



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking “Manage Cookies” at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies



Microsoft

Microsoft Security

Solutions

Products

Services

Partners

|



All Microsoft



Light



Dark

[Blog home](#) / Endpoint security

Search the blog



[News](#) [Endpoint security](#) [Microsoft Defender](#)

9 min read

Windows Defender Exploit Guard: Reduce the attack surface against next-generation malware

By [Microsoft Threat Intelligence](#)

October 23, 2017



Microsoft Defender for Endpoint

Windows Defender Exploit Guard is a new set of intrusion prevention capabilities that ships with the [Windows 10 Fall Creators Update](#). The four components of Windows Defender Exploit Guard are designed to lock down the device against a wide variety of attack vectors and block behaviors commonly used in malware attacks, while enabling enterprises to balance their security risk and productivity requirements.

Traditional antivirus technologies are an integral aspect of the endpoint security stack through the identification and removal of malicious executables using a combination of cloud-based machine learning and heuristics. Despite advances in antivirus detection capabilities, attackers are continuously adapting and have been expanding their arsenal of tricks and techniques to compromise endpoints, steal credentials, and execute ransomware attacks without ever needing to write anything to disk. This emerging trend of fileless attacks, which compose over 50% of all threats, are extremely dangerous, constantly changing, and designed to evade traditional AV. Fileless attacks have two types: those that use non-traditional executable files (e.g., documents with active content in them), and those that exploit vulnerabilities.

Windows Defender Exploit Guard utilizes the capabilities of the Microsoft [Intelligent Security Graph \(ISG\)](#) and the world-class security research team at Microsoft to identify active exploits and common behaviors to stop these types of attacks at various stages of the kill chain. Although the underlying vulnerability being exploited varies, the delivery mechanism differs, and the payload changes, there is a core set of behaviors and vectors that many different attacks adhere to. By correlating streams of events to various malicious behaviors with the ISG, Windows Defender Exploit Guard provides the capability and controls needed to handle these types of emerging threats.

The four components of Windows Defender Exploit Guard are:

- [Attack Surface Reduction \(ASR\)](#): A set of controls that enterprises can enable to prevent malware from getting on the machine by blocking Office-, script-, and email-based threats
- [Network protection](#): Protects the endpoint against web-based threats by blocking any outbound process on the device to untrusted hosts/IP through Windows Defender SmartScreen

- **[Controlled folder access](#)**: Protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders
- **[Exploit protection](#)**: A set of exploit mitigations (replacing EMET) that can be easily configured to protect your system and applications

Attack Surface Reduction (ASR): Intelligence to control the surface area of the device

Email and Office applications are generally thought of as keystones of enterprise productivity, yet they are the most common vector for attacks and can cause nightmares for security administrators. Both Office and email serve as simple and easy ways to distribute mechanism for bad actors to kick off malware and fileless attacks. Although Office macros and scripts have many productive use cases, malicious actors can use them to directly perform exploits that operate entirely in memory and are often undetectable by traditional AV techniques. All it takes is for a single user to enable macros on a legitimate-looking Office file, or to open an email attachment that executes a malicious PowerShell script, to compromise a machine.

Attack Surface Reduction provides enterprises with a set of built-in intelligence that can block the underlying behaviors used by these malicious documents to execute without hindering productive scenarios. By blocking malicious behaviors independent of what the threat or exploit is, ASR can protect enterprises from never before seen zero-day attacks like the recently discovered [CVE-2017-8759](#), [CVE-2017-11292](#), and [CVE-2017-11826](#).

The different behaviors ASR provides coverage for in Fall Creators Updated are split among [Office, scripts, and email](#).

For Office apps, ASR can:

- Block Office apps from creating executable content
- Block Office apps from launching child process
- Block Office apps from injecting into process
- Block Win32 imports from macro code in Office
- Block obfuscated macro code

Although malicious Office macros are oftentimes responsible for utilizing techniques like injection and launching of executables, ASR can also protect end-users from emerging exploits like [DDEDownloader](#), which has been recently gaining in popularity. This exploit uses the Dynamic Data Exchange (DDE) popup in Office Documents to run a PowerShell downloader; however, in doing so, it launches a child process that the corresponding child process rule blocks.

(Note: To learn more about security settings that ensure Microsoft Office applications securely open documents with DDE fields, read [Microsoft Security Advisory 4053440](#).)

For script, ASR can:

- Block malicious JavaScript, VBScript, and PowerShell codes that have been obfuscated
- Block JavaScript and VBScript from executing payload downloaded from internet

To highlight the intelligence behind ASR, we can look at how it can address obfuscated code as an example; in this case, there is a machine learning model powering our obfuscation detection capabilities that gets retrained multiple times per week in our cloud protection service. The model is updated on client, where it interfaces with [Antimalware Scan Interface \(AMSI\)](#) to make a determination on whether or not a script has been obfuscated for malicious purposes. When a high-confidence match occurs, any attempt made to access the script is blocked.

For email, ASR can:

- Block execution of executable content dropped from email (webmail/mail-client)

Enterprise administrators can set policies on their corporate email (e.g., Office 365) to limit the files that can be delivered to end user inboxes. However, they don’t have control over the files that are delivered via personal email on company devices. Given the increase in spear-phishing, employees’ personal emails are also targeted and need to be protected. ASR enables enterprise administrators to apply file policies on personal email for both webmail & mail-clients on company devices.

For any line of business applications running within your enterprise, there is the capability to customize file and folder based exclusions if your applications include unusual behaviors that may be impacted by ASR detection.

Attack Surface Reduction exceptions

Files and folder to exclude from attack surface reduction rules ⓘ

Files and folders ⓘ

Examples: C:\Path, %ProgramFiles%\Path\Filename.exe

Add

ASR has a dependency on [Windows Defender Antivirus](#) being the primary AV on the device and its [real-time protection](#) feature must be enabled. The Windows 10 Security [baseline](#) recommends enabling most of the rules in Block Mode to protect your devices from these threat vectors.

Network protection: Blocking outbound connection

The internet is home to a swath of malicious websites that are designed to lure and trick users. They use phishing, deceptive ads, tech scams, social engineering, and other means as part of their campaigns. For some attacks, they seek to acquire information or get immediate financial payout, while others may attempt to install malware on the machine. Oftentimes malware will attempt to connect with a command-and-control server (C&C) to seek further instructions and deliver additional malicious payloads, such that the attacker can spread to additional machines on the network.

Windows Defender SmartScreen protects Microsoft Edge from socially engineered malware, phishing, and other web-based threats through the power of the Intelligent Security Graph (ISG). This has made Microsoft Edge one of the most secure browsers out there, outperforming Chrome and Firefox in NSS Lab’s recent [test results for phishing protection between August 23 and September 12, 2017](#).

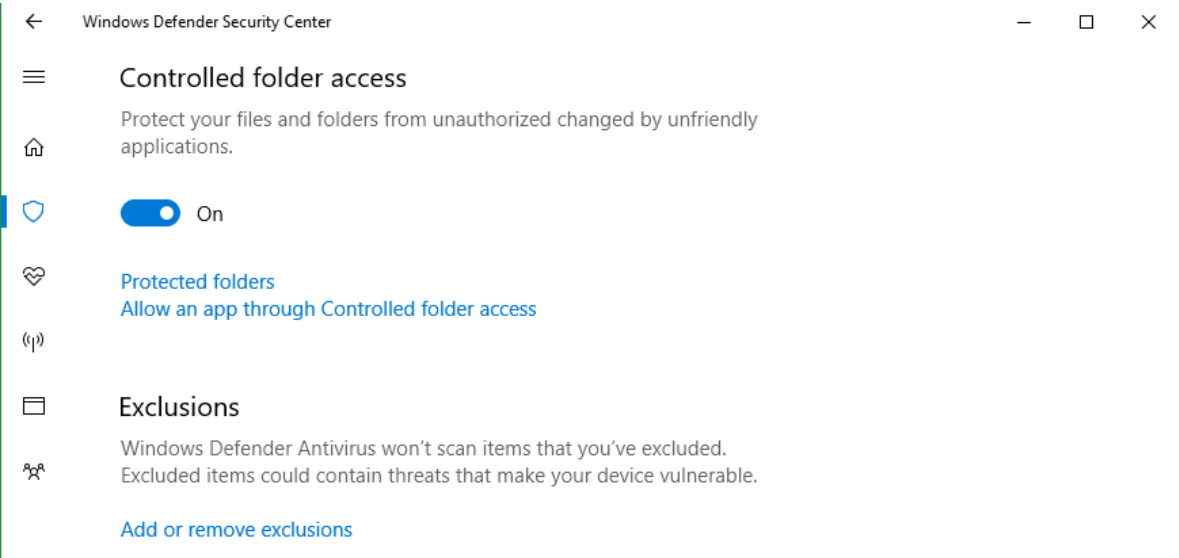
Windows Defender Exploit Guard’s network protection capability utilizes this same intelligence from ISG to vet, and if necessary block, all outbound connections before they are made. This brings the same level of protection that we previously just had for Microsoft Edge across the entire system and network stack.

By integrating a new network filtering driver into the kernel, the network protection capability can evaluate and block outbound network traffic based on ISG’s hostname and IP address-related reputation intelligence. With a combination of cloud lookups and performant caching to perform these reputation checks, the network protection capability can render web-based malware that depends on a communication channel inoperable.

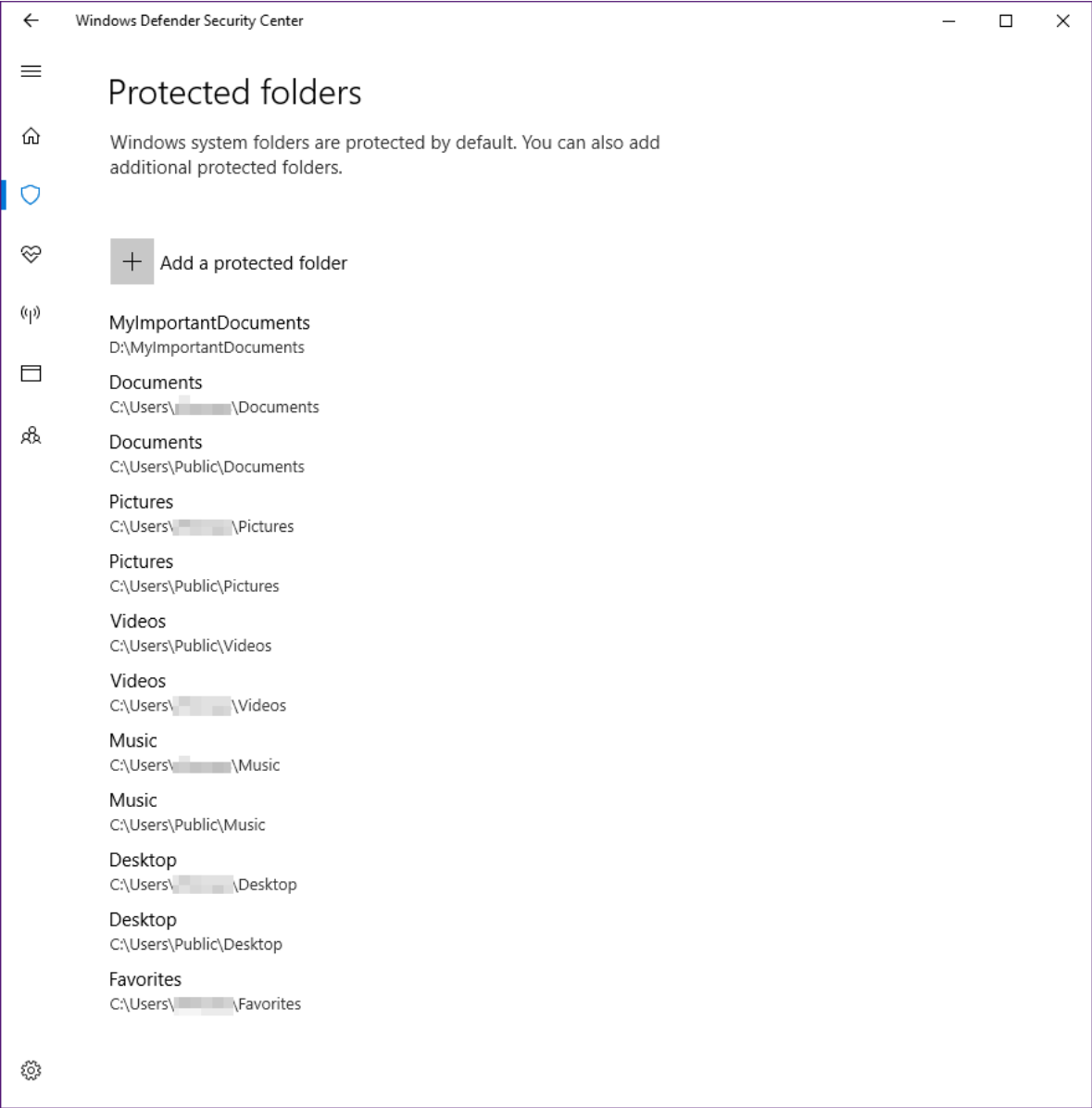
Regardless if the outbound call is to phishing, socially engineered malware, or a C&C website, or if the call originates from a browser or a background process, network protection can intercept and kill the connection. These filtering capabilities can also augment and work in concert with similar protection capabilities from others security solutions, browsers, etc.

Controlled folder access

Encryption of files by ransomware and other unauthorized apps means losing control of your data: documents, precious photos and videos, and other important files. For enterprises and small businesses, losing access to files can mean disrupted operations. [Controlled folder access](#) protects files by locking down critical folders, allowing only authorized apps to access files. Unauthorized apps, including malicious and suspicious executable files, DLLs, scripts, and others will be denied access even when they are running with the user’s or administrator’s privilege, which malware is often be able to secure.



By default, Controlled folder access protects common folders where documents and other important data are stored, but it’s also flexible. You can add additional folders to protect, including those on other drives. You can also allow apps that you trust to access protected folders, so if you’re using unique or custom app, your normal everyday productivity will be not affected.



When enabled, controlled folder access blocks unauthorized access and notifies the user of any attempt by unauthorized apps to access or modify files in protected folders. It delivers this protection in real-time.

Exploit Protection

Windows Defender Exploit Guard’s exploit protection represents the suite of vulnerability mitigation and hardening techniques that are built directly into Windows 10. As you install the Fall Creators Update, the appropriate mitigation settings will already be configured and applied on the machine.

Rest In Peace (RIP) EMET

Users of the Enhanced Mitigation Experience Toolkit (EMET) will notice that it was automatically uninstalled from your machine during the upgrade. This is because WDEG includes the best of EMET built directly into Windows 10, so it’s now just part of the platform. You can the find previous user experiences for configuring EMET vulnerability mitigation capabilities in Windows Defender Security Center. For more information, read [Moving Beyond Emet II – Windows-Defender-Exploit-Guard](#).

Figure shows using the Windows Security Center Exploit Protection control to enable mitigation Address Filtering (EAF) to unpatched application Word 2007

It is important to note that Exploit Guard’s exploit protection accepts a different format for the mitigation configuration than EMET did. To make the process of migrating to Exploit Protection and Windows Defender Exploit Guard easier, there is a PowerShell module that converts EMET XML settings files into Windows 10 mitigation policies for Exploit Guard. This PowerShell module also provides an additional interface for Windows Defender Security Center to configure its mitigation settings.

More information about this PowerShell module, and details on the EMET features relative to security in Windows 10 can be found in the topic [Understanding Windows 10 in relation to the Enhanced Mitigation Experience Toolkit](#). For more details on Windows 10’s threat mitigations, please refer to our [Windows 10 Threat Mitigations](#). Finally, the Windows 10 Security [baseline](#) provides a recommended Exploit Protection XML to apply.

Windows Defender Exploit Guard manageability

All the Windows Defender Exploit Guard components are manageable by Group Policy (GP), System Center Configuration Manager (SCCM), and Mobile Device Management (MDM) such as Microsoft Intune.

All components support running in both Audit and Block modes. When Block mode is enabled and a corresponding malicious behavior is observed, Windows Defender Exploit Guard blocks the event from occurring in real-time. Block events for Attack Surface Reduction, Controlled folder access and Network Protection surface a

notification toast to the endpoint in real-time as well as an event log, and can be centrally viewed by security operations personnel in the Windows Defender Advanced Threat Protection ([Windows Defender ATP](#)) console. Instead of actually blocking the behavior, Audit Mode detects if an event would have occurred and surfaces that information to the event log and WD ATP console. This enables enterprises to evaluate how a rule or feature within Windows Defender Exploit Guard will perform in their enterprise and determine if there are exclusions that are needed to setup. Additionally, Audit mode provides an immense amount of optics into what kinds of behaviors are going on across the enterprise, providing valuable information to security admins to determine if a rule needs to be moved to block mode.

Windows Defender Advanced Threat Protection

[Windows Defender ATP](#) provides a single pane of glass experience for managing and viewing all the security feeds and events happening on managed endpoints across the enterprise. With Windows Defender ATP, the entire process tree execution can be seen for Exploit Guard events, making it extremely easy to determine what happened, such that a proper response can be executed. In the figure below you can see an example of how a malicious document in Word was used to drop an executable, which was then blocked when it attempted to access the C:*Demo* folder.

Controlled folder access blocking sample ransomware

Network Protection blocking phishing test via Chrome browser

Exploit Guard is also surfaced in the Security Analytics dashboard of the Windows Defender ATP console, enabling enterprises to view how the feature is configured across their device and to drive compliance with recommendations based on best practice security configurations.

In the end, Windows Defender Exploit Guard is one of the most important new defenses that we’ve added to Windows 10 in the Fall Creators Update. In many ways, it completes our stack for preventive protection. Organizations that deploy it alongside Windows Defender Antivirus will find that they have a highly effective and differentiated solution for addressing modern fileless attacks and host intrusion. We recommend you evaluate it at the earliest opportunity and we look forward to your feedback.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, [sign up for a free trial](#).

Misha Kutsovsky (@mkutsovsky)

Program Manager, Windows Active Defense

Learn more about Windows 10 Fall Creators Update

[Microsoft 365 Security and Management Features Available in Fall Creators Update](#)

[Windows Defender Exploit Guard: Reduce the attack surface against next-generation malware](#)

[Stopping ransomware where it counts: Protecting your data with Controlled folder access](#)

[Making Microsoft Edge the most secure browser with Windows Defender Application Guard](#)

[Introducing Windows Defender Application Control](#)

[Hardening the system and maintaining integrity with Windows Defender System Guard](#)

[Move away from passwords, deploy Windows Hello. Today!](#)

[What’s new in Windows Defender ATP Fall Creators Update](#)

[Antivirus evolved](#)

Talk to us

Questions, concerns, or insights on this story? Join discussions at the [Microsoft community](#) and [Windows Defender Security Intelligence](#).

Follow us on Twitter [@WDSecurity](#) and Facebook [Windows Defender Security Intelligence](#).

Related Posts

[Research](#) [Threat intelligence](#) [Cloud threats](#) ·

Mar 17, 2020 · 8 min read

Secured-core PCs: A brief showcase of chip-to-cloud security against kernel attacks >

Secured-core PCs combine virtualization, operating system, and hardware and firmware protection. Along with Microsoft Defender ATP, Secured-core PCs provide end-to-end protection against advanced attacks that leverage driver vulnerabilities to gain kernel privileges.

[News](#) [Device management](#) · Oct 21, 2019 · 5 min read

Microsoft and partners design new device security requirements to protect against targeted firmware attacks >

We’ve been working with partners to design what we call Secured-core PCs, devices that meet a specific set of device requirements that apply the security best practices of isolation and minimal trust to the firmware layer.

[News](#) [Threat intelligence](#) [Supply chain attacks](#) ·

Feb 3, 2020 · 4 min read

Guarding against supply chain attacks—Part 2: Hardware risks >

Part 2 examines the hardware supply chain, its vulnerabilities, how you can protect yourself, and Microsoft’s role in reducing hardware-based attacks.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social



What's new

- Surface Pro
- Surface Laptop
- Surface Laptop Studio 2
- Surface Laptop Go 3
- Microsoft Copilot
- AI in Windows
- Explore Microsoft products
- Windows 11 apps

Business

- Microsoft Cloud
- Microsoft Security
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Microsoft 365 Copilot
- Small Business

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Certified Refurbished
- Microsoft Store Promise
- Flexible Payments

Developer & IT


- Azure
- Developer Center
- Documentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Visual Studio


Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education
- How to buy for your school
- Educator training and development
- Deals for students and parents
- Azure for students

Company

- Careers
- About Microsoft
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility
- Sustainability

 English (United States)

 Your Privacy Choices

Consumer Health Privacy

Sitemap

Contact Microsoft

Privacy

Manage cookies

Terms of use

Trademarks

Safety & eco

Recycling

About our ads

© Microsoft 2024