**Response to Prebid Queries for RFP**

***Date: 27-Sep-2024***

| | |
|---|---|
| **RFP Name** | **RFP for Endpoint Detection and Response (EDR) solution for StockHolding** |
| **RFP Ref. No.** | IT-08/2024-25 _ GEM/2024/B/5378533 |
| **RFP Date** | 09-Sep-2024 |

| S. No. | Page No. | Section | Reference Clause No. | Document Reference | Clarification sought/Query | *Response* |
|---|---|---|---|---|---|---|
| 1 | 7 | Eligibility Criteria | Point 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. | Kindly modify as:<br>The Bidder should have experience of EDR implementation at customer premises / Cloud based and deployment of minimum 10000 agents at customer premises in any Financial Institution / PSU / Government Organization / Large Corporates in India not older than 03 (three) years from RFP date. | *No change* |
| 2 | 8 | Eligibility Criteria | Point 12 | OEM proposed solution should be in-line with SEBI regulatory Framework. Confirmation on OEMs letterhead with reference to Circular numbers and points. | OEM's will not be providing a clear certificate with regards the above mentioned confirmation of the SEBI regulatory framework . Requesting to waive off the point. | ***Modified as:***<br>*OEM proposed solution should be in-line with SEBI regulatory Framework. Confirmation on Bidder/ OEMs letterhead with reference to Circular numbers and points.* |
| 3 | 7 | Eligibility Criteria | Point 6 | The bidder must have following valid Certifications:<br>• ISO 27001:2013 certified | Currently we are undergoing the process of getting certified for ISO 27001:2022 . A letter from our ISO partner can be provided to validate the same. | ***Modified as:***<br>*The bidder must have minimum ISO 27001:2013 certification or higher. ISO Certification has to be submitted by the bidder.* |
| 4 | 7 | Eligibility Criteria | Point 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. | Kindly modify as:<br>The Bidder should have experience of EDR 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 05 (five) years from RFP date. | ***Modified as:***<br>*The Bidder should have experience of EDR and 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 05 (five) years from RFP date.* |
| 5 | 3 | Data Sheet | 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 | As our company crosses 500 Cr we are exempted from EMD as per. General Terms and Conditions on GeM 4.0 (Version 1.16) dt 17th July 2024. Hence kindly suggest whether we have to submit EMD. | *Need to submit proof for exemption along with Technical bid* |
| 6 | NA | General Query | NA | As per Undertaking for Custom Bid for Services Creation on GeM<br>Make In India:<br>Required features is not available for any Make In India EDR OEM. | MII is not required mentioned under Undertaking for Custom Bid for Services Creation on GeM. But in the GEM bid page 2 of 6 it is mentioned as MII Compliance - Yes. Kindly provide clarity on whether MII is required or not. | *MII clause is not mandatory for this RFP* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | 7 | Eligibility Criteria | Point 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. | It is mentioned that Implementation of EDR solution for at least Five years is required. Do you accept global clients experience also or required experience with Indian clients only. | *Only EDR solution experience in India only* |
| 8 | 7 | Eligibility Criteria | Point 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. | We would like to know if we could submit the customer references/PO for EDR of one customer and the reference/PO for DLP implementation of another customer. | *Yes. EDR and DLP experiences can be separately provided of independent customers* |
| 9 | 22 | Technical Specification | API Integration And Reporting | 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. | Can you provide more details on the integration requirements with existing security and IT operation systems like existing SIEM / XDR. | *Bidder has to provide support for integration of cloud based EDR solution with StockHolding's SIEM running on Qradar. It might require API based integration as we need to collect logs at centralised SIEM Solution.* |
| 10 | 10 | Scope of Work | NA | General Query | Are there any specific third-party tools that you currently uses for vulnerability assessments, and should the EDR solution be compatible with them?<br>- To ensure the compatibility with existing tools | *Bidder can propose more than one Agent / OEM to meet the requirement of Eligibility Criteria Serial Number 7.* |
| 11 | 10 | Scope of Work | NA | General Query | Will additional licenses (if required) follow the same cost structure or can it be renegotiated?<br>*- To calculate most approximate cost.* | *Additional licenses will follow the same cost structure as mentioned in the RFP* |
| 12 | 10 | Scope of Work | Operation Phase | General Query | Please clarify if we can size the team to manage the EDR and DLP implementations and also during Operation Phase? | *The bidder is required to deploy onsite resources exclusively during the implementation phase until deployment is completed across all systems. After the implementation, onsite engineers will be needed on a case-by-case basis throughout the duration of the contract* |
| 13 | 11 | Scope of Work | Deployment Phase | General Query | What support from your IT team can the bidder expect during the implementation across branch locations?<br>- The document does not mention the level of support from internal teams during the multi-phase deployment. | *Bidder has ownership to complete the deployment.* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 14 | 10 | Scope of Work | Pre-Deployment Phase | General Query | As per the pre-deployment phase, do you want the vendor to perform a security and vulnerability assessment of the existing infra? | *Bidder has to conduct the VA of tenant provided to us by OEM during pre-deployment phase. Vulnerabilities if any needs to be close in consultation with OEM* |
| 15 | 10 | Scope of Work | NA | General Query | Do you want the vendor to perform vulnerability assessment and patch upgrades for all the servers and endpoints in scope during the engagement? If yes, what is the frequency? Does this include PT as well? | *EDR solution should have inbuilt capability to detect vulnerabilities of end points. Same has been included in point number 52 to 59. Bidder needs to comply for the same* |
| 16 | 14 | Scope of Work | Point viii | General Query | Please let us know if Stockholding has their own Threat Intelligence Tool or want the vendor to provide the same? | *StockHolding expects Solution must have dedicated Threat Intelligence module within same console and platform capable of providing full details around adversaries group worldwide. Please refer point number 25 in "Next-Gen Anti-Virus and EDR"* |
| 17 | 16 | Scope of Work | Sl. No 6 | General Query | Could you specify the data retention policy for telemetry data collected from endpoints? Do you want to store same on-premises data to be stored on Cloud instance or is it additional time period? Also please clarify who is supposed to manage log storage infra (both on-prem and cloud) | *Kindly refer Annexure 4. point number 11. 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* |
| 18 | 16 | Scope of Work | NA | General Query | Can you provide more details of the segregation of roles level wise or vendor can decide based on the overall scope? | *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* |
| 19 | 10 | Scope of Work | NA | General Query | Are there any existing third-party vendors or service providers that we will need to collaborate with during the EDR and DLP implementation? If so, can you provide details on their roles and responsibilities? | *Bidder can coordinate with inhouse SOC team members of StockHolding* |
| 20 | 10 | Scope of Work | NA | General Query | Can you please provide detailed information about the current SOC setup, including the existing tools and technologies in use? | *Details can be provided to successful bidder* |
| 21 | 10 | Scope of Work | NA | General Query | Do you want EDR and DLP from the same OEM or different OEMs can be included? | *DLP should be part of EDR deployment* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 22 | 10 | Scope of Work | NA | General Query | Please clarify if the support is onsite or remote? | ***Modified as:***<br>*The bidder is required to deploy onsite resources exclusively during the implementation phase until deployment is completed across all systems. After the implementation, onsite engineers will be needed on a case-by-case basis throughout the duration of the contract* |
| 23 | 10 | Scope of Work | NA | General Query | Please update if Stockholding has their ITSM tool or vendor needs to provide the same? | *StockHolding has their own ITSM tool* |
| 24 | 8 | Eligibility Criteria | Point 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. | Request to Please remove the Gartner & IDC Certifications as this is not in line to Government notification for promoting Make in India Products: P-45014/33/2021-BE-II (E-64737) | *No change* |
| 25 | 10 | Scope of Work | NA | 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. | Request to change the Point as "All the systems/components in the proposed solution should be integrated with the StockHolding's current security and IT operation systems like SOC, SIEM, AD etc. and all such security and operations management systems which has been and will be deployed in the StockHolding from time to time." | *No change* |
| 26 | 10 | Scope of Work | NA | 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. | Request to change the Point as " web access policies can be implemented which blocks active C&C communication attempts identified by the solution. | *No change* |
| 27 | 10 | Scope of Work | NA | 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. | Request to change the Point as "solution should be able to scan StockHolding's Email Solution at endpoints, create / add identified threats. The Solution can work in conjunction with email, but it should not be dependent on it." | *No change* |
| 28 | 10 | Scope of Work | NA | 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. | Request to change the Point as "Data movement of sensitive information & classifications based on a combination of content patterns and file types." | *No change* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 29 | 15-23 | Technical Specification | Point 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:<br> Notification for any similar changes in files/ folders across multiple hosts.<br> Dashboard to showcase hosts with most violations, Top Changes made, change trends with change severity ratings.<br> Change Log<br> Attribute any Adversary with the relevant File changes for better context. | Request to change the Point as: Solution 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:<br> Notification for any similar changes in files/folders across multiple hosts.<br> Dashboard to showcase hosts with most violations.<br> Attribute any Adversary with the relevant File changes for better context. | *No change* |
| 30 | 15-23 | Technical Specification | Point 38 | solution should be able to provide visual data flow based on web origins, Classifications, content patterns, Sensitivity Labels (Microsoft) | Request to change the Point as "solution should be able to provide reports to show the origins, Classifications," | *No change* |
| 31 | 15-23 | Technical Specification | Point 42 | Solution should have ability to create simulation for the defined rules (allows/block) before its actually applied | Request to change the Point as "Solution should have ability to define rules (allows/block)" | *No change* |
| 32 | 15-23 | Technical Specification | Point 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. | Request to change the Point as "The solution should have pre-defined applications and multiple application groups and 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. The endpoint solution should be able to perform discovery of unmanaged devices." | *No change*<br>*This is to prevent battery-powered laptops from being constantly scanned, extending their battery life and reducing network congestion during peak usage hours.* |
| 33 | 15-23 | Technical Specification | Point 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. | Request to please remove this Point as it will be part of separate Data Privacy solution. | *No change* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 34 | 15-23 | Technical Specification | Point 53 | Solution should provide real-time vulnerability status for all windows endpoints without requiring scan. | Request to change the Point as "Solution should provide real-time vulnerability status for all windows endpoints." | *No change* |
| 35 | 15-23 | Technical Specification | Point 68 | The solution must have real time streaming of alerts via API and bidder should configure the same in StockHolding environment. | Request to change the Point as "The solution must have real time details of alerts and bidder should configure the same in StockHolding environment." | *No change* |
| 36 | 15-23 | Technical Specification | Point 70 | The solution must support standardized and customizable reports in pdf, csv and json formats. | Request to change the Point as "The solution must support standardized and customizable reports in pdf, csv formats." | *No change* |
| 37 | 15-23 | Technical Specification | Point 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) | Request to change the Point as "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 along with details of the identified device such as Name, IP Address,OS details, etc." | *No change* |
| 38 | 15-23 | Technical Specification | Point 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),<br>and data at the endpoint (endpoint) in a single view. | Request to change the Point as "The solution should have a dashboard view designed for use by executives & also can provide information from data at rest (storage) and endpoint (endpoint) reports." | *No change* |
| 39 | 15-23 | Technical Specification | Point 75 | The reports should be exported to at least CSV and json formats. | Request to change the Point as "The reports should be exported to at least CSV or json formats." | *No Change* |
| 40 | 15-23 | Technical Specification | Point 76 | The system should provide options to save specific reports as favourites for reuse. | Request to change the Point as "The system should provide options to save specific reports." | *No change* |
| 41 | 15-23 | Technical Specification | Point 77 | The DLP Solution creates DLP Detections for abnormal behaviours. | Request to change the Point as "The DLP Solution creates DLP Detections report" | *No change* |
| 42 | 15-23 | Technical Specification | Point 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. | Request to change the Point as "The solution provide DLP reports that shows the details about the DLP violations." | *No change* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 43 | 7 | Eligibility Criteria | Point 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. | We request you to kindly relax the clause for wider participation & amend the clause as follows :<br>"The Bidder should have experience of EDR **OR** DLP implementation through Cloud based **OR** **On-Premised 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." | *No change* |
| 44 | 10 | Scope of Work | Point 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. | We understand that bidders scope is limited to applying the policies in the proposed EDR & DLP solution as per the recommend enations of the findings of Stockholding security auditing team. Kindly confirm the understanding. | *Here configuration audit means hardening of tenant as per the best practices.* |
| 45 | 10&11 | Scope of Work | 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). | Kindly provide the details of the all the system which needs to be integrated with proposed solution using API integration | *API Integration to be completed on approximately 25+ Servers.* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 46 | 10&11 | Scope of Work | Phase 1, Phase 2 and Phase 3 Implementation | 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).<br>2. Phase 2 Implementation: Deployment in StockHolding’s Branch locations - Number of Counts. 1000 end points<br>3. Phase 3 Implementation: Deployment in StockHolding’s Branch locations - Number of Counts. 1000 end points along with all activities as mentioned below. | There is an ambiguity in the endpoint license count. As per the implementation Phases -1 , 2 & 3 ,there is a total of 3000 (850+150-Phase-1 , 1000 in Phase-2 & 3 each) end point counts whereas as per RFP pg no 25 ,License for 2900 endpoints is asked. Kindly clarify the total license counts to be considered. | *Please consider 2900 license count. Last phase has 900 end point counts.* |
| 47 | 11 | Scope of Work | Point 3 | Conduct testing to ensure proper functionality and integration with existing security infrastructure. | Kindly provide the details of the existing security infrastructure system which needs to be integrated with proposed solution. | *Security Infrastructure Servers deployed on Windows and Linux platform* |
| 48 | 16 | End point Detection and Response | Point 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. | We understand that compute & storage required for storing the telemetry data in StockHoldings premises will be provided by StockHolding team. Kindly confirm. | *Yes* |
| 49 | 16 | End point Detection and Response | Point 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. | We understand that StockHolding already had Microsoft Active Directory Group Policy Update (GPO) which can be utilised by bidders to deploy the agent. Kindly confirm. | *Bidder can provide the detail steps for deploying the agents through AD Group policy.<br>Dependency should not be on Stockholding resources, where as platform can be provided for deployment of agents* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 50 | 8 | Eligibility Criteria | Point 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<br>per the IDC's latest Endpoint security market share report | This is with reference to the OM vide P45014/33/2021-BE-II(E-64737) Dated: 20.12.2022, buyer should promote Make In India and should not keep any restrictive clauses viz. Gartner reports, IDC reports, Forrester Wave, etc. in the bids which can restrict the make in India bidders from participation.<br>Hence, we request you to kindly remove the restrictive clauses as per the above-mentioned OM. Copy of OM is enclosed herewith for your kind perusal. | *No change* |
| 51 | 8 | Eligibility Criteria | Point 7 | 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.<br>Note: Above criteria is not applicable for integrated endpoint DLP with proposed EDR. | This is with reference to the OM vide P45014/33/2021-BE-II(E-64737) Dated: 20.12.2022, buyer should promote Make In India and should not keep any restrictive clauses viz. Gartner reports, IDC reports, Forrester Wave, etc. in the bids which can restrict the make in India bidders from participation.<br>Hence, we request you to kindly remove the restrictive clauses as per the above-mentioned OM. Copy of OM is enclosed herewith for your kind perusal. | *No change* |
| 52 | 7 | Eligibility Criteria | Point 10 | Bidder must have support office/center at Tier 1 cities in India. | Kindly clarify the point.<br>Is Bidder should have office in all Tier 1 cities. | *Yes. They should have office in all Tier 1 cities* |
| 53 | 25 | Terms and Conditions (A. Payment:) | NA | Annual Payment - 100% Payment against Delivery on submission of Original Invoice and confirmation of License Certificate duly authorized by StockHolding Official | Kindly modify as:<br>100% Payment against Delivery on submission of Original Invoice and confirmation of License Certificate duly authorized by StockHolding Official | *No change* |
| 54 | 10 | Requirement | NA | 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.<br>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. | We need complete scope of work details regarding customisation, enabling, disabling, and parameterisation during the contract period.<br>Also share all platform details which requires integrations. | *The bidder is required to deploy onsite resources exclusively during the implementation phase until deployment is completed across all systems. After the implementation, onsite engineers will be needed on a case-by-case basis throughout the duration of the contract* |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| 55 | 10 | Scope of Work | Enhanced Endpoint Security | 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. | For this we need to align call with our Professional Service team to define the scope of work for deployment in 5% endpoints. | *Yes, the OEM needs to complete the installation and implementation on 5% of endpoint devices following the completion of their secure tenant configuration.* |
| 56 | 11 | Scope of Work | c) Deployment Phase | 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.<br>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.<br>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.<br>g. Support the end-users and departments in the pre and post deployment during contract period. | Share all platform (Vendor & Product details) which requires integrations. | *Details can be provided to successful bidder* |
| 57 | 12 | Scope of Work | Monitoring and Reporting | i. Monitor device connections and activities to detect unauthorized devices or policy violations.<br>ii. Generate reports on device compliance status and incidents | Kindly modify as:<br>Monitor and Generate reports based on Security Policy for Threat Protection Policy and Tamper Protection. | *No change* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 58 | 12 | Scope of Work | 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.<br>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.<br>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.<br>4. Ensure that the DLP solution complies with relevant regulations and standards.<br>5. DLP should be configured to provide real-time visibility into data movement across sources, egress channels and destinations.<br>6. Custom data classification for accurate contextual visibility into data egress events.<br>7. Data movement of sensitive personally identifiable information (PII) and reduce noise with nuanced classifications based on a combination of content patterns, sensitivity | DLP should be able to monitor and take necessary actions based on Content and File based policy's. | *Data Loss Prevention should comply all the mentioned points.* |
| 59 | 12 | Scope of Work | 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. | Need more details | *Policies needs to modified as per the changing requirements of regulatory compliance.* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 60 | 15 | Technical Specification | Point 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:<br>1. Next-Gen Anti-Virus<br>2. End Point Detection and Response (EDR)<br>3. Device control (USB, BLUETOOTH)<br>4. Rogue Device Discovery, Detection and Reporting<br>5. Endpoint/Host Firewall<br>6. Vulnerability Detection on End Points Apps, OS and Asset Inventory<br>7. FIM (File Integrity Monitoring)<br>8. Remote Response from EDR Console<br>9. SOAR (Automated Response Capabilities)<br>Note – Above Modules must be accessible through single Unified Console itself and not via any multiple consoles." | This seems to be from a specific vendor as most of the solutions for EDR are focused on:<br>1. Next-Gen Anti-Virus<br>2. End Point Detection and Response (EDR)<br>3. Device control (USB, BLUETOOTH)<br>4. Remote Response from EDR Console<br>5. Extended Detection and Response followed by Managed Detection & Response as a Service<br><br>Need change in point to have above points as mandatory and rest can be optional or good to have from single agent. | *Modified as:*<br>*"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:*<br>*1. Next-Gen Anti-Virus*<br>*2. End Point Detection and Response (EDR)*<br>*3. Device control (USB, BLUETOOTH)*<br>*4. Rogue Device Discovery, Detection and Reporting*<br>*5. Endpoint/Host Firewall*<br>*6. Vulnerability Detection on End Points Apps, OS and Asset Inventory*<br>*7. FIM (File Integrity Monitoring)*<br>*8. Remote Response from EDR Console*<br>*9. SOAR (Automated Response Capabilities)*<br>*Note – Above Modules must be accessible through single Unified Console itself and not via any multiple consoles."*<br><br>*Bidder can propose more than one agent / OEM to achieve all 9 features, subjected to proposed OEM's solutions are meeting the eligibility criteria.* |
| 61 | 15 | Technical Specification | Point 2 | The agent must be same for all types of systems. All features listed above must be part of single agent and from same OEM | This seems to be from a specific vendor. | *Modified as:*<br><br>*All features listed above must be part of single agent or bidder can propose more than one Agent / OEM to meet the requirement* |
| 62 | 15 | Technical Specification | Point 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<br>to StockHolding's. | Kindly modify as:<br>Telemetry data can be stored on Cloud Platform for atleast 180 days and locally up to 30 days on respective endpoint systems | *Modified as:*<br>*The collected telemetry from all endpoints must be stored in OEM's Cloud for minimum period of 180 days and The collected telemetry from all endpoints must be stored in StockHolding premise in a human readable format without any additional cost.* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 63 | 17 | Technical Specification | Point 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. | For Endpoints reboot can be scheduled. However for Servers reboot is required | *No change* |
| 64 | 17 | Technical Specification | Point 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. | Is it okay if the EDR detections give link to analysis the sample using Virus Total or In-house threat Intel Tool. | *No change* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 65 | 18 | Technical Specification | Point 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:<br>1. Notification for any similar changes in files/folders across multiple hosts.<br>2. Dashboard to showcase hosts with most violations, Top Changes made, change trends with change severity ratings.<br>3. Change Log<br>4. Attribute any Adversary with the relevant File changes for better context. | Is FIM is for Servers or for both endpoints and Servers.<br>Can it be changed to only servers? | *Both. For end points and Servers* |
| 66 | 19 | Technical Specification | Point 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. | Can we change this to either SOAR or XDR module<br>Can playbooks be optional | *No change* |
| 67 | 19 | Technical Specification | Point 25 | Solution must have dedicated Threat Intelligence module within same console and platform capable of providing full details around adversaries group worldwide. | Can this point changed to - Solution must have dedicated Threat Intelligence site (same or different platform) for providing full details around adversaries group worldwide. | *No change* |
| 68 | 20 | Technical Specification | Point 31 | The endpoint firewall must be able to allow, drop and log/monitor bidirectional 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. | Can solution manage Windows Firewalls with Domain, Private and Public Networks to Monitor and Block. | *EDR should provide functionality of Firewall not windows inbuilt firewall* |
| 69 | 20 | Technical Specification | Point 32 | Firewall Policy should work based on the internal/external network configuration, should be Location aware. | Can solution manage Windows Firewalls with Domain, Private and Public Networks to Monitor and Block. | *EDR should provide functionality of Firewall not windows inbuilt firewall* |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| 70 | 20 | Technical Specification | Point 36 | Solution should show the data flow chart from source to destination including the egress channel | Can this point be modified if required. | *No change* |
| 71 | 20 | Technical Specification | Point 38 | solution should be able to provide visual data flow based on web origins, Classifications, content patterns, Sensitivity Labels (Microsoft) | Can this point be optional or "good to have" | *No change* |
| 72 | 20 | Technical Specification | Point 39 | Solution have ability to create detection based on the data restriction policy, and define severity for the detection. | Can this point changed to - Solution have ability to create detection based on the data restriction policy. | *No change* |
| 73 | 20 | Technical Specification | Point 42 | Solution should have ability to create simulation for the defined rules (allows/block) before its actually applied | Can this point be optional or "good to have" | *No change* |
| 74 | 20 | Technical Specification | Point 43 | Ability to create workflow for automation based on the triggered detections for alerting and response action like isolation the device, etc. | Can this point be optional or "good to have" | *No change* |
| 75 | 20 | Technical Specification | Point 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. | Can this point be optional or "good to have" | *No change* |
| 76 | 20 | Technical Specification | Point 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) | Can this point be optional or "good to have" | *No change* |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| 77 | 21 | Technical Specification | Point 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. | Can this point be optional or "good to have" | *No change* |
| 78 | 21 | Technical Specification | Point 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. | Can this point be optional or "good to have" | *No change* |
| 79 | 21 | Technical Specification | Point 51 | The solution should enforce policies to detect low and slow data leaks. | Can this point be optional or "good to have" | *No change* |
| 80 | 22 | Technical Specification | Point 52-59 | Vulnerability Assessment | Can this point be optional or "good to have" | *No change* |
| 81 | 22 | Technical Specification | Point 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. | Can this point be optional or "good to have" | *No change* |
| 82 | 23 | Technical Specification | Point 77 | The DLP Solution creates DLP Detections for abnormal behaviours. | Can this point be optional or "good to have" | *No change* |
| 83 | 23 | Technical Specification | Point 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. | Can this point be optional or "good to have" | *No change* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 84 | NA | Technical Specification | End point Detection and Response End Point Agent | "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:<br> Next-Gen Anti-Virus<br> End Point Detection and Response (EDR)<br> Device control (USB, BLUETOOTH)<br> Rogue Device Discovery, Detection and Reporting<br> Endpoint/Host Firewall<br> Vulnerability Detection on End Points Apps, OS and Asset Inventory<br> FIM (File Integrity Monitoring)<br> Remote Response from EDR Console<br> SOAR (Automated Response Capabilities)<br>Note – Above Modules must be accessible through single Unified Console itself and not via any multiple consoles." | "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:<br> Next-Gen Anti-Virus<br> End Point Detection and Response (EDR)<br> Device control (USB, BLUETOOTH, PRINTER, WIFI, PRTSC & CAMERA)<br> Rogue Device Discovery, Detection and Reporting<br> Endpoint/Host Firewall & Application Control<br> Vulnerability Detection on End Points Apps, OS and Asset Inventory<br> FIM (File Integrity Monitoring) and Log inspection module for servers<br> Remote Response from EDR Console<br> SOAR (Automated Response Capabilities)<br>Note – Above Modules must be accessible through single Unified Console itself and not via any multiple consoles." | *Modified as:*<br>*"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:*<br>*1. Next-Gen Anti-Virus*<br>*2. End Point Detection and Response (EDR)*<br>*3. Device control (USB, BLUETOOTH)*<br>*4. Rogue Device Discovery, Detection and Reporting*<br>*5. Endpoint/Host Firewall*<br>*6. Vulnerability Detection on End Points Apps, OS and Asset Inventory*<br>*7. FIM (File Integrity Monitoring)*<br>*8. Remote Response from EDR Console*<br>*9. SOAR (Automated Response Capabilities)*<br>*Note – Above Modules must be accessible through single Unified Console itself and not via any multiple consoles."*<br>*Bidder can propose more than one agent / OEM to achieve all 9 features, subjected to proposed OEM's solutions are meeting the eligibility criteria.* |
| 85 | NA | Technical Specification | Endpoint Data Monitoring and Protection | 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. | Need more Clarifications and use case for statement "solution should have the capability to define the third-party application" Please share the use case.<br>Need More Clarification & use case for statement "The endpoint solution should be able to perform discovery only when the endpoint is connected to external power or Machine is Idle." | *No change.*<br>*This is to prevent battery-powered laptops from being constantly scanned, extending their battery life and reducing network congestion during peak usage hours* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 86 | NA | Technical Specification | Rogue or Unmanaged Device Detection | 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. | The proposed solution (NDR) must be able to actively or passively detect 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). | *No Change* |
| 87 | NA | Extra relevant points | Rogue or Unmanaged Device Detection | Addition of New Clause | Solution should Continuously analyzes current and historical network metadata and correlates these related threat events into a single view for full visibility of the attack cycle. | *Not Required* |
| 88 | NA | Extra relevant points | Rogue or Unmanaged Device Detection | Addition of New Clause | Solution Should support advanced and sophisticated machine learning techniques to detect network traffic anomalies. Correlates the events and maps out every step of the attack, giving a better idea of how to respond and prevent future attacks. | *Not Required* |
| 89 | NA | Extra relevant points | Rogue or Unmanaged Device Detection | Addition of New Clause | Solution Should have capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc..) | *Not Required* |
| 90 | NA | Extra relevant points | Vulnerability Assessment | Addition of New Clause | Solution should offer virtual patching to protect earlier and more effectively, blocking exploits on arrival— especially with critical servers and workloads where it is difficult to apply vendor patches. Solution provider should be market leader in disclosing vulnerabilities in the market | *Not Required* |
| 91 | NA | Extra relevant points | Vulnerability Assessment | Addition of New Clause | Solution should have capability to Scan the System for Open Vulnerabilities & Exploits & assign only recommended applicable HIPS rule to protect the system from various threats. | *Not Required* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 92 | NA | Extra relevant points | Compliance | Addition of New Clause | Proposed solution should store all the telemetry data collected from endpoints at MeitY compliant data Centre in India | *Not Required* |
| 93 | 8 | Eligibility Criteria | Point 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 | The proposed EDR/EPP Solution must be listed as leaders in Gartner's Magic quadrant for End Point Protection/leaders or strong performers in Forrester Wave's latest report for EDR/EPP Solutions or Top 3 Leader's as per the IDC's latest Endpoint security market share report. Last 3 years EDR/EPP reports need to be considered for any one or more industry analyst | *No change* |
| 94 | 29 | 2 | ELIGIBILITY CRITERIA | 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 | If we can provide Provisional Financial Report for 2023-24 | *No Provisional Financial Report is allowed to be su* |
| 95 | 29 | 6 | ELIGIBILITY CRITERIA | ISO 27001:2013 certified | Can we provide ISO 27001:2022 certified | *<u>Modified as:</u>*<br>*The bidder must have minimum ISO 27001:2013 certification or higher. ISO Certification has to be submitted by the bidder.* |
| 96 | 29 | 10 | ELIGIBILITY CRITERIA | Bidder must have support office/center at Tier 1 cities in India - GST and address to be provided along with Contact Details | Bidder must have support office/center at Tier 1 cities in India - Support Location List to be provided along with Contact Details | *No Change* |
| 97 | 27 | - | NDA | Non-Disclosure Agreement | NDA Format not available in RFP | *Details can be provided to successful bidder* |
| 98 | 23 | - | SLA | Service Level Agreement | SLA Format not available in RFP | *SLA requirements are mentioned. There is no SLA format required to be published/mentioned* |
| 100 | 10 | 2 | a) Enhanced Endpoint Security | 2. Phase 2 Implementation: Deployment in StockHolding's Branch locations - Number of Counts. 1000 end points | Request for Clarification: Could you please confirm the server OS and version details? | *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* |
| 101 | 20 | 43 | Data Loss Prevention | Ability to create workflow for automation based on the triggered detections for alerting and response action like isolation the device, etc. | Request for Clarification: Could you please elaborate isolation the device, etc. what the use case ? | *Compromised system must send immediate alerts to a centralized monitoring location to ensure swift communication. Upon detection of a compromise, the affected system should be isolated from the network to prevent further infection and protect other systems.* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 102 | 20 | 38 | Data Loss Prevention | Solution should be able to provide visual data flow based on web origins,<br>Classifications, content patterns, Sensitivity Labels (Microsoft) | Request for Clarification: Could you please elaborate....Do you required the data classification functionality ? or Please share the usecase details. | *Visual data flow is a graphical representation of how data moves through a system, highlighting its origins, destinations, and transformations. By visualizing data flow, organizations can gain insights into data usage, identify potential security risks, and optimize data processes* |
| 103 | 21 | 45 | Data Loss Prevention | The solution should Provide “Cloud Storage Applications” group which<br>monitor sensitive content accessed by this cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud. | Request for Clarification: Could you please elaborate. or Please share the use case details. | *This comes under Data loss protection to prevent sensitive data. To establish a dedicated group responsible for monitoring and controlling the access and upload of sensitive content to cloud storage applications within an organization. there's a growing concern about the security of sensitive information stored in these applications. Accidental or intentional uploads of confidential data can lead to data breaches, compliance violations, and reputational damage.* |
| 104 | 27 | | Legal | Limitation of liability | We propose to modify the clause such that-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 the total value of contract or SOW ~~Rs. 1,00,00,000 (Rupees One Crore) or extent of the business loss/damage to Stockholding - whichever is lower.~~ | *No Change* |
| 105 | 27 | | Legal | Termination clause | We propose to add below provision as Termination for Default<br><br>In the event StockHolding materially breaches this Agreement or any statement of work, which breach is not cured within sixty (60) days after written notice specifying the breach is given to the StockHolding, the bidder may (i) terminate this Agreement or any portion thereof or the applicable statement of work by giving written notice to the Bank. | *No Change* |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| 106 |  |  | Legal | Addition of new clause | <u>We propose to add new clause</u> : During the term of the Contract and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s of the other Party or aid any third person to do so, without the specific written consent of the other Party. This provision shall however not apply to any solicitation conducted through general advertisement of employment opportunities through placement agencies, public advertisement or otherwise which do not specifically target such employees.<br>The above restriction also applies to each party's affiliates, agents, vendors, contractors, and any third parties with whom such party has a relationship (collectively, "Representatives"). Representatives are also prohibited from soliciting or inducing any employee, consultant, or independent contractor of other party to leave their employment or engagement with such other party. | *No Change* |
| 107 | 7 | Eligibility Criteria | Point 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. | The Bidder/OEM 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. or **The Bidder should have experience of 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.** | *No Change* |