Community Bank

• Trust • Security • Progress

Tender Document

[Open Tender]
[One Stage Two Envelope]

Supply and Installation of Next Generation Endpoint and Server Security Solution for Community Bank Bangladesh PLC.

Invitation for Tender No: CBBL/HO/ICT/18-2025/607
Dated: 07th December 2025
Tender issued on: 07th December 2025

COMMUNITY BANK BANGLADESH PLC. ICT DIVISION, HEAD OFFICE

Community Bank

• Trust • Security • Progress

Tender Document

[Open Tender]
[One Stage Two Envelope]

Supply and Installation of Next Generation Endpoint and Server Security Solution for Community Bank Bangladesh PLC.

Invitation for Tender No: CBBL/HO/ICT/18-2025/607
Dated: 07th December 2025
Tender issued on: 07th December 2025

Invitation for Tender Offer

BID SCHEDULE
For

Project Sl.	Project Description
01	Supply and Installation of Next Generation Endpoint and Server Security Solution for Community Bank Bangladesh PLC.

INVITATION TO BID

Community Bank Bangladesh PLC is planning to Renew Update Endpoint and Server Security solution in line with the current requirement of building a shield against sophisticated cyber-attacks proactively. Intending to implement the plan, this document describes the scope, requirements, and related components in detail.

The last date for submission of Tender is **17th December, 2025**. Sealed Quotation Envelope (Technical & Financial in separate envelopes) shall be addressed to "The CITO, Community Bank Bangladesh PLC., Police Plaza Concord (Level 12(GSD), Tower 2), Gulshan 1, Dhaka-1212.", by 04:00 PM.

Also note that technical proposal will be evaluated after completing initial scrutiny of the required documents submitted along with the proposal. Financial proposal of the technically eligible bidders only, will be opened.

CBBL reserves the right to change the dates mentioned in the tender at any time, if required.

EXECUTIVE SUMMARY

Community Bank Bangladesh PLC. (CBBL), a concern of Bangladesh Police Kallyan Trust, is established with a vision to serve communities to progress with the tailor-made secured solutions abiding by the highest level of Corporate Governance and Trust.

It aims to contribute in the economic growth of the country by providing financial products and services to the communities across geographies. State-of-the-art Core Banking System will enable the operation to manage centrally in optimum magnitude.

Community Bank runs on its three core building blocks i.e. Trust, Security and Progress.

EXECUTIVE SUMMARY

Community Bank Bangladesh PLC. (CBBL), a concern of Bangladesh Police Kallyan Trust, is established with a vision to serve communities to progress with the tailor-made secured solutions abiding by the highest level of Corporate Governance and Trust.

It aims to contribute in the economic growth of the country by providing financial products and services to the communities across geographies. State-of-the-art Core Banking System will enable the operation to manage centrally in optimum magnitude.

Community Bank runs on its three core building blocks i.e. Trust, Security and Progress.

SCOPE OF WORK

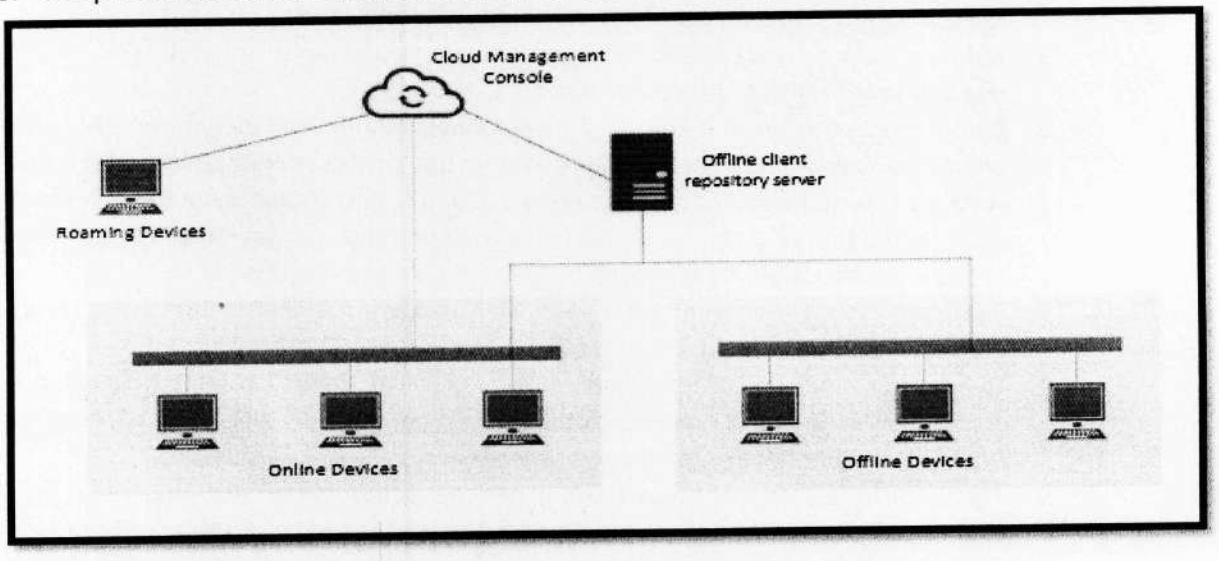
The project Work mentioned below is to be performed as per the specifications and conditions mentioned in the different parts of this document. The broad items of minimum specified work are as under Follows:

1. The proposed solution should have inbuilt next-generation signature-less, behavior-based Endpoint and Server Security technology to provide zero-day malware protection including anti-malware, anti-ransomware, and zero-day malware cleaner to protect the users from advanced malware, Ransomware, APT & advanced threats and that should be managed from a central enterprise management console.
2. The implementation Scope of the proposed solution should be considered all workstations across the Head Office as well as branches and sub-branches.
3. The solution should comply with all statutory and other legal requirements in terms of installation, integration, running, operation and maintenance of the System as specified in the RFP.
4. In case of any problem is due to software, the Supplier will diagnose the problem and propose appropriate measures to solve it.
5. To prepare and submit a technical hands-on guide of real-time work plan and documentation.
6. Operations, Maintenance and Support Services for the contract period.
7. Bidders are required to include in their proposals any integral components or features unintentionally not mentioned in this tender but deemed essential and critical to be included as part of the solution for successful implementation of the project separately as optional items with details description/explanation.

Technical and Solution requirement Specifications

The purpose of this RFP is to inform potential Bidders of a business opportunity and to solicit proposals as per the requirements of Community Bank.

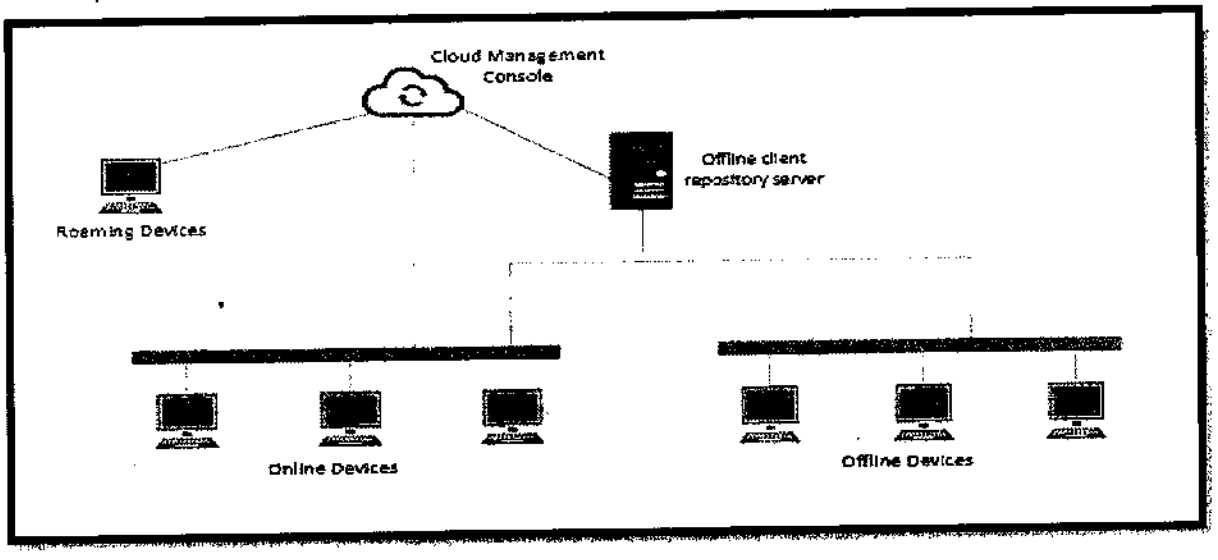
1. Community Bank branches are spread all over the country, with a centrally located Head Office in Dhaka. This document lays specifications concerning the proposed endpoint solutions for servers and workstations separately intending to enhance the protection of Enterprise IT infrastructure and to reduce downtime in rendering its IT-based Business Services.
2. The RFP specifies indicative requirements of the Endpoint and Server Security solution; detailed functional specifications of the solution needs for the project. This project will enable Bank to take proactive measures regarding protecting its endpoint devices such as servers and workstations against all kinds of cyber-attacks like malware, exploits, ransomware and zero-day attacks etc.
3. The preferable basic Architecture for online and offline endpoints is shown below:



Technical and Solution requirement Specifications

The purpose of this RFP is to inform potential Bidders of a business opportunity and to solicit proposals as per the requirements of Community Bank.

1. Community Bank branches are spread all over the country, with a centrally located Head Office in Dhaka. This document lays specifications concerning the proposed endpoint solutions for servers and workstations separately intending to enhance the protection of Enterprise IT infrastructure and to reduce downtime in rendering its IT-based Business Services.
2. The RFP specifies indicative requirements of the Endpoint and Server Security solution; detailed functional specifications of the solution needs for the project. This project will enable Bank to take proactive measures regarding protecting its endpoint devices such as servers and workstations against all kinds of cyber-attacks like malware, exploits, ransomware and zero-day attacks etc.
3. The preferable basic Architecture for online and offline endpoints is shown below:



Bidder's Qualification

Bidders must response the following points as the required Organizational Eligibility Criteria according to the formats. Modification/addition of the following format by the bidder will not be accepted. Moreover, bidders must submit evidence for the relevant documents as per their response.

1. This invitation for RFP is open to eligible bidders from Local Company Only.
2. **Mandatory Qualification:** The bidder must have successfully completed at least two endpoint deployment projects, within the banking sector. Failure to meet this requirement will result in disqualification.
3. The Bidder shall provide evidence that it is a current legal entity.
4. The Bidder/System Integrator must be the authorized representative /partner of the OEM. **The proof in support of the same must be enclosed.**
5. Bidders must demonstrate prior experience in successfully completing at **least two deployment projects** of the same product.
6. Bidder must warrant that key project personnel, should have minimum OEM certified engineers / equivalent certification / knowledge on Technology related to Endpoint security Solution and Endpoint Security Software, and should have been sufficiently involved in similar past installation. The bidder must submit details profile of the resources who would be deployed on-ground for this engagement
7. Bidders are required to submit a **valid Manufacturing Authorization** Form from the **original equipment manufacturer (OEM)** as part of their proposal.
8. The Bidder shall provide references in respect of major projects of similar type completed in the **last Five (5) number** of Experience by the bidder in any large organization and having its offices/branches across Bangladesh.
9. The Bidder must warrant that there is no legal action being taken against it for any cause in any legal jurisdiction. If such an action exists and the Bidder considers that it does not affect its ability to deliver the RFP requirements, it shall provide details of the action(s).
10. The cost of bidding and submission of tender documents is entirely the responsibility of bidders, regardless of the conduct or outcome of the tendering process.

Instructions to the Bidders

1. Bidders are expected to examine the attached specifications and all instructions contained in this Request for Proposal. Failure to do so will be at the Bidder's risk.
2. Bidders should submit the followings papers in order:
    a. **Vendor Profile**
        - Valid Trade license
        - Certificate of Incorporation (if applicable)
        - VAT, TAX, TIN certificate
        - Manufacturers Authorization Letter
    b. **Technical Proposal**
        - Response to the Attached Specifications duly signed by an authorized person.
        - Supported documents and Datasheets
    c. **Relevant Documents**
        - 5 (Five) years' experience certificate
        - Implementation and Rollout Plan
        - Tender Signatory Authority Document attested by the company
        - List of certified technical expertise for the quoted solution.
    d. **Financial Proposal**

    The financial proposal must be as per provided format:
        - Price should be quoted considering 03 Years
        - Price should be quoted in BDT including VAT, TAX/AIT and related charges if required as per Bangladesh Government rules.
3. All Documents mentioned in the checklist must be submitted.
4. All correspondence in connection with the proposal and the purchase order is to be in English.

Bid Security

Bid Security of Taka 50,000.00 (Taka Fifty Thousand) for the participated project in the form of Payment Order in favor of Community Bank Bangladesh PLC. The bid security should be valid for 3 (Three) months after the date of bid opening and must be submitted inside the financial proposal.

Training

A Comprehensive training shall be the key to successful Operations and Maintenance; hence, the Bidder is required to provide required training to COMMUNITY BANK BANGLADESH PLC. nominated Officials at COMMUNITY BANK BANGLADESH PLC. The successful Bidder is free to propose the training plan. **No separate charges will be paid for training.**

Instructions to the Bidders

1. Bidders are expected to examine the attached specifications and all instructions contained in this Request for Proposal. Failure to do so will be at the Bidder's risk.
2. Bidders should submit the followings papers in order:
    a. **Vendor Profile**
        - Valid Trade license
        - Certificate of Incorporation (if applicable)
        - VAT, TAX, TIN certificate
        - Manufacturers Authorization Letter
    b. **Technical Proposal**
        - Response to the Attached Specifications duly signed by an authorized person.
        - Supported documents and Datasheets
    c. **Relevant Documents**
        - 5 (Five) years' experience certificate
        - Implementation and Rollout Plan
        - Tender Signatory Authority Document attested by the company
        - List of certified technical expertise for the quoted solution.
    d. **Financial Proposal**

    The financial proposal must be as per provided format:
        - Price should be quoted considering 03 Years
        - Price should be quoted in BDT including VAT, TAX/AIT and related charges if required as per Bangladesh Government rules.
3. All Documents mentioned in the checklist must be submitted.
4. All correspondence in connection with the proposal and the purchase order is to be in English.

Bid Security

Bid Security of Taka 50,000.00 (Taka Fifty Thousand) for the participated project in the form of Payment Order in favor of Community Bank Bangladesh PLC. The bid security should be valid for 3 (Three) months after the date of bid opening and must be submitted inside the financial proposal.

Training

A Comprehensive training shall be the key to successful Operations and Maintenance; hence, the Bidder is required to provide required training to COMMUNITY BANK BANGLADESH PLC. nominated Officials at COMMUNITY BANK BANGLADESH PLC. The successful Bidder is free to propose the training plan. **No separate charges will be paid for training.**

TERMS & CONDITIONS

1. This invitation for Tenders is open to eligible tenderers from only locally registered companies.
2. The bidder shall not be under a declaration of ineligibility for corrupt, fraudulent, collusive or coercive practices.
3. The bidder with a consistent history of litigation or a number of arbitration awards against it, shall not be eligible to tender.
4. The bidder shall have the legal capacity to enter into the contract.
5. The bidder shall not be insolvent, bankrupt or being wound up, its business activities shall not be suspended, and it shall not be the subject of proceedings for any of the foregoing.
6. The bidder shall have fulfilled its obligations to pay taxes under the relevant national laws and regulations.
7. The bidder shall process the necessary professional and technical qualifications and competence, financial resources, including after-sales service, specific product experience, and reputation.
8. The bidder shall ensure compliance with global financial regulations, and Bangladesh Bank guidelines and polices.
9. Considering experience, quality, and other relevant factors, CBBL is not liable to select the lowest bidder, or any single bidder.
10. Must provide a detailed profile of the resources who will be engaged during the project;
11. All Price(s) should be in BDT including all VAT and TAX.
12. Financial offer(s) should be valid for Minimum (06) Six months .
13. The bank will carry out a detailed evaluation of the quotation according to the information supplied by the bidder through its proposal.
14. Bank reserves the right to accept or reject any or all quotation at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for the Bank's action.
15. Any bid not accompanied by an acceptable bid security shall be rejected as non-responsive even if that bid is found technically responsive during technical evaluation.
16. The bid security of unsuccessful bidders will be returned after selection of the successful bidder. The bid security of the successful bidder will be returned when the bidder has signed the agreement and furnished the required performance security.
17. The bid security may be forfeited if (a) the bidder withdraws its bid during the period of bid validity specified in the bid form; (b) if a successful bidder fails to sign the contract and (c) if a successful bidder fails to furnish the performance security.

18. Only technically qualified bidder will be eligible for opening financial proposal.
19. CBBL reserves the sole discretion, without obligation, to update, amend or supplement the information in this RFP.
20. The successful bidder must adhere to and comply with CBBL's ICT Security policies and standards.
21. After the receipt of award from the Bank, Security of 10% (ten percentage) of project value in the form of Pay Order or Bank Guarantee (BG) for 01 (one) year, or till project completion, whichever comes later, should be submitted.
22. The RFP document is not a recommendation, offer or invitation to enter a contract, agreement, or other arrangement in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between the Bank and any successful Bidder.

18. Only technically qualified bidder will be eligible for opening financial proposal.
19. CBBL reserves the sole discretion, without obligation, to update, amend or supplement the information in this RFP.
20. The successful bidder must adhere to and comply with CBBL's ICT Security policies and standards.
21. After the receipt of award from the Bank, Security of 10% (ten percentage) of project value in the form of Pay Order or Bank Guarantee (BG) for 01 (one) year, or till project completion, whichever comes later, should be submitted.
22. The RFP document is not a recommendation, offer or invitation to enter a contract, agreement, or other arrangement in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between the Bank and any successful Bidder.

Reserve Right

The Bank reserves the right to:

- Reject any and all responses received in response to the RFP, with or without assigning any reasons whatsoever.
- Waive or change any formalities, irregularities, or inconsistencies in proposal format delivery.
- Negotiate any aspect of the proposal with any Bidder and negotiate with more than one Bidder at a time.
- Extend the time for submission of all proposals.
- Select the most responsive Bidders (in case no Bidder satisfies the eligibility criteria in totality).
- Select the next most responsive Bidder if negotiations with the Bidder of choice fail to result in an agreement within a specified time frame.
- Share the information/ clarifications provided in response to RFP by any Bidder, with any other Bidder(s) /others, in any form.
- Cancel the RFP/Tender at any stage without assigning any reason whatsoever.

Confidentiality/Non-Disclosure

- The information contained in this RFP (or accumulated through other written, electronic or verbal communication) is proprietary to CBBL and must be treated by Bidder as CONFIDENTIAL. The information is to be used by each Bidder only for the purpose of preparing a response to this RFP. The information in this document may not be used or shared with other parties for any other purpose without CBBL's written permission.
- CBBL reserves the right to use information submitted in response to this document in any manner it may deem appropriate. Documents submitted may be reviewed and evaluated by any CBBL personnel. Bidder may request confidential treatment of any portion of its response but must clearly indicate what portion of the document is to be considered. CBBL will review such requests and grant such requests at its sole discretion. In the event that confidentiality cannot be granted, the Bidder will be permitted to withdraw its proposal.
- Except as required by law, any copies or versions of this Confidential Information that may be in the Bidder's possession, whether on paper or contained in computer systems, shall be returned to, or deleted, destroyed, or otherwise eliminated upon request or completion of the Services.

References

Before awarding any contract, CBBL reserves the right to require the Bidder to submit evidence of qualifications that it deems appropriate. This evidence may pertain to financial, technical, and other qualifications, as well as the Bidder's relevant experience and skills.

Negotiations

CBBL reserves the right to enter into financial negotiation with the Bidder/s as an outcome of internal evaluation criteria. Each Bidder acknowledges and agrees that CBBL will have no liability or obligation to any Bidder, except to the party, if any, awarded a contract by CBBL in its sole discretion, and CBBL shall be fully and forever released and discharged of all liability and obligation in connection with this RFP.

Bidder Responsibility

It is the Bidder's responsibility to ensure its complete understanding of the requirements and instructions specified by CBBL. In the event that clarification is required, Bidder should submit written inquiries

Inspection and Right to Audit

Due to regulatory requirement, the Bidder shall allow the authorized personnel of CBBL and/or its regulators the opportunity of inspecting and auditing Bidder's operations and the business records, which are directly relevant to the Services, provided by the Bidder.

Penalty

If the selected bidder fails to deliver the project according to the scope of work within the specified timeframe, a penalty of 5% of the work order value will be imposed. However, this penalty may be waived upon receiving a satisfactory explanation from the selected bidder.

Indemnity

The Bidder shall indemnify and hold harmless CBBL from and against any third-party Claims arising out of the infringement of any third party's intellectual property rights caused by CBBL's use of the Bidder's deliverables provided that this indemnity shall not apply to the following cases:

- The modification of the Bidder's deliverables provided hereunder by any person other than the Bidder or its personnel.
- CBBL's failure to use any modification to the Bidder's deliverables made available by the Bidder where the use of such modification would have avoided the infringement;
- Information, materials instructions or specifications that are themselves infringing which are provided by or on behalf of CBBL or which CBBL requests or requires the Bidder to use; or the use of the Bidder's deliverables in a manner not agreed to hereunder;
- Provided that CBBL gives the Bidder written notice of any such claim and sole control over the defense of any such claim.

Negotiations

CBBL reserves the right to enter into financial negotiation with the Bidder/s as an outcome of internal evaluation criteria. Each Bidder acknowledges and agrees that CBBL will have no liability or obligation to any Bidder, except to the party, if any, awarded a contract by CBBL in its sole discretion, and CBBL shall be fully and forever released and discharged of all liability and obligation in connection with this RFP.

Bidder Responsibility

It is the Bidder's responsibility to ensure its complete understanding of the requirements and instructions specified by CBBL. In the event that clarification is required, Bidder should submit written inquiries

Inspection and Right to Audit

Due to regulatory requirement, the Bidder shall allow the authorized personnel of CBBL and/or its regulators the opportunity of inspecting and auditing Bidder's operations and the business records, which are directly relevant to the Services, provided by the Bidder.

Penalty

If the selected bidder fails to deliver the project according to the scope of work within the specified timeframe, a penalty of 5% of the work order value will be imposed. However, this penalty may be waived upon receiving a satisfactory explanation from the selected bidder.

Indemnity

The Bidder shall indemnify and hold harmless CBBL from and against any third-party Claims arising out of the infringement of any third party's intellectual property rights caused by CBBL's use of the Bidder's deliverables provided that this indemnity shall not apply to the following cases:

- The modification of the Bidder's deliverables provided hereunder by any person other than the Bidder or its personnel.
- CBBL's failure to use any modification to the Bidder's deliverables made available by the Bidder where the use of such modification would have avoided the infringement;
- Information, materials instructions or specifications that are themselves infringing which are provided by or on behalf of CBBL or which CBBL requests or requires the Bidder to use; or the use of the Bidder's deliverables in a manner not agreed to hereunder;
- Provided that CBBL gives the Bidder written notice of any such claim and sole control over the defense of any such claim.

Publicity

Any publicity by the bidder in which the name of CBBL is to be used should be done only with the permission of CBBL.

Privacy and Security Safeguards

The successful Bidder shall disclose in any manner, without the CBBL's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any Bank location. The successful Bidder shall ensure that all subcontractors who are involved in the assessment process shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any Bank location.

Ownership of Deliverables

All the deliverables as per scope of this RFP will become the property of Community Bank Bangladesh PLC (CBBL).

List of Annexures

Sn#	Formats	Description
2	Annexure – I	Technical Specification for Endpoint security Solution
3	Annexure – II	Commercial Bid of Endpoint security Solution Software Solution for 3 Years
4	Annexure – III	Manufacturer's Authorization Form (MAF)

Annexure I

Technical Specifications for NextGen Endpoint and Server Security Solution

1. **Specification for Endpoint Protection for USERS**

Features	Technical Specifications	Bidder Responses
Product	Next Generation Endpoint Protection	
Solution details	Solution should include signature-less deep learning malware detection, exploit prevention, anti-ransomware technology, application white listing and stop zero-day attacks, exploits, ransomware and hackers	
Qty/Users	500 Users	
Brand	To be mentioned by the bidder	
Product with version	To be mentioned by the bidder	
Country of Origin	USA/UK	
Country of Manufacture	USA/UK/EU	
Part No/SKU	Bidder should submit BOQ of proposed solution that should be managed from a single web-based enterprise console.	
Operating System support	Solution should support to be installed on Windows, Mac as per requirement and below mentioned features	
Quality/Certifications	The OEM vendor must be a Leader in the 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for minimum last 12 consecutive reports.	
	Proposed solution should be named a Leader across the G2 Spring 2025 Overall Grid® Reports for Endpoint Protection Suites, EDR, XDR and MDR with last 3 consecutive reports.	
	Proposed solution must be a Leader in the 2024 IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses.	
	Must have a minimum rating of 4.6 out of 5 in Gartner peer review and must be a Gartner® Peer Insights™ "Customers' Choice" vendor in the 2025 Voice of the Customer report for Endpoint Protection Platforms.	
Main Requirements	The proposed solution should be user-based licensing only.	
	The proposed solution should have integrated next generation signature-less endpoint protection technology to provide zero-day malware protection including anti-exploits, anti-ransomware, and zero-day malware cleaner to protect the users from advanced malware, Ransomware, APT, advanced threats, and all these should be managed from same centralized enterprise management console.	
	The proposed solution should have web-based centralized Enterprise Console to manage all endpoint features mentioned below for windows desktop/laptops, etc.	
	The proposed solution should support integration with Active directory for directory structure of computers & users for better management	
	Should have advanced Exploit Prevention to mitigate the methods attackers use to exploit software vulnerabilities	

Annexure I

Technical Specifications for NextGen Endpoint and Server Security Solution

1. **Specification for Endpoint Protection for USERS**

Features	Technical Specifications	Bidder Responses
Product	Next Generation Endpoint Protection	
Solution details	Solution should include signature-less deep learning malware detection, exploit prevention, anti-ransomware technology, application white listing and stop zero-day attacks, exploits, ransomware and hackers	
Qty/Users	500 Users	
Brand	To be mentioned by the bidder	
Product with version	To be mentioned by the bidder	
Country of Origin	USA/UK	
Country of Manufacture	USA/UK/EU	
Part No/SKU	Bidder should submit BOQ of proposed solution that should be managed from a single web-based enterprise console.	
Operating System support	Solution should support to be installed on Windows, Mac as per requirement and below mentioned features	
Quality/Certifications	The OEM vendor must be a Leader in the 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for minimum last 12 consecutive reports.	
	Proposed solution should be named a Leader across the G2 Spring 2025 Overall Grid® Reports for Endpoint Protection Suites, EDR, XDR and MDR with last 3 consecutive reports.	
	Proposed solution must be a Leader in the 2024 IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses.	
	Must have a minimum rating of 4.6 out of 5 in Gartner peer review and must be a Gartner® Peer Insights™ "Customers' Choice" vendor in the 2025 Voice of the Customer report for Endpoint Protection Platforms.	
Main Requirements	The proposed solution should be user-based licensing only.	
	The proposed solution should have integrated next generation signature-less endpoint protection technology to provide zero-day malware protection including anti-exploits, anti-ransomware, and zero-day malware cleaner to protect the users from advanced malware, Ransomware, APT, advanced threats, and all these should be managed from same centralized enterprise management console.	
	The proposed solution should have web-based centralized Enterprise Console to manage all endpoint features mentioned below for windows desktop/laptops, etc.	
	The proposed solution should support integration with Active directory for directory structure of computers & users for better management	
	Should have advanced Exploit Prevention to mitigate the methods attackers use to exploit software vulnerabilities	

	Should have integrated protection technology with real-time threat intelligence to prevent, detect and remediate all types of advanced threats, such as targeted attacks, malicious URLs, web exploit code, unexpected system changes via command-and-control traffic	
	Should have integrated options to stop crypto-ransomware and automatically rolls any impacted files back	
	Should have Forensic-level system clean-up	
	Must provide a remote access to the end devices in order to perform a further investigation or take appropriate action.	
Application Control	Administrator should be able to add files, folders or extensions to an exclude list so that they are not scanned on access	
	Should enable automatic submissions of unknown/suspected virus samples to vendor and automatic response/delivery of the cure	
	Administrator should be able to lock down all anti-virus configurations at the desktop & User should be prevented from being able to uninstall the anti-virus software	
	Administrator must be able to distribute new and update anti-virus software, virus definitions and policies automatically to clients and servers from a central location	
	Administrator should be able to initiate virus sweeps remotely in case of an outbreak	
	Solution must mitigate exploits in vulnerable applications:	
	a) Protect web browsers	
	b) Protect web browser plugins	
	c) Protect Java applications	
	d) Protect media applications	
	e) Protect office applications	
	Solution should provide centralized event logging to locate and cure virus problems.	
	Solution should have Application Control module with the ability to block or be alerted to the use of a long list of Unauthorised applications (e.g. File Sharing, Games, etc.)	
	Solution should protect processes by -	
	a) Preventing process hollowing attacks	
	b) Preventing DLLs loading from untrusted folders	
Device control	Solution must offer device control solution with MTP/PTP category that includes devices such as phones, tablets, cameras and media players that connect using the MTP or PTP protocols.	
	Solution should have integrated Device Control module with a feature to set devices to 'Read Only', 'Add Exceptions' and 'Block' to black listing and whitelisting of the devices.	
	Below permission should be applicable:	
	Allow: Peripherals are not restricted in any way.	
	Block: Peripherals are not allowed at all.	
Data Loss Prevention	Solution should offer Data Loss Prevention (DLP) to restrict unauthorized data flow using prebuilt or custom rules.	
	Must be able to monitor and restrict the transfer of files containing sensitive data.	

	Must have the capability to create custom DLP policies or policies from templates.	
	Must have DLP policy templates that cover standard data protection for different regions.	
	Solution should have Data control that enables you to monitor and control the transfer of files from computers to storage devices and applications connected to the internet.	
	Solution should support Data Protection Policy to monitor data copied or shared through external mediums and internet browsers.	
Web Protection	Solution must support Malicious Traffic Detection to monitor non-browser-based traffic for any Command & Control (C&C) Servers connection.	
	Solution should have a Live Web Protection module integrated into existing endpoint agent with no endpoint configuration required to blocks URLs that are hosting malware and should support all major browsers	
	Vendor should have Threat Analysis Centres to provide proactive rapid protection against known and unknown threats.	
	Solution should have decision caching technology for scanning modes.	
	Solution should have genotype technology.	
	Solution should have the feature in which user activity is logged and viewable directly within management Console, allowing administrators to audit and identify undesirable behaviour	
	Solution should prevent users from compromising browsing policies	
	Solution should have Web Filtering on category basis with at least 14 categories	
	Should have capabilities to publish updates through HTTP and report remote machines through internet	
	Solution Web Filtering should allow to configure the policy to Allow, Warn, Block	
	Solution should have the customization to allow or block certain websites as required by administrator	
Live protection	Solution should provide Live Protection to check the latest threat information from OEM Labs online, automatically submit malware samples to OEM Labs, Live Protection during scheduled scans, Collect reputation data during on-demand scans	
	Should have tamper protection - a local administrator cannot make any of the following changes on their computer unless they have the necessary password:	
	- Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Live Protection.	
	- Disable tamper protection.	
	- Uninstall the endpoint agent software from user machine.	
	Solution should offer the tamper protection with the option of generating OTP	
Zero-day protection	The antivirus solution should provide enhanced antivirus protection for desktops, laptops of all the attacks originating from places inside/outside of the network due to virus and/or other malicious programming code	

	Must have the capability to create custom DLP policies or policies from templates.	
	Must have DLP policy templates that cover standard data protection for different regions.	
	Solution should have Data control that enables you to monitor and control the transfer of files from computers to storage devices and applications connected to the internet.	
	Solution should support Data Protection Policy to monitor data copied or shared through external mediums and internet browsers.	
Web Protection	Solution must support Malicious Traffic Detection to monitor non-browser-based traffic for any Command & Control (C&C) Servers connection.	
	Solution should have a Live Web Protection module integrated into existing endpoint agent with no endpoint configuration required to blocks URLs that are hosting malware and should support all major browsers	
	Vendor should have Threat Analysis Centres to provide proactive rapid protection against known and unknown threats.	
	Solution should have decision caching technology for scanning modes.	
	Solution should have genotype technology.	
	Solution should have the feature in which user activity is logged and viewable directly within management Console, allowing administrators to audit and identify undesirable behaviour	
	Solution should prevent users from compromising browsing policies	
	Solution should have Web Filtering on category basis with at least 14 categories	
	Should have capabilities to publish updates through HTTP and report remote machines through internet	
	Solution Web Filtering should allow to configure the policy to Allow, Warn, Block	
	Solution should have the customization to allow or block certain websites as required by administrator	
Live protection	Solution should provide Live Protection to check the latest threat information from OEM Labs online, automatically submit malware samples to OEM Labs, Live Protection during scheduled scans, Collect reputation data during on-demand scans	
	Should have tamper protection - a local administrator cannot make any of the following changes on their computer unless they have the necessary password:	
	- Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Live Protection.	
	- Disable tamper protection.	
	- Uninstall the endpoint agent software from user machine.	
	Solution should offer the tamper protection with the option of generating OTP	
Zero-day protection	The antivirus solution should provide enhanced antivirus protection for desktops, laptops of all the attacks originating from places inside/outside of the network due to virus and/or other malicious programming code	

	The solution should have single, Configurable Installation with centralized configuration & policy management	
	Solution should have genotype technology that should be able to detect malicious behaviour even before specific signature-based detection has been issued. This technology shall be available at endpoint, email & web security components of OEM	
	Solution should provide the centralized scanning of all network machines	
	Solution should be capable of pushing client installation from a web-based Admin console and it should also support manual installation of client	
	Administrator should have flexibility to schedule scan and update at the endpoints from central server	
	Solution should be able to capture Viruses, Trojans, Worms, Spyware and Malware, adware and PUA from single agent	
	Solution should provide the functionality of the Download Reputation that allows for a check to be performed against files as they are downloaded, to determine the reputation of the file	
	Solution should have Host Intrusion Prevention System (HIPS) technology which works in 4 Layers to provide zero-day protection without the need for updates (unknown virus detection & repair)	
	Solution should have run time detection technology i.e. behavioural & heuristic scanning to protect from unknown viruses and buffer overflow protection integrated with AV scan engine for protection from threats/ exploits that uses buffer overflow	
	Solution must have the capability to clean, quarantine or delete viruses and should be able to detect new classes of viruses by normal virus definition update mechanisms	
	Solution vendor should provide definitions with incremental updates. Should support daily update for definition files. Size of daily update should be below 30kb in size	
	Alerts on virus activity should be passed on to administrator	
	Should be able to manage preinstalled Windows firewall from same dashboard	
	Should be able to stop encryption attacks like CryptoLocker, CryptoWall, TorrentLocker, CTB-Locker, etc.	
	Should be able to stop mass encryption of documents and other files on local disks (including USB drives) and remote shares on network drives (SMB) even if it happens from an (abused) trusted legitimate process	
	Should make just-in-time copies of files in a safe file store (cache of files getting modified during perceived malicious activity) before they are changed on the disk	
	The cleaner should not only detect and remove malware, but also should be capable enough to remove traces left behind on the system, such as other files and registry keys	
	Should be able to enforce Data Execution Prevention (DEP) to prevents abuse of buffer overflows	
	Should have Mandatory Address Space Layout Randomization (ASLR) to prevents predictable code locations	
	Should support Bottom Up ASLR for improved code location randomization	

	Should have Null Page (Null Dereference Protection) to stop exploits that jump via page 0	
	Should support Heap Spray Allocation for pre-allocated common memory areas to block example attacks	
	Should have Dynamic Heap Spray to stop attacks that spray suspicious sequences on the heap	
	Should support Stack Pivot to stop abuse of the stack pointer	
	Should support Stack Exec (MemProt) to stop attacker' code on the stack	
	Should support Stack-based ROP Mitigations (Caller) to stop standard Return-Oriented Programming attacks	
	Should support Branch-based ROP Mitigations (Hardware Augmented) to stop advanced Return-Oriented Programming attacks	
	Should have Structured Exception Handler Overwrite Protection (SEHOP) to stop abuse of the exception handler	
	Should support Import Address Table Filtering (IAF) (Hardware Augmented) to stop attackers that lookup API addresses in the IAT	
	Should support Load Library to prevent loading of libraries from UNC paths	
	Should support Reflective DLL Injection to prevent loading of a library from memory into a host process	
	Should support VBScript God Mode to prevent abuse of VBScript in IE to execute malicious code	
	Should support WoW64 to stop attacks that address 64-bit function from WoW64 process	
	Should support Syscall to stop attackers that attempt to bypass security hooks	
	Should have Hollow Process to stop attacks that use legitimate processes to hide hostile code	
	Should give priority to system libraries for downloaded applications (DLL Hijacking)	
	Should have Application Lockdown to stop logic-flaw attacks that bypass mitigations	
	Should have Java Lockdown to prevent attacks that abuse Java to launch Windows executables	
	Should support Squiblydoo AppLocker Bypass to prevent regsvr32 from running remote scripts and code	
	Should have protection for CVE-2013-5331 & CVE-2014- 4113 via Metasploit for In-memory payloads: Meterpreter & Mimikatz	
	Should be able to add machine learning technology with deep leaning	
	Solution must have the feature to conserve bandwidth by blocking inappropriate browsing and warns users before visiting productivity-impacting websites. Blocks site categories likely to consume high bandwidth.	
	Proposed solution should show the alert description along with User & Device	
	Solution should offer pre-defined administration roles to divide up security tasks according to the administrators' responsibility level.	
	Solution should provide protection against:	

	Should have Null Page (Null Dereference Protection) to stop exploits that jump via page 0	
	Should support Heap Spray Allocation for pre-allocated common memory areas to block example attacks	
	Should have Dynamic Heap Spray to stop attacks that spray suspicious sequences on the heap	
	Should support Stack Pivot to stop abuse of the stack pointer	
	Should support Stack Exec (MemProt) to stop attacker' code on the stack	
	Should support Stack-based ROP Mitigations (Caller) to stop standard Return-Oriented Programming attacks	
	Should support Branch-based ROP Mitigations (Hardware Augmented) to stop advanced Return-Oriented Programming attacks	
	Should have Structured Exception Handler Overwrite Protection (SEHOP) to stop abuse of the exception handler	
	Should support Import Address Table Filtering (IAF) (Hardware Augmented) to stop attackers that lookup API addresses in the IAT	
	Should support Load Library to prevent loading of libraries from UNC paths	
	Should support Reflective DLL Injection to prevent loading of a library from memory into a host process	
	Should support VBScript God Mode to prevent abuse of VBScript in IE to execute malicious code	
	Should support WoW64 to stop attacks that address 64-bit function from WoW64 process	
	Should support Syscall to stop attackers that attempt to bypass security hooks	
	Should have Hollow Process to stop attacks that use legitimate processes to hide hostile code	
	Should give priority to system libraries for downloaded applications (DLL Hijacking)	
	Should have Application Lockdown to stop logic-flaw attacks that bypass mitigations	
	Should have Java Lockdown to prevent attacks that abuse Java to launch Windows executables	
	Should support Squiblydoo AppLocker Bypass to prevent regsvr32 from running remote scripts and code	
	Should have protection for CVE-2013-5331 & CVE-2014- 4113 via Metasploit for In-memory payloads: Meterpreter & Mimikatz	
	Should be able to add machine learning technology with deep leaning	
	Solution must have the feature to conserve bandwidth by blocking inappropriate browsing and warns users before visiting productivity-impacting websites. Blocks site categories likely to consume high bandwidth.	
	Proposed solution should show the alert description along with User & Device	
	Solution should offer pre-defined administration roles to divide up security tasks according to the administrators' responsibility level.	
	Solution should provide protection against:	

	* Ransomware attacks that target MBR.	
	* Destructive Boot records attacks.	
	* Boot kit installation.	
	Solution must support the active adversary mitigation techniques:	
	* Prevent Credential Theft Protection	
	* Prevent Code cave evacuation	
	* Prevent Privilege escalation	
	* Prevent APC violation	
	Solution must have Deep Learning technology with a model size of 10-20 MB	
	Should be able to stop mass encryption of documents and other files on local disks (including USB drives) and remote shares on network drives (SMB) even if it happens from an (abused) trusted legitimate process	
	Should be able to monitor files when they are accessed by a process (read/write)	
	Solution should support the time-based policies.	
	Solution must have the privilege to whitelist the USB device on the basis of Hardware ID.	
	Should enable automatic submissions of unknown/suspected virus samples to vendor and automatic response/delivery of the cure.	
	Should have Deep Learning Malware Analysis, Machine learning detection and prioritization of suspicious events	
	Should have the provision to integrate with Managed Detection Response (MDR) that should provide 24/7 threat hunting, detection, and response capabilities delivered by an expert team as a fully-managed service in the same single agent without any change on it.	
	Solution should have PUA scanning that will inform administrator which applications have been found. Should able to configure anti-virus policies to allow or remove applications on this list that should give full control over what is available to users, enabling administrators to retain or remove individual applications as required.	
Reporting	Solution should have the granular reporting and should include	
	a) Security Events (Shows all security events, such as malware detections, on your devices and let you filter them to generate reports)	
	b) Audit Logs (Record of all activities and changes made to the system.)	
	c) Policy Violators (Shows the users who tried to access blocked websites or download blocked files most often.)	
	d) Blocked Sites Access Record (Shows the blocked websites that users tried to visit most often and the users who tried to visit them.)	
	e) Application Control Policy Violators (Shows the servers/users that tried to access blocked applications most often and the application they tried to access.)	
	f) Warned Sites (Shows the top websites for which we display a warning and the users who most often ignore the warnings)	

	g) Blocked Applications (Shows the top blocked applications and the servers/users that tried to access them)	
	Should extend investigation capability to 30 days without bringing a device back online	
Installation/Implementation	Bidder should be experienced and capable to install, implement and commissioning the offered solution successfully by their own Certified Engineers	
Warranty and Support	Minimum 1 (One) / 3 (Three) years warranty from the date of successful commissioning.	
	24x7x365 Enhanced Support via telephone & email with remote access support by manufacturer directly	
	Free Security Updates, Patches, Software Features Updates & Upgrades	
	Solution must have the option to raise the Support ticket directly to the OEM from the management Console	

2. Specification for Endpoint Protection for SERVERS

Features	Technical Specifications	Bidder Responses
Product/Solution	Next Generation Server Protection	
Solution details	Solution should include signature-less deep learning malware detection, exploit prevention, anti-ransomware technology, application white listing and stop zero-day attacks, exploits, ransomware and hackers	
Qty	50 Servers	
Brand	To be mentioned by the bidder	
Product/Version	To be mentioned by the bidder	
Country of Origin	USA/UK	
Country of Manufacture	USA/UK/EU	
Part No/SKU	Bidder should submit BOQ of proposed solution that should be managed from a single web-based enterprise console.	
Quality/Certifications	The OEM vendor must be a Leader in the 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for minimum last 12 consecutive reports.	
	Proposed solution should be named a Leader across the G2 Spring 2025 Overall Grid® Reports for Endpoint Protection Suites, EDR, XDR and MDR with last 3 consecutive reports.	
	Proposed solution must be a Leader in the 2024 IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses.	
	Must have a minimum rating of 4.6 out of 5 in Gartner peer review and must be a Gartner® Peer Insights™ "Customers' Choice" vendor in the 2025 Voice of the Customer report for Endpoint Protection Platforms.	
Platform	Should support Windows Server, VM, Microsoft Azure, Amazon AWS	
MANDATORY TECHNICAL FEATURES:		
Attack Surface Reduction	Application Whitelisting (Server Lockdown)	
	Web Security	
	Download Reputation	
	Web Control/Category-based URL Blocking	
	Peripheral Control (e.g., USB)	

	g) Blocked Applications (Shows the top blocked applications and the servers/users that tried to access them)	
	Should extend investigation capability to 30 days without bringing a device back online	
Installation/Implementation	Bidder should be experienced and capable to install, implement and commissioning the offered solution successfully by their own Certified Engineers	
Warranty and Support	Minimum 1 (One) / 3 (Three) years warranty from the date of successful commissioning.	
	24x7x365 Enhanced Support via telephone & email with remote access support by manufacturer directly	
	Free Security Updates, Patches, Software Features Updates & Upgrades	
	Solution must have the option to raise the Support ticket directly to the OEM from the management Console	

2. Specification for Endpoint Protection for SERVERS

Features	Technical Specifications	Bidder Responses
Product/Solution	Next Generation Server Protection	
Solution details	Solution should include signature-less deep learning malware detection, exploit prevention, anti-ransomware technology, application white listing and stop zero-day attacks, exploits, ransomware and hackers	
Qty	50 Servers	
Brand	To be mentioned by the bidder	
Product/Version	To be mentioned by the bidder	
Country of Origin	USA/UK	
Country of Manufacture	USA/UK/EU	
Part No/SKU	Bidder should submit BOQ of proposed solution that should be managed from a single web-based enterprise console.	
Quality/Certifications	The OEM vendor must be a Leader in the 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for minimum last 12 consecutive reports.	
	Proposed solution should be named a Leader across the G2 Spring 2025 Overall Grid® Reports for Endpoint Protection Suites, EDR, XDR and MDR with last 3 consecutive reports.	
	Proposed solution must be a Leader in the 2024 IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses.	
	Must have a minimum rating of 4.6 out of 5 in Gartner peer review and must be a Gartner® Peer Insights™ "Customers' Choice" vendor in the 2025 Voice of the Customer report for Endpoint Protection Platforms.	
Platform	Should support Windows Server, VM, Microsoft Azure, Amazon AWS	
MANDATORY TECHNICAL FEATURES:		
Attack Surface Reduction	Application Whitelisting (Server Lockdown)	
	Web Security	
	Download Reputation	
	Web Control/Category-based URL Blocking	
	Peripheral Control (e.g., USB)	

	Application Control	
BEFORE IT RUNS ON DEVICE	Deep Learning Malware Detection: - Deep Learning Malware Detection - Deep Learning Potentially Unwanted - Applications (PUA) Blocking - False Positive Suppression	
	Anti-Malware File Scanning	
	Live Protection	
	Pre-Execution Behaviour Analysis (HIPS)	
STOP RUNNING THREAT	Data Loss Prevention	
	Exploit Prevention: - Enforce Data Execution Prevention - Mandatory Address Space Layout Randomization - Bottom-up ASLR - Null Page (Null Deference Protection) - Heap Spray Allocation - Dynamic Heap Spray - Stack Pivot - Stack Exec (MemProt) - Stack-based ROP Mitigations (Caller) - Branch-based ROP Mitigations (Hardware Assisted) - Structured Exception Handler Overwrite (SEHOP)	
	Runtime Behavior Analysis (HIPS)	
	Malicious Traffic Detection (MTD)	
	Active Adversary Mitigations: - Credential Theft Protection - Code Cave Mitigation - Man-in-the-Browser Protection (Safe Browsing) - Malicious Traffic Detection - Meterpreter Shell Detection	
	Anti-Ransomware Protection: - Ransomware File Protection - Automatic File Recovery - Disk and Boot Record Protection - Man-in-the-Browser Protection	
	Enhanced Application Lockdown: - Web Browsers (including HTA) - Web Browser Plugins - Java - Media Applications - Office Applications	
REMEDIATION	Automated Malware Removal	
	Synchronized Security Heartbeat	
	Signatureless Malware Cleaner	
VISIBILITY	Cloud Workload Discovery and Protection (AWS EC2/S3, Azure)	
	Cloud Workload Protection (Google Cloud Platform)	
	AWS Map, Multi-region Visualization	
	Synchronized App Control	
CONTROL	Server-specific Policy Management	
	Update Cache and Message Relay	
	Automatic Scanning Exclusions	
	Synchronized Security Heartbeat	
Cloud Environment	Cloud Environment Monitoring: AWS, Azure, GCP, Kubernetes, IaC and Docker Hub registries	

	Security Monitoring (CSPM best practice rules)	
	AWS Native Service Integrations (Amazon GuardDuty, AWS Security Hub, Amazon Inspector etc.)	
	Azure Native Service Integrations (Azure Sentinel and Advisor)	
	AI-powered Anomaly Detection	
	Advanced Search Capabilities	
	Asset Inventory	
EXPLOIT PREVENTION	Enforce Data Execution Prevention	
	Mandatory Address Space Layout Randomization	
	Bottom-up ASLR	
	Null Page (Null Deference Protection)	
	Heap Spray Allocation	
	Dynamic Heap Spray	
	Stack Pivot	
	Stack Exec (MemProt)	
	Stack-based ROP Mitigations (Caller)	
	Branch-based ROP Mitigations (Hardware Assisted)	
	Structured Exception Handler Overwrite (SEHOP)	
	Import Address Table Filtering (IAF)	
	Load Library	
	Reflective DLL Injection	
	Shellcode	
	VBScript God Mode	
	Wow64	
	Syscall	
	Hollow Process	
	DLL Hijacking	
	Squiblydoo Applocker Bypass	
	APC Protection (Double Pulsar / AtomBombing)	
	Process Privilege Escalation	
ACTIVE ADVERSARY MITIGATION	Credential Theft Protection	
	Code Cave Mitigation	
	Man-in-the-Browser Protection (Safe Browsing)	
	Malicious Traffic Detection	
	Meterpreter Shell Detection	
ANTI-RANSOMWARE	Ransomware File Protection	
	Automatic File Recovery	
	Disk and Boot Record Protection	
APPLICATION LOACKDOWN	Web Browsers (including HTA)	
	Web Browser Plugins	
	Java	
	Media Applications	
	Office Applications	
Deep Learning (AI)	Should have Deep Learning Malware Analysis, Machine learning detection and prioritization of suspicious events	
Installation/Implementation	Bidder should be experienced and capable to install, implement and commissioning the offered solution successfully by their own Certified Engineers	
Warranty and Support	Minimum 3 (Three) years warranty from the date of successful commissioning.	
	24x7x365 Enhanced Support via telephone & email with remote access support by manufacturer directly	

	Security Monitoring (CSPM best practice rules)	
	AWS Native Service Integrations (Amazon GuardDuty, AWS Security Hub, Amazon Inspector etc.)	
	Azure Native Service Integrations (Azure Sentinel and Advisor)	
	AI-powered Anomaly Detection	
	Advanced Search Capabilities	
	Asset Inventory	
EXPLOIT PREVENTION	Enforce Data Execution Prevention	
	Mandatory Address Space Layout Randomization	
	Bottom-up ASLR	
	Null Page (Null Deference Protection)	
	Heap Spray Allocation	
	Dynamic Heap Spray	
	Stack Pivot	
	Stack Exec (MemProt)	
	Stack-based ROP Mitigations (Caller)	
	Branch-based ROP Mitigations (Hardware Assisted)	
	Structured Exception Handler Overwrite (SEHOP)	
	Import Address Table Filtering (IAF)	
	Load Library	
	Reflective DLL Injection	
	Shellcode	
	VBScript God Mode	
	Wow64	
	Syscall	
	Hollow Process	
	DLL Hijacking	
	Squiblydoo Applocker Bypass	
	APC Protection (Double Pulsar / AtomBombing)	
	Process Privilege Escalation	
ACTIVE ADVERSARY MITIGATION	Credential Theft Protection	
	Code Cave Mitigation	
	Man-in-the-Browser Protection (Safe Browsing)	
	Malicious Traffic Detection	
	Meterpreter Shell Detection	
ANTI-RANSOMWARE	Ransomware File Protection	
	Automatic File Recovery	
	Disk and Boot Record Protection	
APPLICATION LOACKDOWN	Web Browsers (including HTA)	
	Web Browser Plugins	
	Java	
	Media Applications	
	Office Applications	
Deep Learning (AI)	Should have Deep Learning Malware Analysis, Machine learning detection and prioritization of suspicious events	
Installation/Implementation	Bidder should be experienced and capable to install, implement and commissioning the offered solution successfully by their own Certified Engineers	
Warranty and Support	Minimum 3 (Three) years warranty from the date of successful commissioning.	
	24x7x365 Enhanced Support via telephone & email with remote access support by manufacturer directly	

	Solution must have the option to raise the Support ticket directly to the OEM from the management Console	
	Free Security Updates, Patches, Software Features Updates & Upgrades	

Annexure II

Commercial Bid
STANDARD FORMAT OF FINANCIAL PROPOSAL

Commercial Bid of Endpoint security Solution for 1 and 3 Years (Amount in BDT including VAT & TAX).

Sn#	Product Description	Order Quantity	Unit Price	Total Price
A	B	C	D	E
1	USER Protection	500		
2	SERVER Protection	50		
In word (Taka excluding VAT and TAX):			**Total**	
In word (Taka including VAT and TAX):			**Grand Total**	

*For one year Price

Sn#	Product Description	Order Quantity	Unit Price	Total Price
A	B	C	D	E
1	USER Protection	500		
2	SERVER Protection	50		
In word (Taka excluding VAT and TAX):			**Total**	
In word (Taka including VAT and TAX):			**Grand Total**	

*For three-year Price

Declaration:

- Price has been quoted against the responded specifications attached herein
- All price includes VAT and all applicable taxes as per Govt. Rules
- Delivery time will have to be mentioned & must meet the deadline.
- Testing, Commission, implement & live operation must be included.
- The price offer should be covered three years warranty.
- The Bank reserves the right to choose either a one (01)-year or three (03)-year license.

Signature of Bidder with Seal and Date:

_____

Annexure II

Commercial Bid
STANDARD FORMAT OF FINANCIAL PROPOSAL

Commercial Bid of Endpoint security Solution for 1 and 3 Years (Amount in BDT including VAT & TAX).

Sn#	Product Description	Order Quantity	Unit Price	Total Price
A	B	C	D	E
1	USER Protection	500		
2	SERVER Protection	50		
In word (Taka excluding VAT and TAX):			**Total**	
In word (Taka including VAT and TAX):			**Grand Total**	

*For one year Price

Sn#	Product Description	Order Quantity	Unit Price	Total Price
A	B	C	D	E
1	USER Protection	500		
2	SERVER Protection	50		
In word (Taka excluding VAT and TAX):			**Total**	
In word (Taka including VAT and TAX):			**Grand Total**	

*For three-year Price

Declaration:

- Price has been quoted against the responded specifications attached herein
- All price includes VAT and all applicable taxes as per Govt. Rules
- Delivery time will have to be mentioned & must meet the deadline.
- Testing, Commission, implement & live operation must be included.
- The price offer should be covered three years warranty.
- The Bank reserves the right to choose either a one (01)-year or three (03)-year license.

Signature of Bidder with Seal and Date:

Annexure III

MANUFACTURER'S AUTHORISATION FORM (MAF)

To: *[Contact Person]* *[Name of the Procuring Entity]* *[Address of the Procuring Entity]*	Date:
Invitation for Tender No:	

We who are established and reputable providers of having offices at and do hereby authorize

M/s (Name and address of Agent /Dealer) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per the terms and conditions of the tender and the contract for the services offered against this invitation for tender offer by the above firm.

Yours faithfully,

(Name) for and on behalf of
(Name of Provider)

Note:

This is a draft. This letter of authority should be on the letterhead of the service provider concerned and should be signed by a competent authority of the service provider.