RFI SPECIFICATION

COVER PAGE (SUMMARY)

BIDDERS MUST SUBMIT ANNEXURE 1 TOGETHER WITH THE INVITATION TO BID DOCUMENT

RFI No:	3126/2025
Description	Request for information (RFI) for provision of indicative pricing and price structure for Advanced Endpoint Security Solution
Publication Date	30 July 2025
Virtual Vendor Briefing Session	A Non-Compulsory Virtual Briefing Session will be held as follows: Date: 06 August 2025 Time: 11h00 am (South African Time) Venue: Online (Teams) Link: **Join the meeting now**
Closing Date for questions / queries	Date: 15 August 2025
Proposal Submission Address	Proposals will be accepted electronically via the following email address: tenders@sita.co.za
RFI Closing Details and Address	Date: 25 August 2025 Time: 11h00 am (South African Time) Email: tenders@sita.co.za
RFI Validity Period	N/A

PROSPECTIVE RESPONDENTS MUST REGISTER ON NATIONAL TREASURY'S CENTRAL SUPPLIER DATABASE PRIOR TO SUBMITTING RESPONSES.

Contents

ANNEX A: **INTRODUCTION**

1. PURPOSE AND BACKGROUND

1.1. PURPOSE

The purpose of this Request for Information (RFI) is to invite information/cyber security solutions Original Equipment Manufacturers (OEMs) (hereinafter referred to as “bidders”) to submit indicative pricing and pricing structure for Endpoint Security Solutions.

This RFI is solely for information gathering purpose and NOT to select or an award. The information collected in this fashion will not be used to lead to sourcing from one supplier only nor will it be used to write the ultimate specification in a matter that would suit just one specific supplier.

1.2. BACKGROUND

SITA published an RFI for Advanced Endpoint Security Solutions in May 2024. It is with this in mind that SITA is now requesting indicative pricing to provide a better service with the lowest possible price to our clients.

1.3 OBJECTIVE

The respondents to the Request for Information (RFI) are requested to submit detailed information for Advanced Endpoint Security Solutions within a

1.3.1 On-prem, Air-Gapped End-Point Protection with E/X/MDR

1.3.2 Cloud Services to enable SITA to establish Security as a Service capability E/X/MDR

The RFI scope is for the below capabilities but not limited.

1. Endpoint Protection (EPP)
2. Server Antivirus
3. eXtended Detection and Response (XDR)
4. Data Loss Prevention (DLP)
5. Network Detection and Response (NDR)
6. Email Security
7. Web Gateway

2. CONFIDENTIALITY

2.1 The information contained in this document is of a confidential nature, and must only be used for purposes of responding to this RFI. This confidentiality clause extends to all respondent(s) or associates whom you may decide to involve in preparing a response to this RFI.

2.2 For purposes of this process, the term "confidential information" shall include all technical and business information, including, without limiting the generality of the foregoing, all secret knowledge and information (including any and all financial, commercial, market, technical, functional and scientific information, and information relating to a party's strategic objectives and planning and its past, present and future research and development), technical, functional and scientific requirements and specifications, data concerning business relationships, demonstrations, processes, machinery, know-how, architectural information, information contained in a party's software and associated material and documentation, plans, designs and drawings and all material of whatever description, whether subject to or protected by copyright, patent or trademark, registered or un-registered, or otherwise disclosed or communicated before or after the date of this process.

2.3 The receiving party shall not, during the period of validity of this process, or at any time thereafter, use or disclose, directly or indirectly, the confidential information of SITA or the client (even if received before the date of this process) to any person whether in the employment of the receiving party or not, who does not take part in the performance of this process.

2.4 The receiving party shall take all such steps as may be reasonably necessary to prevent SITA and the client confidential information coming into the possession of unauthorised third parties. In protecting the receiving party's confidential information, SITA and the client shall use the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorised use or disclosure of the confidential information as the receiving party uses to protect its own confidential information.

2.5 Any documentation, software or records relating to confidential information of SITA or the client, which comes into the possession of the receiving party during the period of validity of this process or at any time thereafter or which has so come into its possession before the period of validity of this process:

a. Shall be deemed to form part of the confidential information of SITA or the client;
b. Shall be deemed to be the property of SITA or the client;
c. Shall not be copied, reproduced, published or circulated by the receiving party unless and to the extent that such copying is necessary for the performance of this process and all other processes as contemplated in; and
d. Shall be surrendered to SITA or the client on demand, and in any event on the termination of the investigations and negotiations, and the receiving party shall not retain any extracts.

3. Precedence of documents

3.1 This RFI consists of a number of sections. Where there is a contradiction in terms between the clauses, phrases, words, stipulations or terms and herein referred to generally as stipulations in this RFI and the stipulations in any other document attached hereto, or the RFI submitted hereto, the relevant stipulations in this RFI shall take precedence.

3.2 Where this RFI is silent on any matter, the relevant stipulations addressing such matter and which appears in the SITA Procurement Policy and Procedures shall take precedence. RFI shall refrain from incorporating any additional stipulations in its RFI submitted in terms hereof other than in the form of a clearly marked recommendation that SITA may in its sole discretion elect to import or to ignore. Any such inclusion shall not be used for any purpose of interpretation unless it has been so imported or acknowledged by SITA.

3.3 It is acknowledged that all stipulations in the SITA Procurement Policy and Procedures are not equally applicable to all matters addressed in this RFI. It however remains the exclusive domain and election of SITA as to which of these stipulations are applicable and to what extent. The bidders are hereby acknowledging that the decision of SITA in this regard is final and binding. The onus to enquire and obtain clarity in this regard rests with the bidders. The bidders shall take care to restrict its enquiries in this regard to the most reasonable interpretations required to ensure the necessary consensus.

4. Briefing and information session

4.1 A Non-compulsory virtual briefing session will be held on 06 August 2025.

5. Submission of documents

5.1 Bidders shall submit RFI response in accordance with the prescribed manner of submissions as specified below.

5.2 RFI responses must be submitted electronically to SITA at Tenders@sita.co.za on or before 25 August 2025 not later than 11h00 South African Standard Time (UTC+2).

5.3 Respondents are requested to complete their responses in electronic format, in the spaces provided for answers within this document.

5.4 All additions to the information documents i.e. appendices, supporting documentation, photographs, technical specifications and other support documentation covering suggested solutions etc. shall be submitted as part of this RFI. No product information or company profiles will be considered.

5.5 No information shall be accepted by SITA if submitted in any manner other than as prescribed above.

5.6 SITA will not be liable for any costs incurred by the respondents in the preparation of response to this RFI. The preparation of responses will be made without obligation to accept any of the suggestions included in any response, or to discuss the reasons why such suggestions were accepted or rejected.

6. TECHNICAL INFORMATION REQUEST

6.1 In the submission to the Request for Information the responded are requested to submit detailed indicative client pricing and pricing structure for the Advanced Endpoint Security Solutions.

Table 1 – Advanced Endpoint Security Solutions requirements

ITEM NR	TECHNICAL FUNCTIONALITY REQUIREMENTS	On-prem, Air-Gapped		Cloud Services Security as a Service	
		Recommended Retail Unit Price	SITA Economies of Scale	Recommended Retail Unit Price	SITA Economies of Scale
1	On-prem, Air-Gapped and Cloud Services End-Point Protection with EDR • Provide a single agent to include EPP, EDR and DLP • Support Major releases of enterprise Linux				

ITEM NR	TECHNICAL FUNCTIONALITY REQUIREMENTS	On-prem, Air-Gapped		Cloud Services Security as a Service	
		Recommended Retail Unit Price	SITA Economies of Scale	Recommended Retail Unit Price	SITA Economies of Scale
	- Apple MacOS - Android - Apple iOS" • Supports the mapping of the rules with MITRE ATT&CK framework techniques • The solution should support automatic file submissions to sandbox environment for malware analysis • The solution must be on-prem and air-gapped and fully functional • Detects and investigates security incidents and can remediate endpoints to pre-infection state. It includes data loss prevention, sandboxing, Endpoint firewalls, and endpoint detection and response • Management and reporting for deployment on-premises. • Integration to SIEM/ third party products • Endpoint Detection and Response – with guided investigations utilizing 30-days or more of historical endpoint data • Endpoint Security for Windows (with Adaptive Threat Protection) • Endpoint Security for Linux and MacOS • Endpoint Security for legacy systems and embedded type devices • Endpoint Security for Mobile (Android & iOS) • Local threat Intelligence Exchange • Data Encryption • Device Control • Application Control for PC's • End Point Protection for Insights for profiling "Top Attacks" with guidance to improve protection, and access to deploy Anti-Virus Strategic Innovation Alliance (SIA) partner products • Next Generation Antivirus (NGAV) = Endpoint-based threat detection, investigation, and response. This may include Endpoint Detection and Response (EDR) • Endpoint-based Exploit Prevention				

ITEM NR	TECHNICAL FUNCTIONALITY REQUIREMENTS	On-prem, Air-Gapped		Cloud Services Security as a Service	
		Recommended Retail Unit Price	SITA Economies of Scale	Recommended Retail Unit Price	SITA Economies of Scale
	• Endpoint-based host intrusion prevention system • File and folder access protection. • Endpoint-based web and browser control • Antivirus program to prevent and remove ransomware from all devices • Protection from Exploits (Zero-day, memory-based attacks etc.) • Agentless protection for isolated systems & unmanaged devices • Single Data-Lake • Flexible deployment options • Single natively integrated platform with disaster recovery/continuity options				
2	Server Anti-virus Protection • Endpoint Security for Servers including Adaptive Threat Protection module with Dynamic Application Containment and Real Protect • Application Control for Servers • Malware Detection and Prevention • Protection from Exploits (Zero-day, memory-based attacks etc.) • Data Loss Prevention • Protection Against Malicious Attacks • Endpoint Security Firewall Module				
3	Extended Detection and Response (XDR) • Advanced Extended Detection and Response (XDR) with capabilities to automatically collect and correlate data, telemetry across multiple security layers – Endpoints, Servers, (Windows, Linux and Mac) and Network. • Collects and correlates data across email, endpoints, servers, cloud workloads, and networks, enabling visibility and context into advanced threats. • Threats must be analysed, prioritized, hunted, and remediated to prevent data loss and security breaches				

ITEM NR	TECHNICAL FUNCTIONALITY REQUIREMENTS	On-prem, Air-Gapped		Cloud Services Security as a Service	
		Recommended Retail Unit Price	SITA Economies of Scale	Recommended Retail Unit Price	SITA Economies of Scale
	• The solution must comply with data residency and sovereignty rules of the organization, where collected data and files are analysed, correlated and stored locally on-premises in the customers data center that is air-gapped. For the avoidance of doubt, no files, detections logs, telemetry should be uploaded to the cloud for analysis or correlation. • For the transport of manual update files, the vendor must provide a secure USB device that scans the host PC for malware in an agent-less manner and scans the files for malware before allowing the files to be copied to the USB flash drive. • Single data lake that is on-prem and capable of functioning in an air-gapped environment.				
4	Network Detection and Response (NDR) • The NDR/network sensor should support the detection of suspicious/malicious behaviors reflected in the network from unmanaged devices connected to the network, including end user machines, mobile devices, printers and others (independent of the operating system of the device). • Solutions should be deployed on premises in an air-gapped environment along with on premise sandboxing capability and function fully. • The solution should support native integration with the XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors, endpoints, servers, and networks.				
5	WEB Gateway Protection • Web Security, Gateway edition software, gateway anti-malware, and content security reporter • Web Protection should enable the following functionality: category-based and reputation-based web filtering, anti-virus, proxy, cache, authentication, SSL scanning, content control, and gateway anti-malware with behavior analysis capabilities. • Decrypt and inspect TLS/SSL-encrypted data for hidden threats and then re-encrypt it for secure transmission if no threats are found.				

ITEM NR	TECHNICAL FUNCTIONALITY REQUIREMENTS	On-prem, Air-Gapped		Cloud Services Security as a Service	
		Recommended Retail Unit Price	SITA Economies of Scale	Recommended Retail Unit Price	SITA Economies of Scale
	• Parse the content for sensitive data (e.g., payment card numbers, proprietary information) and then block or alert on the discovery according to company policy. • Log user activity, threats, and policy violations for administrators to use for the purposes of monitoring, reporting, forensic analysis, etc.				
6	Email Gateway Protection Email Routing & Delivery • Directs incoming and outgoing emails to the appropriate destination (e.g. server or user). • Ensures email delivery to correct recipients using protocols like SMTP (Simple Mail Transfer Protocol). Spam Filtering • Identifies and blocks unwanted or unsolicited emails (spam) using various filtering techniques (e.g., keyword matching, Bayesian filtering, DNS blacklists). Virus and Malware Scanning • Scans email attachments and content for viruses, worms, trojans, and other malicious payloads. • Provides antivirus protection by checking for known threats using virus signature databases. Data Loss Prevention (DLP) • Monitors outgoing emails for sensitive information (e.g., credit card numbers, social security numbers) to prevent unintentional data leaks. Email Encryption • Encrypt email content to protect sensitive information during transit. • Supports technologies like TLS (Transport Layer Security) or end-to-end encryption. Attachment Management • Limits or blocks certain types of attachments that may pose a security risk (e.g., executable files, compressed files). • Can scan or strip attachments based on content type. Authentication & Authorization				

ITEM NR	TECHNICAL FUNCTIONALITY REQUIREMENTS	On-prem, Air-Gapped		Cloud Services Security as a Service	
		Recommended Retail Unit Price	SITA Economies of Scale	Recommended Retail Unit Price	SITA Economies of Scale
	• Ensures emails are sent by authorized senders (e.g., using SPF, DKIM, and DMARC). • Prevents email spoofing or impersonation attacks by verifying the legitimacy of the sender. Email Archiving • Automatically archives incoming and outgoing emails for compliance, retention, or later retrieval. • Supports long-term storage and quick retrieval of email data. Quarantine Management • Suspends potentially harmful emails for further review. • Allow administrators or users to review quarantined emails before release or deletion. Policy Enforcement • Enforce corporate policies for email use, ensuring compliance with legal or industry regulations (e.g., GDPR, HIPAA). • Controls outbound email content based on organization-defined rules. Reporting & Monitoring • Provides detailed reports on email traffic, security threats, and filtering performance. • Allows monitoring of email activity for suspicious behavior. Failover and Redundancy • Ensures continued email flow even in the event of network outages or server failures. • Provides backup servers and reroutes email in case of failures. Policy-based Routing • Directs emails through different routes based on pre-set rules or conditions (e.g., by region, user group, or email content type). Advanced Threat Protection (ATP) • Detects advanced threats like phishing, spear-phishing, and business email compromise (BEC). • Uses behavioral analysis and machine learning to identify and block sophisticated attacks				
7	DLP (Data loss Prevention/Protection) Solution • For laptops, desktops, and servers.				

ITEM NR	TECHNICAL FUNCTIONALITY REQUIREMENTS	On-prem, Air-Gapped		Cloud Services Security as a Service	
		Recommended Retail Unit Price	SITA Economies of Scale	Recommended Retail Unit Price	SITA Economies of Scale
	• End user device control, with support for: • Storage devices: CD/DVD, USB • Non-storage devices: COM and LPT ports, infrared and imaging devices, modems, PCMCIA card, print screen key. • Continuous data monitoring. • Web-based management console for policy configuration and deployment, consolidated endpoint reporting, fingerprint extraction, and updates • Record forensic data capture of DLP violations. • Apply granular device control policies to specific endpoints, to control/block access to unauthorized USB storage, 3G modems, and mobile devices. • "Be integrated in the following security Solution solutions with no additional hardware: a. Endpoint b. Mail Servers c. Messaging Gateway d. Web Gateway" • Provide visibility and control of data in motion. • Track and record sensitive data flowing through network egress points. • Detect and react to improper data use based on keywords, regular expressions, and file attributes. • Reduce administration through central management with central management console along with the endpoint and email DLP modules. • Provide out-of-the-box DLP templates satisfy major compliance regulations and ensure that Personally Identifiable Information (PII) and sensitive data files are protected. • Allows the organization to create custom templates and modify existing templates to suit our business requirements. • Support policy management that allows administrators to enforce preventative actions on messages based on scanning conditions. • Send notification to the sender of the email about the detention/modification of the message or the removal of attachments from it. • Provide Role Based Access Control (RBAC) capability				

ITEM NR	TECHNICAL FUNCTIONALITY REQUIREMENTS	On-prem, Air-Gapped		Cloud Services Security as a Service	
		Recommended Retail Unit Price	SITA Economies of Scale	Recommended Retail Unit Price	SITA Economies of Scale
	• Support DANE (DNS-based Authentication of Named Entities) to secure outbound messages by verifying SMTP server identity.				
8.	List of additional security solutions				

6.1. INTEGRATION REQUIREMENTS

No integration Requirement

6.2. TRAINING

Not Applicable

7. Contact details

The following contact details are applicable:

(a) For general enquiries contact cindy.kobe@sita.co.za

(b) For technical enquiries contact lyverne.prinsloo@sita.co.za

ANNEX B:**Terms and definitions**

1. ABBREVIATIONS

ICT Information and Communication Technology

SITA State Information Technology Agency

(1) DEFINITIONS

"Yes"	Indicates that this software is available in included in the supplier response. Provide confirmation that the listed features are available, subject to verification.
"No"	Indicates that this software is not available and excluded from the supplier response.