The Big Comparison of Microsoft Defender for Endpoint Features by Operating System v1.0 (10 July 2021)
Ru Campbell
campbell.scot/the-big-comparison-of-defender-for-endpoint-features-by-operating-system
twitter.com/rucam365
linkedin.com/in/rlcam

Feature	Description	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2008 R2 + 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server SAC	macOS	Linux	Android phones	iOS
Attack surface reduction												
Attack surface reduction rules												
Block abuse of exploited vulnerable signed drivers	Protect against vulnerable signed drivers that allow kernel access and system compromise.			1709+			✓	1803+				
Block Adobe Reader from creating child processes	Prevents payloads breaking out of Adobe Reader.			1809+			✓	1809+				
Block all Office applications from creating child processes	Prevents Word, Excel, PowerPoint, OneNote, and Access creating child processes.			1709+			✓	1809+				
Block credential stealing from LSASS	Prevents untrusted processes accessing LSASS directly.			1803+			✓	1809+				
Block executable content from email client and webmail	Prevents Outlook and popular webmail providers launching scripts or executable files.			1709+			✓	1809+				
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+			✓	1809+				
Block execution of potentially obfuscated scripts	Identifies and blocks script obfuscation with suspicious properties.			1709+			✓	1809+				
Block JavaScript or VBScript from launching downloaded executable content	Prevents JavaScript or VBScript fetching and launching executables.			1709+			✓	1809+				
Block Office applications from creating executable content	Prevents the Office suite from saving executable content to disk.			1709+			✓	1809+				
Block Office applications from injecting code into other processes	Prevent attempts to migrate code into another process in Word, Excel, and PowerPoint.			1709			✓	1809+				
Block Office communication applications from creating child processes	In Teams and Outlook, prevent child processes being created.			1809+			✓	1809+				
Block persistence through WMI event subscription	Prevent C2 abuse of WMI to attain device persistence.			1903+				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+			✓	1809+				
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+			✓	1809+				
Block Win32 API calls from Office macros	Protects against Office VBA Win32 API calls, mostly found in legacy macros.			1709+			✓	1809+				
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+			✓	1809+				
ASR rules in warn mode if supported by rule	Allow users to override ASR blocked events.			1809+			✓	1809+				
Exploit protection	Successor to Enhanced Mitigation Experience Toolkit (EMET) with protection against over twenty exploit types.			1709+			✓	1803+				
Web protection	Comprised of web content filtering (access based on site category) and web threat protection (phishing, exploit sites, low rep sites).			1709+			✓	1803+				
Network protection	Extends web protection to the entire OS and third-party browsers, blocking outbound traffic to low-reputation or custom indicators.			1709+			✓	1803+				
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.			✓					10.15.4+ not all properties			
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 – printer protection	Block the use of unauthorised print devices based on vendor ID and product ID.			1909+								

Feature	Description	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2008 R2 + 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server SAC	macOS	Linux	Android phones	iOS
Endpoint protection platform												
Microsoft Defender Antivirus (MDAV) preinstalled	Core antimalware engine that provides behaviour-based, heuristic, and real-time AV protection; powers "next-generation protection" features.			✓		✓	✓	1803+				
System Centre Endpoint Protection (SCEP) / Microsoft Antimalware for Azure (MAA) / etc	"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 Security Essentials (consumer-level).	✓	✓		✓							
Preventative antivirus	"Traditional" signature-based antivirus approach to potential threats.	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Block at first sight	Sends hash value of executables with mark of the web to cloud to determine reputation; if unknown hash, upload file for more analysis.			1803+								
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	Locks changes to MDAV via registry, PowerShell, and GPO; limits endpoint configuration to MDM channels (Intune).			✓		✓	✓	1803+				
Potentially unwanted app protection	Blocks software that isn't necessarily malicious but otherwise undesirable, such as advertising injectors and cryptominers.			✓		✓	✓		✓	✓		
Microsoft Defender Antivirus active/passive/disable if third party AV	MDAV can detect the presence of a third party and enter passive mode to still scan and detect threats, but not remediate, unless EDR in block mode is enabled.			Automatic		Manual – disable only	Manual - passive	1803+ Manual - passive				
Unmanaged device discovery	Endpoints passively collect events and extract device information (basic mode) or actively probe observed devices (standard mode; default).			1809+								
Respect indicators of compromise – files and certificates	Custom block or allow controls on the endpoint based on hash value or CER/PEM files.			1703+		✓	✓					
Respect indicators of compromise – IPs, URLs, domains	Custom block or allow controls based on public IP or FQDNs (or full web paths for Microsoft web browsers).			1709+								

Feature	Description	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2008 R2 + 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server SAC	macOS	Linux	Android phones	iOS
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.			✓		✓ if MDAV active	✓	1803+				
Automated investigation and response (AIR)	Uses inspection algorithms based on security analyst processes to examine and take (configurable) remedial action.			1709+			✓					
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.			✓								
Device response actions												
Run antivirus scan	Initiates a full or quick MDAV scan even if MDAV is in passive mode.			1709+			✓	1809+				
Restrict app execution	Implements a code integrity (Application Control) policy limiting files to those signed by Microsoft.			1709+			✓	1809+				
Isolate from the network (full)	Limits network connectivity on the endpoint to only the Defender for Endpoint service.			1703+			✓	1809+				

Isolate from the network (selective)	Limits network connectivity on the endpoint to Defender for Identity and Office 365 communication apps, such as Outlook and Teams.			1709+			✓	1809+				
Live response	Establishes a remote shell connection to the endpoint to collect forensics, run scripts, analyse threats, and threat hunt.			1709+			✓	1809+				
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+			✓	1809+				

Feature	Description	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2008 R2 + 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server SAC	macOS	Linux	Android phones	iOS
Threat and vulnerability management												
OS vulnerabilities	Informs TVM recommendations and weaknesses based on operating system vulnerabilities.	✓	✓	✓	✓	✓	✓	✓	✓	✓ ex. SUSE + Debian		
Software product vulnerabilities	Informs TVM recommendations and weaknesses based on individual software vulnerabilities; not limited to Microsoft apps.		✓	1709+	✓	✓	✓	✓	✓			
OS configuration assessment	Informs TVM recommendations based on system settings for the OS itself.		✓		✓	✓	✓	✓	✓			
Software product configuration assessment	Informs TVM recommendations based on app configurations.		✓		✓	✓	✓	✓	✓			

Feature	Description	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2008 R2 + 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server SAC	macOS	Linux	Android phones	iOS
Mobile OS Support												
Microsoft Tunnel	A VPN gateway for Intune managed mobile devices that leverages Azure AD for Conditional Access benefits.										✓ Unified	✓ Preview
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.										✓	✓

Approach	Description	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2008 R2 + 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server SAC	macOS	Linux	Android phones	iOS
Onboarding												
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).	✓	✓		✓	✓						
Azure Defender	MDE is included as part of the Azure Defender for servers licensing and can be managed from the Azure Security Centre. Using Azure Arc, can be extended to systems not hosted in Azure.			Enterprise Multi-Session	✓	✓	✓			✓ Preview		
Microsoft Endpoint Manager Intune	Microsoft's MDM service and can be used for onboarding supported OSs.			✓					✓		✓	✓
Microsoft Endpoint Manager Configuration Manager	On-premises based endpoint and server management solution.		✓	✓	2012 R2	✓	✓	1803+				
Jamf Pro	Alternative MDM for macOS.								✓			
Puppet / Ansible	Scalable automation and orchestration platforms for Linux.									✓		