Ref. ..... الرقم : .....

Date ..... التاريخ : .....

إعلان طرح عطاء لجنة شراء لوازم والخدمات الاستشارية (رئيسية)

تعلن جامعة الحسين بن طلال /لجنة شراء لوازم والخدمات الاستشارية (رئيسية) عن طرح العطاء التالي :			
رقم العطاء	موضوعه	ثمن نسخة العطاء	آخر موعد لإيداع العروض والشراء
2023/6	تجديد رخص إدارة مكافحة الفيروسات والجدار الناري	75 دينار غير مستردة	آخر موعد للشراء والإيداع نسخ العطاء الساعة العاشرة من صباح يوم الأربعاء الموافق 2023/10/4 آخر موعد لفض عروض العطاء الساعة الحادية عشر من صباح يوم الأربعاء الموافق 2023/10/4

يرجى من الراغبين في الاشتراك مراجعة أمين سر لجنة شراء لوازم والخدمات الاستشارية (رئيسية) في مقر الجامعة- معان -اعتباراً من تاريخه مع مراعاة ما يأتي :

1-إحضار رخصة مهن وشهادة تسجيل ساريتي المفعول (أصلية أو صورة مصدقة عنها) مع العرض المقدم .

2-تقديم نسخة أصلية من عرض الأسعار يرفق فيها (نموذج عرض الأسعار الأصلي).

3. توضع النسخة الأصلية في مغلف منفصل ويكتب عليها من الخارج بشكل واضح (النسخة الأصلية).

4. تقديم صورة عدد (2) من النسخة الأصلية من عرض الأسعار بالإضافة إلى نسخة إلكترونية على(C D) من العرض المقدم.

5- توضع كل صورة بشكل مستقل ويكتب عليها من الخارج وبشكل واضح.

6- تقديم كفالة تأمين دخول عطاء بنسبة (3%) من قيمة العرض المقدم بمغلف منفصل ويكتب علية من الخارج كفالة الدخول وبشكل واضح .

7- تسلم العروض لأمين سر اللجنة في مبنى الرئاسة الطابق الثاني في موعد أقصاه الساعة العاشرة صباحاً من يوم الأربعاء الموافق 2023/10/4 .

8- يحق للجامعة إلغاء العطاء دون أبداء الأسباب دون أن يترتب على ذلك أي مطالبة مالية أو قانونية.

9- الجامعة غير ملزمة بإحالة العطاء على اقل الأسعار ودون أن يترتب على ذلك أي مطالبة مالية أو قانونية.

10- تكون مدة العرض المقدم 120 يوما .

11- يعتبر نظام المشتريات الحكومية رقم (8) لعام 2022 جزء لا يتجزأ من وثائق العطاء .

12- طريقة الدفع حسب أنظمة وتعليمات الجامعة ، واي شرط يرد ضمن العرض بخالف ذلك لن يتم الاخذ به ، ويحق للجنة استبعاد العرض من الدراسة الفنية .

13- أجور الإعلان على من يرسو عليه العطاء مهما تكرر .

رئيس لجنة شراء لوازم والخدمات الاستشارية (رئيسية)

أ.د احمد محمد ابو جري

AL-Hussein Bin Talal University

Proposal For

(Security solution)

2023

1- Tender Sheet (RFP) Overview

The purpose of this RFP is to seek quotes to purchase hardware equipment's and Software needed to support the need for the following:

1. Next generation firewall
2. Endpoint Protection Platforms (EPP)

This document is an invitation for qualified bidders to offer their solutions and ideas to deliver, install, accommodate, and test such project based on latest technologies in this field, all technical details are mentioned in the technical specifications section.

2- General Terms & Conditions

- It will be the bidder's sole responsibility and on his own expenses to understand the site nature and environment and all requirement that are related to the tender or that may influence it's pricing.
- It is the bidder responsibility to deliver, install, configure, test and support the awarded systems with all of its hardware and software components.
- Bidders requiring further information or clarifications may notify AHU in writing at Central Tendering Department within one week from the date of publication the RFP, AHU will respond in writing to any request for information or clarification of the bid.
- Bidder should have enough experience and certified technical staff to do the installation and support. CVs for staff and reference for similar project must also be included in the bidder offer.
- If any Item needed during the installation and was not stated in the offer; then it is the bidder's responsibility to provide it at no cost.
- The bidder must respond to any written or telephone maintenance request by the university within 24 hours from the date of notification. Otherwise, the regulations and instructions in force at the university will be applied.
- The university has the right to exclude or change any of the components of the tender if the price exceeds the specified budget (where it is entitled to increase or decrease 25% of the required quantities).
- The total period of delivery of the project (supply, installation, operation, testing and training) is **6 weeks** from the date of submission of the tender issued by the university.
- The supplier company must provide a guarantee for all items and components of the tender including spare parts and technical support for the submitted programs and updates, and the guarantee must be covered by an official letter from the manufacturer for a period of not less than **Three years**.

3- Evaluations of Offers

These criteria used to evaluate the offers:

- Compliance with specifications.
- Price.
- Quality of proposed products (Brands).
- Bidder Qualifications (Team CVs & Reference)
- Warrantee, maintenance and technical support.
- Training.
- Installation and testing plan.
-

4- Requests for Proposal

- The RFP prepared by the bidder as well as all correspondence and documents relating to the RFP exchanged by the bidder and the university and supporting documents and printed literature shall be written in English.
- The offers containing erasures or alterations will not be considered until it is duly signed and stamped by the authorized signatory.
- Bids should be quoted in Jordanian Dinar (JD) only. Where other currencies are used, the bidder must specify the equivalent Jordanian Dinar and the exchange rate used. All applicable taxes must be clearly indicated.

5- Training

- Site Training: during installation and configuration, a knowledge transfer, and a detailed elucidation for every step of work must take place by the company team for AHU technical staff.
- Certified Training: The offer should include professional certified training courses for AHU technical team, it should be delivered by a vendor certified trainer.

6- Implementation, Installation and Testing Plan

- The bidder must provide an implementation plan. It must have detailed project schedule.
- Project schedule must take into consideration the work environment of AHU including the periods during which network and service interruption is not possible. These periods include but not limited to student registration period, online exams period, and ordinary working hours.
- All equipment and Software modules must be individually tested as well as the whole systems must be tested entirely.

7- Technical Specifications

- It will be the bidder responsibility to offer a complete system solution that will achieve all required specs.
- Bidders can quote for multiple options, and AHU has the right to exclude any Item.
- Bidders must provide all the patch cords that might be needed for connecting the offered solutions to AHU infrastructure.

7.1-anti virus

General Specifications	Quantity	Comply Yes/No For each
• **Integrated Management:** ✓ Must have a unified console for managing multiple products such as Advanced Endpoint Protection, Email Gateway, Server Security, Mobile Control etc ✓ All settings for these products MUST be configured from a Central Dashboard without the need to access additional consoles. • **Multi-Platform Management:**Windows, Mac, and Linux machines must be managed from one management console. • **Updating Bandwidth Consumption :** ✓ Updating of endpoints should have the ability to set pre-configured available bandwidth used for both software updating and threat definition updates(e.g., 64, 128, 256Kbps, etc.) ✓ Must have the option to set up a local cache updating server within the on-premise network environment to minimize large software engine update. ✓ Must have an Update Management Policy that contains the configuration of update schedules on managed endpoints. • **Deployment Options :**Deploying the endpoint agent must support the following methodology: Email setup link,via AD Startup/Shutdown script,AD Login script,SCCM ,Include the endpoint agent installation to a gold image • **SIEM Integration :**Must have the capability to extract events and alerts information from the Cloud Dashboard to a local SIEM. • **API for Endpoint Management:** ✓ Must have APIs offered as RESTful HTTP endpoints over the public internet. ✓ APIs must have the capability to query tenants, enumerate and manage endpoints and servers, and query alerts and manage them programmatically. • **Role Management:** ✓ Must have the capability to allow the separation of estate management to different administrator login.	**1200 User 30 server For 3 years**	

✓ Must provide admins the capability to assign predefined administrative roles to users who need access to the Admin Console. ✓ Must be able to create custom roles and assign the products and access needed. • **Microsoft AD Synchronization:** Must have the capability to only allow outbound synchronization of Users/Groups from the local Active Directory servers to the Cloud Dashboard for policy management. • **Microsoft Azure AD Authentication** ✓ Must have the capability to log in to the Admin Dashboard and Self Service Portal using Azure AD Login ✓ Must have the capability to automatically login to the Admin Dashboard/Self Service Portal if already authenticated in the web browser with Azure AD login from a different application/service. • **Policies** ✓ Selected policies should be able to be applied to either users or devices. ✓ Policies must have the capability to be disabled automatically based on a scheduled time and date. • **Enhanced Tamper Protection** ✓ Must have the capability to prevent local administrative users or malicious processes from disabling the endpoint protection. ✓ Must have the capability to prevent the following actions on the endpoint protection solution: Stopping services from the Services UI,Kill services from the Task Manager UI,Change Service Configuration from the Services UI,Stop Services/edit service configuration from the command line,Uninstall,Reinstall,Kill processes from the Task Manager UI (desired),Delete or modify protected files or folders,Delete or modify protected registry keys ✓ Must be able to export Tamper Protection passwords in CSV or PDF formats. • **Threat Protection** ✓ Must protect against multiple threats, both known and unknown, and provide a trusted and integrated approach to threat management at the endpoint. ✓ Must protect endpoint systems against viruses, spyware, Trojans, rootkits, and worms on workstations and laptops regardless of their nature or the concealment mechanisms used. ✓ Must protect against threats related to executable files, as well as document files containing active elements such as macros or scripts. It must protect against exploits resulting from discovery (whether published or not) of security flaws in systems or software. ✓ Must have the capability to 'lookup' files in real-time to verify if they are malicious. This feature checks suspicious files against the latest malware in the vendor's Threat Intelligence database in the cloud. ✓ Must have the capability to do real-time scanning of local files and network shares the moment the user tries to access them. Access must be denied unless the file is healthy. ✓ Must have the capability to do real-time scanning of end-users Internet Access. It must monitor and classify the Internet websites according to their level of risk, and make this technology available to endpoint systems. A site known to host malicious code or phishing sites must be proactively blocked by the solution to prevent any risk of infection or attack		

against a flaw of the browser used. The solution must carry out checks against a database of compromised websites that are constantly being updated with new sites identified per day. ✓ Must protect managed systems from malicious websites in real-time, whether end-users work within the company or outside the company's secure network - at home or through public Wi-Fi. All browsers on the market must be supported (Internet Explorer, Firefox, Safari, Opera, Chrome, etc.) • **Anti-rootkit Detection** :Must identify a rootkit when reviewing an element without overloading the endpoint system. Rootkits must be proactively detected. • **Suspicious Behavior Detection** ✓ Must be able to protect against unidentified viruses and suspicious behavior. ✓ Must have both pre-execution behavior analysis and runtime behavior analysis. ✓ Must be able to identify and block malicious programs before execution. ✓ Must be able to dynamically analyze the behavior of programs running on the system and detect then block activity that appears to be malicious. This may include changes to the registry that could allow a virus to run automatically when the computer is restarted. ✓ Must provide protection against buffer overflow attacks • **Scanning** ✓ Must provide a scheduled scanner to run depending on the selected frequency or by manually triggering through Windows Explorer to scan the specified directories (local, remote or removable), with analysis parameters used, which may be different from the ones selected for real-time protection. ✓ Must have the capability to scan archives such as zip, cab, etc. which can be enabled via policy settings. • **Advanced Deep Learning mechanism** ✓ The system shall be light speed scanning; within 20 milliseconds, the model shall able to extract millions of features from a file, conduct deep analysis, and determine if a file is benign or malicious. This entire process happens before the file executes. ✓ Must be able to prevent both known and never-seen-before malware, likewise must be able to block malware before it executes. ✓ Must protect the system even with offline and will not rely on signatures. ✓ Must classify files as malicious, potentially unwanted apps (PUA) or benign. Deep learning must also focus on Windows portable executables. ✓ Able to perform new Zero days threat scanning offline (without internet). ✓ Must be Smarter - should be able to process data through multiple analysis layers, each layer making the model considerably more powerful. ✓ Must be scalable - should be able to process significantly more input, can accurately predict threats while continuing to stay up-to-date. ✓ Must Lighter - model footprint shall be incredibly small, less than 20MB on the endpoint, with almost zero impact on performance. ✓ The deep learning model shall be trail and evaluate models end-to-end using advanced developed packages like Keras, Tensorflow, and Scikit-learn.		

• **Exploit Prevention/Mitigation must detect and stop the following known exploits:** ✓ Enforcement of Data Execution Protection (DEP) ✓ Prevents abuse of buffer overflows" ✓ Mandatory Address Space Layout Randomization (ASLR) ✓ Prevents predictable code locations" ✓ Improved code location randomization" ✓ Null Page (Null Dereference Protection) ✓ Stops exploits that jump via page 0" ✓ Heap Spray Allocation ✓ Reserving or pre-allocating commonly used memory addresses, so they cannot be used to house payloads." ✓ Dynamic Heap Spray ✓ Stops attacks that spray suspicious sequences on the heap" ✓ Stack Pivot ✓ Stops abuse of the stack pointer" ✓ Stack Exec (MemProt) ✓ Stops attacker's code on the stack" ✓ Stack-based ROP Mitigations (Caller) ✓ Stops standard Return-Oriented Programming attacks" ✓ Branch-based ROP Mitigations (Hardware Augmented) ✓ Stops advanced Return-Oriented Programming attacks" ✓ Structured Exception Handler Overwrite Protection (SEHOP) ✓ Stops abuse of the exception handler" ✓ Import Address Table Access Filtering (IAF) (Hardware Augmented) ✓ Stops attackers that lookup API addresses in the IAT" ✓ LoadLibrary API calls ✓ Prevents loading of libraries from UNC paths" ✓ Reflective DLL Injection ✓ Prevents loading of a library from memory into a host process" ✓ Shellcode monitoring ✓ Detecting the adversarial deployment of shellcode involves multiple techniques to address things like fragmented shellcode, encrypted payloads, and null free encoding ✓ VBScript God Mode ✓ Have the ability to detect the manipulating of the safe mode flag on VBScript in the web browser ✓ WoW64 ✓ Must have the ability to prohibit the program code from directly switching from 32-bit to 64-bit mode (e.g., using ROP) while still enabling the WoW64 layer to perform this transition." ✓ Syscall ✓ Stops attackers that attempt to bypass security hooks" ✓ Hollow Process Protection ✓ Stops attacks that use legitimate processes to hide hostile code"		

- ✓ DLL Hijacking
- ✓ Gives priority to system libraries for downloaded applications"
- ✓ Application Lockdown
- ✓ Will automatically terminate a protected application based on its behavior; for example, when an office application is leveraged to launch PowerShell, access the WMI, run a macro to install arbitrary code or manipulate critical system areas; the solution must block the malicious action – even when the attack doesn't spawn a child process."
- ✓ Java Lockdown
- ✓ Prevents attacks that abuse Java to launch Windows executables"
- ✓ Prevents regsvr32 from running remote scripts and code"
- ✓ CVE-2013-5331 & CVE-2014-4113 via Metasploit
- ✓ In-memory payloads: Meterpreter & Mimikatz"
- ✓ Dynamic Shellcode Protection
- ✓ Detects and blocks behavior of stagers"
- ✓ EFS Guard
- ✓ Protection against Encrypting File System attacks"
- ✓ CTF Guard
- ✓ Protects against a vulnerability in the ""CTF"" Windows component"

- **Advanced Exploit Mitigation**
  - ✓ Must be able to protect against a range of exploits or "active adversary" threats such as the following:
  - ✓ Credential Theft
  - ✓ Theft of passwords and hash information from memory, registry, or hard disk."
  - ✓ APC Violation
  - ✓ Attacks using Application Procedure Calls (APC) to run malicious codes."
  - ✓ Privilege Escalation
  - ✓ Attacks escalating a low-privilege process to higher privileges to access systems."
  - ✓ Malicious code that's been inserted into another, legitimate application."
  - ✓ Application Verifier Exploits
  - ✓ Attacks that exploit the application verifier in order to run unauthorized software at startup."
- **Malicious Traffic Detection (MTD):** Must be able to detect communications between endpoint computers and command and control servers involved in a botnet or other malware attacks.
- **Intrusion Prevention System (IPS)**
  - ✓ Must be able to prevent malicious network traffic with packet inspection (IPS).
  - ✓ Must be able to scan traffic at the lowest level and block threats before harming the operating system or applications.
- **Anti-Ransomware Protection**
  - ✓ Must have the ability for the encrypted files to be rolled back to a pre-encrypted state.
  - ✓ Both Anti-Exploit and Ransomware protection does not need to have a Cloud Lookup to perform the detection.

✓ When the Anti-crypto function suspects that certain behavior is not in keeping with its intended process, the Data Recorder starts caching data while the said behavior is closely reviewed to identify if the application is legitimate or if the activity is warranted. The maximum size of the data recorder is 100MB, and the Anti-crypto function caches files under 75MB. ✓ The anti-crypto function shall look back at all the malicious file modifications made by that process and restores them to their original location. ✓ Should a ransomware infection managed to get in, detailed historical tracking of where the infection originated and how it propagated will be reported courtesy of the Threat Cases (RCA). ✓ Must be able to protect from ransomware that encrypts the master boot record and from attacks that wipe the hard disk. • **AMSI Protection** ✓ Must be able to protect against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI). ✓ Must be able to scan code forwarded via AMSI before it runs, and the applications used to run the code are notified of threats. If a threat is detected, an event is logged. • **Data Loss Prevention (DLP)** ✓ Must be able to monitor and restrict the transfer of files containing sensitive data. ✓ Must have the capability to create custom DLP policies or policies from templates. ✓ Must have DLP policy templates that cover standard data protection for different regions. • **Peripheral Control** ✓ Must have the capability to control and restrict removable mass storage devices (USB sticks, CD Rom, USB external hard drives, iPods, MP3 players, etc.), as well as connection devices (Wi-Fi, Bluetooth, Infrared, Modems, etc.). ✓ Must have the capability to add device exemptions either by Model ID or Instance ID. • **Application Control** ✓ Must have the capability to limit the applications needed for specific user groups. ✓ Must be able to detect and block application categories that may not be suitable for use in an enterprise environment. ✓ Must have application categories for commonly used applications. • **Web Control** ✓ Must be able to block risky downloads, protect against data loss, prevent users from accessing web sites that are inappropriate for work, and generate logs of blocked visited sites. ✓ Must have security options to configure access to ads, uncategorized sites, or dangerous downloads. ✓ Must provide the administrator the ability to define "acceptable web usage" settings (defined by categories) in order to control the sites on which users are allowed to visit. Admin must have control access to websites that have been identified and classified in their own categories.		

✓ Must have a data loss protection option that allows the administrator to control access to web-based email and file downloads, with choices of blocking the data, allowing data sharing, or customizing this choice. • **Windows Firewall Policy** ✓ Must be able to monitor and configure Windows Firewall on managed computers and servers using a Windows Firewall policy. ✓ Must be able to apply the Windows Firewall policy to individual devices (computers or servers) or groups of devices. ✓ Root Cause Analysis ✓ Must have the capability to identify what happened, where a breach originated, what files were impacted, and provides guidance on how to strengthen an organization's security posture ✓ Must be able to record chain of events that occurred after an infection has been detected, enabling you to determine the origin of the infection, any resulting damage to assets, potentially exposed data, and the chain of events leading up to the halting of the infection. ✓ Shall provide a summary of the event: What the exploit was discovered, where the beacon event occurred (an asset), when it occurred, how the infection succeeded. Eg. "Outlook.exe." ✓ Shall provide recommendations to address the problem: Things to look for post-attack. Eg. Aside from files being restored from encrypted ones, check browser settings to ensure no vulnerabilities were created as a result of the infections. ✓ Activity Record allows administrators to add notes to the case. All case-related notes will be listed in this column. ✓ There are also buttons to enable the admin to modify the status of the case (New, In Progress, Closed) and to set priority (Low, Medium, High). When closing, the administrator can add notes and is also required to confirm (via checkboxes) that remediation steps were taken: analyzed impact on files/assets and relevant environmental improvements were implemented. ✓ Shall provide a tabular view of everything affected during the attack. Items can be filtered based on type — e.g., files, processes, registry keys. The administrator can view information about each item, e.g., Filename (victim file or malware agent), process ID, start/stop timestamp of the event. ✓ Shall indicate the beginning of the root cause, charting out the series of events resulting from the attack as a collection of nodes. Each node contains specific information about files, processes, registry keys, etc. involved at that stage. The beacon event (marked with a blue dot) will be identified in the chain, but any events executed by the process identified as the beacon event will also be shown. • **Advance System Clean** ✓ Must have the capability to trigger a deep clean upon any active detection from exploit or ransomware detection. ✓ The next-gen endpoint shall provide advanced Clean detection of malware by looking for the following:		

○ Files ✓ flagged as bad ✓ File has been downloaded from the internet ✓ Author's name/version information is missing from file properties, i.e., Impersonating a common windows system file. Reboot survivability is vigorously protected. ✓ Un-common file extension used. ✓ Contains PE structure anomalies and suggestions of obfuscation ○ Processes ✓ Listening for incoming connections ✓ Missing source executable file ✓ No UI elements ✓ Address Space Layout Randomization (ASLR) has been removed from the system. • **Data Lake for server** ✓ Must be able to run security queries on all managed devices, even if they are offline ✓ Must be able to query data from either: ✓ Endpoints that are currently connected (90 days of data stored on the device) ✓ The Data Lake in the cloud (30 days of cloud storage) ✓ Must be able to schedule queries. ✓ Must be able to query security data from multiple Sophos products, including Sophos Firewall and Sophos Email, as well as Intercept X. Example use cases include: ✓ IT Operations ✓ Identify unmanaged, guest, and IoT devices ✓ Why is the office network connection slow? Which application is causing it? ✓ Look back 30 days for unusual activity on a missing or destroyed device ✓ Threat Hunting for server ✓ Extend investigations to 30 days without bringing a device back online ✓ Use ATP and IPS detections from the firewall to investigate suspect hosts ✓ Compare email header information, SHAs, and other IoCs to identify malicious traffic to a domain • **Block Applications** ✓ Must have an option to immediately detect and remove potentially malicious Portable Executable (PE) files from protected computers in the environment. ✓ Must have an option to block applications using their SHA-256 hash. • **On-demand Threat Intelligence** ✓ Must have an option to 'request intelligence' on suspicious files, which will upload the file to our malware research team for further analysis. ✓ Must be able to provide a report summary of the machine learning analysis of a suspicious file. ✓ Must be able to provide a summary report with a more in-depth analysis of a suspicious file to help you decide if it's malicious or clean. • **Endpoint Isolation**		

✓ Must have an option to 'manually isolate' protected endpoints from the network while investigating a threat case. ✓ Must have an option to 'automatically isolate' compromised endpoints from the network. • **Forensic Data Export** ✓ Must have an option to generate a Forensic Snapshot of a malicious activity that occurred on a protected endpoint. ✓ Must be able to convert the generated Forensic Snapshot into a format where advanced queries can be run, such as SQLite or JSON file format. ✓ Must have an option to enable audit of Windows Authentication events, which allows Forensic Snapshots to contain more information on logon events. ✓ Must have the capability to upload the forensic snapshot to an AWS S3 bucket. • **Live Query for server** ✓ Must provide security analysts, and IT admins the ability to run SQL queries to answer almost any question they can think of across their endpoints and servers. ✓ Must be based on Osquery that allows administrators to understand the current running state of a device. ✓ Must be able to quickly discover IT operations issues to maintain IT hygiene and ask detailed questions to hunt down suspicious activity via SQL queries. ✓ Must have the capability to Pivot Queries that allows admins to select a significant piece of data in query results and use it as the basis for a new query. ✓ Must use powerful, out-of-the-box, fully-customizable SQL queries that can quickly search up to 90 days of current and historical on-disk data. Example use cases include: ➢ IT Operations ➢ Why is a machine running slowly? Is it pending a reboot? ➢ Which devices have known vulnerabilities, unknown services, or unauthorized browser extensions? ➢ Are there programs running that should be removed? ➢ Is remote sharing enabled? Are unencrypted SSH keys on the device? Are guest accounts enabled? ➢ Does the device have a copy of a particular file? ➢ Threat Hunting ➢ What processes are trying to make a network connection on non-standard ports? ➢ List detected IoCs mapped to the MITRE ATT&CK framework ➢ Show processes that have recently modified files or registry keys ➢ Search details about PowerShell executions ➢ Identify processes disguised as services.exe • **Remote Access for server** ✓ Must provide a command-line interface that can remotely access devices in order to perform a further investigation or take appropriate action. ✓ Must provide admins the capability to remotely connect to managed devices and get access to a command-line interface to perform actions such as:		

✓ Reboot a device pending updates ✓ Terminate suspicious processes ✓ Browse the file system ✓ Edit configuration files ✓ Remote Access option must only be available to Admin accounts using Multi-Factor Authentication (MFA). ✓ Must have control over which specific admin accounts have Remote Access capability. ✓ Remote access sessions must be included in Audit Logs (when it started, ended or if the connection was lost) ✓ Must be available on Windows, Mac, and Linux operating systems. • **CPU branch tracing for server:** mitigation for Return Oriented Programming (ROP) exploits • **Server Lockdown**: prevents unauthorized software from running on servers • **File Integrity Monitoring for server**: to monitor system-critical files and registry keys for additional security • **Synchronized Security** : Must be able to work with other security products of the vendor to share information and respond to incidents.		

7.2-Next Generation Firewall / CyberSecurity Gateway Solution

General Specifications	Quantity	Comply Yes/No For each
Base Firewall Features • **Firewall Specifications** ▪ Firewall throughput 75000 Mbps ▪ IPSec VPN throughput 62000 Mbps ▪ NGFW throughput 23000 Mbps ▪ IPS throughput 29000 Mbps ▪ Concurrent connections 16,000,000 ▪ New connections/sec 365,000 ▪ IPsec VPN concurrent tunnels 8500 ▪ SSL VPN concurrent tunnels 7500 ▪ SSL/TLS Inspection 8000 Mbps ▪ 4x GbE copper ▪ 4x SFP+ 10 GbE fiber ▪ 4 x 2.5 GbE copper ▪ 1 x RJ45 MGMT \ 1 x COM RJ45 \ 1 x Micro-USB (cable incl.) ▪ Virtual, Hardware or Cloud (AWS and/or Azure) form factor • **General Management** ▪ Purpose-built streamlined user interface ▪ Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN ▪ Self-documenting menu system ▪ Advanced trouble-shooting tools in GUI (e.g. Packet Capture)	**2**	

- Full command-line-interface (CLI) accessible from GUI
- Role-based administration
- Jumbo Frame Support
- Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers
- Self-service user portal
- Configuration change tracking
- Flexible device access control for services by zones
- Email or SNMP trap notification options
- SNMP and Netflow support
- Central managment support from Cloud Firewall Manager
- Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
- API for 3rd party integration
- HA with Active \ Passive Option
- Remote access option for Support

- **Firewall, Networking & Routing**
  - Unified policy model enabling policies to be managed on a single screen
  - Policy test simulator tool to enable firewall rule and web
  - policy simulation and testing by user, IP and time of day
  - Stateful deep packet inspection firewall
  - FastPath Packet Optimization
  - User, group, time, or network based policies
  - Access time polices per user/group
  - Enforce policy across zones, networks, or by service type
  - Zone isolation and zone-based policy support
  - Custom zones on LAN or DMZ
  - Customizable NAT policies with IP masquerading
  - Flood protection: DoS, DDoS and portscan blocking
  - Country blocking by geo-IP
  - VLAN DHCP support and tagging
  - VLAN bridge support
  - Routing: static, multicast (PIM-SM) and dynamic (BGP, OSPF)
  - Upstream proxy support
  - Protocol independent multicast routing with IGMP snooping
  - Bridging with STP support and ARP broadcast forwarding
  - WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rule
  - Wireless WAN support (n/a in virtual deployments)
  - 802.3ad interface link aggregation
  - Full configuration of DNS, DHCP and NTP
  - Dynamic DNS
  - Protocol independent multicast routing with IGMP snooping
  - Bridging with STP support and ARP broadcast forwarding
  - IPv6 support with tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec
  - Wildcard support for domain name host objects
  - VLAN DHCP support and tagging
  - Multiple bridge support
- **Multiple Firewall Management**
  - Cloud-based management and reporting for multiple firewalls provides group policy management.
  - Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group
  - Task Manager provides a full historical audit trail and status monitoring of group policy changes
  - Backup firmware management which stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access
  - Firmware updates which offer one-click firmware updates to be applied to any device
  - Zero-touch deployment enables the initial configuration to be performed in Cloud-based management

- and then exported for loading onto the device from a flash drive at startup, automatically connecting the device back to the cloud management platform.
- Firmware update scheduling
- Multi-firewall reporting across firewall groups
- Save, schedule and export reports from the cloud management portal.

- **SD-WAN**
  - Support for multiple WAN link options including VDSL, DSL, cable, and 3G/4G/LTE cellular withessential monitoring, balancing, failover and fail-back
  - Application path selection and routing, which is used to ensure quality and minimize latency for
  - mission-critical applications such as VoIP
  - Enhanced SD-WAN, a Security feature which leverages the added clarity and reliability of application identification that comes with the sharing of Application Control information between managed endpoints and Firewall.
  - Enhanced SD-WAN application routing over preferred links via firewall rules or policy-based routing
  - Affordable, flexible, and zero-touch or low-touch deployment
  - Centralized VPN orchestration
  - Unique Ehernet Layer 2 tunnel with routing
  - Integration with Azure Virtual WAN for a complete SD-WAN overlay network
- **Traffic Shaping & Quotas**
  - Network or user based traffic shaping (QoS) (Web and App based traffic shaping are included with the Web Protection Subscription)
  - Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical
  - Real-time VoiP optimization
- **Authentication**
  - Transparent, proxy authentication (NTLM/ Kerberos) or client authentication
  - Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
  - Server authentication agents for Active Directory SSO
  - Client authentication agents for Windows, Mac OS X, Linux 32/64
  - Authentication certificates for iOS and Android
  - Single sign-on: Active directory, eDirectory
  - Authentication services for IPSec, L2TP, PPTP, SSL
  - Captive Portal
- **User Self-Service Portal**
  - Download the Authentication Client
  - Download SSL remote access client (Windows) and configuration files (other OS)
  - Hotspot access information
  - Change user name and password
  - View personal internet usage
  - Access quarantined messages (requires Email Protection)
- **Route-based VPN**
  - Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
  - L2TP and PPTP
  - Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Andriod VPN client support
  - IKEv2 support
  - SSL client for Windows & configuration download via user portal
- **VPN Client**
  - IPSec and SSL support
  - Easy provisioning and deployment
  - Free (unlimited SSL and IPSec remote access licenses included at no extra charge)
  - Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH
  - Send device security status to the firewall
  - Intelligent split-tunneling for optimum traffic routing
  - NAT-traversal support
  - Client-monitor for graphical overview of connection status
  - Mac and Windows Support
  - Remote access IPSec policy provisioning

- Group support which enables imports from AD/LDAP etc.

Cloud Sandbox Protection

- Suspicious files subjected to threat intelligence analysis in parallel with full sandbox analysis
- Supports one-time download links
- Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis
- Machine Learning technology with Deep Learning scans all dropped executable files
- Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
- In-depth malicious file reports and dashboard file release capability
- Includes exploit prevention and Cryptoguard Protection technology from endpoint security
- Detects sandbox evasion behavior
- Aggressive behavioral, network, and memory analysis

Network Protection Features

- **Intrusion Prevention Systems (IPS)**
  - High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection
  - Thousands of signatures
  - Granular category selection
  - Support for custom IPS signatures
  - IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added
- **Advance Threat Protection and Coordinated Security**
  - Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
  - Instant insights into endpoint health status, with the option to automatically respond to security incidents by isolating infected systems.
  - Provides visibility into top risk users, unknown applications, advanced threats and suspicious payloads
  - Automatically identify, classify and control all unknown applications on the network
  - Solicit application information from the endpoint for traffic that does
  - not match any application control signature.
  - Deep forensic and analytics capabilities into users, threats, applications, web usage, and other activity on the network.
  - Limit access to network resources or completely isolate compromised systems until they are cleaned up
  - Sharing telemetry and health status between endpoint and the firewall to provide a
  - coordinated response.
- **Clientless VPN**
  - HTML5 self-service portal with support for RDP, SSH, Telnet and VNC.

Web Protection Features

- **Web Protection and Control**
  - Fully transparent proxy for anti-malware and web-filtering
  - Enhanced Advanced Threat Protection
  - URL Filter database with millions of sites across more than 70 categories
  - Surfing quota time policies per user/group
  - Access time polices per user/group
  - Malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email
  - Advanced web malware protection with JavaScript emulation
  - Live Protection real-time in-the-cloud lookups for the latest threat intelligence
  - Second independent malware detection engine for dual-scanning
  - Real-time or batch mode scanning
  - Pharming Protection
  - HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions

- SSL protocol tunnelling detection and enforcment
- Web Keyword Monitoring and Enforcement
- Certificate validation
- High performance web content caching
- File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)
- SafeSearch enforcement

- **Cloud Application Visibility**
  - Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
  - Discover Shadow IT at a glance
  - Drill down to obtain details on users, traffic, and data
  - One-click access to traffic shaping policies
  - Filter cloud application usage by category or volume
  - Detailed customizable cloud application usage report for full historical reporting
- **Application Protection and Control**
  - Enhanced application control with signatures and Layer 7 patterns for thousands of applications
  - Application control based on category, characteristics (e.g. bandwidth and productivity consuming), technology (e.g. P2P) and risk level
  - Application Risk Meter provides and overall risk factor based on the risk level of applications on the network
  - Identify, classify and control previously unknown applications active on the network
  - Per-user or network rule application control policy enforcement
- **Web & App Traffic Shaping**
  - Custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared

Web Server Protection Features

- **Web Application Firewall Protection**
  - Reverse proxy
  - URL hardening engine with deep-linking and directory traversal prevention
  - Form hardening engine
  - SQL injection protection
  - Cross-site scripting protection
  - Antivirus scan
  - HTTPS (SSL) encryption offloading
  - Cookie signing with digital signatures
  - Path-based routing
  - Outlook anywhere protocol support
  - Reverse authentication (offloading) for form-based and basic authentication for server access
  - Virtual server and physical server abstraction
  - Integrated load balancer spreads visitors across multiple servers
  - Skip individual checks in a granular fashion as required
  - Match requests from source networks or specified target URLs
  - Support for logical and/or operators
  - Assists compatibility with various configurations and non-standard deployments
  - Options to change WAF performance parameters
  - Scan size limit option
  - Allow/Block IP ranges
  - Wildcard support for server paths
  - Automatically append a prefix/suffix for authentication
- **Logging and Reporting**
  - Hundreds of on-box reports with custom report options (NOTE: individual log, report and widget availability depends on enabled software subcriptions):
  - Dashboards (Traffic, Security, and User Threat Quotient),
  - Applications Report (App Risk, Blocked Apps, Web Uses, Search Engines, Web Servers, FTP),
  - Network & Threats Report (IPS, ATP, Wireless),

- VPN Reports
- Email usage and protection Reports
- Optional Compliance reports (HIPAA, GLBA, SOX, FISMA, PCI-DSS, NERC CIP v3, and CIPA)
- Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks
- Report anonymization
- Report scheduling to multiple recipients by report group with flexible frequency options
- Standard and granular logging options
- Export reports as HTML, PDF, Excel (XLS)
- Security Audit report
- Web Keyword Content Report
- Report bookmarks
- Full log viewer with retention customization by category

- **Cloud Firewall Reporting**
  - Pre-defined reports with flexible customization options
  - Reporting for Firewalls (hardware, software, virtual, and cloud)
  - Intuitive user interface provides graphical representation of data
  - Report dashboard provides an at-a-glance view of events over the past 24 hours
  - Easily identify network activities, trends, and potential attacks
  - Easy backup of logs with quick retrieval for audit needs
  - Simplified deployment without the need for technical expertise
  - Create custom reports with powerful visualization tools
  - Syslog search and view
  - Syslog data storage in cloud
  - On-demand reporting in cloud
  - 7 day cloud storage for Central Firewall reporting
  - New Cloud Application (CASB) report
  - No extra charge
- **On-Box Reporting**
  - No extra charge
  - Hundreds of on-box reports with custom report options: Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Search Engines, Web Servers, Web Keyword Match, FTP), Network and Threats (IPS, ATP, Wireless, Security Heartbeat, Sandstorm), VPN, Email, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
  - Built-in storage for log data storage for historical reporting
  - Current Activity Monitoring: system health, live users, IPSec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks
  - Report anonymization
  - Report scheduling to multiple recipients by report group with flexible frequency options
  - Export reports as HTML, PDF, Excel (XLS)
  - Report bookmarks
  - Log retention customization by category
  - Syslog Support
  - Full-featured Live Log Viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization

Warranty and Support

- Hardware warranty & RMA with Advanced Exchange 5 Years
- 24x7 Enhanced Plus Support via Telephone & Email with Remote Consultation from STSE (up to 4 hrs) 5 Years
- FREE Security Updates & Patches
- FREE Software Features Updates & Upgrades
- Protection Bundle Includes for 3 Years:
- Base License: Networking, Wireless, Unlimited Remote Access VPN, Site-to-Site VPN, reporting
- Network Protection: advanced TLS and DPI engine, IPS, ATP, Security Heartbeat, SD-RED VPN, reporting
- Web Protection: advanced TLS and DPI engine, Web Security and Control, Application Control, reporting
- Zero-Day Protection: Machine Learning and Sandboxing File Analysis, reporting

▪ Central Orchestration: SD-WAN VPN Orchestration, Cloud Firewall Advanced Reporting (30-days), XDR ready ▪ Enhanced Support: 24/7 support, feature updates, advanced replacement hardware warranty for term ▪ Enhanced Plus Support Upgrade: Upgrade your support with VIP support, HW warranty for add-ons, TAM option (extra cost) **Central Management and Reporting (included at no charge)** ▪ Central Management : Group firewall management, backup management, firmware update scheduling ▪ Central Firewall Reporting: Prepackaged and custom report tools with seven days cloud storage for no extra charge		

Description		Quantity	Unit price	Total Price (JD)
Anti-virus	XIntercept for workstation for 3years	1200		
	XDR for server for 3 years	30		
Firewall for 3 years		2		
Budgetary Price (JD)				