Name	GUID	Description	mapping type	target ID	target type	target name	target ref	Refs	Advanced hunting action type	Dependencies
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2	This rule helps prevent credential stealing by locking down Local Security Authority Subsystem Service (LSASS). LSASS authenticates users who sign in on a Windows computer. Microsoft Defender Credential Guard in Windows normally prevents attempts to extract credentials from LSASS. Some organizations can't enable Credential Guard on all of their computers because of compatibility issues with custom smartcard drivers or other programs that load into the Local Security Authority (LSA). In these cases, attackers can use tools like Mimikatz to scrape cleartext passwords and NTLM hashes from LSASS. By default the state of this rule is set to block. In most cases, many processes make calls to LSASS for access rights that are not needed. For example, such as when the initial block from the ASR rule results in a subsequent call for a lesser privilege which subsequently succeeds. For information about the types of rights that are typically requested in process calls to LSASS, see: Process Security and Access Rights. Enabling this rule doesn't provide additional protection if you have LSA protection enabled since the ASR rule and LSA protection work similarly. However, when LSA protection cannot be enabled, this rule can be configured to provide equivalent protection against malware that target lsass.exe.	mitigates	T1003.001	sub-technique	LSASS Memory	attack-pattern--65f2d882-3141-4d48-8a06-29bf77ec9f90	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-credential-stealing-from-the-windows-local-security-authority-subsystem	AsrLsassCredentialTheftAudited AsrLsassCredentialTheftBlocked	Microsoft Defender Antivirus
Block execution of potentially obfuscated scripts	5beb7efe-fd9a-4556-801d-275e5ffc04cc	This rule detects suspicious properties within an obfuscated script. Important: PowerShell scripts are now supported for the "Block execution of potentially obfuscated scripts" rule. Script obfuscation is a common technique that both malware authors and legitimate applications use to hide intellectual property or decrease script loading times. Malware authors also use obfuscation to make malicious code harder to read, which hampers close scrutiny by humans and security software.	mitigates	T1027.010	sub-technique	Command Obfuscation	attack-pattern--d511a6f6-4a33-41d5-bc95-c343675d1377	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-execution-of-potentially-obfuscated-scripts	AsrObfuscatedScriptAudited AsrObfuscatedScriptBlocked	Microsoft Defender Antivirus, AntiMalware Scan Interface (AMSI)
Block execution of potentially obfuscated scripts	5beb7efe-fd9a-4556-801d-275e5ffc04cc	This rule detects suspicious properties within an obfuscated script. Important: PowerShell scripts are now supported for the "Block execution of potentially obfuscated scripts" rule. Script obfuscation is a common technique that both malware authors and legitimate applications use to hide intellectual property or decrease script loading times. Malware authors also use obfuscation to make malicious code harder to read, which hampers close scrutiny by humans and security software.	mitigates	T1027.013	sub-technique	Encrypted/Encoded File	attack-pattern--0d91b3c0-5e50-47c3-949a-2a796f04d144	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-execution-of-potentially-obfuscated-scripts	AsrObfuscatedScriptAudited AsrObfuscatedScriptBlocked	Microsoft Defender Antivirus, AntiMalware Scan Interface (AMSI)
Block use of copied or impersonated system tools (preview)	c0033c00-d16d-4114-a5a0-dc9b3a7d2ceb	This rule blocks the use of executable files that are identified as copies of Windows system tools. These files are either duplicates or impostors of the original system tools. Some malicious programs may try to copy or impersonate Windows system tools to avoid detection or gain privileges. Allowing such executable files can lead to potential attacks. This rule prevents propagation and execution of such duplicates and impostors of the system tools on Windows machines. Note: This capability is currently in preview. Additional upgrades to improve efficacy are under development.	mitigates	T1036.003	sub-technique	Rename System Utilities	attack-pattern--bd5b58a4-a52d-4a29-bc0d-3f1d3968eb6b	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-use-of-copied-or-impersonated-system-tools-preview		Microsoft Defender Antivirus
Block use of copied or impersonated system tools (preview)	c0033c00-d16d-4114-a5a0-dc9b3a7d2ceb	This rule blocks the use of executable files that are identified as copies of Windows system tools. These files are either duplicates or impostors of the original system tools. Some malicious programs may try to copy or impersonate Windows system tools to avoid detection or gain privileges. Allowing such executable files can lead to potential attacks. This rule prevents propagation and execution of such duplicates and impostors of the system tools on Windows machines. Note: This capability is currently in preview. Additional upgrades to improve efficacy are under development.	mitigates	T1036.005	sub-technique	Rename System Utilities	attack-pattern--1c4e5d32-1fe9-4116-9d9d-59e3925bd6a2	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-use-of-copied-or-impersonated-system-tools-preview		Microsoft Defender Antivirus
Block process creations originating from PSExec and WMI commands	d1e49aac-8f56-4280-b9ba-993a6d77406c	This rule blocks processes created through PsExec and WMI from running. Both PsExec and WMI can remotely execute code. There's a risk of malware abusing functionality of PsExec and WMI for command and control purposes, or to spread an infection throughout an organization's network. Warning: Only use this rule if you're managing your devices with Intune or another MDM solution. This rule is incompatible with management through Microsoft Endpoint Configuration Manager because this rule blocks WMI commands the Configuration Manager client uses to function correctly.	mitigates	T1047	technique	Windows Management Instrumentation	attack-pattern--01a5a209-b94c-450b-b7f9-946497d91055	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-process-creations-originating-from-psexec-and-wmi-commands	AsrPsexecWmiChildProcessAudited AsrPsexecWmiChildProcessBlocked	Microsoft Defender Antivirus
Block Office applications from injecting code into other processes	75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84	This rule blocks code injection attempts from Office apps into other processes. Note: The Block applications from injecting code into other processes ASR rule does not support WARN mode. Important: This rule requires restarting Microsoft 365 Apps (Office applications) for the configuration changes to take effect. Attackers might attempt to use Office apps to migrate malicious code into other processes through code injection, so the code can masquerade as a clean process. There are no known legitimate business purposes for using code injection. This rule applies to Word, Excel, OneNote, and PowerPoint.	mitigates	T1055	technique	Process Injection	attack-pattern--43e7dc91-05b2-474c-b9ac-2ed4fe10114d	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-office-applications-from-injecting-code-into-other-processes	AsrOfficeProcessInjectionAudited AsrOfficeProcessInjectionBlocked	Microsoft Defender Antivirus
Block JavaScript or VBScript from launching downloaded executable content	d3e037e1-3eb8-44c8-a917-57927947596d	This rule prevents scripts from launching potentially malicious downloaded content. Malware written in JavaScript or VBScript often acts as a downloader to fetch and launch other malware from the Internet. Although not common, line-of-business applications sometimes use scripts to download and launch installers.	mitigates	T1059.005	sub-technique	Visual Basic	attack-pattern--dfd7cc1d-e1d8-4394-a198-97c4cab8aa67	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-javascript-or-vbscript-from-launching-downloaded-executable-content	AsrScriptExecutableDownloadAudited AsrScriptExecutableDownloadBlocked	Microsoft Defender Antivirus, AMSI
Block JavaScript or VBScript from launching downloaded executable content	d3e037e1-3eb8-44c8-a917-57927947596d	This rule prevents scripts from launching potentially malicious downloaded content. Malware written in JavaScript or VBScript often acts as a downloader to fetch and launch other malware from the Internet. Although not common, line-of-business applications sometimes use scripts to download and launch installers.	mitigates	T1059.007	sub-technique	JavaScript	attack-pattern--0f4a0c76-ab2d-4cb0-85d3-3f0efb8cba0d	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-javascript-or-vbscript-from-launching-downloaded-executable-content	AsrScriptExecutableDownloadAudited AsrScriptExecutableDownloadBlocked	Microsoft Defender Antivirus, AMSI
Block abuse of exploited vulnerable signed drivers	56a863a9-875e-4185-98a7-b882c64b5ce5	This rule prevents an application from writing a vulnerable signed driver to disk. In-the-wild, vulnerable signed drivers can be exploited by local applications - that have sufficient privileges - to gain access to the kernel. Vulnerable signed drivers enable attackers to disable or circumvent security solutions, eventually leading to system compromise. The Block abuse of exploited vulnerable signed drivers rule doesn't block a driver already existing on the system from being loaded.	mitigates	T1068	technique	Exploitation for Privilege Escalation	attack-pattern--b21c3b2d-02e6-45b1-9800-e69051040839	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-abuse-of-exploited-vulnerable-signed-drivers	AsrVulnerableSignedDriverAudited AsrVulnerableSignedDriverBlocked	Microsoft Defender Antivirus
Block untrusted and unsigned processes that run from USB	b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4	With this rule, admins can prevent unsigned or untrusted executable files from running from USB removable drives, including SD cards. Blocked file types include executable files (such as .exe, .dll, or .scr) Important: Files copied from the USB to the disk drive will be blocked by this rule if and when it's about to be executed on the disk drive.	mitigates	T1091		Replication Through Removable Media	attack-pattern--3b744087-9945-4a6f-91e8-9dbceda417a4	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-untrusted-and-unsigned-processes-that-run-from-usb	AsrUntrustedUsbProcessAudited AsrUntrustedUsbProcessBlocked	Microsoft Defender Antivirus
Block Win32 API calls from Office macros	92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b	This rule prevents VBA macros from calling Win32 APIs. Office VBA enables Win32 API calls. Malware can abuse this capability, such as calling Win32 APIs to launch malicious shellcode without writing anything directly to disk. Most organizations don't rely on the ability to call Win32 APIs in their day-to-day functioning, even if they use macros in other ways.	mitigates	T1106	technique	Native API	attack-pattern--3910d824f-0ef1-47a0-b0ee-c59a75e27670	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-win32-api-calls-from-office-macros	AsrOfficeMacroWin32ApiCallsAudited AsrOfficeMacroWin32ApiCallsBlocked	Microsoft Defender Antivirus, AMSI
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access. Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	mitigates	T1137	technique	Office Application Startup	attack-pattern--2c4d4e92-0ccf-4a97-b54c-86d66298b853	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-all-office-applications-from-creating-child-processes	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	Microsoft Defender Antivirus
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access. Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	mitigates	T1137.001	sub-technique	Office Template Macros	attack-pattern--79a47ad0-fc3b-4821-9f01-a026b1ddba21	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-all-office-applications-from-creating-child-processes	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	Microsoft Defender Antivirus
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access. Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	mitigates	T1137.002	sub-technique	Office Test	attack-pattern--ed7efd4d-ce28-4a19-a8e6-c58011eb2c7a	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-all-office-applications-from-creating-child-processes	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	Microsoft Defender Antivirus
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access. Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	mitigates	T1137.003	sub-technique	Outlook Forms	attack-pattern--a9e2cea0-c805-4bf8-9e31-f9f0513a3634	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-all-office-applications-from-creating-child-processes	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	Microsoft Defender Antivirus
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access. Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	mitigates	T1137.004	sub-technique	Outlook Home Page	attack-pattern--bf147104-abf9-4221-95d1-e8185859441	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-all-office-applications-from-creating-child-processes	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	Microsoft Defender Antivirus
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access. Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	mitigates	T1137.005	sub-technique	Outlook Rules	attack-pattern--3d1b9d7e-3921-4d25-845a-7d9f15c0da44	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-all-office-applications-from-creating-child-processes	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	Microsoft Defender Antivirus
Block Office communication application from creating child processes	26190899-1602-49e8-8b27-eb1d0a1ce869	This rule prevents Outlook from creating child processes, while still allowing legitimate Outlook functions. This rule protects against social engineering attacks and prevents exploiting code from abusing vulnerabilities in Outlook. It also protects against Outlook rules and forms exploits that attackers can use when a user's credentials are compromised. Note: This rule blocks DLP policy tips and ToolTips in Outlook. This rule applies to Outlook and Outlook.com only.	mitigates	T1137.005	sub-technique	Outlook Rules	attack-pattern--3d1b9d7e-3921-4d25-845a-7d9f15c0da44	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-office-communication-application-from-creating-child-processes	AsrOfficeCommAppChildProcessAudited AsrOfficeCommAppChildProcessBlocked	Microsoft Defender Antivirus
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access. Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	mitigates	T1137.006	sub-technique	Add-ins	attack-pattern--34f1d81d-fe88-4f97-bd3b-a3164536255d	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-all-office-applications-from-creating-child-processes	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	Microsoft Defender Antivirus
Block Office applications from creating executable content	3b576869-a4ec-4529-8536-b80a7769e899	This rule prevents Office apps, including Word, Excel, and PowerPoint, from creating potentially malicious executable content, by blocking malicious code from being written to disk. Malware that abuses Office as a vector might attempt to break out of Office and save malicious components to disk. These malicious components would survive a computer reboot and persist on the system. Therefore, this rule defends against a common persistence technique. This rule also blocks execution of untrusted files that may have been saved by Office macros that are allowed to run in Office files.	mitigates	T1137.006	sub-technique	Add-ins	attack-pattern--34f1d81d-fe88-4f97-bd3b-a3164536255d	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-office-applications-from-creating-executable-content	AsrExecutableOfficeContentAudited AsrExecutableOfficeContentBlocked	Microsoft Defender Antivirus, RPC
Block Office communication application from creating child processes	26190899-1602-49e8-8b27-eb1d0a1ce869	This rule prevents Outlook from creating child processes, while still allowing legitimate Outlook functions. This rule protects against social engineering attacks and prevents exploiting code from abusing vulnerabilities in Outlook. It also protects against Outlook rules and forms exploits that attackers can use when a user's credentials are compromised. Note: This rule blocks DLP policy tips and ToolTips in Outlook. This rule applies to Outlook and Outlook.com only.	mitigates	T1203	technique	Exploitation for Client Execution	attack-pattern--be2dcee9-a7a7-4e38-afd6-21b31ecc3d63	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-office-communication-application-from-creating-child-processes	AsrOfficeCommAppChildProcessAudited AsrOfficeCommAppChildProcessBlocked	Microsoft Defender Antivirus

Block executable files from running unless they meet a prevalence, age, or trusted list criteria	01443614-cd74-433a-b99e-2ecdc07bfc25	This rule blocks executable files, such as .exe, .dll, or .scr, from launching. Thus, launching untrusted or unknown executable files can be risky, as it might not be initially clear if the files are malicious. Important: You must enable cloud-delivered protection to use this rule. The rule Block executable files from running unless they meet a prevalence, age, or trusted list criterion with GUID 01443614-cd74-433a-b99e-2ecdc07bfc25 is owned by Microsoft and is not specified by admins. This rule uses cloud-delivered protection to update its trusted list regularly. You can specify individual files or folders (using folder paths or fully qualified resource names) but you can't specify which rules or exclusions apply to.	mitigates	T1204	technique	User Execution	attack-pattern--8c32eb4d-809f-4fc5-bf60-c44476c131b5	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-executable-files-from-running-unless-they-meet-a-prevalence-age-or-trusted-list-criterion	AsrUntrustedExecutableAudited AsrUntrustedExecutableBlocked	Microsoft Defender Antivirus, Cloud Protection
Block Adobe Reader from creating child processes	7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c	This rule prevents attacks by blocking Adobe Reader from creating processes. Malware can download and launch payloads and break out of Adobe Reader through social engineering or exploits. By blocking child processes from being generated by Adobe Reader, malware attempting to use Adobe Reader as an attack vector are prevented from spreading.	mitigates	T1204.002	sub-technique	Malicious File	attack-pattern--232b7f21-adf9-4b42-b936-b9d8f7df856e	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-adobe-reader-from-creating-child-processes	AsrAdobeReaderChildProcessAudited AsrAdobeReaderChildProcessBlocked	Microsoft Defender Antivirus
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access. Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	mitigates	T1204.002	sub-technique	Malicious File	attack-pattern--232b7f21-adf9-4b42-b936-b9d8f7df856e	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-all-office-applications-from-creating-child-processes	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	Microsoft Defender Antivirus
Block executable content from email client and webmail	be9ba2d9-53ea-4cdc-84e5-9b1eeee46550	This rule blocks email opened within the Microsoft Outlook application, or Outlook.com and other popular webmail providers from propagating the following file types: Executable files (such as .exe, .dll, or .scr) Script files (such as a PowerShell .ps1, Visual Basic .vbs, or JavaScript .js file)	mitigates	T1204.002	sub-technique	Malicious File	attack-pattern--232b7f21-adf9-4b42-b936-b9d8f7df856e	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-executable-content-from-email-client-and-webmail	AsrExecutableEmailContentAudited AsrExecutableEmailContentBlocked	Microsoft Defender Antivirus
Use advanced protection against ransomware	c1db55ab-c21a-4637-bb3f-a12568109d35	This rule provides an extra layer of protection against ransomware. It uses both client and cloud heuristics to determine whether a file resembles ransomware. This rule doesn't block files that have one or more of the following characteristics: The file has already been found to be unharmful in the Microsoft cloud. The file is a valid signed file. The file is prevalent enough to not be considered as ransomware. The rule tends to err on the side of caution to prevent ransomware. Note: You must enable cloud-delivered protection to use this rule.	mitigates	T1486	technique	Data Encrypted for Impact	attack-pattern--b80d107d-fa0d-4b60-9684-b0433e8bdba0	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#use-advanced-protection-against-ransomware	AsrRansomwareAudited AsrRansomwareBlocked	Microsoft Defender Antivirus, Cloud Protection
Block Webshell creation for Servers	a8f5898e-1dc8-49a9-9878-85004b8a61e6	This rule blocks web shell script creation on Microsoft Server, Exchange Role. A web shell script is a specifically crafted script that allows an attacker to control the compromised server. A web shell may include functionalities such as receiving and executing malicious commands, downloading and executing malicious files, stealing and exfiltrating credentials and sensitive information, identifying potential targets etc.	mitigates	T1505.003	sub-technique	Web Shell	attack-pattern--5d0d3609-d06d-49e1-b8c9-b544e0c618cb	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-webshell-creation-for-servers		Microsoft Defender Antivirus
Block abuse of exploited vulnerable signed drivers	56a863a9-875e-4185-98a7-b882c64b5ce5	This rule prevents an application from writing a vulnerable signed driver to disk. In-the-wild, vulnerable signed drivers can be exploited by local applications - that have sufficient privileges - to gain access to the kernel. Vulnerable signed drivers enable attackers to disable or circumvent security solutions, eventually leading to system compromise. The Block abuse of exploited vulnerable signed drivers rule doesn't block a driver already existing on the system from being loaded.	mitigates	T1543	technique	Create or Modify System Process	attack-pattern--106c0cf6-bf73-4601-9aa8-0945c2715ec5	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-abuse-of-exploited-vulnerable-signed-drivers	AsrVulnerableSignedDriverAudited AsrVulnerableSignedDriverBlocked	Microsoft Defender Antivirus
Block abuse of exploited vulnerable signed drivers	56a863a9-875e-4185-98a7-b882c64b5ce5	This rule prevents an application from writing a vulnerable signed driver to disk. In-the-wild, vulnerable signed drivers can be exploited by local applications - that have sufficient privileges - to gain access to the kernel. Vulnerable signed drivers enable attackers to disable or circumvent security solutions, eventually leading to system compromise. The Block abuse of exploited vulnerable signed drivers rule doesn't block a driver already existing on the system from being loaded.	mitigates	T1543.003	sub-technique	Windows Service	attack-pattern--2959d63f-73fd-46a1-abd2-109d7dcede32	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-abuse-of-exploited-vulnerable-signed-drivers	AsrVulnerableSignedDriverAudited AsrVulnerableSignedDriverBlocked	Microsoft Defender Antivirus
Block persistence through WMI event subscription	e6db77e5-3df2-4cf1-b95a-636979351e5b	This rule prevents malware from abusing WMI to attain persistence on a device. Important: File and folder exclusions don't apply to this attack surface reduction rule. Fileless threats employ various tactics to stay hidden, to avoid being seen in the file system, and to gain periodic execution control. Some threats can abuse the WMI repository and event model to stay hidden. Note: If CcmExec.exe (SCCM Agent) is detected on the device, the ASR rule is classified as "not applicable" in Defender for Endpoint settings in the Microsoft Defender portal.	mitigates	T1546.003	sub-technique	Windows Management Instrumentation Event Subscription	attack-pattern--91096bdd-8c0a-475a-9cc1-5e029b2fad58	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-persistence-through-wmi-event-subscription	AsrPersistenceThroughWmiAudited AsrPersistenceThroughWmiBlocked	Microsoft Defender Antivirus, RPC
Block rebooting machine in Safe Mode (preview)	33ddedf1-c6e0-47cb-833e-de6133960387	This rule prevents the execution of commands to restart machines in Safe Mode. Safe Mode is a diagnostic mode that only loads the essential files and drivers needed for Windows to run. However, in Safe Mode, many security products are either disabled or operate in a limited capacity, which allows attackers to further launch tampering commands, or simply execute and encrypt all files on the machine. This rule blocks such attacks by preventing processes from restarting machines in Safe Mode.	mitigates	T1562.009	sub-technique	Safe Mode Boot	attack-pattern--28170e17-8384-415c-8486-2e6b294cb803	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-rebooting-machine-in-safe-mode-preview		Microsoft Defender Antivirus
Block process creations originating from PSExec and WMI commands	d1e49aac-8f56-4280-b9ba-993a6d77406c	This rule blocks processes created through PsExec and WMI from running. Both PsExec and WMI can remotely execute code. There's a risk of malware abusing functionality of PsExec and WMI for command and control purposes, or to spread an infection throughout an organization's network. Warning: Only use this rule if you're managing your devices with Intune or another MDM solution. This rule is incompatible with management through Microsoft Endpoint Configuration Manager because this rule blocks WMI commands the Configuration Manager client uses to function correctly.	mitigates	T1569.002	sub-technique	Service Execution	attack-pattern--f1951e8a-500e-4a26-8803-76d95c4554b4	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-process-creations-originating-from-psexec-and-wmi-commands	AsrPsexecWmiChildProcessAudited AsrPsexecWmiChildProcessBlocked	Microsoft Defender Antivirus
Block process creations originating from PSExec and WMI commands	d1e49aac-8f56-4280-b9ba-993a6d77406c	This rule blocks processes created through PsExec and WMI from running. Both PsExec and WMI can remotely execute code. There's a risk of malware abusing functionality of PsExec and WMI for command and control purposes, or to spread an infection throughout an organization's network. Warning: Only use this rule if you're managing your devices with Intune or another MDM solution. This rule is incompatible with management through Microsoft Endpoint Configuration Manager because this rule blocks WMI commands the Configuration Manager client uses to function correctly.	mitigates	T1570	technique	Lateral Tool Transfer	attack-pattern--bf90d72c-c00b-45e3-b3aa-6856056d4c5	https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-process-creations-originating-from-psexec-and-wmi-commands	AsrPsexecWmiChildProcessAudited AsrPsexecWmiChildProcessBlocked	Microsoft Defender Antivirus