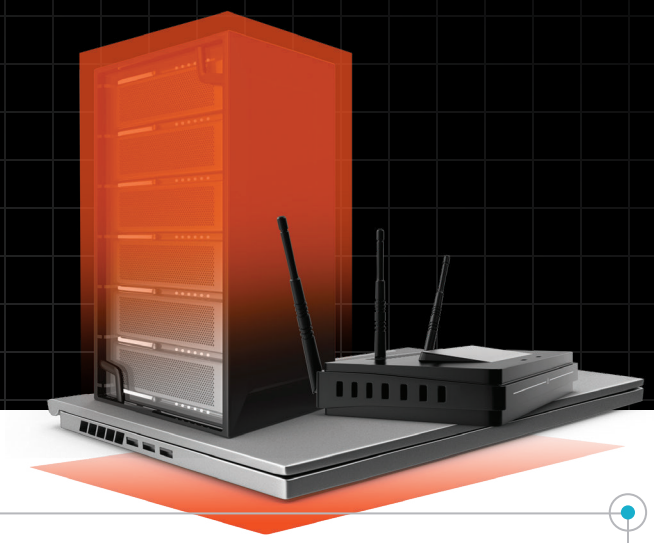
SUPPLY CHAIN SECURITY FOR GOVERNMENT AGENCIES_

Trust your tech, from core to cloud.



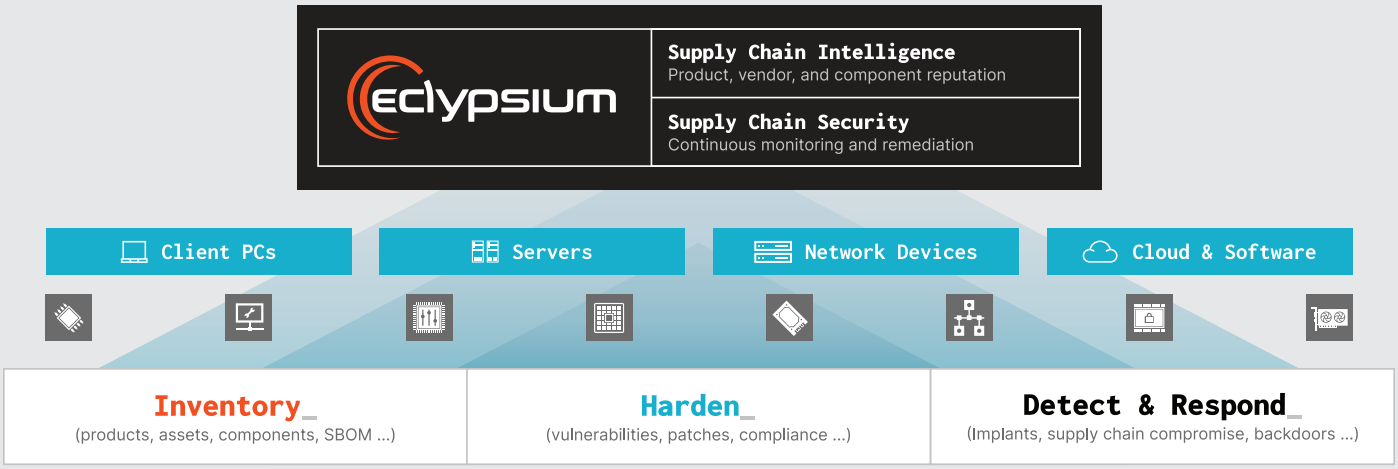
Each piece of the IT infrastructure you rely on to support your mission depends on an incredibly complex supply chain. Every hardware, firmware, and software component can include vulnerabilities or even malicious low-level code.

Attackers take advantage of supply chain complexity, targeting vulnerabilities in hardware, firmware, and software components. These types of threats evade EDR and can maintain persistence after patching and rebooting—leading to devastating results.

> The lack of transparency and trust within the global software supply chain has emerged as a critical issue for organizations of all kinds. Whether driven by the desire to prevent attacks or regulatory mandates, – or both – security and risk management (SRM) leaders must act proactively and aggressively to build resiliency and respond to growing threats.
>
> —Predicts 2024: Supply Chain Technology, Gartner

DEFEND AGAINST SUPPLY CHAIN THREATS_

Eclypsium equips civilian and defense teams to trust the hardware, firmware, and software components in their digital supply chains. Eclypsium provides the supply chain intelligence needed to understand IT product risk, and also a supply chain security platform to validate the integrity of IT products and protect low-level components.



INVENTORY_

Dynamic inventory of production assets - Build an inventory of every piece of enterprise IT infrastructure, down to the hardware, firmware, and software level.

On-demand SBOMs - Generate software bills of material on demand (SBOM), including hardware and firmware components of devices (HBOM and FBOM).

Assess product risk - Equip threat assessment teams with supply chain intelligence to easily understand the risk inherent in IT products.

HARDEN_

Prioritize infrastructure vulnerabilities - Gain insights into low-level vulnerabilities in hardware, firmware, and software components.

Simplify compliance - Track issues at the hardware and firmware levels in frameworks such as NIST 800-53.

Automate firmware updates - Schedule and automatically apply critical firmware patches.

DETECT & RESPOND_

Detect low-level threats - Alert on implants and other indicators of compromise for low-level components of your IT infrastructure.

Defend against tampering and counterfeit components - Validate that assets have not been tampered with and have authentic components.

Correlate with other data - Send alerts to SIEM and SOAR to give analysts improved context and prioritize vulnerability management.

ECLYPSIUM BENEFITS_

Protect Production Assets
Improve mean-time-to-detection and the security posture for your enterprise IT.

Reduce Supply Chain Risk
Make better IT procurement decisions and quickly assess the impact of supply chain threats.

Device Zero Trust
Extend zero trust assurance to the foundational, bare-metal compute levels.

Integrity Assurance
Easily implement security controls for device integrity and firmware security.

ABOUT ECLYPSIUM_

Eclypsium's cloud-based and on-premises platform provides 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.