Ref:APCOB/IT/1416904/2026-27
Date:23.04.2026

SHORT TENDER NOTICE

Procurement of Add-on Licenses for Sophos XDR Endpoint Security Solution

Preface

The Andhra Pradesh State Co-operative Bank Limited (APCOB) is one of the most respected and leading Bank in the State of Andhra Pradesh with 18 Branches in CRDA region of Andhra Pradesh State.

Objective of the RFP:

APCOB intend to issue Request for Proposal Document, hereinafter called as a Tender, Sealed tenders are invited from eligible and authorized vendors for Procurement of Add-on Licenses for Sophos XDR Endpoint Security Solution"for approximately 200 endpoints till Sep 2028

Ref: APCOB/IT/1416904/2025-26
Existing License No: LN1001709832

vendors who are eligible to participate in the competitive Tendering for providing following

Schedule:

Application Fee (Non refundable)	Rs 2000/-(Rupees Two thousand Only)
Bid Submission Start Date	23.04.2026
Bid Submission End Date	28.04.2026 @ 5:00 pm

Point of Contact for Bid Submission	Sri. M Vijay Kumar Dy. General Manager **The A.P.State Co.op Bank Ltd.,** NTR Sahakara Bhavan, Governorpet, Vijayawada 520002 Phone: 0866 2429094 e-mail: itinfra@apcob.org
Address for Tender Submission	Sri. M Vijay Kumar Dy. General Manager **The A.P.State Co.op Bank Ltd.,** NTR Sahakara Bhavan, Governorpet, Vijayawada 520002 Phone: 0866 2429094 e-mail: itinfra@apcob.org

- Bank reserves the rights for any changes in the tender like changes in bids notification, bids opening, evaluation of bids and vendors etc.

Scope of Work:

- Supply of add-on licenses for Sophos XDR endpoint security solution
- Licenses must be fully compatible with existing deployment and central console
- No separate console or parallel deployment should be proposed
- Subscription period: Till 25.09.2028

The Application shall have Anti-virus, Anti-malware, Ransomware protection, XDR and DLP.

The detailed scope of work is as follows:

S. No.	Technical Specifications	Compliance (Yes/No)
1	The Proposed solution should be an integrated advanced endpoint protection platform designed to Prevent organizations from being hacked, Detect the execution of malicious code, ransomwares, exploits, MBR attacks, and remove and block such imminent threats.	
2	Solution should offer Real-time Scanning for Local Files and Network Shares during Read & Write operation	
3	Solution must have its own proprietary scan engine.	
4	Solution must have the capability to exclude applications that are normally detected as Potentially Unwanted.	
5	Solution must have the application control lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office. Also, there should be option to request for addition of applications not present under app categories, if any.	
6	Solution should have feasibility to secure the uninstallation of antivirus client by user	

	without a password. This password should be unique for every machine and should be visible only to admin of the Management console. Also once used, the password should have a single click button/option to regenerate a random password again, so that same password cannot be used again.	
7	In case a machine is deleted from management console, solution should still provide functionality to re-protect such machine and should also have mechanism to retrieve respective uninstallation password.	
8	Solution should offer the real time protection to check the latest threat information from OEM online and should have the option to Automatically submit malware samples to OEM.	
9	Solution should offer security options to configure access to advertisements, uncategorized sites and risky downloads	
10	Solution should offer the below options for Risky downloads to the user- Allowed: Allows all risky file types. Warning: Warns the user that a file may be risky before they can download it. Blocked: Blocks all risky file types. Specify: This allows you to set a number of individual file types to Allow, Warn, or Block.	
11	Should be able to monitor files when they are accessed by a process (read/write)	
12	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.	
13	The polices should have option to either be configurable as device based or user based. Applied web filtering policies should follow	

	the user and be applicable on whichever device the user logs in and should not be device based.	
14	Proposed solution should show the alert description along with User & Device	
15	Solution should support command and control servers & Runtime Behavior Analysis / HIPS	
16	Solution must provide the Application Category, so as to block the Applications as required by the administrator.	
17	Solution must offer the Device Control/Peripheral control, with the Option of Read Only, Allow, Block access to the device.	
18	Solution must have the privilege to whitelist the USB device on the basis of Hardware ID.	
19	Solution should have the option to block the website on the category basis.	
20	Solution should have the flexibility of creating the policy on the basis of device or User.	
21	Solution should have the data loss prevention functionality	
22	Solution must have the privilege to block the usage of the applications like Torrents, VPN, Video Players, Proxy tools etc.	
23	Solution should have privilege to define the time based policies	
24	RBAC should be part of the solution. In addition to RBAC, all admins should have MFA functionality so that authentication into management console can be secured with dual layer. OTP for MFA should be either available on SMS/email or third part	

	OTP apps.	
25	Client should have a self-help tool to identify known issues within product if any, along with guided reference to solution, so that team can immediately rectify such issues and make sure security is intact	
26	Client should provide functionality to perform network connectivity test to corresponding update server management servers etc., to narrow down any troubleshooting related problems instantly	
27	Client should provide the functionality to simply drag and drop PE files for reputation checks, deep learning checks etc., to determine the characteristics of a suspected file in real time.	
28	Management console for endpoint should be cloud based for ease of access, but at the same time should be hosted within Indian jurisdiction i.e., OEM should mandatorily have data center hosted in India.	
29	Reports should have a scheduling option so that endpoint related reports can be received over the email in CSV, PDF formats. Also, such reports frequency should be configurable to weekly, monthly, daily.	
30	Solution should support robust API functionality to integrate with third part SIEM, RMM solution platforms.	
31	The proposed solution should have achieved 100% detection in the MITRE Ingenuity ATT&CK Evaluation.	
32	Must have a feature that groups together suspicious events reported to help in doing forensic work.	
33	Must have an option to manually create an	

	investigation.	
34	Must have the option to add notes.	
35	Must include information about the attack tactics and techniques used in the detected suspicious event.	
36	Must have the option to pivot data into a query or consult third-party threat analysis websites.	
37	Each investigation record must have an option to:	
38	Set priority	
39	Change status	
40	Assign the investigation to an admin account	
41	Must provide a command-line interface that can remotely access devices in order to perform a further investigation or take appropriate action.	
42	Must provide admins the capability to remotely connect to managed devices and get access to a command-line interface to perform actions such as:	
43	Reboot a device pending updates	
44	Terminate suspicious processes	
45	Browse the file system	
46	Edit configuration files	
47	Must have control over which specific admin accounts have Remote Access capability.	
48	Remote access sessions must be included in Audit Logs (when it started, ended or if	

	the connection was lost)	
49	Must be available on Windows, Mac, and Linux operating systems.	
50	Must provide security analysts, and IT admins the ability to run SQL queries to answer almost any question they can think of across their endpoints and servers.	
51	Must be based on OS Query that allows administrators to understand the current running state of a device.	
52	Solution must offer version control functionality to control the version of endpoint agents being deployed across organization.	
53	Must be able to quickly discover IT operations issues to maintain IT hygiene and ask detailed questions to hunt down suspicious activity via SQL queries.	
54	Must use powerful, out-of-the-box, fully-customizable SQL queries that can quickly search up to 90 days of current and historical on-disk data.	
55	Proposed solution should be quoted with three years subscription option for the above cited feature/functionalities.	
56	Solution must have adaptive protection capabilities that can automatically change the endpoint behavior to more aggressive during a malicious/suspicious activity and reduce the aggressiveness once the threat is eliminated.	
57	CSP platform where the security solution is hosted should be MEITY Approved in case of cloud endpoint security offering and datacenter should be within Indian jurisdiction.	
58	Solution should have Configuration Health	

	Score functionality that gives a quick insight in to the present severity level of configuration in comparison with global organizations of similar endpoint footprint. And should also suggest automatic fixes in case a configuration health score severity is identified as not optimum.	
59	XDR solution should also be hybrid in nature i.e., should have capability to integrate third party security products as well, to gather threat relevant telemetry from different sources for better co-relation and visibility.	

The support services will include the following:

- **Business-driven response priority** based on severity levels.
- **Problem resolution support** for troubleshooting and issue resolution.
- **24x7 global toll-free telephone support** for immediate assistance.
- **24x7 web support access and onsite support** whenever required by the Bank.
- **Transfer rights** for software usage as per licensing terms.

	INSPECTION	
	APCOB shall have the right to inspect or to test the product to confirm their conformity to the ordered specifications. The successful bidder shall provide all reasonable facilities and assistance to the inspector at no charge to APCOB. In case any inspected or tested products fail to conform to the specifications, APCOB may reject the same and successful bidder shall replace the rejected product with the products in conformity with the specification required free of cost to APCOB. Any delay due to above shall attract relevant penalty clauses of the tender.	
	PROJECT TIMELINESS	
	A time of 7 days will be given from the start of the contract period for completing the project.	
	Placement of Purchase Order (PO)	1 Day

	Acceptance of PO	1 DAY
	Signing of contract	5 DAYS
	Supply, Installation, Configuration of Products/Licenses and Commissioning of the services	7 DAYS
	RESPONSIBILITY OF BIDDER	
	Installation, Configuration Commissioning of Software. Submission of Invoice with proper relevant documents.	

1. **Consolidate Requirement:**

S. No.	Name of Work	Quantity
1.	Procurement of Add-on Licenses for Sophos XDR Endpoint Security Solution	200 Nos

Eligibility Criteria:

- The bidder must be a Registered Company and having its operations for a minimum period of 3 Years and bidder may be Registered Company/firm/MSME/LLC.
- Average Annual financial turnover during the last / Previous 3 years ending 31st March of 2025 should not be less than 10 Lakhs.
- Bidder must have its own valid PAN No. and GST Registration No. TIN & CIN registered in the state of Andhra Pradesh.
- L1 Bidder shall mandatorily submit the MAF from the OEM.
- Authorized partner/reseller of Sophos
- Experience in endpoint security solutions
- Presence in AP or Hyderabad,Telangana.

Other Terms and Conditions:

- Total cost inclusive of all taxes, service tax, and surcharge, if any, to be indicated.
- 100% Payment shall be made after completion of work and upon the submission of invoice along with the work completion report.

Technical Bid:

- Submit in a sealed envelope marked **"Technical Bid"**.
- Include compliance with specifications, signed eligibility documents, and no pricing information.

Commercial Bid:

- Submit in a separate sealed envelope marked **"Commercial Bid"**.
- Include price details and total cost.

Note:

1. Technical and Commercial Bids must be in separate envelopes.
2. **Only technically qualified bids** will move to the Commercial Bid opening.

Sd/-

Dy.General Manager(ITD)