SOLUTIONS_

5 REASONS A VULNERABILITY SCANNER CAN'T DO SUPPLY CHAIN SECURITY

As the frequency and impact of supply chain attacks have increased, organizations naturally need to mitigate their risk and control the attack surface of their assets. However, supply chain security poses a variety of challenges that go well beyond the scope of traditional vulnerability management tools. Organizations now need to see deeper into their devices than the application and OS levels seen by traditional scans. They need tools that understand how all the low-level components and code from various vendors and suppliers are all intended to work together and if there are mistakes that can put the asset at risk. And they need tools that confirm that each asset and component is authentic, intact, and free from threats.

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

1 Supply Chain Validation and Integrity Checking

Why it matters	Device and supply chain risk is not limited to CVEs. You must also be able to verify that all assets and components are genuine and have not been tampered with in the supply chain or after deployment.
What Eclypsium customers receive	• Up-to-date library millions of supply chain components, covering more than 95,000 enterprise devices down to the firmware and hardware. • Simple scans to independently verify the integrity of their devices and supply chain

Before you can trust a device you must know far more than simply if it has vulnerabilities. You must be able to verify that each asset is authentic and hasn't been altered or tampered with. This means that organizations need to be able to verify what is "good" as well as detect what is "bad". The ability to cover both of these requirements is unique to Eclypsium.

Eclypsium has by far the industry's largest library of supply chain and firmware profiles. The Eclypsium database includes over 8.6 million elements spanning more than 100 vendors and 40,000 models. Eclypsium is constantly expanding and maintaining this database as vendors roll out new updates.

This massive catalog of industry components and firmware means that Eclypsium can proactively verify that the actual code in a device exactly matches what "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 Deeper Insight Into Assets, Components, and Configurations

Why it matters	Much of the supply chain attack surface is hidden beneath the level of the operating system. It requires extensive expertise to even reliably see down to these levels and even more expertise to recognize subtle problems once you get there.
What Eclypsium customers receive	• Coverage for more than 4,000 firmware vulnerabilities. • Specialized drivers to ensure low-level access to firmware. • Coverage for vulnerabilities and misconfigurations even without a CVE match. • Independent audit of vulnerabilities, updates, and advisories throughout the components supply chain

Supply chain security is a highly-specialized security discipline that requires considerable focus and expertise. Organizations must be able to reliably see below the level of the operating system and this can require specialized drivers and OS-independent visibility that simply aren't found in traditional vulnerability scanners. Eclypsium also maintains the industry's most complete database of supply chain vulnerabilities that goes well beyond those covered by traditional scanners, covering more than 4,000 supply chain-specific vulnerabilities.

Eclypsium goes well beyond simply doing CVE lookups and actively audits each asset and component to find problems. For example, by observing hardware state and behavior, Eclypsium has previously found missing BIOS write protections, even on a system where it was not previously reported and there is no CVE assigned. This type of vulnerability has been widely exploited in the wild by threats such as LoJax and MosaicRegressor.

Additionally, the NVD often does not map all affected devices to a particular CVE. This can lead to false negatives during traditional NVD lookup scans. Eclypsium analyzes vendor advisories to find any potential gaps in the NVD database such as Intel Xeon E5-2670v3 being affected by CVE-2022-36372 or likewise, CVE-2020-0592 affecting Dell devices as stated in their official updates.

Likewise, Eclypsium provides an independent check of vulnerabilities, updates, and vulnerabilities of supply chain components even when a supplier doesn't propagate a fix. For example, microcode updates can be delivered as part of OS updates, as part of BIOS/UEFI firmware updates, or in some cases, by neither. This can leave organizations vulnerable to Meltdown, Spectre, MDS, Zenbleed, and the new Downfall vulnerability. By tracking the latest supply chain updates from manufacturers, Eclypsium allows organizations to clearly see when code is out of date, vulnerable, or out of support.

3

Integrity Checking and Threat Detection

Why it matters	Security teams need to know if their devices have been altered or compromised either in the supply chain or after being deployed. Simply patching a device that is already compromised may not fix the problem. Teams also need to detect threats where a vendor's "valid" code and processes have been compromised.
What Eclypsium customers receive	• Industry's leading coverage of supply chain threats. • Industry's largest library of firmware and component profiles. • Multiple visibility and access techniques 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 supply chain and asset-level threats. Naturally, this represents an entire area of security capabilities that are not found in vulnerability scanners.

This is important for several reasons. Most organizations have more vulnerabilities than they can patch, leading to significant windows of exposure. As a result, security teams must be able to verify that their devices have not been compromised before they were able to be patched. For example, attackers have heavily targeted enterprise network devices and VPNs as initial access vectors into enterprises. Simply patching a compromised switch or VPN will likely not address the threat or the

overall risk to the organization.

Additionally, malicious code on a device can allow attackers to disrupt any updates and to report false information either to the operating system or user interface. For example, in the recent iLOBleed attacks, ransomware operators were able to compromise the BMCs of data center servers. The attacker code was able to prevent any updates from being applied, yet falsely showed that the update was applied successfully in the UI. This allowed the attackers not only to cause massive damage but also to reinfect the data center even after the threat was initially detected.

Security teams also need to be able to evaluate the "valid" code they receive from vendors. Vendors have repeatedly delivered malicious code to customers due to having their build environment or update processes compromised as seen in the notorious SolarWinds attack. Additionally, vendors may intentionally include dangerous functionality that would not show up on a vulnerability scan. For example, Eclypsium's heuristic analysis recently identified an insecure backdoor being used within a wide range of Gigabyte devices.

Eclypsium is the industry leader in the detection of supply chain threats. This includes the industry's deepest visibility into known threats, as well as the industry's most complete database of valid firmware. Additionally, Eclypsium monitors the behavior of all supply chain code and components to identify any malicious behavior or threats introduced via a compromised vendor or supply chain.

4 Superior Coverage Across Enterprise Assets

Why it matters	Attackers have heavily targeted devices that are often overlooked or that are difficult for traditional vulnerability management tools to scan. This has led to a massive increase in attacks on network devices such as VPNs, enterprise firewalls, and network and application infrastructure.
What Eclypsium customers receive	• Automated device discovery to ensure coverage of all devices. • Ability to detect low-level 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 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 low-level 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.

5

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.

Additionally, vulnerability scanning is only a part of what it takes to maintain regulatory compliance. Standards such as NIST's SP 800-53 require a coordinated effort across many security disciplines beyond vulnerability management such as maintaining highly detailed inventories of all software, hardware, and firmware, as well as monitoring their configuration, baseline, integrity, and much more. Elclypsium provides a multi-disciplinary approach to device and supply chain level security, allowing teams to cover many areas with a single tool.

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.

Next Steps_

Naturally, there are far more than 5 areas in which a supply chain 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.