Ultimate Comparison of Microsoft Defender for Endpoint Features by OS

v6.0 (February 2024) | Author: Ru Campbell MVP

campbell.scot | twitter.com/rucam365 | linkedin.com/in/rlcam | github.com/rucam/defender-comparison

		Windows			Windows Server			macOS	Linux	Android	iOS
Feature	Description	7 SP1	8.1	10/11	2008 R2	2012 R2	2016	2019 / 2022				
Attack surface reduction											
ASR rules											
Block abuse of exploited vulnerable signed drivers	Protect against vulnerable signed drivers that allow kernel access and system			1709+		✓	✓	✓			
Block Adobe Reader from creating child processes	Prevents payloads breaking out of Adobe Reader.			1809+		✓	✓	✓			
Block all Office applications from creating child processes	Prevents Word, Excel, PowerPoint, OneNote, and Access creating child processes.			1709+		✓	✓	✓			
Block credential stealing from LSASS	Prevents untrusted processes accessing LSASS directly.			1803+		✓	✓	✓			
Block executable content from email client and webmail	Prevents Outlook and popular webmail providers launching scripts or executable files.			1709+		✓	✓	✓			
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	Using cloud-delivered protection, block executables depending on various reputational metrics.			1803+		✓	✓	✓			
Block execution of potentially obfuscated scripts	Identifies and blocks script obfuscation with suspicious properties.			1709+		✓	✓	✓			
Block JavaScript or VBScript from launching downloaded executable content	Prevents JavaScript or VBScript fetching and launching executables.			1709+				✓			
Block Office applications from creating executable content	Prevents the Office suite from saving executable content to disk.			1709+		✓	✓	✓			
Block Office applications from injecting code into other processes	Prevent attempts to migrate code into another process in Word, Excel, and PowerPoint.			1709+		✓	✓	✓			
Block Office communication applications from creating child processes	In Teams and Outlook, prevent child processes being created.			1809+		✓	✓	✓			
Block persistence through WMI event subscription	Prevent C2 abuse of WMI to attain device persistence.			1903+				✓			
Block process creations originating from PSExec and WMI commands	Prevents PSExec or WMI created processes from running, as is common in lateral movement techniques. Not compatible with ConfigMgr.			1803+		✓	✓	✓			
Block untrusted and unsigned processes that run from USB	Executable files on USB drives or SD cards are prevented from executing unless trusted or signed.			1803+		✓	✓	✓			
Block Webshell creation for Servers	For the Exchange server role only, block web shell script creation.						✓	✓			
Block Win32 API calls from Office macros	Protects against Office VBA Win32 API calls, mostly found in legacy macros.			1709+				✓			
Use advanced protection against ransomware	Using cloud-delivered protection heuristics, if a lower reputation file resembles ransomware and has not been signed, it is blocked.			1803+		✓	✓	✓			
ASR rules in warn mode if supported by rule	Allow users to override ASR blocked events.			1809+				✓			
Exploit protection	Successor to Enhanced Mitigation Experience Toolkit (EMET) with protection against over twenty exploit types.			1709+				✓			
Web protection	Comprised of web content filtering (access based on site category) and web threat protection (phishing, exploit sites, low rep sites).			1709+		✓	✓	✓	✓	✓	
Network protection	Extends web protection to the entire OS and third-party browsers, blocking outbound traffic to low-reputation or custom indicators. On mobile, protection against Wi-Fi threats.			1709+		✓	✓	✓	✓	✓	✓	✓
Controlled folder access	Ransomware protection where protected folders are specified, and only allow-listed applications may make modifications to them.			1709+		✓	✓	✓			
Device control – removable storage protection	Block the use of unauthorised removable storage media based on properties such as vendor ID, serial number, or device class.			✓					✓			
Device control – removable storage access control	Audit and control read/write/execute operations on removable storage media based on properties similar to removable storage protection.			✓					✓			
Device control – device installation	Control the installation of specific devices, e.g. block all except allowed or vice-versa			✓					✓			
Device control – printer protection	Block the use of unauthorised print devices based on vendor ID and product ID.			1809+								
Endpoint protection platform											
Microsoft Defender Antivirus (MDAV) / Next-Generation Protection	Core antimalware engine that provides behaviour-based, heuristic, and real-time AV protection; powers "next-generation protection" features in addition to standard signature-based detections.			✓		✓	✓	✓			
System Centre Endpoint Protection (SCEP) / Microsoft Antimalware for Azure (MAA)	"Down-level" operating systems do not have an antivirus engine built-in, however Microsoft's antimalware platform is available through other channels such as SCEP (comes with ConfigMgr), MAA (if managed with Azure), or Windows Defender (consumer-level).	✓	✓		✓	Only if not using unified agent					
Preventative antivirus (not "next-generation protection")	"Traditional" antivirus approach to potential threats. May have behavioural monitoring capabilities but is not the Next Generation Protection MDAV client seen in Windows.	✓	✓		✓			✓	✓		
Block at first sight	Block execution for up to 60 seconds while sending hash value of executable with mark of the web to cloud to determine reputation; if unknown hash, upload file for more analysis. (Roughly) degree of false positive tolerance is configurable using cloud-block level.			1803+		✓	✓	✓	Supports cloud-block level but not hold	Supports cloud-block level but not hold		
Cloud-delivered protection	Sends metadata to the cloud protection service to determine if a file is safe based on machine learning and Intelligent Security Graph.			✓		✓	✓	✓	✓	✓		
Tamper protection	Blocks uninstallation and other defense evasion techniques. On mobiles, detect if out of protection for seven days and inform device compliance.			✓		✓	✓	✓	✓	✓	✓	✓
Tamper protection for exclusions	Extends tamper protection to MDAV exclusions but only if DisableLocalAdminMerge is enabled, the device is Intune/ConfigMgr managed, and exclusions are managed by Intune.			✓		✓	✓	✓				
Contextual file and folder exclusions	Refine the scope of exclusions by controlling how they apply based on scan type, trigger, process, and/or file/folder.			✓		✓	✓	✓				
Potentially unwanted app protection	Blocks software that isn't necessarily malicious but otherwise undesirable, such as advertising injectors and cryptominers.			✓		✓	✓	✓	✓	✓		
Passive mode	If third-party endpoint protection is also running, antimalware engine doesn't provide preventative real-time protection (including ASR rules, etc) but can scan on-demand. Can be supplemented by EDR in block mode.			✓ Automatic		✓ Manual	✓ Manual	✓ Manual	✓ Manual	✓ Manual		
Respect indicators of compromise – files and certificates	Custom block or allow controls on the endpoint based on hash value or CER/PEM files.			1703+		✓	✓	✓	Files	Files		
Respect indicators of compromise – IPs and URLs	Custom block or allow controls based on public IP or FQDNs (or full web paths for Microsoft web browsers).			1709+		✓	✓	✓	✓	✓	✓	
Windows Defender Firewall with Advanced Security (WFAS)	Control the inbound and outbound network traffic allowed on the device based on the type of network connected, as well as other controls such as IPsec.	✓	✓	✓	✓	✓	✓	✓				
Troubleshooting mode	Instead of excluding a device from tamper protection to test problems, with troubleshooting mode a local admin can override endpoint security policy. During the troubleshooting window, configuration changes can be made. Diagnostic files are made available.			20H1+		✓	✓	✓	✓			
Performance mode	For Dev Drive, reduce the performance hit real-time protection has by performing scans asynchronously rather than synchronously (scan after open).			22H2+								
Host firewall reporting	Dedicated reporting available in the Microsoft 365 Defender portal about inbound + outbound connections and app connections.			✓		✓	✓	✓				
Investigation and response											
Alerts	Detected threats or potential malicious activity that should be reviewed, presented with a story, affected assets, and details.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Incidents	Aggregation of alerts with the same attack techniques or attributed to the same attacker.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device groups	Control RBAC permissions to devices and alerts, auto-remediation levels, and web content filtering. One device belongs to one group.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device tags	Create logical group affliction for filtering, reporting, and automatic device group membership. One device can have many tags.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Advanced hunting	Kusto query language (KQL) based tool for exploration of raw data across Microsoft 365 Defender, including custom detection rules.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
EDR in block mode	Remediates malicious artifacts in post-breach detections, including if third party AV is in use and MDAV is in passive mode.			✓		✓	✓	✓				
Automated investigation and response (AIR)	Uses inspection algorithms based on security analyst processes to examine and take (configurable) remedial action.			1709+		✓	✓	✓				
Deception	Automatically generate and deploy decoy assets such as hosts, accounts, and lures to trigger high confidence detections.			1809+								
File response actions											
Stop and quarantine file	Stop any running processes and quarantine the file, unless signed by Microsoft.			1703+		✓	✓	✓				
Automatically collect file for deep analysis	Executes the file in a cloud environment and report on behaviours such as contacted IPs, files created on disk, and registry modifications.			✓		✓	✓	✓				
Download quarantined file	Download a zipped version of the file that has been quarantined by Microsoft Defender Antivirus if collected under your sample submission policy.			1703+			✓	✓				
Device response actions											
Run antivirus scan	Initiates a full or quick even if in passive mode.			1709+		✓	✓	✓	✓	✓		
Restrict app execution	Implements a code integrity (Application Control) policy limiting files to those signed by Microsoft.			1709+				✓				
Isolate from the network (full)	Limits network connectivity on the endpoint to only the Defender for Endpoint service			1703+		✓	✓	✓	✓	✓		
Isolate from the network (selective)	Limits network connectivity on the endpoint to Defender for Endpoint and Microsoft 365 communication apps, such as Outlook and Teams.			1709+								
Forcibly release from isolation	Produce a device-unique script to end device isolation if it becomes unresponsive.			21H2+								
Contain device from the network	Block inbound and outbound communication with an unmanaged MDE discovered device.			✓				✓				
Contain user from the network	Blocks an identity on onboarded devices from inbound risky traffic (e.g. RPC, SMB, RDP, etc).			✓		✓	✓	✓				
Live response	Establishes a remote shell connection to the endpoint to collect forensics, run scripts, analyse threats, and threat hunt.			1709+		✓	✓	✓	✓	✓		
Collect an investigation package	Builds a zip file with folders on files on forensic information such as installed programs, autoruns, processes, SMB sessions, and system info.			1703+		✓	✓	✓	✓ via Live Response	✓ via Live Response		
Microsoft Defender Vulnerability Management											
OS vulnerabilities	Informs MDVM recommendations and weaknesses based on operating system vulnerabilities.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Software product vulnerabilities	Informs MDVM recommendations and weaknesses based on individual software vulnerabilities; not limited to Microsoft apps.		✓	1709+	✓	✓	✓	✓	✓	✓	✓	✓
OS configuration assessment	Informs MDVM recommendations based on system settings for the OS itself.		✓	1709+	✓	✓	✓	✓	✓	✓		
Software controls configuration assessment	Informs MDVM recommendations based allignment with control standards.		✓	1709+	✓	✓	✓	✓	✓	✓		
Software product configuration assessment	Informs MDVM recommendations based on app configurations.		✓	1709+	✓	✓	✓	✓	✓	✓		
Device discovery	Endpoints passively or actively collect events and extract device information (basic mode) or actively probe observed devices (standard mode; default). This refers to OSs that can perform discovery.			1809+				✓				
Software usage insights	In the software inventory, findout software usage statistics such as median usage over 30d.			✓								
Security baseline assessments (add-on license)	Assess devices against security benchmarks such as CIS and STIG (specific benchmarks vary by OS.			✓	✓	✓	✓	✓				
Firmware assessments (add-on license)	Informs MDVM recommendations based on exposure to firmware vulnerabilities.			✓		✓	✓	✓	✓	✓		
Block vulnerable applications (add-on license)	Temporarily block or warn on launch all known vulnerable versions of an application until the remediation request is completed. Based on file indicators of compromise and enforced by MDAV. First-party apps not supported.			1809+								
Browser extensions (add-on license)	For Edge, Chrome, and Firefox, report installed browser extensions and their permission risk in the Microsoft 365 Defender inventory page.			1709+		✓	✓	✓				
Certificate inventory (add-on license)	For certificates in the local machine store, report them in the Microsoft 365 Defender inventory page. Includes validity period, key size, issuer, etc.			1709+		✓	✓	✓				
Mobile Threat Defense											
Microsoft Tunnel	A VPN gateway for Intune managed mobile devices that leverages Azure AD for Conditional Access benefits.									✓ Unified	✓ Standalone	
Jailbreak detection	Raise alerts for potential defence evasion by reporting jailbroken devices and mark them as high risk.										✓	
Mobile application management (MAM) support	Requires device have MDE app and AAD registration but doesn't require full MDM enrolment. Then sends risk score to control access.									✓	✓	
Potentially unwanted or malicious app scanning	Uses both signatures and ML/heuristics to protect against unsafe apps and files.									✓		
Phishing protection	Using a loopback VPN, protects against potentially malicious web traffic in browsers, email, app, and messaging apps.									✓	✓	
Privacy controls	For MDM or MAM (enrolled or unenrolled) devices, end users can configure what is shared with admins. Admins can also configure privacy settings of alerts.									✓	✓	
Optional permissions and disable web protection	Allows you to not require the previously mandatory permissions (e.g. VPN) at the expense of the web protection capability.									✓	✓	
Mobile network protection	Wi-Fi threat protection, such as against pineapple devices, and alerts/remediation options with a suspicious network is detected.									✓	✓	
Onboarding and management											
Microsoft Monitoring Agent (MMA) required	Windows OSs without EDR capabilities built-in require MMA installed with a workspace ID and key specified (obtained from portal).	✓	✓		✓	Only if not using unified agent	Only if not using unified agent					
'Unified solution' agent available	For down-level Windows Server OSs, the unified solution agent (MSI installer) provides near parity with Windows Server 2019's capabilities and removes the need for the Microsoft Monitoring Agent.					✓	✓					
Security Management for MDE	Manage configuration using Endpoint Manager admin centre just like Intune devices without enrolling device in MDM. Also known as "MDE Attach". Supports MDAV, firewall, ASR rules, and EDR sensor settings. Device must already be onboarded.			✓		✓	✓	✓				
Windows Subsystem for Linux (WSL) 2	Using a plug-in, WSL 2.0.7+ will be available in MDE device inventory as a Linux device (same name as Windows host but separate object).			2004+								
Microsoft Defender for Cloud (Microsoft Defender for Servers)	MDE is included as part of the Microsoft Defender for Servers licensing (a paid component of Defender for Cloud). Using Azure Arc, can be extended to systems not hosted in Azure (on-premises; third-party cloud).			Enterprise Mulit-Session	✓	✓	✓	✓	✓			
Microsoft Intune	Microsoft's MDM service and can be used for onboarding supported OSs.			✓					✓		✓	✓
Microsoft Configuration Manager	On-premises based endpoint and server management solution.	✓	✓			✓	✓	✓				
Jamf Pro	Alternative MDM for macOS.								✓			
Puppet / Ansible / Chef	Scalable automation and orchestration platforms for Linux.								✓			