PRODUCT BRIEF

Eclypsium for Endpoints

OVERVIEW

From the most widespread ransomware campaigns to advanced nation-state adversaries, attackers are increasingly turning to vulnerabilities and threats at the firmware layer in order to evade detection and subvert traditional security controls. The Eclypsium firmware security platform brings simple, automated security to this all-important layer, allowing organizations to easily Identify, Verify, and Fortify the firmware and hardware within end-user devices including laptops and desktop systems.

For the first time, security teams can have a single efficient tool to automate firmware-level device inventory, vulnerability assessment, patching, threat detection and response, and supply chain risk management for all their end-user assets.

Firmware Attacks in the Wild

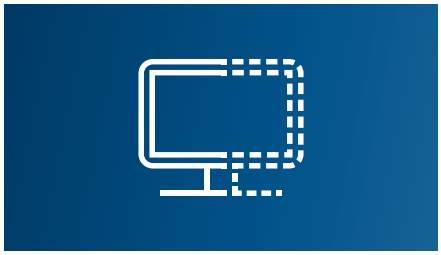
As OS-level security has improved, attackers of all types have increasingly shifted their focus to the relatively unguarded firmware layer. Trickbot, one of the most common forms of malware in the wild and a key enabler of ransomware, has added functionality to automatically scan devices for vulnerabilities at the firmware level. Vulnerable devices can be easily compromised with firmware-level implants such as the recently discovered MosaicRegressor implant, which can give attackers virtually unlimited control and persistence within a device.

CORE FUNCTIONALITY

Eclypsium for Endpoints is a cloud-based firmware security solution that gives teams full visibility and control over their many endpoint devices. Key capabilities include the ability to:

Identify

Establish automated and continuous visibility into the firmware, hardware configuration, and components within your endpoint devices. Quickly zero in on important devices, attributes, or changes that can impact your security.



Verify

Verify the integrity of all firmware and detect known and unknown firmware threats including rootkits, implants, and backdoors. Proactively identify risks from outdated or vulnerable firmware or device misconfigurations.

Fortify

Remotely apply patches or updates to proactively mitigate device risks. Receive automated alerts to any firmware integrity changes and drive automated responses via integration with your existing IT and security tools with pre-built integrations with leading SIEMs, vulnerability management, and device management tools.

COMMON USE CASES

Ransomware and Advanced Threat Protection

Proactively detect the presence of firmware-focused ransomware and malware. Ensure devices are free from firmware implants and backdoors. Receive automated alerts to any firmware integrity changes.

Cloud-Based Remote Updates and Patching

Keep devices in a secure state by remotely patching or updating out-of-date or vulnerable device firmware. Assess corporate and BYOD devices used remotely for firmware vulnerabilities and misconfigurations that put devices at risk. Ensure all devices including BYOD devices are configured to use hardened firmware settings.

Security for Remote and Traveling Workers

Monitor the integrity of end-user devices that are deployed remotely or are traveling in high-risk areas. Receive automated alerts to any changes in device integrity and find weaknesses in device posture that could put the device at risk.

Supply Chain Risk Management

Directly ship new devices to remote workers, while validating their firmware is safe and has not been compromised in the supply chain. Evaluate newly acquired systems to proactively identify any vulnerabilities or unexpected changes to SBOM.

DETAILED FEATURES AND CAPABILITIES

IDENTIFY: ENDPOINT VISIBILITY AND INVENTORY

Eclypsium collects and analyzes detailed information from a variety of 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. This ensures security teams can have up to date detailed visibility into all their endpoints including:

- **Basic 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 Option (Expansion) ROM firmware.
- **Device, Component, and Other Firmware Details** – Bootloader information, component hardware and firmware configuration, Trusted Platform Module state, vendor-specific firmware, and other types of firmware.

VERIFY: VULNERABILITY ASSESSMENT AND INTEGRITY

Eclypsium analyzes endpoint firmware and hardware configurations for issues that affect the security posture of the device. This makes it easy to identify andvestigate devices based on their risk and then apply updates as available to remediate the risk. Key capabilities include:

- **Find Out-of-Date Firmware** - Find endpoints that have outdated firmware that may include vulnerabilities or other device issues..
- **Find Vulnerabilities** - Identify devices with vulnerabilities and CVEs affecting system or component firmware that are often missed by traditional software vulnerability scans.
- **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.
- **Sort Endpoints 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 endpoints that are affected and have been scanned for specific vulnerabilities.

VERIFY: THREAT DETECTION AND RESPONSE

Eclypsium analyzes endpoints for any signs of active threats. This includes detection of both known and unknown threats as well as ongoing verification to identify any unexpected changes to device integrity.

- **Changes to Device Baseline** - Quickly identify any devices with changes to their baseline to easily recognize when high-value systems have unexpected or unplanned changes.
- **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 white 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.
- **Abnormal Behavior** - Firmware behavior is often very predictable, and Eclypsium can analyze firmware to reveal anomalous behavior or functionality that can indicate a potential threat.

FORTIFY: PATCHING, REMEDIATION, AND THREAT RESPONSE

Eclypsium gives teams the tools to proactively solve problems and mitigate firmware risk. Security teams can easily update firmware and device code to remediate vulnerabilities and trigger automated alerts and workflows to respond to security events.

- **Patch Management and Updates** - Remediate problems directly through the Eclypsium console or via API to download and install firmware updates.
- **Automated Responses** - Powerful REST API integrates with other enterprise security tools such as SIEM and SOAR solutions to trigger automated responses and playbooks.
- **Dynamic Alerting** - Configurable alerts let you monitor groups of devices for specific vulnerabilities or indications of compromise and notify endpoint operation or incident response teams when they are detected.
- **Emergency Patching** - When vulnerabilities or configuration errors become actively exploited in the wild, multiple methods are available to hot-fix firmware updates.

ECLYPSIUM FOR ENDPOINTS: SUPPORTED DEVICES

Eclypsium supports a wide range of endpoint devices, including laptops, workstations, and tablets. Eclypsium supports the Windows, macOS, and Linux operating systems and runs on virtually all x86 based platforms, including systems from Apple, Asus, Dell, Fujitsu, HP, Lenovo, Quanta, and Toshiba.

Supported Operating Systems

The following Operating Systems are supported in their 64-bit variants:

- Windows 7, 8, 8.1, 10
- macOS 10.12 (“Sierra”), through 11.4 (“Big Sur”)
- Windows Server 2012, 2016, 2019
- Ubuntu 16.04 - 21.04
- Debian 8.x - 11.x
- RHEL/CentOS 6 - 8, Current Fedora distributions
- SLES 11 - 12, OpenSuse Leap 15, OpenSuse Leap 42.3

Supported Hardware and Chipsets

- **Intel Systems** - Eclysium supports all Intel systems from the Intel 2nd generation (code name “Sandy Bridge”) or later,including Intel Core, Core M, Xeon, and Atom-based systems.
- **AMD Systems** - Eclypsium supports AMD Zen and Zen2 generation CPUs including:
  - Ryzen 1xxx - 3xxx series models
  - EPYC 7xxx series models

INTEGRATIONS

The Eclypsium platform integrates with popular deployment and security tools, making it easy to manage and secure enterprise devices down to the firmware and hardware level. A powerful REST API lets organizations integrate Eclypsium with their existing tools and processes. Verified integrations include:

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

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

ABOUT ECLYPSIUM

Eclypsium is the enterprise firmware security company. Our comprehensive, cloud-based platform identifies, verifies, and fortifies firmware and hardware wherever it exists in your extended global networks: in laptops, tablets, servers, network gear, and connected devices. The Eclypsium platform secures against persistent and stealthy firmware attacks, provides continuous device integrity, delivers firmware patching at scale, and prevents ransomware and malicious implants. Serving security-conscious Fortune 1000 enterprises and federal agencies, Eclypsium was named a Gartner Cool Vendor in Security Operations and Threat Intelligence, a TAG Cyber Distinguished Vendor, one of the World’s 10 Most Innovative Security Companies by Fast Company.