Blocker
AutoElevate Feature

Blocker

Protect your organization and combat malware and Living off the Land (LOTL) Attacks.

The Blocker feature in AutoElevate can block 200+ native Windows applications, binaries, and .dll files that are typically used as LOTL attack vectors.

The need for robust security measures has never been more critical. LOTL (aka Malware-Free) attacks have become a significant threat in today's digital landscape, making up for 75% of all attacks in 2023*. Bad actors infiltrate networks and wreak havoc using legitimate components of the Windows Operating System, which often escape detection by traditional Anti-Malware applications.

Blocker addresses this danger by curating a comprehensive list of attack vectors and allows you to choose which items to block from executing, rendering them useless to bad actors. With our Recommendation Engine and detailed application execution audit logs, you can easily define rules that allow these applications to operate as well as allow specific parent processes to run child applications or processes. With Blocker, you get:

Enhanced Security

Safeguard your organization against potential security breaches by blocking listed applications, binaries, and .dll files. These native Windows binaries are rarely used by end-users directly, so blocking them should have minimal impact on most typical business environments. However, blocking them will prevent malware from exploiting them against you. Our Recommendation Engine makes this quick and simple.

Easy Rule Management

With intuitive logs and a user-friendly interface, setting up rules to block specific processes becomes effortless. Easily create rules that allow specified parent processes to execute child processes when required (such as your RMM tool needing to run a script or an application calling an updater).

Minimized False Positives

Blocker's curated list focuses explicitly on known attack vectors helping to ensure minimal disruption to your legitimate applications and operations.

*CrowdStrike 2024 Global Threat Report

CyberFOX.com
sales@cyberfox.com

02.24

CyberFOX™