WEBROOT
an opentext company

FAQ | Webroot® Evasion Shield

What is Webroot Evasion Shield?

Webroot Evasion Shield adds new and additional protection against evasive Script and PowerShell attacks. This first release offers brand new patented Webroot technology to detect, block and remediate (by quarantining) malicious and evasive script attacks, whether they are file-based, fileless, obfuscated or encrypted. In addition, it prevents malicious behaviors from executing in PowerShell, JavaScript and VB Script files that are commonly used to launch evasive attacks.

How do I get Webroot Evasion Shield?

You need to do nothing. Webroot Evasion Shield is an integral part of your May 2020 console update and is now a new policy component of Webroot Business Endpoint Protection.

What do I need to do to use Webroot Evasion Shield?

Scripts are commonly used in many IT environments, so the Webroot Evasion Shield is turned off by default.

To activate Webroot Evasion Shield you will need to go into the Policies tab of your console and select the Script Remediation Policy – it works like any other policy. More details below.

What Policy Options do I have?

We have kept the policy process very simple.

» Off - Webroot Evasion Shield protection is off (default shipping policy).

» Detect and Report - Detection and reporting are made active so you can monitor the Scripts already running in an IT environment and decide whether to white or blacklist them using the report. This initial step ensures that legitimate scripts are not falsely prevented from executing

» Detect and Remediate – Means that the Webroot Evasion Shield is turned on any evasive malicious script activity is being prevented and the script quarantined, reported and any system changes auto-remediated.

What does the Webroot Evasion Shield cost?

While advanced features like the Webroot Evasion Shield are often charged for by others, we are not charging extra for Evasion Shield. It is now simply a part of your existing licensing arrangements and is included at no extra cost with your Webroot endpoint protection.

Using Evasion Shield

Evasion Shield detections include file-based and file-less threats that have been detected and reported according to policy settings. To remediate any of the threats listed, please check your policy settings. This remainder of this FAQs addresses some frequently asked questions regarding using Webroot Evasion Shield.

Will all of my devices now be protected from Evasion Shield Script threats?

To protect all of your devices you will need to visit the Endpoint Policies section of the Webroot management console to select an Endpoint Policy and turn the Evasion Shield Policy Setting from Off (Default setting) to either:

» **Detect and Report** – Threats will be detected, reported to the console and not quarantined

» **Detect and Remediate** – Threats will be detected, reported to the console and quarantined

IMPORTANT: You will also need to ensure that each device has upgraded to the latest Webroot Business Endpoint Protection agent version 9.0.28.00. Any other agent version before this will not fully support Evasion Shield Script Protection.

Can I see which of my devices have Evasion Shield Enabled and have encountered Evasion Shield Script detections?

There are two new On Demand reports accessible from the Reports Tab in the Webroot management console, the Evasion Shield Script Protection Status report and the Evasion Shield Script Detections report.

The Evasion Shield Script Protection Status report displays a count of all the devices that have the Evasion Shield in these statuses; Detect and Remediate, Detect and Report, Off and Unsupported. You can click the graph to display a full list of all the devices in each status category.

The Evasion Shield Script Detections report displays a list of all the devices that have had Evasion Shield script detections and the script file that was detected. You can click each script file for more information and whitelist that file if required.

What type of threats does evasion shield – Script Protection detect?

Evasion shield Script Protection will detect and block (according to policy settings) malicious script files including JS, VBS, PowerShell, wscript, cscript, macros, and more. This shield includes file-based scripts as well as file-less scripts which often evade other malware detection software. On Windows 10, there is enhanced protection for file-less scripts, obfuscated scripts, and other sophisticated script attacks.

I have a recurring file-less threat, how can I clean up my machine?

The Webroot Evasion Shield will detect and block (according to policy settings), file-based and file-less malicious scripts. For file-based scripts, the policy can be enabled to allow for remediation and thus the file will be quarantined and no longer able to run on the machines.

In the case of file-less scripts, there is no file to quarantine so the Webroot Evasion Shield will block the script execution but cannot remediate. If the file-less script is set to execute repeatedly, Webroot will detect and block each execution. If you need assistance removing a file-less infection from your machine, please reach out to Webroot support and our Advanced Malware Removal team will assist with machine cleanup to remediate.

Support can be contacted here:
https://www.webroot.com/us/en/business/support/contact

How can I whitelist a script that I wrote?

The Webroot Evasion Shield utilizes the file whitelist capability from the Webroot management console. Instructions on how to whitelist a script by file are here:

https://answers.webroot.com/Webroot/ukp.aspx?pid=12&app=vw&vw=1&login=1&solutionid=3105

Since scripts can have dynamic MD5s, the whitelisting is done by file/folder name in the Webroot management console. For instructions on how to whitelist a file/folder containing your script, go here:

https://answers.webroot.com/Webroot/ukp.aspx?pid=12&app=vw&vw=1&login=1&solutionid=3105

I use a lot of scripts in my environment, how can I test if Webroot will block any of them before enabling script protection?

To test your existing scripts:

1. Create (or modify) a policy with the Evasion Shield – Script Protection set to Detect and Report only.
2. Assign this policy to some devices where you will test.
3. Make sure that the policy is applied to the device. The device will obtain a new policy according to its existing poll interval. You can force a device to obtain an updated policy by running WSDaemon.exe –poll from the command line on a given device.
4. Run your scripts on the machine.
5. If any scripts are detected as malicious, they will be reported to the console and displayed on the "threats detected" tab of the console.
6. If no scripts are detected/displayed in the console, then your scripts are deemed as safe by Webroot and will not trigger any detections.
7. You can now change your policy to Detect and Remediate and safely protect your machines from malicious scripts without fear of interference with your scripts.

What results should I expect by using Webroot Evasion Shield Script protection??

Evasion techniques are growing in use and our internal and external testing shows much improved defenses with the new Webroot Evasion Shield activated. Our only reason for defaulting to off is to allow Administrators to ensure no legitimate Scripts are mistakenly blocked.