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, cloud infrastructure like VMware, and network devices. Additional specifics about support are available on our website through hyperlinks below.

INFRASTRUCTURE INVENTORY_

Eclypsium creates an inventory of all IT infrastructure assets like PC and Mac endpoints, servers, network infrastructure devices, enterprise connected IoT devices and cloud (virtual) infrastructure, down to their hardware, firmware and software components. The level of details can vary by vendor and model.

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.

Device State and Configuration

- Baseboard
- Processor, chipset, and system-on-chip
- Storage
- Network (management interface, baseband/wireless)
- Peripheral devices

Firmware and Software

- System and device-level firmware (UEFI, BIOS, etc)
- Network OS firmware (Cisco IOS, Juniper JunOS, Palo Alto Networks PAN-OS, Fortinet FortiOS, F5 Networks TMOS, etc.)
- PC boot-level firmware and bootloaders (UEFI GPT and MBR)
- PC operating system (kernel and device drivers)
- Processor microcode and firmware microcode and expansion firmware)
- Network and wireless firmware
- Graphics firmware
- Storage firmware
- Server management firmware (BMC, iLO, iDRAC, EMS, MegaRAC, Intel SPS, etc.)
- PC management (Intel Management Engine)
- Security components and firmware (discrete TPM, integrated firmware TPM, AMD Platform Security Processor, Intel CSME, etc.)
- Peripheral devices (including microcode and expansion firmware)

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.

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.

Prioritize Supply Chain Vulnerabilities

Identify devices with vulnerabilities and CVEs affecting hardware and firmware components that are often missed by traditional software vulnerability scans. Eclypsium goes beyond CVE mapping, analyzing binaries, configurations, update packages, vendor advisories, and dynamic analysis of extracted firmware and software.

Correlate Impacted Components with Assets

Discover which assets contain a specific vulnerable or suspect hardware, firmware, or software component.

Discover Misconfigured Infrastructure

Identify unused, disabled, or misconfigured features, such as: measured or trusted boot protections, root of trust security, firmware storage protections, signature enforcement, hypervisor-based security, DMA protections, signed firmware and software updates, Trusted Platform Modules, integrity protections, Trusted Execution Environments and Technologies (TEE, TXT), CPU security, memory protections, etc.

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.

Monitor Drift and Deviations from 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.

info@eclypsium.com
eclypsium.com

Verify Integrity and Detect Unexpected Modifications 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.
Detect Compromise Detect both known and unknown threats, including persistent implants, backdoors, or malicious alterations delivered through the supply chain. Eclypsium employs a number of detection techniques including binary analysis, dynamic analysis, emulation, integrity verification, local and global known-good state, machine learning, and analysis of logs for indicators of compromise.
Dynamic Alerting Configurable alerts let you monitor groups of devices for indications of compromise and notify security operations or incident response teams.
Supply Chain Threat Response Assess the impact of newly announced supply chain threats. Eclypsium stores historical assessment data and analysis results, correlates suspect components with assets, captures information about modified and malicious modules, and components, and configurations.
Automated Responses A powerful REST API integrates with other enterprise security tools such as SIEM and SOAR solutions to trigger automated responses and playbooks.

SUPPORTED INFRASTRUCTURE_

Endpoint Devices

Eclypsium supports many 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, Gigabyte, HP, Lenovo, Microsoft, MSI, and Toshiba.

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

Physical and Virtual Servers

Eclypsium supports 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 Cisco, 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 and Cloud Infrastructure

Eclypsium uniquely provides visibility for routers, switches, gateways, VPN appliances, security appliances, and other products from more than 30 vendors including Arista, Cisco, Citrix, Extreme Networks, F5, Fortinet, HPE Aruba, Juniper, Dell, Palo Alto Networks, Pulse Secure, Check Point, NetApp, and Accellion.

Many organizations are using both public and private cloud virtual infrastructure, such as VMware vSphere, F5 BIG-IP Virtual Edition, and other virtual appliances. Eclypsium is continuously adding capabilities to monitor and assess risk with this type of modern infrastructure.

SUPPORTED HARDWARE_

Eclypsium supports x86-based and Apple hardware. For details on supported hardware, visit **eclypsium.com/platform/specs/**

INTEGRATIONS_

A powerful REST API enables integrations for fleet deployment, intelligence feeds, system access and authentication, and security operations tooling.

DEPLOYMENT_

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

INFRASTRUCTURE ASSESSMENT_

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

User Endpoints

For PC and Mac endpoints, the Eclypsium sensor offers configuration options to enable flexibility in deployment and trade-off between depth and speed of assessment. 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 can be deployed in two modes:

1. As a continuously running service (persistent deployment)
2. As a temporary running application (ephemeral deployment) for one-time assessments

Server Infrastructure

For servers, Eclypsium offers two methods of assessment:

1. A sensor that supports server-specific components and firmware
2. Remote assessment through the Redfish remote server management interface

Network and Cloud Infrastructure

For network devices, Eclypsium conducts authenticated remote assessments through vendor-provided management interfaces like F5 Network iControl or SSH.

For cloud infrastructure like VMware, Eclypsium performs remote assessments using several methods:

1. Over VMware ESXi and vSphere APIs
2. Automated collection and analysis of VMware ESXi support bundles
3. A bootable assessment tool