

SPECIFICATIONS

point Protection for PCs (Windows/Mac) and Servers (Windows/Li

#	DESCRIPTION
1	Advanced Threat Protection Platform - The proposed solution must be an integrated advanced endpoint protection platform capable of preventing organizations from being hacked. It must detect the execution of malicious code, ransomware, exploits, Master Boot Record (MBR) attacks, and must be able to remove and block such imminent threats.
2	Real-Time Zero-Day Ransomware Defense with Proprietary File Rollback - The solution must detect and block previously unseen ransomware variants in real time and automatically restore any affected files to their original state using the vendor's own proprietary rollback technology, without relying on Windows Volume Shadow Copy Service (VSS).
3	Real-Time Scanning - The solution must offer real-time scanning of local files and network shares during both read and write operations.
4	Proprietary Scan Engine - The endpoint protection solution must have its own proprietary scan engine developed and maintained by the OEM.
5	Exclusion of Potentially Unwanted Applications (PUAs) - The solution must have the capability to exclude applications that are typically detected as Potentially Unwanted Applications (PUAs), allowing administrators to configure exceptions as needed.
6	Application Control - The solution must provide Application Control functionality that allows administrators to detect and block applications deemed unsuitable for organizational use, even if they are not direct security threats.
7	Secure Uninstallation Control - The solution must support secure uninstallation of the antivirus client by enforcing a unique uninstall password for each machine: - The password should only be visible to administrators via the Centralized Management Console. - Once used, the password should automatically become invalid. - There must be an option to generate a new random password with a single click.
8	Re-Protection of Deleted Endpoints - In the event that a machine is deleted from the management console, the solution must support re-protection of such endpoints.
9	Online Threat Intelligence and Malware Sample Submission - The solution must offer real-time threat protection by checking the latest threat intelligence updates from the OEM vendor's online services.

10	Web Access and Download Risk Controls - The solution must offer configurable security options to manage access to: - Advertisements - Uncategorized websites - Risky downloads
11	Risky Download Handling Options - The solution must provide flexible handling of risky file downloads with the following user-configurable options: ~~Allowed: Permit all risky file types to be downloaded~~
12	Process-Based File Monitoring - The solution must be capable of monitoring files when they are accessed by a process, including both read and write operations, to ensure advanced visibility and threat detection.
13	Bandwidth Conservation and Web Filtering - The solution must include features to conserve network bandwidth by: - Blocking access to inappropriate or non-work-related websites. - Warning users before they visit websites known to impact productivity. - Blocking categories of websites that are likely to consume high bandwidth (e.g., streaming, file sharing, gaming).
14	Comprehensive Alert Reporting - The proposed solution must provide detailed alert descriptions that include both the user and device information associated with each alert, enabling efficient threat investigation and response.
15	Customizable End-User Notification & Response Options - Must allow admins to tailor end-user prompts, show/hide alerts, and allow/block user remediation
16	Robust support for detecting C2 communications, advanced Runtime Behavior Analysis and Host Intrusion Prevention System (HIPS) capabilities - The solution should provide robust support for detecting and blocking Command and Control (C2) communications, and must include advanced Runtime Behavior Analysis and Host Intrusion Prevention System (HIPS) capabilities to proactively identify and mitigate malicious activities at the endpoint level.
17	Application Control - Solution must provide application categorization and allow administrators to block specific applications as required.
18	Device and Peripheral Control - Must support granular control over peripheral devices (e.g., USBs, printers, storage), including options to set access as Read Only, Allow, or Block.
19	USB Whitelisting by Hardware ID - The solution must allow whitelisting of USB devices based on unique hardware identifiers (HWID).
20	Web Filtering by Category - Should offer the ability to block websites based on predefined categories.

21	Comprehensive Web Control - Web control should: - Block risky downloads - Prevent data leakage - Restrict access to inappropriate websites - Generate logs of blocked attempts - Control access to ads, uncategorized, or harmful sites
22	Policy Flexibility by User or Device - Must support the creation and application of security policies based on user identity or device type.
23	Data Loss Prevention (DLP) - The solution must include built-in Data Loss Prevention (DLP) functionality to prevent unauthorized access and sharing of sensitive data.
24	Application Blocking for Risky Software - Must allow administrators to block high-risk applications such as Torrents, VPNs, Proxy Tools, and Video Players, and detect emerging applications for upstream firewall reporting and enforcement.
25	Time-Based Policy Enforcement - Should allow the definition of time-based policies for specific actions or restrictions.
26	Role-Based Access Control (RBAC) - Must support granular RBAC for different admin roles.
27	Multi-Factor Authentication Enforcement - All administrative access must be protected with Multi-Factor Authentication (MFA) using OTP via SMS, email, or third-party apps.
28	Threat Intelligence Sharing with Gateway Firewall - Must be capable of sharing threat intelligence/feeds with the gateway firewall, enabling automated blocking without requiring a separate product or subscription.
29	Single Pane of Glass Integration via API - Management console should offer API-based integration with gateway firewall management UI, enabling unified visibility and management.

30	The proposed endpoint protection solution must include a Client/Agent Self Help Client Self-Help Diagnostic Tool - Diagnostic Tool capable of collecting essential system information and product-specific log files to diagnose installation and operational health issues. The tool should: (a) Automatically identify common product-related issues. (b) Provide guided resolutions or remediation steps for immediate issue resolution. (c) Be operable both remotely via the Centralized Management Console and locally on the endpoint device. (d) Support secure log collection and reporting to assist with troubleshooting and support engagement. This capability is essential to minimize downtime, streamline issue resolution, and ensure continuous endpoint protection without requiring manual intervention from IT support teams.
31	Network Connectivity Testing - Client/Agent should have built in tool to perform network connectivity tests to update and management servers for troubleshooting.
32	File Analysis via Drag-and-Drop - The client should support drag-and-drop submission of PE (Portable Executable) files for real-time reputation checks and deep learning-based analysis.
33	Cloud-Based Management Console - The management console must be completely cloud-hosted with no dependency with on premise management consoles.
34	Scheduled Report Generation - Reports should support email delivery in CSV/PDF formats, with customizable frequency (daily, weekly, monthly).
35	Robust API Support - Solution must support robust APIs to integrate with third-party SIEM and RMM platforms.
36	Network Intrusion Prevention (IPS) - Must include the capability to prevent malicious network traffic using packet inspection.
37	Protection Against Application Hijacking Techniques. - It must detect and prevent: - Process Hollowing - Untrusted DLL Loading
38	Multi-Rule Data Control Policies - Must allow the creation of multi-rule DLP policies for groups/users to protect data such as financial records, health information, and PII (Personally Identifiable Information) in files and emails.

39	Cross-Integration with Same OEM Vendor Firewall - Endpoint console must support integration with the same vendor's firewall console for centralized visibility and control via API.
40	Cross-Platform Compatibility - Must support the latest versions of: - Windows 10+ - Windows Server 2016+ - macOS - Linux
41	Account Health Check Dashboard - Admin console must include a Configuration Health Check section that displays status of licensed protection features.
42	Custom and Template-Based DLP Policies - Should support both custom DLP policy creation and use of predefined templates.
43	Sensitive Data Transfer Monitoring and Restriction - Must monitor and restrict transfer of files containing sensitive data.
44	Built-in Email Security Integration with Threat Correlation to Endpoint - The same OEM vendor must have a cloud-based email security service available for future expansion with licensing options. The email solution must natively integrate with the central management platform to correlate threats such as malicious attachments, URLs, and indicators of compromise with affected endpoints and users.
45	The solution must have a protection mechanism that automatically triggers heightened defense mechanisms when a hands-on-keyboard attack is detected. In this mode, commonly abused but otherwise benign actions must be blocked to delay attacker activity and provide administrators with time to respond and remediate. The feature must be policy-driven, allow manual activation/deactivation per device, support extended protection periods during investigations, and provide visibility through alerts and event logs via the centralized management console.
46	Safe Mode Abuse Prevention and Protection - The solution must include persistent policy controls to: - Block Safe Mode Abuse: Prevent adversaries from programmatically restarting devices into Safe Mode. - Enable Protection in Safe Mode: Ensure key runtime defenses—such as anti-ransomware and AI-powered malware protection—remain active even when the endpoint is booted into Safe Mode.
47	Remote Ransomware Protection - The solution must provide zero-touch defense against ransomware executing over the network from compromised remote devices, automatically detecting and blocking any attempt to encrypt data across network shares or mapped drives.
48	Gartner Leadership - The proposed solution must be recognized as a 'Leader' in the Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) for continuously five reports until 2024

Unified Endpoint Management (iOS, Android, Chrome OS and Windows)

#	DESCRIPTION
1	Unified UEM + Mobile Threat Defense Agent - The solution must deliver both Enterprise Mobility Management (EMM) and Mobile Threat Defense (MTD) in a single agent and console, eliminating the need for separate products or integrations.
2	On-Device, AI-Powered Malware & Phishing Protection - Must utilize on-device deep-learning models to detect zero-day mobile malware, phishing URLs, and malicious applications in real time—without requiring cloud lookups for primary verdicts.
3	Full Android & iOS Feature Parity - Must support identical policy sets, threat detection, and remediation actions on both Android and iOS platforms, including device encryption checks, application vetting, and OS-level vulnerability monitoring.
4	Centralized Management Console with Multi-Tenant Scalability - Management must be delivered via same endpoint management Centralized console with built-in multi-tenant support, role-based access control, and API integrations.
5	Containerization & App-Wrapping for Corporate Data - Must provide automatic containerization or app-wrapping of corporate email and data, enforcing per-app VPN, copy/paste restrictions, and DLP policies at the mobile OS level.
6	Advanced Jailbreak/Root & Exploit Prevention - Must detect and block jailbreak, root-kit, and OS-exploit attempts—including runtime prevention of privilege escalation—without relying on periodic scans or external services.
7	Granular Geofencing & Location-Aware Policies - Must support dynamic policy enforcement based on geofences and trusted Wi-Fi networks, automatically strengthening controls when devices leave approved zones. (Geo-fencing / Time-fencing / Wi-Fi fencing)
8	Automated Threat Intelligence Sharing to Network & Endpoint - Must natively share mobile-detected threats (malicious app, phishing site, compromised device) into Centralized management console, triggering actions on same OEM vendor firewalls and endpoints—requiring no third-party integrations.
9	User Licensing - Must be covered under a single, predictable per user subscription for mobile devices that includes both Enterprise Mobility Management and Mobile Threat Defense/Security.

10	Self Service Portal - Must be provided with a User Self Service Portal that allows users to enroll their device with UEM solution. Also it must be capable in delivering functionalities such as remotely locate, lock or wipe devices and reset user password without having to contact the helpdesk.
11	Mobile Threat Security/Defense - Must protect users, their devices, and corporate data from known and never-before-seen mobile threats by leveraging AI driven scanning and detection engine. The solution must stop mobile specific threats missed by mobile app stores (Google Play Protect/App Store Protection): - Must block malware and ransomware, including potentially unwanted applications (PUA)
12	Application Management — (a) Remote App Installation The solution must support installation of applications—both silently and with user interaction—including deployment of managed apps on iOS devices. (b) Remote App Uninstallation The solution must support uninstallation of applications—both silently and with user interaction—across all managed platforms. (c) Application Inventory The solution must maintain and report a real-time list of all installed applications on each managed device. (d) Apple Volume Purchasing Program (VPP) Integration The solution must integrate with Apple's Volume Purchasing Program to automate app procurement and deployment for iOS/macOS. (e) App Installation Controls The solution must allow administrators to whitelist or blacklist specific applications, preventing unauthorized app installs. (f) App Removal Protection The solution must be able to block end-users from uninstalling any managed security or business-critical applications.

Additional Requirements

DESCRIPTION
Partner must provide Architect level Certification of one employee
Partner must provide Engineer level Certification of one employee
Partner must provide Partner Authorization Letter from the Vendor

QTY	PRODUCT	LICENSE TERM
725	Endpoint Protection for PCs (Windows/Mac)	03 Years
118	Endpoint Protection for Servers (Windows/Linux)	03 Years
20	Central Mobile Advanced	03 Years