THE ECLYPSIUM SUPPLY CHAIN SECURITY PLATFORM_

Trust your tech, from core to cloud.

Most organizations implicitly trust the foundational layers of their IT infrastructure—a fact that makes low-level exploits especially desirable targets for attackers. The Eclypsium supply chain security platform equips organizations to continuously monitor and remediate the critical low-level components of their IT infrastructure during procurement, deployment, and operation.

This datasheet provides details on Eclypsium's capabilities for clients, servers, and network devices. Additional specifics about support are available on our website through hyperlinks below.

INVENTORY FOR ASSETS AND COMPONENTS_

Eclypsium creates an inventory of assets and their low-level components including system UEFI and BIOS firmware, processors and chipsets, PCI devices, networking components, peripheral devices, Trusted Platform Module, Intel's Management Engine, and more. The level of details can vary by vendor and model.

	Clients	Servers	Network Devices
Identifying Information Device traits such as IP address (optional), MAC address, hostname, and Operating System (e.g., vendor, version).	✓	✓	✓
Detailed Firmware and Hardware Information Processor, chipset, devices, firmware vendor, release dates, system and device manufacturers, model number, etc.	✓	✓	✓
Hardware State and Configurations			
CPU, chipset, and I/O registers, and other related settings	✓	✓	
PCI/PCIe Information - PCI/PCIe device configuration and option (Expansion) ROM firmware	✓	✓	
Device, Component, and Other Firmware Details			
Bootloader information	✓	✓	
Vendor-specific firmware and other types of firmware	✓	✓	✓
Component hardware and firmware configuration	✓	✓	
Trusted Platform Module state	✓	✓	

HARDENING_

Eclypsium analyzes low-level components for vulnerabilities and misconfigurations that affect the security posture of the device. This makes it easy to prioritize issues for remediation. Eclypsium can help apply updates in most cases, although this can vary by manufacturer.

	Clients	Servers	Network Devices
Find Devices with Affected Components When a new issue is first discovered, organizations need to assess their impact by tracking down which devices include the specific components affected by the issue. This requires component-level visibility.	✓	✓	
Find Out-of-Date Firmware Find devices that have outdated firmware that may be affected by vulnerabilities or other issues.	✓	✓	✓
Find Vulnerabilities Identify devices with vulnerabilities and CVEs affecting hardware and firmware components that are often missed by traditional software vulnerability scans.	✓	✓	✓
Sort Devices by Risk Quickly sort devices based on their cumulative risk. Filter by OS, group, vendor, product, component, security feature, vulnerability to further refine the view.	✓	✓	✓
Search by Vulnerability Search and investigate specific vulnerabilities and find all devices that are affected and have been scanned for specific vulnerabilities.	✓	✓	✓
Find Device Misconfigurations Identify configuration issues that can put the device at risk such as disabled BIOS write protections or unlocked components such as SMI or Flash descriptors.	✓	✓	✓
Patch Management and Updates* Remediate problems directly through the Eclypsium console or via API to download and install firmware updates.	✓	✓	✓

* Capabilities vary depending on manufacturer and model.

DETECTION AND RESPONSE_

Eclypsium uses a variety of mechanisms to detect indicators of compromise for attacks that are designed to evade EDR and other security controls. When a new supply chain threat is discovered, Eclypsium can help your organization mount a rapid response by identifying and remediating vulnerable components in your supply chain and looking for signs of exploitation in your environment.

	Clients	Servers	Network Devices
Changes to Baselines Quickly identify any devices that deviate from their baseline to easily recognize when high-value systems have unexpected or unplanned changes. Baselines can also be applied to groups of devices.	✓	✓	✓
Detection of Unknown Binaries Eclypsium maintains the industry's most extensive library of known vendor firmware and can identify any firmware that is not on this continuously maintained allow list.	✓	✓	✓*
Detection of Known Threats Detect the presence of a wide variety of known threats such as rootkits, hardware implants, and backdoors. Users can import and define their own firmware-specific YARA rules.	✓	✓	✓
Detection of Behavioral Anomalies Eclypsium creates and analyzes heuristic models of system behavioral data to reveal anomalies that can indicate a potential threat. For example, it would help to detect a firmware implant utilizing hardware mechanisms to avoid detection.	✓	✓	
Dynamic Alerting Configurable alerts let you monitor groups of devices for specific vulnerabilities or indications of compromise and notify security operations or incident response teams.	✓	✓	✓
Supply Chain Threat Response When a new vulnerable or suspect component becomes known, Eclypsium equips security teams to quickly identify affected systems.	✓	✓	✓
Automated Responses A powerful REST API integrates with other enterprise security tools such as SIEM and SOAR solutions to trigger automated responses and playbooks.	✓	✓	✓

* Capabilities vary depending on manufacturer and model.

SUPPORTED ASSET TYPES_

Clients

Eclypsium supports a wide range of endpoint devices, including laptops, workstations, and tablets, as well as specialized equipment using modern computing platforms, such as automated teller machines (ATMs) and point-of-sale systems. Eclypsium supports Windows, macOS, and many Linux distributions and runs on virtually all x86 based platforms, including systems from Apple, Asus, Dell, Fujitsu, HP, Lenovo, Quanta, and Toshiba.

For details on supported operating systems, hardware, and chipsets, visit **eclypsium.com/platform/specs/**

Servers

Eclypsium supports a wide range of servers and microservers and their underlying components. Eclypsium supports Windows and many distributions of Linux, and runs on virtually all x86 based platforms including servers from Dell, HPE, Lenovo, Quanta, and Supermicro, etc. Eclypsium also supports firmware integrity monitoring as well as risk and patch management within VMware ESXi environments.

For details on supported servers and microservers, visit **eclypsium.com/platform/specs/**

Network Devices

Eclypsium supports a wide range of routers, switches, gateways, VPN appliances, security appliances, and other products from vendors including Arista, Cisco, Citrix, Extreme Networks, F5, Fortinet, HPE Aruba, Juniper, Palo Alto Networks, and Pulse Secure.

SUPPORTED HARDWARE_

- Intel Core- and Core M-based systems, 2nd generation or later
- Intel Xeon-based servers
- Intel Atom-based systems
- AMD Zen-based systems
- Apple M1, M2

For details on supported hardware, visit **eclypsium.com/platform/specs/**

INTEGRATIONS_

In addition to a powerful REST API that allows for ad hoc integrations, the following tested integrations are available:

Deployment	Additional Visibility and Analysis
• Airwatch by VMWare • Microsoft SCCM • JAMF • Tanium • Microsoft Intune	• Intel intelligence feeds

System Access and Authentication	Security Analytics
• Cloudflare Access • Ping Identity • Okta • Google SSO	• Kenna Security • Splunk

DEPLOYMENT_

The Eclypsium Analytics Service is a SaaS and runs on a cloud instance. An on-premises deployment is possible where required.

DATA COLLECTION_

The Eclypsium supply chain security platform offers several methods for monitoring and remediating devices.

Eclypsium Endpoint Sensor

The Eclypsium endpoint sensor offers robust monitoring and remediation options for clients and servers. This sensor uses a kernel driver to collect system data and sends metadata to the cloud analytics service over an encrypted and authenticated channel. The sensor also performs real-time analysis of running system configuration and operation to detect implants and suspicious behavior.

The sensor can be deployed in two modes: as a continuously running service (persistent deployment) or as a temporary running application (ephemeral deployment). The sensor also has multiple configuration options to enable flexibility in deployment and trade-off between depth and speed of scan. The ephemeral deployment can even be run during boot to avoid any runtime interaction.

Remote Scans

Eclypsium has also developed methods of remotely scanning infrastructure devices, including network equipment and servers. Eclypsium uses either authenticated or unauthenticated remote interfaces (such as SSH, Redfish, or vSphere APIs) to collect data and perform remediation on supported infrastructure devices.