Endpoint Security Specifications

A/A	Requirements
1	**General**
1.1	Solution must support the following operating systems: - Microsoft Windows 7 SP1, 8, 8.1, 10,11 - Microsoft Windows Server 2008 R2 ,2012(R2), 2016,2019,2022
1.2	The solution must support for virtual, VDI environments.
2	**Protection Requirements**
2.1	Real-time detection & cleaning of all kinds of threats: viruses, worms, Trojans, backdoors, rootkits, spyware, adware, ransomware, keyloggers, phishing, SPAMS, zero-day threats & potentially unwanted/unsafe software.
2.2	The detection engine should also include Advanced Machine Learning (AML) as an advanced layer of protection with an option to adjust the aggressiveness of the AML.
2.3	Suggested solution must include the following components from a single agent: - HIPS (Host Intrusion Prevention System) - Deep Behavioral Scanning - Client Firewall - Advanced Memory Scanner - Ransomware Shield - Cloud Sandboxing (Optional) - Network Attack Protection (IDS) - Botnet Protection - Exploit Blocker - UEFI Scanner - Email Client Protection - Phishing Protection - Secure Browser - Brute-force attack protection - Web Control - Device Control
2.4	The solution should have integration with Intel's hardware based ransomware detection technology to detect complex ransomware.
2.5	The solution should have detection rates with low false positive in 3rd party AV testing reports.
2.6	The solution should be able to detect new & evolving threats using multi-layered approach to detect threats at different stages of the kill-chain. List the capabilities in detail.
2.7	Solution must have dedicated component to prevent new variants of ransomware.
2.8	The Solution should be able to block zero-day exploits against vulnerabilities in popular software.
2.9	The solution should be password-protected to prevent from making any unauthorized configuration changes, interrupting any AV process.
2.10	The solution should have the ability to replace the existing 3rd party endpoint solution without any consequence or loss of core antimalware capability.
2.11	Solution should have offline protection capabilities (without signature updates, internet connection, or management console connection).
2.12	The solution should have dedicated component to monitor, detect & block attacks by scanning suspicous behavior at the memory level on the endpoints.
2.13	The solution should contain firewall component to automatically apply different firewall profiles based on the connected network.
2.14	The solution should be able to rollback updates to a previous version, while pausing the updates for a defined period.
2.15	The solution should automatically scan the removable storage devices for malware upon inserting to any endpoint.
2.16	Solution should be able to allow/block/read/write on USB storage devices/CD-DVD based on users or computers to minimize the data theft.
2.17	Solution should be able to also allow/block: - Disk storage (HDD, USB removable disk) - CD/DVD - USB printer - FireWire Storage

A/A	Requirements
	- Bluetooth Device - Smart card reader - Imaging Device - Modem - LPT/COM port - Portable Device
2.18	Suggested solution must include proactive scanning of all scripts by automatically submitting suspicious payloads to cloud sandboxing environment.
2.19	The solution should run suspicous samples using static code analysis, deep inspection, machine learning, in-memory analysis & AI for behaviour based detection.
2.20	The solution should allow any user to submit a suspicious sample for deeper analysis using sandboxing & ML directly from the product anonymously.
2.21	The solution can restrict the submission of certain files based on the file type or file extension.
2.22	Solution should have the capability to delete the submitted samples from the cloud server storage immediately after the analysis.
2.23	The solution must have the capability to control the applications access to registry, start/terminate another application, modify state of other applications etc.
2.24	Suggested solution must have built-in integration with outlook to scan incoming mails for any malicious content, prevent SPAMS & phishing emails.
2.25	The solution should provide the ability to easily implement full disk encryption on the desktops.
2.26	The proposed vendor should be a leader & Top Players in the Market Quadrant for more than 3 years.
3	**Monitoring & Reporting**
3.1	Management console provides full visibility to all the suspicious samples submitted for deeper analysis including behavior of the suspicious files & the action taken.
3.2	Management console should have built-in dashboards, reports & notification templates & ability to customize if needed.
3.3	Management console should have the ability to convert dashboards into PDF files & schedule them to be emailed to others.
3.4	The management console should support multi-tenancy & role-based access.
3.5	Solution should provide an online tool to monitor & manage license, e.g. view all activations, & deactivate endpoints, even if they are not activated from the management console.
3.6	The solution should have the ability to automatically upgrade the endpoint agents without any user interruption.
3.7	The solution should discover new machines & deploy the agents automatically.
3.8	The console should allow to execute remote commands on the endpoints, push 3rd party software, perform operations like scan, update, restart etc.
3.9	The solution must report all software installed across the endpoints. The software details should contain information such as name, publisher, version etc.
3.10	The solution should be able to integrate with existing SIEM solution.

الشروط الخاصة للعطاء:

1- أن تكون مدة تجديد التراخيص 3 سنوات شمسية من تاريخ تسليم التراخيص لجميع البنود.

2- أن يتم التوريد والتركيب والتشغيل والتأكد من عملها حسب الاصول، **مع التأكيد على قيام الشركة بإزالة البرمجية السابقة عن الاجهزة والخوادم في الجامعة**.

3- تقديم الدعم الفني (في الموقع أو عن بعد) حسب الحاجة وحسب الطلب لمدة 3 سنوات من تاريخ تسليم التراخيص.

ملاحظات مهمة:

1- عدد الاجهزة المطلوب تزويدها بالبرمجية (1000).

2- عدد الخوادم المطلوب تزويدها بالبرمجية (50).

3- تنتهي التراخيص الحالية بتاريخ 29-02-2024.