SOLUTION BRIEF

5 Reasons a Vulnerability Scanner Can't Do Firmware Security

As the frequency and impact of firmware and supply chain attacks have increased, organizations naturally need to mitigate their risk and control their firmware and hardware attack surface. However, firmware security poses a variety of challenges that go well beyond the capabilities of traditional vulnerability management tools. Firmware-level security requires a variety of specialized functions and expertise not found in scanners that are primarily designed for software and operating systems.

This document introduces 5 fundamental differences between Eclypsium and traditional enterprise vulnerability scanners and what these capabilities mean for your security practice.

1 Device Validation and Integrity Checking

Why it matters	Understanding device risk is not limited to CVEs. You must also be able to verify that all equipment is genuine and has not been tampered with in the supply chain or after deployment.
What Eclypsium customers receive	• Up-to-date insight into the specific firmware that should be present on more than 95,000 enterprise devices. • Simple scans to independently verify the integrity of their devices and supply chain

Eclypsium has by far the industry's largest library of firmware profiles. The Eclypsium database includes over 6 million elements from over 200,000 update packages, covering more than 95,000 distinct devices that include a vast range of vendors, device types, and models. Eclypsium is constantly expanding and maintaining this database as vendors roll out new firmware.

Why is this important? Unlike many kinds of software, firmware must remain highly predictable. By maintaining a massive catalog of industry firmware, Eclypsium's device scans can verify the observed, actual firmware matches the firmware profile that "should" be on the device. Without this foundational information it's virtually impossible to independently verify the integrity of devices and hardware… and by extension the technology supply chain that provides them.

Vulnerability scanners fundamentally lack this level of insight. Such tools are focused on detecting CVEs, not verifying that a device and its underlying code actually is what it claims to be. Without the ability to validate the integrity of a device, an organization could easily patch a device that is already compromised and remain blind to the risk tied to the device.

2 Superior Breadth of Coverage

Why it matters	Attackers seek out vulnerabilities anywhere they can, including in network devices. Security teams can't afford to only scan for vulnerabilities in the rare cases where it is convenient.
What Eclypsium customers receive	• Automated device discovery to ensure coverage of all devices. • Ability to detect firmware vulnerabilities even without an authenticated scan. • Coverage for devices often overlooked by traditional scans such as networking infrastructure.

While vulnerability scanners may include support for some firmware CVEs, they fall well short of seeing an organization's true firmware attack surface. Eclypsium's coverage advantages can be traced to 3 key areas:

- **Automated Device Discovery** - Eclypsium includes unique automated device discovery in order to find devices that may be overlooked or missed by traditional scans.
- **Superior Coverage for Enterprise Devices** - While traditional scanners focus on traditional laptops and servers, Eclypsium also includes coverage for other critical enterprise devices such as networking devices and VPNs which have been heavily targeted by ransomware and advanced threat actors.
- **Ability to Detect Vulnerabilities With Unauthenticated Scans** - Detection of firmware vulnerabilities often requires deep, authenticated access to a system. This is often not practical or sometimes outright avoided due to concerns about how a scan could affect the target device. Eclypsium supports detailed device-based fingerprinting that can identify vulnerable devices without the need to authenticate to the device.

3 Superior Depth of Coverage

Why it matters	Firmware misconfigurations and vulnerabilities are unique and hard to observe. While vulnerability scanners can rely on second-hand OS insight, firmware code must be directly assessed.
What Eclypsium customers receive	• Coverage for more than 4,000 firmware vulnerabilities. • Specialized drivers to ensure low-level access to firmware. • OS-independent visibility • Industry-leading firmware vulnerability research

Firmware is a highly-specialized security discipline that requires considerable focus and expertise. Unlike traditional security tools that focus on a few highly commodified operating systems, there is incredible diversity when it comes to firmware. Every vendor and every underlying component may have its own firmware, with its own underlying vulnerabilities. Eclypsium maintains the industry's most complete database of firmware vulnerabilities that goes well beyond those covered by traditional scanners. This includes more than 4,000 firmware-specific vulnerabilities and growing every day.

Additionally, firmware is the lowest-level code on any device, and even gaining reliable access to this level can be a challenge. Eclypsium is the industry leader in the analysis of firmware, and includes its own proprietary techniques to ensure access to firmware within enterprise devices. This includes specialized drivers needed in order to see firmware that traditional scanners lack. Additionally, recent attacks such as iLOBleed have shown how attackers can disrupt firmware updates and report false information to the operating system to trick staff or software into thinking the update was successful. Eclypsium includes multiple ways of access firmware for analysis including methods that do not rely on the operating system to ensure that all results are accurate.

4 Comprehensive View of Device Security and Compliance Posture

Why it matters	The security of a device relies on dozens of low-level features and settings all working together that can easily leave a device defenseless if not properly configured.
What Eclypsium customers receive	• Audit of all firmware configurations and boot settings, ensuring all components and protections are enabled and working together. • Device-level view of risk. • Compliance reports aligned to standard regulatory frameworks, like NIST 800-53

Physical devices are highly complex systems that rely on an incredible number of components working together: properly configured Secure Boot settings, maintaining the dbx Revocation database, Intel Boot Guard features, TPM, Intel Management Engine (ME), Microsoft System Guard Secure Launch, System Management Mode, and many more. A misconfiguration or weakness in any component can lead to a loss of integrity of the overall system. The same principles extend to the many components within a system. For example, a lack of DMA safeguards (PDF) could allow attackers to gain control of system memory even after a fully secure boot process.

Vulnerability scanning tools focus on individual CVEs and do not have this holistic view or approach to the security of a device. Understanding these low-level details of how the device chipset, operating system, and hardware components must work together is no small task, and one that is not at all covered by vulnerability scanners.

Eclypsium also helps organizations focus on the risks that matter the most. The platform prioritizes vulnerabilities based on real-world threat intelligence, so that teams are not overwhelmed by alerts and can focus on what matters most to the network.

Eclypsium brings this critical device-level view into the health and integrity of every device. This ensures that all of the available device protections are enabled and working together and that the system is in the best possible state based on its available capabilities.

5

Threat Detection and Response

Why it matters	Security teams need to know if their devices were compromised before they could be patched
What Eclypsium customers receive	• Industry's leading coverage of firmware threats. • Industry's largest library of firmware profiles. • Multiple views of firmware to detect evasion attempts. • Behavioral analysis of firmware to detect unknown threats.

It is important to remember that vulnerability management is only a portion of the Eclypsium solution. The platform also includes the industry's most advanced view into firmware and hardware-level threats. Naturally, this represents an entire area of security capabilities that are not found in vulnerability scanners.

This is important for several reasons. Attackers have heavily targeted enterprise network devices and VPNs as initial access vectors into enterprises. An attacker may try to keep that position hidden until the culmination of the attack, and it is up to security teams to verify if their devices have been compromised before they could be updated.

Eclypsium is the industry leader in the detection of firmware threats. This includes the industry's deepest visibility into known threats, as well as the industry's most complete database of valid firmware. The database of known "good" firmware doesn't mean that the firmware is inherently trusted, but it does allow Eclypsium to quickly check the integrity of any device to see if the firmware has been altered in any way. Additionally, Eclypsium monitors the behavior of firmware to identify any malicious behavior to identify unknown firmware threats or threats introduced via a compromised vendor or supply chain.

Next Steps

Naturally, there are far more than 5 areas in which a firmware security platform will differ from traditional vulnerability scanning tools. However, this list hopefully serves as a starting point for understanding not only some of the specific differences in capabilities but also the differences in the overall approach of these very different solutions.

If you would like to learn more about the Eclypsium solution or see how it can work in your environment, please reach out to the team at info@eclypsium.com.