Stock Holding Corporation of India Limited

(StockHolding)

RFP Reference Number: IT-08/2024-25

Date: 09-Sep-2024

GEM Reference No. - GEM/2024/B/5378533

REQUEST FOR PROPOSAL FOR ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION FOR STOCKHOLDING

DISCLAIMER

The information contained in this Request for Proposal (RFP) document or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Stock Holding Corporation of India Limited (StockHolding), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by StockHolding to any parties other than the applicants who are qualified to submit the bids ("bidders"). The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. StockHolding makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. StockHolding may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

RFP Document Details

Sr. No.	Description	Remarks
1	Name of Organization	Stock Holding Corporation of India Limited
2	RFP Reference Number	IT-08/2024-25
3	Requirement	Request for proposal (RFP) for Endpoint Detection and Response (EDR) solution for StockHolding
4	Interest free Earnest Money Deposit (EMD) [*]	Rs.2,00,000/- (Indian Rupees Two Lakhs only) by way of RTGS/NEFT to be paid to Stock Holding Corporation of India Limited as Earnest Money Deposit should be submitted separately before submission of online bids by way of RTGS/NEFT on StockHolding's Bank Account No.: 004103000033442 Bank: IDBI Bank (Nariman Point Branch) IFSC: IBKL0000004. Please share the UTR details to us on below mentioned email address.
5	Email Id for queries up to Pre-Bid Meet	PRIT@stockholding.com
6	Date of Issue of RFP Document	09-Sep-2024
7	Date, Time and place for online Pre-bid meeting	18-Sep-2024 11:00 AM For participation in pre-bid meeting, please send mail for online meeting link to PRIT@stockholding.com before 17-Sep-2024 05:00 PM
8	Last Date for Submission of Online Bid	30-Sep-2024 07:00 PM
9	Date of opening bid	30-Sep-2024 07:30 PM

[*] - Bidders registered under Micro, Small and Medium Enterprises (MSME) for specific trade are exempted from EMD. Bidders shall upload the scanned copy of necessary documents as part of eligibility criteria documents.

This bid document is not transferable.

StockHolding reserves the right to modify/update activities/ dates as per requirements of the process.

Table of Contents

SUBMISSION OF PROPOSAL....5
ELIGIBILITY CRITERIA (Documents to be Submitted Online)....7
BIDS PREPARATION AND SUBMISSION DETAILS....9
Submission of Bids....9
Evaluation of Bids....9
REQUIREMENT....10
Scope of Work....10
Technical Specification....15
Bidder Responsibility....23
Service Level Agreement (SLA) and Penalty....23
Penalty Clause....24
Contract Duration....25
Terms and Conditions....25
Refund of Earnest Money Deposit (EMD):....26
Performance Bank Guarantee (PBG):....26
Force Majeure....26
Dispute Resolution....26
Right to alter RFP....27
Integrity Pact....27
Non-Disclosure Agreement (NDA)....27
Indemnify....27
Limitation of Liability....27
Subcontracting....27
Termination Clause....27
ANNEXURE - 1 - Details of Bidder's Profile....28
ANNEXURE - 2 – Eligibility Criteria....29
ANNEXURE – 3 – Technical Bid....31
ANNEXURE - 4 - Commercial Price Bid Format....40
ANNEXURE - 5 – Integrity Pact....41
ANNEXURE- 6 - Covering Letter on bidder's Letterhead of Integrity Pact....47
ANNEXURE – 7 – Compliance Statement....48
ANNEXURE – 8 – Format of Bank Guarantee....49

SUBMISSION OF PROPOSAL

StockHolding invites e-tender through GeM Portal, in two bid system (Technical and Commercial bid), from firm/company/ to avail Endpoint Detection and Response (EDR) solution for StockHolding

Submission of Bids:
The online bids will have to be submitted within the time specified on website https://gem.gov.in/ the following manner:-

1. Technical Bid (.pdf files)
2. Commercial Bid (.pdf files)

Invitation for bids:
This "Invitation for bid" is meant for the exclusive purpose of "Endpoint Detection and Response (EDR) solution for StockHolding as per the terms, conditions, and specifications indicated in this RFP and shall not be transferred, reproduced or otherwise used for purposes other than for which it is specifically issued. The purpose of this RFP to appoint suitable bidder for implementing cloud based Endpoint Detection and Response (EDR) solution for StockHolding is multifaceted, aiming to address critical cybersecurity needs related to endpoint protection, detection of threats, and rapid response capabilities.

Due Diligence:
The bidder is expected to examine all instructions, Forms, Terms, Conditions and Specifications in this RFP. Bids shall be deemed to have been made after careful study and examination of this RFP with full understanding of its Implications. The Bid should be precise, complete with all details required as per this RFP document. Failure to furnish all information required by this RFP or submission of Bid not as per RFP requirements will be at the bidder's risk and may result in rejection of the bid and the decision of StockHolding in this regard will be final and conclusive and binding.

Cost of Bidding:
The bidder shall bear all costs associated with the preparation & submission of its bid and StockHolding will in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

Contents of this RFP Document:
The requirements, bidding procedure, general terms & conditions are prescribed in this RFP document with various sections

a Bidder Details – Annexure 1
b Format for Eligibility Criteria - Annexure 2
c Format for Technical Bid – Annexure 3
d Format for Price Bid (Commercial) Bids - Annexure 4
e Integrity Pact (Text) - Annexure 5
f Covering Letter of Integrity Pact - Annexure 6
g Compliance Statement – Annexure 7
h Format of Bank Guarantee – Annexure 8

Clarifications regarding RFP Document:

a) Before bidding, the bidders are requested to carefully examine the RFP Document and the Terms and Conditions specified therein, and if there appears to be any ambiguity, contradictions, gap(s) and/or discrepancy in the RFP Document, they should forthwith refer the matter to StockHolding for necessary clarifications.
b) A bidder requiring any clarification for their queries on this RFP may be obtained via email to PRIT@StockHolding.com
c) StockHolding shall not be responsible for any external agency delays.
d) StockHolding reserves the sole right for carrying out any amendments / modifications / changes in the bidding process including any addendum to this entire RFP
e) At any time before the deadline for submission of bids / offers, StockHolding may, for any reason whatsoever, whether at its own initiative or in response to a clarification requested by bidders, modify this RFP Document.
f) StockHolding reserves the rights to extend the deadline for the submission of bids, if required. However, no request from the bidders for extending the deadline for submission of bids, shall be binding on StockHolding.
g) StockHolding reserves the right to amend / cancel / postpone / pre-pone the RFP without assigning any reasons.
h) It may be noted that notice regarding corrigendum/addendums/amendments/response to bidder's queries etc., will be published on StockHolding's website only. Prospective bidders shall regularly visit StockHolding's same website for any changes/development in relation to this RFP.
i) It may be noted that bidder mentioned in the document may be either OEM/Distributor/System Integrator (SI).

Validity of offer:

The offer should remain valid for a period of at least **90 days** from the date of submission.

ELIGIBILITY CRITERIA (Documents to be Submitted Online)

Guidelines to be followed prior to submitting an application-

Bidder should upload all supporting documents at the time of submission duly signed and stamped on their company's letter head.

SI.	Criteria	Documents to be submitted by Bidder
1	The Bidder should be a registered Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 with experience of implementing Endpoint Detection and Response (EDR) solution for at least 05 (five) years.	▪ Copy of Certificate of Incorporation issued by the Registrar of Companies ▪ Copy of PAN and GST ▪ Self-declaration by the bidder on company Letter Head duly signed by the Authorized Signatory
2	Should have an average annual turnover of at least Rs. 50 Lakhs per annum for last 05 (five) financial years (2019-20, 2020-21, 2021-22, 2022-23 and 2023-24). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last 05 (five) financial years.
3	Bidder should have positive Net worth in the last 05 (five) audited financial years	Certificate from CA mentioning Net worth for the past 05 (five) financial years.
4	The Bidder should have experience of EDR with DLP implementation through Cloud based and deployment of minimum 3000 agents at customer premises in any Financial Institution / PSU / Government Organization / Large Corporates in India not older than 03 (three) years from RFP date.	Copy of Purchase Orders / Completion Certificate
5	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 2 (two) years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
6	The bidder must have following valid Certifications: • ISO 27001:2013 certified	Relevant ISO Certificate
7	The proposed EDR Solution must be listed as leaders in Gartner's latest Magic quadrant for End Point Protection/leaders or strong performers in Forrester Wave's latest report for EDR Solutions or Top 3 Leader's as per the IDC's latest Endpoint security market share report.	Copy of latest Gartner's/ Forrester's Report clearly highlighting the proposed EDR solution.
8	For Endpoint DLP, The proposed DLP must be listed as leaders in Gartner's latest Magic quadrant or strong performers in Forrester Wave's latest report. Note: Above criteria is not applicable for integrated endpoint DLP with proposed EDR.	Copy of latest Gartner's/ Forrester's Report clearly highlighting the proposed Endpoint DLP
9	Bidder to submit MAF (Manufacturer Authorization Certificate) from OEM with tender reference number	MAF from OEM to be submitted.
10	Bidder must have support office/center at Tier 1 cities in India.	GST and address to be provided along with Contact Details

11	Bidder to provide undertaking that no penalties, amounting to up to 10% of the contract value per year, have been imposed in the last three years by any of its client(s).	Self-declaration from bidder on their letter head duly signed by authorized signatory
12	OEM proposed solution should be in-line with SEBI regulatory Framework.	Confirmation on OEMs letterhead with reference to Circular numbers and points.

BIDS PREPARATION AND SUBMISSION DETAILS

The online bids will have to be submitted within the time specified on website https://gem.gov.in/ . Bidders must familiarize (if not already) with the Portal and check/ fulfil the pre-requisites to access and submit the bid there.

Submission of Bids

a) The required documents for Eligibility Criteria, Commercial Bid must be submitted (uploaded) online on GeM portal. Eligibility Criteria and Commercial Bid should be complete in all respects and contain all information asked for in this RFP document
b) The offer should be valid for a period of at least 90 days from the date of submission of bid.
c) The Bidder shall fulfil all statutory requirements as described by the law and Government notices. The Bidder shall be solely responsible for any failure to fulfil the statutory obligations and shall indemnify StockHolding against all such liabilities, which are likely to arise out of the agency's failure to fulfil such statutory obligations.
d) The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP document(s). Failure to furnish all information required as mentioned in the RFP document(s) or submission of a proposal not substantially responsive to the RFP document(s) in every respect will be at the bidder's risk and may result in rejection of the proposal.
e) Delayed and/or incomplete bid shall not be considered.
f) There may not be any extension(s) to the last date of online submission of Eligibility Criteria details and commercial Price bids. This will be at the sole discretion of StockHolding.

Evaluation of Bids

StockHolding will evaluate the bid submitted by the bidders under this RFP. The eligibility bid submitted by the Bidder will be evaluated against the Eligibility criteria set forth in the RFP. The Bidder needs to comply with all the eligibility criteria and technical specifications mentioned in the RFP to be evaluated for evaluation. Noncompliance to any of the mentioned criteria would result in outright rejection of the bidder's proposal. The decision of *StockHolding* would be final and binding on all the bidders to this document.

StockHolding may accept or reject an offer without assigning any reason what so ever. The bidder is required to comply with the requirement mentioned in the RFP. Non-compliance to this may lead to disqualification of a bidder, which would be at the discretion of *StockHolding*.

g) Please note that all the information desired needs to be provided. Incomplete information may lead to non-consideration of the proposal.
h) The information provided by the bidders in response to this RFP document will become the property of StockHolding.

Evaluation Process

First the 'Eligibility Criteria bid document' will be evaluated and only those bidders who comply the Eligibility criteria and Technical Specification will be eligible for 'Commercial bid'. In the second stage, for only those bidders who meets the 'Eligibility Criteria', Commercial bids will be opened. Further, L1 bidder will be selected based on the lowest quote submitted by the bidder.
Further, StockHolding reserves the right to negotiate with L1 bidder and based on the negotiation price submitted, order will be placed to the selected bidder.

REQUIREMENT

Stockholding inviting bids from firm/company/organization for implementing Cloud based Endpoint Detection and Response (EDR) solution for StockHolding and support for the period of 03 (three) years with 02 (two) years as extension.

The scope of work for Endpoint Detection and Response (EDR) involves following key components to ensure comprehensive protection and response capabilities for endpoints (computers, laptops, servers, cloud deployments etc.) along with device control, Data loss protection (DLP), device discovery and Threat hunting to be provided jointly by OEM and successful bidder to support StockHolding's endpoints through StockHolding's proxy servers.

Proposed solution should interoperate without obstructing other endpoint security solutions and software's deployed in StockHolding.

The solution should comply and meet all technical features as proposed in this RFP as StockHolding will evaluate and use all the features in our environment. All feature customisation, enabling, disabling, and parameterisation during the contract period to be ensured by successful bidder / OEM without any additional cost to the StockHolding.

If required, the StockHolding or its subsidiaries (maximum 1,000) may purchase additional licences at the same rate as discovered in the RFP during the Contract period.

Scope of Work

The successful bidder shall adhere to the following activities as part of their scope during the engagement period.

a) The successful bidder has to provide detailed solution document, project implementation plan, architecture diagram (HLD and LLD) for proposed EDR solution, within fifteen days from the date of issuance of purchase order by the StockHolding. The solution provider should provide a detailed Plan of action (POA) for implementation of entire solution as per the RFP within 15 days of issuance of PO.
b) Provision of 2900 enterprise licenses from OEM for endpoint security solution by successful bidder.
c) Fixing of Configuration Security Review findings, after first setup and thereafter as and when carried out by Security team or compliance audit findings within the prescribed time limits.
d) Solution will be rolled out only after closure of all security findings by OEM and Bidder and review by StockHolding.
e) For all types of technical support services/ Essential Support: 24x7x365 days with named Technical Account Manager (TAM) must be provided to StockHolding & SLA where involvement of OEM is required. There should be a back-to-back agreement between StockHolding and successful bidder/OEM.
f) Successful Bidder will ensure Services from the OEM to be available round the clock during the contract period.

Scope of work shall include:

a) Enhanced Endpoint Security

Stockholding has approx. 2900 end points and servers spanning across 210+ branches and corporate office. OEM has to complete the installation and implementation on 5% of endpoints devices post they will handover to their bidder for completing the deployment on remaining endpoints in a phase wise manner.

1. **Phase 1 Implementation:** Implementation and configuration of dedicated tenant on Cloud for StockHolding's Next generation antivirus and Endpoint Detection and Response, Device control, Endpoint firewall, Data loss Prevention, Vulnerability assessment, Device discovery, Sandboxing, 24x7x365 Managed Threat Hunting, File Integrity monitoring, Rogue and unmanaged device

detection, API integration and Reporting modules and deployment of agents for Mahape Location by OEM and bidder (Servers and desktop Systems - Number of Counts 150 + 850).

2. **Phase 2 Implementation:** Deployment in StockHolding's Branch locations - Number of Counts. 1000 end points
3. **Phase 3 Implementation:** Deployment in StockHolding's Branch locations - Number of Counts. 1000 end points along with all activities as mentioned below.

b) Pre-Deployment Phase

1. Conduct a current state assessment of existing endpoint security measures.
2. Identify gaps and vulnerabilities in current endpoint security.
3. Develop a deployment plan based on assessment findings.

c) Deployment Phase

1. Deploy EDR agents on all the StockHolding endpoints desktops, laptops and Servers as per the best practices performed by OEM.
2. Configure EDR policies and rules tailored to StockHolding's needs and security requirements.
3. Conduct testing to ensure proper functionality and integration with existing security infrastructure.
4. Provide user training and awareness sessions on EDR capabilities and usage guidelines.

The successful bidder shall ensure that;

a. The solution must be able to detect/block/quarantine/clean the files/IT-threats for the hashes and IOC/IOA released by RBI/Cert-in/any other regulatory bodies in India through its agent on endpoint and / or OEM has to provide the dedicated scan engine for detection/clean of these hashes and IOC/IOA released by advisories.
b. The solution must be compliant to detect/block/quarantine/clean all the alerts and advisories released by SEBI/Cert-in/any other regulatory authority in India.
c. The Bidder shall be responsible of all technical activities like Vulnerability assessment, Configuration audit, patching, upgrade and updates, troubleshooting, included but not limited to licensing and configuration of all the third-party components provide along with the solution without any extra cost to StockHolding.
d. All the systems/components in the proposed solution should be integrated with the StockHolding's current security and IT operation systems like SOC, PIMs, DLP, AD, ITAM, NAC, NTP, etc. and all such security and operations management systems which has been and will be deployed in the StockHolding from time to time.
e. Web Proxy Integration: Integration with web proxy where web access policies can be implemented which blocks active C&C communication attempts identified by the solution.
f. Integration with StockHolding's Email Solution, create / add identified threats file integrity hash value. The Solution can work in conjunction with email, but it should not be dependent on it.
g. Support the end-users and departments in the pre and post deployment during contract period.

d) Operation Phase

1. Continuous monitoring of endpoints for suspicious activities and threats.
2. Real-time detection of malware, unauthorized access attempts, and other security incidents.
3. Incident response planning and execution based on EDR alerts and findings.

e) Response and Remediation

1. Define incident response procedures and escalation paths.
2. Coordinate with StockHolding IT and security teams to investigate and respond to EDR alerts.
3. Contain and mitigate threats identified through EDR capabilities.

f) Device Control Capabilities

1. Policy Definition
    i. OEM and Bidder should define policies specifying which types of devices (e.g., USB drives, smartphones, laptops) are allowed or blocked.
    ii. Specify conditions under which devices are allowed (e.g., only encrypted devices, specific vendor IDs).
2. Enforcement Mechanism
    i. Implement mechanisms to enforce these policies at the endpoint level.
    ii. Control access based on device attributes (e.g., type, manufacturer, serial number).
3. Monitoring and Reporting
    i. Monitor device connections and activities to detect unauthorized devices or policy violations.
    ii. Generate reports on device compliance status and incidents.

g) Posture Check

1. Endpoint Assessment
    i. Assess endpoint security configuration (e.g., antivirus status, firewall settings, OS and Build number).
    ii. Evaluate compliance with corporate security policies and standards.
2. Remediation
    i. Automatically remediate non-compliant endpoints (if supported) or provide guidance to users on how to bring their systems into compliance.

h) Data Loss Prevention

1. Data Protection across Environments: Bidder in consultation with OEM and StockHolding stakeholders deploy the DLP solutions aiming to protect data across various environments including on-premises networks and outgoing channels.
2. In coordination with Networking department identify and engage stakeholders such as IT, security teams, compliance officers, and end-users to understand their needs and expectations.
3. Gather detailed requirements related to data protection, compliance needs (e.g., GDPR, Cert-in, SEBI guidelines and regulations etc. and organizational policies and based on that policies to be created for DLP monitoring and reporting.
4. Ensure that the DLP solution complies with relevant regulations and standards.
5. DLP should be configured to provide real-time visibility into data movement across sources, egress channels and destinations.
6. Custom data classification for accurate contextual visibility into data egress events.
7. Data movement of sensitive personally identifiable information (PII) and reduce noise with nuanced classifications based on a combination of content patterns, sensitivity labels, web sources and file types.
8. Establish procedures for responding to DLP incidents, including data breaches or policy violations.

9. Generate and review reports on DLP incidents, policy violations, and overall effectiveness to support audits and compliance efforts. Reports should be provided as per the technical specifications provided for Reporting.
10. Regularly review and update DLP Policies and configurations to adapt new threats, regulatory changes or organizational changes and evaluate the performance and effectiveness of the DLP solution.
11. Make necessary adjustments to policies, configurations, and deployment strategies to enhance data protection and minimize impact on endpoint performance.

i) Updates and Upgrades:

1. For StockHolding's tenant, we should get both manual and auto-update functionalities for new version updates and upgrades ensures flexibility and reliability in managing software updates.
2. **Manual and Automatic Updates Approach**
   Offering both manual and auto update options allows StockHolding's IT team to choose the approach that best suits StockHolding operational requirements and policies.
3. **Risk Management:** Manual updates can be used for critical updates that require careful oversight, while auto updates can handle routine patches and maintenance tasks.
4. **Patch Management**
   i. Implement regular updates and patches for EDR software and agent components.
   ii. Ensure compatibility with operating systems and other endpoint software.
5. **Implementation Considerations:**
   User Notifications: Regardless of the update method chosen, clear communication and notifications to end users about upcoming updates are essential to manage expectations and minimize disruptions.
6. **Rollback Mechanism:** It's recommended to have a rollback mechanism in place in case an update causes unexpected issues, allowing quick restoration to the previous stable (n-1) version.

By incorporating both manual and auto update functionalities into StockHolding's tenant system, OEM can optimize software management, enhance security, and ensure that the software meets operational needs effectively.

j) Reporting and Analysis

1. **Performance Matrix**
   i. After deployment of solution in StockHolding network environment, Bidder needs to analyse Key performance indicators (KPIs) for EDR effectiveness (e.g., mean time to detect, mean time to respond) and required to provide their assessment report on half yearly basis till completion of the contract period.
   ii. Regularly generate and review reports on EDR activities, incidents, and outcomes.
   iii. Conduct periodic security assessments on half yearly basis and audits to evaluate EDR efficacy and identify areas for improvement in consultation with OEM.
   iv. Continuous Monitoring: Should be configured for all the endpoints assets of StockHolding's includes desktops, servers, cloud environments, laptops and other critical assets for any signs of malicious activity or security breaches.
   v. Threat Detection: Utilizing this platform along with advanced threat detection technologies it should identify and alerts on suspicious behaviour, indicators of compromise (IOCs), and potential security incidents in real-time.

vi. Proactive Threat Hunting: This involves actively searching for hidden threats and anomalies within the StockHolding's environment that may evade automated detection systems.
vii. Incident Response Support: In the event of a confirmed security incident threat hunting should provide rapid incident response support. This includes containment, investigation, root cause analysis, and remediation guidance to minimize the impact of the incident.
viii. Threat Intelligence Integration: Threat intelligence should be integrate from its global intelligence network and external sources. This helps enhance detection capabilities and provide context for identified threats.
ix. Security Analytics and Reporting: Threat hunting should generate comprehensive reports and analytics on security events, incidents, and trends. These reports helps StockHolding understand our security posture, identify recurring issues, and make informed decisions.
x. Customized Alerts and Notifications: Threat hunting delivers customized alerts and notifications based on predefined rules and thresholds, ensuring timely awareness of security incidents and potential threats.
xi. Compliance and Regulatory Support: Module should help StockHolding in meeting compliance requirements by providing relevant security monitoring, reporting, and documentation as needed.
xii. Continuous Improvement: OEM should works closely with clients to continuously improve security posture through proactive recommendations, threat insights, and ongoing optimization of security policies and configurations.

2. **Patch Management**
   i. Implement regular updates and patches for EDR software and agent components.
   ii. Ensure compatibility with operating systems and other endpoint software.

k) Documentation and Knowledge Transfer

1. Maintain detailed records of EDR configurations, policies, incidents, and resolutions.
2. Document lessons learned and best practices for future reference.
3. Provide knowledge transfer sessions to StockHolding.
4. Create and maintain comprehensive documentation including deployment guides, configuration details, policy definitions and troubleshooting procedures.

l) Compliance and Governance

1. Regulatory Compliance
   i. Ensure EDR deployment aligns with regulatory requirements and industry standards (e.g. ISO 27001:2013).
   ii. Periodically review and update policies to address changing compliance landscapes.

m) Continuous Improvement

1. Feedback and Improvement
   i. Solicit feedback from stakeholders and end-users to improve EDR effectiveness and user experience.
   ii. Implement process improvements based on feedback and lessons learned from incidents.

n) Training and Awareness

1. OEM along with bidder will provide ongoing training from and awareness programs to educate StockHolding's SOC operation team members and users on EDR functionalities and our role in maintaining endpoint security.

o) Emergency Response Planning

1. Bidder in consultation with StockHolding's Network team need to develop contingency plans for critical incidents affecting EDR operations and endpoint security.

Technical Specification

OEM and bidder ensure that EDR solution and related modules supports listed Technical specifications and they will make sure that they will configure the solution in such a way that StockHolding will check all the listed technical features and used in StockHolding Network architecture. Any non-compliance to below mentioned Technical specifications may lead to rejection of bid.

Sl. No	End point Detection and Response	Compliance (Yes/No)
	End Point Agent	
1	"Unified End Point agent for desktops, laptops, servers etc. must provide below features/functionalities in the form of dedicated module for each of them and not via any custom behaviour rules: ▪ Next-Gen Anti-Virus ▪ End Point Detection and Response (EDR) ▪ Device control (USB, BLUETOOTH) ▪ Rogue Device Discovery, Detection and Reporting ▪ Endpoint/Host Firewall ▪ Vulnerability Detection on End Points Apps, OS and Asset Inventory ▪ FIM (File Integrity Monitoring) ▪ Remote Response from EDR Console ▪ SOAR (Automated Response Capabilities) Note – Above Modules must be accessible through single Unified Console itself and not via any multiple consoles."	
2	It must be a standalone package containing all the required components /plug-ins / add-ons for the above stated features from the same OEM. There must not be any dependency on any other 3rd party and/or existing StockHolding's solutions (ex: Active Directory, NAC, Asset management, etc.) The agent must be same for all types of systems. All features listed above must be part of single agent and from same OEM.	

3	The endpoint agent must be able to communicate to the single unified cloud (OEM) console for all crucial functionalities/purposes: ▪ Send Live Telemetry data ▪ Send Endpoint Security alerts / threats data in real time ▪ Obtain the latest endpoint security policy configurations ▪ Evaluating files/processes against OEM threat Intel and as well as customized / StockHolding's specified Behaviour-Attributes/ IOCs (domains, hashes, IP Addresses, etc.) ▪ Submission of quarantined files to the console for further evaluation ▪ Agent updates/upgrades ▪ Remote access (terminal/bash/CLI) from console, or Remote Command Execution from console (Terminal, PowerShell, Bash, CLI, etc.)	
4	The EDR Solution must have manual and auto updates/ upgrade feature and function allowing Stockholding to decide patching cycle i.e N-2, N-1, staggered rollout of security updates, patches to end points.	
5	The endpoint agent must collect continuous and near real time events from managed endpoints, including, but not limited to, information of process execution, URL's Accessed, user login, administrator access, file activity, Suspicious in-memory executions, DNS resolutions, Network operations, Disk operations, Registry changes etc.	
6	The collected telemetry from all endpoints must be stored in StockHolding premise for a minimum period of 180 day. It must also be possible to obtain this telemetry data from cloud instance as and when required by StockHolding's (for up to last 180 days) in a human readable format without any additional cost to StockHolding's.	
7	The endpoint agent must have low resource utilization (Disk, RAM, CPU) at the endpoint level for all endpoints, except while executing scheduled scans and/or during attack/breach containment and remediation, and support all major Windows OS: Win 10, 11 and upcoming OS for desktops/laptop and 2016, 2019, 2022 etc. for servers and major flavours of Linux OS (RHEL, Ubuntu, CentOS etc.), Oracle enterprise Linux version 8.0 and above. Endpoint agent must support virtual infrastructures and virtualized data centres.	
8	Solution must support all Internet browsers (Microsoft edge, Google Chrome. Mozilla Firefox etc.) and Java platforms.	
9	Solution should not be dependent on operating system updates or specific versions to deliver functionality. Endpoint agent must operate in both user and kernel space on Windows at least and operate in at least user mode on other OS, to provide full visibility and to eliminate blind spots for all OS.	
10	The endpoint agent should offer tamper protection to ensure that its files, processes, and data on endpoint may not be altered/terminated/erased in any way, even by StockHolding's Administrators. Administrators and/or End-Users must also not be able to uninstall/remove/disable endpoint agent and/or its plugins/components (if any) without authorization token/code/key.	

11	Deployment of endpoint agent must be possible through mechanisms such as Microsoft Active Directory Group Policy Update (GPO), 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.	
12	The agent must also have forensics capability within itself, with no additional utility or application (either OEM, 3rd party or StockHolding's provided) being required to perform forensics on any managed endpoint.	
Next-Gen Anti-Virus and EDR		
13	The endpoint agent must have the capability/functionalities of Next-Gen Antivirus and End Point Detection and Response (EDR) in a unified component/module without depending upon any other 3rd party/Stockholding solution or infrastructure. Must be compatible and fully functional on Windows, Linux and MAC OS (same platforms as defined in Point above for end point agent).	
14	The endpoint agent must offer comprehensive protection, without depending upon traditional signature based techniques, against known malware and 0-day / unknown malware, with AI/ML techniques-based protection on the agent itself (offline protection or static AI/ML and Behavioural based protection), along with Sandboxing (directly integrated with / available from endpoint agent) and cloud-based Threat intel from OEM (online protection) and as well as StockHolding's specified custom Behaviour- attributes / IOCs (Indicator of Compromise) as and when received from any GoI body/source.	
15	This protection (both offline and online) includes techniques such as file-based malware, file less / script-based malware, Behavioural based detection, DLL Side loading, in memory attacks, common exploits like Return-oriented programming (ROP) attacks, Heap Spray Attacks, Structured Exception Handling Overflow Protection (SEHOP) corruption, Null page exploits, MS Office macros, Java exploits, shell code detection, Process injection detection, privilege escalation. The solution must also have Exploit Prevention for Windows, Linux and MAC	
16	The endpoint agent policy configuration must offer modules like Next Gen Antivirus/Anti Malware AI/ML based detection and prevention, File (full content and/or meta data/attribute) analysis, Process blocking, Adware and Spyware protection, Behavioural detection and prevention, Script based / File less malware protection, Anti-Ransom ware, 0-day post-exploitation detection, Sandboxing, Dynamic Threat Intel, Protection from exploits and Lateral Movement detection and prevention on the endpoints	

17	Policy/configuration/settings on the OEM Cloud console must support the granular level feature management, i.e., it should be possible to enable/disable detection, reporting and blocking (independently) for each of these modules as and when required.	
18	Threats reported from the endpoints will be presented in cloud console in near real time (through information sent by endpoint agent) in the form of full attack chain visualization (tree/graph) and provide all the required information gathered from telemetry: Initiating process (parent), child process(es), command line, network operations, DNS queries, disk operations, registry changes, vulnerabilities, sandboxing report of quarantined files in the console itself. Full MITRE ATT&CK framework and adversary and/or malware attribution must be incorporated into threat detection and analysis.	
19	Action(s) to be taken for remediation of these threats must also be taken care of from the console itself. The minimum set of actions include delete quarantined files, clean impacted files, isolate/contain an endpoint from network, remote terminal / CLI access to execute commands: ex download artefacts, modify registry, process termination and service termination. Automated Sandboxing and File Integrity monitoring (for StockHolding's specified critical files) must be supported in the solution. It should be possible to revert abnormal/unauthorized changes (disk, registry) by malware/malicious process(es) on one or more affected endpoints from the console itself based on the recorded change information as per threat data captured by the solution. Remote should not be over RDP (For windows) as that may hamper end user's productivity.	
20	FIM (File Integrity Monitoring) must closely monitor for any changes (creation, deletion and modification) in real time within System Files, Folders, Registries for all designated and managed systems within StockHolding's. It must provide at the bare minimum: ▪ Notification for any similar changes in files/folders across multiple hosts. ▪ Dashboard to showcase hosts with most violations, Top Changes made, change trends with change severity ratings. ▪ Change Log ▪ Attribute any Adversary with the relevant File changes for better context.	
21	It must be possible to block custom Indicators of Compromise (IOCs) : IP addresses and hashes at the managed endpoint itself through EDR console.	
22	Remediation for incidents on affected endpoints for any type of detected threat(s) as above should not be dependent upon backups, shadow copies and/or on any other 3rd party / StockHolding's solution. No reserve storage space on endpoint machine must be required by or allocated to the endpoint agent for remediation on any OS version. Solution must have surgical remediation for incidents instead of relying upon backups as the first resort.	

23	There must be a provision to configure and execute (real time and scheduled) scans on managed endpoints based on configured threat prevention policies / configuration / settings (at least on Windows) and without adversely impacting endpoint resources (CPU, RAM, Disk) in order to detect dormant threats present in these endpoints.	
24	Solution must have inbuilt dedicated SOAR module for endpoints to automate day to day tasks like notifications and response actions on suspicious endpoints without any additional cost. These notifications and response actions must be based upon pre-defined playbooks as well as capability to create custom workflow or playbook as well.	
25	Solution must have dedicated Threat Intelligence module within same console and platform capable of providing full details around adversaries group worldwide.	
Device Control		
26	The endpoint agent must be able to detect, identify and block the system (endpoint: desktop/server) from accessing physical devices such as removable storage devices, Wired, and Wireless Network Adapters (over USB channel), imaging devices, printers and others. This feature must be enabled in the endpoint agent itself without dependency on any other 3rd party / StockHolding's solution (ex: Active Directory Group Policy). All access events/logs must be sent to the cloud solution by endpoint agent for viewing and reporting. Must be compatible at least on Windows, MAC, Linux OS.	
27	The solution must provision whitelisting of authorized removable devices from corresponding policies/ configuration/ settings from the same console as that for the proposed solution for this project. Whitelisting should consist of options such as read only and both read and write access. Whitelisting may be carried out based on properties like device type (removable storage, camera, printer, etc.), device properties like Serial Number, Vendor and Product Name at the bare minimum.	
28	The agent must be able to monitor outgoing data transfers to USB devices to scan malware and classify the same accordingly (based on file type) and report the same on console along with endpoint details, process user details, removable device details and data transfer summary and date-time. There should be a provision to enable/disable this monitoring/reporting mode as well via policies.	
29	There should be a provision for displaying customizable OR inbuilt alerts/messages to endpoint (users) in case of unauthorized and/or authorized removable devices are connected to the endpoint.	
Endpoint Firewall		
30	The endpoint agent must have inbuilt component for Client/Host/endpoint firewall as a part of the same solution and must not be dependent on any other 3rd party / existing StockHolding's solution and/or infrastructure.	

31	The endpoint firewall must be able to allow, drop and log/monitor bi-directional traffic at the endpoint level for all protocols (at least for TCP, UDP and ICMP) based on customizable polices/settings/configurations on the same console as the proposed solution. The policies may be configured to allow, block, and/or monitor traffic in specified direction (originating from endpoint or targeted at endpoint), based on target/initiator IP Addresses (and subnets as well) and port(s) and protocol(s) at the bare minimum.	
32	Firewall Policy should work based on the internal/external network configuration, should be Location aware.	
33	The configured firewall policies for desktops and servers should not abnormally interfere with normal functioning of these endpoints in any way to ensure there is no outage in the StockHolding's network and/or required services are not impacted.	
Data Loss Prevention		
34	The solution should have unified agent i.e same agent of EDR to perform data protection	
35	Data protection deployed without requiring additional software push or reboot	
36	Solution should show the data flow chart from source to destination including the egress channel	
37	Solution should provide predefined content patterns, option to create custom content pattern using regex	
38	solution should be able to provide visual data flow based on web origins, Classifications, content patterns, Sensitivity Labels (Microsoft)	
39	Solution have ability to create detection based on the data restriction policy, and define severity for the detection.	
40	Solution should be able to give the details of the events triggered by data protection	
41	Solution should be able to monitor the control the data egress from managed or custom application based on the defined rules	
42	Solution should have ability to create simulation for the defined rules (allows/block) before its actually applied	
43	Ability to create workflow for automation based on the triggered detections for alerting and response action like isolation the device, etc.	
Endpoint Data Monitoring and Protection		
44	The solution should have pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also, solution should have the capability to define the third-party application. The solution should be able to define the policies for the inside and out of office endpoint machines. The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files. The endpoint solution should be able to perform discovery only when the endpoint is connected to external power or Machine is Idle.	

45	The solution should Provide "Cloud Storage Applications" group which monitor sensitive content accessed by this cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud. For Example (Should support from day 1(Supported Windows OS - Win 10, Win 11, Win 2016, Win 2019 win 2022 supported)	
46	Endpoint solution should support win 32 and 64 bit OS, Support wide variety of platforms (Below support from Day1):Win 10, Win 11, Win 2016, Win 2019 win 2022 supported, VDI (VMWare)	
Data Identification & Policy Management		
47	The solution should have a comprehensive list of predefined policies and templates and patterns to identify and classify information pertaining to different industry like Finance, Banking, PII, PCS and India IT Act.	
48	The solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file.	
49	The solution should be able to recursively inspect the content of compressed archives.	
50	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.	
51	The solution should enforce policies to detect low and slow data leaks.	
Vulnerability Assessment		
52	Solution identifies vulnerabilities tied to assets in the environment without deploying any additional agents.	
53	Solution should provide real-time vulnerability status for all windows endpoints without requiring scan.	
54	Solution provides information such as Severity, Vulnerable products, Vector, Number of Vulnerable Hosts, and Patch Recommendations for each vulnerability identified.	
55	Solution automatically "closes out" vulnerabilities without requiring user intervention as patches are installed.	
56	Solution identifies unpatched vulnerabilities that are known to be targeted by named adversaries.	
57	Delivers vulnerability management, not just vulnerability reporting.	
58	Solution prioritizes unpatched vulnerabilities that exist on systems generating detections	
59	Solution should provide the visibility if the reboot is required for the system after the patch installed.	
24*7*365 Threat Hunting		
60	24x7x365 human lead proactive threat hunting	
61	Proactively detect attack that goes undetected (beyond platform detections)	

62	Experienced hunters that uncover e-crime & nation states threat actors on daily basis	
63	Threat Hunting should be offered as an integrated service by the Platform vendor	
64	Proactive threat hunters equipped with threat intelligence (daily basis) and proactive threat hunting tools.	
65	Generating detection with details of the threat actor activities observed in the environment	
66	Email alert the stake- holders about the adverbial activity detected in the environment.	
API Integration And Reporting		
67	The solution must support integration with SIEM products and bidder should integrate the proposed solution with Qradar SIEM at AWS and or any other SIEM solution services procured by StockHolding from its Service provider.	
68	The solution must have real time streaming of alerts via API and bidder should configure the same in StockHolding environment.	
69	The solution must be capable to Query device status via API including OS, version, first seen, last seen and bidder should configure the same.	
70	The solution must support standardized and customizable reports in pdf, csv and json formats.	
Rogue or Unmanaged Device Detection		
71	The endpoint agent must be able to actively or passively scan StockHolding's network (within broadcast domain and/or across multiple subnets) to identify devices that are not having the OEM agent installed in them, to identify managed devices (having endpoint agent installed), and unsupported devices (which does not support endpoint agent). This feature must be inbuilt into the existing EDR agent and must not be dependent on any other 3rd party / existing StockHolding's solution and/or infrastructure, ex: separate VM, Active Directory, Asset Inventory, NAC, or any other.	
72	The details of such identified devices must be sent to the cloud solution by endpoint agent for viewing and reporting. The solution must be able to then classify these devices based on retrieved scan information and the derive the classified type, such as Computer: Desktop, Server, Printer, Network Infra like Switches, Firewall, etc.), along with details of the identified device such as Name, IP Address, MAC, OS details, detection time and date (whatever is possible)	
Reporting and Analytics		
73	The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view.	
74	The system should allow automatic schedule of reports to identified recipients.	
75	The reports should be exported to at least CSV and json formats.	

76	The system should provide options to save specific reports as favourites for reuse.	
77	The DLP Solution creates DLP Detections for abnormal behaviours.	
78	The DLP dashboard must display the number of cases in the designated period that fall above the risk score threshold that you have selected. Risk score thresholds must be customizable and instantly produce a report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.	
Maintenance & Support		
79	Must have 24x7 local and phone support. Response time within four hours for non-critical and one hour for critical cases. Support may include additional features like security reviews and access to named technical account manager.	
80	Customer portal - able to easily submit suspicious file samples, report technical issues and track progress on submitted requests.	
81	Site specific customized documentation should be included with the product.	
82	Dedicated named TAM should be included as a part of the Support.	
83	Solution must include deployment and on-boarding support.	
84	Pre & Post installation must be supported by OEM and SI. OEM has to review and certify.	
85	Must provide training options for administration, incident response and threat hunting.	

Bidder Responsibility

The System Integrator (SI) and OEM need to take the responsibility of the following activities throughout the contract period.

Sr. No.	Activities	Responsibility		Remarks
		System Integrator (SI)	OEM	
1	Supply of License	YES	YES	
2	EDR Agent Deployment in StockHolding's locations	YES	YES	OEM will deploy 5% of endpoints devices, rest SI will deploy.
3	Provisioning of Technical Account Manager (TAM)	-	YES	OEM will provide shared TAM for entire engagement period
4	Support for entire Contract period	YES	YES	Back lining with OEM
5	Software upgrade/update	-	YES	

Service Level Agreement (SLA) and Penalty

The bidder needs to execute a Service Level Agreement with the StockHolding covering all terms and conditions of this tender. Bidder need to strictly adhere to Service Level Agreements (SLA). Services delivered by bidder should comply with the SLA mentioned in the table below.

Essential Support: 24 x 7 x 365 days with named Technical Account Manager (TAM)

a) It should offer proactive engagement to help us maximize the benefits of platform.
b) Response time aligns within four hours for non-critical and one hour for critical cases.
c) Essential support may include knowledge base articles, online communities, troubleshooting assistance and additional features like security reviews and access to named technical account managers.
d) SLA (Service Level Agreement) for EDR (Endpoint Detection and Response) typically defines the expected response and resolution times based on the severity of the incidents.

Here's a general outline for SLA tiers based on severity levels:

High Severity:

a) Response Time: Immediate to very short, typically within 1 hour.
b) Resolution Time: Urgent action required, Aim for resolution within 4 hours.
c) Examples: Critical security incidents such as active ransomware, widespread data breach, or critical system compromise.

Medium Severity:

a) Response Time: Prompt response required, typically within 4 hours.
b) Resolution Time: Action required within 24 hours.
c) Examples: Suspicious activities on critical systems, potential malware infections affecting multiple endpoints.

Low Severity:

a) Response Time: Response within 8 hours.
b) Resolution Time: Action required within 48 hours.
c) Examples: Minor alerts, low-risk anomalies that do not immediately impact critical operations.

These SLA tiers help prioritize and manage incident response based on the criticality and potential impact of each security event detected by the Endpoint Detection and Response system. It's important for organizations to customize these SLAs based on their specific operational needs and risk tolerance levels.

Preventive Maintenance / Review of Tenant on OEMs cloud

Event	Criticality	Penalty Calculation
Unavailability of conducting preventive maintenance / Security Review of OEM's tenant on half yearly basis.	High	For each instance of breach, penalty will be 1% of the total License and implementation Cost.

Penalty Clause

In case of delay in completion of any milestone within stipulated time by the successful bidder, StockHolding will impose a penalty as per below:

Schedule	Timelines	Penalty
Software Delivery as well as One-time EDR Implementation (Covering Implementation, Migration, Testing, Go-Live, Documentation & Training)	Within 4 weeks from the date of PO	1% of the total License and implementation Cost /week subject to maximum of 10% of the total License & implementation Cost.
SLA for uptime of the solution	>=99.99% on Monthly basis.	NIL
	99% to 99.95%	0.5% of the total License and implementation Cost. Subsequently a penalty of 0.5% will

		increase for every hour delay beyond 99.95% to 99%
	Below 99.95%	1% of the total License and implementation Cost. Subsequently a penalty of 1% will increase for every hour delay beyond 99.95%

Note:

a) The uptime will be calculated as per the formula given below:

Uptime: {(Actual Uptime + Excusable Down Time) / Schedule Hrs} x 100

- Actual Uptime means, of the scheduled hours, the aggregate number of hours in any month during which each defined and supported equipment is actually available for use.
- Excusable downtime means the aggregate number of hours in any month during which each defined and supported service is down during scheduled hours due to preventive maintenance, scheduled outages, LAN cabling faults, infrastructure problems or any other situation which is not attributable to vendor's failure to exercise due care in performing its responsibilities.
- Scheduled hours means the days of the week and the hours per day for which the vendor has committed to an availability service level for a system or network and during which periods such Availability Service Level will apply.

b) Total hours in a month will be taken as: 24hrs*no. of days in respective month. Any downtime scheduled at StockHolding will not be considered for above calculation.

c) The penalty will be affected at the time of release of any payment, subject to maximum of 10% of Total Support Cost.

d) If the uptime falls below 98.0% twice during any quarter, contract / Order may be cancelled, and StockHolding may claim entire advance amount with interest from the bidder.

Contract Duration

Successful bidder shall enter into contract for the period of 03 (three) years with 02 (two) years of extension.

Terms and Conditions

A. Payment:

Milestone	Payment term
License Cost (2900 End Points)	Annual Payment - 100% Payment against Delivery on submission of Original Invoice and confirmation of License Certificate duly authorized by StockHolding Official
Training Cost	100% Payment post successful training
Implementation of End points (One time)	100% Payment post successful installation
OEM Support Cost (for 3 years)	Annual advance Payment against submission of Original Invoice
Vendor Support Cost (for 3 year)	Half-yearly Payment based on the SLA calculation against submission of Original Invoice

Note:

a. All payment will be released on submission of invoice and necessary report.

b. For any SLA breach, applicable Penalty/Penalties may be recovered from payment

c. Payments will be released only after submission and verification of the required Bank Guarantee (BG). No payment will be made to successful bidder, until the BG verification is done.

B. Taxes & levies:

a. Applicable GST payable at actual as per prevailing rate of taxes as per Government notification
b. In case of tax exemption or lower TDS; Bidder has to submit letter from Government Authority for tax exemption or lower TDS (to be submitted along with each of the invoice(s) (c) Applicable TDS will be deducted from payment(s).

C. Bidder to abide by labour laws, human rights and regulations in India = of business. Bidder to adhere to laws addressing child, forced or trafficked labour.

Refund of Earnest Money Deposit (EMD):

a. EMD will be refunded through NEFT to the successful bidder on providing (a) an acceptance confirmation against the PO issued by *StockHolding* and (b) submission of Performance Bank Guarantee wherever applicable and should be valid for 30 days beyond the contract period.
b. In case of unsuccessful bidders, the EMD will be refunded to them through NEFT within 15 days after selection of successful bidder subject to internal approval of *StockHolding*.

Performance Bank Guarantee (PBG):

Successful Bidder shall, at own expense, deposit with the *StockHolding*, within fifteen (15) days on issuance of PO, a Bank Guarantee (BG) for the value of 5% of the Contract Value from scheduled commercial banks as per Annexure - 8. This Bank Guarantee shall be valid up to 60 days beyond the completion of the contract period. No payment will be due to the successful bidder based on performance, until the BG verification is pending.

Bank Guarantee may be discharged / returned by *StockHolding* upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the Bank Guarantee.

StockHolding reserves the right to invoke the BG in the event of non-performance by the successful bidder.

Force Majeure

The Bidder will not be held responsible for breach of executing any obligation or delay in executing any obligations during below given circumstances / conditions:

a. War, Riots, Strike, Fire, Flood, Earthquake, Storm, Pandemic breakout, Power failure, Theft etc.
b. Any Governmental priorities (Necessary proof for validation viz. Govt. Gazette notifications, Leading Newspaper reports, etc. should be made available) (c) Sabotage or omission of StockHolding

Dispute Resolution

In the event of any dispute arising out of or in connection with this Order, the parties shall use their best endeavour to resolve the same amicably AND if the dispute could not be settled amicably, the matter shall be settled in the court under Mumbai jurisdiction only. The final payment will be released only after the Bidder complies with above-mentioned clause

Right to alter RFP

a. StockHolding reserves the right to alter the RFP terms and conditions at any time before submission of the bids.
b. StockHolding reserves the right to modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever. We further understand and accept that StockHolding's decision in this regard will be final and binding on all bidders.

Integrity Pact

The Bidder will have to enter in to an Integrity Pact with StockHolding. The format (text) for the Integrity Pact is provided as Annexure-5. The successful Bidder will have to submit a signed and stamped copy of the Integrity Pact by the authorized signatory of the successful Bidder.

Non-Disclosure Agreement (NDA)

The successful Bidder will sign a Non-Disclosure Agreement (NDA) with StockHolding for the contract period. The draft text of the NDA will have to be approved by legal department of StockHolding.

Indemnity

The Bidder should hereby indemnify, protect and save StockHolding against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the equipment offered by the Bidder. Any publicity by Bidder in which name of StockHolding is used should be done only with the explicit permission of StockHolding.

Limitation of Liability

Neither party shall, in any event, regardless of the form of claim, be liable for any indirect, special, punitive, exemplary, speculative or consequential damages, including, but not limited to any loss of data, business loss due to unavailability of services, and loss of income or profits, irrespective of whether it had an advance notice of the possibility of any such damages. Subject to the above and notwithstanding anything to the contrary elsewhere contained herein, the maximum liability, of selected bidder (vendor) shall be, regardless of the form of claim, restricted to Rs. 1,00,00,000 (Rupees One Crore) or extent of the business loss/damage to Stockholding - whichever is lower.

Subcontracting

As per scope of this RFP, sub-contracting is not permitted. The bidder shall not assign or sub-contract the assignment or any part thereof to any other person/firm.

Termination Clause

StockHolding reserves right to terminate the contract by giving 30 days prior written notice in advance –

a) If Half-yearly Preventive Maintenance / Review of Tenant not done by the successful bidder in a year;
b) If the uptime falls below 99% twice during any quarter.
c) If at any point of time, the services of bidders are found to be non-satisfactory;
d) If at any point of time, StockHolding finds out deviation to sub-contracting clause;

ANNEXURE - 1 - Details of Bidder's Profile
(To be submitted along with technical bid on Company letter head)

Details filled in this form must be accompanied by sufficient documentary evidence, in order to verify the correctness of the information.

Sl. No	Parameters	Response	
1	Name of the Firm/Company		
2	Year of Incorporation in India		
3	Names of the Partners/Directors		
4	Company PAN no		
5	Company GSTN no. (please attach annexures for all states)		
6	Addresses of Firm/Company		
	a) Head Office		
	b) Local Office in Mumbai(if any)		
7	Authorized Contact person		
	a) Name and Designation		
	b) Telephone number		
	c) E-mail ID		
8	**Financial parameters**		
	Business Results (last five years)	Annual Turnover	Networth
		(Rs. in Crores)	(Rs. in Crores)
	2019-20		
	2020-21		
	2021-22		
	2022-23		
	2023-24		
	(Only Company figures need to be mentioned not to include group/subsidiary Company figures)	(Mention the above Amount in INR only)	

N.B. Enclose copies of Audited Balance Sheet along with enclosures
Dated this..... Day of 2024

(Signature)

(In the capacity of)

ANNEXURE - 2 – Eligibility Criteria
To be submitted as part of Technical Bid

SI.	Criteria	Documents to be submitted by Bidder
1	The Bidder should be a registered Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 with experience of implementing Endpoint Detection and Response (EDR) solution for at least 05 (five) years.	▪ Copy of Certificate of Incorporation issued by the Registrar of Companies ▪ Copy of PAN and GST ▪ Self-declaration by the bidder on company Letter Head duly signed by the Authorized Signatory
2	Should have an average annual turnover of at least Rs. 50 Lakhs per annum for last 05 (five) financial years (2019-20, 2020-21, 2021-22, 2022-23 and 2023-24). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last 05 (five) financial years.
3	Bidder should have positive Net worth in the last 05 (five) audited financial years	Certificate from CA mentioning Net worth for the past 05 (five) financial years.
4	The Bidder should have experience of EDR with DLP implementation through Cloud based and deployment of minimum 3000 agents at customer premises in any Financial Institution / PSU / Government Organization / Large Corporates in India not older than 03 (three) years from RFP date.	Copy of Purchase Orders / Completion Certificate
5	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 2 (two) years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
6	The bidder must have following valid Certifications: • ISO 27001:2013 certified	Relevant ISO Certificate
7	The proposed EDR Solution must be listed as leaders in Gartner's latest Magic quadrant for End Point Protection/leaders or strong performers in Forrester Wave's latest report for EDR Solutions or Top 3 Leader's as per the IDC's latest Endpoint security market share report.	Copy of latest Gartner's/ Forrester's Report clearly highlighting the proposed EDR solution.
8	For Endpoint DLP, The proposed DLP must be listed as leaders in Gartner's latest Magic quadrant or strong performers in Forrester Wave's latest report. Note: Above criteria is not applicable for integrated endpoint DLP with proposed EDR.	Copy of latest Gartner's/ Forrester's Report clearly highlighting the proposed Endpoint DLP
9	Bidder to submit MAF (Manufacturer Authorization Certificate) from OEM with tender reference number	MAF from OEM to be submitted.
10	Bidder must have support office/center at Tier 1 cities in India.	GST and address to be provided along with Contact Details
11	Bidder to provide undertaking that no penalties, amounting to up to 10% of the contract value per year,	Self-declaration from bidder on their letter head duly signed by authorized signatory

	have been imposed in the last three years by any of its client(s).	
12	OEM proposed solution should be in-line with SEBI regulatory Framework.	Confirmation on OEMs letterhead with reference to Circular numbers and points.

Note:

a. Letter of Authorization shall be issued by either Managing Director having related Power of Attorney issued in his favour or a Director of the Board for submission of Response to RFP
b. All self-certificates shall be duly signed and Stamped by Authorized signatory of the Bidder Firm unless specified otherwise.
c. Bidder response should be complete, Yes/No answer is not acceptable.
d. Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. StockHolding will not make any separate request for submission of such information.

Dated this..... Day of 2024
(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

ANNEXURE – 3 – Technical Bid

Sl. No	End point Detection and Response	Compliance (Yes/No)
	End Point Agent	
1	"Unified End Point agent for desktops, laptops, servers etc. must provide below features/functionalities in the form of dedicated module for each of them and not via any custom behaviour rules: ▪ Next-Gen Anti-Virus ▪ End Point Detection and Response (EDR) ▪ Device control (USB, BLUETOOTH) ▪ Rogue Device Discovery, Detection and Reporting ▪ Endpoint/Host Firewall ▪ Vulnerability Detection on End Points Apps, OS and Asset Inventory ▪ FIM (File Integrity Monitoring) ▪ Remote Response from EDR Console ▪ SOAR (Automated Response Capabilities) Note – Above Modules must be accessible through single Unified Console itself and not via any multiple consoles."	
2	It must be a standalone package containing all the required components /plug-ins / add-ons for the above stated features from the same OEM. There must not be any dependency on any other 3rd party and/or existing StockHolding's solutions (ex: Active Directory, NAC, Asset management, etc.) The agent must be same for all types of systems. All features listed above must be part of single agent and from same OEM.	
3	The endpoint agent must be able to communicate to the single unified cloud (OEM) console for all crucial functionalities/purposes: ▪ Send Live Telemetry data ▪ Send Endpoint Security alerts / threats data in real time ▪ Obtain the latest endpoint security policy configurations ▪ Evaluating files/processes against OEM threat Intel and as well as customized / StockHolding's specified Behaviour-Attributes/ IOCs (domains, hashes, IP Addresses, etc.) ▪ Submission of quarantined files to the console for further evaluation ▪ Agent updates/upgrades ▪ Remote access (terminal/bash/CLI) from console, or Remote Command Execution from console (Terminal, PowerShell, Bash, CLI, etc.)	
4	The EDR Solution must have manual and auto updates/ upgrade feature and function allowing Stockholding to decide patching cycle i.e N-2, N-1, staggered rollout of security updates, patches to end points.	
5	The endpoint agent must collect continuous and near real time events from managed endpoints, including, but not limited to, information of process execution, URL's Accessed, user login, administrator access, file activity, Suspicious in-memory executions, DNS resolutions, Network operations, Disk operations, Registry changes etc.	

6	The collected telemetry from all endpoints must be stored in StockHolding premise for a minimum period of 180 day. It must also be possible to obtain this telemetry data from cloud instance as and when required by StockHolding's (for up to last 180 days) in a human readable format without any additional cost to StockHolding's.	
7	The endpoint agent must have low resource utilization (Disk, RAM, CPU) at the endpoint level for all endpoints, except while executing scheduled scans and/or during attack/breach containment and remediation, and support all major Windows OS: Win 10, 11 and upcoming OS for desktops/laptop and 2016, 2019, 2022 etc. for servers and major flavours of Linux OS (RHEL, Ubuntu, CentOS etc.), Oracle enterprise Linux version 8.0 and above. Endpoint agent must support virtual infrastructures and virtualized data centres.	
8	Solution must support all Internet browsers (Microsoft edge, Google Chrome. Mozilla Firefox etc.) and Java platforms.	
9	Solution should not be dependent on operating system updates or specific versions to deliver functionality. Endpoint agent must operate in both user and kernel space on Windows at least and operate in at least user mode on other OS, to provide full visibility and to eliminate blind spots for all OS.	
10	The endpoint agent should offer tamper protection to ensure that its files, processes, and data on endpoint may not be altered/terminated/erased in any way, even by StockHolding's Administrators. Administrators and/or End-Users must also not be able to uninstall/remove/disable endpoint agent and/or its plugins/components (if any) without authorization token/code/key.	
11	Deployment of endpoint agent must be possible through mechanisms such as Microsoft Active Directory Group Policy Update (GPO), 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.	
12	The agent must also have forensics capability within itself, with no additional utility or application (either OEM, 3rd party or StockHolding's provided) being required to perform forensics on any managed endpoint.	
Next-Gen Anti-Virus and EDR		
13	The endpoint agent must have the capability/functionalities of Next-Gen Antivirus and End Point Detection and Response (EDR) in a unified component/module without depending upon any other 3rd party/Stockholding solution or infrastructure. Must be compatible and fully functional on Windows, Linux and MAC OS (same platforms as defined in Point above for end point agent).	

14	The endpoint agent must offer comprehensive protection, without depending upon traditional signature based techniques, against known malware and 0-day / unknown malware, with AI/ML techniques-based protection on the agent itself (offline protection or static AI/ML and Behavioural based protection), along with Sandboxing (directly integrated with / available from endpoint agent) and cloud-based Threat intel from OEM (online protection) and as well as StockHolding's specified custom Behaviour- attributes / IOCs (Indicator of Compromise) as and when received from any GoI body/source.	
15	This protection (both offline and online) includes techniques such as file-based malware, file less / script-based malware, Behavioural based detection, DLL Side loading, in memory attacks, common exploits like Return-oriented programming (ROP) attacks, Heap Spray Attacks, Structured Exception Handling Overflow Protection (SEHOP) corruption, Null page exploits, MS Office macros, Java exploits, shell code detection, Process injection detection, privilege escalation. The solution must also have Exploit Prevention for Windows, Linux and MAC	
16	The endpoint agent policy configuration must offer modules like Next Gen Antivirus/Anti Malware AI/ML based detection and prevention, File (full content and/or meta data/attribute) analysis, Process blocking, Adware and Spyware protection, Behavioural detection and prevention, Script based / File less malware protection, Anti-Ransom ware, 0-day post-exploitation detection, Sandboxing, Dynamic Threat Intel, Protection from exploits and Lateral Movement detection and prevention on the endpoints	
17	Policy/configuration/settings on the OEM Cloud console must support the granular level feature management, i.e., it should be possible to enable/disable detection, reporting and blocking (independently) for each of these modules as and when required.	
18	Threats reported from the endpoints will be presented in cloud console in near real time (through information sent by endpoint agent) in the form of full attack chain visualization (tree/graph) and provide all the required information gathered from telemetry: Initiating process (parent), child process(es), command line, network operations, DNS queries, disk operations, registry changes, vulnerabilities, sandboxing report of quarantined files in the console itself. Full MITRE ATT&CK framework and adversary and/or malware attribution must be incorporated into threat detection and analysis.	

19	Action(s) to be taken for remediation of these threats must also be taken care of from the console itself. The minimum set of actions include delete quarantined files, clean impacted files, isolate/contain an endpoint from network, remote terminal / CLI access to execute commands: ex download artefacts, modify registry, process termination and service termination. Automated Sandboxing and File Integrity monitoring (for StockHolding's specified critical files) must be supported in the solution. It should be possible to revert abnormal/unauthorized changes (disk, registry) by malware/malicious process(es) on one or more affected endpoints from the console itself based on the recorded change information as per threat data captured by the solution. Remote should not be over RDP (For windows) as that may hamper end user's productivity.	
20	FIM (File Integrity Monitoring) must closely monitor for any changes (creation, deletion and modification) in real time within System Files, Folders, Registries for all designated and managed systems within StockHolding's. It must provide at the bare minimum: ▪ Notification for any similar changes in files/folders across multiple hosts. ▪ Dashboard to showcase hosts with most violations, Top Changes made, change trends with change severity ratings. ▪ Change Log ▪ Attribute any Adversary with the relevant File changes for better context.	
21	It must be possible to block custom Indicators of Compromise (IOCs) : IP addresses and hashes at the managed endpoint itself through EDR console.	
22	Remediation for incidents on affected endpoints for any type of detected threat(s) as above should not be dependent upon backups, shadow copies and/or on any other 3rd party / StockHolding's solution. No reserve storage space on endpoint machine must be required by or allocated to the endpoint agent for remediation on any OS version. Solution must have surgical remediation for incidents instead of relying upon backups as the first resort.	
23	There must be a provision to configure and execute (real time and scheduled) scans on managed endpoints based on configured threat prevention policies / configuration / settings (at least on Windows) and without adversely impacting endpoint resources (CPU, RAM, Disk) in order to detect dormant threats present in these endpoints.	
24	Solution must have inbuilt dedicated SOAR module for endpoints to automate day to day tasks like notifications and response actions on suspicious endpoints without any additional cost. These notifications and response actions must be based upon pre-defined playbooks as well as capability to create custom workflow or playbook as well.	
25	Solution must have dedicated Threat Intelligence module within same console and platform capable of providing full details around adversaries group worldwide.	
Device Control		

26	The endpoint agent must be able to detect, identify and block the system (endpoint: desktop/server) from accessing physical devices such as removable storage devices, Wired, and Wireless Network Adapters (over USB channel), imaging devices, printers and others. This feature must be enabled in the endpoint agent itself without dependency on any other 3rd party / StockHolding's solution (ex: Active Directory Group Policy). All access events/logs must be sent to the cloud solution by endpoint agent for viewing and reporting. Must be compatible at least on Windows, MAC, Linux OS.	
27	The solution must provision whitelisting of authorized removable devices from corresponding policies/ configuration/ settings from the same console as that for the proposed solution for this project. Whitelisting should consist of options such as read only and both read and write access. Whitelisting may be carried out based on properties like device type (removable storage, camera, printer, etc.), device properties like Serial Number, Vendor and Product Name at the bare minimum.	
28	The agent must be able to monitor outgoing data transfers to USB devices to scan malware and classify the same accordingly (based on file type) and report the same on console along with endpoint details, process user details, removable device details and data transfer summary and date-time. There should be a provision to enable/disable this monitoring/reporting mode as well via policies.	
29	There should be a provision for displaying customizable OR inbuilt alerts/messages to endpoint (users) in case of unauthorized and/or authorized removable devices are connected to the endpoint.	
Endpoint Firewall		
30	The endpoint agent must have inbuilt component for Client/Host/endpoint firewall as a part of the same solution and must not be dependent on any other 3rd party / existing StockHolding's solution and/or infrastructure.	
31	The endpoint firewall must be able to allow, drop and log/monitor bi-directional traffic at the endpoint level for all protocols (at least for TCP, UDP and ICMP) based on customizable polices/settings/configurations on the same console as the proposed solution. The policies may be configured to allow, block, and/or monitor traffic in specified direction (originating from endpoint or targeted at endpoint), based on target/initiator IP Addresses (and subnets as well) and port(s) and protocol(s) at the bare minimum.	
32	Firewall Policy should work based on the internal/external network configuration, should be Location aware.	
33	The configured firewall policies for desktops and servers should not abnormally interfere with normal functioning of these endpoints in any way to ensure there is no outage in the StockHolding's network and/or required services are not impacted.	
Data Loss Prevention		
34	The solution should have unified agent i.e same agent of EDR to perform data protection	

35	Data protection deployed without requiring additional software push or reboot	
36	Solution should show the data flow chart from source to destination including the egress channel	
37	Solution should provide predefined content patterns, option to create custom content pattern using regex	
38	solution should be able to provide visual data flow based on web origins, Classifications, content patterns, Sensitivity Labels (Microsoft)	
39	Solution have ability to create detection based on the data restriction policy, and define severity for the detection.	
40	Solution should be able to give the details of the events triggered by data protection	
41	Solution should be able to monitor the control the data egress from managed or custom application based on the defined rules	
42	Solution should have ability to create simulation for the defined rules (allows/block) before its actually applied	
43	Ability to create workflow for automation based on the triggered detections for alerting and response action like isolation the device, etc.	
Endpoint Data Monitoring and Protection		
44	The solution should have pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also, solution should have the capability to define the third-party application. The solution should be able to define the policies for the inside and out of office endpoint machines. The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files. The endpoint solution should be able to perform discovery only when the endpoint is connected to external power or Machine is Idle.	
45	The solution should Provide “Cloud Storage Applications” group which monitor sensitive content accessed by this cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud. For Example (Should support from day 1(Supported Windows OS - Win 10, Win 11, Win 2016, Win 2019 win 2022 supported)	
46	Endpoint solution should support win 32 and 64 bit OS, Support wide variety of platforms (Below support from Day1):Win 10, Win 11, Win 2016, Win 2019 win 2022 supported, VDI (VMWare)	
Data Identification & Policy Management		
47	The solution should have a comprehensive list of predefined policies and templates and patterns to identify and classify information pertaining to different industry like Finance, Banking, PII, PCS and India IT Act.	
48	The solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file.	
49	The solution should be able to recursively inspect the content of compressed archives.	

50	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.	
51	The solution should enforce policies to detect low and slow data leaks.	
Vulnerability Assessment		
52	Solution identifies vulnerabilities tied to assets in the environment without deploying any additional agents.	
53	Solution should provide real-time vulnerability status for all windows endpoints without requiring scan.	
54	Solution provides information such as Severity, Vulnerable products, Vector, Number of Vulnerable Hosts, and Patch Recommendations for each vulnerability identified.	
55	Solution automatically "closes out" vulnerabilities without requiring user intervention as patches are installed.	
56	Solution identifies unpatched vulnerabilities that are known to be targeted by named adversaries.	
57	Delivers vulnerability management, not just vulnerability reporting.	
58	Solution prioritizes unpatched vulnerabilities that exist on systems generating detections	
59	Solution should provide the visibility if the reboot is required for the system after the patch installed.	
24*7*365 Threat Hunting		
60	24x7x365 human lead proactive threat hunting	
61	Proactively detect attack that goes undetected (beyond platform detections)	
62	Experienced hunters that uncover e-crime & nation states threat actors on daily basis	
63	Threat Hunting should be offered as an integrated service by the Platform vendor	
64	Proactive threat hunters equipped with threat intelligence (daily basis) and proactive threat hunting tools.	
65	Generating detection with details of the threat actor activities observed in the environment	
66	Email alert the stake- holders about the adverbial activity detected in the environment.	
API Integration And Reporting		
67	The solution must support integration with SIEM products and bidder should integrate the proposed solution with Qradar SIEM at AWS and or any other SIEM solution services procured by StockHolding from its Service provider.	
68	The solution must have real time streaming of alerts via API and bidder should configure the same in StockHolding environment.	
69	The solution must be capable to Query device status via API including OS, version, first seen, last seen and bidder should configure the same.	

70	The solution must support standardized and customizable reports in pdf, csv and json formats.	
Rogue or Unmanaged Device Detection		
71	The endpoint agent must be able to actively or passively scan StockHolding's network (within broadcast domain and/or across multiple subnets) to identify devices that are not having the OEM agent installed in them, to identify managed devices (having endpoint agent installed), and unsupported devices (which does not support endpoint agent). This feature must be inbuilt into the existing EDR agent and must not be dependent on any other 3rd party / existing StockHolding's solution and/or infrastructure, ex: separate VM, Active Directory, Asset Inventory, NAC, or any other.	
72	The details of such identified devices must be sent to the cloud solution by endpoint agent for viewing and reporting. The solution must be able to then classify these devices based on retrieved scan information and the derive the classified type, such as Computer: Desktop, Server, Printer, Network Infra like Switches, Firewall, etc.), along with details of the identified device such as Name, IP Address, MAC, OS details, detection time and date (whatever is possible)	
Reporting and Analytics		
73	The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view.	
74	The system should allow automatic schedule of reports to identified recipients.	
75	The reports should be exported to at least CSV and json formats.	
76	The system should provide options to save specific reports as favourites for reuse.	
77	The DLP Solution creates DLP Detections for abnormal behaviours.	
78	The DLP dashboard must display the number of cases in the designated period that fall above the risk score threshold that you have selected. Risk score thresholds must be customizable and instantly produce a report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.	
Maintenance & Support		
79	Must have 24x7 local and phone support. Response time within four hours for non-critical and one hour for critical cases. Support may include additional features like security reviews and access to named technical account manager.	
80	Customer portal - able to easily submit suspicious file samples, report technical issues and track progress on submitted requests.	
81	Site specific customized documentation should be included with the product.	
82	Dedicated named TAM should be included as a part of the Support.	
83	Solution must include deployment and on-boarding support.	

84	Pre & Post installation must be supported by OEM and SI. OEM has to review and certify.	
85	Must provide training options for administration, incident response and threat hunting.	

Note:

a. Bidder response should be complete, Yes/No answer is not acceptable.
b. Any non-compliance to above mentioned Technical specifications may lead to rejection of bid.

Dated this..... Day of 2024
(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

ANNEXURE - 4 - Commercial Price Bid Format

S/ N.	Line Item	Quantity	Unit Price (₹)	1st Year Price (₹)	2nd Year Price (₹)	3rd Year Price (₹)
License Cost (A)						
1	Endpoint Prevent	2900				
2	Endpoint Detection and Response	2900				
3	USB & Bluetooth control	2900				
4	Host Firewall	2900				
5	Application Monitoring	2900				
6	Asset Monitoring	2900				
7	Account Monitoring	2900				
8	Endpoint DLP	2900				
9	Vulnerability Management - OS, Apps	2900				
10	RAW Log telemetry (Log retention for 180 days On-prem, 180 days of RAW telemetry storage in readable format) These logs to be stored in customer premise to be compliant with SEBI guidelines.	1				
11	Premium Support 24x7 Telephonic and Email	1				
12	TAM (Technical Account Manager)	1				
13	24x7 Human based Threat Hunting	2900				
Training by OEM (for ten persons) (B)		1			Not Applicable	Not Applicable
One-time Implementation Cost (C)					Not Applicable	Not Applicable
Vendor Support Cost (D)						
Total Yearly Cost (₹) (A+B+C+D)						
GST (₹)						
Total 03 Years Cost including GST (₹)						

Notes:

a All payments will be made in INR.

b StockHolding or its subsidiaries (maximum 1,000) may purchase additional licences at the same rate as proposed by the successful bidder during the Contract period. For 2nd and 3rd year License cost should be maximum escalation upto 10% of previous year Price. Post 3rd Year, StockHolding may choose to extend the contract period for another 02 (two) years with the maximum escalation upto 10% of previous year License Price for the selected bidder.

ANNEXURE - 5 – Integrity Pact

(To be executed on plain paper and submitted only by the successful bidder)

(_____ Name of the Department / Office) RFP No._____ for_____

This pre-bid pre-contract Integrity Pact (Agreement) (hereinafter called the Integrity Pact) (IP) is made on _____ day of the _____, between, on one hand, StockHolding ., a company incorporated under Companies Act, 1956, with its Registered Office at 301, Centre Point Building, Dr. B R Ambedkar Road, Parel, Mumbai – 400012 , acting through its authorized officer, (hereinafter called **Principal**), which expression shall mean and include unless the context otherwise requires, his successors in office and assigns) of the First Part **And** M/s._____ _____(with complete address and contact details)represented by Shri _____ (i.e. Bidders hereinafter called the **`Counter Party'**) which expression shall mean and include , unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

AND WHEREAS the PRINCIPAL/Owner values full compliance with all relevant laws of the land, rules, regulations economic use of resources and of fairness/transparency in its relation with Bidder(s) /Contractor(s)/Counter Party(ies).

AND WHEREAS, in order to achieve these goals, the Principal/Owner has appointed Independent External Monitors (IEM) to monitor the Tender (RFP) process and the execution of the Contract for compliance with the principles as laid down in this Agreement.

WHEREAS THE Principal proposes to procure the Goods/services and Counter Party is willing to supply/has promised to supply the goods OR to offer/has offered the services and WHEREAS the Counter Party is a private Company/Public Company/Government Undertaking/ Partnership, constituted in accorded with the relevant law in the matter and the Principal is a Government Company performing its functions as a registered Public Limited Company regulated by Securities Exchange Board of India. **NOW THEREFORE**, To avoid all forms of corruption by following a system that is fair, transparent and free from any influence prejudiced dealings prior to, during and subsequent to the tenor of the contract to be entered into with a view to "- Enabling the PRINCIPAL to obtain the desired goods/services at competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and Enabling the Counter Party to abstain from bribing or indulging in any type of corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the PRINCIPAL will commit to prevent corruption, in any form, by its officials by following transparent procedures. The parties hereto hereby agree to enter into this Integrity Pact and agree as follows**:**

I. Commitment of the Principal / Buyer

1. The Principal Owner commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

- No employee of the Principal/Owner, personally or through any of his/her family members, will in connection with the Tender (RFP) or the execution of the contract, procurement or services/goods, demand, take a promise for or accept for self or third person, any material or immaterial benefit which the person not legally entitled to.
- The Principal/Owner will, during the Tender (RFP) Process treat all Bidder(s)/Counter Party(ies) with equity and reason. The Principal / Owner will, in particular, before and during the Tender (RFP) Process, provide to all Bidder(s) / Counter Party (ies) the same information and will not provide to any Bidder(s)/Counter Party (ies) confidential / additional information through which the Bidder(s)/Counter Party (ies) could obtain an advantage in relation to the Tender (RFP) Process or the Contract execution.
- The Principal / Owner shall endeavor to exclude from the Tender (RFP) process any person, whose conduct in the past been of biased nature.

2. If the Principal / Owner obtains information on the conduct of any of its employees which is a criminal offence under the Indian Penal Code (IPC) / Prevention of Corruption Act, 1988 (PC Act) or is in violation of the principles herein mentioned or if there is a substantive suspicion in this regard, the Principal / Owner / StockHolding will inform the Chief Vigilance Officer through the Vigilance Officer and in addition can also initiate disciplinary actions as per its internal laid down policies and procedures.

II. Commitments of Counter Parties/Bidders

1. The Counter Party commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of bid or during any pre-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following. Counter Party (ies) / Bidders commits himself to observe these principles during participation in the Tender (RFP) Process and during the Contract execution.
2. The Counter Party will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the PRINCIPAL, connected directly or indirectly with the bidding process, or to any person organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.
3. The Counter Party further undertakes that it has not given, offered or promised to give directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Principal / StockHolding or otherwise in procurement the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Principal / StockHolding for forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Principal / StockHolding.
4. Bidder / Counter Party shall disclose the name and address of agents and representatives, if any, handling the procurement / service contract.
5. Bidder / Counter Party shall disclose the payments to be made by them to agents / brokers; or any other intermediary if any, in connection with the bid / contract.
6. The Bidder / Counter Party has to further confirm and declare to the Principal / StockHolding that the Bidder / Counter Party is the original integrator and has not engaged any other individual or firm or company, whether Indian or foreign to intercede, facilitate or in any way to recommend to Principal / StockHolding or any of its functionaries whether officially or unofficially to the award of the contract to the

Bidder / Counter Party nor has any amount been paid, promised or intended to the be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

7. The Bidder / Counter Party has to submit a Declaration along with Eligibility Criteria, as given at Annexure. If bids are invited through a Consultant a Declaration has to be submitted along with the Eligibility Criteria as given at Annexure.
8. The Bidder / Counter Party, either while presenting the bid or during pre- contract negotiation or before signing the contract shall disclose any payments made, is committed to or intends to make to officials of StockHolding /Principal, or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.
9. The Bidder / Counter Party will not collude with other parties interested in the contract to impair the transparency, fairness and progress of bidding process, bid evaluation, contracting and implementation of the Contract.
10. The Bidder / Counter Party shall not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
11. The Bidder shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the Principal / StockHolding as part of the business relationship, regarding plans, proposals and business details, including information contained in any electronic data carrier. The Bidder / Counter Party also Undertakes to exercise due and adequate care lest any such information is divulged.
12. The Bidder / Counter Party commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
13. The Bidder / Counter Party shall not instigate or cause to instigate any third person including their competitor(s) of bidding to commit any of the actions mentioned above.
14. If the Bidder / Counter Party or any employee of the Bidder or any person acting on behalf of the Bidder / Counter Party, either directly or indirectly, is a relative of any of the official / employee of Principal / StockHolding, or alternatively, if any relative of an official / employee of Principal / StockHolding has financial interest / stake in the Bidder's / Counter Party firm, the same shall be disclosed by the Bidder / Counter Party at the time of filing of tender (RFP).
15. The term `relative" for this purpose would be as defined in Section 2 Sub Section 77 of the Companies Act, 2013.
16. The Bidder / Counter Party shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employees / officials of the Principal / StockHolding
17. The Bidder / Counter Party declares that no previous transgression occurred in the last three years immediately before signing of this IP, with any other Company / Firm/ PSU/ Departments in respect of any corrupt practices envisaged hereunder that could justify Bidder / Counter Party exclusion from the Tender (RFP) Process.
18. The Bidder / Counter Party agrees that if it makes incorrect statement on this subject, Bidder / Counter Party can be disqualified from the tender (RFP) process or the contract, if already awarded, can be terminated for such reason.

III. Disqualification from Tender (RFP) Process and exclusion from Future Contracts

1. If the Bidder(s) / Contractor(s), either before award or during execution of Contract has committed a transgression through a violation of Article II above or in any other form, such as to put his reliability or credibility in question, the Principal / StockHolding is entitled to disqualify the Bidder / Counter Party / Contractor from the Tender (RFP) Process or terminate the Contract, if already executed or exclude the Bidder / Counter Party / Contractor from future contract award processes. The imposition and duration of

the exclusion will be determined by the severity of transgression and determined by Principal / StockHolding. Such exclusion may be for a period of 1 year to 3 years as per the procedure prescribed in guidelines of the Principal / StockHolding.

2. The Bidder / Contractor / Counter Party accepts and undertake to respect and uphold the Principal / StockHolding's absolute right to resort to and impose such exclusion.
3. Apart from the above, the Principal / StockHolding may take action for banning of business dealings / holiday listing of the Bidder / Counter Party / Contractor as deemed fit by the Principal / Owner / StockHolding.
4. The Bidder / Contractor / Counter Party can prove that it has resorted / recouped the damage caused and has installed a suitable corruption prevention system, the Principal / Owner/ StockHolding may at its own discretion, as per laid down organizational procedure, revoke the exclusion prematurely.

IV. Consequences of Breach Without prejudice to any rights that may be available to the Principal / StockHolding / Owner under Law or the Contract or its established policies and laid down procedure, the Principal / StockHolding / Owner shall have the following rights in case of breach of this Integrity Pact by the Bidder / Contractor(s) / Counter Party:-

1. Forfeiture of EMD / Security Deposit : If the Principal / StockHolding / Owner has disqualified the Bidder(s)/Counter Party(ies) from the Tender (RFP) Process prior to the award of the Contract or terminated the Contract or has accrued the right to terminate the Contract according the Article III, the Principal / StockHolding / Owner apart from exercising any legal rights that may have accrued to the Principal / StockHolding / Owner, may in its considered opinion forfeit the Earnest Money Deposit / Bid Security amount of the Bidder / Contractor / Counter Party.
2. Criminal Liability: If the Principal / Owner / StockHolding obtains knowledge of conduct of a Bidder / Counter Party / Contractor, or of an employee of a representative or an associate of a Bidder / Counter Party / Contractor which constitute corruption within the meaning of PC Act, or if the Principal / Owner / StockHolding has substantive suspicion in this regard, the Principal /
3. StockHolding / Owner will inform the same to the Chief Vigilance Officer through the Vigilance Officer.

IV. Equal Treatment of all Bidders/Contractors / Subcontractors / Counter Parties

1. The Bidder(s) / Contractor(s) / Counter Party (ies) undertake (s) to demand from all subcontractors a commitment in conformity with this Integrity Pact. The Bidder / Contractor / Counter-Party shall be responsible for any violation(s) of the principles laid down in this Agreement / Pact by any of its sub-contractors / sub-bidders.
2. The Principal / StockHolding / Owner will enter into Pacts on identical terms as this one with all Bidders / Counterparties and Contractors.
3. The Principal / StockHolding / Owner will disqualify Bidders / Counter Parties / Contractors who do not submit, the duly signed Pact, between the Principal / Owner / StockHolding and the Bidder/Counter Parties, along with the Tender (RFP) or violate its provisions at any stage of the Tender (RFP) process, from the Tender (RFP) process.

VI. Independent External Monitor (IEM)

1. The Principal / Owner / StockHolding has appointed competent and credible Independent External Monitor (s) (IEM) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Integrity Pact.

2. The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the Chief Executive Officer and Managing Director, StockHolding Ltd.
3. The Bidder(s)/Contractor(s) / Counter Party(ies) accepts that the IEM has the right to access without restriction, to all Tender (RFP) documentation related papers / files of the Principal / StockHolding / Owner including that provided by the Contractor(s) / Bidder / Counter Party. The Counter Party / Bidder / Contractor will also grant the IEM, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his or any of his Sub-Contractor‟s Tender (RFP) Documentation / papers / files. The IEM is under contractual obligation to treat the information and documents of the Bidder(s) / Contractor(s) / Sub-Contractors / Counter Party (ies) with confidentiality.
4. In case of tender (RFP)s having value of 5 crore or more, the Principal / StockHolding / Owner will provide the IEM sufficient information about all the meetings among the parties related to the Contract/Tender (RFP) and shall keep the IEM apprised of all the developments in the Tender (RFP) Process.
5. As soon the IEM notices, or believes to notice, a violation of this Pact, he will so inform the Management of the Principal / Owner /StockHolding and request the Management to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit nonbinding recommendations. Beyond this, the IEM has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The IEM will submit a written report to the CEO&MD, StockHolding. Within 6 to 8 weeks from the date of reference or intimation to him by the Principal / Owner / StockHolding and should the occasion arise, submit proposals for correcting problematic situations.
7. If the IEM has reported to the CEO&MD, StockHolding Ltd. a substantiated suspicion of an offence under the relevant IPC/PC Act, and the CEO&MD, StockHolding has not within reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the IEM may also transmit the information directly to the Central Vigilance Officer.
8. The word `IEM‟ would include both singular and plural.

VII. Duration of the Integrity Pact (IP)

This IP begins when both the parties have legally signed it. It expires for the Counter Party / Contractor / Bidder, 12 months after the completion of work under the Contract, or till continuation of defect liability period, whichever is more and for all other Bidders, till the Contract has been awarded. If any claim is made / lodged during the time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by the CEO&MD StockHolding

VIII. Other Provisions

1. This IP is subject to Indian Law, place of performance and jurisdiction is the Head Office / Regional Offices of the StockHolding /Principal / Owner who has floated the Tender (RFP).
2. Changes and supplements in any Procurement / Services Contract / Tender (RFP) need to be made in writing. Change and supplement in IP need to be made in writing.
3. If the Contractor is a partnership or a consortium, this IP must be signed by all the partners and consortium members. In case of a Company, the IP must be signed by a representative duly authorized by Board resolution.
4. Should one or several provisions of this IP turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

5. Any dispute or difference arising between the parties with regard to the terms of this Agreement / Pact, any action taken by the Principal / Owner / StockHolding in accordance with this Agreement / Pact or interpretation thereof shall not be subject to arbitration.

IX. Legal and Prior Rights

All rights and remedies of the parties hereto shall be in addition to all the other legal rights and remedies belonging to such parties under the Contract and / or law and the same shall be deemed to be cumulative and not alternative to such legal rights and remedies aforesaid. For the sake of brevity, both the Parties agrees that this Pact will have precedence over the Tender (RFP) / Contract documents with regard to any of the provisions covered under this Integrity Pact.

IN WITHNESS WHEREOF the parties have signed and executed this Integrity Pact (IP) at the place and date first above mentioned in the presence of the following witnesses:-

---

(For and on behalf of Principal / Owner / StockHolding

(For and on behalf of Bidder / Counter Party / Contractor)

WITNESSES:

1._____ (Signature, name and address)

2._____ (Signature, name and address)

Note: In case of Purchase Orders wherein formal agreements are not signed references to witnesses may be deleted from the past part of the Agreement.

ANNEXURE- 6 - Covering Letter on bidder's Letterhead of Integrity Pact

To,

---------- ----------

Sub**:** RFP REF NO: IT-08/2024-25 dated 09-Sep-2024 Endpoint Detection and Response (EDR) solution for StockHolding

Dear Sir,

DECLARATION

Stock Holding Corporation of India Limited (StockHolding) hereby declares that StockHolding has adopted Integrity Pact (IP) Program as advised by Central Vigilance Commission vide its Letter No. ---------- Dated ---------- and stands committed to following the principles of transparency, equity and competitiveness in public procurement. The subject Notice Inviting Tender (RFP) (NIT) is an invitation to offer made on the condition that the Bidder will sign the Integrity Agreement, which is an integral part of tender (RFP) documents, failing which the tender (RFP)er / bidder will stand disqualified from the tender (RFP)ing process and the bid of the bidder would be summarily rejected. This Declaration shall form part and parcel of the Integrity Agreement and signing of the same shall be deemed as acceptance and signing of the Integrity Agreement on behalf of the StockHolding

Yours faithfully,

For and on behalf of StockHolding Corporation of India Limited
(Authorized Signatory)

ANNEXURE – 7 – Compliance Statement
(To be submitted on Company Letter Head)

RFP REF NO: IT-08/2024-25 dated 09-Sep-2024 for Endpoint Detection and Response (EDR) solution for StockHolding

DECLARATION

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the StockHolding. We also agree that the StockHolding reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

Sr. No.	Item / Clause of the RFP	Compliance (Yes / No)	Remarks/Deviations (if any)
1	Objective of the RFP		
2	Scope of Work		
3	Eligibility Criteria		
4	Service Level Agreement (SLA) / Scope of Work		
5	Non-Disclosure Agreement		
6	Payment Terms		
7	Bid Validity		
8	Integrity Pact		
9	All General & Other Terms & Conditions in the RFP		
10	Technical Specification		

(If Remarks/Deviations column is left blank it will be construed that there is no deviation from the specifications given above)

Date:

Signature with seal

Name & Designation:

ANNEXURE – 8 – Format of Bank Guarantee

This Bank Guarantee is executed by the ---------- (Bank name) a Banking Company incorporated under the Companies Act, 1956 and a Scheduled Bank within the meaning of the Reserve Bank of India Act, 1934 and having its head office at ---------- and branch office at _____(hereinafter referred to as the "Bank", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) and Branch office at _____ in favour of Stock Holding Corporation of India Limited, a Company incorporated under the Companies Act, 1956 and having its Registered Office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400 012 (hereinafter referred to as "StockHolding", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) at the request of _____, a Company incorporated under the Companies Act, 1956 and having its Registered Office at (hereinafter referred to as the "Service Provider", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns).

Whereas

A. StockHolding has, pursuant to the Tender No. _____, issued the Purchase Order dated _____ to the Service Provider for providing _____
B. In terms of the said Tender, the Service Provider has agreed to furnish to StockHolding, a Bank guarantee for Rs. _____ /- (Rupees _____ only) till _____ (date).
C. The Bank has, at the request of the Service Provider, agreed to give this guarantee as under.

NOW IN CONSIDERATION OF THE FOREGOING:

1. We, the Bank, at the request the Service Provider, do hereby unconditionally provide this guarantee to StockHolding as security for due performance and fulfilment by the Service Provider of its engagements, commitments, operations, obligations or liabilities including but not limited to any sums / obligations / claims due by the Service Provider to StockHolding for meeting, satisfying, discharging or fulfilling all or any obligation or liability of the Service Provider, under the said Tender / Purchase Order.

2. We, the Bank, hereby guarantee and undertake to pay StockHolding up to a total amount of Rs. _____/- (Rupees _____ only) under this guarantee, upon first written demand of StockHolding and without any demur, protest and without any reference to the Service Provider.
3. Any such demand made by StockHolding shall be conclusive and binding on the Bank as regards the amount due and payable notwithstanding any disputes pending before any court, Tribunal, or any other authority and/ or any other matter or thing whatsoever as the liability of the Bank under these presents being absolute and unequivocal.
4. We, the Bank, agree that StockHolding shall have the fullest liberty without consent of the Bank to vary the terms of the said Tender/ Purchase Order or to postpone for any time or time to time exercise of any powers vested in StockHolding against the Service Provider and to forbear or enforce any of the Terms & Conditions relating to the said Tender / Purchase Order and the Bank shall not be relieved from its liability by the reason of any such variation, or extension being granted to the Service Provider or for any forbearance, act or omission or any such matter or thing whatsoever.
5. We, the Bank, agree that the guarantee herein contained shall be irrevocable and shall continue to be enforceable until it is discharged.
6. This Guarantee shall not be affected by any change in the Constitution of the Bank or the Service Provider or StockHolding.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN ABOVE:

1. The liability of the bank under this guarantee is restricted to a sum of Rs. _____/- (Rupees _____ only).
2. This Bank Guarantee will be valid for a period up to _____ (date).
3. A written claim or demand for payment under this Bank Guarantee on or before _____ (date) is the only condition precedent for payment of part/full sum under this guarantee.

For Issuing Bank

Name of Issuing Authority:

Designation of Issuing Authority:

Employee Code:

Contact Number:

Email ID: