The Arab American University
Purchasing Procurement Dep.

الجامعة العربية الامريكية
دائرة اللوازم والمشتريات

التاريخ: **16/11/2022**

رقم الاستدراج: **Q063-2023**

السادة: ....

تلفون: ....

إيميل: ....

استدراج عروض أسعار: الرجاء تزويدنا بأسعار اللوازم التالية شامل لضريبة القيمة المضافة: **BR2223-000122**

#	اسم الصنف	الوحدة	الكمية	السعر	اجمالي تكلفة البند
1	Email Security Solutions including Email gateway, Email ATP for Office 365	EACH	1		

المجموع الكلي (ش.ض)	دولار	

تعليمات الاستدراج | **ختم وتوقيع المورد:**

**	آخر موعد لتسليم العروض هو يوم:	الثلاثاء
**	الموافق:	11/22/2022
**	طبيعة البنود المطلوبة:	Email Security Solutions
**	بعملة:	دولار
**	الأسعار تشمل التوصيل ل:	الحرم الرئيسي - جنين
**	نوع التوريد:	توريد كامل
**	يرجى إرسال العرض ب:	بالظرف المغلق

شروط الاستدراج:

** ضرورة تحديد مدة الكفالة إن وجدت.

** ضرورة تحديد مدة التوريد من تاريخ استلام امر الشراء، و في حال عدم الالتزام يتم فرض غرامة تأخير .

** ختم وتوقيع المورد المعتمد على هذا النموذج، وكتابة رقم الاستدراج واسم الشركة كما هو مسجل لدى الضريبة على الظرف.

** للمراجعة والاستفسار بخصوص المواصفات يرجى الاتصال على هاتف 042418888 رقم داخلي 1481

** للمراجعة والاستفسار بخصوص المواصفات عن طريق فاكس 042510972 أو بريد الكتروني manal.daraghmah@aaup.edu

** لمشاهدة العطاءات والاستدراجات، يرجى الدخول الى الرابط http://www.aaup.edu/tenders

مدير دائرة اللوازم و المشتريات
أ. حسن ربايعة
دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING DEPARTMENT
16/11/22

Request for Quotation (RFQ)

Email Security Solutions including Email gateway, Email ATP for Office 365

Table of Contents

General Terms & Conditions

1. The Bidder, Vendor or OEM Solution must possess all the required specifications mentioned in Part 'Mandatory Requirements'.
2. The Bidder, Vendor or OEM should not be currently blacklisted by any Govt. dept. /Public Sector Unit.
3. The Bidder, Vendor or OEM must be Gartner's quadrant, Forrester, NSS Labs, or any equivalent Test report & certifications.
4. The Bidder, Vendor or OEM should be in the 5. Gartner Magic Quadrant and Forrester for last 3 years.
5. The Bidder, Vendor or OEM should have deployed similar type of solution within the last 2 years in Palestine.
6. The Bidder, Vendor or OEM must have support office in Palestine.
7. Bidder, Vendor or OEM must be able to provide a Presentation and POC on request.

Cloud Email Security Gateway

- Proposed solution must have fast, comprehensive email protection with a large threat detection network capable of visibility into 100 thousand emails per day, with 50 thousand malware samples as minimum without service degradation.
- Block unwanted email with reputation filtering, which is based on threat intelligence.
- Support at least 600 User email accounts.
- Sophisticated Spam protection with catch rate of up to 99%.
- Forged Email Detection and protection.
- High-performance virus scanning solution integrated at the gateway.
- Graymail detection and safe unsubscribe.
- Advanced Malware Protection with Advanced Threat Grid to provide file reputation scoring and blocking, file sandboxing, and file retrospection for continuous analysis of threats.
- *Sandbox environment must be capable for executing file submissions of 1500 per hour, during business peak hours, without introducing queuing delays.
- Outbreak Filters to defend against emerging threats and blended attacks.
- Data Loss Prevention feature to prevent sensitive information from leaking out.
- Encryption - Allow us the capability to encrypt emails in transit.
- Protection against executable files (direct or compressed), malicious code, scripts and malformed web addresses.
- Protection against Email DoS attack (Denial of Service) and Mail flooding.
- Protection against malicious URL.
- Whitelisting/blacklisting capabilities (Per user or globally).
- Alert, notification, summary dashboards, built-in reporting and blocking.
- *Deep email header inspection.
- Preventing Open Spam Relays from inside/outside organization.
- The proposed solution must support multiple MX record hosting, by which the solution must be capable for delivering emails through different interfaces with multiple IP addresses.

دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING DEPARTMENT

- High Availability.
- Real-time reporting capabilities.
- Scheduled email reports on a variety of activities.
- System overview dashboard - Monitor and report on outbound messages from a centralized, custom system overview dashboard. Unified business reporting with a single view for comprehensive insight across your organization. Get the details of any report for advanced visibility.
- Detailed message tracking - Track a message by envelope recipient, envelope sender, subject, attachments, and message events including DLP policy or IDs.
- The proposed solution must cover the cost of licenses renewal for 3 years starting from the date of preliminary acceptance.

Solutions to Email Security Risks

To protect against e-mail threats, use specialized anti-phishing technology and:

- Use a strong email password
- Monitor your email habits
- Use two-factor authentication
- Look out for “Phishing Emails”
- Don’t open attachments without scanning them first
- Never access emails from public WiFi
- Change your password as often as possible
- Avoid giving your email address away

Automated Response & Incident Management

- The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible.
- The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI
- The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI
- The incident should display the complete identity of the sender (Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager
- The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allow for deletion even by the product administrator
- The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.
- The solution should have options for managing and remediating incidents through email by providing incident management options within the in the notification email itself.
- Integration with Security Data lake to be implemented in future will be got done without extra cost.

Reporting and Analytics

- The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network).
- The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients
- The reports should be exported to at least CSV, PDF, HTML formats.
- The system should provide options to save specific reports as favorites for reuse.
- The system should have pre-defined reports which administrators can leverage
- The Proposed Solution dashboard must display the number of cases in the designated period that fall above the risk score threshold that you've selected. Risk score thresholds must be customizable and instantly produce a report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.
- Workflow operations includes operations such as:
  - -Assigning incidents
  - -Changing incident status
  - -Changing incident severity
  - -Ignoring incidents
  - -Tagging incidents
  - -Adding comments

- The solution should integrate with any SIEM solution.
- Features for disabling or modifying default rules, scenarios, and configurations should be available.

Email ATP

- The Solution should provide email attachment sandboxing for both Inbound and outbound mails.
- The Solution should have multiple AV/APT engines for anti-virus and malware scanning. Solution should provide on cloud AV/APT service from day1
- The Solution should provide email attachment sandboxing for both Inbound and outbound mails. The Solution should be patient zero protection as well.
- The Solution should Full System Emulation techniques to protect against memory attack with Multiple file format support.
- Sandbox Service should have Kernel visibility with minimal OS version dependencies.
- It should support execution of OS X files and Android applications.
- It should support the execution of various OS or support hardware emulation.
- Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, WPD, XML, XPS and another file type. Spreadsheet: CSV, ODS, SYLK, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and another file type. PowerPoint: ODP, PPS, PPT, PPTX, PPTM, POTX, POTM, PPAM and another file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MACH- O, MSI, PIF, PL, PS1, PY, SCR, SH, SYS, VB, WSF and another file type. Archive File: 7Z, ACE, APK, ARJ, BZIP, CAB, CHM, DMG, GZ, ISO, JAR, LHA, LZMA, NUPKG, RAR, TAR, TARGZ, TNEF, WAR, XAR, XZ, ZIP, ZIPX and another file type. Media: ODG, SVG, SWF, TIFF and another file type. Misc.: CLASS, EML, HTML, IQY, PCAP, URL and another file type.
- The solution should provide the exception bypass, Email id exclusion (send or receive) with features for override.
- The Proposed solution should provide 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.
- The proposed solution should have multi-layered detection framework including: static, behavioral, heuristic, signature-based, file context, metadata and machine learning detection methods.
- The proposed solution should be able to provide in- depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.
- There should be options to bypass scanning of a particular domain/file type from APT.
- The solution should have option to store email or file in queue in case the similar file with same hash value receive in the given timespan then the action should be followed.
- Solution should have Content disarm and reconstruction (CDR) capability, which protects against exploits and weaponized content that have not been seen before.

Mandatory Requirements

- Bidder, Vendor or OEM will be fully responsible for Implementation, Configuration, Installation and tanning of Cloud Email Security Gateway.
- Bidder, Vendor or OEM official in-person tanning for at least 2 employees is a must.
- Ongoing Support: Bidders must disclose detailed information confirming the warranty period, replacement strategy of faulty parts, spare parts stock status and length of repair period. Bidders should have sufficient workforce and equipment to provide quality service.

  Detailed System/Equipment Requirements and Technical Architecture:

  Technical Specifications –
  - The bidder should clearly specify and state the methodology, architecture, and design to implement the primary site along with the integration with the current email infrastructure.
  - The entire schedule, with specific milestones must also be presented.
  - Solution Architecture Design.
  - Implementation methodology along with Node and connectivity details.
  - Issue, Suggestion & Risks.
  - Project time schedule & dependency.
  - Integration & Acceptance Test.
- After the installation is complete, Bidders are required to carry out a complete series of commissioning and acceptance tests (POC) for the complete solution with documentation.
- The acceptance tests (POC) shall be carried out to demonstrate the capacity and effectiveness of each feature installed.
- Provide all document and materials which may be required to test (POC) the solution provided.
- Solution should protect against common threats against latest Email Security Risks in 2022

  1- Spoofing and Phishing
  2- Vulnerabilities in E-mail Security
  3- Domain's squatting
  4-Client-Side Attacks
  5-Dangerous Files
  6-Crypto-ransomware
  7- Configuration Errors
  8- Browser Exploit Kit
  9- Spear Phishing attacks and Business E-mail Compromise (BEC)
  10-File Format Exploits.
- All currency in the proposal shall be quoted in $ USD Dollars and prices shall be Including VAT.

Contact details

Please supply details of the certified and expert person(s) at your organisation who can be contacted and verified by AAUP. Please give their name, title, address and location, telephone number, fax number and e-mail address.

Company details

a) Please give details of your company, stating its full registered address and company registration number and all legal documents.

b) Please set our details of the partner and vendor company and specify the relationship between it and your company and provide detailed level of partnership and certification.

Your Organisation's staff

a) Please give details of your staff numbers, skills, duties and locations those who will be associated with the proposed work. Please set out any key skills or employee dependencies and the availability of replacement skills in those areas.

b) Please explain the organisational and management structure of your organisation (including an organogram of your executive management) and the roles and responsibilities of the management teams involved in relation to the services in the proposed solution.

Your history, approach, vision and values

a) Please describe in brief terms, your organisation's history and the history of provision of outsourcing services.

b) Over what period of time have you been providing services which are similar to those which are the subject of our request.

c) Please provide details of your corporate and business values and how this affects your organisation and the services it offers.

Customers

Please supply a list of customers to whom similar services to our request.

References

Please provide references of work done in the past and the success ratio where services were provided similar to our request.

Standards and procedures

a) Please provide details of your quality assurance processes and management systems and if applicable any quality related accreditations or certifications you hold.

b) Please set out your policies, procedures and processes in relation to the protection of all information and data in relation to the services and in relation to other security and confidentiality matters.

c) Please provide a brief risk management overview of the risks that you foresee in the delivery of each area of the requirements you are responding to. Please categorise these risks according to whether they are risks for AAUP, for you, or risks that are to be shared jointly. Please specifically state how you propose to manage and/or mitigate these risks.

d) Please confirm that all goods, services, software and intellectual property which would be provided or supplied by you in the course of the provision of the services are compliant with applicable regulatory framework.

e) Please give details of the systems and processes that are intended to be used to ensure security of personal customer data.

Support and Training

A. Support should be available 24/7/365 according to follow the sun principle
B. Local partner of the vendor must have trained personnel and an available stock of hardware / software in order to provide an immediate response
C. Official training is a must for AAUP responsible team and security member.

Other capabilities

Please set out any additional capabilities or other services you provide beyond the scope of those contained in the proposed solution which may be of interest to AAUP.

دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING
DEPARTMENT