moving-beyond-emet-ii-windows-defender-exploit-guard

By swiat

Published: 2017-08-09 · Archived: 2026-04-05 22:01:00 UTC

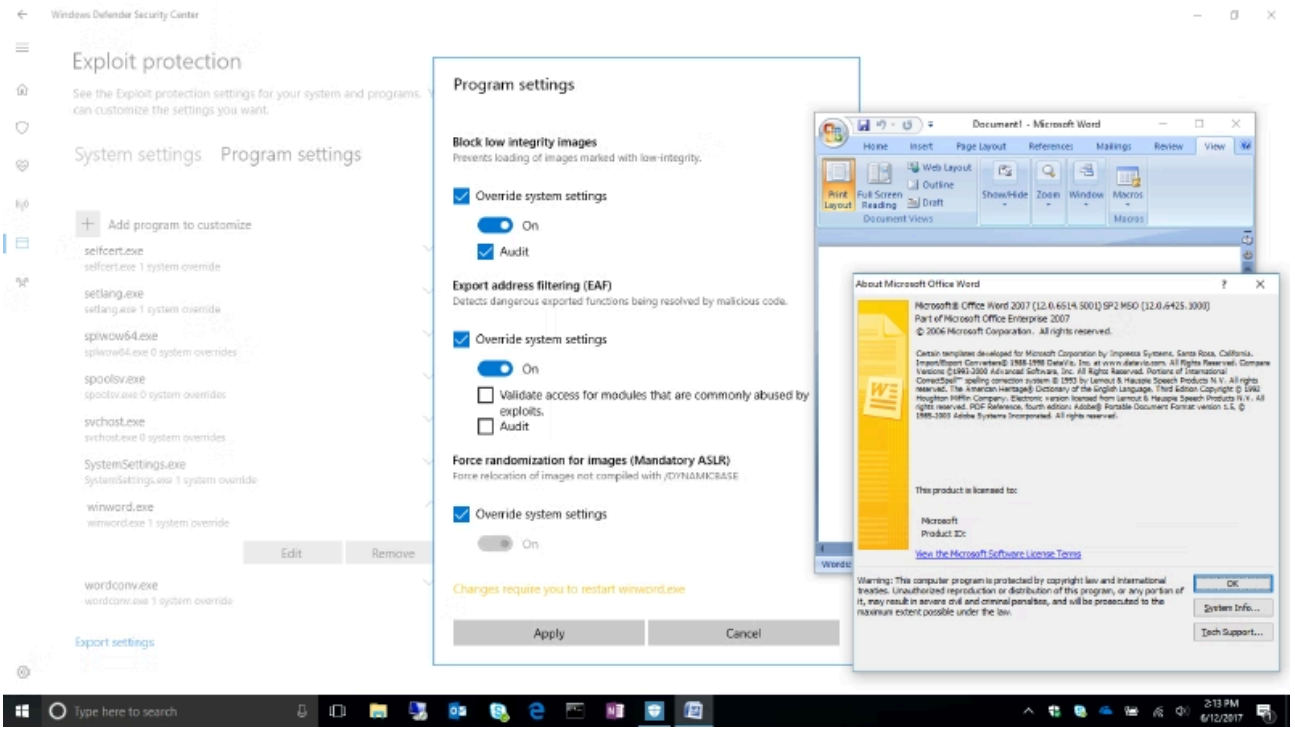
/ By / August 9, 2017

Since we last wrote about the future of EMET and how it relates to Windows 10 back in November 2016 (see Moving Beyond EMET), we have received lots of invaluable feedback from EMET customers and enthusiasts regarding the upcoming EMET end of life. Based on that feedback, we are excited to share significant new exploit protection and threat mitigation improvements coming with the Windows 10 Fall Creators Update!

We recently introduced Windows Defender Exploit Guard (WDEG) which will complete our journey to incorporate all of the security benefits of EMET directly into Windows. This effort was significantly influenced by two insights that came up most frequently in our survey data, customer support calls, and conversations with EMET stakeholders and security enthusiasts. More than anything else, our customers have expressed that they want (1) a user-friendly UI for configuring mitigation settings and (2) a way to protect their legacy apps on Windows 10.

As such, with the Windows 10 Fall Creators Update, you can now audit, configure, and manage Windows system and application exploit mitigations right from the Windows Defender Security Center (WDSC). You do not need to deploy or install Windows Defender Antivirus or any other additional software to take advantage of these settings, and WDEG will be available on every Windows 10 PC running the Fall Creators Update. Windows Insiders can start trying out WDEG today following these simple steps:

1. Right-click the WDSC icon in the taskbar notification area and click **Open** , or search the Start menu for **Windows Defender Security Center**.
2. From the Windows Defender Security Center, click on **App & browser control**.
3. Scroll to the bottom of the resulting screen to find **Exploit protection settings**.



In addition to the new user-friendly interface in WDSC, we have added the same legacy app protections that our EMET customers have come to expect, thus achieving parity between Windows 10 mitigation support and all of the mitigation features provided by EMET. While we strongly recommend the use of Control Flow Guard (CFG) to provide the strongest protections available, we understand that many enterprises depend on legacy apps to run their business operations, many of which may never get recompiled with CFG. These users can now use Exploit Guard to help secure such apps on modern systems by configuring control flow protections for legacy apps, similar to those offered by EMET but built-in directly to Windows 10 as part of WDEG. These legacy app control flow protections include:

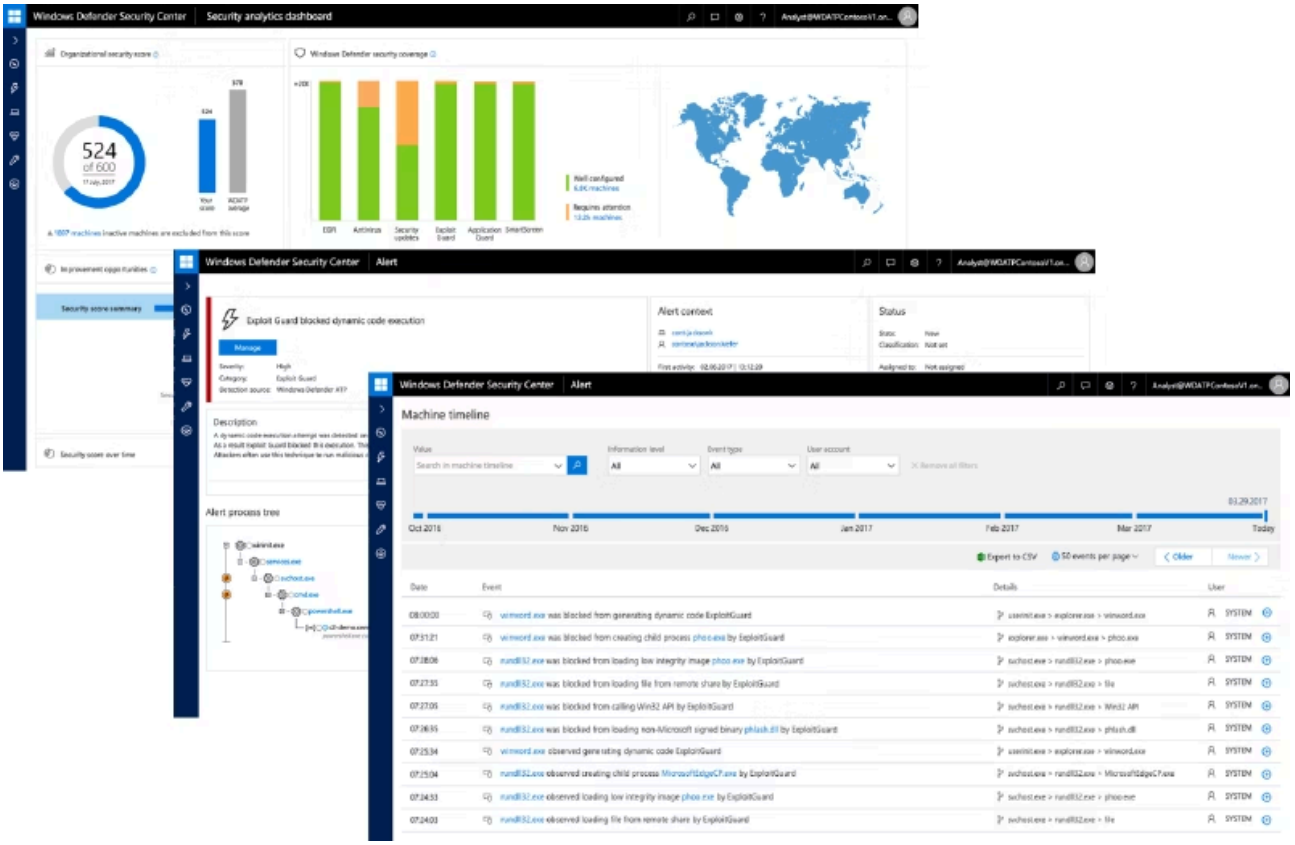
- Export Address Filtering (EAF)
- Import Address Filtering (IAF)
- Validate API Invocation (CallerCheck)
- Simulate Execution (SimExec)
- Validate Stack Integrity (StackPivot)

Another common ask from our customers was for auditing support. To facilitate easy deployment and usage of mitigations without the burden of application compatibility side effects, we have introduced audit mode support for both EMET legacy app mitigations as well as existing native mitigations provided by Windows.

Although EMET shipped with a set of recommended configuration settings, we know that many EMET customers customized the policy to suit the specific needs of their business. To help facilitate the migration to Windows Defender Exploit Guard, we have added a new PowerShell module that converts EMET XML settings files into Windows 10 mitigation policies for WDEG. More information about this PowerShell module, and about how EMET features relate to security features in Windows 10, can be found in the topic Understanding Windows 10 in relation to the Enhanced Mitigation Experience Toolkit.

NOTE: To prevent possible compatibility, performance, and stability issues, Windows will automatically block or remove EMET on Windows 10 systems starting with the Windows 10 Fall Creators Update.

Lastly, Windows Defender Exploit Guard includes much more than the features integrated from EMET, and we look forward to discussing host intrusion prevention capabilities and other WDEG components in a future blog post. In terms of upcoming features, WDEG will soon be fully integrated with Windows Defender ATP (WDATP) to provide a single-pane-of-glass view across the Windows security stack. Violations of configured WDEG mitigations will be logged by WDATP and used as additional signals for more advanced exploit detection.



For more details on Windows 10's threat mitigations, please refer to our Windows 10 Threat Mitigations documentation on Microsoft Docs.

- Nate Nunez, OS Security

Source: https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/