SOLUTION BRIEF

5 Reasons an EPP/EDR Can't Do Firmware Security

As attackers have pushed firmware and supply chain attacks to the forefront of security, many traditional security vendors have opportunistically added "firmware-specific features" to their products. However, firmware security is not an add-on. Firmware-level security requires highly specialized functions built on a unique set of capabilities and expertise not found in endpoint security and EDR tools.

Let's briefly look at 5 fundamental differences between Eclypsium and EPP/EDR and what it means for your security practice.

1 An Industry-Wide Firmware Database

Why it matters	You can't reliably verify device integrity or validate the supply chain without it.
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. This means Eclypsium immediately detects any change to the integrity of the firmware, even if the threat is completely unknown to the industry. 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. Also, this type of detection doesn't need to wait for malicious code to run, or rely on OS-level cat-and-mouse adaptations that constantly occur between malware and security tools.

EPP and EDR simply lack this level of insight. An industry-wide firmware database requires dedicated, ongoing effort in order to provide global coverage and remain up-to-date with the latest designs of vendors and supply chain suppliers. It is one of the highly specialized capabilities that a firmware security platform brings to the table.

2 Firmware Threat Expertise and OS Independence

Why it matters	Firmware threats can be highly complex, and attackers use them specifically to subvert security running in the OS.
What Eclypsium customers receive	• Multiple views of firmware to detect evasion attempts • OS-independent analysis techniques • Industry's leading coverage of firmware threats • Behavioral analysis of firmware to detect unknown threats

As firmware threats have gained prominence, some EPP/EDR vendors have opportunistically claimed "firmware threat insight" in their brochures. However, this only addresses a fraction of the overall firmware threat landscape. Certainly, defenders don't have the luxury of being opportunistic when it comes to protecting their critical assets from threats.

But EPP/EDR tools share a more fundamental problem: they are architected to fight threats at the OS level. One of the main reasons attackers target firmware in the first place is that it can allow them to subvert or deceive systems running in higher layers. For example, the recent iLOBleed highlighted the ability of malicious firmware to prevent staff from updating firmware, yet falsely reporting that the firmware was successfully updated. Firmware also can contain its own independent communication stacks as seen by the PLATINUM group's use of Intel AMT as an OS-independent command-and-control channel.

Eclypsium provides a wealth of detection capabilities uniquely focused on firmware and device-level threats. Instead of relying on OS reports, multiple Eclypsium techniques are used in concert to collect firmware information, including methods that are independent of the operating system. Creating multiple perspectives is critical when dealing with firmware threats: attackers have gone to firmware to evade security in the first place.

Additionally, Eclypsium leverages behavioral analysis of firmware in order to detect new or unknown firmware threats, or even firmware threats that have been introduced into "valid" code in the technology supply chain. All of these capabilities are required if an organization is going to detect an advanced firmware threat.

3

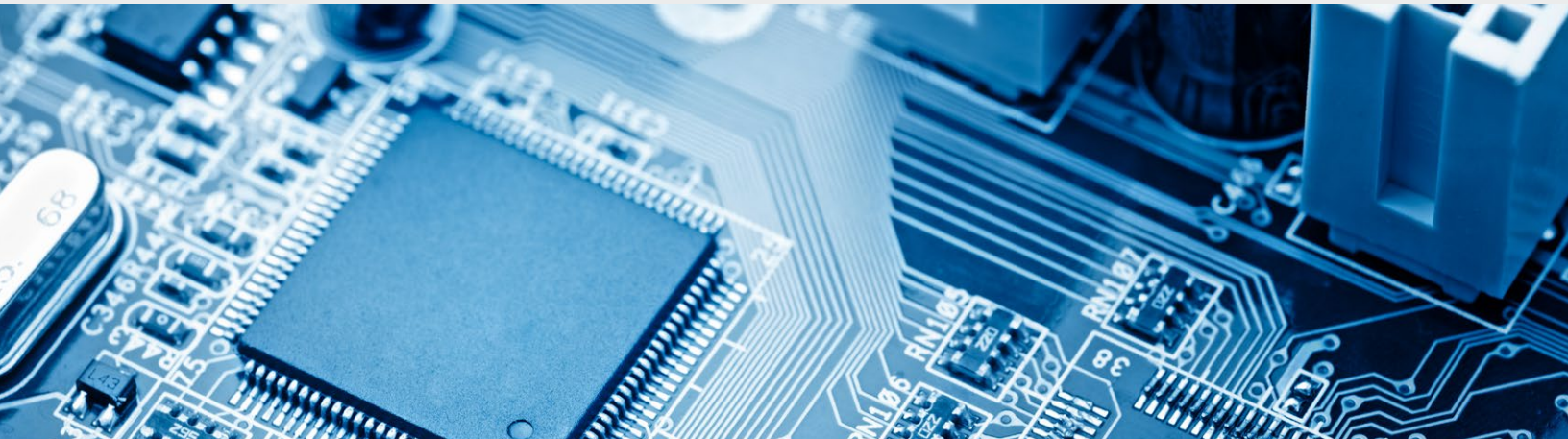
Coverage Across Enterprise Devices Types

Why it matters	Servers, VPNs, networking devices, and devices that can't support security agents are a major part of the firmware attack surface.
What Eclypsium customers receive	• Vulnerability and threat detection in network devices • Deep vulnerability and threat detection for servers and BMCs • Network scanning • Automated discovery of devices

EPP/EDR tools are overwhelmingly applied to traditional laptops and workstations, and to a lesser extent, to servers. This leaves some of the most active areas of the firmware attack surface unguarded. Firmware within network devices such as VPNs, routers, and application and network controllers have become some of the most popular initial access vectors for ransomware and advanced threat actors. These critical devices not only provide the initial foothold, but they also allow attackers to use the broad connectivity of these devices to spread to countless other devices and establish persistence. This can give an adversary a significant presence in a target network before ever touching a traditional endpoint running EPP/EDR software.

Additionally, EPP/EDR tools don't address the unique firmware capabilities and threat vectors that are unique to server hardware. EPP/EDR tools focus on the operating system level, and as such, generally treat servers simply as big endpoints. There is very little specialization that is unique to their protection of servers. However, at the hardware and firmware level servers are strikingly different from other endpoints. A single server can easily have 3x as many types of firmware components as a traditional endpoint, and these components are often the most commonly targeted pieces of firmware. For example, the baseboard management controller (BMC) within a server provides a remote administrator with complete control over a server and all its contents. Recent attacks such as the recent iLOBleed illustrate how real-world attackers target these critical firmware components in order to both cause damage and establish ongoing persistence.

Eclypsium provides coverage across all of an organization's critical devices whether laptops, servers, or networking equipment. This includes the ability to proactively discover and identify devices even if they are not equipped with a security agent. The solution makes sure security teams can know exactly what hardware they have, if there are any vulnerabilities in those devices, or if they have been compromised by threats.



4 Granular Protection for Atomic Hardware Components

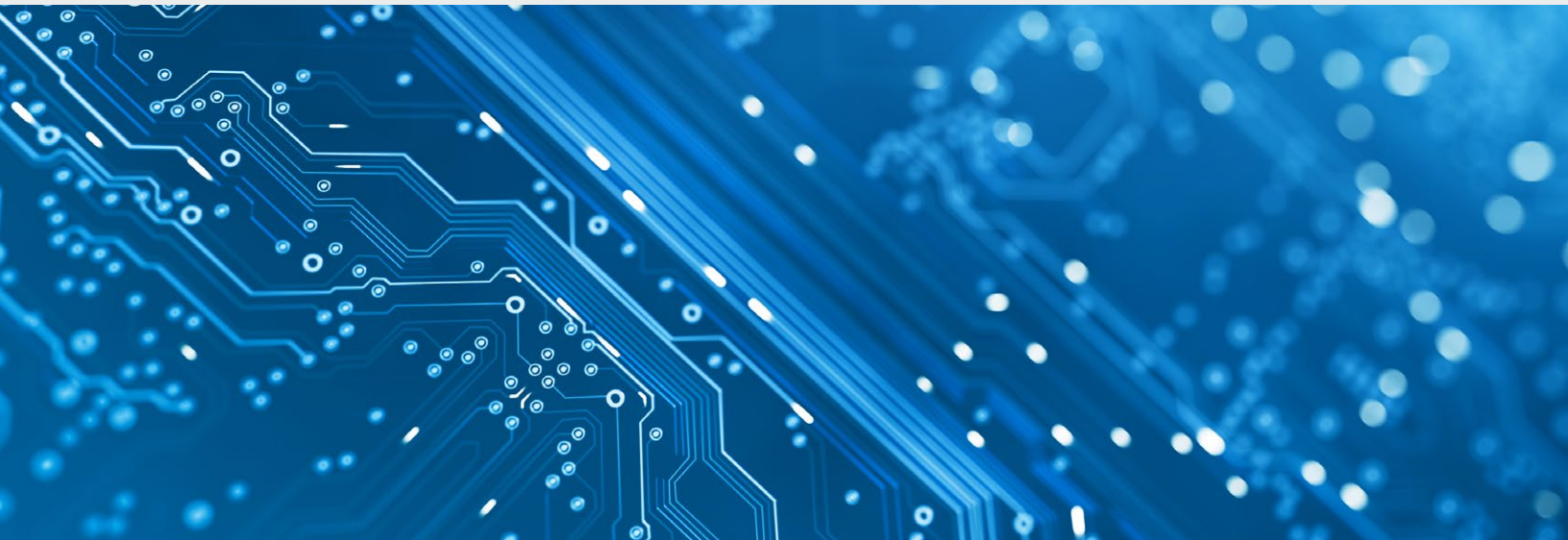
Why it matters	Dozens of underlying components with complex supply chains provide places for threats or weaknesses to hide
What Eclypsium customers receive	• Analysis of more than **60 classes of device sub-components** for vulnerabilities and threats. • Verification of the most complex supply chains

EPP/EDR tools have virtually no visibility or coverage for the dozens of underlying components within a device beyond the system-level UEFI/BIOS. Coverage for these components is critical because they have been used in real-world attacks and represent the most convoluted and poorly controlled portion of the technology supply chain.

Implants in the firmware of storage drives have been used to allow attackers to protect their malicious code in areas that the firmware can hide from the operating system. Well-known tools such as PCILeech can allow attackers to take advantage of vulnerable PCIe adapters to directly read and write system memory. Compromised firmware in network adapters can allow attackers to machine-in-the-middle traffic, redirect traffic, or hide command-and-control traffic. Virtually any component within a device can be co-opted as part of an attack, or provide a place for attackers to hide.

Hardware components are also sourced from a wide range of suppliers, spanning many countries of origin, often being replaced based on cost and availability pressures. Every one of this constantly changing roster of suppliers and sub-suppliers represents an opportunity for vulnerabilities or threats to be knowingly or unknowingly introduced into the supply chain.

In addition to the system UEFI and BIOS, Eclypsium analyzes firmware from more than 60 **classes** of components including storage, cameras, keyboards, Trusted Platform Modules (TPMs), and network adapters. Once again, this level of insight into the components of a device is an absolute requirement for independently verifying the integrity of the supply chain, and is a capability that only a true firmware security platform can provide.



5 Comprehensive View of Firmware Integrity and Compliance

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 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.

EPP/EDR tools do not have this holistic view or approach to the security of a device. Their focus on malicious binaries or detecting discrete indicators of compromise. These tools are designed to find specific signs of threats, not to verify the actual health of the device.

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.

Next Steps

Naturally, there are far more than 5 areas in which a firmware security platform will differ from traditional endpoint security 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.