



**Annexure 1: BID SPECIFICATION: RFP 3112-2025**

**REQUEST FOR PROPOSAL FOR PROCUREMENT OF LICENSES OF AN ENDPOINT SECURITY SOLUTION FOR SITA CLIENT FOR PERIOD OF THREE (3) YEARS.**

**TECHNICAL, PRICING AND PREFERENCE POINTS REQUIREMENTS**

Contents

[1. Introduction and Background 3](#_Toc201931394)

[1.1 Purpose 3](#_Toc201931395)

[1.2 Background 3](#_Toc201931396)

[2. Scope of Bid 3](#_Toc201931397)

[2.1 Scope of Work 3](#_Toc201931398)

[2.2 Delivery addresses 4](#_Toc201931399)

[2.3 Customer Infrastructure and environment requirements 4](#_Toc201931400)

[3. Requirements 4](#_Toc201931401)

[3.1 Product / Service / Solution Requirements 4](#_Toc201931402)

[4. Bid Evaluation Stages 5](#_Toc201931403)

[4.1 Mandatory Administrative responsiveness (Stage 1) 6](#_Toc201931404)

[4.1.1 Attendance of briefing session 6](#_Toc201931405)

[4.1.2 Registered Supplier 6](#_Toc201931406)

[4.1.3 Bid Submission Instructions 6](#_Toc201931407)

[4.2 Technical returnable documents 7](#_Toc201931408)

[4.2.1 Instruction and evaluation criteria 7](#_Toc201931409)

[4.2.2 Technical mandatory requirements (Stage 2) 7](#_Toc201931410)

[4.3 Technical Functionality evaluation Requirements (Stage 3) 11](#_Toc201931411)

[4.4 Technical Proof of Concept (Demonstration) Requirements (Stage 4) 23](#_Toc201931412)

[4.5 Special Conditions of Contract Verification (Stage 5) 37](#_Toc201931413)

[4.5.1 Special Conditions of Contract 38](#_Toc201931414)

[4.5.2 Declaration of compliance and acceptance SCC 45](#_Toc201931415)

[4.6 Price and Preference Points Evaluation (Stage 6) 45](#_Toc201931416)

[4.6.1 Costing and Preference Evaluation 45](#_Toc201931417)

[4.6.2 Costing and Pricing Conditions 45](#_Toc201931418)

[4.6.3 Rate of Exchange Pricing Information 46](#_Toc201931419)

[4.6.4 Bid Exchange Rate Conditions 47](#_Toc201931420)

[4.6.5 Declaration of Acceptance 47](#_Toc201931421)

[Annex A: Bidder substantiating evidence 53](#_Toc201931422)

[5. Technical Mandatory Requirement Evidence 53](#_Toc201931423)

[5.1 Bidder Certification / Affiliation requirements 53](#_Toc201931424)

[5.2 Bidder experience and capability requirements 53](#_Toc201931425)

[5.3 On-prem air gapped capability requirements 54](#_Toc201931426)

[5.4 OEM/OSM Rating Requirements 54](#_Toc201931427)

[5.5 Data residency and sovereignty requirements 54](#_Toc201931428)

[5.6 Single solution requirements 54](#_Toc201931429)

[5.7 OEM/OSM Presence Requirement 55](#_Toc201931430)

[5.8 Special Conditions of Contract 55](#_Toc201931431)

[5.10 Technical/Product Functional Requirement 55](#_Toc201931432)

[5.11 Technical Functionality Requirements 55](#_Toc201931433)

[5.12 Technical Proof of concept (Demonstration)Requirements 55](#_Toc201931434)

[5.13 Preference Points Preferential Goals Evidence 55](#_Toc201931435)

[Annex B: THIRD-PARTY RISK MANAGEMENT (TPRM) ASSESSMENT 57](#_Toc201931436)

[Annex C: Product/Service functional Requirements. ADDENDUM 1 63](#_Toc201931437)

# Introduction and Background

## Purpose

The purpose of this RFP is to invite suppliers (hereinafter referred to as “bidders”) to submit bids for the supply and implementation of Endpoint security solution, with maintenance and support for a period of three (3) years.

## Background

A SITA client submitted a tasking for the supply and implementation of Endpoint Security Solution for protection against ransomware. The ideal solution should enable robust threat prevention, detection, and response capabilities while offering centralized management, scalability, and seamless integration with existing systems. The solution must also have on-prem air-gapped XDR and needs to mitigate the risks associated with the protection and security of sensitive data on endpoint devices. The solution needs to provide visibility into:

* Single Central Management console
* Reporting
* On-premises deployment
* On-premises air gapped (XDR) Extended detection and response with guided investigations of historical endpoint data.
* Endpoint security with EDR for Windows, Linux, MacOS, and Android, iOS
* Device and application control
* Extended Detection and Response
* Data Loss Prevention
* Network Detection and Response (NDR)
* Single console
* Multi-Tenancy
* multiple networks with different security levels
* Threat Intelligence
* Attack Surface Risk Management & Reduction
* Forensics
* Mobile Security

# Scope of Bid

## Scope of Work

The scope of work for End Point Security it’s to planning, design, supply, installation, configurations and migration of the current endpoint solution with maintenance and support for the period of three (03) years.

The following services further needs to be addressed within the scope:

1. The successful bidder must be able to provide End Point security services.
2. The Bidders Level partnership with the OEM/OSM must include installation, configuration, maintenance and support.
3. The planning, design, supply, installation and configurations of End Point security solution as per technical specifications functionalities.
4. Every requirement specification is substantiated by evidence as proof of compliance.
5. Migration solution from old to new solution.
6. Onsite (On-Prem) Monitoring Tool with Software Licence’s.
7. The Bidder must be accredited with the OEM/OSM for technical support.

**NOTE 1:**

**Successful Bidder must consider a cost-free transitioning period as follows:**

1. **No billing for duration of transitioning into the new product to assist the client to avoid paying for two products with the same functionality.**
2. **Email gateway will only be implemented when the existing contract concludes in March 2027, Bidders must only cost the Email gateway from F/Y 27/28**

## Delivery addresses

Table 1: Delivery addresses

|  |  |  |
| --- | --- | --- |
| **No.** | **Business name** | **Physical address** |
|  | SITA | SITA 459 Tsitsa street,  Erasmuskloof,  Pretoria 0102 |

## Customer Infrastructure and environment requirements

Information on the environment and system functionality as indicated below:

* 1. Active directory 2016
  2. Exchange server 2016/2019
  3. SQL Server 2014, 2016
  4. 180 + Active Directory sites.
  5. 3000 + physical and virtual servers.
  6. 29000 End-user devices.
  7. 3000 + Computer objects (Excluding servers).
  8. No internet access to the environment. (Ringfenced)
  9. Other Server operating systems: 2012 R2/2016 Standard
  10. Desktop operating systems: Windows 7 and Windows 10/11 Pro and Enterprise.
  11. 9 Domino mail servers

# Requirements

## Product / Service / Solution Requirements

|  |  |
| --- | --- |
| **Product/service** | **Quantity** |
| End User Devices Antivirus Protection (End Point Protection) with EDR | 26 000 |
| Server Antivirus Protection | 3000 |
| Extended and Detection Response (XDR) Protection On-prem, Air gapped (Servers, Endpoints, and network) | 29 000 |
| Network Detection and Response (NDR) | 3 |
| Web Gateway Protection Software | 2 000 |
| Email Gateway Security Protection | 4 000 |
| DLP (Data Loss Prevention/Protection) | 29000 |
| Deployment and Migration of the Solution | Once Off |
| Highest OEM Support for maintenance and incident response | 3 Years |

**PROJECT DELIVERY SCHEDULE AND PERFORMANCE**

* 1. Support via telephone or on-site visits,
  2. Troubleshooting application queries,
  3. Troubleshooting analyser communication queries,
  4. Configuration queries on the application,
  5. Assisting in the training related to the application,
  6. Supply and installation of application,
  7. Implementation of the solution,
  8. Free updates which address bug fixes, performance issues and ease of use of the application,
  9. Critical issues response time (e.g. total system failure) – 4 hours, from time off call received, or advise client if the problem is external (e.g. Network failure),
  10. Non-Critical issues response time (e.g. analyser communication problems) – 24 hours, from time off call received, or advise client if the problem is external (e.g. Network failure),
  11. Maintenance services to ensure that support is available 24hours, 7days per week and 52 weeks per year for the support calls logged by SITA,

**2. SERVICE DELIVERY SCHEDULE AND PERFORMANCE METRICS**

* 1. Non-Critical issues response time (e.g. analyser communication problems) – 24 hours, from time off call received, or advise client if the problem is external (e.g. Network failure),
  2. Maintenance services to ensure that support is available 24hours, 7days per week and 52 weeks per year for the support calls logged by SITA,

# Bid Evaluation Stages

The bid evaluation process consists of several stages, according to the nature of the bid. A bidder must qualify for each stage to be eligible to proceed to the next stage of the evaluation. The stages are:

Table 2: Bid Evaluation Stages

|  |  |  |
| --- | --- | --- |
| **Stage** | **Description** | **Applicable for this bid YES/NO** |
| Stage 1 | Mandatory Administrative responsiveness | YES |
| Stage 2 | Technical Mandatory responsiveness | YES |
| Stage 3 | Technical Functional Requirements | YES |
| Stage 4 | Technical Proof of Concept (Demonstration) Requirements | YES |
| Stage 5 | Special Conditions of Contract verification | YES |
| Stage 6 | Price / Preference points | YES |

## Mandatory Administrative responsiveness (Stage 1)

### Attendance of briefing session

1. A **Compulsory Physical briefing session** will be held. The bidder must sign the briefing session attendance register using the same information (bidder company name, bidder representative person name and contact details) as submitted in the bidder’s response document. Any bidder who fails to attend the compulsory briefing session will be disqualified.

**NOTE (1):**

Bidder who wishes to attend the **Compulsory Physical Briefing session** needs to notify the responsible Specialist indicated in the Bid Document of attending the session. The details of the Compulsory Physical Briefing session will then be sent to those Bidders.

**NOTE (2):**

Bidders will be required to sign a Non-Disclosure Agreement (NDA) to obtain any further relevant site or current equipment details before the information will be provided.

**NOTE (3):**

Any Bidder who fails to attend the **Compulsory Physical Briefing session** will be disqualified.

### Registered Supplier

1. Only responses from bidders who are registered as a Supplier on National Treasury’s Central Supplier Database (CSD) in terms of National Treasury’s Instruction Note 4A of 2016/17 will be considered for award on this RFP.
2. In the case of joint ventures or consortiums the bidder must demonstrate that at least one of the parties to the bid response attended the briefing session
3. **Bidders need to complete all the SBD documents which needs to be submitted as stated in the Invitation to Bid Document.**

### Bid Submission Instructions

**Note that a Two Envelope process will be followed and therefore bidders must submit as follows:**

1. **One (1) original file excluding pricing** which must be submitted in **a separate envelope**;
2. **One (1) hard copy excluding pricing** which must be submitted in **a separate envelope**;
3. **One (1) electronic copies on USB memory stick/ flash drive** in Portable Document Format (**PDF) of the RFP Document and Technical / Functionality Response.**
4. **One (1) electronic copies on USB memory stick/ flash drive** in Portable Document Format **(PDF)** **of pricing only**.
5. It is the Bidder’s responsibility to ensure that the information and contents on the electronic copies is the same as in the hard copies.
6. To ensure that the electronic copies are not damaged, the bidder must submit the USB’s (memory stick/ flash drive) in a sealed padded envelope and be clearly marked.
7. Bidders shall submit Bid responses in accordance with the prescribed manner of submission as specified above. **Failure to comply with the above instructions on submitting a proposal will lead to disqualification.**
8. The **RFP** Responses (hard and electronic copies) must be clearly marked as follows: Bidder’s Name & Contact Details, **RFP** Number, **RFP** Description, and Closing Date.
9. All Bids in this regard shall only be accepted if they have been placed in the tender box before or on the closing date and stipulated time.
10. Late bids shall not be considered.
11. The Bid response must be signed by an authorised employee, agent or representative of the bidder. The Bid response Bid must bear the initials of the signatory at the bottom of every page as an indication that the bidder has familiarised itself with the terms and conditions of this **RFP** document.
12. Faxed or e-mailed bids will not be accepted.
13. Bidders shall submit Bid responses in accordance with the prescribed manner of submission as specified in this document. **Failure to comply with the bid submission requirements will lead to disqualification.**
14. Bidders are required to submit all returnable documents/information together with their Bids/proposals on or before the closing time and date of the Bids/proposals.
15. All services supplied in accordance with the bidder’s proposal must be in accordance with all applicable legal requirements in terms

## Technical returnable documents

### Instruction and evaluation criteria

1. The bidder must comply with ALL the requirements as per the Technical Mandatory Requirements below by providing substantiating evidence in the form of documentation or information, failing which it will be regarded as “NOT COMPLY”.
2. The bidder must provide a unique reference number (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response.
3. The bidder must comply with ALL the TECHNICAL MANDATORY REQUIREMENTS in order for the bid response to proceed to the next stage of the evaluation.

### Technical mandatory requirements (Stage 2)

Table 3: Technical Mandatory Requirements

| **Mandatory Requirements** | **Substantiating evidence of compliance (used to evaluate bid)** | | | **Evidence reference (to be completed by bidder)** |
| --- | --- | --- | --- | --- |
| **BIDDER CERTIFICATION/ AFFILIATION REQUIREMENTS** | | | | |
| The Bidder **must** be an Original Software Manufacturer (OSM)/ Original Equipment Manufacturer (OEM), or accredited as Partner/ Reseller **to provide licences of an Endpoint Security Solution to a minimum of 3000+ users in the past five (05) years from the publication of this bid.** | Attach to **ANNEX A** a copy of valid documentation (letter/certificate/license) as proof that the Bidder is an Original Software Manufacturer (OSM)/ Original Equipment Manufacturer (OEM) or accredited as a Reseller/ Partner to provide **a to provide licences of an Endpoint Security Solution to a minimum of 3000+ users in the past five (05) years from the publication of this bid.**  **NOTE (1):**  Original Equipment Manufacturers (OEM)/Original Software Manufacturers (OSM) using reseller model are not eligible to participate for this bid.  **NOTE (2):**  SITA reserves the right to verify the information provided. | | | <provide unique reference to locate substantiating evidence in the bid response – see Annex A, section 5.1> |
| 1. **BIDDER EXPERIENCE AND CAPABILITY REQUIREMENTS** | | | | |
| The Bidder **must** have provided, designed, planned, tested, maintained, supported and deployed **licences of an Endpoint Security Solution to a minimum of 3000+ users in the past five (05) years from the publication of this bid.** | The Bidder **must** complete **table** **14** by providing reference details from at least two (2) customers to whom **licences of an Endpoint Security Solution was designed, planned, tested, maintained, supported and deployed to a minimum of 3000+ users in the past five (05) years from the publication of this bid.**  **NOTE (1):**  The Bidder **must provide** the following information when completing **table 14:**   * 1. Company name; **and**   2. Reference Person Name, Tel **and/or** email; **and**   3. Project Scope of Work; **and**   4. Project Start and End-date.   **NOTE (2):**  Failure to comply **fully** to the requirements as indicated above will result in disqualification.  **NOTE (3):**  SITA reserves the right to verify information provided. | | | <provide unique reference to locate substantiating evidence in the bid response – see Annex A, section 5.2> |
| 1. **ON PREM AIR GAPPED CAPABILITY REQUIREMENTS** | | | | |
| The solution must perform all the specified functions in an **air-gapped** environment and allow for multi-tenancy.  Endpoint Protection (EPP)  extended Detection and Response (XDR)  Data Loss Prevention (DLP)  Network Detection and Response (NDR)  Email security  Web Gateway  IOC (Indicators of Compromise) | Signed letter from OEM/OSM confirming that the listed functions are available on-premises and can function **air-gapped**:  Endpoint Protection (EPP)  Extended Detection and Response (XDR)  Data Loss Prevention (DLP)  Network Detection and Response (NDR)  Email security  Web Gateway  IOC (Indicators of Compromise)  **Note:** SITA reserves the right to verify the information provided. | | | <provide unique reference to locate substantiating evidence in the bid response – see Annex A, section 5.3> |
| 1. **OEM/OSM RATING REQUIREMENTS** | | | | |
| OEM/OSM of the proposed solution must be a leader on the Gartner Magic Quadrant / Forrester Wave for End-Point Protection. | Provide the Gartner Magic Quadrant/Forrester Wave for End-Point Protection for 2025 to validate the OEM/OSM position.  **Note:** SITA reserves the right to verify the information provided. | | | <provide unique reference to locate substantiating evidence in the bid response – see Annex A, section 5.4> |
| **5. DATA RESIDENCY AND SOVEREIGNTY REQUIREMENT** | | | | |
| The Bidders 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 compliance with the organization’s data sovereignty and compliance laws. | Provide the letter that confirms that 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 compliance with the organizations data sovereignty and compliance laws.  **Note:** **SITA reserves the right to verify the information provided**. | | | <provide unique reference to locate substantiating evidence in the bid response – see Annex A, section 5.5> |
| **6. SINGLE SOLUTION REQUIREMENTS** | | | | |
| The solution must provide all the functionality from a single OEM/OSM:   * Endpoint Protection (EPP) * eXtended Detection and Response (XDR) * Data Loss Prevention (DLP) * Network Detection and Response (NDR) * Email security * Web Gateway * IOC | Provide a letter that confirms that all the functionality is provided by a single OEM/OSM.   * Endpoint Protection (EPP) * eXtended Detection and Response (XDR) * Data Loss Prevention (DLP) * Network Detection and Response (NDR) * Email security * Web Gateway * IOC   **Note:** **SITA reserves the right to verify the information provided.** | | | <provide unique reference to locate substantiating evidence in the bid response – see Annex A, section 5.6> |
| **7.** **OEM/OSM PRESENCE REQUIREMENT** | | | | |
| OEM/OSM or accredited Partner/Reseller should have a local commercial, technical and support teams (available within the borders of the country). | OEM/OSM or accredited Partner /Reseller must provide their local proof of address in the form of lease agreement or three months utilities bill not older than three months.  **Note:** **SITA reserves the right to verify the information provided**. | | | <provide unique reference to locate substantiating evidence in the bid response – see Annex B, section 5.7> |
| **8. SPECIAL CONDITIONS OF CONTRACT ACCEPTANCE** | | | | | |
| Bidder **must accept ALL** the Special Conditions of contract | | The Bidder **must accept ALL** the Special Conditions of Contract by completing and signing the declaration of Acceptance in the Declaration of Compliance and Acceptance under the Special Conditions **(Section 4.5.2).**  **NOTE (1):**  Failure to complete and sign the SCC in **section 4.5.2** will result in disqualification. | <provide unique reference to locate substantiating evidence in the bid response – **see** ANNEX A, paragraph 5.8**>** | | |
| **9. THIRD PARTY RISK ASSESSMENT** | | | | | |
| The Bidder must confirm compliance to Third-Party Risk Management Assessment. | | The Bidder must comply to the Third-Party Risk Management Assessment requirement by completing All the questions in **Annex B.**  **NOTE (1):**  SITA reserves the right to verify information provided.  **NOTE (2):**  Failing to complete all the questions or not Accepting the Declaration of Acceptance above will result in disqualification. | <Provide unique reference to locate substantiating evidence in the bid response – see **Annex A par 5.11 and** **Annex B**> | | |
| **10.** **TECHNICAL PRODUCT / SERVICE FUNCTIONAL REQUIREMENTS** | | | | | |
| **The Bidder must confirm compliance to the Technical/Product Functional Requirements** | | The Bidder must confirm that they comply with the **Product/Service Functional Requirements** by completing **Annex C: Addendum 1**.  **NOTE (1):**  Failure to comply fully to the requirements as indicated above will result in disqualification.  **NOTE (2):**  SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – see Annex A, paragraph 5.10 and Annex C: Addendum 1**>** | | |

## Technical Functionality evaluation Requirements (Stage 3)

1. The Bidder must complete in full all the TECHNICAL FUNCTIONALITY requirements.
2. The Bidder **must provide a unique reference number** (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response. During evaluation, SITA reserves the right to treat substantiation evidence that cannot be located in the bid response, as “NOT COMPLY”.
3. The evaluation (scoring) of bidders’ responses to the requirements will be determined by the completeness, relevance and accuracy of substantiating evidence
4. Weighting of requirements: The score for the desktop evaluation of TECHNICAL FUNCTIONALITY REQUIREMENTS will be calculated as follows:
5. Each Bidder will be evaluated on each individual requirement as indicated in table 4 and 5 below. The value scored for each requirement will be multiplied with the specified weighting for the relevant requirement to obtain the percentage achieved for each requirement.
6. SITA reserves the right to verify information / evidence provided by the Bidder.

**Table 4:** Technical Functionality Evaluation Rating Scale

| **Evaluation criteria** | **Score** |
| --- | --- |
| Irrelevant (Does not meet the minimum requirement) | 0 |
| Good (Meets the minimum requirements) | 3 |
| Excellent (Exceeds the minimum requirements) | 5 |

(a) **Weighting of requirements:** The score for the desktop evaluation of TECHNICAL FUNCTIONALITY REQUIREMENTS will be calculated as follows:

**Table 5:** Technical Functionality Weighting Requirements

|  |  |  |
| --- | --- | --- |
| **No.** | **Technical Functionality requirements** | **Weighting** |
| **BIDDER’S CAPABILITY** | | |
| 1. | On-prem, Air-Gapped End-Point Protection with EDR | 15% |
| 2. | Servers Antivirus Protection (Including virtual servers) | 15% |
| 3. | On-prem, Air-Gapped Extended and Detection Response (XDR) Protection (Servers, Endpoints) | 15% |
| 4. | Network Detection and Response (NDR) | 15% |
| 5. | Web Gateway | 15% |
| 6. | Email gateway | 10% |
| 7. | DLP (Data loss Prevention/Protection) Solution | 15% |
| TOTAL | | 100% |

1. **Minimum threshold**. To be eligible to proceed to the next stage of the evaluation the bid must achieve a **minimum threshold overall score of 60%.**

**NOTE (1):**

The Bidder must achieve at least **60%** for each of the technical Functional requirement sections indicated in table above, failing which will result in disqualification.

**NOTE (2):**

SITA reserves the right to verify All the information provided.

**NOTE (3):**

Bidders should take note of the Minimum Requirements as well as the Minimum Threshold.

Should the bidder not meet the Minimum Requirements, or the Minimum Threshold the Bidder

Table 6: Technical Functionality Requirements

| **ITEM NR** | **TECHNICAL FUNCTIONALITY REQUIREMENTS** | **Scoring** | **Substantiating evidence and evaluation criteria**  **(used to evaluate bid)** | **Weighting** | **Substantiation reference**  **(to be completed by bidder)** |
| --- | --- | --- | --- | --- | --- |
| **1** | **On-prem, Air-Gapped End-Point Protection with EDR**  The Bidder must provide documentation indicating how the proposed product or solution complies with **ALL** **Core Technical Functionality Requirements** for Endpoint Protection   * Single agent to include EPP, EDR and DLP * All currently supported Microsoft Operating Systems   + Windows 11   + Windows Server 2012 - 20219 * Legacy Microsoft Operating Systems:   + Windows 7 - Windows 10   + Windows Server 2008 - Windows Server 2012 * Major releases of enterprise Linux   + 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 has the ability to 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. * 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 |  | Evidence:  The bidder must provide the product specification brochure, architecture design, or documentation indicating how the proposed product or solution complies with the technical requirements for End-user device protection with EDR.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **2** | **Servers’ Anti-virus Protection**  The Bidder must provide documentation indicating how the proposed product or solution complies with **ALL Core Technical Functionality Requirements** for 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating how the proposed product or solution complies with the technical requirements for Server anti-virus protection.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **3** | **On-Prem Air- Gapped Extended Detection and Response (XDR)**  The Bidder must provide documentation indicating how the proposed product or solution complies with **ALL** **Core Technical functionality Requirements** for On-Prem Air-Gapped 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 can then be analysed, prioritized, hunted, and remediated to prevent data loss and security breaches. * 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. * The solution must be deployed fully on-premise, in an air-gapped environment and support multi-tenancy. * 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating how the proposed product or solution complies with the technical requirements for Server anti-virus protection.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **4** | **Network Detection and Response (NDR)**  The Bidder must provide documentation indicating how the proposed product or solution complies with **ALL** **NDR** **Core Technical Functionality Requirements**.   * 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating the proposed product or solution complies with the technical requirements NDR.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **5** | **WEB Gateway Protection**  The Bidder must provide documentation indicating how the proposed product or solution complies with **ALL Core Technical Functionality Requirements** for WEB Gateway.   * Web Security, Gateway edition software, gateway anti-mailware, and content security reporter * The 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. * 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating the proposed product or solution complies with the technical requirements for Email gateway protection.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 10% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **6** | **Email Gateway Protection**  The Bidder must provide documentation indicating how the proposed product or solution complies with **ALL Core Technical Functionality Requirements** for Email Gateway.   * 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   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.  Allows administrators or users to review quarantined emails before release or deletion.   * Policy Enforcement   Enforces 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating the proposed product or solution complies with the technical requirements for Email gateway protection.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **7** | **DLP (Data loss Prevention/Protection) Solution**  The Bidder must provide documentation indicating how the proposed product or solution complies with **ALL Core Technical Functionality Requirements** for DLP solutions.   * Data Identification & Classification * Content Inspection & Monitoring * Policy Definition & Enforcement * Data Masking & Redaction * Incident Detection & Response * User Activity Monitoring * Endpoint Protection * Data Encryption * Reporting & Compliance * Scalability & Integration * User Education & Awareness * Multi-Platform Support * Data Retention & Disposal * Data identifier and template libraries for easy policy creation. * Data discovery capabilities that locate digital assets stored on laptops, desktops, and servers. * 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: * Endpoint * Mail Servers * Messaging Gateway * Web Gateway" * give you visibility and control of data in motion. * track and record if sensitive data is 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. * can send a 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 * support DANE (DNS-based Authentication of Named Entities) to secure outbound messages by verifying SMTP server identity. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating the proposed product or solution complies with the technical requirements for Endpoint Security Protection with DLP.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |

## Technical Proof of Concept (Demonstration) Requirements (Stage 4)

1. Only those bids that successfully passed all the previous evaluation stages will progress to this evaluation stage, namely Technical Proof of Concept (Demonstration) Requirements.
2. The Bidder will be required to do a Technical Proof of Concept (Demonstration) s of their proposed system that contains the ability to support the business objectives in relation to the required technology infrastructure and the required components.
3. The evaluation panel may request demonstration or explanation regarding any or all aspect of the technical Functionality requirements
4. **Weighting of requirements**: The score for the Technical Proof of Concept (Demonstration) Requirements. will be calculated as follows:
5. Each Bidder must PRESENT and will be evaluated on the understanding of the system requirement and presenting the most fit as follows:

**Table 7: Technical Proof of Concept (Demonstration) Evaluation Rating Scale**

| **Evaluation criteria** | **Score** |
| --- | --- |
| **Irrelevant** (Does not meet minimum requirement) | **0** |
| **Good** (Meets the minimum requirements) | **3** |
| **Excellent** (Exceeds the minimum requirements) | **5** |

1. **Weighting of requirements:** The full scope of requirements will be determined by the following weights as per the table below.

**Table 8: Technical Proof of Concept (Demonstration) Weighting Requirements**

|  |  |  |
| --- | --- | --- |
| **No.** | **Technical Functionality requirements** | **Weighting** |
| **BIDDER’S CAPABILITY** | | |
| 1. | On-prem, Air-Gapped End-Point Protection with EDR | 15% |
| 2. | Servers Antivirus Protection (Including virtual servers) | 15% |
| 3. | On-prem, Air-Gapped Extended and Detection Response (XDR) Protection (Servers, Endpoints) | 15% |
| 4. | Network Detection and Response (NDR) | 15% |
| 5. | Web Gateway | 15% |
| 6. | Email gateway | 10% |
| 7. | DLP (Data loss Prevention/Protection) Solution | 15% |
| TOTAL | | 100% |

1. Presentation and Demonstration information will be provided by the Bidder at the Presentation and Live Proof of Concept Demonstration session.
2. Each Bidder will be evaluated on each individual requirement as indicated in the table below by providing a Live Demonstration to score each section of the requirements.
3. The value scored for each requirement will be multiplied by the specified weighting for the relevant requirement.
4. **Minimum threshold.** To be eligible to proceed to the next stage of the evaluation the bid must achieve a **minimum threshold overall score of 60%.**

**NOTE (1):**

**The bidder must achieve at least 60% for each of the Technical Functional requirement sections as indicated in table above, failing which will result in disqualification.**

**NOTE (2):**

SITA reserves the right to verify All the information provided.

**Table 9: Technical Proof of Concept (Demonstration) Requirements**

| **ITEM NR** | **TECHNICAL FUNCTIONALITY REQUIREMENTS** | **Scoring** | **Substantiating evidence and evaluation criteria**  **(used to evaluate bid)** | **Weighting** | **Substantiation reference**  **(to be completed by bidder)** |
| --- | --- | --- | --- | --- | --- |
| **1** | **On-prem, Air-Gapped End-Point Protection with EDR**  The Bidder must demonstrate how the proposed product or solution complies with **ALL** **Core Technical Functionality Requirements** for Endpoint Protection   * Single agent to include EPP, EDR and DLP * All currently supported Microsoft Operating Systems   + Windows 11   + Windows Server 2012 - Latest * Legacy Microsoft Operating Systems:   + Windows 7 - Windows 10   + Windows Server 2008 - Windows Server 2012 * Major releases of enterprise Linux   + 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 has the ability to 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. * 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 |  | Evidence:  The bidder must provide the product specification brochure, architecture design, or documentation indicating how the proposed product or solution complies with the technical requirements for End-user device protection with EDR.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **2** | **Servers’ Anti-virus Protection**  The Bidder must demonstrate how the proposed product or solution complies with **ALL Core Technical Functionality Requirements** for 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating how the proposed product or solution complies with the technical requirements for Server anti-virus protection.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **3** | **On-Prem Air- Gapped Extended Detection and Response (XDR)**  The Bidder must demonstrate how the proposed product or solution complies with **ALL** **Core Technical functionality Requirements** for On-Prem Air-Gapped 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 can then be analysed, prioritized, hunted, and remediated to prevent data loss and security breaches. * 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. * The solution must be deployed fully on-premise, in an air-gapped environment and support multi-tenancy. * 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating how the proposed product or solution complies with the technical requirements for Server anti-virus protection.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum | 15% | <<provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **4** | **Network Detection and Response (NDR)**  The Bidder must demonstrate how the proposed product or solution complies with **ALL** **NDR** **Core Technical Functionality Requirements**.   * 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating the proposed product or solution complies with the technical requirements NDR.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **5** | **WEB Gateway Protection**  The Bidder must demonstrate how the proposed product or solution complies with **ALL Core Technical Functionality Requirements** for WEB Gateway.   * Web Security, Gateway edition software, gateway anti-mailware, and content security reporter * The 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. * 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating the proposed product or solution complies with the technical requirements for Email gateway protection.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 10% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **6** | **Email Gateway Protection**  The Bidder must provide documentation indicating how the proposed product or solution complies with **ALL Core Technical Functionality Requirements** for Email Gateway.   * 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   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.  Allows administrators or users to review quarantined emails before release or deletion.   * Policy Enforcement   Enforces 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. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating the proposed product or solution complies with the technical requirements for Email gateway protection.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |
| **7** | **DLP (Data loss Prevention/Protection) Solution**  The Bidder must demonstrate how the proposed product or solution complies with **ALL Core Technical Functionality Requirements** for DLP solutions.   * Data Identification & Classification * Content Inspection & Monitoring * Policy Definition & Enforcement * Data Masking & Redaction * Incident Detection & Response * User Activity Monitoring * Endpoint Protection * Data Encryption * Reporting & Compliance * Scalability & Integration * User Education & Awareness * Multi-Platform Support * Data Retention & Disposal * Data identifier and template libraries for easy policy creation. * Data discovery capabilities that locate digital assets stored on laptops, desktops, and servers. * 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: * Endpoint * Mail Servers * Messaging Gateway * Web Gateway" * give you visibility and control of data in motion. * track and record if sensitive data is 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 consolealong 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. * can send a 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 * support DANE (DNS-based Authentication of Named Entities) to secure outbound messages by verifying SMTP server identity. |  | Evidence:  The bidder must provide the product specification brochure, architecture design or documentation indicating the proposed product or solution complies with the technical requirements for Endpoint Security Protection with DLP.  Evaluation*:*  0= Does not meet minimum requirement  3= Meets minimum requirements  5= Exceeds minimum requirements | 15% | <provide unique reference to locate substantiating evidence in the bid response – Annex A, section 5.9> |

## Special Conditions of Contract Verification (Stage 5)

1. The successful supplier will be bound by Government Procurement: General Conditions of Contract (GCC) as well as this Special Conditions of Contract (SCC), which will form part of the signed contract with the successful Supplier. However, SITA reserves the right to include or waive the condition in the signed contract.
2. SITA reserves the right to:
   1. Negotiate the conditions; **or**
   2. Automatically disqualify a bidder for not accepting these conditions; **or**
   3. Award to multiple bidders; **or**
   4. Not to award; **or**
   5. To do a partial award.
3. In the event that the bidder qualifies the proposal with own conditions and does not specifically withdraw such own conditions when called upon to do so, SITA will invoke the rights reserved in accordance with subsection 4.5. (b) above.

### Special Conditions of Contract

#### Contracting Conditions

1. **Formal Contract** - The supplier must enter into a formal written contract (agreement) with SITA.
2. **Right to Audit** - SITA reserves the right, before entering into a contract, to conduct or commission an external service provider to conduct a financial audit or probity to ascertain whether a qualifying bidder has the financial wherewithal or technical capability to provide the goods and services as required by this tender.
3. Right of Award. SITA reserves the right to award the contract for required goods or services to multiple Suppliers.

#### Delivery Address

1. The supplier must deliver the required products or services at as indicated in Section 2.2, Delivery Address

#### Delivery Schedule

* 1. The scope of work (Section 2.1) and Section 3 (Requirements) must be completed in 30 days after the contract has been awarded to all below SITA buildings i.e. decommission, supply, install and configure.
  2. The Supplier is responsible to perform the work as outlined in the following Breakdown Structure (WBS):

| **WBS** | **Statement of Work** | **Delivery Timeframe** |
| --- | --- | --- |
|  | Supply, install and implement | Daily, weekly, Monthly |
|  | Maintain and support | Daily, weekly, Monthly |

#### Services and Performance Metrics

1. The bidder is responsible to provide the following services as specified in the Service Breakdown Structure (SBS):

| **SBS** | **Service Element** | **Service Level** |
| --- | --- | --- |
|  | Call Centre | 24h x 7days x 52weeks |
|  | Call Centre | 8h x 5d, 07:30 – 16:30 |
|  | Incident Response | Maximum 4 hours |
|  | Incident Restore | Maximum 8 hours |
|  | Availability Metrics | 99% Availability |

#### Supplier Performance Reporting

**(a) The Supplier will report on a weekly basis to SITA during the design, installation and implementation phase of the project; weekly written reports are to be presented to the SITA/Client on the progress of the preceding week until installation process has been completed.**

**(b) Quarterly meetings to be scheduled between SITA and service provider and also AD-HOC meetings from both sided.**

**(c) The Supplier will be required to generate regular reports as outputs during the maintenance and support cycle within the following service levels (the report type will drive the service level agreement; definition of the content of each report type will be finalised at the time of concluding the contracted service level agreement).**

**(d) Support via telephone or on-site visits.**

* 1. **Troubleshooting application queries.**
  2. **Troubleshooting analyser communication queries.**

**(g) Configuration queries on the application**

**(h) Assisting in the training related to the application.**

**(i) Free updates which address bug fixes, performance issues and ease of use of the application.**

**(j) Critical issues response time (e.g. total system failure) – 4 hours, from time off call received, or advise client if the problem is external (e.g. Network failure)**

**(k) Non-Critical issues response time (e.g. analyser communication problems) – 24 hours, from time off call received, or advise client if the problem is external (e.g. Network failure)**

**(l) Maintenance support Services to ensure that support is available 24hours, 7days a week and 52 weeks per year for the support calls logged by SITA, on behalf of the SITA Client.**

#### Penalties

1. A penalty of 15% of the monthly contract value or any specific deliverable may be imposed if it is found that the Service Provider failed to meet agreed deliverables, and such failure was not caused by a failure of the client to comply with its obligations.
2. Where penalties are imposed, the relevant monthly invoice will be reduced by the penalty amount, or a credit note for the penalty amount will be submitted to **SITA** within 2 (two) months of the target not being met.
3. **SITA** reserves the right to enforce these penalties, or not, depending on the merit of each case.

#### Certification, Expertise and Qualification

* 1. Supplier must have OEM documentation (valid certificate, license or membership card) here and complaint throughout the whole project.
  2. The Supplier must utilise at least two (2) technical employees who are OEM/OSM security system enterprise certified for the entire period of the contract.
  3. The Supplier represents that,
     1. **it has the necessary expertise, skill, qualifications and ability to undertake the work required in terms of the Statement of Work or Service Definition and;**
     2. **it is committed to provide the Products or Services; and**
     3. **perform all obligations detailed herein without any interruption to the Customer.**
  4. The Supplier must provide the service in a good and workmanlike manner and in accordance with the practices and high professional standards used in well-managed operations performing services similar to the Services;
  5. The Supplier must perform the Services in the most cost-effective manner consistent with the level of quality and performance as defined in Statement of Work or Service Definition;
  6. **Original Equipment Manufacturer (OEM) or Original Software Manufacturer (OSM) work. The Supplier must ensure that work or service is performed by a person who is certified by Original Equipment Manufacturer or Original Software Manufacturer.**
  7. Original Equipment Manufacturers (OEM)/Original Software Manufacturers (OSM) using reseller model are not eligible to participate for this bid

#### Logistical Conditions

**(a) Hours of work**, 07h00 – 16h00.

(b) Provision to be made for work which will be Saturday and Sunday at the Head Office for two weekends.

(c) In the event that SITA grants the Supplier permission to access SITA's Environment including hardware, software, internet facilities, data, telecommunication facilities and/or network facilities remotely, the Supplier must adhere to SITA's relevant policies and procedures (which policy and procedures are available to the Supplier on request) or in the absence of such policy and procedures, in terms of, best industry practice.

**(d) Tools of Trade**. The Supplier must bring their necessary tools of trade in order for them to perform their duties adequately.

**(e) On-site and Remote Support**. The Supplier must give off-site and remote support, and only when off-site support is not sufficient, then on-site support will be required upon approval by SITA representative.

**(f) Support and Help Desk**. After hours helpdesk support is required for the period of the first three months per site during weekdays including weekends and public holidays.

#### Skills transfer Training

1. The Bidder must ensure that the SITA technical staff receives the required training to ensure the safe operation of the solution.
2. The in-post training provided must include the possible primary cause and solutions to all the alarm events that can be encountered on the new solution.
3. Free In-post training must be provided on an on-going basis to ensure that the responsible SITA technical staff is acquainted with the safe operation of the solution and interpretation of all alarm conditions.
4. The bidder must provide the required free in-post training material i.e., instruction manual to the responsible SITA technical staff.

#### Regulatory, Quality and Standards

1. Products used to deliver the goods /services must comply with ISO9001 standard.
2. The bidder will quote only SITA-certified products for this bid, i.e. products that are listed on the

SITA product database. The database and certification process are available at [www.sita.co.za/prodcert.htm](http://www.sita.co.za/prodcert.htm). Non-certified products will not be accepted.

1. As proof of certification, the individual product certificates for the quoted products must be attached to this bid.
2. The bidder must for the duration of the contract ensure that the proposed product or solution conform to the list of Government Minimum Interoperability Standards (MIOS).

#### Company and Personnel Security Clearance Requirements

* 1. **Company security screening:** The supplier may be required to undergo a company security screening conducted by the State Security Agency (SSA). Should the SSA find the supplier **not suitable** after the conduct of the security screening, the business relationship will be terminated. The following documentation will be required for the company security screening process to be conducted:
     1. Copy of company registration documentation;
     2. Copy(ies) of identity documentation of Director(s), Member(s) or Trustee(s);
     3. Copy of valid tax clearance certificate.
  2. **Security suitability check for individuals:** **SITA** may, at its own discretion and in line with its policies and procedures, require employees of the supplier to be subjected to a security suitability check before commencement of a project or delivering of a service. The security suitability check is conducted by **SITA** in order to ensure that individuals meet the minimum security requirements and also to verify personal information. The supplier will be required to replace any employee(s) who is found to be not suitable after the conduct of the security screening. The following documentation will be required for the security suitability check:
     1. Copy of identity document;
     2. Copy(ies) of qualification(s) if **SITA** requires verification thereof;
     3. Fingerprints – will be taken electronically;
     4. Signed consent form for the conduct of background checks.
  3. **Security clearance:** A security clearance, issued by either the SSA or Defence Intelligence (DI) is required if any employee of the supplier will have or may gain access to classified information throughout the duration of the project or in the process of delivering a service. The level of security clearance required – **Confidential**, **Secret** or **Top Secret**, will be determined at the sole discretion of SITA. The supplier will have to replace any employee who do not qualify for a security clearance or is found not suitable by the SSA or DI. The following documentation will be required for the security clearance process:
     1. Completed Z204 or DD1057 security clearance application form;
     2. Fingerprints;
     3. Personal documentation of the applicant, including but not limited to, identity document, passport, marriage certificate (if applicable), divorce order (if applicable), qualifications, salary advice and bank statements.

#### Confidentiality and non -disclosure conditions

1. The Supplier, including its management and staff, must before commencement of the Contract, sign a non-disclosure agreement regarding Confidential Information
2. Confidential Information means any information or data, irrespective of the form or medium in which it may be stored, which is not in the public domain and which becomes available or accessible to a Party as a consequence of this Contract, including information or data which is prohibited from disclosure by virtue of:
   1. the Promotion of Access to Information Act, 2000 (Act no. 2 of 2000);
   2. being clearly marked "Confidential" and which is provided by one Party to another Party in terms of this Contract;
   3. being information or data, which one Party provides to another Party or to which a Party has access because of Services provided in terms of this Contract and in which a Party would have a reasonable expectation of confidentiality;
   4. being information provided by one Party to another Party in the course of contractual or other negotiations, which could reasonably be expected to prejudice the right of the non-disclosing Party;
   5. being information, the disclosure of which could reasonably be expected to endanger a life or physical security of a person;
   6. being technical, scientific, commercial, financial and market-related information, know-how and trade secrets of a Party;
   7. being financial, commercial, scientific or technical information, other than trade secrets, of a Party, the disclosure of which would be likely to cause harm to the commercial or financial interests of a non-disclosing Party; and
   8. being information supplied by a Party in confidence, the disclosure of which could reasonably be expected either to put the Party at a disadvantage in contractual or other negotiations or to prejudice the Party in commercial competition; or
   9. information the disclosure of which would be likely to prejudice or impair the safety and security of a building, structure or system, including, but not limited to, a computer or communication system; a means of transport; or any other property; or a person; methods, systems, plans or procedures for the protection of an individual in accordance with a witness protection scheme; the safety of the public or any part of the public; or the security of property; information the disclosure of which could reasonably be expected to cause prejudice to the defence of the Republic; security of the Republic; or international relations of the Republic; or plans, designs, drawings, functional and technical requirements and specifications of a Party, but must not include information which has been made automatically available, in terms of the Promotion of Access to Information Act, 2000; and information which a Party has a statutory or common law duty to disclose or in respect of which there is no reasonable expectation of privacy or confidentiality;
3. Notwithstanding the provisions of this Contract, no Party is entitled to disclose Confidential Information, except where required to do so in terms of a law, without the prior written consent of any other Party having an interest in the disclosure;
4. Where a Party discloses Confidential Information which materially damages or could materially damage another Party, the disclosing Party must submit all facts related to the disclosure in writing to the other Party, who must submit information related to such actual or potential material damage to be resolved as a dispute;
5. Parties may not, except to the extent that a Party is legally required to make a public statement, make any public statement or issue a press release which could affect another Party, without first submitting a written copy of the proposed public statement or press release to the other Party and obtaining the other Party's prior written approval for such public statement or press release, which consent must not unreasonably be withheld.

#### Guarantee and warranties

1. The supplier confirms that:
   1. The warranty of goods supplied under this contract remains valid for the duration of the contract after the goods were delivered, installed and commissioned with a sign off, including the clients signature
   2. as at Commencement Date, it has the rights, title and interest in and to the Product or Services to deliver such Product or Services in terms of the Contract and that such rights are free from any encumbrances whatsoever.
   3. the Product is in good working order, free from Defects in material and workmanship, and substantially conforms to the Specifications, for the duration of the Warranty period.

#### Intellectual Property Rights

1. SITA retains all Intellectual Property Rights in and to SITA's Intellectual Property. As of the Effective Date, the Supplier is granted a non-exclusive license, for the continued duration of this Contract, to perform any lawful act including the right to use, copy, maintain, modify, enhance and create derivative works of SITA's Intellectual Property for the sole purpose of providing the Products or Services to SITA pursuant to this Contract; provided that the Supplier must not be permitted to use SITA's Intellectual Property for the benefit of any entities other than SITA without the written consent of SITA, which consent may be withheld in SITA's sole and absolute discretion. Except as otherwise requested or approved by SITA, which approval is in SITA's sole and absolute discretion, the Supplier must cease all use of SITA's Intellectual Property, at of the earliest of:
   1. termination or expiration date of this Contract;
   2. the date of completion of the Services; and
   3. the date of rendering of the last of the Deliverables
2. If so required by SITA, the Supplier must certify in writing to SITA that it has either returned all SITA Intellectual Property to SITA or destroyed or deleted all other SITA Intellectual Property in its possession or under its control
3. SITA, at all times, owns all Intellectual Property Rights in and to all Bespoke Intellectual Property.
4. Save for the license granted in terms of this Contract, the Supplier retains all Intellectual Property Rights in and to the Supplier’s pre-existing Intellectual Property that is used or supplied in connection with the Products or Services
5. Provide SITA with the compliant Occupational Health and Safety File (required on site for period of installation and proof of compliance).

#### General

1. The supplier will be bound by Government Procurement: General Conditions of Contract.
2. (GCC) as well as this Special Conditions of Contract (SCC), which will form part of the signed contract with the Supplier. However, SITA reserves the right to include or waive the condition in the signed contract.
3. SITA reserves the right to:
   1. Negotiate the conditions, or
   2. Automatically disqualify a bidder for not accepting these conditions, or
   3. Before entering a contract, conduct or commission an external service provider to audit or conduct probity to ascertain whether a qualifying bidder has the technical capability to provide the goods and services as required by this tender.

#### Counter Conditions

1. Bidders’ attention is drawn to the fact that amendments to any of the Bid Conditions or setting of counter conditions by bidders may result in the invalidation of such bids.

#### Fronting

1. The SITA supports the spirit of Broad Based Black Economic Empowerment and recognizes that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, equitable, transparent and legally compliant manner. Against this background the SITA will not condone any form of fronting.
2. The SITA, in ensuring that bidders conduct themselves in an honest manner will, as part of the bid evaluation processes, conduct or initiate the necessary enquiries/investigations to determine the accuracy of the representation made in bid documents. Should any of the fronting indicators as contained in the Guidelines on Complex Structures and Transactions and Fronting, issued by the Department of Trade and Industry, be established during such enquiry/investigation, the onus will be on the bidder / contractor to prove that fronting does not exist. Failure to do so within a period of 14 days from date of notification may invalidate the bid / contract and may also result in the restriction of the bidder/contractor to conduct business with the public sector for a period not exceeding ten (10) years, in addition to any other remedies SITA may have against the bidder/contractor concerned.

#### Business Continuity and Disaster Recovery Plans

1. The bidder confirms that they have written business continuity and disaster recovery plans that define the roles, responsibilities, and procedures necessary to ensure that the required services under this bid specification is in place and will be maintained continuously in the event of a disruption to the bidder’s operations, regardless of the cause of the disruption.

#### Supplier Due Diligence

1. SITA reserves the right to conduct supplier due diligence prior to final award or at any time during the Contract period and this may include pre-announced / non-announced site visits. During the due diligence process the information submitted by the bidder will be verified and any misrepresentation thereof may disqualify the bid or Contract in whole or parts thereof.

#### Preference Goal Requirements conditions

1. The Bidder’s commitment for the Preference Goal Requirements in this tender will be legally binding and the Bidder needs to perform against their commitment for the duration of the contract which will form part of the Contractual Agreement.
2. The Bidder must sustain or improve the company’s BBBEE Level for the duration of the contact which will form part of the Contractual Agreement.
3. Performance of Preference Goal Requirements will be determined annually. Bidders must submit their Preference status report indicating progress against the Bidder’s Preferential commitments within 30 days of the yearly anniversary of the contract.
4. Bidders need to keep auditable substantive records / evidence and upon request by SITA/Department must be made available for audit and, or due diligence purposes.
5. SITA reserves the right to require from a Bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim with regards to preferences, in any manner required by SITA.
6. SITA reserves the right to verify information / evidence provided by the Bidder.
7. SITA/Department reserves the right to introduce a **penalty of 1%** of the overall annual year spent by SITA/Department for the prior year if the Bidder fails to comply to **paragraphs (a), (b) and (c) above**.

### Declaration of compliance and acceptance SCC

I (we), the bidder hereby declare that I (we) accept ALL the Special Conditions of Contract as specified in par 4.5.1 above and shall comply with all stated obligations:

Name of Bidder:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Price and Preference Points Evaluation (Stage 6)

### Costing and Preference Evaluation

1. In terms of the SITA Preferential Procurement Policy (PPP), the following preference point system is applicable **for this** Bid:
   1. **the 90/10 system (90 Price and 10 Specific Goals) for requirements with a Rand value above R50 000 000 (all applicable taxes included).**
2. Points will be allocated for each of the **Preferential Goal Requirements** for this tender as indicated in **table 10** dependant on **paragraph 1.**
3. Points for this tender shall be awarded for:
   1. Price; and
   2. Preference points for specific goals.
4. The maximum points for this tender will be allocated as follows, subject to **paragraphs 3** above:

**Table 10: Points allocation**

|  |  |
| --- | --- |
| **Description** | **Points**  **Table 13** |
| Price | 90 |
| Preference points for specific goals | 10 |
| Total points for Price and preference points for specific goals | **100** |

### Costing and Pricing Conditions

1. **SOUTH AFRICAN PRICING**

The total price must be VAT inclusive and be quoted in South African Rand (ZAR).

1. **TOTAL PRICE**
   1. Bidder will be bound by the following general costing and pricing conditions and SITA reserves the right to negotiate the conditions or automatically disqualify the bidder for not accepting these conditions:
   2. All quoted prices are the total price for the entire scope of required services and deliverables to be provided by the bidder.
   3. The cost of delivery, labour, S&T, overtime, etc. must be included in this bid.
   4. All additional cost must be clearly specified.
   5. SITA reserves the right to negotiate pricing with the successful bidder prior to the award as well as envisaged quantities.
   6. The Successful Bidder **must** consider a cost-free transitioning period as follows:
2. No billing for duration of transitioning into the new product to assist the client to avoid paying for two products with the same functionality.
3. Email gateway will only be implemented when the existing contract concludes in March 2027, Bidders must only cost the Email gateway from F/Y 27/28
   1. These conditions will form part of the Contract between SITA and the Bidder. However, **SITA** reserves the right to include or waive the condition in the Contract.
   2. The Bidder **must** include their Costing Proposal and indicate the reference page(s) in both their proposal and SBD 1 form as part of their bid submission.
   3. Note: Bidders will complete Bidder’s Costing Proposal and include this as part of the hard copy submission documents and on the memory stick.
   4. The Bidder’s Costing Proposal should be divided into the following categories and should take account of the following, however, is not limited to these categories

| **#** | **Categories** |
| --- | --- |
| 1.1 | **End User Devices Antivirus Protection (End Point Protection) with EDR** |
| 1.2 | Server Antivirus Protection |
| 1.3 | Extended and Detection Response (XDR) Protection (Servers, Endpoints, and network (NDR)) |
| 1.4 | Network Detection and Response (NDR) |
| 1.5 | Web Gateway Protection Software |
| 1.6 | Email Gateway Security Protection |
| 1.7 | DLP (Data Loss Prevention/Protection) |
| 1.8 | Deployment and Migration of the Solution |
| 1.9 | Highest OEM Support for maintenance and incident response |

* 1. **Bidders must complete and submit their Costing Proposal in Excel spreadsheet format.**
  2. The bidder must complete the declaration of acceptance as per **section 4.6.5** below by marking with an “X” either “ACCEPT ALL”, or “DO NOT ACCEPT ALL”, failing which the declaration will be regarded as “DO NOT ACCEPT ALL” and the bid will be disqualified.

### Rate of Exchange Pricing Information

Provide the **TOTAL BID PRICE** for the duration of Contract and clearly indicate the Local Price and Foreign Price, where –

* 1. **Local Price** means the portion of the TOTAL price that is NOT dependent on the Foreign Rate of Exchange (ROE) and;
  2. **Foreign Price** means the portion of the TOTAL price that is dependent on the Foreign Rate of Exchange (ROE).
  3. **Exchange Rate** means the ROE (ZA Rand vs foreign currency) as determined at time of bid.

### Bid Exchange Rate Conditions

The Bidders must use the exchange rate provided in the table below:

**Table 11:** **Bid Exchange Rate**

|  |  |
| --- | --- |
| **Foreign currency** | **South African Rand (ZAR) exchange rate** |
| 1 US Dollar | R17,59 |
| 1 Euro | R20,63 |
| 1 Pound | R24,19 |

**Note (1):**

The ROE indicated in the Bid Specification is to ensure a competitive bidding process.

**Note (2):**

The ROE will be fluctuating. The details of the ROE fluctuation will be negotiated during the contracting stage.

### Declaration of Acceptance

|  | **ACCEPT ALL** | **DO NOT ACCEPT ALL** |
| --- | --- | --- |
| 1. The bidder declares to ACCEPT ALL the Costing and Pricing conditions as specified in **par 4.6.2** above by indicating with an “X” in the “ACCEPT ALL” column, or 2. The bidder declares to NOT ACCEPT ALL the Costing and Pricing Conditions as specified in **par 4.6.2** above by -    1. Indicating with an “X” in the “DO NOT ACCEPT ALL” column, and;    2. Provide reason and proposal for each of the condition not accepted. |  |  |
| **Comments by bidder:**  Provide the condition reference, the reasons for not accepting the condition. | | |

* 1. **PREFERENCE REQUIREMENTS**

1. **The Bidder must complete in full all the PREFERENCE requirements.**
2. **Allocation of points per requirements:** The points allocation of bidders’ responses to the requirements will be determined by the completeness, relevance and accuracy of substantiating evidence.
3. Points will be allocated for each **PREFERENCE requirement** as per the criteria set in each section in the **table 12** below.
4. **The Bidder must provide a unique reference number** (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response. During evaluation, SITA reserves the right to treat substantiation evidence that cannot be located in the bid response, as “NOT COMPLY”. The evidence needs to be attached to **ANNEX A**.
5. **Preference Goal Requirements:**
   1. The **Bidder must complete the 90/10 preference point system** and submit proof or documentation required in terms of this tender.
   2. The specific Preferential Goal Requirements for this tender is indicated in **table 13** below.
   3. The Bidder must indicate their commitment to claim points for each of the preference points **by signing at par 4.5 in the Invitation to Bid document.**
   4. Failure on the part of a bidder to submit proof or documentation required or to comply to paragraph (d) above in terms of this tender to claim preference points for the **Preference Goal Requirements** for this tender, will be interpreted to mean that preference points are not claimed.
   5. The Bidder’s **commitment** for the Preference Goal Requirements in this tender will be legally binding and the Bidder needs to perform against their commitment for the duration of the contract which will form part of the Contractual Agreement.
   6. The Bidder must sustain, or improve the company’s B-BBEE Level for the duration of the contact which will form part of the Contractual Agreement.
   7. Performance of Preference Goal Requirements will be determined annually. Bidders must submit their Preference status report to **SITA** indicating progress against the Bidder’s Preferential commitments within 30 days after each quarter from the commencement date of the contract.
   8. Bidders need to keep auditable substantive records / evidence and upon request by **SITA** must be made available for audit and, or due diligence purposes.
   9. **SITA** reserves the right to require from a Bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim with regards to preferences, in any manner required by **SITA**.
   10. **SITA** reserves the right to verify information / evidence provided by the Bidder.
   11. **SITA** reserves the right to introduce a penalty of 1% of the overall annual year spent by **SITA** for the prior year if the Bidder fails to comply to paragraphs (e), (f) and (g) above.

**Table 12: Preference Goal Requirements**

| **Preference Goal Requirement #** | **Preferential Goal Requirements** | **Preferential Goal Requirements**  **(Specific Goals)** | |
| --- | --- | --- | --- |
|  | **Preferential Goal Requirements allocated for this tender** | **Substantiating evidence and evidence reference to be completed by bidder.  Evaluation per requirement: Each requirement indicated in the table below must be completed and points will be allocated based on the evidence required below:** | **Evidence reference for the** |
|  | **B-BBEE Requirements** |  | |
| 1) | **B-BBEE Requirements**  Promotion of Transformational Objectives. | **Evidence:** The Bidder must provide a copy of the following relevant evidence for the Preferential Goal points which the Bidder qualifies for:   1. **Columns A, B, C and D in table 13:**   Copy of relevant proof of the following to confirm the B-BBEE status of the contributor as defined in the Broad-Based Black Economic Empowerment Act:   * + - * 1. ***B-BBEE certificate*** *(from a SANAS Accredited Agency the dtic);*   **or**  ***Sworn affidavit*** in the format provided by CIPC - ***Applicable to EMEs and QSEs only;***  **and/ or**   1. **Column D in table 13:**   Copy of ***South African Identification Document (ID***);  **and/ or**   1. **Column E in table 13:**   Copy of ***Medical Certificate*** ***clearly indicating the disability in line with the B-BBEE status claimed as defined in the Broad-Based Black Economic Empowerment Act***.  **Note:**  The CIPC (Companies and Intellectual Property Commission) registration documents will also be used as evidence to confirm compliance to the Preferential procurement requirements as part of the evaluation process.  **Points allocation:** Points will be allocated for bidders that meets the requirements as indicated in **table 13 in section 4.7.** | <provide unique reference to locate substantiating evidence in the bid response – **Annex A, section 6.7**> |

**Table 13:** B-BBEE Points as part of the Preference Goal requirements (Preferential Goal Requirements for **(90/10) system**)

**Note: Bidder to select the section for points they wish to claim (Mark as Y=Yes) in the table below.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Ownership** | | | |  |  |  |
|  | **Reference #** | **Contributor Level as defined in the Broad-Based Black Economic Empowerment Act** | **EME/QSEs** | **Black Owned (BO) (51% or more)** | **Black Woman Owned (BWO) (More than 30%)** | **Youth Owned** | **Owned by People living with disabilities** | **Score** | **Bidder to select the section for points they wish to claim (Mark as Y= Yes)** |  |
|  |  |
|  |  |  | **(A)** | **(B)** | **(C)** | **(D)** | **(E)** | **(F)** |  |  |
|  | **1** | **Level 1** | **3** | **2** | **2** | **2** | **1** | **10** |  |  |
|  | **2** | **Level 1** | **3** | **2** | **2** | **2** | 0 | **9** |  |  |
|  | **3** | **Level 1** | **3** | **2** | **2** | 0 | 0 | **7** |  |  |
|  | **4** | **Level 1** | **3** | **2** | 0 | 0 | 0 | **5** |  |  |
|  | **5** | **Level 2 and 3** | **2** | **1** | **0,5** | **0,5** | **0,5** | **4,5** |  |  |
|  | **6** | **Level 2 and 3** | **2** | **1** | **0,5** | **0,5** | 0 | **4** |  |  |
|  | **7** | **Level 2 and 3** | **2** | **1** | **0,5** | 0 | 0 | **3,5** |  |  |
|  | **8** | **Level 2 and 3** | **2** | **1** | 0 | 0 | 0 | **3** |  |  |
|  | **9** | **Level 4 and 5** | **1** | **0,5** | **0,25** | **0,25** | **0,25** | **2,25** |  |  |
|  | **10** | **Level 4 and 5** | **1** | **0,5** | **0,25** | **0,5** | 0 | **2,25** |  |  |
|  | **11** | **Level 4 and 5** | **1** | **0,5** | **0,25** | 0 | 0 | **1,75** |  |  |
|  | **12** | **Level 4 and 5** | **1** | **0,5** | 0 | 0 | 0 | **1,5** |  |  |
|  | **13** | **Level 6** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **14** | **Level 7** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **15** | **Level 8** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **16** | **Non-Contributor** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **Total Maximum Score Allocation:** | | **10** |  |  |  |  |  |  |  |
|  | F= A+B+C+D+E | | | | | | | |  |  |

1. Bidder substantiating evidence

# Technical Mandatory Requirement Evidence

## ****Bidder Certification / Affiliation requirements****

Attach to ANNEX A a copy of valid documentation (letter/certificate/license) as proof that the Bidder is an Original Software Manufacturer (OSM)/ Original Equipment Manufacturer (OEM) or accredited as a Reseller/ Partner to provide a to provide licences of an Endpoint Security Solution to a minimum of **3000+** users in the past five (05) years from the publication of this bid **here**.

**NOTE (1):**

Original Equipment Manufacturers (OEM)/Original Software Manufacturers (OSM) using reseller model are not eligible to participate for this bid.

**NOTE (2):**

SITA reserves the right to verify the information provided.

## ****Bidder experience and capability requirements****

Complete table below, noting that:

1. Provide reference information from at least two(2) customer to whom **licences of an Endpoint Security Solution was designed, planned, tested, maintained, supported and deployed to a minimum of 3000+ users in the past five (05) years from the publication of this bid.**
2. Scope of work must be related.

**Note (1):**

The Bidder **must provide** the following information when completing **table 14:**

* 1. Company name; and
  2. Contact person, telephone **and/or** e-mail address; **and**
  3. Project scope of Work; **and**
  4. Project start and End date.

**Note (2):**

Failure to comply **fully** to the requirements as indicated above will result in disqualification.

**Note (3):**

SITA reserves the right to verify information provided.

Table 14: References

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Company Name** | **Reference Person Name, Tel and/or email** | **Project Scope of Work** | **Project start and end date** |
| 1 | <Company name> | <Person Name>  <Tel>  <email> | < Provide scope details of a project from at least from at least two (2) customers to whom licences of an Endpoint Security Solution was designed, planned, tested, maintained, supported and deployed to a minimum of 3000+ usersin the past five (05) years from the publication of this bid> | Start Date:  End Date: |
| 2 | <Company name> | <Person Name>  <Tel>  <email> | < Provide scope details of a project from at least from at least two (2) customers to whom licences of an Endpoint Security Solution was designed, planned, tested, maintained, supported and deployed to a minimum of 3000+ usersin the past five (05) years from the publication of this bid> | Start Date:  End Date: |

## ****On-prem air gapped capability requirements****

1. Signed letter or letter from OEM/OSM confirming that the listed functions are available on-premises and can function **air-gapped**: Endpoint Protection (EPP), Extended Detection and Response (XDR), Data Leak Prevention (DLP)

Network Detection and Response (NDR), Email Gateway security, Web Gateway, IOC (Indicators of Compromise), Data Lake

**Note:** SITA reserves the right to verify the information provided.

## ****OEM/OSM Rating Requirements****

1. Provide the Gartner Magic Quadrant/Forrester Wave for End-Point Protection for 2025 to validate the OEM/OSM position.

**Note:** SITA reserves the right to verify the information provided

## ****Data residency and sovereignty requirements****

1. Provide the letter that confirms that 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 compliance with the organizations data sovereignty and compliance laws.

**Note:** SITA reserves the right to verify the information provided.

## ****Single solution requirements****

1. Provide a letter that confirms that all the functionality is provided by a single OEM/OSM.

Endpoint Protection (EPP), eXtended Detection and Response (XDR), Data Loss Prevention (DLP), Network Detection and Response (NDR), Email Gateway Security, Web Gateway, Indicators of Compromise (IOC)

**Note:** SITA reserves the right to verify the information provided.

## OEM/OSM Presence Requirement

OEM/OSM or accredited Partner/Reseller must provide their local proof of address in the form of lease agreement or three months utilities bill not older than three months.

**NOTE (1):**

SITA reserves the right to verify information provided.

## Special Conditions of Contract

The Bidder **must accept ALL** the Special Conditions of Contract by completing and signing the declaration of Acceptance in Declaration of compliance and acceptance under the Special Conditions **(Section 4.5.2)**.

**NOTE (1):**

Failure to **accept ALL** the Special Conditions of Contract will result in disqualification.

* 1. **Third Party Risk Management Assessment**

The Bidder **must comply** with the Third-Party Risk Management Assessment requirement **by completing** **All the questions** in **ANNEX B** and **attach it here**.

**NOTE (1):**

SITA reserves the right to verify information provided.

**NOTE (2):**

Failing to complete all the questions or not Accepting the Declaration of Acceptance above will result in disqualification.

## Technical/Product Functional Requirement

The Bidder must confirm that they comply with the **Technical/Product Functional Requirements** **by completing and signing** **Annex C : Addendum 1** and **attach it here**.

## Technical Functionality Requirements

1. The Bidder must attach proof of evidence to confirm that they comply with the Technical Functional Requirements and bidders must achieve at least an overall threshold of **60%** for all the Technical Functional requirement sections as indicated in **Section** **4.3**

## Technical Proof of concept (Demonstration)Requirements

Presentation and Demonstration information will be provided by the Bidder at the Presentation and Live Proof of Concept Demonstration session as indicted in **section 4.4**.

## Preference Points Preferential Goals Evidence

The Bidder **must**:

* + 1. **Preference Goal Requirements:**

Bidder to select the section for points they wish to claim (Mark as Y=Yes) in **either tables 13**  dependant on which preference system the Bidder selects in line with **section 4.7; and**

Provide a copy of the following relevant evidence for the Preferential Goal points which the Bidder qualifies for as set out in **table 12** in **section 4.7** **below** and **attach it here**:

* + - * 1. **Columns A, B, C and D in tables 13:**

Copy of relevant proof ***(B-BBEE certificate or sworn affidavit)*** of B-BBEE status level of contributor as defined in the Broad-Based Black Economic Empowerment Act:

***B-BBEE certificate (from a SANAS Accredited Agency);***

**or**

***Sworn affidavit* in the format provided by CIPC - *Applicable to EMEs and QSEs only;***

**and/ or**

* + - * 1. **Column D in tables 13 :**

Copy of **South African Identification Document (ID);**

**and/ or**

* + - * 1. **Column E in tables 13 :**

*Copy of Medical Certificate* ***clearly indicating the disability in line with the B-BBEE status claimed as defined in the Broad-Based Black Economic Empowerment Act***.

**Note:**

The CIPC (Companies and Intellectual Property Commission) registration documents will also be used as evidence to confirm compliance to the Preferential procurement requirements as part of the evaluation process.

* + 1. Indicate their commitment to claim points for each of the preference points **by signing at par 4.5 in the Invitation to Bid document.**

**NOTE (1):**

**Failure on the part of a bidder to comply to paragraphs (1) and (2) above, will be interpreted to mean that preference points are not claimed.**

Annex B: THIRD-PARTY RISK MANAGEMENT (TPRM) ASSESSMENT

1. **Instructions**
2. In terms of the approved SITA Third-Party Risk Management Framework, all Bidders responding to this bid must complete the following section by answering ALL the questions.
3. By completing the Third-Party Risk Management Assessment, the Bidder agrees to provide all reasonable supporting documentation when requested to do so, as well as during contract finalisation as this is a pre-award condition of this bid.
4. Any risk identified during the assessment process will have to be mitigated and/or remediated before or during the contract finalisation phase. A detailed mitigation plan, that is acceptable to SITA, may also be required.
5. Supplier due diligence, as contained in the Special Conditions of Contract, is also applicable to this Third-Party Risk Management process.
6. The following 6 (six) risk elements will be assessed:
   1. Company risk: 10 questions;
   2. Financial risk: 6 questions;
   3. Operational risk: 8 questions;
   4. Governance and compliance risk: 6 questions;
   5. Information security and privacy risk: 7 questions;
   6. Reputational risk: 6 questions.
   7. **Evaluation Criteria**
      1. **Company risk**
   8. Questions 2, 3, 6, 8, 9, 10:

| **Evaluation criteria** | **Score** |
| --- | --- |
| Yes | 0 |
| Partially meet requirements | 0.5 |
| No | 1 |

* 1. Questions 1, 4, 5:

| **Evaluation criteria** | **Score** |
| --- | --- |
| Yes | 1 |
| Partially meet requirements | 0.5 |
| No | 0 |

* 1. Question 7:

| **Evaluation criteria** | **Score** |
| --- | --- |
| Yes, actively operating for more than 5 years | 1 |
| 2-5 Years actively operating | 0.5 |
| No, actively operating for less than 2 years | 0 |

* + 1. **All questions for all other risk elements:**

| **Evaluation criteria** | **Score** |
| --- | --- |
| Yes | 1 |
| Partially meet requirements | 0.5 |
| No | 0 |

* 1. **Third Party Risk Assessment**
  2. The assessment of bidders’ responses to the questions will be determined by the completeness (i.e. all questions answered), undertaking signed (where required) and accuracy of substantiating evidence, when requested. Please note that SITA reserves the right to verify the information provided.

| **Question to assess each risk element** | **Bidders response:**  **Mark relevant box with an “X”** | | |
| --- | --- | --- | --- |
| **Company Risk** | | | |
| 1. Have you disclosed all interests and relationships as required in **SBD 4**, including whether any of your directors, members, trustees, or shareholders are employed by the state, have relationships with SITA employees, or have interests in other entities (whether they are also bidding for this contract, or not)? | Yes | Partially | No |
| 1. Are you currently involved in litigation against SITA – or do you foresee litigation being instituted within the next 6 months? | Yes | Partially | No |
| 1. Are there any law suits or ongoing litigation that could affect this transaction in any way or the bidder as an ongoing concern? | Yes | Partially | No |
| 1. Is customer service delivery or contract performance actively monitored by you? | Yes | Partially | No |
| 1. Do you have formal strategic planning processes in place? | Yes | Partially | No |
| 1. Are any of your directors or shareholders Prominent Influential People (PIP) or Politically Exposed Persons (PEP)? | Yes | Partially | No |
| 1. Has your company been actively operating as a going concern for more than 5 years? | Yes | 2-5 Years | Less than 2 years |
| 1. Is the company busy with a re-organisational/restructuring process that may impact this transaction? | Yes | Partially | No |
| 1. Are any of your suppliers located in a region where geopolitical risk exposure is high? | Yes | Partially | No |
| 1. Has any current director of the bidder ever served as a director of a company during a period where a Government contract was cancelled? | Yes | Partially | No |
| **Financial Risk** | | | |
| 1. Did you have positive revenue growth in the past three years? | Yes | Partially | No |
| 1. Is the proposed bid price going to be **less than 40%** of your total annual revenue for the previous financial year? | Yes | Partially | No |
| 1. Is the financial health of your company in good standing? | Yes | Partially | No |
| 1. Were your Annual Financial Statement (AFS) unqualified in the last financial year? | Yes | Partially | No |
| 1. Do you have sufficient cash in the bank (2 or more months’ worth of operating cost) to operate under restricted conditions for at least 2 months? | Yes | Partially | No |
| 1. Do you have a clean credit record: No current or pending judgement, adverse listing, business rescue or principal sequestration listing? | Yes | Partially | No |
| **Operational Risk** | | | |
| 1. Do you have operational redundancy (resilience) in terms of technology and energy resources to ensure high availability of services? | Yes | Partially | No |
| 1. Are your dependencies for logistics either fully under your own control **or** managed through supplier performance management contracts? (Choose “Yes” if fully under your own control and “No” for supplier contracts) | Yes | Partially | No |
| 1. Do you have operational procedure standards in place across the organisation, such as change control, release management, access control, incident management, back-up regimes and restore tests, etc? | Yes | Partially | No |
| 1. Do you have human resources management in place, including succession planning and mitigation against key reliance on single individuals? | Yes | Partially | No |
| 1. Do you have sound supply chain processes in place? | Yes | Partially | No |
| 1. Do you have sound third party risk management processes in place (fourth party for SITA)? | Yes | Partially | No |
| 1. Do you have a fully-fledged research and development (R&D) department to ensure continuous improvement? | Yes | Partially | No |
| 1. Do you rely on locally manufactured components or have actively managed the risk relating to lead times or delivery delays? (Choose “Yes” is you rely on locally manufactured components or can actively manage lead times and prevent delivery delays where manufacturing is not local i.e. not in South Africa) | Yes | Partially | No |
| **Governance and Compliance Risk** | | | |
| 1. Do you comply with all legislation, including labour, health and safety regulations? | Yes | Partially | No |
| 1. Do you have the appropriate governance frameworks (Cobit, ITIL, King) in place with due monitoring against set standards? | Yes | Partially | No |
| 1. Do you have an internal audit function compliant with IIA standards (insourced, outsourced or co-sourced) in place? | Yes | Partially | No |
| 1. Do you follow formally documented enterprise risk management processes? | Yes | Partially | No |
| 1. Are all statutory requirements of the entity up to date? Specifically, the following: CIPC Returns, Tax returns, UIF and COIDA. | Yes | Partially | No |
| 1. Do you have comprehensive insurance in place, including cover for assets, business disruption and liability? | Yes | Partially | No |
| **Information Security and Privacy Risk** | | | |
| 1. Are your physical security perimeters appropriately safeguarded? | Yes | Partially | No |
| 1. Do you have video surveillance of areas that will contain SITA information/products? | Yes | Partially | No |
| 1. Do you conduct security and suitability verification of all employees prior to employment? | Yes | Partially | No |
| 1. Do you have identification verification controls in place in all your buildings? | Yes | Partially | No |
| 1. Are your access control protocols verified to be effective by Internal and/or External Auditors? | Yes | Partially | No |
| 1. Do you have Security Information and Events Management (SIEM) processes in place? | Yes | Partially | No |
| 1. Do you have sufficient information security and cyber arrangements in place for employees working from home? | Yes | Partially | No |
| **Reputational Risk** | | | |
| 1. Do you have anti-bribery and corruption, anti-money laundering and fraud prevention practices in place? | Yes | Partially | No |
| 1. Please confirm that neither the company, nor any of its directors has been named in any corruption scandal (choose “Yes” to confirm **not being named** in a corruption scandal) | Yes | Partially | No |
| 1. Do you have a social responsibility programme in place? | Yes | Partially | No |
| 1. Do you have an environmental protection policy, including potential harmful emission or hazardous waste management? | Yes | Partially | No |
| 1. Do you actively manage your organisation’s energy consumption? | Yes | Partially | No |
| 1. Is your employment equity plan up to date and actively managed? | Yes | Partially | No |

* 1. **Third Party Risk Management Declaration**
  2. The bidder hereby makes the following declaration and confirm the following information (mark with a “X” in the corresponding column):

| **Statement of Declaration** | **Accept and Confirm** | **Do not accept and Confirm** |
| --- | --- | --- |
| 1. All questions in this assessment were answered accurately. |  |  |
| 1. SITA can request additional supporting documentation, within reason, to confirm the accuracy and completeness of the information provided in this self-assessment. |  |  |

* + 1. **Declaration of Acceptance**

|  |  |  |
| --- | --- | --- |
|  | **Accept all** | **Do not accept all** |
| 1. The bidder declares that all information provided in this assessment is accurate. 2. The bidder understands that any false information may constitute misrepresentation.    1. SITA reserves the right to verify the information provided. 3. By completing the Third-Party Risk Management Assessment the Bidder agrees to provide all reasonable supporting documentation when requested to do so, as well as during contract finalisation as this is a **pre-award condition of this bid.** 4. The bidders understand and agrees that this section will form part of the contract and is legally binding. |  |  |
| **Any additional comments by bidder pertaining to the third-party risk assessment:** | | |

**NOTE: Failing to complete all the questions, or not Accepting the Declaration of Acceptance will lead to disqualification.**

Annex C: Product/Service functional Requirements. ADDENDUM 1

**NB: The bidder must confirm that they comply with the following Product / Service Functional requirements as indicated below as this will be legal contractual binding:**

**Table 15: Product/Service Functional Requirements**

|  |  |
| --- | --- |
| License Name | Functionality Required |
| **End User Devices Antivirus Protection (End Point Protection) with EDR** | * Solution must be Air gapped/ On -Premises * Solution must to be managed by a single console * must comply with data residency and sovereignty rules * The solution must provide all the functionality from a single OEM/OSM * Single agent to include EPP, EDR and DLP * Complete protection of the endpoint using malware behaviour blocking techniques. * Scanning of boot-sector of USB storage devices when plugging in. * Automatic/Manual scanning of the endpoint. * Complete event monitoring for detailed information of events. * Block files and processes typically associated with ransomware. * Detect and block infected executable files. * Terminate programs that exhibit malicious behaviour associated with attacks. * Apply device-control rules to end-points. * Granular permissions for USB storage * Identify network connections utilising malware network fingerprinting * Agent can apply application control rules to the endpoints. * Allow for the remote install of agents * Solution should Supported all industries base Operating Systems as well as legacy Operating systems * Predictive Machine Learning capabilities * Supports the mapping of the rules with MITRE ATT&CK framework techniques. * Provides the ability to collect and identify operating systems logs, logs of databases, and applications that are relevant for the security team. * Ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving. * The solution should support automatic file submissions to sandbox environment for malware analysis. * Ability to monitor critical operating system and application elements files, directories, registry keys to detect suspicious behaviour, such as modifications, or changes in ownership or permissions. |
| **Servers Antivirus Protection** | * Solution must be Air gapped/ On -Premises * Solution must to be managed by a single console * must comply with data residency and sovereignty rules * The solution must provide all the functionality from a single OEM/OSM * Servers Antivirus Protection 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.) * Protection Against Malicious Attacks |
| **Web Gateway Protection Software** | * Solution must be Air gapped/ On -Premises * Solution must to be managed by a single console * must comply with data residency and sovereignty rules * The solution must provide all the functionality from a single OEM/OSM * be deployable as an Appliance (bare metal) or Virtual Appliance that can support VMware and other virtualization platforms. * to scan inbound and outbound traffic for malware. * prevent malware from entering the network. * "Block and Report: virus and spyware downloads, botnets, C&C communication, malware callback attempts, tunnelling., blended threats, web threats, worms, bots, spyware, key loggers, malicious mobile code, rootkits, phishing, content threats, non-business content, ActiveX and Java applets" * decrypt, inspect and re-encrypt HTTPS content. * support zero-day exploit scanning and detection of advanced persistent threats and botnets, by integration with malware sandbox system using execution analysis to inspect suspicious files offline. * protect against new threats and suspicious activity in real time. * identify and blocks botnet and targeted attack C&C communications using global threat intelligence. * perform URL categorization and reputation measurement to identify inappropriate or malicious sites in real-time. * "Support multiple deployment modes: Bridge mode, Forward Proxy, Reverse Proxy" * integrate with ICAP devices. * provide web request caching for enhanced performance. * monitor all known communication protocols and applications. * centralize logging, reporting, configuration management. * support scanning for zero-day exploits and browser exploits. |
| **Email Gateway Protection** | * Solution must be Air gapped/ On -Premises * Solution must to be managed by a single console * must comply with data residency and sovereignty rules * The solution must provide all the functionality from a single OEM/OSM * scan incoming and outgoing emails to intercept unsolicited messages, inappropriate content, and dangerous viruses. * provide advanced threat protection and/or gateway module on the same hardware/virtual appliance. * integrate to a native cybersecurity platform for a broader visibility and expert security analytics, leading to more detections and an earlier, faster response. * integrate into existing anti-spam/antivirus network topology by acting as a Mail Transfer Agent in the mail traffic flow (MTA mode) or as an out-of-band appliance monitoring the network for cyber threats. * leverage an Email Reputation Services (ERS) technology to maximize spam protection and determine spam based on the reputation of the originating Mail Transfer Agent (MTA). * check all inbound SMTP traffic by the IP databases to see whether the originating IP address is clean, or it has been blocked as a known spam vector. * support directory harvest attack (DHA) protection to prevent senders from using a directory harvest attack (DHA) to obtain user email addresses for spam message transmission. * support SMTP traffic throttling to block messages which reaches the specified threshold. * support Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication (DMARC) email validation system to detect spoofing and phishing by verifying servers that are authorized to send email messages for a domain. * add approved and blocked senders list based on domains, IP address or subnet, or email address. * support all Industry Based operating systems in its custom sandbox virtual machines. * protect against spam, malware, phishing, BEC, and ransomware email attacks. * use advanced detection technology to discover targeted threats in email messages, including spear-phishing and social engineering attacks. * identity and detect graymail based on their category (e.g. marketing and newsletter, social network notifications, forum notifications, bulk email message). * support predictive machine learning technology to detect emerging unknown security risks in email messages. * support attachment analysis and content filtering that utilizes multiple detection engines and sandbox simulation to investigate file attachments. Supported file types include a wide range of executable, Microsoft Office, PDF, web content, and compressed files. * have an integrated threat simulation sandbox environment to analyse files, including password-protected archives and document files, and URLs to test for malicious behaviour, detect exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviours or characteristics. * support URL rewriting and URL time-of-click protection capabilities. * have a web reputation technology to scan URLs in email messages and track the credibility of web domains by assigning a reputation score based on factors including website's age, historical location changes and indications of suspicious activities discovered through malware behaviour analysis, such as phishing attacks that are designed to trick users into providing personal information. * support dynamic URL scanning and crawl on the web pages of untested URLs in real-time to determine whether the pages contain malicious patterns to keep users from zero-day phishing attacks. * be able to perform actions on email messages with QR codes to protect against image-based QR code phishing attacks. * include Business Email Compromise protection. Business Email Compromise (BEC) protection to protect organizations against sophisticated scams targeting businesses that regularly send wire transfers to international clients. BEC scams usually exploit vulnerabilities in different email clients and make an email message look as if it is from a trusted sender. * support detection of cousin domains (or look-alike domain) in email messages (from and reply to headers) based on the settings you configure to detect spam and phishing messages. * support policy-based Email Encryption to encrypt email content for confidentiality and secure delivery in MTA mode. * be able to share indicators of compromise (IoC’s) with both network and endpoint security layers. * support MITRE ATT&CK framework for effective threat detection and response. |
| **Extended Detect and Response (XDR)** | * Solution must be Air gapped/ On -Premises * Solution must to be managed by a single console * must comply with data residency and sovereignty rules * The solution must provide all the functionality from a single OEM/OSM * 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. * The XDR solution should allow the Analyst to perform threat hunting. The solution should support the use of complex filters to perform queries to all available data (detection logs, telemetry) coming from the Advanced Endpoint Protection agents across endpoints and servers and the network sensors. All functionalities must be on-prem and able to function in an air-gapped environment. * The solution should be able to integrate with real-time threat intelligence to consume feeds, filters and detection models, in the case of air-gapped environments the solution must have a procedure to get intelligence feeds, filters, detection models, and other signatures in a manual method. * 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. * The XDR solution should provide advanced protection capabilities for non-file-based threats example fileless attack protection, protection of web based threats example preventing the access to dangerous websites, connections to C&C servers, behavioral protection example protection of ransomware associated behaviors such as unauthorized encryption activities. * The XDR solution should provide protection to the user when browsing in internet, attempting to connect to dangerous websites * The XDR solution should provide a bidirectional and stateful host-based FW. It should allow the administrator or analyst to configure granular FW rules to filter packets by IP address, Port and Mac address. It should support all IP based protocols and frame types. * The solution should be able to detect threats on unmanaged devices or devices where the security agent is not installed, to achieve that the solution should leverage the use of NDR/Network Sensors integrated with the XDR component. * Single data lake that is on-prem and capable of functioning in an air-gapped environment. * The solution should have a built-in High Availability feature. * "The XDR solution must allow the security analyst to perform response actions during manual investigations, from the details of the correlated detections the response actions are: * Collection of suspicious files from remote endpoints and servers. * Remote shell sessions to remote endpoints and servers. * Isolation of endpoints and servers from the network. * Send suspicious files to a sandbox for detonation and analysis * Memory dumps and termination of process" * The solution must have in-built playbooks to automate the execution of response actions and enrichment of alerts, in addition it must allow the Security Analyst to build custom playbooks. * The XDR solution should have integration with 3rd party components example but not limited, SIEM, Threat Intelligence platforms, Ticketing systems, FWs etc. * The XDR solution should have integrated Threat Intelligence and support the integration with 3rd party Threat Intelligence sources (through standard methods TAXII, API, MISP, manually added) to consume and share intel feeds, perform auto and manual sweepings to identify IOCs matches in the environment. * The XDR solution should allow the Analyst to trigger response actions directly from the results of the query, example: from the investigation results, select objects to be added to the blocking list, select the endpoint to be isolated from the network. * The XDR solution should allow the Analyst to perform threat hunting. The solution should support the use of complex filters to perform queries to all available data (detection logs, telemetry) coming from the Advanced Endpoint Protection agents across endpoints and servers and the network sensors. * The sandbox should support the analysis of different file types. |
| **Network Detection and Response (NDR)** | * Solution must be Air gapped/ On -Premises * Solution must to be managed by a single console * must comply with data residency and sovereignty rules * The solution must provide all the functionality from a single OEM/OSM * 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). * The NDR/network sensor should use different detection techniques, engines to identify malicious files, engines to identify traffic from applications, leverage reputation servers to identify the connection or connection attempts to malicious destinations. * The NDR/network sensor should support flexible deployment options, including different appliance sizes and the possibility to be deployed as hardware appliance or virtual appliance. * The NDR/network sensor solution should have a local reputation server deployed on-premises to answer File and URL/websites reputation queries from the appliances. * Able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections. * Upon detection of the threat, able to perform behavior analysis. * Provides risk-based alerts or logs to help prioritize remediation effort. * Solutions should be deployed on premises in an air-gapped environment along with on premise sandboxing capability and function fully. * Supports throughput up to 10 Gbps in single appliance. * Not causes interruption to the current network environment, as uses mirror or span ports to analyze network traffic. * Supports to monitor traffic from multiple segments like WAN, DMZ, Servers and network, simultaneously on a single appliance. * Able to detect any suspicious communication within and outside of the organization network. * Must have a correlation engine to automatically corelate across multiple protocol, multiple sessions and volume traffic analysis. * Provides correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal. * Able to detect Network Attacks and Exploits. * 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. |
| **DLP (Data loss Prevention/Protection) Solution** | * Solution must be Air gapped/ On -Premises * Solution must to be managed by a single console * must comply with data residency and sovereignty rules * The solution must provide all the functionality from a single OEM/OSM * Data identifier and template libraries for easy policy creation. * File type recognition, with support for: Executable files, Documents and encoding methods, Graphics, Vector Graphics, Multimedia files, Compressed files, Databases, Spreadsheets, Presentation and diagram files, Desktop publishing files, Linked and embedded files and Encrypted files * Data discovery capabilities that locate digital assets stored on laptops, desktops, and servers. * 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. * Expanded privacy protection that includes filters for: * Network channels: Network protocols, such as HTTP and FTP * System and application channels: A local computer’s applications and peripherals. * Multiple matching engines to detect structured and unstructured data. * Policy enforcement actions, such as block, allow, alert, encrypt, justify, and log. * Continuous data monitoring. * Web-based management console for policy configuration and deployment, consolidated endpoint reporting, fingerprint extraction, and updates * to restrict the copy or upload of certain data, based on keywords, regular expressions, or file types to external storage or to the Internet. * increase the speed of audits and enforcement with real-time reporting of integrated DLP violations. * 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. * create specific exceptions based on make and serial number of the USB storage device. * "Be integrated in the following security Solution solutions with no additional hardware: Endpoint, Mail Servers, Messaging Gateway and Web Gateway" * educate employees on corporate data usage policies through alerts, blocking and reporting. * give you visibility and control of data in motion. * track and record if sensitive data is flowing through network egress points. * identify risky business processes and help to improve organizational data usage policies. * detect and react to improper data use based on keywords, regular expressions, and file attributes. * simplify deployment with an add-on module with no additional hardware or software requirements. * provide at-least 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 or modify existing templates to suit our business requirements. * provide DLP functionality that can provide basic protection against leaks of confidential data by file extension, dictionary, and regular expressions. * support policy management that allows administrators to enforce preventative actions on messages based on scanning conditions. * can send a notification to the sender of the email about the detention/modification of the message or the removal of attachments from it. * "Support enhanced directory service integration:   + LDAPv3-compliant directory service servers   + Multiple Active Directory/LDAP servers for user authentication and policy matching   + Kerberos authentication for Active Directory integration" * provide Role Based Access Control (RBAC) capability |

**I, the bidder (Full names) …………………………………………………………. representing (company**

**name) …………………………………………………………….** Hereby confirm that I comply with the above

**Technical Functional/ Product Requirements** and understand that it will form part of the contract and is legally binding.

Thus, done and signed at ……………………………………. On this………day of…………….….20….

……………………………….

**Signature Designation**