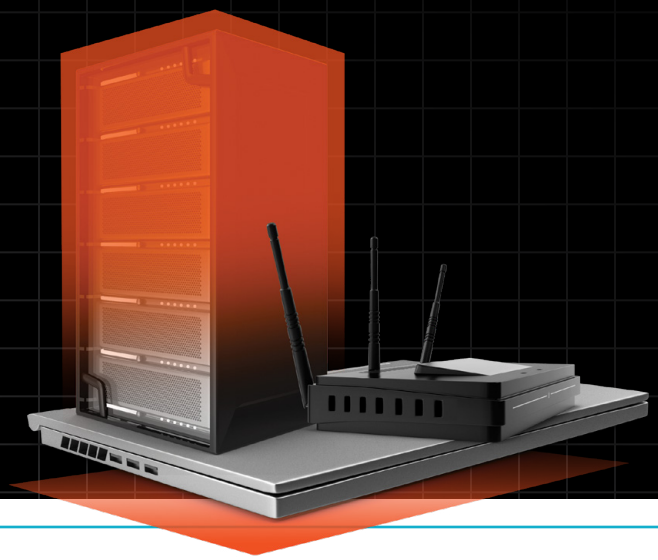
SOLUTIONS_

SERVICE OFFERINGS_



The Eclypsium platform helps organizations verify the integrity of enterprise hardware and firmware across devices in production. Customers use the platform to inventory firmware and hardware components, identify vulnerable or unauthorized firmware, monitor for drift, and detect threats that evade traditional EDR and OS-level security tools.

Eclypsium research has identified and disclosed vulnerabilities affecting firmware, secure boot implementations, BMCs, and enterprise infrastructure components. Our services offerings make our researchers available to compliment and extend the value you get from the platform, including firmware analysis, integrity validation, and device telemetry to help organizations assess hardware and firmware risk throughout the device lifecycle.

Service Offerings Throughout The Device Lifecycle_

Eclypsium provides services and tooling that inspect firmware and hardware below the operating system. These assessments help organizations validate device integrity during manufacturing, procurement, operations, and decommissioning.

Manufacturing

Verify that devices match expected hardware and firmware baselines before deployment.

Procurement

Validate that devices arrive with authentic components and no evidence of tampering or unauthorized modification.

Operations

Monitor firmware integrity, detect drift, and identify threats or configuration changes that can persist below the OS.

Hardware Supply Chain Risk Assessment_

Enterprise devices contain firmware, embedded controllers, and third-party components that traditional security tools often cannot inspect. Attackers increasingly target these layers because they provide persistence and can evade OS-level visibility.

Device Teardown

Ideal for evaluating new devices prior to deployment.

Competitive Assessment

Compare the security profile of two devices under consideration.

Operational Assessment

Inspect a fielded device for malicious activity (threats, implants, malware).

Eclypsium assessments analyze firmware and hardware trust relationships, including platform root of trust technologies, embedded controllers, and device configuration state. These assessments help organizations identify vulnerable components, unauthorized modifications, and supply chain exposure before systems enter production environments.

Firmware Compromise Assessment_

Most incident response workflows focus on operating systems, applications, and network activity. Firmware compromise often requires different telemetry, analysis methods, and validation techniques.

Eclypsium investigators analyze suspicious firmware indicators identified by the Eclypsium platform, including integrity failures, anomalous firmware behavior, unauthorized changes, and persistence mechanisms below the OS. The goal is to determine whether findings represent operational drift, misconfiguration, or active compromise.

Consulting Support_

Establishing infrastructure trust requires more than deployment alone. Eclypsium provides advisory services focused on firmware integrity, hardware supply chain risk, and operational security controls for enterprise infrastructure.

Cyber Supply Chain Risk Management (C-SCRM)

Risk management practices, standards, and operational use of SBOM/FBOM.

Device Risk Management

Integrate firmware updates and integrity monitoring into IT/SecOps workflows.

Secure Decommissioning

Ensure retired/upcycled systems do not retain sensitive data.

Product Security Assurance for Firmware and Hardware_

Some of the world's largest OEMs and ODMs rely on Eclypsium to audit their systems for supply chain security issues in hardware, firmware, and platform root of trust (PRoT). This should not come as a surprise given that Eclypsium has researched and disclosed major flaws in secure boot, bare metal cloud deployments, and data center baseboard management controllers (BMCs).

Eclypsium researchers have been **researching and assessing platform supply chain security for over a decade**. Our findings have been published in hundreds of articles and presented at the largest security conferences. Eclypsium is already helping some of the largest equipment manufacturers, enterprises and government organizations in this space. Our services team is available to help your organization address this critical concern.

About Eclypsium_

Eclypsium protects the foundation of enterprises and government agencies from hidden risks in hardware supply chains by securing the critical software, firmware, and hardware across every enterprise device. Eclypsium unifies inventory, hardening, threat detection, and response for the entire fleet, eliminating risk across the device lifecycle, from onboarding to production to secure disposition. With support for every major enterprise hardware vendor, Eclypsium protects hundreds of thousands of end-user devices, servers, network infrastructure, GPU clusters, and enterprise IoT assets. Powered by an industry leading database of over 30 million device binaries, Eclypsium is the single platform to establish trust in hardware infrastructure and the device supply chain our customers rely on. For more information, visit eclypsium.com.