PRODUCT BRIEF

Eclypsium for Servers

OVERVIEW

Attackers naturally seek out the most high-value targets, and for most enterprises, this means their servers. These critical assets have become the ultimate goal for today's "big game hunting" ransomware and attackers seeking to inflict the maximum amount of damage to an organization. These and other threat actors are increasingly turning to vulnerabilities and threats at the firmware layer in order to evade 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, hardware, and components within their servers whether hosted in local, cloud, or hybrid environments. For the first time, security teams have a single tool to automate firmware-level device inventory, vulnerability assessment, patching, threat detection and response, and supply chain risk management for their entire fleet of server infrastructure.

Firmware Attacks in the Wild

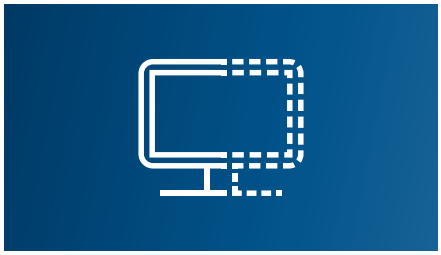
Firmware attacks are on the rise and servers are fast becoming attackers' favorite targets. Recent industry analysis has shown that 80% of enterprises have suffered a firmware attack in the past two years. At the same time, ransomware operators have heavily focused on servers both to cause disruption and to steal data as part of "double extortion" schemes. For example, the Cl0p ransomware group recently targeted Accellion File Transfer Appliances to steal and extort payment from enterprises. Likewise, the DarkSide ransomware group behind the Colonial Pipeline has both been known to target firmware and steal data from enterprise servers as part of their attacks.

CORE FUNCTIONALITY

Eclypsium for Servers is a cloud-based firmware security solution that gives teams full visibility and control over their many servers both locally and in the cloud. Key capabilities include the ability to:

Identify

Establish automated and ongoing visibility into the firmware, hardware configuration, and the dozens of components within your enterprise servers. Quickly zero in on important devices, components, 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 enabling malware. Ensure devices are free from firmware implants and backdoors. Receive automated alerts to any firmware integrity changes.

Cloud-Based Remote Validation, Updates, and Patching

Keep servers in a secure state by remotely patching or updating out-of-date or vulnerable device firmware. Remotely assess bare-metal service providers and devices for firmware vulnerabilities and misconfigurations that can put the device at risk. Verify that firmware of re-provisioned servers was properly reflashed and in a known good state. Ensure that all devices are properly configured to use hardened firmware settings.

Supply Chain Risk Management

Evaluate equipment vendors or service providers before purchasing to identify vulnerabilities or insecure components or configurations. Verify newly acquired systems to ensure they have not been compromised in the supply chain and to proactively identify any vulnerabilities or unexpected changes to SBOM.

Secure Virtualized Environments Down to the Hardware

Virtual environments still rely on hardware, and any vulnerabilities or threats in the firmware of the physical host can put virtualized assets at risk. With Eclypsium, teams can ensure their virtualization strategy is built on a secure hardware foundation. Easily monitor the integrity, find vulnerabilities, and apply appropriate updates to the underlying hardware supporting their VMware ESX environments.

DETAILED FEATURES AND CAPABILITIES

IDENTIFY: SERVER VISIBILITY AND INVENTORY

Eclypsium collects and analyzes detailed information from a variety of low-level components including system UEFI and BIOS firmware, BMC firmware, processors and chipsets, PCI devices, networking components, storage drives, PCIe devices, 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 all firmware and device configurations for issues that affect the security posture of the device. This makes it easy to identify and investigate devices based on their risk and then apply updates as available to remediate the risk. Key capabilities include:

- **Find Out-of-Date Firmware** - Find servers that have outdated firmware that may include vulnerabilities or cause other performance or stability 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 Devices by Risk** - QQuickly 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.

VERIFY: THREAT DETECTION AND RESPONSE

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

- **Changes to Device Baseline** - Quickly identify any devices with changes to their baseline to easily recognize when high-value systems have any 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** - Detects 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 AND AUTOMATED 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.

ECLYPSIUM FOR SEVERS: SUPPORTED DEVICES

Eclypsium supports a wide range of server manufacturers, devices, and their underlying components. Eclypsium supports Windows Linux operating systems 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 ESX environments.

Supported Operating Systems

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

- 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
- Windows 7, 8, 8.1, 10
- macOS 10.12 (“Sierra”), through 11.4 (“Big Sur”)

Supported Hardware and Chipsets

- **Intel Systems** - Eclypsium supports all Intel systems from the Intel 2nd generation (code name “Sandy Bridge”) or later. This includes a wide variety of devices 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.