

DRIVING NEW FRONTIERS FOR SUSTAINABLE GROWTH

**REQUEST FOR PROPOSAL FOR THE ACQUISITION OF INTEGRATED
CLOUD EMAIL SECURITY SOLUTION, LICENSING AND SUPPORT FOR A
PERIOD OF 36 MONTHS AT AIRPORTS COMPANY SOUTH AFRICA**

TENDER NUMBER: COR6857/2022/RFP



**AIRPORTS COMPANY
SOUTH AFRICA**

AGENDA

- 
- 1 Introductions
 - 2 Bid Schedule
 - 3 General Administration
 - 4 Minimum Administrative Requirements
 - 5 Evaluation Criteria
 - 6 Tender Document Organisation
 - 7 Bidders Response File
 - 8 Technical Requirements
 - 9 Questions
 - 10 Closing Remarks



AIRPORTS COMPANY
SOUTH AFRICA





BID SCHEDULE

Activity	Date
Bid Advertisement	28 April 2022
Bid documents issued	28 April 2022
Optional Briefing Session	10h00 – 12h00, 12 May 2022
Enquiries and clarification	27 May 2022 at 17h00 PM
Tender Closing date	12h00, 03 June 2022
Bid Evaluation	June 2022
BAC Submission	July 2022
Award to Successful Bidder	July 2022





GENERAL ADMINISTRATION

- **ENQUIRIES AND CLARIFICATION:**

- To be directed to sydney.mfeka@airports.co.za cell : 062 934 0554
- **All enquiries must have a tender reference number and description on the subject of the email**

- Please submit your submission through email to Sydney.Mfeka@airports.co.za. On the subject of the email use the following “COR6857/2022/RFP - REQUEST FOR PROPOSAL FOR THE ACQUISITION OF INTEGRATED CLOUD EMAIL SECURITY SOLUTION, LICENSING AND SUPPORT FOR A PERIOD OF 36 MONTHS AT AIRPORTS COMPANY SOUTH AFRICA”
- RFP Submission checklist in conjunction with Functional/Technical evaluation criteria elements
- **SUBMISSION AND CLOSE OF BID: Friday, 03 June 2022 and closes at 12:00pm**



EVALUATION PROCESS

Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Check if all the documents have been received	Check if Bidder meets the mandatory criteria/requirements	Evaluate on functionality or the technical aspect of the bid	Evaluate price and Preference (B-BBEE)	Post tender negotiations



MANDATORY REQUIREMENTS

- Bidders must provide relevant OEM Accreditation for the proposed Integrated Cloud Email Security solution implementation with integration into M365 APIs based implementation.
- Bidders must provide the certification for the cloud environments being utilized as being certified in the following (SOC-2 or ISO 27001)
- Bidders must provide a minimum of three (3) contactable reference(s) letters where an integrated cloud email security solution with integration into M365 APIs for advanced mail protection features was successful implemented.



MINIMUM ADMINISTRATIVE REQUIREMENTS

** ACSA will only award this tender to a bidder whose tax affairs have been confirmed to be in order. Provide the valid pin.

Bidders must be registered on Central Supplier Database (CSD), Attach CSD registration Certificate.

Bidders MUST meet the Minimum Administrative Requirements.

Compliant (Compliant) bids will then proceed to next phase of evaluation



EVALUATION CRITERIA

Hurdle phase - Bids MUST obtain Minimum qualifying score of 70 points in order to proceed to the next phase of the evaluation. **Annexure B is very critical.**

DEMONSTRATE THE EVALUATION CRITERIA



TENDER DOCUMENT ORGANISATION

The Tender Pack is organised as follows

- **RFP Document**
 - Annexure A - Scope of work
 - Annexure B – Evaluation Criteria
 - Annexure C - ACSA Non-Disclosure agreement



NOTICE

Bidders are requested to always check on e-tenders portal for the updates.

All Questions and Answers will be posted on e-tenders portal

www.etenders.gov.za

And any other updates



BIDDERS RESPONSE FILE

Bidders are required to ensure that each returnable document is returned under the correct Appendices as shown in the Main RFP document.



ARCHITECTURAL ANALYSIS

1 Planning

- Establish what information exists within Forrester and Gartner for Email Security Gateways and Integrated Cloud Email Security (ICES) Solutions.
- Explore who the leaders, strong performers & contenders are for Forrester and who the leaders and challengers are for Gartner.
- Establish what the criteria that are generally used in the market are with a view to how these would influence ACSA's decision

3 Results & Direction

- Document Results based on evaluation criteria
- Present results to key stakeholders (This includes engagement with VP analysts from independent research and consulting firms)
- Establish what potential future direction ACSA may take based on results (Consideration for RFP open to market with clear SOW and evaluation criteria)

2 Analysis

- List the most significant ICES providers (With consideration for existing ACSA estate, strategic objectives and current investments, specifically in relation to M365)
- Analyze how they are able to deliver on Malicious attachments protection, protection against malicious links, protection against impersonation, management and operations reporting, deployment and integration, governance alignment and continuous improvement
- Link "ability to deliver" to functional and non-functional requirements the platform must meet

The Email Security market faces increasing client demand for cloud-delivered solutions and is splitting between solutions focused on Secure Email Gateways or Integrated Cloud Email Security Solutions. Continued increases in the volume and success of phishing attacks and migration to cloud email require a revaluation of email security controls and processes.

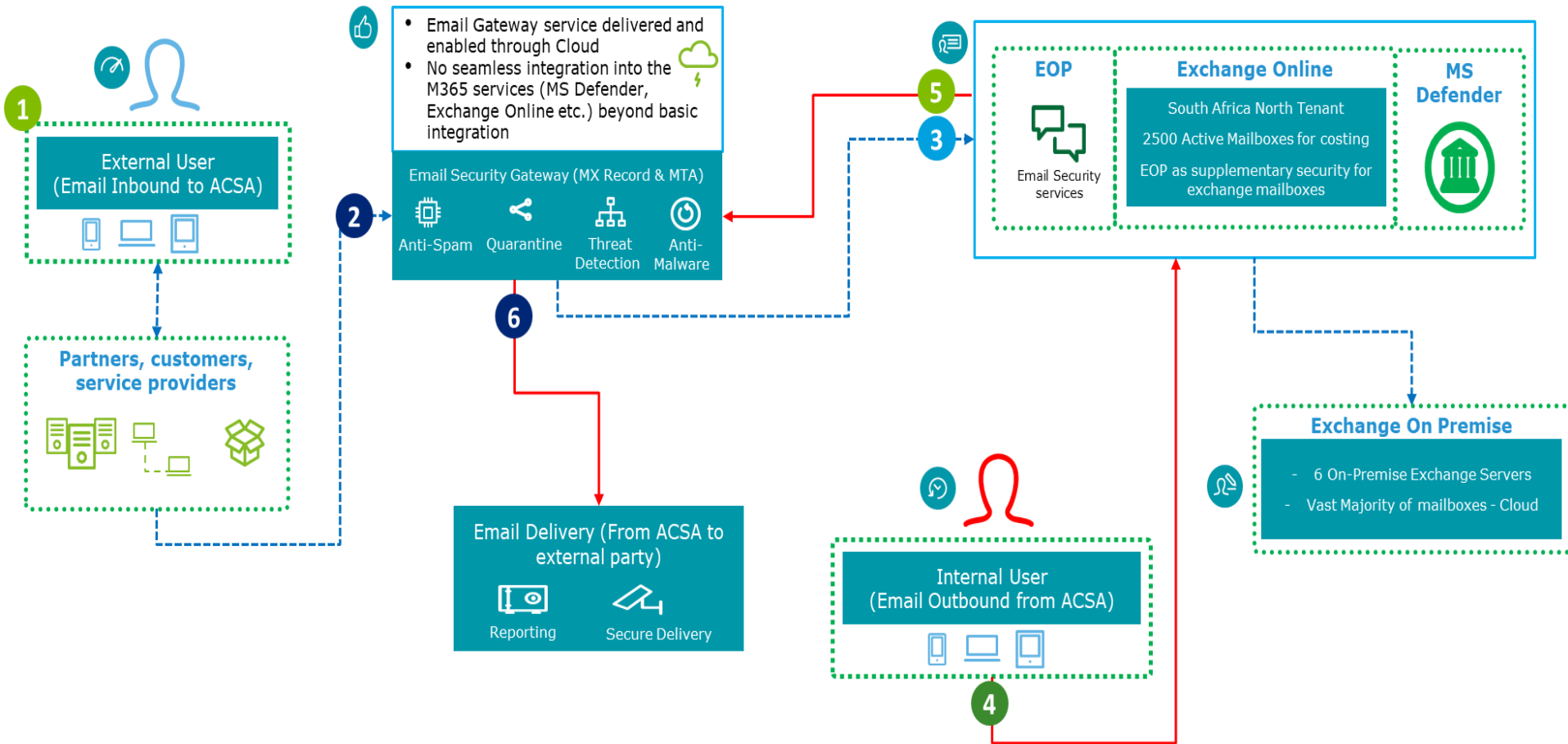
Solutions that integrate directly into cloud email via an API, rather than as a gateway, ease deployment and improve detection accuracy, while still taking advantage of the integration of the bulk of phishing protection with the core platform. The evolution in threats has led to increased demand for other techniques and services, such as domain-based message authentication, reporting and conformance (DMARC), cloud access security broker (CASB)/API integrations, continuous awareness and mail-focused security orchestration, automation and response (MSOAR)



CONCEPTUAL ARCHITECTURE

1 2 3 **External originating email flow**

4 5 6 **Internal originating email flow**



ACSA M365 INVESTMENT

Confidential



AIRPORTS COMPANY SOUTH AFRICA

16



Microsoft Security Enabling Investment

Microsoft 365 E5

Protection Domains	Technologies	Areas of Coverage
Identity and Access Management	Azure Active Directory P2	User accounts
	Windows Hello	Device Access
	Credential Guard	Device Access
	Azure Information Protection P2	Data Governance
	Microsoft Cloud App Security	App & Information Governance
	Office 365 Cloud App Security	App & Information Governance
	Office 365 Data Loss Prevention	Data Governance
	Windows Information Protection	Data Governance
	BitLocker	Data Protection
Threat Protection	Windows Defender Advanced Threat Protection	Endpoint Protection
	Office 365 Advanced Threat Protection	Office Cloud Protection
	Office 365 Threat Intelligence	Office Cloud Protection
	Azure Advanced Threat Protection	Hybrid Identity Protection
	Device Guard	Device Protection
Security Management	Secure Score	Security Controls Maturity Management
	Microsoft security and compliance center	Security Controls Maturity Management
	Windows Security Center	Security Controls Maturity Management
Compliance	Advanced eDiscovery	Data Governance and Compliance
	Customer Lockbox	Data Governance and Compliance
	Advanced Data Governance	Data Governance and Compliance

Security Operations Center



Azure
Sentinel

Security Information and Event Management
Security Orchestration, Automation and Response (SOAR)
Threat Assessment & Hunter
Threat neutralization
Security Analytics
Incident Response Workflow
Forensics
Malware Analysis
Threat Research
Threat & Infiltration Propagation & Simulation
Risk Management Workflow
Reporting & Dashboarding





QUESTIONS





CLOSING REMARKS

- FEEDBACK ON ACSA TENDER PROCESS; AND
- ERRORS IN THE TENDER DOCUMENT
- ACSA CONTRACT TEMPLATE TO BE USED – PROPOSED AMENDMENTS



**THANK YOU
&
GOOD LUCK!**

