Eclypsium

SOLUTION BRIEF_

ECLYPSIUM FOR DATA CENTERS

Continuous Monitoring for Supply Chain and Firmware Security

Security frameworks and standards are increasingly emphasizing supply chain and firmware security, and for good reason. Attackers are actively targeting IT supply chains and using backdoors and implants to evade detection and maintain persistence.

Yet most data center operators have very little visibility into the components that go into their servers and network appliances, and cannot demonstrate compliance with standards and best practices having to do with cybersecurity supply chain risk management (C-SCRM) or firmware security.

Establish Trust in Servers and Network Appliances

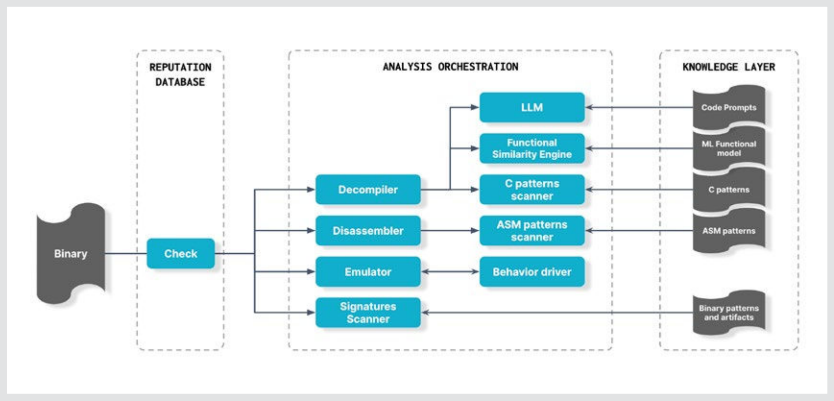
The Eclypsium supply chain security platform is the first-ever solution that is purpose-built for continuously monitoring the integrity and security of IT infrastructure assets. Our platform provides visibility into the hardware and firmware components of servers and network appliances—diving below the operating system to uncover vulnerabilities, misconfigurations, and threats that EDR and vulnerability scanners miss.

Benefits for Data Center Operators

Continuously monitor compliance	Implement security controls for firmware integrity, supply chain security, and more	Monitor drift from desired state in component firmware
Harden components with vulnerability management and patching	Detect backdoors, implants, and other evasive threats	Integrate supply chain security visibility into ITSM, CMDB, SIEM, etc.

How It Works

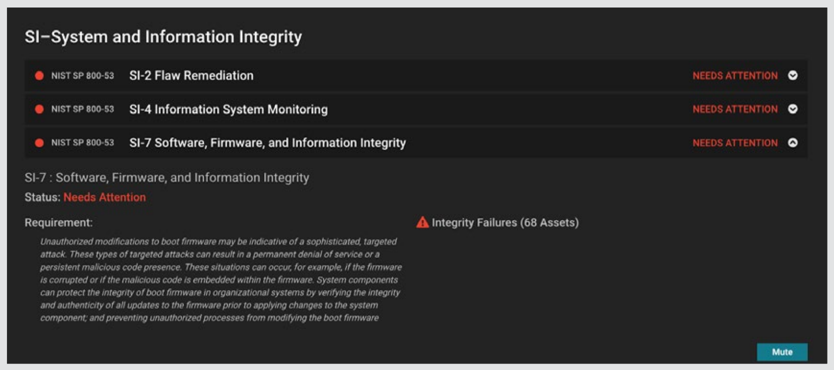
The Eclypsium supply chain security platform uses sensors to scan devices and extract firmware binaries and other system metadata. This data is sent to a cloud-hosted single customer tenant for analysis. This scanning process is configurable so that target devices can be scanned regularly on a schedule that does not interfere with operations. For example, production servers can be scanned every time that they boot up.



Eclypsium's Automata system provides deep analysis of all the firmware binaries in your environment to detect previously unknown vulnerabilities and threats.

Eclypsium maintains the industry's only reputation database of firmware and microcode—more than 12 million different firmware binaries! This gives operations teams confidence that they are running trusted, approved firmware. Eclypsium enables operations teams to set baselines for individual devices as well as groups of devices, and to detect drift in specific component firmware from desired states. In addition, Eclypsium's automated binary analysis replicates the tooling and techniques of human security researchers to continuously analyze firmware binaries used in production and uncover zero-day vulnerabilities and malicious behavior (see diagram below).

Eclypsium can help with remediation of discovered vulnerabilities by speeding up the patching process, including with automated updates via the Redfish API in some supported cases. When a supply chain incident occurs, Eclypsium can help operations and security teams quickly identify affected components in their device fleets.



SI–System and Information Integrity

● NIST SP 800-53 SI-2 Flaw Remediation NEEDS ATTENTION

● NIST SP 800-53 SI-4 Information System Monitoring NEEDS ATTENTION

● NIST SP 800-53 SI-7 Software, Firmware, and Information Integrity NEEDS ATTENTION

SI-7 : Software, Firmware, and Information Integrity
Status: Needs Attention

Requirement:

Unauthorized modifications to boot firmware may be indicative of a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur, for example, if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component; and preventing unauthorized processes from modifying the boot firmware

⚠ Integrity Failures (68 Assets)

Eclypsium makes it easy to monitor and report on compliance with standards such as NIST 800-53 rev5.

ABOUT ECLYPSIUM_

Eclypsium's cloud-based platform provides digital supply chain security for critical software, firmware and hardware in enterprise infrastructure. Eclypsium helps enterprises and government agencies mitigate risks to their infrastructure from complex technology supply chains. For more information, visit eclypsium.com.