REQUEST FOR QUOTATION
FOR

Supply and Installation of Enterprise Anti-Virus Software Licenses

AT

THE ASSAM CO-OPERATIVE APEX BANKLTD.

INFORMATION TECHNOLOGY DEPARTMENT
HEAD OFFICE: 151, HEM BARUA ROAD, PANBAZAR, GUWAHATI
ASSAM – 781001, INDIA

REF NO.: ACAB/HO/IT/Cyber Security/72
RELEASE DATE:23-01-2023

PARTICULARS	**DEADLINE**
Date of Release of RFQ	23-01-2023
Last date of submission of the Proposal	13-02-2023, 15:00 hours
Date of opening of the Technical Proposal	13-02-2023, 16:00 hours
Date of opening of the Commercial Proposal	Will be informed on the date of opening of Technical Bid

Bank email id for RFQ related communication: it@apexbankassam.com

Contents

1 Introduction 3
1.1 About Assam Co-operative Apex Bank Ltd. 3
1.2 Objective 3
2 Scope of Work 4
3.1 Scope Summary 4
3.2 Detailed Scope of Work 4
a. Endpoint Security (Anti-Virus) 4
3 Payment Terms: 6
4 Contract Period: 6
5 Validity 6
6 Extension of Validity 6
7 Currency of the quotation 6
8 Project Timeline: 6
9 Order Cancellation 6
10 Vendor's Obligations 7
11 Information Ownership 7
12 Use of Contract Documents and Information 7
13 Submission of Proposal 7
14 Evaluation Methodology 8
15 Negotiation 9
16 Right to Accept or Reject any or All quotations 9
17 Liquidated Damages & Penalties 9
18 Annexures: 10
Annexure 01 Covering Letter 10
Annexure 02: Bidder's Information 11
Annexure 03: Conformity letter 13
Annexure 04: Functional and Technical Specification 14
Annexure 05: Manufacturer's Authorization Form 19
Annexure 06: Self declaration for Blacklisting 20
Annexure 07: Commercial Bill of Material 21

1 Introduction

1.1 About Assam Co-operative Apex Bank Ltd.

The Assam Co-operative Apex Bank Ltd. (ACAB) was established in 1948. Since then, the Bank has developed and expanded its activities/ operations and has grown in manifolds. The Bank has a wide network of 67 branches and 6 Zonal Offices, spread throughout the state providing effective banking products and other related services to the public of Assam.

The ACAB as a pioneer in Banking in Assam, has taken banking to the doorsteps of the people of the State and has been able to nurture and develop banking habits among the people of the State. This has changed the saving habits of people from the traditional methods to the modern banking facilities to earn remunerative returns for their savings invested with the Bank and utilize various attractive and innovative banking products offered by ACAB.

1.2 Objective

The Bank is currently having 500 nos. of endpoint system (approx.) at various branches of the Bank. Most of the systems are running in Linux (Ubuntu 11.04 and above) platform. Some of the systems are running in windows (Windows 8 and above) platform. The bank is currently having Symantec anti-virus as endpoints and wishes to procure 500 nos. of volume license of Symantec End point security antivirus software. Through this RFQ the Bank is requesting the various bidders to submit the quotation for Symantec End point Security antivirus Software as per the specification provided in Annexure 04 – Functional and Technical Specification.

Eligibility Evaluation Criteria:

SlNo	Eligibility Description	Documents to be submitted as Bidder
1	The Bidder should be in existence in India for minimum of Three years as on 31.03.2022	Certificate of Registration/ Incorporation whichever is applicable
2	The bidder submitting the offer should be having a turnover of minimum Rupees 50 Lacs (INR Fifty Lacs) Per year during last three years i.e. 2019-2020, 2020-2021 and 2021-2022.	Copy of the audited balance sheet of the company for the consecutive last three financial years (2019-2020, 2020-2021 and 2021-2022) should be submitted.
3	The Bidder should have reported profit (Profit after Tax) for the financial years (2019-2020, 2020-2021 and 2021-2022).	Copy of the audited balance sheet of the company for the consecutive last three financial years (2019-2020, 2020-2021 and 2021-2022) should be submitted.
4	The bidder should be the authorized partner / representative of the OEM.	The Bidder need to submit the MAF from the OEM of Endpoint protection software.
5	The bidder should submit an authorization letter from manufacturer (OEM) to this effect should be furnished. This letter should specify that in case authorized representative is not able to perform obligations as per contract during contract period, the Original Equipment Manufacturer would provide the same.	Manufacturer Authorization Form (MAF)

2 Scope of Work

3.1 Scope Summary

The scope of services for this engagement would include, but not limited to:

a. Bidder to Supply, Install, Customize, Configure, Parameterize, Implement, Integrate, Maintain and Manage Endpoint Security Solutions as listed in the subsequent sections of this proposal.
b. Bidder is required to ensure that business is not impacted due to infrastructure change management which is in relation with new or enhanced security solution implementation, integration, or operationalization.
c. Bidder is required to test the security updates/ upgrades/ patches and is required to inform the Bank of any security updates/ upgrades/ patches made available in the Solution procured/ taken over through this RFQ.
d. Bidder/OEM is required to provide Technical Support Services during the tenure of the contract.

3.2 Detailed Scope of Work

The detailed scope of the solutions is provided below. The solutions are required to fulfill the security guideline as defined by NABARD.

a. Endpoint Security (Anti-Virus)

i. Bidders are requested to supply Symantec Enterprise Anti-Virus Software covering 500 number of Endpoints & Servers which must be a dedicated purpose-built platform that can be deployed independently without any functional reliance on existing or 3rd party layers of security, fully adhering to defense in depth architecture. Solution must function independently, if any of the layers of security is replaced or becomes non-functional at any point during entire project period.
ii. The solution must be sized appropriately by the bidder with no additional costs from customer to ensure performance, scalability, and sizing as required to deliver the technical requirements of this project during operational phase.
iii. The bidder shall propose a dedicated endpoint based solution to ensure Enterprise security & SOC teams are equipped with an Endpoint Detection & Response system enabling the analysts for centralized Incident response capabilities against Advanced Targeted & unknown threat attacks.
iv. The bidder will be responsible for implementation of the antivirus solution in all PC/Servers spread across all branches/HO/Data Centers/DRC of bank. Bidder resources are required to visit the branch/HO/Data Center for implementation of the Anti-virus software without any additional cost to the Bank other than the contracted amount.
v. The solution must provide security threat Intelligence feeds to run in offline/non-sharing airgap mode, without the requirement to submit any analysis or data to the cloud or 3rd party solutions for analysis or detection verdicts.
vi. The proposed solution must support SNMP, Syslog, etc. for integration with all leading SIEM/SOC solutions. The Solution components must also be providing access over REST API's with OEM documentation.
vii. The Solution should be able to define rules and policy definitions, enforce security policies at various levels and be able to prevent unauthorized access or malicious traffic.
viii. Both Endpoint (Antivirus) and Server security management from single console.

ix. The solution should be deployed in high availability mode at DC & Standalone at DR.

x. Solution must be accessible via web UI and shall not require any plugins or thick client requirements for Admins and Analysts to access and manage the solution.

xi. Endpoint security monitors system-level activities to allow threat investigators to rapidly assess the nature and extent of targeted attacks. The solution must protect the bank's end user system both windows (Windows 8 and above) and Linux (Ubuntu 11.04 and above) by effective protection against scripts, injection attacks through behavior analysis detection of advanced malware, such as ransomware threat, etc.

xii. The Antivirus server need to be configured by the vendor at the DC and DRC. The Centralized Server should push all updates to the endpoints at regular interval and the endpoints should be configured properly to get updated from the centralized server located at DC/DRC of the Bank.

xiii. The Antivirus server will have to be integrated with existing Active Directory of bank.

xiv. The bidder will be responsible to provide the required configuration of centralized server required for anti-virus management at DC & DR location. Bank or its vendor will provide the required virtual/physical server with OS and bidder will be responsible for entire centralized server configuration.

xv. Bidder will be required to directly co-ordinate with Bank's team or appointed vendor related to the implementation & go-live of the anti-virus solution.

3 Payment Terms:

For License cost along including implementation cost:

- 60% on delivery of Licenses.
- 30% on implementation and go-live
- Balance 10% on Final Sign-Off 1 month post go-live & smooth operations

4 Contract Period:

Three (3) Years from the date of Go-live of the project.

5 Validity

The Vendor shall keep the quotation valid for a period of six months from the last date for the submission of quotation.

6 Extension of Validity

In case circumstances require, the BANK may request the vendors, within the validity period of the quotation, to extend the validity of the quotation for any additional periods as required.

7 Currency of the quotation

All prices and monetary terms to be quoted in INDIAN RUPEES (INR) only.

8 Project Timeline:

10.1 Delivery, installation & completion of Central Site for Centralized Antivirus Solution should be completed within four weeks from the date of purchase order.

10.2. Completion of Antivirus client installation and making live for obtaining updates from central site and integration with Active Directory services for all 500 nodes in HO/ZOs/Branch offices should be completed within two months from the date of purchase order. The successful vendor has to depute adequate Technical Support Staff for this activity.

9 Order Cancellation

The Bank reserves the right to cancel the contract placed on the selected vendor and recover expenditure incurred by the Bank under the following circumstances:-

- ✓ If the selected vendor fails to complete the assignment as per the timelines prescribed in the contract and the extension if any allowed, it will be a breach of contract.
- ✓ In case the selected vendor fails to deliver the quantity as stipulated in the delivery schedule, The Bank reserves the right to procure the same or similar product from alternate sources at the risk, cost and responsibility of the selected vendor.
- ✓ The Bank reserves the right to recover any dues payable by the selected vendor from any amount outstanding to the credit of the selected vendor, including the pending bills and/or invoking The Bank guarantee under this contract.

In case of cancellation of order, any payments made by the Bank to the vendor would necessarily have to be returned to the Bank with interest @15% per annum, further the vendor would also be required to compensate the Bank for any direct loss suffered by the Bank due to the cancellation of the contract and any additional expenditure to be incurred by the Bank to appoint any other vendor. This is after repaying the original amount paid.

10 Vendor's Obligations

The selected vendor is obliged to work closely with the Bank's staff, act within its own authority and abide by directives issued by the Bank and implementation activities.

The selected vendor is responsible for managing the activities of its personnel or its representatives and will hold itself responsible for any misdemeanors. The vendor is under obligation to provide system integration services as per the contract.

The selected vendor will treat as confidential all data and information about the Bank, obtained in the execution of their responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Bank.

11 Information Ownership

All information processed, stored, or transmitted by Vendor equipment belongs to the Bank. By having the responsibility to maintain the equipment, the vendor does not acquire implicit access rights to the information or rights to distribute the information. The vendor understands the civil, criminal, or administrative penalties may for failure to protect information appropriately.

12 Use of Contract Documents and Information

The selected vendor shall not, without the Bank's prior written consent, disclose the Contract or any provision thereof or any specification, plan, drawing, pattern or information furnished by or on behalf of the Bank in connection therewith, to any person other than a person employed by the selected vendor in the performance of the Contract. Disclosure to any such employed person shall be made in confidence & shall extend only as far as may be necessary for purposes of such performance.

The selected vendor shall not, without the Bank's prior written consent, make use of any document or information except for purposes of performing the Contract.

Any document, other than the Contract itself, shall remain the property of the Bank and shall be returned (in all copies) to the Bank on completion of the vendor's performance under the Contract if so required by the Bank.

13 Submission of Proposal

The Bidder shall submit the proposal in the manner prescribed hereunder: -

i. The proposal shall be sealed and shall consist of two parts namely Technical proposal and Commercial proposal. Each of the proposal shall be submitted in two separate sealed envelopes. The Envelop Marked A shall contain the Technical proposal, and the Envelop marked B shall contain the

Commercial proposal.

ii. The Technical proposal shall be submitted as below: -

a) All the Annexures need to be duly filled along with all enclosures and documentary proof.

b) The Technical proposal should not have any indication of the Price or cost in any manner anywhere. If such an indication is found, the Bid shall be summarily rejected.

c) The soft copy of the technical proposal should be submitted along with the technical bid envelope.

iii. The Commercial Bid shall be submitted as below:

a) The Commercial proposal shall consist of Bill of Material as per Annexure 07 duly filled and signed by the authorized person on behalf of the Bidder in the ORIGINAL and soft copy of the commercial Bid.

b) The Commercial proposal shall be exclusive of all Rates and taxes as applicable.

c) The soft copy of the Commercial proposal should submit along with the commercial proposal envelope.

14 Evaluation Methodology

The evaluation will be a three-stage process. The stages are:

Eligibility evaluation – The Bank shall scrutinize the Eligibility bid submitted by the bidder. A thorough examination of supporting documents to meet each eligibility criteria (Section 2) shall be conducted to determine the Eligible bidders. Bidders not complying with the eligibility criteria are liable to be rejected and shall not be considered for Technical Evaluation.

Technical evaluation – The Bidder fully complied with the minimum technical specifications as mentioned in Annexure 04 without any deviation will be considered as technically qualified bidders. The Bidders are requested to submit this Technical compliance sheet "Annexure 04- Functional and Technical Specification" in OEM's letter head with seal and signature of authorized signatory and no deviations accepted.

Only Technically qualified bidders will be considered for commercial proposal opening.

In the event if only one bidder qualifies in technical evaluation, the Bank will have the right to place the order with the single qualified vendor. However, the Bank having rights to allow more than one bidder for commercial evaluation if only single bidder technically qualifies.

Commercial proposal evaluation - Based upon the prices of the vendors as discovered in the commercial evaluation whose prices will be the lowest will be declared as L-1 Bidder.

Commercial bid valuation shall be considered as below in case of any kind of discrepancy:

a. If there is a discrepancy between words and figures, the amount in words shall prevail;

b. If there is a discrepancy between percentage and amount, the amount calculated as per the stipulated percentage basis shall prevail;

c. Where there is a discrepancy between the unit rate and the line item total resulting from multiplying the unit rate by the quantity, the unit rate will govern;

d. Where there is a discrepancy between the amount mentioned in the proposal and the line item total present in the schedule of prices, the amount obtained on totaling the line items in the Bill of Materials will prevail;

e. The amount stated in the correction form, adjusted in accordance with the above procedure, shall be considered as final and binding;

f. If there is a discrepancy in the total, the correct total shall be arrived at by the Bank;

g. At the sole discretion and determination of Bank, it may add any other relevant criteria for evaluating the proposals received in response to this RFQ;

h. During the process of technical & financial evaluation if Bank decides to withdraw any collateral item offered in the proposal, the financial value of that item will be reduced from the financial offer of all the Bidder(s) and Total Cost of Ownership will be recalculated accordingly.

i. The financials will be calculated till two decimal points only.

15 Negotiation

Vendor who is declared as L-1 in the commercial evaluation may be called for negotiation before awarding the contract. However, the Bank having rights to negotiate with next to L-1 vendor if the L-1 vendor doesn't accept the Bank's offer.

16 Right to Accept or Reject any or All quotations

The BANK reserves the right to accept or reject any quotation and to annul the process and reject all quotations, at any time without any liability or any obligation for such acceptance, rejection or annulment, without assigning any reasons.

17 Liquidated Damages & Penalties

Bank shall levy penalty/liquidated damages on the bidder to the extent of 1% of the value of the delayed deliverables for each week of delay in Go-live subject to maximum 10% of the total cost of ownership (contract value). However, imposing penalty shall be at the discretion of Bank.

In case of any delay beyond 3(three) months, Bank shall issue notice of termination.

18 Annexures:

Annexure 01 Covering Letter

REF NO.: ACAB/HO/IT/Cyber Security/72 Dated 23-01-2023

The Managing Director
The Assam Co-operative Apex Bank Ltd.
Head Office: Hem Barua Road, Panbazar, Guwahati, Assam
Pin – 781001

Sub:: Covering Letter

Sir,

Having examined the RFQ (REF NO.: ACAB/HO/IT/Cyber Security/72 Dated 23-01-2023) including all annexures, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to deliver services in conformity with the said RFQ and in accordance with our proposal and total cost indicated in the Commercial Bid and made part of this proposal.

We undertake, if our quotation is accepted, to deliver services and complete the project in accordance with the scheduled timelines.

We agree to abide by this quotation for the period of180 days and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

We understand that the bank is not bound to accept the lowest or any bid the bank may receive.

Yours faithfully,

Place:

Dated: this ____day of 20___.

……

(Signature)

Seal:

Annexure 02: Bidder's Information

Name of the Bidder	
Constitution & Year of Establishment	
Registered Office/Corporate office Address	
Mailing Address	
Name and designations of the persons authorized to make commitments to the Bank	
Telephone: Fax: e-mail:	
Name & Addresses of Directors/Promoters	
Details of Organization Structure	
Description of business, service profile & client profile	
Gross annual turnover of the bidder (not of the group): Amount in INR Crore 2019-20: 2020-21: 2021-22:	
Net Profit of the bidder (not of the group): Amount in INR Crore 2019-20: 2020-21: 2021-22:	
Permanent Account Number	
GST Number	

DECLARATION

We hereby declare that the information submitted above is complete in all respects and true to the best of our knowledge. We understand that in case any discrepancy or inconsistency or incompleteness is found in the information submitted by us, our application is liable to be rejected.

Place:

Date:

SEAL

(Authorized Signatory)

Annexure 03: Conformity letter

Conformity with Hardcopy Letter

REF NO.: ACAB/HO/IT/Cyber Security/72 Dated 23-01-2023

The Managing Director
The Assam Co-operative Apex Bank Ltd.
Head Office: Hem Barua Road, Panbazar, Guwahati, Assam
Pin – 781001

Sir,

Sub: Supply and Installation of Enterprise Anti-Virus Software Licenses

Further to our proposal dated _____, in response to the Request for Quotation issued by The Assam Co-operative Apex Bank Ltd. ("Bank") we hereby covenant, warrant and confirm as follows:

The soft-copies of the proposal submitted by us in response to the RFQ issued by the Bank, conform to and are identical with the hard-copies of aforesaid proposal required to be submitted by us, in all respects.

Yours faithfully,

Dated: this ____ day of 20___.

……

(Signature)

S e a l :

Annexure 04: Functional and Technical Specification

Sr. No.	Particulars	Bidder's Compliance (F/N)	Bidder Remarks, if any
1	The Solution should provide 5-layers of protection into a single agent.		
1.1	Network threat protection should analyze incoming data and blocks threats while they travel through the network before hitting the system. Rules-based firewall and browser protection should be included to protect against web-based attacks.		
1.2	Signature-based antivirus should eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits etc.		
1.3	Correlate different linkages between users, files, and websites to detect rapidly mutating threats. By analyzing key file attributes, The solution should accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks.		
1.4	Have artificial intelligence to provide zero-day protection and stop new and unknown threats by monitoring more than 1000 file behaviors while they execute in real-time to determine file risk.		
1.5	Remediation and side effect repair engine should aggressively scans infected endpoints to locate Advanced Persistent Threats and remove tenacious malware. Administrator should remotely be able to trigger this and remedy the infection remotely from the management console.		
2	The Solution should check for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system.		
3	The solution should enhance protection for business critical systems by only allowing to run or by blocking blacklisted applications (known to be bad) from running. Finger printing of all applications should from centralized console.		
4	The solution should help prevent internal and external security breaches by monitoring application behavior and controlling file access, registry access, processes that are allowed to run, and devices information can be written to.		
5	The solution should allow administrator to run custom scripts on their endpoints to verify and report compliance; quarantine location and peer-to-peer enforcement lockdown and isolate a non-compliant or infected system.		
6	The solution should automatically detects what location a system is connecting from, such as a hotspot, wireless network, or VPN and adjusts the security to offer the best protection for the environment.		
7	The solution should have the ability to find whether the endpoint is out of compliance and should accomplish remediation, either via self-contained capabilities or integration with external resources		
8	The solution should automatically engage in an aggressive scan mode if it detects large number of malware or high-risk threats on windows		

Sr. No.	Particulars	Bidder's Compliance (F/N)	Bidder Remarks, if any
	clients.		
9	The solution should auto-compile, auto-protect when the operating system kernel is not compatible with precompiled auto-protect kernel module especially for Linux variants.		
10	The solution should have incident investigation and response utilizing the integrated EDR capabilities in endpoint protection		
11	If any endpoint is having more than three days older virus definition and if such endpoint tries to connect the network, then the solution must immediately install latest virus definition by connecting to the endpoint management server and blocking all connections to the other network resources like internet, intranet applications etc.		
12	If the host is non-compliant with the policies, the solution must automatically initiate remedial action, which may include running isolating it from network, downloading and executing/inserting a software, running scripts, by setting required registries keys. The solution should recheck host for compliance after remediation and grant access for the compliant host to the network.		
13	The solution must be able check whether required software, security patches and hot fixes have not been installed on the endpoint as mandated by organization, the solution should be set to connect to an update server to download and install the required software based on the policy.		
14	The solution must have reports that incorporate multi-dimensional analysis and robust graphical reporting in an easy-to-use dashboard.		
15	The solution must have group update provider reduces network overhead and decreases the time it takes to get updates by enabling one client to send updates to another, enabling more effective updates in remote locations.		
16	The solution should pre-emptively block exploits using heap spray techniques, abuse of java security manager etc. and must be signature-less and works regardless of flaw/bug/vulnerability		
17	Solution should collect and share the threat intelligence from / to external sources using industry formats such as STIX ,TAXII, etc.		
18	Solution should detect command and control traffic activity with IP level events, URL events, and DNS activity using detection mechanisms like static analysis, behavioral analysis, and reputation analysis from intelligence network.		
19	The solution should utilize multiple detection approach by combining virtualization and emulation to capture more malicious behavior across a wider range of custom environments.		
20	The solution should use a combination of static and dynamic analysis techniques to unmask cleverly disguised malware. It should detect packed malware and VM-aware ones that alter their behavior in an artificial environment.		
21	Solution should have dashboard to include the latest high risk tasks,		

Sr. No.	Particulars	Bidder's Compliance (F/N)	Bidder Remarks, if any
	search capabilities, recent samples, multiple processing stats, e.g. queue size, sandbox execution time, event count, tasks complete, and risk scores over say last 24 hours		
22	The solution must prevent clients from downloading full definition packages.		
23	The solution should manage single license for windows (Windows 8 and above), linux(Ubuntu 11.04 and above) and mac Operating Systems and management server should not be separate.		
24	The solution should detect malware that evades detection by using polymorphic custom packers by unpacking in a light weight virtual environment with no performance over-head.		
25	Solution should provide anomaly detection to detect and report on suspicious information found in a file. Preferable capabilities to include, TLS callback activity, CVE and exploit detection, shell-code detection, debugger detection, watermark tampering, and non-standard file alignment, RFC compliant etc.		
26	The solution should set up peer-to-peer authentication policy, which can grant or block inbound access to the remote computers that have the client installed.		
27	The Solution should provide manage windows, Linux and mac agents from same centralized console.		
28	The solution should download content updates from the central server when computers are idle so that it does not affect bandwidth		
29	If the endpoint client detects a network attack, solution must automatically activate active response to block all communication to and from the attacking computer		
30	The solution should have the ability to find whether the endpoint is out of compliance and should accomplish remediation, either via self-contained capabilities or integration with external resources		
31	The Solution must have a layer of protection that enables organization to go on the offensive and lure attackers out of hiding and reveal attacker intent and tactics via early visibility, so that the information can be used to enhance security posture.		
32	The solution should provide incident investigation and response utilizing the EDR capabilities in endpoint.		
33	The solution's EDR should be able expose advanced attacks with precision machine learning, behavioral analytics and threat intelligence minimizing false positives.		
34	The Solution should provide report over email, CSV, html or pdf.		
35	The solution should be in the leaders quadrant of latest Gartner Report for endpoint security.		
36	Solution should be able to do Real time virus detection, cleaning/quarantine.		
37	Solution should be able to do Heuristic scanning to allow rule-based detection of unknown viruses.		

Sr. No.	Particulars	Bidder's Compliance (F/N)	Bidder Remarks, if any
38	Solution should be able to quarantine files and files should be available in Quarantine Manager.		
39	Scanning of compressed file archives in ZIP, JAR etc. formats. Protection from viruses hiding in compressed files, such as Internet downloads and e-mail attachments.		
40	Solution should be able to do Proactive protection against zero-day threats.		
41	Solution should have the Facility of Vulnerability analysis tool.		
42	Solution should have the ability to Scan CD ROM and other external Drives automatically in real-time when accessed.		
43	Solution should have functionality of Central management console to centrally control desktop configurations, including scanning and cleaning options.		
44	Solution should have Centralized Audit trail logging and reporting capability with ability to communicate the reports using email.		
45	Solution should have Role based administration of the solution.		
46	Solution should have the ability to Real-time lock down of client configuration - allow or prevent users from changing setting or unloading/uninstalling the software.		
47	Solution should Automatic downloads of latest virus signature updates from the Internet to desktops and servers, across different platform running Windows. The distribution should happen seamlessly from a single management console.		
48	Solution should Remote deployment of Client software using Web-based installation/remote installation/ Log-in script/Client Packager.		
49	Solution should have ability to force an update (PUSH) to client.		
50	Solution should have an in built feature for Device control.		
51	Solution should Support for additional features like Desktop Firewall, Intrusion Prevention System etc.		
52	Solution should support Parental Control application.		
53	Solution should have 24x7 Technical Customer Care Support.		
54	The Antivirus must be compatible/support to run on Operating systems like Windows server 2012/2016/2019/2022.		
55	Antivirus should protect their own program files.		
56	Reporting of total system information to troubleshoot the problems and Web based Secured Management Console.		
57	Solution should Block auto play of USB device.		
58	The Antivirus solution must be able to auto quarantine or auto delete spyware without end user intervention.		
59	Prevent malicious website and prevent dangerous downloads from spreading malware & SPAM.		
60	Endpoint should Detect attackers by luring them into a decoy minefield		
61	Endpoint should Coax them into revealing their intent, tactics, and		

Sr. No.	Particulars	Bidder's Compliance (F/N)	Bidder Remarks, if any
	targets–so you can adapt your security posture.		
62	Endpoint should Bait the trap by simply flipping a switch.		
63	Endpoint solution should Lock down endpoints by specifying which applications can/cannot run with smart Application Control.		
64	Enable safe download and use of any app with Application Isolation		
65	Beat crippling ransomware and unknown attacks with a combination of signature less and critical endpoint technologies.		
66	Maximize protection and minimize false positives with machine learning technologies		
67	Block zero-day attacks that prey on memory-based vulnerabilities in popular applications.		
68	Solution should have a single agent for Anti-Virus and EDR capability		
69	The proposed solution must support SNMP, Syslog, etc. for integration with all leading SIEM/SOC solutions.		

Annexure 05: Manufacturer's Authorization Form

Note: This authorization letter should be printed on the letterhead of all the original equipment manufacturer (OEM) and should be signed by a competent person having the power of attorney to bind the manufacturer.

To,

The Managing Director
Assam Co-operative Apex Bank Ltd. Head Office, Pan Bazar
Guwahati – 781001

Dear Sir,

Sub: RFQ no. ACAB/HO/IT/XXXX Dated 23/01/2023

Dear Sir,

We _____ who are established and reputed manufacturer _____ having organization 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 RFQ.

We hereby extend our full guarantee and warranty as per terms and conditions of the RFQ and the contract for Software supply, installation, commissioning, services and support offered against this RFQ by the above firm.

Place:

Date: Seal and signature of the OEM

Annexure 06: Self declaration for Blacklisting

REF NO.: ACAB/HO/IT/Cyber Security/72 Dated 23-01-2023

The Managing Director
The Assam Co-operative Apex Bank Ltd.
Head Office: Hem Barua Road, Panbazar, Guwahati, Assam
Pin – 781001

Sir,

Sub: Self declaration for blacklisting

We hereby declare that we_____have not been blacklisted by any Co-operative Bank, Public Sector Bank, RBI, State Government or Central Government body or ministry.

Signature

Dated:this ____ dayof 20___.

……

(Signature)

S e a l :

Note: This should be submitted in the bidder's letter head and signed by the authorized signatory.

Annexure 07: Commercial Bill of Material

Sl no	Symantec Endpoint Protection – Enterprise Antivirus Software with 3 Years License and Support	Year 1 (Procurement)			Total Amount
		Qty	Rate (INR)	Amount	
1	Centralized Antivirus Server with all plugins /Components /addons, Management Server, Reporting features, etc. with 500 end-user licenses including implementation cost.	500	-	-	-

Note:

1. The implementation cost should be included with unit rate. At no point in time Bank will consider payment of implementation cost separately.
2. The prices, once offered, must remain firm and must not be subject to escalation for any reason within the period of validity. The price would be inclusive of all applicable taxes under the Indian law like customs duty, excise duty, import taxes, freight, forwarding, insurance, delivery, etc. exclusive of applicable GST
3. The Bidder is responsible for all the arithmetic computation & price flows. The Bank is not responsible for any errors in computation by the bidder.