SOLUTIONS_

7 REASONS WHY VENDOR PLATFORM SECURITY IS NOT ENOUGH

Securing IT assets demands continuous effort from both technology vendors and purchasing organizations. Vendors must deliver secure offerings with timely updates and defenses against known threats, and it's up to end-users to apply those patches and configure security features correctly.

However, this model often breaks down when we look below the OS and into the supply chain of system components. The industry has witnessed a surge in low-level UEFI implants and attacks targeting code within network gear, security appliances, and server BMCs. These and countless other techniques play a key role across the attack lifecycle (PDF) from initial access through taking complete, persistent control of virtually any class of asset. Naturally, OS vendors, hardware vendors, and OEMs have added new platform-level security features to resist these threats. And while initiatives such as Microsoft's Secured-core PCs and Apple's Secure Enclave are important, these efforts do not remove the need for independent, cross-platform security tools.

As supply chain and firmware risks increase, the need for these independent tools is greater than ever. Here are 7 key reasons why:

1 Security Controls ALWAYS Complement Platform Security

The mandate to "always verify" is a key tenet of Zero Trust and modern security practice. So while vendors are expected to build the most secure systems possible, organizations are expected to have independent security controls that continuously verify assets and monitor for problems. The more privileged the code, the greater the need for monitoring. Yet traditional tools like EDR and vulnerability scanners don't protect at the firmware and supply chain levels, leaving organizations exposed. Eclypsium provides the independent view to verify that firmware hasn't been compromised and is properly configured and free of vulnerabilities.

Example: NIST 800-53 consistently calls out firmware when addressing security controls. Lenovo issued a security advisory after an Eclypsium customer discovered some ThinkSystem servers were shipped with the Intel ME firmware in manufacturing mode.

2 Secure Systems Don't Stay Secure

All reputable vendors believe their products to be secure when they are released. But security is always a moving target and new vulnerabilities are discovered every day. A secure firmware layer and boot process depend on dozens of technologies working together, and a vulnerability in any one component can put the entire system at risk. Relying exclusively on vendor-supplied security measures assumes that this complex system will remain invulnerable indefinitely. Independent security controls provide the necessary layer of protection when problems inevitably arise.

Example: The recently discovered Glupteba malware specifically designed to subvert built-in Windows security features such as PatchGuard and DSE (Driver Signature Enforcement).

3 Vendor-Supplied Security Is Highly Inconsistent

Organizations have many types of devices (servers, laptops, network gear), often with multiple vendors in each class, and multiple models from each vendor. The vendor-supplied security features vary widely from vendor to vendor and even from model to model. The best security features are usually limited to the latest and most expensive models, often requiring specific hardware. Organizations must be able to secure their entire fleet of devices, not just the newest. Eclypsium provides protection across critical device types, vendors, and models so that security is consistent and predictable.

Example: OEMs offer Secured-core PCs only as their top-of-the-line devices, which must meet specific hardware requirements.

4

Device and OS Vendors Don’t Address Components and Subsystems

Vendor-supplied security controls don’t extend to the dozens of critical components such as drives, network interfaces, GPUs, PCIe interfaces, and more. Each component has its own firmware, with its own potential vulnerabilities and attack surface that are outside the scope of vendor-supplied security. These components each have their own history of vulnerabilities and threats and can play unique roles in a cyberattack. Eclypsium extends security to these critical components so that organizations can identify risks and threats even beyond the system firmware.

Example: Review how the recent PixieFail vulnerabilities in a common UEFI network stack affect a wide range of vendors and products.

5

Long Device Lifecycles Mean Many Opportunities for Mistakes

Devices have long supply chains and long life cycles, and small changes can put the entire device at risk. How will staff verify that newly acquired systems have vulnerabilities that need to be managed and all the necessary controls are properly configured? Or that all security features are configured and functioning properly after an update? Or after a security incident, IR, or recovery process? Instead of requiring staff to dive into myriad low-level checks, Eclypsium automates the process and provides an independent way to verify that systems are properly configured.

Example: Spectre vulnerabilities re-introduced after updating kernel drivers.

6

Vendors Can Be Compromised

The notorious Sunburst attack against SolarWinds and its customers highlights the severe downstream consequences when a technology vendor is compromised. While Sunburst is the most well-known example, there have been dozens of breaches in critical supply chain vendors that have put critical code in the hands of attackers. Eclypsium not only verifies the integrity of firmware and checks for known threats, but it also models the behavior of firmware to recognize suspicious or malicious behavior at the firmware level even if the firmware appears to be valid.

Example: Western Digital breach exposing firmware for a wide range of storage drives.

7

Problems in the Supply Chain are Often Bigger than Any One Vendor

Secure platforms rely on the coordination of suppliers, OS vendors, open-source projects, OEMs, VARs, and so on. The widespread BootHole vulnerability highlights how a problem in one area can impact all the others. A vulnerability in the GRUB2 bootloader affected virtually every Linux distribution as well as most Windows systems that don’t even use GRUB2 due to their reliance on a common UEFI certificate authority.

Fixes can also be exceedingly slow, as vendors and OEMs will often want to do their own testing. Eclypsium provides a consistent way to know exactly which systems are affected by newly discovered vulnerabilities and can check to see if devices have been compromised long before vendor fixes are available.

Example: Review the best practices and challenges tied to protecting an organization against BootHole.

About Eclypsium

Eclypsium provides visibility and control over an organization's firmware risk and proactively identifies digital supply chain threats. These capabilities allow organizations to ensure the security posture and integrity of IT infrastructure, including servers and network infrastructure, as well as traditional end-user laptops.

Eclypsium enables organizations to augment and extend their existing security processes in the following key areas:

Gain Visibility: Eclypsium allows teams to easily audit their many device types, vendors, and models to see exactly what is inside. The staff gets fine-grained insight into the myriad hardware and firmware components within a device.

Manage Risk: Eclypsium highlights the firmware vulnerabilities, misconfigurations, and outdated code that can put devices at risk but are often invisible to traditional vulnerability scanners. This includes device configurations and policy settings that are essential to maintain a robust device-level security posture. When problems are found, Eclypsium can remotely apply patches or updates to mitigate the risk.

Detect Firmware Threats: Eclypsium automatically verifies system and component firmware integrity and includes the ability to detect known and unknown threats such as implants, backdoors, and rootkits. The solution can automatically notify staff of any changes to the device's integrity or security posture and trigger automated responses and playbooks via the powerful REST API.

To learn more about Eclypsium, please reach out to us at info@eclypsium.com.