Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/007/2026-27)					
Sl. No.	**Page. No.**	**Point No:**	**Heading / Subheading**	**Queries**	**Pre-Bid Response**
1	15	2	Supported OS	Please list all OS versions in use, including legacy / EOL versions and Linux versions.	The solution should support Windows 10/11 64bit, Windows Server STD2019, 2022, 2025. Legacy OS (EOS) platform application support not required.
2	15	12	EDR Capability	Please confirm that the EDR capability should be validated by an independent evaluation.	The solution should provide advanced EDR capabilities, including real-time endpoint monitoring, behavioural analysis, threat detection, investigation, threat hunting, automated incident response, and containment. The tender does not mandate independent third-party evaluation of EDR capabilities. The proposed solution, however, will be assessed against the requirements in Annexure I/II (including items 12, 13, 43, 44 and 52) and through the technical demonstration under item 40.

NABFINS Ltd. BENGALURU

3	16	19, 49	Vulnerability / Patch	Please confirm whether the requirement is only visibility or also compensating controls, or actual patch deployment.	The requirement under Items 19 and 49 is limited to identification of vulnerable applications and OS components, risk-based visibility of endpoint vulnerabilities, identification of missing security patches, and remediation recommendations. The proposed solution patch control should be available in centerlised console. Apart from the endpoint security capabilities already specified in Annexure I/II (for example, firewall, application control, device control and endpoint isolation). Bidders may mention additional capabilities in their brochure.
4	16	18, 58, 59	SIEM / SOAR / ITSM	Please name the SIEM, SOAR and ITSM products and versions in use, so that integration can be confirmed.	Will be shared with the successful bidder.
5	14	5	Annexure 1, Scope of Work for selected vendor/bidder	As the bidder is required to uninstall and replace the existing EDR solution during the implementation phase, kindly confirm whether support from the incumbent OEM/vendor will be made available for agent removal, policy migration, troubleshooting, and transition activities.	The selected bidder shall be responsible for existing EDR agent removal, policy migration, troubleshooting and smooth transition to the proposed solution. The incumbent vendor support is not enlisted for the same. NABFINS DIT team will ensure all machines availability over remote desktop.

NABFINS Ltd.

6			General	Kindly provide details of the existing Endpoint Security / Antivirus / EDR solution currently deployed.	Will be shared with the successful bidder.
7			General	Kindly provide the details of existing SIEM and ITSM tool	Will be shared with the successful bidder.
8	15	2	Minimum Technical Requirement , Sl.No 2	Kindly provide the OS Distribution of Linux and MAC systems	The solution should support Windows 10/11 64bit, Windows Server STD2019, 2022, 2025. Legacy OS (EOS) platform application support not required.
9	15	7	Minimum Technical Requirement , Sl.No 7	Kindly clarify whether the Phishing Protection requirement refers to endpoint/web-based phishing protection capabilities within the EDR/XDR solution or includes email security functionality as part of the scope	Phishing Protection requirement is limited to endpoint and web-based phishing protection capabilities within the proposed Endpoint Protection/EDR solution. Email security functionality is excluded from the current scope.
10	15	8	Minimum Technical Requirement , Sl.No 8	Kindly elaborate on the expected scope and functionality of the Application Control requirement. While we can whitelist/block an application through EDR/XDR ,these capabilities may not be equivalent to a dedicated Application Control. Please clarify whether basic application control features within an EDR/XDR platform would be considered compliant.	Yes. Basic Application Control capabilities available within the proposed EDR solution shall be considered compliant. The solution should support application allow whitelisting/blocklisting and restriction of unauthorized or unapproved applications. A dedicated Application Control solution is not required as part of the current scope.

NABFINS Ltd. BENGALURU

Lazar A

11	16	17	Minimum Technical Requirement , Sl.No 17	Are any threat intelligence (TI) feeds/ TI Platform currently being utilized?	Currently no dedicated threat intelligence platform is being utilized. The proposed solution must meet Item 17 using the OEM's own continuously updated threat intelligence, and support custom IOC management under Item 44. The solution should also be able to share events and IOCs with the existing SIEM/SOC platform through standard mechanisms (Syslog, REST API, CEF/LEEF or equivalent) as per Items 18, 33 and 58. Further details of the existing environment will be shared with the selected bidder
12	16		Minimum Technical Requirement , Sl.No 27	Kindly elaborate on the expected offline protection capabilities. Specifically, please clarify whether the requirement pertains to malware detection and prevention in the absence of internet connectivity or any other specific functionality.	Item 27 requires that the endpoint agent continue to protect the endpoint when it is temporarily disconnected from the management console or the internet. At a minimum, the following should work locally, using the agent's on-board detection engines and the most recently downloaded policies and updates: Real-time malware and ransomware detection and prevention (Items 3-5), using local signature, heuristic, behavioural and machine-learning engines. Behavioural monitoring and exploit protection (Items 6 and 11), as supported by the agent. Enforcement of the last applied policies for device control, application control and host firewall

NABFINS Ltd. BENGALURU

					(Items 8-10). Tamper protection of the agent (Item 25). Local storage of events and detections, which sync to the console once connectivity is restored.
13	17	42	Minimum Technical Requirement , Sl.No42	Are DLP features expected from the same EDR/XDR tool?	Yes. DLP capabilities are expected to be provided as part of the proposed EDR/XDR solution, preferably through integrated functionality within the same platform.
14	18	54, 55	Minimum Technical Requirement , Sl.No 54, 55	Is there an existing Data Loss Prevention (DLP) solution deployed within the environment?	Yes. Basic DLP capabilities are currently available within the existing environment. However, enhancement of DLP functionalities is expected as part of the proposed solution.

NABFINS Ltd. BENGALURU

15	18	57	Minimum Technical Requirement , Sl.No 57	Kindly elaborate on the expected scope and functionality of the Web Upload Control requirement. As web upload restriction and data exfiltration control capabilities are typically associated with dedicated DLP, Secure Web Gateway (SWG), or Browser Security solutions, they may not be available as native features within EDR/XDR platforms	Basic Web Upload Control is expected as part of the proposed solution to monitor and restrict unauthorized uploads of sensitive data to external websites and cloud-based applications. Integrated DLP capabilities within the EDR/XDR platform will be acceptable. Dedicated SWG or Browser Security solutions are not mandatory.
16			Supported OS	Please list all OS versions in use, including legacy / EOL versions and Linux versions.	The solution should support Windows 10/11 64bit, Windows Server STD2019, 2022, 2025. Legacy OS (EOS) platform application support not required.
17			EDR Capability	Please confirm that the EDR capability should be validated by an independent evaluation.	The solution should provide advanced EDR capabilities, including real-time endpoint monitoring, behavioural analysis, threat detection, investigation, threat hunting, automated incident response, and containment. The tender does not mandate independent third-party evaluation of EDR capabilities. The proposed solution, however, will be assessed against the requirements in Annexure I/II (including items 12, 13, 43, 44 and 52) and through the technical demonstration under item 40.

NABFINS Ltd. BENGALURU

18			Vulnerability / Patch	Please confirm whether the requirement is only visibility or also compensating controls, or actual patch deployment.	The requirement covers endpoint visibility, identification of vulnerabilities and missing patches, and basic compensating controls. Actual patch deployment will be managed through the existing patch management process.
19			SIEM / SOAR / ITSM	Please name the SIEM, SOAR and ITSM products and versions in use, so that integration can be confirmed.	Will be shared with the successful bidder.
20			Quantity and scope	Please confirm that the current requirement is 2,339 laptop/desktop licenses and 15 Windows Server licenses, with one cloud console. Are virtual machines, Linux/macOS endpoints or additional devices included in the initial quantity?	Please align with the provisions of the RFP.
21			License term alignment	Please clarify when the three-year subscription term begins: contract execution, license activation, delivery, or completion of deployment.	The 03 years' license subscription period will start from the day the centralized console is configured and delivered to NABFINS.
22			Mandatory product features	Annexure I lists XDR, Endpoint DLP, MITRE ATT&CK mapping, automated response, IOC management and ITSM integration, but does not clearly state whether each is mandatory. Please identify which requirements are mandatory or optional, and whether these capabilities must be included in the quoted license.	EDR, Endpoint DLP, MITRE ATT&CK mapping, automated response, IOC management and ITSM integration shall be considered mandatory requirements. Vendors shall include these capabilities in the quoted licensing and clearly specify any additional licensing or subscription costs. Advanced XDR features may be quoted as optional.

NABFINS Ltd. BENGALURU

Lazar. A

23			Deployment schedule and dependencies:	The tender requires delivery of the Endpoint security solution within three weeks and endpoint installation within 60 days. Please confirm when each period starts and how delays caused by unavailable endpoints, branch coordination, remote-access restrictions or other NABFINS dependencies will be handled.	Vendor to align adequate resources to ensure delivery and installation within the RFP timelines. NABFINS shall cordinate and ensure machines' availability.
24			Branch Locations	Please share the list of branch locations including adderess location to accound for the breakup of the endpoints deployment and scheduled implementation timelines	Installation of endpoint security at branch offices is to be carried out remotely, using remote desktop software, by the 04 resources deployed by the selected bidder, in coordination with the branch offices (Annexure I, Scope of Work items 6 and 7).
25			Existing security product and migration	Please identify the current endpoint security product and any specific uninstall, migration or coexistence requirements. Please confirm whether NABFINS will provide necessary access, credentials and remote deployment facilities.	The selected bidder shall be responsible for existing EDR agent removal, policy migration, troubleshooting and smooth transition to the proposed solution. The incumbent vendor support is not enlisted for the same. NABFINS DIT team will ensure all machines availability over remote desktop.



26			Scope related clarification - Implementation of security	Please confirm -The scope of the RFP is limited to License procurement and Implementation only and Managed Security services for the proposed solution is out of scope for this RFP	The scope of this RFP is limited to license procurement, installation, configuration, deployment and implementation of the proposed solution. Managed Security Services (MSS), including ongoing monitoring and management by the service provider, are excluded from the current scope.
27			Future license additions and pricing	The tender allows additional licenses during the contract. Please clarify whether the quoted unit rates must remain fixed for all additional licenses and whether there is a maximum quantity or purchase threshold.	Numbers mentioned in the RFP is as per the current requirement. During the contract period NABFINS may require additional quantity of licences. Cost for the additional licence shall be billed pro-rata basis. Quoted unit rates shall remain fixed.
28			Future license additions and pricing	NABFINS may order additional licenses during the three-year term. Please confirm the maximum potential quantity, whether quoted unit rates remain fixed, and how pro-rata pricing will be calculated for additions so that all licenses expire on the same date.	Will be shared with the successful bidder.
29		14 & 16	Scope of Work – OEM (Sl. No. 2) / Sl. No. 28 – Cloud	The RFP specifies that the cloud console must have DC and DR within India. Kindly confirm whether the SaaS management console and all customer security-related data, including endpoint telemetry, logs and incident data, must be hosted	Yes. The SaaS management console and all customer security-related data, including endpoint telemetry, logs, incident data and backups should be hosted and stored exclusively in data centre located within India.

NABFINS Ltd. BENGALURU

				and stored exclusively in an Indian data centre.	
30		17	Sl. No. 41 – XDR	The RFP specifies Extended Detection and Response (XDR) across Endpoint, Identity, Email, Network and Cloud telemetry. Kindly confirm whether the proposed solution should support unified event correlation and threat detection across all these security domains.	Yes. The proposed solution shall support unified event correlation, threat detection and visibility across Endpoint, Identity, Network and Cloud security domains. Vendors shall ensure these capabilities are included in the proposed solution and clearly specify any additional licensing or integration requirements.
31		15 & 18	Sl. No. 2 – Supported OS / Sl. No. 48 – EOL/EOS Detection	Kindly confirm whether the EOL/EOS detection capability should identify unsupported and end-of-life operating systems across Windows, Linux and macOS environments, including their respective version details.	The requirement under Item 48 is limited to end-of-support (EOS) detection. End-of-life (EOL) detection is not required. The solution should identify operating systems and applications that are unsupported, meaning the vendor no longer provides security updates, on all endpoints running the proposed agent, covering every OS family listed in Item 2, as well as supported by the OEM.

NABFINS Ltd. BENGALURU

32		18	Sl. No. 47 – Software Inventory / Sl. No. 48 – EOL/EOS Detection	Kindly confirm whether the EOL/EOS detection feature should identify unsupported and end-of-life third-party applications, including Java, Adobe products, SQL Server, web browsers and other installed software, along with their version details.	Yes. The requirement includes End-of-Support (EOS) detection of OS, third-party applications, including web browsers and other installed software, along with their respective version details. EOL detection is not required.
33		18	Sl. No. 46 – Endpoint Asset Inventory	The RFP specifies hardware, OS, software, user, IP, agent and security-status inventory. Kindly clarify whether the endpoint asset inventory should also include hardware warranty expiry tracking and manufacturer End-of-Life (EOL)/End-of-Support (EOS) information.	Hardware warranty expiry tracking and manufacturer EOL information are not required. However, manufacturer End-of-Support (EOS) information may be included wherever available.
34		16	Sl. No. 19 – Vulnerability Management	The RFP specifies risk-based visibility of endpoint vulnerabilities. Kindly confirm whether the Vulnerability Management module should support CVE identification and CVSS-based vulnerability scoring and prioritization to facilitate risk-based remediation.	The Vulnerability Management module shall support CVE identification, CVSS-based vulnerability scoring and risk-based prioritization to facilitate effective vulnerability assessment and remediation.

NABFINS Ltd. BENGALURU

35		18	Sl. No. 49 – Patch Visibility	The RFP specifies identification of missing security patches and remediation recommendations. Kindly clarify whether the solution should also support automated OS and third-party application patch deployment, with administrator approval workflows and scheduled patch installation.	The requirement is limited to identifying missing security patches and providing remediation recommendations. Automated OS and third-party application patch deployment, including approval workflows and scheduled installations, is not required as part of the current scope.
36		14 & 15	Scope of Work / Sl. No. 2 – Supported OS	Kindly confirm whether the proposed solution should support centralized monitoring and management of Windows servers, Linux servers, laptops and desktops through the endpoint security platform.	The proposed solution shall support centralized monitoring and management of Windows servers, laptops and desktops through a unified endpoint security management console.
37		15 & 19–22	Sl. No. 14 – Central Management / Annexure II	Kindly confirm whether all endpoint security functionalities, including EDR, XDR, Vulnerability Management, Asset Inventory and Patch Management, should be managed through a single unified endpoint agent and centralized management console, without requiring multiple independent agents.	The proposed solution should provide centralized management through a unified management console and a single endpoint agent wherever technically feasible. Multiple independent agents should be avoided to minimize endpoint resource utilization and management complexity.

NABFINS Ltd. BENGALURU

Lagan.A

38		8	Bidder qualifications	Kindly clarify whether the bidder is required to have successfully executed similar Antivirus / Endpoint Security projects for BFSI/Government organisations (Central and State)/ PSUs/ Public and Pvt Ltd during the last 7 years. Also, please confirm whether projects completed within the last 7 years will be considered eligible and whether any minimum number or project value is prescribed.	Please align with the provisions of the RFP.
39		9	Bidder qualifications-EMD	In case a bidder avails EMD exemption by submitting a valid Udyam Registration Certificate as an eligible Micro or Small Enterprise (MSE), kindly clarify the mode of submission of Performance Security by the successful bidder. Whether the Performance Security can be remitted through direct bank transfer, or whether it must be submitted in the form of a Bank Guarantee (BG) or any other prescribed instrument? Further, kindly specify the applicable amount/percentage, validity period and the timeline for submission of such Performance Security.	Please align with the provisions of the RFP.



40			Annexure I – Technical Specifications	Kindly confirm whether the OEM must provide an escalation matrix and dedicated technical support for critical security incidents throughout the contract period.	The OEM shall provide prompt technical support in cases where the endpoint protection solution fails to detect or respond to malware attacks, or experiences service disruptions or operational issues, ensuring timely resolution and uninterrupted security operations.
41			Annexure I – Technical Specifications	Kindly clarify whether the existing antivirus solution, if any, must be uninstalled before deployment of the proposed solution. Will migration assistance be provided by the existing OEM/ SI or NABFINS?	The bidder shall be responsible for uninstalling the existing antivirus/endpoint protection solution and deploying the proposed solution.
42			General	OEM Solution should permits hosting any region should not restrict only in India since threat intelligence should be broader visibility and costing will be minimal compare to indian location	The OEM solution, including the management console and all customer security-related data, shall be hosted exclusively within India. The proposed solution must have both Primary DC and DR facilities located in India.
43			General	OEM may not have integration with Third Party SIEM. OEM can have their integration within their own SIEM	The proposed solution shall have the capability to integrate with third-party SIEM solutions, including log and security event forwarding through standard protocols or APIs. Integration capability is mandatory, even if the OEM provides its own native SIEM platform.



44			General	OEM solution may exclude in Endpoint DLP web upload, cloud storage, email, printing, clipboard etc. Since RBI has mandate Standalone DLP rather than keeping along with AV	Endpoint DLP capabilities shall be included in the proposed solution as per NABFINS requirements. The solution should support data protection controls covering web uploads, cloud storage, printing and clipboard activities. Vendors shall clearly specify the available functionalities and any additional licensing costs. Standalone DLP solutions may also be proposed, provided they meet all the required security and regulatory requirements.
45			General	OEM Solution should have **Unique Patented Solutions** for blocking all Malware , Virus and New sophisicated Threats occurs in Future	The proposed solution shall incorporate advanced and proven security technologies to detect, prevent and block malware, viruses, ransomware, zero-day attacks and emerging sophisticated threats. Patented technology may be considered an added advantage but shall not be mandatory.
46			General	OEM has Inbuilt Ticket Module , Need to integrate with other third party solution	The solution shall support integration with third-party ITSM/ticketing systems through standard APIs or other supported integration mechanisms. Availability of an inbuilt ticketing module is acceptable but shall not replace the mandatory third-party integration capability.



47			General	OEM Solution should exclude complete Endpoint DLP Features ie Cloud Upload and Web Upload. Since RBI has mandate Standalone DLP rather than keeping along with AV	Endpoint DLP capabilities shall be included in the proposed solution as per NABFINS requirements. The solution should support data protection controls covering web uploads, cloud storage, printing and clipboard activities. Vendors shall clearly specify the available functionalities and any additional licensing costs. Standalone DLP solutions may also be proposed, provided they meet all the required security and regulatory requirements.
48			General	OEM should permits installing multiple agents , cant be controlled within one single agents	The solution may use multiple agents wherever technically required to deliver the proposed security functionalities. However, centralized monitoring and management through a unified console shall be mandatory, with minimal endpoint resource utilization and compatibility with the existing IT environment.
49			General	OEM must exclude Automated response/playbooks based on defined conditions ,since it is SOAR activity should be part of SIEM not in Antivirus	Automated response/playbook orchestration based on predefined conditions (SOAR capabilities) is excluded from the current Endpoint Protection/EDR scope and shall be addressed through the SIEM/SOAR platform. Basic endpoint-level response actions, such as process termination and endpoint isolation, shall remain part of the EDR solution.

NABFINS Ltd. BENGALURU

Lazan

50			General	OEM Solution must exclude block and read options , since all OEM' solution has limitation on AV for other OS like linux and Mac	Please align with the provisions of the RFP.
51		2	Supported OS	Please list all OS versions in use, including legacy / EOL versions and Linux versions.	The solution should support Windows 10/11 64bit, Windows Server STD2019, 2022, 2025. Legacy OS (EOS) platform application support not required.
52		12	EDR Capability	Please confirm that the EDR capability should be validated by an independent evaluation.	The solution should provide advanced EDR capabilities, including real-time endpoint monitoring, behavioural analysis, threat detection, investigation, threat hunting, automated incident response, and containment. The tender does not mandate independent third-party evaluation of EDR capabilities. The proposed solution, however, will be assessed against the requirements in Annexure I/II (including items 12, 13, 43, 44 and 52) and through the technical demonstration under item 40.



53		19, 49	Vulnerability / Patch	Please confirm whether the requirement is only visibility or also compensating controls, or actual patch deployment.	The requirement under Items 19 and 49 is limited to identification of vulnerable applications and OS components, risk-based visibility of endpoint vulnerabilities, identification of missing security patches, and remediation recommendations. The proposed solution patch control should be available in centerlised console. Apart from the endpoint security capabilities already specified in Annexure I/II (for example, firewall, application control, device control and endpoint isolation). Bidders may mention additional capabilities in their brochure.
54		18, 58, 59	SIEM / SOAR / ITSM	Please name the SIEM, SOAR and ITSM products and versions in use, so that integration can be confirmed.	Will be shared with the successful bidder.
55			Payment Terms		Please align with the provisions of the RFP.
56			Profitability Criterion		Please align with the provisions of the RFP.



57			Annexure I - XDR requirement	For the mandatory XDR requirement across endpoint, identity, email, network and cloud telemetry, please list the specific NABFINS systems to integrate (identity provider/AD, email platform, firewalls, cloud tenants). Can XDR be met through integration of existing NABFINS logs, or must native OEM sensors be supplied? If extra connectors or licenses are needed, which BOQ line should carry them?	NABFINS requires XDR integration covering endpoint devices (desktops, laptops and servers) and network security devices, including firewalls and other supported network components.
58			Annexure I - Endpoint DLP	Is Endpoint DLP required on all 2339 laptops/desktops and all 15 servers? Will NABFINS provide data classification and DLP policies, or is the bidder expected to design them? Is a separate DLP license acceptable if bundled within the agent price?	Please align with the provisions of the RFP.
59			Annexure I - Supported OS vs BOQ lines	How many of the 2339 laptops/desktops run macOS or Linux, and are there any Linux servers?	The solution should support Windows 10/11 64bit, Windows Server STD2019, 2022, 2025. Legacy OS (EOS) platform application support not required.
60			Scope - remote installation across 19 states	Which remote desktop software and software distribution tool will NABFINS provide for branch installations? Will branch users and admin credentials be made available?	The details will be shared with the successful bidder. The solution can be installed remotely, and NABFINS DIT will provide the necessary support and assistance during the implementation.

NABFINS Ltd. BENGALURU

61			Timelines - installation within 60 days	Will delays attributable to NABFINS be excluded from the 60-day installation period and from the related LD? Examples include branch unavailability, offline devices, network issues and access delays.	NABFINS DIT will provide the necessary support and assistance during the implementation.
62			Timelines, Order Cancellation and LD clauses	Please clarify the start reference for the 3-week license and console delivery: PO issue date, PO acceptance/receipt, or agreed schedule.	PO issue date.
63			Contract period / Price Validity	From which date does the 3-year license subscription start: PO, license delivery, console activation or installation completion? Is this the same as contract execution?	The 03 years' license subscription period will start from the day the centralized console is configured and delivered to NABFINS.
64			BOQ - Cost for resource (man power), 4 Nos	How should the resource line (4 Nos) be priced: lump sum per resource, per month, or per man-day? What is the expected engagement duration? Will any extension beyond 60 days caused by NABFINS be paid separately?	The cost of resource shall be mentioned for each resource, borne by the bidder and the timeline is for completing the entire installation. NABFINS will not pay any additional cost.
65			Price Validity / Rate Validity and Pro-rata	For additional licenses on a pro-rata basis, Is a minimum order quantity acceptable as per OEM policy?	Will be shared with the successful bidder.

NABFINS Ltd. BENGALURU

66			Award Method - QCBS; Annexure II 59 features; demonstration	Please share the detailed technical evaluation criteria for the 70% technical score: marks per parameter, demonstration rubric and minimum qualifying score. Will partial No responses in Annexure II lead to disqualification or only reduced marks?	Please refer to extant provisions of the RFP.
67			Integrity Pact - Section 3 damages	What is meant by liquidated damages of the Contract value under Integrity Pact Section 3? Is there an upper cap?	Please refer to extant provisions of the RFP.
68			Eligibility - Turnover and Profitability	If audited financials are not yet available at submission, is a provisional CA certificate with UDIN acceptable for turnover and profitability?	If audited financials are not available, provisional CA certificate is acceptable (with UDIN).

NABFINS Ltd. BENGALURU

69			Eligibility - Turnover and Profitability	We request that the requirement of minimum annual turnover of ₹300 lakh in each individual financial year may kindly be replaced with a minimum average annual turnover of ₹300 lakh during the last three financial years.	Please refer to extant provisions of the RFP.
70			SIEM Integration, API, ITSM Integration requirements	Which SIEM, SOAR and ITSM tools does NABFINS currently use? Is a native connector required, or are Syslog/CEF/REST API exports sufficient?	Will be shared with the successful bidder.
71			SLA / Support Requirements	What severity definitions and response/resolution times does NABFINS expect for the support SLA? Is onsite support required after installation, or only remote/OEM support?	The support from the OEM shall be online. Response and resolution timeline will be defined on the contract.
72			Scope - Demonstration by eligible bidders	What is the format, duration and date of the demonstration? Will it be a live cloud tenant or a PoC on NABFINS endpoints?	Technically qualified bidders need to arrange for demonstration and the dates will be notified by Nabfins

NABFINS Ltd. BENGALURU

73			Experience	As per the RFP, Bidder prior similar experience with Govt or Enterpise will be exceptable ?	Please refer to extant provisions of the RFP.
74			Annexure I - Spec 10 Firewall	Spec 10 – Firewall: We request NABFINS to kindly add the following to the existing requirement: "Centrally managed application-based inbound/outbound network control enforced by the endpoint agent, and/or central management of the OS-native host firewall (inbound/outbound application, port and network rules) from the OEM console, shall also be considered compliant."	The XDR integration requirement shall be limited to endpoint devices (desktops, laptops and servers) and network security devices, including firewalls and other supported network components.
75			Annexure I - Spec 14 Central Management	Spec 14 – Central Management: We request NABFINS to kindly add: "The centralized management may be delivered through integrated web-based consoles/modules of the same OEM, accessible with single sign-on and providing a unified dashboard for alerts and reports."	The centralized management solution may be provided through integrated web-based consoles or modules from the same OEM, provided that it supports single sign-on (SSO), centralized administration, and a unified dashboard for security alerts, monitoring and reporting. All specified functional and security requirements must be met.



76			Annexure I - Background, Spec 26 Performance, Spec 31 Deployment	Annexure I – Background : We request NABFINS to kindly add: "The endpoint solution may comprise one or more agents/modules from the same OEM, provided all are centrally deployed and managed."	The endpoint protection solution may comprise one or more agents or modules from the same OEM, provided that all components are centrally deployed, managed and monitored through a unified management console, meeting the specified security requirements.
77			Annexure I - Spec 41 XDR	Spec 41 – XDR: We request NABFINS to kindly add: "XDR telemetry for identity, email, network and cloud may be achieved through the OEM's native sensors and/or through integration and ingestion of logs from NABFINS's existing identity, email, network and cloud platforms into the OEM's XDR/analytics platform."	XDR integration shall be limited to endpoint devices (desktops, laptops and servers) and network security devices, including firewalls and other supported network components. Integration may be achieved through native OEM sensors/connectors or existing NABFINS logs and APIs, wherever technically feasible, ensuring effective threat detection, correlation, investigation and response.
78			Annexure I - Spec 50 Endpoint Risk Score	Spec 50 – Endpoint Risk Score: We request NABFINS to kindly add: "Risk-based classification/tagging of endpoints (e.g., Critical/High/Medium/Low) derived from vulnerabilities, threats, configuration and posture shall also be considered compliant."	Risk Score can be defined as per OEM/NABFINS Standard.

NABFINS Ltd. BENGALURU

79			Annexure I - Spec 12 EDR Capability	Spec 12 – EDR Capability: We request NABFINS to kindly add the required telemetry retention period, e.g.: "Endpoint telemetry for threat hunting shall be retained for a minimum of 30 days online; extended retention may be offered as an option."	The solution should provide advanced EDR capabilities, including real-time endpoint monitoring, behavioural analysis, threat detection, investigation, threat hunting, automated incident response, and containment. The tender does not mandate independent third-party evaluation of EDR capabilities. The proposed solution, however, will be assessed against the requirements in Annexure I/II (including items 12, 13, 43, 44 and 52) and through the technical demonstration under item 40.
80			Annexure I - Scope of Work for OEM (Point 2), Spec 28 Cloud, Spec 30 HA	Scope of Work for OEM, Point 2 / Spec 28 – Cloud: We request NABFINS to kindly add: "Hosting on the OEM's India cloud region with high availability across multiple availability zones/data centres within India shall be considered compliant with the DC and DR requirement. OEM's global threat-intelligence/reputation lookups (file hashes, URLs) that do not store NABFINS data outside India are permitted."	The requirement is that the centralized console is hosted with both the Data Centre (DC) and the Disaster Recovery (DR) site located inside India. The hosting may be on a public cloud provider's infrastructure or in the OEM's own data centres. Bidders must state in the technical responsethe hosting model, the provider, the location of the DC and DR sites and the architecture, as required by Item 28.

NABFINS Ltd. BENGALURU

81	Page 15 & Page 19	Clause 9: Device Control	Annexure I & Annexure II	Control of removable media such as USB storage devices, external drives and other peripherals. Policies shall support allow/block/read-only controls where applicable. Kindly confirm whether native OS-level USB blocking/rules or scripts can be leveraged for Linux servers if USB lockdown is strictly required, while dedicated enterprise Device Control policy management is deployed across Windows and macOS workstations	NABFINS right now don't have any Linux-based machines in its current IT environment. Therefore, Linux-specific USB control requirements are not applicable. The bidder shall ensure removable media control through centralized Device Control policies across Windows endpoints, supporting allow, block and read-only controls wherever applicable.

NABFINS Ltd. BENGALURU

Lazarus

82	Page 16 & Page 21	Clause 28: Cloud & Scope of Work for OEM: Item 2	Annexure I & Annexure II	Solution shall be cloud-hosted, as specified by the purchaser. Vendor shall clearly state architecture, data location and infrastructure requirements. Kindly clarify and permit a Hybrid Management Architecture, wherein: EDR, Threat Hunting, and remediation activities are delivered via OEM Cloud with local India data residency and the Management of Endpoint protection and DLP solutions will be hosted on Customer's designated private cloud. Alternatively, kindly amend the clause to : Solution shall be cloud-hosted/Hybrid, as specified by the purchaser. Vendor shall clearly state architecture, data location and infrastructure requirements	Please refer to extant provisions of the RFP.

NABFINS Ltd. BENGALURU

83	Page 17 & Page 21	Clause 41: XDR	Annexure I & Annexure II	Extended Detection & Response across endpoint, identity, email, network and cloud telemetry. Kindly clarify and confirm that the scope of this tender is primarily focused on Endpoint Detection and Response (EDR) with open integration/export capabilities to external telemetry sources (Identity, Email, Network, Cloud) or an enterprise SIEM/SOC platform via standard APIs/Syslog Alternatively, kindly amend the clause to : 'The endpoint platform shall support rich endpoint telemetry collection and provide open APIs / integration mechanisms to ingest, share, or correlate telemetry with enterprise SIEM/XDR/SOC solutions for identity, network, email, and cloud visibility.	The primary scope of this tender is Endpoint Detection and Response (EDR), with XDR capabilities covering endpoint devices and network security devices, including firewalls. The solution shall support integration with the existing SIEM/SOC platform through standard APIs, Syslog or other supported integration mechanisms for centralized monitoring, threat detection, event correlation and incident response.
84		2, 29, 32	Environment	Provide total endpoint count and breakup by Windows workstations, Windows servers, Linux, macOS and virtual machines.	Please refer to extant provisions of the RFP.

NABFINS Ltd. BENGALURU

85		2	Environment	Provide the exact Windows editions/builds, Linux distributions and macOS versions to be supported.	The solution should support Windows 10/11 64bit, Windows Server STD2019, 2022, 2025. Legacy OS (EOS) platform application support not required.
86		10	Firewall	Confirm whether centralized management of the native Windows firewall is acceptable, or a proprietary host firewall is mandatory.	Centralized management of the native Windows Firewall is acceptable, provided the solution supports centralized policy configuration, monitoring, enforcement and reporting. A proprietary host firewall is not mandatory, provided all specified security requirements are met.
87		10	Firewall	Confirm whether the host-firewall requirement applies to Windows only or also to macOS and Linux.	The host-firewall requirement is applicable to Windows endpoints. Linux-specific requirements are not applicable, as NABFINS does not have Linux-based machines in its current IT environment. Centralized management and monitoring shall be supported wherever applicable.
88		26	Performance	Define acceptable CPU, RAM, disk and bandwidth impact and whether these values must be demonstrated during PoC.	The endpoint protection solution shall have minimal impact on CPU, RAM, disk utilization and network bandwidth without affecting the normal performance or availability of business applications. The bidder shall provide the OEM-recommended resource utilization specifications. These parameters shall be evaluated and demonstrated during the technical demonstration to ensure acceptable

NABFINS Ltd. BENGALURU

					performance under normal operating conditions.
89		19, 21, 49, 50	Vulnerability	Confirm whether endpoint telemetry is sufficient or an authenticated vulnerability scanner is mandatory.	The solution shall provide visibility about missing security patches, outdated software, known vulnerabilities and endpoint misconfigurations. Integration with external vulnerability assessment tools is not required.
90		49	Patch	Confirm whether the scope is missing-patch visibility only or also patch deployment/remediation.	The requirement covers endpoint visibility, identification of vulnerabilities and missing patches, and basic compensating controls. Actual patch deployment will be managed through the existing patch management process.
91		48	EOL/EOS	Confirm whether an OEM-maintained lifecycle database is mandatory or query-based reporting is acceptable.	An OEM-maintained lifecycle database is not mandatory. Query-based reporting is acceptable, provided the solution can identify and report End-of-Support (EOS) operating systems and software versions accurately.

NABFINS Ltd. BENGALURU

92		50	Risk score	Define the required endpoint risk-scoring methodology, factors and weighting.	Risk Score can be defined as per OEM/NABFINS Standard.
93		41, 58, 59	XDR	Identify current identity, email, firewall, cloud, SIEM, SOAR and ITSM products and versions.	Details of the existing IT infrastructure, including product names, versions and integration requirements, will be shared with the successful bidder, wherever required for implementation and integration. SOAR and ITSM solutions are currently not available in NABFINS.
94		41	XDR	Specify required telemetry retention for endpoint, Data Lake, detections, cases and audit logs.	The solution shall support a minimum of 30 days of online retention for endpoint telemetry, security detections, incident cases and audit logs required for threat hunting and investigation. The bidder shall clearly specify the Data Lake retention capacity, storage requirements and associated costs for any extended retention period.
95		44	IOC	For hashes, IPs, domains and URLs, specify whether detection, searching, blocking and remediation are mandatory for every type.	The solution shall support detection, searching, threat investigation and blocking of malicious file hashes, IP addresses, domains and URLs. Remediation capabilities shall be provided wherever technically feasible. The bidder shall clearly specify the supported capabilities for each IOC type.

NABFINS Ltd. BENGALURU

Lazar

96		44	IOC	Confirm whether STIX/TAXII, bulk import/export, expiry, tagging and approval workflow are mandatory.	Not mandatory.
97		45	Automation	Confirm whether an embedded SOAR/playbook engine is mandatory or existing SIEM/SOAR automation is acceptable.	An embedded SOAR or playbook engine is not mandatory. The solution shall provide built-in incident detection, alerting and response capabilities, including automated endpoint isolation and threat containment wherever supported. Integration with the existing SIEM solution may be considered for centralized monitoring and security event correlation.
98		45, 58	Automation	List mandatory response actions and whether analyst approval is required before execution.	The solution shall support the following response actions, wherever technically feasible: - Isolation of infected or compromised endpoints. - Blocking of malicious file hashes, IP addresses, domains and URLs. - Quarantine or removal of detected malware. - Termination of malicious processes. - Initiation of endpoint remediation actions. - Generation of alerts and incident notifications. Automated response actions shall support configurable approval workflows. Critical actions impacting business operations shall require authorized analyst or

NABFINS Ltd. BENGALURU

					administrator approval before execution.
99		42, 54-57	DLP	Confirm the operating systems on which complete DLP functionality is mandatory.	Complete DLP functionality shall be mandatory for Windows endpoints. The bidder shall ensure centralized policy management, monitoring and enforcement of data protection controls across the supported operating systems. Linux-specific requirements are not applicable, as NABFINS does not have Linux-based machines in its current IT environment.

NABFINS Ltd. BENGALURU

100		42	DLP	Confirm mandatory DLP channels: USB, web, cloud storage, email, print, clipboard, network share and collaboration applications.	DLP shall cover removable media (USB storage devices), web uploads, cloud storage, printing, clipboard operations and network file sharing, wherever supported by the respective operating systems. Email DLP is not required. The bidder shall clearly specify the supported DLP channels and enforcement capabilities across Windows and macOS endpoints.
101		42	DLP	Confirm whether email DLP may be delivered through an integrated email-security service.	Email DLP not required.
102		56	DLP	List personal and corporate cloud-storage services that must be controlled.	The solution shall support monitoring and control of commonly used personal and corporate cloud-storage services, including Google Drive, Microsoft OneDrive, Dropbox and other similar file-sharing platforms. The bidder shall specify the supported services and available enforcement capabilities.
103		55	DLP	Clarify the meaning of DLP quarantine: file quarantine, transfer block, evidence copy or analyst review.	DLP quarantine shall primarily refer to blocking unauthorized data transfers and preventing sensitive data leakage. The solution shall also provide file quarantine, evidence capture and incident review capabilities for investigation and audit purposes.

NABFINS Ltd. BENGALURU

Lagan

104		42	DLP	Specify sensitive-data types and whether regex, exact data match or document fingerprinting is required.	Please refer to extant provisions of the RFP.
105		18, 58	SIEM	Identify the existing SIEM/SOC platform, version and mandatory export format.	Will be shared with the successful bidder.
106		58	SIEM	Define which response actions must be initiated from SIEM/SOAR back into the endpoint/XDR platform.	The solution shall support response actions through the endpoint/XDR platform, including endpoint isolation, termination of malicious processes, malware quarantine/removal and blocking of malicious file hashes, IP addresses, domains and URLs, wherever technically feasible. Integration with SIEM for initiating response actions is not mandatory. The solution shall support centralized incident monitoring, investigation and response through its management console.
107		59	ITSM	Identify the ITSM product/version and required ticket creation and bidirectional status synchronization workflow.	NABFINS does not currently have an ITSM solution in place. Therefore, ITSM integration and bidirectional ticket synchronization are not mandatory under the present scope.

NABFINS Ltd. BENGALURU

108		28, 34	Cloud	Specify required data-hosting region and applicable data-residency restrictions.	Please refer to extant provisions of the RFP.
109		34	Compliance	Identify the specific statutory, regulatory, data-protection and audit requirements.	The solution shall comply with applicable RBI cybersecurity guidelines and directions, CERT-In directions, the Digital Personal Data Protection Act, 2023, and other relevant statutory, regulatory and data-protection requirements applicable to NABFINS. The solution shall also support audit requirements, security log retention, incident reporting, monitoring and evidence preservation.
110		22	Audit	Specify audit-log retention and define whether tamper-resistant means immutable/WORM storage or restricted modification.	Audit logs shall be retained for a minimum period of 180 days online, or as required by applicable regulatory guidelines, whichever is higher. Tamper-resistant storage shall ensure that audit logs cannot be altered or deleted by unauthorized users. Immutable/WORM storage or equivalent controls providing protection against unauthorized modification and deletion shall be acceptable.

NABFINS Ltd. BENGALURU

Lazar A

111		30	HA	Confirm OEM-managed SaaS redundancy, DR and continuity satisfy the HA and backup/restore requirement.	The endpoint protection solution must operate independently on standalone machines without causing any application downtime or service disruption.
112		32, 37	Licensing	Confirm subscription term, endpoint/server quantities and whether DLP, vulnerability management and integrations may be separate line items.	Please refer to extant provisions of the RFP.
113		35, 36	Support	Provide severity-based response and restoration SLA targets and required OEM involvement.	The support from the OEM shall be online. Response and resolution timeline will be defined on the contract.
114		40	Demo	Define PoC duration, endpoint count, mandatory use cases and success criteria.	Bidder needs to provide technical demonstration. PoC not envisaged.
115			Bid format	Confirm whether Partial/Complied with dependency and explanatory remarks are permitted in addition to Yes/No.	Bidders shall clearly indicate status of compliance with technical requirements.

NABFINS Ltd. BENGALURU