Descriptions	Comply/Not Comply
Multi-Platform Management	
Windows, Mac, and Linux machines must be managed from one management console.	Comply
Deployment Options	
Deploying the endpoint agent must support the following methodology:	
1) Email setup link	Comply
2) via AD Startup/Shutdown script	Comply
3) AD Login script	Comply
4) SCCM	Comply
5) Include the endpoint agent installation to a gold image	Comply
SIEM Integration	
Must have the capability to extract events and alerts information from the Cloud Dashboard to a local SIEM.	Comply
API for Endpoint Management	
Must have APIs offered as RESTful HTTP endpoints over the public internet.	Comply
APIs must have the capability to query tenants, enumerate and manage endpoints and servers, and query alerts and manage them programmatically.	Comply
Role Management	
Must have the capability to allow the separation of estate management to different administrator login.	Comply
Must be able to create custom roles and assign the products and access needed.	Comply
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.	Comply
Microsoft Azure AD Authentication	
Must have the capability to log in to the Admin Dashboard and Self Service Portal using Azure AD Login	Comply
Policies	
Selected policies should be able to be applied to either users or devices.	Comply
Policies must have the capability to be disabled automatically based on a scheduled time and date.	Comply

Enhanced Tamper Protection	
Must have the capability to prevent local administrative users or malicious processes from disabling the endpoint protection,uninstall, kill or stop services	Comply
Threat Protection	Comply
Must protect against multiple threats, both known and unknown, and provide a trusted and integrated approach to threat management at the endpoint.and against viruses, spyware, Trojans, rootkits, worms	Comply
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.	Comply
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.)	Comply
Anti-rootkit Detection	
Must identify a rootkit when reviewing an element without overloading the endpoint system. Rootkits must be proactively detected.	Comply
Suspicious Behavior Detection	
Must be able to protect against unidentified viruses and suspicious behavior.	Comply
Must have both pre-execution behavior analysis and runtime behavior analysis.	Comply
Must be able to identify and block malicious programs before execution.	Comply
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.	Comply
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.	Comply
Must be able to prevent both known and never-seen-before malware, likewise must be able to block malware before it executes.	Comply
Must protect the system even with offline and will not rely on signatures.	Comply
Must classify files as malicious, potentially unwanted apps (PUA) or benign. Deep learning must also focus on Windows portable executables.	Comply
Able to perform new Zero days threat scanning offline (without internet).	Comply

Must be Smarter - should be able to process data through multiple analysis layers, each layer making the model considerably more powerful.	Comply
Must be scalable - should be able to process significantly more input, can accurately predict threats while continuing to stay up-to-date.	Comply
Must Lighter - model footprint shall be incredibly small, less than 20MB on the endpoint, with almost zero impact on performance.	Comply
Exploit Prevention/Mitigation must detect and stop the following known exploits:	
1) Enforcement of Data Execution Protection (DEP)	Comply
2) Mandatory Address Space Layout Randomization (ASLR)	Comply
3) Bottom-up ASLR	Comply
4) Null Page (Null Dereference Protection)	Comply
5) Heap Spray Allocation	Comply
6) Dynamic Heap Spray	Comply
7) Stack Pivot	Comply
8) Stack Exec (MemProt)	Comply
9) Stack-based ROP Mitigations (Caller)	Comply
10) Branch-based ROP Mitigations (Hardware Augmented)	Comply
11) Structured Exception Handler Overwrite Protection (SEHOP)	Comply
12) Import Address Table Access Filtering (IAF) (Hardware Augmented)	Comply
13) LoadLibrary API calls	Comply
14) Reflective DLL Injection	Comply
15) Shellcode monitoring	Comply
16) VBScript God Mode	Comply
17) WoW64	Comply
18) Syscall	Comply
19) Hollow Process Protection	Comply
20) DLL Hijacking	Comply
21) Application Lockdown	Comply
22) Java Lockdown	Comply
23) Squiblydoo AppLocker Bypass	Comply
24) CVE-2013-5331 & CVE-2014-4113 via Metasploit	Comply
25) Dynamic Shellcode Protection *Detects and blocks behavior of stagers*	Comply
26) EFS Guard	Comply
26) CTF Guard	Comply
26) ApiSetGuard	Comply
Advanced Exploit Mitigation	

Must be able to protect against a range of exploits or "active adversary" threats such as the following:	Comply
1) Credential Theft	Comply
2) APC Violation	Comply
3) Privilege Escalation	Comply
4) Code Cave Utilisation	Comply
5) Application Verifier Exploits	Comply
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.	Comply
Intrusion Prevention System (IPS)	
Must be able to prevent malicious network traffic with packet inspection (IPS).	Comply
Must be able to scan traffic at the lowest level and block threats before harming the operating system or applications.	Comply
Anti-Ransomware Protection	
Must have the ability for the encrypted files to be rolled back to a pre-encrypted state.	Comply
Both Anti-Exploit and Ransomware protection does not need to have a Cloud Lookup to perform the detection.	Comply
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.	Comply
The anti-crypto function shall look back at all the malicious file modifications made by that process and restores them to their original location.	Comply
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).	Comply
Must be able to protect from ransomware that encrypts the master boot record and from attacks that wipe the hard disk.	Comply
AMSI Protection	Comply
Must be able to protect against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI).	Comply
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.	Comply
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.).	Comply
Must have the capability to add device exemptions either by Model ID or Instance ID.	Comply
Application Control	
Must be able to detect and block application categories that may not be suitable for use in an enterprise environment.	Comply
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.	Comply
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	Comply
Threat Hunting	
Extend investigations to 30 days without bringing a device back online	Comply
Use ATP and IPS detections from the firewall to investigate suspect hosts	Comply
Compare email header information, SHAs, and other IoCs to identify malicious traffic to a domain	Comply
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.	Comply
Must be able to provide a report summary of the machine learning analysis of a suspicious file.	Comply
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.	Comply
Endpoint Isolation	
Must have an option to 'manually isolate' protected endpoints from the network while investigating a threat case.and an option to 'automatically isolate'	Comply
Threat Hunting	
What processes are trying to make a network connection on non-standard ports?	Comply
List detected IoCs mapped to the MITRE ATT&CK framework	Comply
Show processes that have recently modified files or registry keys	Comply
Search details about PowerShell executions	Comply
Identify processes disguised as services.exe	Comply