الجامعة العربية الأمريكية

فلسطين PALESTINE

2000

ARAB AMERICAN UNIVERSITY

دائرة اللوازم والمشتريات

عطاء رقم 2021.22/ T24

Endpoint and EDR Security solutions

2021-2022

عطاء Endpoint and EDR Security Solutions

وثائق العطاء:

أ- الجزء الأول:

(1) دعوة العطاء

(2) الشروط والتعليمات التنظيمية للعطاء

(3) طريقة الدفع

ب- الجزء الثاني:

(1) جدول الكميات والمواصفات الفنية

الجزء الأول (1)

إعلان طرح عطاء رقم T24-2021.22

Endpoint and EDR Security Solutions

تدعو الجامعة العربية الأمريكية الشركات المختصة الى المشاركة في العطاء المذكور أعلاه.
يمكن الاستفسار أو الحصول على وثائق العطاء من دائرة اللوازم والمشتريات في الجامعة/ مبنى الدوائر الإدارية الطابق الثاني، هاتف- 2418888 04- تحويلة 1488 فاكس 2510972 04 بريد الكترونيpnp@aaup.edu
مقابل مبلغ غير مسترد مقداره 50 دولار أمريكي تدفع في إحدى البنوك المعتمدة وذلك اعتباراً من
يوم (السبت) الموافق 12/2/2022

ملاحظات :

1. تقديم عرضين: فني ومالي، وسيتم دراسة العروض فنياً ومالياً لاختيار العرض المناسب.
2. آخر موعد لتسليم العطاءات هو في تمام الساعة الثانية من يوم(الاحد) 27/2/2022 ولنفس المكان.
3. يجب تقديم كفالة دخول عطاء 5% من قيمة العطاء على شكل كفالة بنكية أو شيك بنكي مصدق لصالح الجامعة العربية الأمريكية .
4. الأسعار (دولار) وتشمل جميع الضرائب بما فيها ضريبة القيمة المضافة وعلى المورد تقديم الفواتير الضريبية وشهادة خصم المصدر.
5. الجامعة غير ملزمة بأقل الأسعار وبدون إبداء الأسباب.
6. رسوم الاعلان على من يرسو عليه العطاء.
7. بإمكانكم الاطلاع على النظام الداخلي لدائرة اللوازم والمشتريات من خلال زيارة صفحة الجامعة العربية الامريكية على الانترنت. www.aaup.edu

دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING DEPARTMENT

(2) الشروط والتعليمات التنظيمية للعطاء

1. على جميع المشاركين في العطاء الالتزام التام بهذه الشروط والتعليمات، وهي تعتبر جزءاً لا يتجزأ من أي أمر شراء أو عقد يبرم مع المشارك الفائز ما لم ينص صراحة على خلاف ذلك في أمر الشراء أو العقد.
2. في هذه الشروط والتعليمات يرمز إلى "الجامعة العربية الامريكية بالاختصار (AAUP).
3. يجب أن تكون الشركة المتقدمة للعطاء مسجلة رسمياً ومشتغلاً مرخصاً.
4. **تقدم الأسعار (دولار) شاملاً لجميع الضرائب** بما في ذلك ضريبة القيمة المضافة (VAT).
5. يلتزم المشارك الفائز بتقديم شهادات خصم المصدر والفواتير الضريبية اللازمة وأية مستندات قانونية أخرى تغطي عملية الشراء.
6. يجب أن تشتمل الأسعار على جميع المصاريف المطلوبة من النقل والتركيب والتشغيل والفحص **والصيانة والتدريب** في المواقع المحددة في جدول المواصفات والكميات المرفق.
7. يجب أن تكون الأسعار المقدمة سارية المفعول لمدة لا تقل عن (90) يوماً من تاريخ تقديم العرض.
8. على المشارك الفائز تقديم كفالة حسن تنفيذ خلال أسبوع من تاريخ الاتفاقية بحيث تعادل (10%) من قيمة الاتفاقية على شكل كفالة بنكية صادرة عن إحدى البنوك العاملة في فلسطين أو شيك مصدق صادر لصالح "الجامعة العربية الامريكية".
9. إذا تخلف المناقص الفائز عن تقديم كفالة حسن التنفيذ عن الموعد المحدد في البند السابق فإنه يحق لـ (AAUP) إلغاء الإحالة.
10. إذا تخلف المناقص الفائز عن التوقيع على عقد التنفيذ و تسليم الكفالات والتأمينات المطلوبه منه خلال أسبوع من تاريخ قرار الاحالة، يعتبر مستنكفا عن تنفيذ العطاء ويصادر مبلغ الكفالة أو التأمين دخول العطاء بالاضافة الى ذلك يتحمل فرق السعر و/أو اي أضرار أخرى قد تلحق بالجامعة نتيجة استنكافه ويحرم من لمشاركة في عطاءات الجامعة لمدة عام.
11. اذا تخلف المناقص الفائز عن تنفيذ العطاء الذي احيل عليه او خالف شرطا من شروط العقد يحق للجامعة مصادرة كفالة دخول العطاء أو حسن التنفيذ أو جزء منها وتنفيذ العطاء مباشرة من الجامعة أو اية جهة تراها مناسبة بالاسعار والشروط والطريقة المناسبة ويتحمل المناقص أي فروقات بالاسعار مضاف اليها 15% من اجمالي قيمة العطاء.
12. يتحمل المناقص المتخلف دفع تعويض بدل اي عطل او ضرر قد يلحق بالجامعة نتيجة لذلك.

دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING DEPARTMENT

13. تعاد كفالة حسن التنفيذ بعد استكمال التوريد وجميع شروط العقد أو أوامر الشراء وبموجب الوثائق الأصولية اللازمة للاستلام.

14. على المشاركين في العطاء ارفاق كتالوجات عن المنتج.

15. يلتزم من يرسو عليه العطاء بدفع غرامة تأخير بواقع (0.1%) عن كل يوم تأخير من قيمة الأعمال المنجزة عن الوقت المحدد في الاتفاقية، ويتم احتساب هذه الغرامات من الدفعات المستحقة له أو من كفالة حسن التنفيذ.

16. يحق لـ (AAUP) إلغاء العطاء دون إبداء الأسباب كما أن (AAUP) غير ملزمة بإحالة العطاء على أقل العروض سعراً دون إبداء الأسباب. ولها أن ترفض كل أو بعض العروض المقدمة لها دون أن يكون لأي من المشاركين الحق في الرجوع إليها بأي خسارة أو ضرر ناجم عن تقديم عرضه ولا يترتب على (AAUP) أي التزامات مادية أو غير مادية مقابل ذلك، كما يحق ل (AAUP) تجزئة العطاء بما تراه مناسبا ودون ابداء أسباب.

17. يلتزم من يرسو عليه العطاء بتقديم كفالة بنكية (صيانة) بقيمة (5%) من قيمة الأعمال المنجزة صالحة لمدة عام من تاريخ تسليم الأعمال.

18. على المشارك في العطاء تقديم عرضه على أساس المواصفات الفنية االمبينة في وثائق العطاء وبموجب الكميات المحددة في جدول الكميات المرفق.

19. لا يجوز للمشارك في العطاء أن يتنازل لأي طرف آخر عن كل أو جزء من أمر الشراء دون الحصول على إذن خطي من (AAUP) مع الاحتفاظ بكامل حقوق (AAUP) وفقاً لشروط أمر الشراء.

20. عند دراسة العروض يؤخذ بعين الاعتبار كفاءة المناقص من الناحيتين المالية والفنية وقدرته على الوفاء بالتزامات العطاء وخبرته في تقديم اللوازم المطلوبة والسمعة التجارية والتسهيلات التي يقدمها ويجوز استبعاد عرضه لنقص كل أو بعض هذه المتطلبات.

21. لا تقبل العروض أو التعديلات التي ترد بعد التاريخ والموعد المحدد كآخر موعد لتقديم العروض.

22. يجب تعبئة جداول المواصفات المرفقة و لن ينظر بأي عرض لا يلتزم بتعبئة الجداول.

- ❖ **ويسمح بتقديم عرضين اثنين فقط كحد اقصى لكل بند.**
- ❖ **يجب تقديم عرضي الاسعار الفني والمالي بنسختين: الأولى ورقية، والأخرى الكترونية (محوسبة).**
- ❖ **تقديم العرضين المالي والفني الورقيين بالظرف المختوم، مع ضرورة وضع ختم الشركة والتوقيع على كل الصفحات (للعرض المالي بالذات).**

دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING
DEPARTMENT

(3)

طريقـــة الدفـــــــع

خلال (90) يوماً من التوريد والقبول والاستلام النهائي، مقابل تقديم الكفالات المطلوبة.

دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING
DEPARTMENT

الجـزء الثانــي

1. جـــــدول الكميـــــات والمواصفات الفنية
Endpoint and EDR Security Solutions

No.	Product	Qty	Unit Price USD	Total Price USD
	Endpoint and EDR Security Solutions	1		
Total				

في حالة وجود استفسار يرجى تزويدنا بها من خلال البريد الالكتروني للرد عليها **pnp@aaup.edu**

دائـرة اللـوازم والمشتريات
PROCUREMENT AND PURCHASING
DEPARTMENT

Table of Contents

1 General Requirements

1. The Proposed Solution must possess all the required specifications mentioned in Part 'Mandatory Requirements'.
2. The Proposed Solution should not be currently blacklisted by any Govt. dept. /Public Sector Unit.
3. The Proposed Solution must be Gartner's quadrant, Forrester Research, or any equivalent Test report & certifications.
4. The Proposed Solution should be a leader in the Gartner Magic Quadrant for last 3 years.
5. The Proposed Solution should have deployed similar type of solution within the last 2 years in Palestine.
6. The Proposed Solution must have support office in Palestine.
7. Solution should protect against common threats such as those identified in the OWASP top 10 latest release.
8. Proposed Solution Provider must be able to provide a Presentation and POC on request.

SOLUTION REQUIREMENTS

Functional Requirements

1. Must be able to prevent AAUP systems from Zero-Day exploits & attacks and not to rely on signature-based detection and protection methods.
2. Proven track record on effectively preventing enterprise endpoint systems from Ransomware and other types of advanced threats.
3. Must provide an intuitive white and black listing capability that is auditable and granular that can be applied to an endpoint, group of endpoints or system-wide.
4. The new solution should remove or minimize the current endpoint protection workloads that are manually handled by ITS staff.
5. Must be able to interoperate with future SIEM, IDS/IPS and other information security systems to provide additional level of protection through early threat detection and prevention.
6. Must be able to provide protection for diverse AAUP digital assets including Microsoft Windows, Linux, Android and Apple OSX based Mobile, desktops, laptops, tablets and servers.
7. Provide a consistent, functional, centralized administrative interface that is intuitive and easy to navigate.
8. Provide capability to make the routine tasks easier to manage.
9. Provide a secure, cloud-based, Hybrid or on-primes console for a single point of administration.
10. The solution should be able to automate the endpoint prevention by autonomously reprogramming and retuning itself using threat intelligence gained from behavioural analysis, reputation, AI and machine learning.
11. Doesn't rely on resource intensive detection and protection methods that can adversely affect the performance of installed AAUP devices.
12. Ability to fully protect and support the AAUP's mobile endpoints that can be disconnected from the networks for an extended period of time.

13. Must provide flexible email notification capability to alert AAUP staff about suspicious activities that may pose security threat to the AAUP's assets.
14. Solution must provide a REST API to communicate and interoperate with other AAUP systems to automate information security operational workloads.
15. All capabilities of the proposed solution must be delivered through a single endpoint agent that cannot consume more than 15% of resources of the installed device at its peak.
16. The solution's agent should have a minimum footprint and performance impact on the AAUP endpoints (should not noticeably impact end user's computing experience during scanning or continuous protection).
17. The administrative console should be scalable to accommodate all related AAUP workloads and must resilient enough to provide maximum uptime.
18. The vendor should provide 24x7 product support over multiple channels including web-chat, Zoom as well as the traditional channels such as email and phone support.
19. The vendor is expected to provide timely support for project planning, deployment, problem resolution for the proposed solution.
20. The vendor is expected to perform knowledge transfer of all necessary operational matter to ITS staff to ensure the AAUP can effectively manage and maintain all ongoing operations of procured solution to keep AAUP assets secure.

Technical Requirements

1. Agent applications should provide protection for the following endpoints types (Approximately **600 endpoints**):
    a. All Windows 7, 8.1 and 10 operating system versions (32 & 64 BIT) including variations of service packs
    b. Apple MacOS Devices
    c. Mobile Apple OSX and Android based systems
    d. Windows Server 2003, 2008, 2008 R2, 2012, @012 R2 and 2016
    e. All Open Source, Commercial and Custom build Linux OS and Server types and versions.
2. Vendor must list the minimum hardware and software requirements for its endpoint agent; specify supported browsers to manage its administrative console application and any other requirement that is necessary to manage the proposed endpoint protection solution.
3. Must be able to retain the administrative console logs for a minimum of 6 months.
4. The false positive threat identification should be less than 0.1% of the installed AAUP endpoints at any given time (for example, if the endpoint agent is installed on 5000 AAUP endpoints, the false positives should be less than 5).
5. The administrative console should be always responsive and accessible from anywhere to provide secure access to manage the endpoint protection solution.
6. The endpoint protection agent should not cause performance degradation on the installed AAUP systems.
7. The administrative console should adhere to responsive design principles to accommodate diverse endpoints (laptops, tablets and phones as applicable).
8. Proposed solution must provide capability to export the collected information to on-premises and other cloud systems for additional processing.
9. The solution's agent must be easy to deploy, re-deploy and manage through its life-cycle.
10. The solution should provide both real-time and historical reporting capability that is intuitive and easy to use.
11. Only relevant information should be presented to the authorized console user (i.e. security trimmed) based on the user's role in the system. However, the console administrator(s) should have ultimate access to the system and all its components.
12. The detected threat information should be communicated to the system administrators and designated ITS staff in real-time.
13. Console should provide all summary statistics in its main landing page.
14. Statistics for different type of threats should be simultaneously displayed in a real-time in the vendor's console.
15. Real-time threat statistics should be displayed in graphic and numerical forms.
16. System should have an open reporting architecture that easy to share, customize and export to other systems.
17. The solution should provide capability to generate status reports for the monitored endpoints on a predefined schedule.
18. Management system should be able to email the scheduled reports to identified AAUP staff.
19. Status reports should be generated in HTML, PDF and Excel formats in order to be shared with management and could be made available on an Intranet.

20. The solution should provide holistic and historic reporting of the protected endpoints (through real-time, ad-hoc and for a specific time period).
21. Any changes or upgrades to the management console should be scheduled and approved by the AAUP.
22. The administration console should be accessible to any authorized AAUP staff on any device and anytime.
23. The AAUP staff should be given different levels of access that is appropriate with their role in the support of the system (such as viewing real-time incident information and statistics and resolving individual incidents) as opposed to system-wide functions (creating and modifying policies for the solution) that is associated with the administrator level access.
24. The AAUP users should be able to be configure scheduled custom reports in addition to standard reports provided by the vendor.
25. Solution should support minimum Transport Level Security version 1.2 (TLS) to provide secure connections.
26. Solution's web console should be capable of filtering events to show only security related data that is relevant and requires immediate attention.
27. The centralized management console should facilitate a granular new agent deployment and control of remote workstations.
28. The proposed endpoint protection solution should not cause or introduce security vulnerabilities to the AAUP system.

Desired Requirements

1. Solution to interoperate with Active Directory through ADFS to provide access to system functions in addition to console's own local security database.
2. Provide integrated, remote remedial workflow, EDR and XDR capability that removes or reduces manual staff intervention.
3. Provide extensive Role-Based-Access (RBAC) to administrative console to ITS staff to enable AAUP staff to complete their workloads in a timely manner.
4. Able to replace the existing endpoint solution (Symantec Endpoint Protection Agents and software) without any consequence or loss of capability.
5. Provide protection from fileless malware.
6. Provide easy and intuitive global search capability that provides intuitive drill-down interface to assist in investigation of suspicious activities.
7. Prevent uninstall of endpoint protection agent from the AAUP owned devices by end-users who have elevated (high privileged) access on those systems.
8. Able to uninstall the endpoint agent from the installed systems through the management console.
9. Able to investigate and mitigate the potentially infected endpoints remotely.
10. Provide SMS notification capability to timely alert the AAUP staff about malware and security threats.
11. Provide extensive, interactive reporting with drill-down capability on captured incidents.

9. Provide extensive, full auditing capabilities for every step of the system workflows.
10. Integration with Azure AD, Microsoft 365 and Office 365 and other AAUP SaaS and cloud Services
11. Should take in consideration that the current Endpoint & EDR system will be expired by 10-April-2022.

2 Mandatory requirements

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.

دائـرة اللـوازم والمشتريات
PROCUREMENT AND PURCHASING
DEPARTMENT

c. Please set out your geographical locations which are relevant to the requirements set out in this RFP and the length of time you have operated from these locations.

Your Organisation's staff

d. 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.

e. 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 RFP.

Your history, approach, vision and values

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

g. Over what period of time have you been providing services which are similar to those which are the subject of RFP.

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

Customers

i. Please supply a list of customers to whom similar services to those contemplated by the RFP are provided and the types of services being provided.

References

j. Please provide references of work done in the past and the success ratio where services were provided similar to those being contemplated by the RFP.

Outsourcing experience

k. Please provide details of previous experience in providing similar services to the services envisaged in this RFP, particularly your experience which relates to implementation/transition, service levels, regulatory compliance, achievement of economies of scale and value for money. Please provide details of size and scale of these services.

l. Please specify any additional related services you could offer to AAUP and the benefits of such services.

Standards and procedures

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

n. 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.

o. 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.

p. 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.

q. 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 and Vendor on-person training and certification for 4 AAUP responsible team and security members.

Other capabilities

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

دائـرة اللـوازم والمـشـتـريـات
PROCUREMENT AND PURCHASING DEPARTMENT