Eclypsium Infrastructure Assurance Platform.

Secure Infrastructure in the Age of AI

Your business runs on infrastructure. We make sure you can trust it. Eclypsium provides continuous assurance of mission-critical infrastructure throughout its lifecycle. The platform inventories hardware and supply chain risk, monitors your entire device fleet, and patches and protects devices across user endpoints, network and edge infrastructure, servers, AI infrastructure, and enterprise IoT.

Trusted infrastructure is under attack

Enterprises trust their hardware vendors to deliver secure devices. Yet network gear, servers, GPUs, and enterprise IoT devices arrive carrying vulnerabilities, misconfigurations, and malicious implants introduced throughout the supply chain. Each device has dozens of components, hundreds of dependencies, and thousands of binaries. Attackers target these layers because they are hard to inspect and give them a persistent place to stage future attacks. Traditional software-layer controls, such as EDR and vulnerability scanners, do not inspect these layers, and many network appliances cannot run an endpoint agent. Eclypsium prevents breaches and builds trust at the hardware layer, detecting known and unknown risks and active threats that other security tools miss.

> “The very devices that are supposed to be our frontline defense are becoming our greatest weakness.”
>
> **Pat Opet**,
> Global CISO
> JPMorgan Chase
> RSAC 2026 keynote

One platform to protect every enterprise device

Eclypsium provides continuous assurance of mission-critical infrastructure throughout its lifecycle, with support for every major enterprise hardware vendor. Eclypsium protects five categories of enterprise devices: user endpoints, servers, network and edge infrastructure, AI infrastructure, and enterprise IoT.

USER ENDPOINTS
Laptops, desktops, and workstations

NETWORK AND EDGE
Switches, routers, firewalls, and VPNs

SERVERS
Data center and on-premises servers

AI INFRASTRUCTURE
GPU servers and AI clusters

ENTERPRISE IOT
Cameras, displays, and other connected devices

Platform capabilities

Inventory Hardware and Supply Chain

Know what is in your fleet and where the risk is. Eclypsium inventories every device and its components, building detailed hardware, firmware, and software bills of materials (HBOM, FBOM, and SBOM). The platform compares firmware and components against Eclypsium's reference database of known-good device binaries to find vulnerable, misconfigured, counterfeit, tampered, and end-of-life devices before they enter production. These inventories support NIST 800-53, EU CRA, DoD Zero Trust Target Levels, CJIS, and C-SCRM programs.

> "The roots of trust in your IT infrastructure are extremely important, yet are extremely difficult to inspect and not well understood. Eclypsium's solution solves these critical problems simply."
>
> **Tim Lisko**, Senior Director of Security Engineering, DigitalOcean

Monitor Your Entire Device Fleet

Know that a device is still trustworthy after deployment. Eclypsium continuously monitors every device against known-good baselines, set for individual assets or device groups. It detects integrity changes, rogue devices, indicators of compromise, and attackers living off the land, including persistent compromises that survive reboot, reimage, and patching. It also catches tampering designed to evade or disable EDR agents.

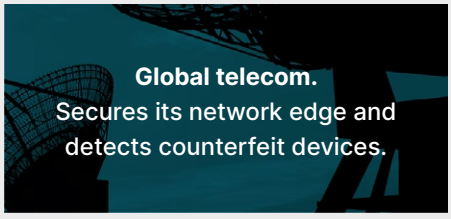
Patch and Protect Devices

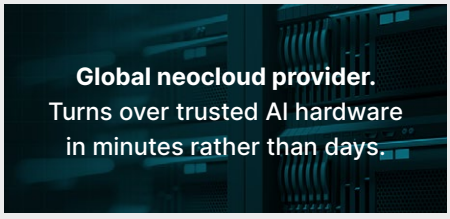
Reduce exploitable hardware risk at scale. Schedule and automatically apply firmware updates on supported devices. Eclypsium identifies vulnerable firmware and insecure configurations, mitigates known and unknown vulnerabilities, and hardens devices against living-off-the-land attack tactics. Fixes are prioritized by severity, recommended mitigations, and whether a vulnerability is known to be exploited in the wild. Configurable alerts, REST APIs, and SIEM/SOAR integrations automate response actions, and configuration drift monitoring keeps protections in place.

Eclypsium Automata

Eclypsium Automata applies our research team's reverse-engineering techniques through automated analysis of firmware and software binaries. Multiple analysis methods identify suspicious code and potential unknown vulnerabilities, extending detection beyond known indicators. Eclypsium's reference database of more than 30 million device binaries supports integrity verification at scale.

Proven in production





Stop assuming your infrastructure is trustworthy. Start verifying it.

See how enterprises and government agencies use Eclypsium to establish trust in their infrastructure. Request a demo at **eclypsium.com/demo**.