

- 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 detect low reputation files and have an action to prompt user or log only. Must be able to configure reputation level to either recommended or strict.

- Must have the capability to do real-time scanning of local files and network shares the moment the user tries to access them. The feature must include real time scanning for remote files. 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.

Advanced Deep Learning mechanism:

- The system shall be light speed scanning; within 20 milliseconds, the model shall be 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 be Lighter - model footprint shall be small, less than 20MB on the endpoint, with almost zero impact on performance.

- The deep learning model shall be trained 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

- Bottom-up ASLR 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

- DLP functionality must run on the same agent as the endpoint protection and all functions mentioned.									
- 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.									
- Must have the option to add custom DLP rule: 1) Content Rule 2) File Rule									
- DLP content rule must have the condition required for content scanning according to file content and destination. Actions must have options to either allow file transfer, allow transfer if user confirms, or block transfer.									
- DLP content rule must have the option to set exclusions based on file name and file type.									
- DLP content rule must have the option to set condition based on content control list (CCL). Must have the capability to add custom CCL and use filters by Region (e.g., Australia, Europe, India, Singapore, UK, USA, Global, Universal), filter by source (Custom, intelligence source (native to solution)), filter by type (e.g., Personally Identifiable Information (PII), HIPAA, PCI-DSS, Financial Data, Document classification, Health Care)									
- DLP file rule must have the condition required to check the destination of file and options for when file type matches and when file name matches. Actions must have options to either allow file transfer, allow transfer if user confirms, or block transfer.									
Must be able to scan different file types: Archive, Media container, Office password protected, Mail, Design, Plain text, Object code, Information rights management, Medical image formats, Image, Script/Markup, Document, Executable, Container, Spreadsheet, Encryption (native to proposed solution), Virtualization container, Disk container, Video, Audio, Database, Encryption, Presentation, Interactive media, and Science/Engineering.									
- DLP file rule must have the option to set the following destination: Email client, Internet browser, Instant messaging, Internet browser-external processes, Voice over IP, and Storage.									
Peripheral Control:									
- Must have the capability to control peripheral devices such as peripherals under the following categories: Bluetooth, Secure removable storage, Floppy drive, Infrared, Modem, Optical drive, Removable storage, Wireless, Media transfer protocol (MTP), and Picture Transfer Protocol (PTP).									
- Must have the capability to add device exemptions either by Model ID or Instance ID.									
- Must be able to set a customized desktop message to appear at the end of a standard notification in order to notify the user of policy violation.									
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 an option for detected controlled applications during scheduled and on-demand scans									
- Must have out of the box application categories and built-in number of signatures per category to choose from such as Archive tool (9) Asset Management tool (14) Browser plug-in (39) Business intelligence tool (44) Digital imaging (31) Distributed computing (8) Document viewer (47) Download manager (62) Email/PIM client (30) ERP software (21) File sharing application (95) FTP client (15) Game (351) Instant messaging (138) Internet browser (96) Jailbreak software (3) Mapping application (6) Media conversion tool (15) Media player (142) Mobile Synchronization (37) Network monitoring/ Vulnerability tool (60) Office suite (48) Online storage (82) Proxy/VPN tool (120) System tool (215) Voice over IP (38)									
- Must have a customized desktop messaging feature to the end of a standard notification to notify the user of policy violation									
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 site.									
- 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 with built-in web categories (i.e., Productivity-related categories, Social Networking, Adult and potentially inappropriate categories, Categories likely to cause excessive bandwidth usage, Business-relevant site 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 the option to Allow, Warn, and Block.									
- 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.									
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									

