PRODUCT BRIEF

eclypsium®

Eclypsium for Network Devices

OVERVIEW

Enterprise network devices such as VPNs, switches, firewalls, routers, and a wide range of of concentrators, gateways, and controllers have quickly become the favorite targets of top ransomware families as well as nation-state threat actors. However, unlike traditional servers and laptops, network devices are rarely updated. Further, they can't be protected by traditional security agents and often have vulnerabilities within the fundamental device code and firmware that are missed by simple vulnerability scans.

The Eclypsium firmware security platform brings simple, automated security to this all-important layer, allowing organizations to easily Identify, Verify, and Fortify the software, firmware, hardware, and components within their network devices. For the first time, security teams have a single tool to easily automate security down to the firmware layer for their fleet of network devices including device discovery, vulnerability assessment, patching, threat detection and response, and supply chain risk management.

Firmware Attacks in the Wild

Beginning in late 2019, the U.S. security agency CISA began issuing a series of alerts detailing nation-state attacks originating from Russia, China, and Iran targeting a wide variety of network devices from enterprise vendors including PulseSecure, Cisco, Citrix, F5, Fortinet, and Juniper. Attackers were able to consistently exploit vulnerabilities in these devices as a way to gain initial access into an environment and spread additional malware payloads. These techniques have since been adopted by some of the most popular ransomware operations including REvil, Ryuk, Conti, and Netwalker, which ultimately have impacted hundreds of enterprises.

CORE FUNCTIONALITY

Eclypsium for Network Devices is a cloud-based firmware security solution that gives teams full visibility and control over their fleet of network devices and networking infrastructure without the need to install agents on the devices themselves. Key capabilities include the ability to:

Identify

Automated discovery of network devices and ongoing visibility into the firmware, hardware configuration, and the dozens of components within your network devices and infrastructure. 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 identify network devices with vulnerabilities that are being actively exploited by ransomware in the wild. Detect firmware-focused ransomware and malware. Ensure devices are free from firmware implants and backdoors. Receive automated alerts to any firmware integrity changes.

Agentless Discovery and Analysis of Network Devices

Eclypsium's agentless solution uses managed endpoints to automatically discover network devices in the enterprise environment. This unique distributed approach means security teams don't have to install a security agent on their network devices, allowing teams to easily get security visibility into devices without adding additional code or waiting on change windows.

Risk Assessment and Remediation

Automatically identify network devices with vulnerabilities and misconfigurations that can put the device at risk and prioritize the vulnerabilities being targeted in real-world attacks. Verify the integrity of devices and detect known and unknown threats. Keep devices in a secure state by remotely patching or updating out-of-date or vulnerable device firmware. Support for updating firmware varies by vendor.

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.

DETAILED FEATURES AND CAPABILITIES

IDENTIFY: DEVICE DISCOVERY AND INVENTORY

Eclypsium automatically discovers and identifies network devices in the enterprise environment. The platform then collects and analyzes detailed information from network devices including their components and configuration. Visibility options can vary by vendor and can include details such as:

- **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** - Firmware manufacturer, release dates, system and device manufacturers, model number, etc.

VERIFY: VULNERABILITY ASSESSMENT AND PATCHING

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 devices 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.
- **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.

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 in devices 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.

* Currently limited to Cisco devices.

ECLYPSIUM FOR NETWORK DEVICES: SUPPORTED DEVICES

Eclypsium supports a constantly-increasing number of network device vendors. Devices are supported with a mix of both authenticated, deep scanning and un-authenticated network-based scanning. Deep, authenticated scan include network and security devices from:

- Cisco
- Juniper
- F5
- Arista
- Pulse

Unauthenticated, network-based scans can secure firmware found in:

- Citrix
- Checkpoint
- Fortinet
- HPE Aruba
- NetApp
- Palo Alto Networks
- And many more

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:

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.