RevBits®

PRODUCT BRIEF

Endpoint Security

RevBits Endpoint Security System Hardening Detects and Prevents Zero-Day Exploits.

Today's expanded enterprise perimeter is comprised of potential technology flaws and backdoors that can be exploited by hackers. A key function within cybersecurity is the ability to enable system hardening to reduce attack surfaces.

IT and security teams enforce restrictive rules to protect the enterprise and its assets. This process is called system hardening. For example, there is no reason for an application, like Word, to spawn another application. There is a growing need for system hardening, as 99% of the time, these types of actions are caused by malware. System hardening enforces and blocks access, using rules provided within endpoint security solutions.

Using system hardening to block zero-day exploits

System hardening includes tools, techniques, and best practices for reducing vulnerabilities found within operating systems, applications, endpoints, databases, servers and external devices. To reduce opportunities for bad actors to gain a foothold within their IT infrastructure, IT teams leverage system hardening rules to restrict superfluous programs, applications, access, permissions and account functions.

Today's expanded enterprise perimeter is comprised of potential technology flaws and backdoors that can be exploited by hackers.

Follina is a new exploit that targets Microsoft Office, taking advantage of a vulnerability within Word. Discovered in the wild, Follina uses (or abuses) the Microsoft Support Diagnostic Tool (MSDT) to spawn a malware application. It took Microsoft three weeks to release an update that addresses this exploit that has been used in attacks by various state-backed and cybercrime threat actors. The security flaw, CVE-2022-30190, is a MSDT remote code execution bug that affects all versions of Windows that still receive security updates. Successful exploits of this zero-day execute arbitrary code with the compromised user's privileges of the calling app to install programs, view, change, and delete data, and create new Windows accounts.

Using cybersecurity solutions for system hardening to block Office applications from spawning other applications can be a general rule that an enterprise may apply. But other rules are more specific, and should not be generally implemented, such as blocking executables from webmail and email clients. Problems can arise when a development team sends binary code to each other to collaborate and conduct quality assurance. In this case, blocking executables from email will actually prevent them from doing their jobs.

System hardening best practices

The system hardening you enable will depend upon the various risk factors within your particular IT infrastructure, your resources, and the priorities that are defined for resolving technology issues. Cybersecurity products, like RevBits Endpoint Security, include automated systems hardening functions to block unknown, zero-day exploits from hackers externally, and from internal personnel with bad intentions. This is a critical capability for organizations to have before a zero-day attack has been discovered, and during the period of time when the exploit is known, but no patch is available from the software vendor or device manufacturer.

RevBits EPS closes system vulnerability gaps

Protecting against cyberattacks requires closing system loopholes that hackers use to exploit systems and gain access to sensitive data. Systems hardening secures computer systems by minimizing vulnerable attack surfaces.

RevBits EPS has over twenty restrictive system hardening features that can be enabled based on specific use cases. Every environment is unique, and system hardening should be applied judicially. Many hardening features are very specific, and they should be applied within segmented networks. This allows a specific rule to be selectively applied by user groups and types.

System hardening can bring substantial benefits. Reducing programs and restricting functionality helps lower operational risk, with fewer incompatibilities and misconfigurations. Reducing attack surfaces improves security by lowering the risk of data breaches from unauthorized access, systems hacking, and successful malware exploits. Fewer programs and accounts, combined with less complexity, also helps create greater transparency for simplified compliance and auditing.

Keep Your Enterprise Protected. Get a Demo or Free Evaluation.
To learn more, visit www.revbits.com

34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • www.revbits.com