Security baseline (FINAL) for Windows 10 and Windows Server, version 20H2

We are pleased to announce the final release of the for Windows 10 and Windows Server, version 20H2 (a.k.a. October 2020 Update) security baseline package!

Please download the content from the Microsoft Security Compliance Toolkit, test the recommended configurations, and customize and implement as appropriate. If you have questions or issues, please let us know via the Security Baseline Community.

This Windows 10 feature update brings very few new policy settings, which we list in the accompanying documentation. At this point, no new 20H2 policy settings meet the criteria for inclusion in the security baseline, but there are a few policies we are going to be making changes to, which we highlight below along with our recommendations.

Tip: If you read the Draft release, we will save you another read. There are no changes since the draft to the actual settings. There were two small changes to the package though; the Baseline-LocalInstall.ps1 script has a change to error handling (thanks to a community member's suggestion) and second, we neglected to include the custom ADMX/L files in the GP Reports so they showed up as additional registry keys which is now fixed also.

Block at first sight

We started the journey for cloud protection several years ago. Based on our analysis of the security value versus the cost of implementation, we feel it's time to add Microsoft Defender Antivirus' Block At First Sight (BAFS) feature to the security baseline. BAFS was first introduced in Windows 10, version 1607 and allows new malware to be detected and blocked within seconds by leveraging various machine learning techniques and the power of our cloud.

BAFS currently requires 6 settings to be configured. Our baseline already sets 2 of them, *Join Microsoft MAPS* and *Send file sample when further analysis is required*. We are now recommending the addition of the following settings to enable BAFS:

Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MAPS\Configure the 'Block at first sight' feature set to **Enabled**

Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-time Protection\Scan all downloaded files and attachments set to **Enabled**

Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-time Protection\Turn off real-time protection set to **Disabled**

Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MPEngine\Select cloud protection level set to **High blocking level**

These new settings have been added to the *MSFT Windows 10 20H2 and Server 20H2 – Defender Antivirus* group policy.

Additional details on BAFS can be found here.

Attack Surface Reduction Rules

We routinely evaluate our Attack Surface Reduction configuration, and based on telemetry and customer feedback we are now recommending configuring two additional Attack Surface Reduction controls: *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules*: *Use advanced protection against ransomware* and *Block persistence through WMI event subscription*.

Introduced in Windows 10, version 1709 the *Use advanced protection against ransomware* rule will scan any executable files and determine, using advanced cloud analytics, if the file looks malicious . If so, it will be blocked unless that file is added to an exclusion list. This rule does have a cloud dependency, so you must have *Join Microsoft MAPS* also configured (which is already part of the security baseline).

Block persistence through WMI event subscription is a rule that was released in Windows 10, version 1903. This rule attempts to ensure WMI persistence is not achieved - a common technique adversaries use to evade detection. Unlike many of the other ASR rules, this rule does not allow any sort of exclusions since it is solely based on the WMI repository.

A friendly reminder that the security baselines set all ASR rules to block mode. We recommend first configuring them to audit mode, then testing to ensure you understand the impacts these rules will have in your environment, and then configuring them to block mode. Microsoft Defender for Endpoints (formally Microsoft Defender Advanced Threat Protection, MDATP) will greatly enhance the experience of testing, deployment, and operation of ASR rules. We would encourage you to look at evaluating, monitoring and customizing links to better prepare your environment.

These new settings have been added to the *MSFT Windows 10 20H2 and Server 20H2 – Defender Antivirus* group policy.

UEFI MAT

You might recall in the draft release of our security baseline for Windows 10, version 1809 we enabled UEFI Memory Attributes Tables, but based on your feedback we removed that recommendation from the final version. After further testing and discussions, we are recommending that you enable *Computer Configuration\Administrative Templates\System\Device Guard\Turn on Virtualization Based Security\Require UEFI Memory Attributes Table*.

Microsoft Edge

Starting with Windows 10, version 20H2 the new Microsoft Edge (based on Chromium) is now installed as part of the operating system. Please ensure you are applying the security baseline for Microsoft Edge to your Windows 10, version 20H2 machines. We have gotten questions about including it on the Windows security baseline, but since Microsoft Edge is a cross platform product and has a different release cadence, we are going to keep it a separate security baseline.

As always, please let us know your thoughts by commenting on this post.