Attack surface reduction rules overview

Article • 05/02/2024 • 4 contributors

Feedback

In this article

Applies to:

- Microsoft Defender for Endpoint Plan 1
- Microsoft Defender for Endpoint Plan 2
- Microsoft Defender XDR
- Microsoft Defender Antivirus

Platforms

- Windows

Tip

As a companion to this article, see our Security Analyzer setup guide to review best practices and learn to fortify defenses, improve compliance, and navigate the cybersecurity landscape with confidence. For a customized experience based on your environment, you can access the Security Analyzer automated setup guide in the Microsoft 365 admin center.

Why attack surface reduction rules are important

Your organization's attack surface includes all the places where an attacker could compromise your organization's devices or networks. Reducing your attack surface means protecting your

Download PDF

organization's devices and network, which leaves attackers with fewer ways to perform attacks. Configuring attack surface reduction rules in Microsoft Defender for Endpoint can help!

Attack surface reduction rules target certain software behaviors, such as:

- Launching executable files and scripts that attempt to download or run files
- Running obfuscated or otherwise suspicious scripts
- Performing behaviors that apps don't usually initiate during normal day-to-day work

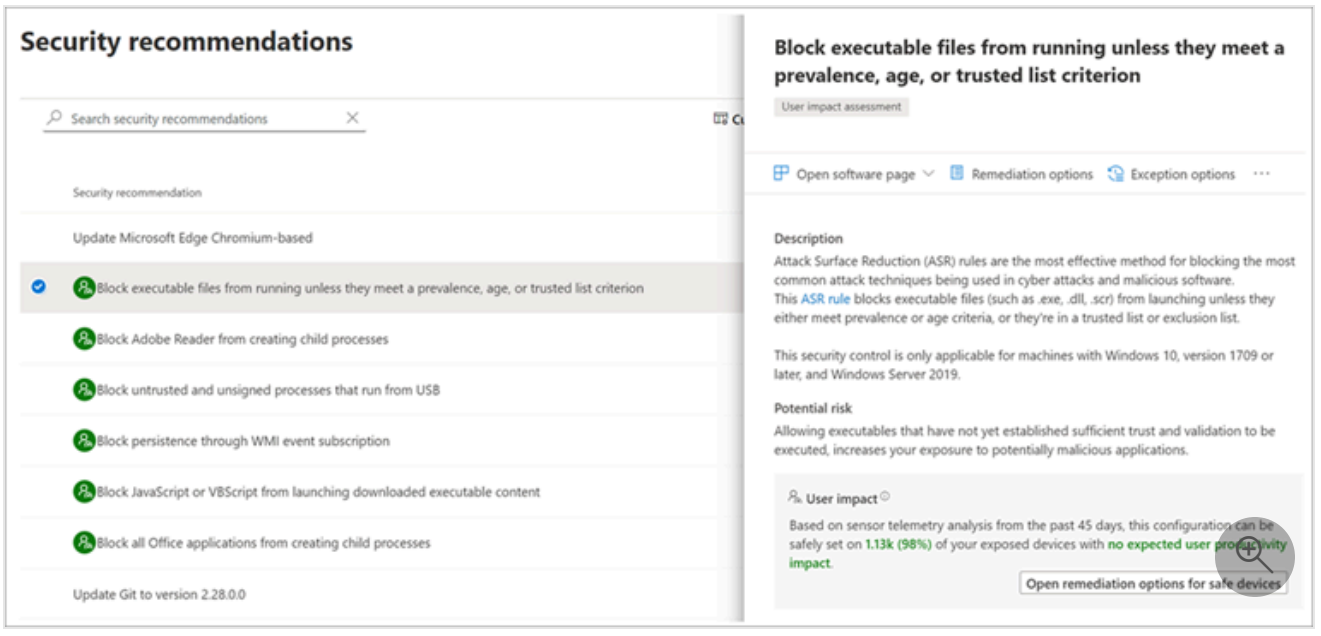
Such software behaviors are sometimes seen in legitimate applications. However, these behaviors are often considered risky because they're commonly abused by attackers through malware. Attack surface reduction rules can constrain software-based risky behaviors and help keep your organization safe.

For a sequential, end-to-end process of how to manage attack surface reduction rules, see:

- Attack surface reduction rules deployment overview
- Plan attack surface reduction rules deployment
- Test attack surface reduction rules
- Enable attack surface reduction rules
- Operationalize attack surface reduction rules

Assess rules before deployment

You can assess how an attack surface reduction rule might affect your network by opening the security recommendation for that rule in Microsoft Defender Vulnerability Management.



In the recommendation details pane, check for user impact to determine what percentage of your devices can accept a new policy enabling the rule in blocking mode without adversely affecting productivity.

See Requirements in the "Enable attack surface reduction rules" article for information about supported operating systems and other requirement information.

Audit mode for evaluation

Audit mode

Use audit mode to evaluate how attack surface reduction rules would affect your organization if enabled. Run all rules in audit mode first so you can understand how they affect your line-of-business applications. Many line-of-business applications are written with limited security concerns, and they might perform tasks in ways that seem similar to malware.

Exclusions

By monitoring audit data and adding exclusions for necessary applications, you can deploy attack surface reduction rules without reducing productivity.

Per-rule exclusions

For information about configuring per-rule exclusions, see the section titled **Configure attack surface reduction rules per-rule exclusions** in the article Test attack surface reduction rules.

Warn mode for users

(**NEW**!) Prior to warn mode capabilities, attack surface reduction rules that are enabled could be set to either audit mode or block mode. With the new warn mode, whenever content is blocked by an attack surface reduction rule, users see a dialog box that indicates the content is blocked. The dialog box also offers the user an option to unblock the content. The user can then retry their action, and the operation completes. When a user unblocks content, the content remains unblocked for 24 hours, and then blocking resumes.

Warn mode helps your organization have attack surface reduction rules in place without preventing users from accessing the content they need to perform their tasks.

Requirements for warn mode to work

Warn mode is supported on devices running the following versions of Windows:

- Windows 10, version 1809 or later
- Windows 11
- Windows Server, version 1809 or later

Microsoft Defender Antivirus must be running with real-time protection in Active mode.

Also, make sure Microsoft Defender Antivirus and antimalware updates are installed.

- Minimum platform release requirement: `4.18.2008.9`
- Minimum engine release requirement: `1.1.17400.5`

For more information and to get your updates, see Update for Microsoft Defender antimalware platform .

Cases where warn mode isn't supported

Warn mode isn't supported for three attack surface reduction rules when you configure them in Microsoft Intune. (If you use Group Policy to configure your attack surface reduction rules, warn mode is supported.) The three rules that don't support warn mode when you configure them in Microsoft Intune are as follows:

- Block JavaScript or VBScript from launching downloaded executable content (GUID `d3e037e1-3eb8-44c8-a917-57927947596d`)
- Block persistence through WMI event subscription (GUID `e6db77e5-3df2-4cf1-b95a-636979351e5b`)
- Use advanced protection against ransomware (GUID `c1db55ab-c21a-4637-bb3f-a12568109d35`)

Also, warn mode isn't supported on devices running older versions of Windows. In those cases, attack surface reduction rules that are configured to run in warn mode runs in block mode.

Notifications and alerts

Whenever an attack surface reduction rule is triggered, a notification is displayed on the device. You can customize the notification with your company details and contact information.

Also, when certain attack surface reduction rules are triggered, alerts are generated.

Notifications and any alerts that are generated can be viewed in the Microsoft Defender portal.

For specific details about notification and alert functionality, see: Per rule alert and notification details, in the article **Attack surface reduction rules reference**.

Advanced hunting and attack surface reduction events

You can use advanced hunting to view attack surface reduction events. To streamline the volume of incoming data, only unique processes for each hour are viewable with advanced hunting. The time of an attack surface reduction event is the first time that event is seen within the hour.

For example, suppose that an attack surface reduction event occurs on 10 devices during the 2:00 PM hour. Suppose that the first event occurred at 2:15, and the last at 2:45. With advanced hunting, you see one instance of that event (even though it actually occurred on 10 devices), and its timestamp will be 2:15 PM.

For more information about advanced hunting, see Proactively hunt for threats with advanced hunting.

Attack surface reduction features across Windows versions

You can set attack surface reduction rules for devices that are running any of the following editions and versions of Windows:

- Windows 10 Pro, version 1709 or later
- Windows 10 Enterprise, version 1709 or later
- Windows Server, version 1803 (Semi-Annual Channel) or later
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

> **Note**
>
> Windows Server 2016 and Windows Server 2012 R2 must be onboarded using the instructions in **Onboard Windows servers** for this feature to work.

Although attack surface reduction rules don't require a Windows E5 license, if you have Windows E5, you get advanced management capabilities. The advanced capabilities - available only in Windows E5 - include:

- The monitoring, analytics, and workflows available in Defender for Endpoint
- The reporting and configuration capabilities in Microsoft Defender XDR.

These advanced capabilities aren't available with a Windows Professional or Windows E3 license. However, if you do have those licenses, you can use Event Viewer and Microsoft Defender Antivirus logs to review your attack surface reduction rule events.

Review attack surface reduction events in the Microsoft Defender portal

Defender for Endpoint provides detailed reporting for events and blocks as part of alert investigation scenarios.

You can query Defender for Endpoint data in Microsoft Defender XDR by using advanced hunting.

Here's an example query:

Kusto Copy

```
DeviceEvents
| where ActionType startswith 'Asr'
```

Review attack surface reduction events in Windows Event Viewer

You can review the Windows event log to view events generated by attack surface reduction rules:

1. Download the Evaluation Package and extract the file *cfa-events.xml* to an easily accessible location on the device.
2. Enter the words, *Event Viewer*, into the Start menu to open the Windows Event Viewer.
3. Under **Actions**, select **Import custom view...**.
4. Select the file *cfa-events.xml* from where it was extracted. Alternatively, copy the XML directly.
5. Select **OK**.

You can create a custom view that filters events to only show the following events, all of which are related to controlled folder access:

Expand table

Event ID	Description
5007	Event when settings are changed
1121	Event when rule fires in Block-mode
1122	Event when rule fires in Audit-mode

The "engine version" listed for attack surface reduction events in the event log, is generated by Defender for Endpoint, not by the operating system. Defender for Endpoint is integrated with Windows 10 and Windows 11, so this feature works on all devices with Windows 10 or Windows 11 installed.

See also

- Attack surface reduction rules deployment overview
- Plan attack surface reduction rules deployment

- Test attack surface reduction rules
- Enable attack surface reduction rules
- Operationalize attack surface reduction rules
- Attack surface reduction rules report
- Exclusions for Microsoft Defender for Endpoint and Microsoft Defender Antivirus

Tip

If you're looking for Antivirus related information for other platforms, see:

- Set preferences for Microsoft Defender for Endpoint on macOS
- Microsoft Defender for Endpoint on Mac
- macOS Antivirus policy settings for Microsoft Defender Antivirus for Intune
- Set preferences for Microsoft Defender for Endpoint on Linux
- Microsoft Defender for Endpoint on Linux
- Configure Defender for Endpoint on Android features
- Configure Microsoft Defender for Endpoint on iOS features

Tip

Do you want to learn more? Engage with the Microsoft Security community in our Tech Community: Microsoft Defender for Endpoint Tech Community.

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Training

Module
Implement Windows security enhancements with Microsoft Defender for Endpoint - Training
Implement Windows security enhancements with Microsoft Defender for Endpoint

Certification
Microsoft Certified: Security Operations Analyst Associate - Certifications
Investigate, search for, and mitigate threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender.