Windows 11 Security baseline

We are pleased to announce the release of the security baseline package for Windows 11!

Please download the content from the [Microsoft Security Compliance Toolkit](#), test the recommended configurations, and customize / implement as appropriate.

Two new settings have been added for this release (which were also added to the Windows Server 2022 release), a new Microsoft Defender Antivirus setting, and a custom setting for printer driver installation restrictions. Additionally, all Microsoft Edge Legacy settings have been removed.

Script Scanning

Script scanning was a parity gap we had between Group Policy and MDM. Since this gap is now closed we are enforcing the enablement of script scanning (*Windows Components\Microsoft Defender Antivirus\Real-time Protection\Turn on script-scanning*).

Restrict Driver Installations

In July a [Knowledge Base article](#) and subsequent patch was released for CVE-2021-34527, more commonly known as "PrintNightmare". We have added a new setting to the MS Security Guide custom administrative template for SecGuide.admx/l (*Administrative Templates\MS Security Guide\Limits print driver installation to Administrators*) and enforced the enablement.

Microsoft Edge Legacy

Microsoft Edge Legacy (EdgeHTML-based) reached end of support on March 9, 2021 and is not part of Windows 11. Therefore, the settings that supported it have been removed from the baseline. Going forward, please use the new Microsoft Edge (Chromium-based) baseline, which is on a separate release cadence and available as part of the [Microsoft Security Compliance Toolkit](#).

Tamper Protection

While you are enabling the Microsoft Security Baseline for Windows 11 (and/or Windows 10, and/or Windows Server 2022/2019/2016), make sure to enable Microsoft Defender for Endpoint's "[Tamper Protection](#)" to add a layer of protection against Human Operated Ransomware.

Please let us know your thoughts by commenting on this post or via the [Security Baseline Community](#).