COMMON ECLYPSIUM USE CASES

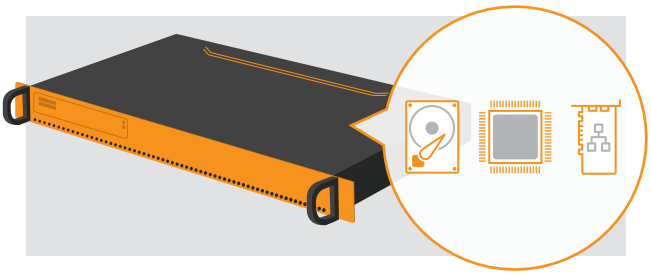
INTRODUCTION

Eclypsium® introduces a new type of enterprise security that defends the underlying hardware and firmware layer of the enterprise. Eclypsium delivers both visibility and active protection so that organizations can ensure the integrity and availability of all their devices, from workstations to critical servers and networking gear. High-level functions of the solution include:

- Visibility of the firmware/hardware attack surface, including system firmware, components, and devices.
- Firmware vulnerability scanning, update management, and virtual patching.
- Detection and mitigation of malicious implants and devices.

Given that Eclypsium provides value across much of the security lifecycle, it naturally opens the solution to a variety of use cases. This document provides a brief introduction into these capabilities and the most common ways that organizations are using them to protect their environments.

ATTACK SURFACE MANAGEMENT

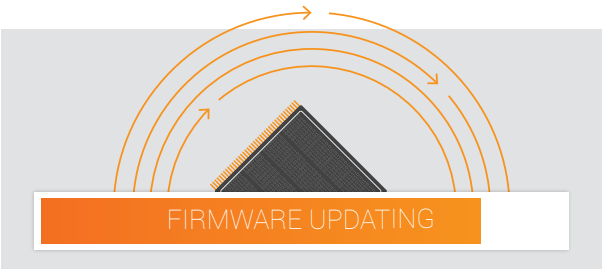


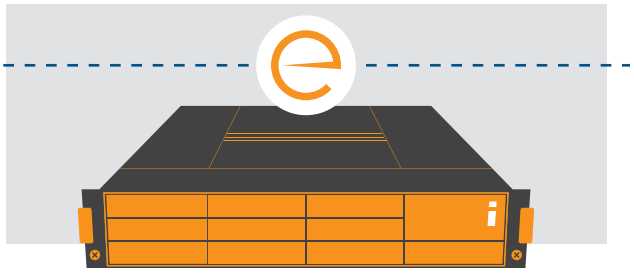
Visibility and Asset Discovery

Firmware and hardware issues are blind spots for most organizations. Eclypsium automatically discovers not only the system firmware of your devices, but also that of the hardware components, as well as the presence of attached add-on devices (such as external network cards or USB devices). This visibility naturally complements device and inventory management efforts by providing visibility into all the code that lives beneath the level of the operating system.

Hardware Vulnerability and Risk Assessment

Eclypsium analyzes devices to proactively reveal any risks within an organization's hardware and firmware. The solution quickly reveals firmware vulnerabilities, device configuration problems, and any missing protections. This audit quickly reveals any weak spots on the device that could be inviting to an attacker or cause availability problems. Additionally, staff can always drill down into any device to see security and configuration details for any device on demand.





Firmware Update Management

If the assessment process identifies any outdated firmware, Eclypsium helps solve the problem. The solution can identify the appropriate firmware version and provide centralized management of system firmware updates, and more. This allows for a centralized approach to managing and actively reducing the organization's hardware and firmware attack surface.

Virtual Patching of Vulnerabilities

When Eclypsium identifies weaknesses, vulnerabilities, or misconfigurations in a system, the solution can provide virtual patching to offer protection until a more permanent fix is available from manufacturers of the system. This provides a layer of protection against exploits that leverage certain types of vulnerabilities in the affected system. For example, the Eclypsium technology can temporarily enforce missing hardware protections, and detect and block exploitation attempts. This can be an important interim layer of protection in times of crisis, as firmware updates and patches can be infrequent, leading to potentially long periods of exposure.

THREAT PREVENTION

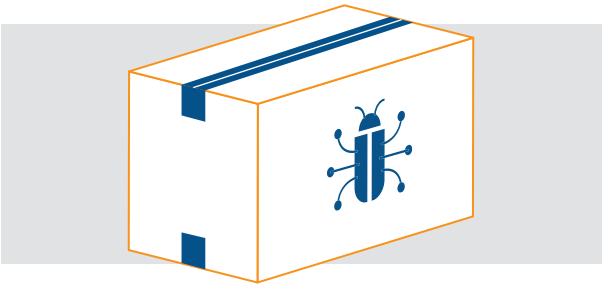
Detection of Threats

Eclypsium monitors devices for a wide variety of compromises at the hardware and firmware level. This includes detection of both known and unknown malicious implants within firmware components. Once again, this can include detection of threats in both system firmware (UEFI/BIOS), the host OS boot chain, and device components including management controllers (BMC/IPMI), Intel Management Engine (ME), network adapters (NIC), storage devices, graphics cards, and more. This also provides incident response teams with an actionable detection of threats that can survive the re-imaging process.

Mitigation and Protection

Eclypsium helps protect your assets from damage, while triggering real-time responses. Configurable alerting can notify staff and trigger responses based on newly detected threats, vulnerabilities, or an integrity failure. Eclypsium also defends against attackers who try to take advantage of device-level weaknesses to overwrite system firmware to render critical servers and network gear unrecoverable ("bricking") or even demand payment to prevent the attack. Eclypsium can identify and protect against these types of attacks by monitoring for compromises, and preventing attackers from corrupting essential firmware and persistent configuration data on critical servers.

.



Protection From Supply Chain Attacks

The industry has increasingly seen a trend of firmware- and hardware-level attacks that are introduced in the hardware supply chain. Industry titans Cisco and Apple are just a few noteworthy examples where implants were discovered in the hardware supply chain. These attacks are traditionally very difficult to detect, as teams often assume that devices are "clean" when they come out of the box. Eclypsium exposes these threats and reveals any hidden firmware implants or backdoors added in the supply chain.

Protecting Employee Laptops During Travel

Employees are often targeted for attack during travel, especially by advanced actors. Such actors often favor the use of firmware implants because they easily evade detection by traditional countermeasures. Eclypsium erases the attacker's advantage and allows staff to travel securely. Organizations can ensure that devices remain safe during travel, can be alerted in real-time to any changes, and verify that devices haven't been compromised upon return.

CONCLUSION

These are just some of the potential use cases for the Eclypsium technology. The hardware layer is a particularly active area of research—and conflict between advanced attackers and defenders. As such, we should expect innovation on both sides and new use cases in the future. If you would like to learn more about any of these scenarios or discuss specific challenges related to your environment, please reach out to the Eclypsium team.