability of Endpoint Detection and Response (EDR) solutions, which focus on continuous monitoring, detection, and response to security threats. Making this feature mandatory favors a limited set of vendors that provide such niche functionality and may restrict participation from other industry-leading EDR providers. To ensure broader vendor participation and alignment with global EDR definitions, we request that this requirement either be removed or made optional.	Please by guided by RFP
65	Annexure XVIII – Solution Compliance Statement -80 - The proposed solution is able to provide DLP functionality without additional agent footprint or 3rd party integration to minimize the complexity and cost of data security.	Data Loss Prevention (DLP) is traditionally a standalone technology focused on protecting sensitive data and ensuring compliance, and it typically operates independently of Endpoint Detection and Response (EDR) solutions. Requiring native DLP within an EDR platform restricts participation to a very limited number of vendors, as most leading EDR solutions are intentionally agent-light and integrate with specialized DLP tools where required. Making embedded DLP a mandatory criterion under EDR scope creates an uneven playing field, limits competition, and contradicts the globally accepted definition of EDR. To ensure vendor neutrality and fair participation, we request that this requirement be removed from the EDR scope.	Please by guided by RFP
66	Annexure XVIII – Solution Compliance Statement -81 - Proposed solution should have data loss prevention capability with pre-defined DLP templates for HIPAA, PCI-DSS etc. And should have capability to create policies on basis of regular expression, key word and dictionary having visibility and control of data that's being transferred to USB ports, CDs, DVDs, removable disks, cloud storage, email clients, FTP, IM, applications, P2P applications and webmails.	These capabilities define a full-fledged Data Loss Prevention (DLP) solution, which is not a core function of Endpoint Detection and Response (EDR). EDR solutions are designed to detect, investigate, and respond to endpoint threats, while DLP is a separate data security and compliance technology often requiring dedicated tools. Making advanced DLP features mandatory under EDR scope favors a very limited set of vendors, restricts fair competition, and could exclude leading EDR providers that adhere to industry standards. To ensure broader participation and vendor neutrality, we request that this requirement be reconsidered or removed from the EDR scope.	Please by guided by RFP

67	Annexure XVIII – Solution Compliance Statement -82 - Solution should allow to discover and monitor the confidential information with capability block, notify the agent user and user justification of the data with real-time view of endpoint status and broad coverage of communication systems including email clients, webmail, IM, P2P, FTP, Skype, Windows File Share, ActiveSync, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS and SMTP and applications like System and application channels: Cloud storage services, Data recorders (CD/DVD)	This specification describes comprehensive Data Loss Prevention (DLP) functionalities rather than Endpoint Detection and Response (EDR) capabilities. EDR solutions are intended to detect, investigate, and respond to endpoint threats, whereas advanced DLP features—such as monitoring and controlling data across communication channels, SaaS platforms, and storage media—are traditionally provided through dedicated DLP solutions. Including these requirements within the EDR scope favors a limited set of vendors offering bundled DLP features, thereby restricting fair competition and prohibiting participation from leading EDR providers aligned with global standards. We therefore request that this requirement be reconsidered or excluded from the EDR specifications to ensure vendor-neutral participation and alignment with industry best practices.	Please by guided by RFP
68	Annexure XVIII – Solution Compliance Statement -83 - Solution should provide outbreak prevention with capability to limit/deny access to shared folders, block vulnerable ports, deny write access to files and folders, deny access to executable compressed files and creating mutual exclusion handling on malware processes/files.	hese functionalities overlap with Host Intrusion Prevention Systems (HIPS), endpoint hardening, and access control tools rather than the core functions of Endpoint Detection and Response (EDR). EDR solutions are designed to detect and respond to advanced threats through behavioral analysis, threat hunting, and automated remediation, not to perform network port blocking, file access restrictions, or outbreak containment at the granular system-control level. Mandating these features within the EDR scope favors specific vendors that combine HIPS/EPP with EDR, thereby limiting fair competition and potentially excluding leading EDR providers aligned with global definitions. We therefore request that this requirement be reconsidered and removed to ensure vendor neutrality and wider participation.	Please by guided by RFP

69	Annexure XVIII – Solution Compliance Statement -84 - The proposed solution must have capability to Integrate with Active Directory .	While Active Directory (AD) integration may support certain use cases, it is not a mandatory requirement for an Endpoint Detection and Response (EDR) solution. For example, SentinelOne EDR automatically fetches endpoint domain details directly from the agent without requiring AD integration, thereby simplifying deployment and reducing dependency on directory services. Making AD integration a compulsory feature risks favoring certain vendor architectures while unnecessarily restricting participation from solutions that achieve the same outcome through agent-based intelligence. We therefore request that this requirement be relaxed to optional, ensuring vendor neutrality and broader participation while maintaining endpoint visibility and domain correlation capabilities.	Please by guided by RFP
70	Annexure XVIII – Solution Compliance Statement -64 - Solution should offer Real-time Scanning for Local Files and Network Shares during Read & Write operation	While real-time scanning of local files is a common feature of endpoint protection platforms (EPP), network share scanning is not part of the core capabilities of an Endpoint Detection and Response (EDR) solution. EDR is designed to detect, investigate, and respond to advanced threats on endpoints, whereas scanning of network shares is typically handled by dedicated file servers or storage security solutions. Mandating network share scanning within the EDR scope creates an overlap with EPP/server AV functionalities, restricts fair competition, and may exclude leading EDR providers that align with global definitions. To ensure broader participation and vendor neutrality, we request that network share scanning be removed from the mandatory EDR requirements.	Please by guided by RFP
71	Annexure XVIII – Solution Compliance Statement – Endpoint Detection and Response (EDR)	The entire endpoint software should be a single agent software deployed with all features and functions of NGAV, HIPS, EDR, Threat Hunting, Application Control, Device Control, Vulnerability Protection, Integrated DLP, Firewall, and Device Control and does not require any agent or software update to enable or disable these modules.	Please be guided by RFP
72	Annexure XVIII – Solution Compliance Statement – Endpoint Detection and Response (EDR)	Proposed solution should be integarted with bank's ITSM tool i.e. Service Desk Plus	Functionality is required for ticketing purpose of alerts generated by EDR.
73	- The proposed solution should include a native, customizable console that enables grouping of endpoints by distributed sites or departments. It must support multi-tenancy to ensure separation of user roles, notifications, dashboards, reports, and event data. Additionally, the solution should allow the creation of specific rules and policies for each group, support hierarchical policy inheritance and offer the flexibility to override inherited policies when needed.	Can we have use case for Multi- tenancy? the solution as capability to allow the creation of specific rules and policies for each group, support hierarchical policy inheritance and offer the flexibility to override inherited policies when needed.	Kindly refer corrigendum

74	- The proposed solution should offer API access to all management functionalities and data. The APIs must be well-documented, readily available at no additional cost, and should not require any extra applications or hardware. The solution should also support the ability to execute APIs directly on console data without limitations, enabling quick and efficient access	We can Do API Access but need to know more on the scenarios in the current environment	Functionality is required for integration with SOAR/SIEM/Firewall etc.
75	- The proposed solution should have the capability to undo all operating system changes and perform necessary corrective actions. It should also be able to reverse any system-level modifications related to the attack, such as registry edits and configuration changes.	Registry modification enforcement is supported. Configuration changes will be stopped if found risky\malicious. HEP provides remediation by back-up mechanisms, but we do not have OS restore points hope this works ?	Please be guided by RFP
76	- Deployment of endpoint agent must be possible through mechanisms such as Microsoft Active Directory Group Policy Update (GPO), deployment tools like Manage Engine., command line execution (escalated and silent: no User interface) and must not require any sort of user interaction and/or intervention during installation and must not require system reboot on any OS. Also, any update/patches/version changes/downgrade to the endpoint agent must not require system reboot as well and such changes (update/patches/version changes/downgrade) to the endpoint agents must be operated directly from the same console. Removal of endpoint agent (if required) must also be possible through similar methods.	Can there be use case or scenario to explain this better	Functionality is required for installation/unistallation using deployement tools.
77	- Solution should have privilege to define the time based policies	Can we get Use case	Please be guided by RFP
78	- The product should provide a curated list of commonly recognized or vendor-recommended exclusions to streamline configuration.	If this is the use case - we can support -Server optimization includes a list of recommended exclusions based on server roles. We do not have recommendations of exclusions based on vendors - the vendors provide it, and it can be applied in HEP.	Please be guided by RFP
79	- Proposed solution should have data loss prevention capability with pre-defined DLP templates for HIPAA, PCI-DSS etc. And should have capability to create policies on basis of regular expression, key word and dictionary having visibility and control of data that's being transferred to USB ports, CDs, DVDs, removable disks, cloud storage, email clients, FTP, IM applications, P2P applications and webmails.	DLP is supported on the web only - browser based , Can we know the use case is about writing data drives or blocking certain data type?	Please be guided by RFP

80	- Solution should provide outbreak prevention with capability to limit/deny access to shared folders, block vulnerable ports, deny write access to files and folders, deny access to executable compressed files and creating mutual exclusion handling on malware processes/files.	All is supported besides write access to files and folders. We support write\read privillages only for USB drives (ME). Alternatively, we can block access to shared folders , is the above use case suffice the need ?	Please be guided by RFP
81	- The proposed solution should provide a listing of third-party applications that can be integrated via API to enable unified prevention, detection, and response across your ecosystem, delivering rapid time to value.	We can send data to SIEM platforms, but we do not have a list of applications to be integrated with.	Please be guided by RFP
82	Annexure V Clause 5 - The Bidder should have experience in implementation/support of EDR/EPP Solutions in at least 2 Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates** in India during the last 5 Fys	The Bidder should have experience in implementation/support of EDR/EPP Solutions in at least **1(ONE)** Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates** in India during the last 5 Fys	Please be guided by RFP
83	Technical Bids (Marks Distribution) Clause 2 - 27 of 99 - Total number of implementations/supports of EDR/MDR/XDR/EPP solutions by bidder. (Only Work Completion Certificate (upto last 10 years) will be considered for award of points) a. ≥ 6 Implementations in Govt. Sector /PSU /PSBs/ FIs/ Corporate* in India - 20 Marks b. ≥ 4 to ≤5 Implementations in Govt. Sector / PSU /PSBs /FIs /Corporate* in India - 15 Marks c. ≥ 2 to ≤3 Implementations in Govt. Sector / PSU /PSBs /FIs/Corporate* in India - 10 Marks	Total number of implementations/supports of EDR/MDR/XDR/EPP solutions by bidder. (Only Work Completion Certificate (upto last 10 years) will be considered for award of points) **a. ≥ 2 Implementations in Govt. Sector /PSU /PSBs/ FIs/ Corporate* in India - 20 Marks** **b. 1 Implementation in Govt. Sector / PSU /PSBs /FIs /Corporate* in India - 15 Mark**	Please be guided by RFP
84	Technical Bids (Marks Distribution) Clause 4 - 28 of 99 - Total number of implementations of proposed solution in Govt. Sector/PSU/PSBs/FIs/Corporate* in India a. >=7 - 10 Marks b. >=5 and <=6 - 6 Marks c. >=3 and <=4 - 2 Marks	Total number of implementations of **EDR/ MDR/ XDR/ EPP** solution in Govt. Sector/PSU /PSBs /FIs /Corporate* in India **a. >=3 - 10 Marks** **b. >=1 and <=2 - 6 Marks**	Please be guided by RFP
85	The Bidder should have experience in implementation/support of EDR/EPP Solutions in at least 2 Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates** in India during the last 5 FYs. - The Bidder has to provide work order copy along with completion certificate /reference letter in their name in this regard	1. We request to consider MSME/Startup exemption for this clause.	Please be guided by RFP
86	Bids (Technical & Commercial) And Bid Evaluation Methodology	2. consider past experience in implementation/support of Firewall installation/NMS/IT infrastructure in at least 2 Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates** in India during the last 5 FYs.	Please be guided by RFP

87	- As per Clause 7 on P.No. 13 Contract Period The contract period is initially for five years. Bank may go for extending the service contract for further years at the maximum of 10% addition to yearly total contract value, and with existing terms and conditions, subject to satisfactory review of the services. Any extension of the contract shall be at the sole discretion of the Bank.	We are requesting to amend this clause as below Contract Period The contract period is initially for five years. Bank may go for extending the service contract for further years at the maximum of 10% addition to yearly total contract value, and with mutual terms and conditions, subject to satisfactory review of the services. Any extension of the contract shall be at the sole discretion of the Bank.	Please be guided by RFP
88	- As per Clause 10.2 on P.No. 30 After sign-off/go-live. Bank will provide sign-off subject to pre-deployment audit of the proposed solution by bank appointed external IS auditor. 90% of Total Solution & Implementation Cost (as per commercial bid format) will be released.	Please help with revised payment terms as this impacts our cash flow and costs. 90% of Total Solution on delivery	Please be guided by RFP
89	- As per Clause 10.2 on P.No. 30 After sign-off/go-live. Bank will provide sign-off subject to pre-deployment audit of the proposed solution by bank appointed external IS auditor. 90% of Total Solution & Implementation Cost (as per commercial bid format) will be released.	Please help with revised payment terms as this impacts our cash flow and costs. 100% of Total Implementation on Implementation	Please be guided by RFP
90	- As per Clause 11.21 on P.No. 36 If the Vendor fails to complete the due performance of the contract in accordance with agreed specifications and conditions to the satisfaction of NHB or abandons the project/contract without completing the same as per the agreed terms, NHB reserves the right to recover damages at 10 percent of the contract value as and by way of liquidated damages, but not as penalty. It is clarified that the liquidated damages shall be over and above the penalty, if any, imposed under Clause 11.17.	We are requesting to amend this clause as below If the Vendor fails to complete the due performance of the contract in accordance with agreed specifications and conditions to the satisfaction of NHB or abandons the project/contract without completing the same as per the agreed terms, NHB reserves the right to recover damages at 5 percent of the contract value as and by way of liquidated damages, but not as penalty. It is clarified that the liquidated damages shall be over and above the penalty, if any, imposed under Clause 11.17.	Please be guided by RFP
91	- The proposed solution should have out-of-box integration with SIEM solutions. It should also integrate with third party security solutions for threat intelligence sharing. The proposed solution should be able to integrate with SIEM/SOAR platform over API. Pg-97	Kindly share the third party security solution for threat intelligence sharing and which SIEM,SOAR platform and other existing solutions working in NHB	Will be shared with successful bidder.
92	- Bidder must implement the solution at DC & DR locations. Pg- 8	As we understand that the solution should be deployed on cloud ,hence the EDR Solution will be avaiable with redunancy on cloud. kindly confirm	Please be guided by RFP
93	- Quantity: 600 nos. of ICT devices/endpoints and 200 nos. of Servers (physical/virtual) Pg- 50	Kindly confirm the endpoint and server quantity in DC and DR.	DC DR ratio is 70:30

94	- The EDR solution will provide endpoint protection to all ICT endpoints of the Bank including desktops, laptops, servers (Windows, Mac as well as Linux) etc. totaling to 800 endpoints. Pg-8	Request you to kindly share the breakup of the number of Windows, Mac, and Linux along with OS version.	Will be shared with successful bidder.
95	- Vendor will be responsible to migrate the implementation from existing EDR solution to onboarded EDR in a secured manner with minimal downtime. Pg -8	Kindly confirm the existing EDR solution.	Will be shared with successful bidder.
96	- Vendor will depute onsite engineer to immediate resolution/mitigation of reported issues. During the period of contract, onsite support for 15 man-days/year have to be provided by the vendor without any charges. Beyond this period, Bank will pay as per the prescribed future rate. Pg -8	We understand that 8 working hours is consider as one man day. Kindly confirm .	
97	- Bidder must specify hardware requirements based on their understanding of the overall solution architecture based on requirement. The same must be documented and shared with NHB along with justification/ reasonability. It is to be noted that NHB will provide virtual servers and not physical servers to meet these hardware requirements. Pg-7	Kindly provide details of existing virtualization(Hypervisor) solution at NHB. Do we need to provide the updates and upgrades for OS and DB.	Bank is using Hyper-V and VMWare both. Updates and upgrades should be done by bidder .
98	- Installation, Commissioning and Operationalization of the complete solution: within 45 days of acceptance of work order. Pg-12	we understand that the vendor has to unistall the existing EDR solution/Agents from endpoints ,servers and install the proposed EDR agents on all the endpoints and servers this entire process with take atleast 60 days. Hence, request NHB to kindly amend the clause as below. "Installation, Commissioning and Operationalization of the complete solution: within 60 days of acceptance of work order."	Please be guided by RFP
99	- The solution must have built-in vulnerability assessment	Request to modify as below: Solution should be able to automatically assess the system vulnerabilities, virtually patch it and provide recommended rules against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor also should provide recommendation for automatic removal of assigned rules if a vulnerability or software no longer exists to optimize the policy - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.	Please be guided by RFP
100	- The solution must provide the means to conduct Inventory Management.	EDR is not an inventory management solution however it possess the capability to provide endpoint inventory where EDR agent has been deployed. Request to modify this point for broader OEM participation and competitive bid. The solution must provide Endpoint Inventory and provide an option to export data in csv/xls format.	Kindly refer corrigendum