



SOLUTION BRIEF

# SECURE DEVICE LIFECYCLE MANAGEMENT

Defend your IT infrastructure against invisible risks across the entire lifecycle.



IT infrastructure brings hidden risks into enterprise environments. Known vulnerabilities in network routers, switches, and firewalls are being actively targeted by nation state threat groups and ransomware gangs like Black Basta. 51% of vulnerabilities in CISA's most recent Routinely Exploited Vulnerabilities report affected network infrastructure.

*The compromise of routing devices is a recent trend in the tactics of espionage-motivated adversaries as it grants the capability for a long-term, high-level access to the crucial routing infrastructure, with a potential for more disruptive actions in the future. A concerted effort is required to safeguard these critical systems and ensure the continued stability and security of the internet.*

– Mandiant, 2025

**51% of top exploited vulnerabilities impacted network infrastructure.**

– CISA, 2023 Top Routinely Exploited Vulnerabilities, November 12, 2024



## THE CHALLENGE\_

At every stage of an IT device's lifecycle, unique cyber risks put company security and operations in jeopardy. Secure Device Lifecycle Management starts before plugging in the devices, and continues through active duty and decommissioning.

### ONBOARDING

Nothing should get plugged into your enterprise network without acceptance testing. From laptops to enterprise switches, technology ships with outdated and vulnerable software, firmware, and hardware all the time.

### IN PRODUCTION

Network devices are a prime target for hackers, with over half of the CISA's Top Routinely Exploited Vulnerabilities affecting network infrastructure. And routers, firewalls, and switches don't let you install EDR and other key security controls, leaving a huge unmonitored attack surface.

### DECOMMISSIONING

Making sure all proprietary data is wiped from IT gear before selling or trashing it is critical for enterprises.

Many organizations have their IT assets destroyed due to lack of confidence that they can be effectively cleansed and resold.

## ECLYPSIUM SECURES DEVICES AT EVERY LIFECYCLE STAGE\_

### Device Onboarding

Eclipsium Assures You that devices have not been tampered with, and are as-expected when delivered.

- BOM of all components and firmware
- Validate the hardware and firmware for authenticity and integrity
- Ensure the supply chain has not been compromised
- Acceptance testing. Validate you are getting what you purchased

**Case Study:** Learn how Digital Ocean saved millions during a company acquisition by validating that the acquired company's devices were secure so they didn't have to buy new gear. [Read the Case Study.](#)



## Production IT and Security Operations Assets

Eclipsium monitors and manages integrity, baseline, vulnerabilities and detects threats in each device in operation.

- Visibility: hardware, component and version inventory (BOM)
- Continuous vulnerability and configuration assessment in components and firmware.
- Integrity and Change Monitoring. Alert on component or firmware changes, persistent threats
- Remediation. Firmware Patch Management across all vendors.
- Compliance with supply chain security controls

**Case Study:** Learn how a Global Telecommunications company inventories, secures, and hardens active duty network devices. [Read Case Study.](#)



## Device Decommissioning

Eclipsium validates that devices are cleansed of any sensitive or identifiable data.

- Device cleansing: factory reset of hardware and firmware components
- Validate cleansing process was successful and no identifiable data resides on any components
- IT Asset Disposition: Resell devices to recover money, with confidence they are clean

[Schedule a live demo to learn how it works.](#)