Community Bank

• Trust • Security • Progress

Procurement of Advanced Endpoint Protection Solution with EPP, EDR and XDR Capabilities

Tender Reference: CBBL/HO/ICTSC/01-2026/01
Issue Date: 12th November 2026.
Submission Deadline: 25th November 2026

Issued by
Community Bank Bangladesh PLC.
Head Office, Dhaka, Bangladesh

Community Bank Bangladesh PLC. ★ ICT Division ★

DOCUMENT CONTROL AND IMPORTANT INFORMATION

Item	Details
Procuring Entity	Community Bank Bangladesh PLC. (CBBL)
Tender Title	Advanced Endpoint Protection Solution with EPP, EDR and XDR Capabilities
Procurement Method	Open Tender – One-Stage, Two-Envelope
Approved Quantity	700 licenses in aggregate for **600 workstations** and **100 servers**
Licence Period	01 January 2027 to 31 December 2029 (three years)
Tender Reference	CBBL/HO/ICTSC/01-2026/01
Submission Address	Head of GSD, Community Bank Bangladesh PLC., Police Plaza Concord, Level 12 (GSD), Tower 2, Gulshan-1, Dhaka-1212

Important instructions to bidders

The tender planning quantity is 700 devices in aggregate: 600 workstations and 100 servers, as stated in the Tender Data Sheet. Bidders shall identify the applicable OEM SKUs, license metrics and any platform-specific differences, and shall provide EPP and EDR coverage for all 700 devices. Any proposed licensing allocation is subject to the Bank's written confirmation.

This tender is technology-neutral. Bidders must identify the exact OEM, product, edition, modules, SKUs, license metric, integrations, dependencies and any separately chargeable components.

Contents

1. Invitation to Tender
2. Background and Objectives
3. Scope of Work and Deliverables
4. Technical and Functional Requirements
5. Bidder Eligibility and Qualification
6. Instructions to Bidders
7. Evaluation and Award
8. Commercial Requirements
9. Contract Conditions and Information Security

Annexure I – Technical Compliance Matrix
Annexure II – Financial Proposal
Annexure III – Manufacturer's Authorization
Annexure IV – Bidder Declaration and Checklist

Community Bank Bangladesh PLC. ICT Division

1. INVITATION TO TENDER

Community Bank Bangladesh PLC. (CBBL), hereinafter referred to as "the Bank", invites sealed tenders from eligible and qualified bidders for the supply, implementation, commissioning, licensing, support and maintenance of an Advanced Endpoint Protection Solution with Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) capabilities for **700 workstations and servers** for three (03) years, from **01 January 2027 to 31 December 2029.**

The procurement shall be conducted through an ***Open Tender using a One-Stage, Two-Envelope procedure***. Bidders shall submit the Technical Proposal and Financial Proposal in separate sealed envelopes, enclosed in one outer envelope.

Tender Particulars	Details
Tender reference	CBBL/HO/ICTSC/01-2026/01
Issue date	12 November 2026
Clarification deadline	18 November 2026
Submission deadline	25 November 2026
Tender opening date	25 November 2026
Submission address	Head of GSD, Community Bank Bangladesh PLC., Police Plaza Concord, Level 12, Tower 2, Gulshan-1, Dhaka-1212
Bid validity	Minimum 180 days from the submission deadline, subject to final Tender Data Sheet

The Bank will first examine administrative and eligibility documents, followed by technical evaluation. Only the Financial Proposals of bidders found eligible and technically responsive will be opened.

2. BACKGROUND AND OBJECTIVES

The Bank has been using endpoint protection across its workstations and servers since January 2020. The existing arrangement covers 550 licenses and is due to expire on 31 December 2026. Under the previous arrangement, conventional endpoint protection was deployed across the endpoint environment, while advanced EDR coverage was limited to 50 servers.

The Bank intends to strengthen its endpoint security posture by procuring 700 licenses with EPP and EDR capabilities for all covered workstations and servers, supported by XDR capabilities for broader security-event correlation and investigation. The solution is intended to improve prevention, detection, investigation, containment and response to malware, ransomware, credential theft, fileless attacks, zero-day exploits and other advanced threats.

The procurement is aligned with *Bangladesh Bank ICT Security Guidelines (Version 4.0), Clause 5.10.4*, which requires endpoint devices connected to an organization's internal network to be protected by endpoint security protection and to run the latest virus definitions. EDR and XDR are additional security capabilities required by the Bank to enhance detection and response; this tender does not represent XDR as an explicit requirement of that clause.

2.1 Objectives

- Strengthen centrally managed endpoint protection across the Bank's workstation and server environment.
- Improve detection, investigation, containment and response capabilities across all covered devices.
- Provide XDR capability to correlate security telemetry across endpoints, servers and other supported, Bank-approved security sources.
- Enable coordinated threat hunting and incident handling through centralized security management.
- Improve **security visibility, reporting, auditability and operational efficiency**.
- Ensure **secure implementation**, knowledge transfer and OEM-backed support throughout the contract period.

3. SCOPE OF WORK AND DELIVERABLES

The successful bidder shall provide all licenses, subscriptions, software components and services necessary to implement, commission, operate and maintain the proposed solution throughout the contract period. This includes configuration, integration, documentation, training, technical support and maintenance. Where replacement of the existing solution is required, the bidder shall remove it and install the proposed solution only with the Bank's prior approval and in accordance with an approved change and rollback plan.

Community Bank Bangladesh PLC. ICT Division

3.1 Licensing and coverage

- Provide 700 licenses in aggregate: **600 workstation licenses and 100 server licenses**, for 01 January 2027 to 31 December 2029.
- Provide **EPP and EDR capabilities** for all **700 covered devices**. EDR coverage limited to only a subset of the 700 devices will not meet the requirement.
- Provide XDR capability and all required platform entitlements, connectors, APIs or modules. Disclose any dependency or additional license and include mandatory components in the financial proposal.
- Support the operating systems and endpoint/server platforms confirmed by the Bank before implementation; submit a compatibility matrix.
- Explain the license metric, device/user/workload rules, license pooling and reassignment, overage treatment and expiry arrangements.
- Provide a bill of quantities identifying workstation and server license categories, if separate SKUs are required, while maintaining the approved aggregate coverage of 700 devices.

3.2 Implementation and commissioning

- Conduct a kick-off meeting and validate the Bank's asset inventory, operating systems and deployment prerequisites.
- Submit an implementation plan covering milestone, deployment waves, roles, dependencies, change control and rollback arrangements.
- **Describe the proposed migration from the existing solution, including any required removal and replacement activities. Such activities shall be performed only with the Bank's prior approval and under an approved change and rollback plan; however, if the bidder proposes the same solution currently implemented in the Bank, submission of a separate migration or removal plan is not mandatory.**
- Configure the management console, security policies, roles, dashboards, alerting, reporting and approved integrations.
- Deploy agents to the 700 covered devices in coordination with the Bank's ICT teams, minimizing operational disruption.
- Configure EDR monitoring, investigation, threat hunting, isolation/containment and response workflows.
- Configure XDR data sources and integrations that are available and approved by the Bank; document all technical and licensing dependencies.
- Conduct functional and security testing, resolve deployment issues and obtain written acceptance from the Bank.
- Provide as-built documentation, configuration records, administrator guides and handover materials.

3.3 Deliverables

No.	Deliverable	Minimum expectation
1	Project plan	Milestones, roles, dependencies, risks and rollout schedule.
2	License schedule	OEM, product/edition, SKU, quantity, license metric and validity.
3	Deployment	700 devices covered by EPP and EDR; 100 devices XDR configured as agreed.
4	Integration record	Data sources, connectors, APIs, data flows and limitations.
5	Testing and acceptance report	Test cases, results, exceptions and remediation.
6	Documentation	Architecture, configuration, operating procedures and escalation matrix.
7	Training	Role-based training, attendance and materials.
8	Support reports	Support cases, SLA performance and periodic service reports.

4. TECHNICAL AND FUNCTIONAL REQUIREMENTS

Bidders shall respond to every requirement in Annexure I using "Comply", "Partially Comply" or "Do Not Comply". Responses shall identify the proposed product feature, module or equivalent capability and provide supporting documentation. Product-specific terminology is not required; equivalent methods that deliver the stated security outcome will be considered.

4.1 EPP – prevention and protection

- Real-time anti-malware protection using signature-based, heuristic, behavioural, machine-learning or equivalent techniques.
- Protection against malware, ransomware, potentially unwanted applications, malicious scripts, exploit attempts and known/unknown threats.
- Exploit prevention and protection against malicious process behaviour, credential theft and suspicious persistence techniques.
- Web, URL and malicious traffic protection where supported by the proposed product and license.

Community Bank Bangladesh PLC. ★ ICT Division ★

- Application control and policy-based control of removable storage and peripherals.
- Tamper protection, secure agent uninstall controls and centrally managed policy enforcement.
- Automatic security content, engine and agent updates with controlled scheduling and reporting.

4.2 EDR – detection and response

- Continuous endpoint activity monitoring and security telemetry collection for all 700 devices.
- Behaviour-based detection of suspicious activity, including fileless attacks, credential theft, lateral movement indicators, malicious scripts and ransomware behaviour.
- Endpoint timeline, process tree, event search, alert prioritization and investigation context.
- Remote investigation and response actions, including device isolation, process termination, file quarantine/remediation and collection of investigation data, subject to authorized controls.
- Threat hunting and historical search across retained telemetry; bidder shall state default and maximum searchable retention and related charges.
- Case management, incident notes, evidence export and audit trail for investigation and response actions.
- Ability to identify affected devices and related indicators of compromise across the covered environment.

4.3 XDR – extended detection and response

- Correlate relevant security events from endpoints and servers with other supported and Bank-approved security data sources through native connectors, APIs, syslog or documented methods.
- Support integration, where technically available and licensed, with network security devices, email security, identity services, cloud services and other security platforms used by the Bank.
- Provide a unified incident view linking related alerts, entities, users, devices, indicators and attack activities.
- Enable cross-source threat detection, incident prioritization, investigation and coordinated response workflows.
- Provide dashboards, correlation rules, alert enrichment and searchable event information.
- Identify included integrations, supported third-party products, connector limitations, ingestion limits and additional charges.
- Do not assume that the Bank will procure additional third-party products or services unless explicitly quoted and approved.

4.4 Central management, architecture and reporting

- Provide a centralized web-based management console with role-based access control and separation of administrative duties.
- Support multi-factor authentication for privileged console access and directory integration where supported.
- Maintain audit logs of administrator actions, policy changes, access, alerts and response actions.
- Use secure communications and current industry-standard encryption for agents, management components and cloud services.
- Support policy-based grouping and reporting for Head Office, branches, sub-branches, workstations and servers.
- Provide dashboards and exportable/scheduled reports for device coverage, agent health, threat events, incidents and license utilization.
- State hosting architecture, data residency, telemetry routing, data storage location, service dependencies and any cross-border data transfer.
- State CPU, memory, storage, bandwidth, proxy, firewall and network prerequisites; describe operation for intermittently connected devices.

4.5 Support and updates

- Provide timely threat intelligence, security content updates, patches, product updates and upgrades throughout the contract period.
- Provide OEM-backed technical support and escalation, including 24x7x365 contact for critical security incidents; state response targets and escalation levels.
- Provide access to the OEM support portal and a facility to raise and track support cases.
- Provide security advisories relevant to the proposed product and guidance for mitigation.

5. BIDDER ELIGIBILITY AND QUALIFICATION

1. The bidder must be a legally registered entity in Bangladesh and hold valid Trade License, TIN and VAT/BIN registration and other applicable statutory documents.

Community Bank Bangladesh PLC ★ ICT Division ★

2. The bidder must be the OEM or an OEM-authorized partner/reseller/system integrator for the proposed solution and submit a valid Manufacturer's Authorization Form (MAF).
3. The bidder must demonstrate successful completion of at least **ONE (01)** endpoint security/EDR deployment project using the proposed solution in the banking or financial services sector. Evidence shall include the client, scope, quantity and completion date, subject to client confidentiality. If the bidder fails to demonstrate the required experience or provide satisfactory supporting evidence, no technical points shall be awarded under this criterion.
4. The bidder must demonstrate at least **THREE (03)** successful deployments of the same proposed product or product family in an enterprise environment. If the bidder doesn't have any experience will not get technical points. If the bidder fails to demonstrate the required experience or provide satisfactory supporting evidence, no technical points shall be awarded under this criterion.
5. The bidder must submit profiles of proposed project personnel, including relevant OEM certifications and experience in endpoint security, EDR and XDR.
6. The bidder must demonstrate local implementation and post-sales support capability and disclose OEM escalation arrangements.
7. The bidder must disclose material litigation, insolvency, debarment, conflict of interest or other matters that may affect its ability to perform.
8. The bidder shall submit audited financial statements for the last three (03) financial years, where available, to demonstrate financial capacity. The Bank may assess financial capacity in accordance with its procurement policy.
9. Administration console and operational training for at least three (03) Bank personnel shall be included in the base contract price.
10. The bidder shall describe its customer support portal and local support arrangements, including availability for critical incidents, escalation channels and OEM support access. Equivalent support arrangements through an OEM-authorized local partner are acceptable.
11. The bidder shall provide details of the proposed implementation and support team, including relevant OEM certifications and security operations experience. CEH or other recognized security certifications may be considered as supporting evidence; no particular certification title shall be an exclusive condition.

5.1 Gartner market reference

Gartner market research may be considered as general market context only. Gartner positioning shall not be used as a mandatory eligibility condition, an exclusive OEM shortlist or a substitute for the functional and security requirements in this tender. Any OEM whose proposed product meets the tender requirements may participate, subject to the stated eligibility and evaluation criteria.

All OEMs and products meeting the requirements of this tender may participate, subject to the stated eligibility, technical and commercial evaluation criteria.

6. INSTRUCTIONS TO BIDDERS

6.1 Two-envelope submission

Submit one sealed outer envelope containing two separately sealed inner envelopes marked **"TECHNICAL PROPOSAL"** and **"FINANCIAL PROPOSAL".** The outer envelope shall show the tender title, reference number and bidder's name/address. The Financial Proposal must not be included in or disclosed through the Technical Proposal.

6.2 Technical Proposal

- The Technical Proposal shall include the Signed letter of bid and bidder profile.
- Legal and statutory documents listed in Section 5.
- **OEM authorization and product details.**
- Completed **Annexure I** with datasheets and supporting evidence.
- Proposed architecture, deployment approach and integration design.
- Implementation, rollout, resource and training plans.
- Relevant project references and completion evidence.
- Support model, escalation matrix and proposed SLA.
- Assumptions, exclusions, dependencies, optional components and deviations.
- The submission checklist in Annexure IV shall be completed.



6.3 Financial Proposal

- The Financial Proposal shall be submitted separately using Annexure II.
- It shall state the fixed three-year price in BDT, annual and unit price breakdown, all applicable taxes and charges, and separately priced optional items.
- The base evaluated price must include every component required to meet the mandatory scope.
- Price validity of at least 180 days from the submission deadline.

6.4 Clarifications and addenda

Clarification requests shall be submitted in writing to the contact designated in the final Tender Data Sheet by the stated deadline. Responses and addenda issued by the Bank shall form part of the tender and shall be communicated consistently to participating bidders.

6.5 Bid security and performance security

The Bidders shall submit a Bid Security equivalent to **5% of the total value of the proposed solution**, in the form of a Payment Order or Bank Guarantee issued in favor of Community Bank Bangladesh PLC. The Bid Security must remain valid for a period of **six (6) months** from the date of bid opening and shall be enclosed within the Financial Proposal envelope.

7. EVALUATION AND AWARD

Stage	Evaluation activity	Outcome
1. Preliminary	Submission, signatures, separate envelopes, bid validity and required documents.	Responsive / non-responsive
2. Eligibility	Legal status, OEM authorization, statutory documents, personnel and mandatory qualification requirements.	Qualified / disqualified
3. Technical	Mandatory EPP, EDR, XDR, security, integration, architecture, implementation and support requirements.	Technically responsive / non-responsive
4. Financial	Open only technically responsive Financial Proposals; check arithmetic, taxes and total cost.	Evaluated financial ranking
5. Due diligence	Verify references, OEM authorization, licensing and commercial terms.	Award recommendation

7.1 Mandatory technical requirements

Only requirements expressly identified as Mandatory in Annexure I, together with the legal, statutory and authorization requirements in Section 5 and the submission requirements in Section 6, shall be treated as pass/fail requirements. Experience criteria in Section 5 that are expressly identified as scored shall be evaluated for points only; absence of such experience shall result in zero points under the relevant criterion and shall not, by itself, disqualify a bidder.

8. COMMERCIAL REQUIREMENTS

8.1 Budget and contract duration

The contract and license subscription period shall be **01 January 2027 to 31 December 2029**. All licenses, subscriptions, support entitlements and required product capabilities and training shall remain valid throughout this period.

8.2 Price requirements

- The bidder shall quote a fixed three-year price in BDT using Annexure II.
- The quoted base price must include all licenses, subscriptions, modules, connectors, implementation, configuration, training, support, updates, taxes and other charges necessary to meet the mandatory requirements.
- Any additional or variable charge, including a charge dependent on data ingestion, storage or integration, shall be clearly disclosed and included in the evaluated price where necessary for compliance.
- The bidder shall provide a fixed three-year price and disclose any proposed price escalation or variable charge. Undisclosed charges will not be accepted.

Community Bank Bangladesh PLC ★ ICT Division ★

- No separate payment shall be claimed for any mandatory item necessary to deliver a compliant solution unless expressly listed and accepted in the contract.

8.3 Payment

All payments shall be subject to verified license entitlements, the applicable milestone being achieved, the Bank's written acceptance where specified, and submission of valid invoices and applicable tax documents. No advance payment shall be made unless separately approved in writing by the Bank.

8.4 Payment Terms:

1. **90% of the total contract value** shall be payable upon successful implementation and **Go-Live of the solution**, subject to the Bank's verification and written acceptance.

2. **The remaining 10% of the total contract value** shall be payable upon successful completion of **THREE (03) years** of operation from the Go-Live date, subject to satisfactory performance throughout the contract period.

9. CONTRACT CONDITIONS AND INFORMATION SECURITY

9.1 Service levels

The bidder shall submit a support and escalation model for the full contract period and complete the proposed SLA table below. Final measurable response and resolution targets shall be approved and incorporated into the contract.

Severity	Example	Bidder response target	Update / workaround target
P1 – Critical	Widespread protection failure, critical security incident or loss of central management with material impact.	Bidder to propose	Bidder to propose
P2 – High	Significant EDR/XDR degradation or major feature unavailable with security impact.	Bidder to propose	Bidder to propose
P3 – Medium	Limited functionality issue with workaround.	Bidder to propose	Bidder to propose
P4 – Low	General query or minor service request.	Bidder to propose	Bidder to propose

9.2 Confidentiality and security

- The bidder and its personnel shall comply with the Bank's ICT Security Policy, information security standards, access controls and security instructions.
- Access to Bank systems, devices, networks, data or facilities shall be limited to authorized personnel, approved purposes and minimum necessary privileges.
- The bidder shall sign confidentiality and non-disclosure undertakings and ensure equivalent obligations for employees and subcontractors.
- The bidder shall not copy, disclose, process, transfer or retain Bank data except as authorized in writing by the Bank.
- The bidder shall disclose data flows, telemetry categories, hosting locations, cross-border transfers, retention and deletion arrangements.
- The bidder shall promptly notify the Bank of any actual or suspected security incident affecting the service, Bank data, credentials, agents or management console and cooperate with investigation and remediation.
- The Bank and its regulators/auditors shall have the right to inspect and audit records, controls and service activities relevant to the contract, subject to applicable law.
- Subcontractors and material service providers shall be disclosed; prior written approval shall be obtained where required by the Bank.
- At expiry or termination, the bidder shall support transition, revoke access, return Bank information and securely delete Bank data as instructed by the Bank and applicable law.

9.3 Ownership and intellectual property

The Bank retains ownership of its data, logs, configurations, incident records and Bank-specific deliverables. The bidder retains ownership of its pre-existing software and intellectual property, subject to the license rights granted to the Bank. The bidder warrants its right to provide the proposed products and services and shall indemnify the Bank against third-party intellectual property infringement claims in accordance with the final contract.

Community Bank Bangladesh PLC. ICT Division

9.4 Delay and remedies

The bidder shall meet milestones in the approved project plan. Liquidated damages, service credits, termination rights and other remedies for delay or service failure shall be stated in the final contract under the Bank's Standard Procurement Policy.

9.5 Bank's rights

The Bank reserves the right, in accordance with its Standard Procurement Policy and applicable law, to accept or reject any or all tenders, cancel or amend the process, seek clarifications, verify submitted information, conduct demonstrations and award the contract to the bidder whose proposal is responsive and offers the best overall value. The Bank is not obliged to select the lowest-priced bidder.

The Bank shall not be obligated to award the contract to the bidder securing the first position in either the technical or financial evaluation. The Bank reserves the right to make the final award decision.

Community Bank Bangladesh PLC. ICT Division

ANNEXURE I – TECHNICAL COMPLIANCE MATRIX

Instructions: Complete every row using "Comply", "Partially Comply" or "Do Not Comply". Identify the exact OEM product, edition, module or service supporting the response and attach documentary evidence. State limitations, dependencies, platform differences and additional costs. Equivalent technologies and alternative implementation methods are acceptable where they meet the stated security outcome.

ID	Requirement	Criteria	Bidder response	Reference Links
A.	**Endpoint Protection and Detection & Response (EPP + EDR) for Users**			
A1	The solution shall provide 600 workstation licenses for current Windows, Linux and macOS releases. The bidder shall supply a compatibility matrix listing supported OS versions, feature differences between Windows and macOS, and any platform-specific limitations.	Mandatory		
A2	Should have integrating anti-exploit, anti-ransomware, deep learning AI, and control technologies to prevent zero-day attacks, reduce the attack surface, and provide advanced Endpoint Protection with Endpoint Detection and Response (EDR) capabilities.	Mandatory		
A3	The solution shall provide integrated signature-based and signatureless endpoint protection, including AI-powered deep-learning malware detection, behavioral analysis, exploit prevention, ransomware protection, reputation-based checks, and automated threat cleanup, subject to the proposed product and supported platform.	Major		
A4	The entire solution must be managed through a single, Central Managed, web-based cloud console, with no on-premises management servers required.	Mandatory		
A5	The proposed solution shall identify specific product tiers, licensing entitlements, and prerequisites required to deliver advanced protection and telemetry.	Major		
A6	The solution shall be centrally managed through a web-based unified management console and provide endpoint detection, investigation, threat hunting, and supported response capabilities.	Major		
A7	The solution must support multiple deployment methods, including a direct-download agent, a centralized installer for deploying agents through on-premises Active Directory.	Major		
A8	The solution must support massage relay server for securing offline machine	Major		
A9	The console must provide granular RBAC, allowing the creation of custom roles with specific permissions (e.g., Helpdesk, Security Analyst, Administrator) for different teams.	Major		
A10	Security policies (e.g., exploit mitigation, application control, device control) must be created and managed centrally and deployed dynamically to groups of endpoints.	Mandatory		
A11	The solution must provide a comprehensive RESTful API to automate tasks, integrate with IT service management (ITSM) tools like ServiceNow, and export data to a SIEM.	Major		
A12	The solution must include built-in, customizable reporting and dashboards for compliance, security posture, and threat activity, with the ability to schedule and export reports.	Major		
A13	Solution must provide a single agent and centralized console that combines real time prevention (next gen AV, behavioral protection) with full EDR capabilities (detection, investigation, response) without requiring separate products or consoles. Agent must enforce prevention policies locally and escalate telemetry to EDR for investigation.	Critical		

Community Bank Bangladesh PLC. ICT Division

A14	Must include both on device ML models for immediate local prevention and cloud-based ML/analytics for advanced detection and enrichment. Models must be continuously updated and support behavioral anomaly detection, fileless attack detection, and script abuse detection.	Critical		
A15	Must utilize a pre-execution deep learning neural network model trained on hundreds of millions of file samples to detect novel zero-day malware without relying on signature updates or cloud lookups.	Critical		
A16	The solution must analyze network traffic to detect and block malicious communication, including command-and-control (C2) activity, using the same agent.	Major		
A17	The solution must include specialized, behavioral protection that detects and blocks ransomware encryption attempts in real-time, automatically rolling back files to their pre-attack state.	Critical		
A18	Must Provide the automatically rolls back of damaged files to a safe state with a single click from console. There should not be limitation on snapshot size. Should also able to detect rouge encryption and stop.	Critical		
A19	Must prevent unauthorized write attempts, encryption, or wiping of the device Master Boot Record (MBR), GUID Partition Tables (GPT), and disk boot sectors to protect against bootkit and wiper malware.	Major		
A20	Must feature agent automatically kills processes, quarantines files and can disconnect the endpoint from the network. Detect Interactive Threat (Windows) and Lateral Movement engines detect hands-on-keyboard and living-off-the-land activity	Major		
A21	The solution must include specific mitigations to block the exploitation of software vulnerabilities (e.g., in browsers, Office applications), including memory and buffer overflow attacks.	Critical		
A22	Must deploy pre-configured, out-of-the-box exploit mitigations targeting memory allocation attacks, privilege escalation, credential theft (e.g., LSASS memory dump protection), and API hooking across all installed applications.	Major		
A23	Provide automated response actions (host isolation, process termination, file quarantine, registry rollback, script blocking) that can be executed manually or via playbooks. Actions must be reversible where applicable and auditable.	Critical		
A24	Must provide automated, real-time Critical Attack Warnings within the management console when human-led, hands-on-keyboard adversary behavior is detected on any endpoint.	Major		
A25	Detection engine must provide confidence scoring, allow suppression/whitelisting, and support adaptive tuning (auto suppress benign behavior) to minimize false positives while preserving detection coverage.	Major		
A26	Must have capability SAML 2.0 SSO SSO-exclusive login, auto-provisioning of users at first login	Major		
A27	The solution shall support endpoint isolation/containment and provide integration capability with network access-control or ZTNA solutions where available.	Major		
A28	The solution must allow policies to restrict execution of unauthorized applications, including scripts and executables, based on a cryptographic hash, certificate, or path.	Major		
A29	Must provide endpoint-enforced application control capable of blocking or restricting specific applications (e.g., P2P, unauthorized administrative software) directly at process start.	Major		
A30	The solution must include built-in, policy-based controls to monitor and restrict the copying of sensitive data to removable media.	Major		

Community Bank Bangladesh PLC. ICT Division

A31	All telemetry and management communications must be encrypted (TLS 1.2+/mutual TLS). Stored telemetry and artifacts in cloud must be encrypted at rest. Provide key management details and compliance attestations.	Mandatory		
A32	Agent must include tamper protection preventing unauthorized uninstall/disable, signed binaries, secure update mechanism, and ability to enforce agent reinstall from console.	Mandatory		
A33	Must include integrated endpoint Peripheral Control to govern, restrict, or audit connected removable media (USB storage, Bluetooth, SD cards, Thunderbolt storage) using the single unified endpoint agent.	Major		
A34	The solution must be capable of detecting and blocking unwanted software (adware, crypto-miners, etc.) that is not strictly malicious but poses a security or productivity risk.	Major		
A35	Solution must support Event Collection records URLs (browser extension on Chrome, Edge, Safari) and DNS events for investigation and create custom rules. Marketplace ingestion integrations) bring web-gateway telemetry and detections into the console .	Major		
A36	The solution must integrate with a cloud-based, real-time threat intelligence service for rapid file and URL reputation checks and behavioral analysis.	Critical		
A37	The solution must continuously monitor process behavior at runtime to identify and block malicious activity, such as script-based attacks, code injection, and credential theft.	Critical		
A38	The solution must detect and flag techniques used by human adversaries, such as lateral movement, persistence mechanisms, and Living-off-the-Land (LotL) binaries.	Major		
A39	The solution shall maintain a continuously updated global threat intelligence capability supporting endpoint detection, file/URL reputation, threat research and adversary intelligence.	Major		
A40	The solution must provide a full EDR capability within the cloud console, allowing security personnel to search, investigate, and respond to threats.	Critical		
A41	The solution must retain a minimum of 30 days of detailed endpoint data in a searchable data lake, queryable via a dedicated SQL-like query language.	Major		
A42	Must include native Account Health Check capabilities that audit endpoint security configurations, detect unmanaged devices,.	Major		
A43	Must automatically construct interactive root cause visualization graphs detailing the entire attack chain, affected processes, registry modifications, and created files for supported detections/threat cases.	Major		
A44	Must provide an encrypted, direct command-line Live Response shell to remotely access endpoints for forensic artifact collection, process termination, script execution, and rebooting.	Major		
A45	Upon detection, the solution must automatically quarantine and remove malicious files and artifacts from the endpoint.	Mandatory		
A46	Agent must continue to detect and prevent threats while offline and securely queue telemetry for later upload when connectivity is restored.	Mandatory		
B.	**Extended Detection & Response (XDR) for Servers**			
B1	The solution shall provide 100 server licenses for supported Windows Server versions and major Linux distributions (e.g., RHEL, CentOS, Ubuntu, Amazon Linux, SUSE, Debian, Oracle Linux). The bidder shall document supported versions, prerequisites and feature differences between Windows and Linux.	Mandatory		

Community Bank Bangladesh PLC ★ ICT Division ★

B2	Endpoint protection, EDR and XDR for servers shall be delivered from the same agent and console as the workstation solution, with server-specific policies and telemetry.	Mandatory		
B3	The Solution shall have capabilities of next-generation server workload protection for physical, and virtual server environments.	Major		
B4	The solution must Supports servers such as domain controllers, allow/monitor/block rules by file path/folder, hash and publisher	Major		
B5	The solution shall provide dedicated server-side exploit mitigation and anti-exploit protections targeting core server processes (e.g., IIS, database engines, remote code injection, privilege escalation) where covered by the proposed protection capabilities.	Critical		
B6	The solution shall utilize on-device AI deep-learning neural networks optimized for enterprise servers to detect zero-day malware without signature updates or cloud dependency	Critical		
B7	The solution shall provide capabilities for server operating systems to detect and report unauthorized modifications to critical system files, directories, and registry keys in real time.	Major		
B8	The solution shall provide XDR investigations beyond the endpoint & server by collecting, searching, and analyzing available security telemetry from supported OEM products and configured third-party integrations, subject to applicable subscriptions and integration requirements.	Major		
B9	The solution shall collect, search, and analyze security telemetry from managed server workloads and store data in a centralized cloud repository (Data Lake) for historical investigation.	Major		
B10	The solution shall provide Live Discover or the applicable OEM threat-hunting capability, supporting predefined and customizable SQL-based queries against supported endpoints, servers, and other available data sources. Scheduled queries and additional query functionality shall be available where supported by the proposed subscription.	Major		
B11	The solution shall provide a Data Lake or equivalent supported central repository for security telemetry, enabling historical investigation and querying of data from managed endpoints and configured data sources. The bidder shall specify applicable storage allowances and retention limits.	Major		
B12	The solution shall support historical investigation of telemetry already stored in the Data Lake for up to 90 days, where included in the proposed entitlement and subject to applicable retention and storage limits. Querying data already stored shall not require the originating endpoint to be online.	Major		
B13	The solution shall provide incident-investigation capabilities to examine available event timelines, affected devices, relevant processes, users, files, indicators of compromise, and associated threat context to help determine incident scope and potential impact.	Major		
B14	The solution shall support AI-assisted investigation and Adaptive Attack Protection where these capabilities are available for the proposed product, platform, and subscription. Administrators shall retain appropriate permissions and control over supported response actions.	Major		
B15	The solution shall support compatible OEM Managed Detection and Response (MDR) services where available and separately licensed or contracted. The bidder shall identify the applicable service, prerequisites, scope, and commercial entitlement. Solution support Threat Hunting and periodic human-led threat hunts. Licensed per endpoint, with XDR coverage via detection library for third-party logs (Firewall, Okta, Zscaler, O365, AWS,google etc.).	Optional		

Community Bank Bangladesh PLC ★ ICT Division ★

B16	The solution shall provide centralized visibility into available endpoint security events, detections, device status, process activity, and relevant user or authentication context. Information from firewalls, identity systems, and other security controls shall be available only where provided by supported telemetry or configured integrations.	Major		
B17	The proposed solution shall support technical security controls, event logging, and centralized reporting aligned with regulated industry frameworks, including PCI DSS, HIPAA, and financial institution audit requirements.	Major		
B18	The solution shall provide centralized visibility and protection for server workloads running on-premises and in public cloud environments (such as AWS, Azure and GCP virtual machines) through the same management console and agent.	Major		
B19	The solution shall provide documented APIs and supported integrations with compatible SIEM, SOAR, identity, and security-management systems. Available functionality may include security-event ingestion, log collection, notifications, ticket creation, data exchange, and supported response actions. The bidder shall identify applicable integration prerequisites, permissions, configuration, and licensing.	Major		
B20	The solution shall have unlimited AI assistant, Threat Hunting, Graph view of an alert which helps identify whole incident.	Major		
B21	The solution shall have 3rd party integrations and own threat intelligence, XDR reduces blind spots and speeds resolution in multi-vendor environments.	Optional		
B22	The solution should be capable of supporting the following Linux environments: CentOS,Debian,Fedora,Oracle,RedHatEnterprise Linux (RHEL),SUSE Linux Enterprise Server,Ubuntu,Virtuozzo	Major		
B23	The Solution should support Legacy Windows OS : Windows 7, Sever 2008 Sp2 onwards	Optional		
B24	The proposed solution must have remote shell that is controlled by the policies and RBAC and should be fully audited so administrators can be aware of who accessed what, when and what commands were executed.	Optional		
B25	The solution should also be able to unquarantined a file from the management interface.	Optional		
B26	The solution should support bulk remediation.	Optional		
B27	The solution should allow analysts to add, edit, and delete notes on threats and alerts directly within the management console, and these notes are visible to all users with appropriate permissions	Optional		
B28	The solution proposed should apply the configuration changes in near real time	Optional		
B29	The solution should be able to help administrators create and exclusion using a hash, Path, Publisher, browser, File type	Optional		
B30	The solution must provide an automated mechanism to decommission endpoint agents that have not communicated with the management console for a configurable period of time.	Optional		
B31	The solution should be able to export the endpoint list to CSV directly from the console and also via and API for further investigations.	Optional		
B32	The solution must perform static (pre-execution) analysis using machine learning models directly on the endpoint, without requiring file signatures or cloud lookups	Optional		
B33	The solution must provide native, real-time monitoring and protection against lateral movement techniques, leveraging	Optional		

Community Bank Bangladesh PLC ★ ICT Division ★

	behavioral analysis to detect and block attacks initiated by remote devices or users on Windows, Linux and macOS systems.			
B34	The solution must be able to support fast, single query search across endpoints and telemetry data for common investigation attributes such as hostnames, file names, timestamps, hash values, URLs etc.	Optional		
B35	The solution should be able to revert changes attributed to the attack, minimizing data loss and keeping unaffected data intact.	Optional		
B36	The agent should have the capability to isolate an endpoint from the internet while still maintaining full connectivity to the management console.	Optional		
B37	The management console must support policy inheritence across a multi-tenant console with a unified policy for Windows, macOS, Linux and containers.	Optional		
B38	The solution should be able to place a device directly into a specific device group during onboarding and installation.	Optional		
B39	The solution must provide device control capabilities that allow administrators to create policies for external devices (USB, Bluetooth, Thunderbolt, SD cards) with the following granularity: by device class, vendor ID, specific serial numbers, type of device etc.	Optional		
B40	The solution must support the creation and enforcement of firewall rules that are location-aware, allowing different policies to be applied based on the endpoint's current network context.	Optional		
B41	The solution must provide autonomous, real-time prevention against zero-day attacks by analyzing behaviors on the endpoint, not just relying on file signatures even when the agents are offline.	Optional		
C.	**Subscription, service and support**			
C1	A three-year subscription for 600 workstation and 100 server entitlements shall include all stated product tiers, maintenance and licensing terms, and renewal options.	Mandatory		
C2	The OEM shall provide technical support with 24×7×365 availability for critical issues (phone, web portal, email/chat), defined response targets, escalation paths and remote-support entitlements. The bidder shall state the support tier included.	Mandatory		
C3	The OEM shall provide continuous protection updates, threat-intelligence feeds, software updates, patches and product upgrades throughout the subscription term at no extra charge.	Mandatory		
C4	OEM support shall be reachable through the online support portal, telephone and in-console support-case creation. The bidder shall describe the support-access process.	Major		

MDR is optional and is not part of the approved base procurement unless separately evaluated, approved and included in the contract.

The Bank shall not be obligated to award the contract to the bidder securing the first position in either the technical or financial evaluation. The Bank reserves the right to make the final award decision.

Community Bank Bangladesh PLC. ICT Division

ANNEXURE II – FINANCIAL PROPOSAL

Quote all prices in BDT. Provide a fixed three-year price for the complete compliant solution for **700 devices** from **01 January 2027 to 31 December 2029**. VAT, AIT and all other applicable taxes and charges must be disclosed and included in the grand total.

A. License and subscription price

Sl.	Description	Quantity	Total Price (BDT)
1	EPP + EDR licenses including Service – Workstations	600	
2	EPP + EDR licenses including Service – Servers	100	
3	XDR platform / entitlement / mandatory modules/License	100	

B. VAT and AIT grand total summary

Price component	Amount (BDT)
Subtotal before taxes	[Quote]
VAT	[Quote]
AIT	[Quote]
Other applicable taxes/duties/charges	[Quote]
GRAND TOTAL – THREE YEARS, INCLUSIVE OF ALL TAXES	[Quote]
Amount in words	**[Write in words]**

C. For Future Expansion (Unit Price)

Sl.	Description	Quantity	Total Price (BDT)
1	EPP + EDR licenses including Service – Workstations	1	
2	EPP + EDR licenses including Service – Servers	1	
3	XDR platform / entitlement / mandatory modules/License	1	

*Including VAT & AIT

D. Optional items (not included in evaluated base price)

Sl.	Optional feature/service	Scope / description	Three-year price (BDT)
1	MDR service	Coverage, service hours, SOC location and response scope	[Quote]
2	Other optional services	Specify	[Quote]

*Including VAT & AIT

Bidder declaration: We confirm that the quoted price includes all components and services required to meet the mandatory tender requirements for 700 devices for the full three-year contract period. No additional payment shall be claimed for a mandatory feature, module, connector, update, support or service not separately disclosed in this proposal.

We acknowledge and agree that the Bank shall not be obligated to award the contract to the bidder securing the highest technical score, the lowest evaluated financial price, or the first position in either evaluation. The Bank reserves the right to make the final award decision.

Authorized signatory : _____

Name : _____

Designation : _____

Company seal : _____

Date : _____

Community Bank Bangladesh PLC. * ICT Division *

ANNEXURE III – MANUFACTURER'S AUTHORIZATION FORM (MAF)

To:

[Contact Person]

[Name of the Procuring Entity]

[Address of the Procuring Entity]

Date:

Invitation for Tender No: *CBBL/HO/ICTSC/01-2026/01*

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.

Community Bank Bangladesh PLC. ICT Division

ANNEXURE IV – BIDDER DECLARATION AND SUBMISSION CHECKLIST

A. Bidder declaration

We, the undersigned, confirm that:

- We have examined the tender document and addenda and accept its requirements, subject to deviations expressly listed in our proposal.
- The information and documents submitted are true, complete and accurate to the best of our knowledge.
- We are legally eligible to participate and have disclosed relevant litigation, conflict of interest, insolvency or debarment information.
- The proposed OEM, product, edition, modules, license metric and third-party dependencies have been fully disclosed.
- The proposed price covers the mandatory scope for 700 devices for the full three-year contract period, inclusive of applicable taxes and charges.
- We will comply with the Bank's confidentiality, information security, access control, audit and regulatory requirements.
- We understand that the Bank may verify our references and submitted information.
- We acknowledge and agree that the Bank shall not be obligated to award the contract to the bidder securing the highest technical score, the lowest evaluated financial price, or the first position in either evaluation. The Bank reserves the right to make the final award decision based on its overall assessment, in accordance with the Bank's procurement policy and applicable regulations.

Bidder's legal name: _____

Authorized signatory: _____

Designation: _____

Signature and company seal: _____

Date: _____

B. Submission checklist

No.	Document / requirement	Included (Yes/No)	Page reference
1	Signed letter of bid	[ ]	
2	Trade License and incorporation/registration documents	[ ]	
3	TIN and VAT/BIN documents	[ ]	
4	Manufacturer's Authorization Form	[ ]	
5	Completed technical compliance matrix with evidence	[ ]	
6	Product datasheets, architecture and integration details	[ ]	
7	Banking/financial sector project references	[ ]	
8	OEM-certified project team profiles	[ ]	
9	Implementation, deployment and training plan	[ ]	
10	Separate sealed Financial Proposal	[ ]	
11	Bid security	[ ]	

Community Bank Bangladesh PLC ICT Division