SUPPLY CHAIN SECURITY FOR GOVERNMENT AGENCIES_

A complete solution, from core to cloud.

Civilian agencies and defense teams need secure, reliable technology to support their missions. However, the complex nature of modern supply chains means that the critical technologies they rely on will pass through many untrusted hands before they are ultimately delivered. And each step in this journey poses a chance for counterfeit products or components, vulnerabilities, or malicious code to be introduced into the supply chain.

> According to the 2022 Verizon DBIR, the **supply chain was responsible for 62% of system intrusion incidents**.

Adversaries have seized upon the supply chain as the ideal attack vector. According to the 2022 Verizon DBIR, the supply chain was responsible for 62% of system intrusion incidents. By targeting technology in the supply chain, attackers can compromise assets early on when defenders are not present. This level of access means threats can be inserted deep within internal components of software, firmware, and hardware within laptops, servers, virtual machines, applications, or the cloud, making them very difficult to detect with traditional security tools.

THE DIGITAL SUPPLY CHAIN ATTACK SURFACE_

Reduced Visibility = Validation Challenges

PHYSICAL

"Hunting for backdoors in Counterfeit Cisco Devices"

PRE-INSTALLED

- Firmware
- Bootloaders
- Kernels
- Operating Systems

3RD-PARTY APPS

slack, Zoom

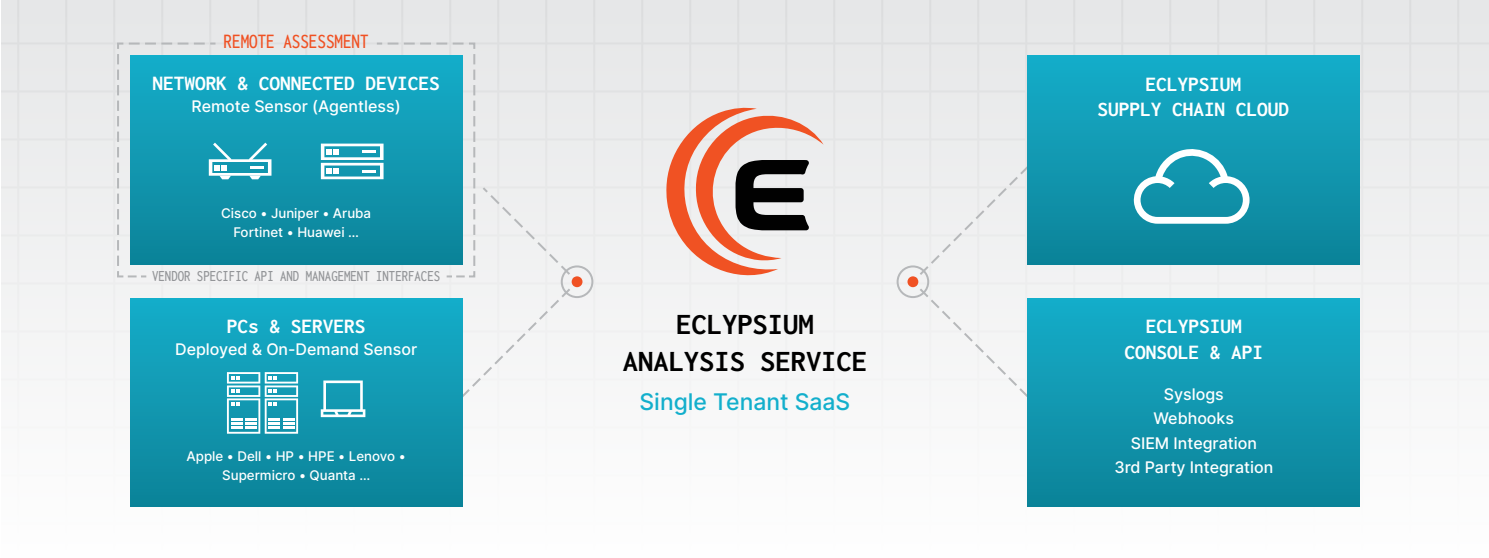
IN-HOUSE SOFTWARE

python Package Index, npm, docker

Increased Customization & Control

WHAT WE DO_

Eclypsium brings simple, verifiable security to the supply chain. Our supply chain security platform proactively verifies the integrity and posture of software, firmware, and hardware throughout an agency's infrastructure. The Eclypsium SaaS platform monitors critical assets from chip to cloud and mitigates risk throughout the asset lifecycle.



WE CAN HELP ORGANIZATIONS_

- **Improve resilience** of critical third-party supply chain infrastructure
- **Establish device-level Zero Trust controls** for modern remote endpoints
- **Automate equipment replacement & maintenance** while prolonging the life of devices

HOW IT WORKS_

Discover and Inventory third-party components, software & firmware in devices

Identify Vulnerable components throughout the supply chain of manufacturers

Verify and Monitor integrity and known-good state of each device

Automate Patching of device software/ firmware across vendor-agnostic fleet

info@eclypsium.com
eclypsium.com