ENTERPRISE DEVICE SECURITY

DEFENDING THE UNPROTECTED ATTACK SURFACE OF THE ENTERPRISE

The world's most sophisticated attackers have steadily relied on firmware implants due to their ability to subvert traditional security at the operating system level and to persist across system re-imaging and even hard drive replacement. However, recently these attack vectors have expanded beyond targeted attacks to large-scale campaigns facing every organization. We are rapidly entering an era where virtually all enterprises are facing these risks and threats, yet most are completely unprepared to address them.

> "By 2022, 70% of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability."
>
> —Gartner Research

ECLYPSIUM PROVIDES SCALABLE DEVICE MANAGEMENT AND PROTECTION FOR DISTRIBUTED ORGANIZATIONS

Eclypsium helps organizations manage and secure corporate and personal laptops, bare metal and cloud servers, network and storage appliances, routers and other devices. We provide the only scalable enterprise device security platform that protects you from threats to devices down to the firmware and hardware level. The Eclypsium platform provides security capabilities ranging from basic device health and patching at scale to protection from the most persistent and stealthiest threats.

COMPREHENSIVE DEVICE SECURITY AT SCALE

Get unmatched visibility into the health of your hardware inventory — down to each hardware component in every device.

Identify vulnerable and misconfigured devices, and mitigate threats with firmware patching.

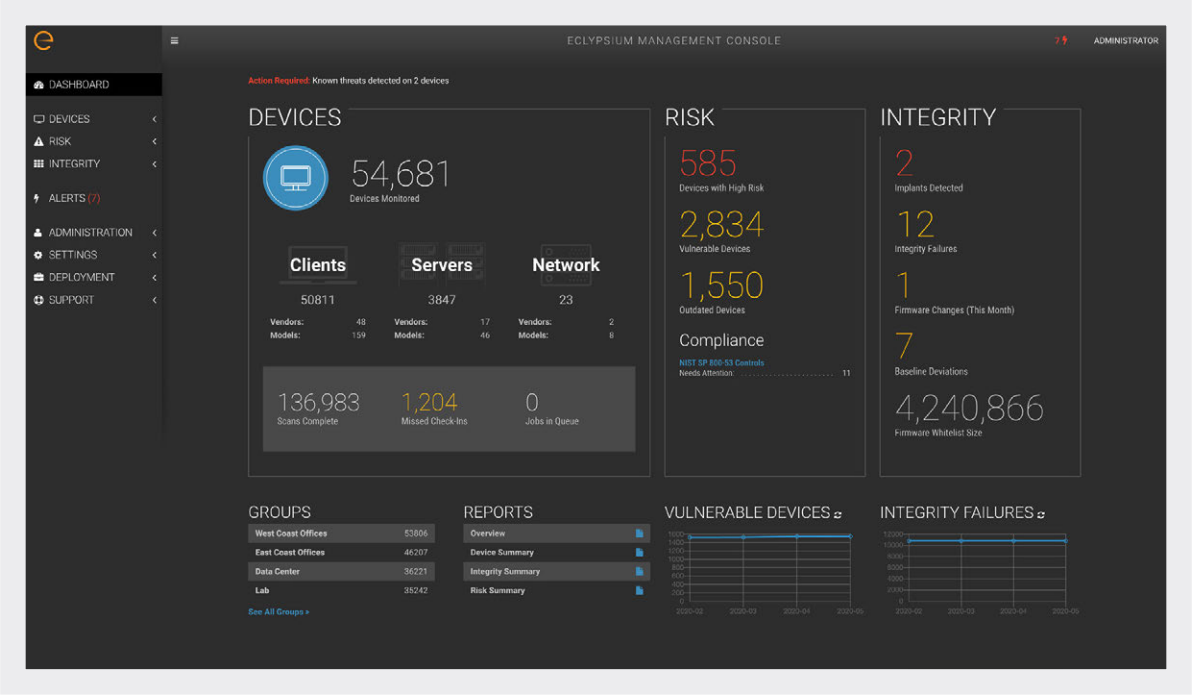
Detect compromised devices. Expose implants and device tampering invisible to traditional software security.

Manage risk, and simplify auditing and compliance with NIST, FISMA, PCI and other standards.

One of the world's largest multinational financial services firms uses Eclypsium to secure laptops from firmware and hardware threats.

DEFENDING THE FOUNDATION
OF THE ENTERPRISE

THE ECLYPSIUM PLATFORM



Comprehensive Device Monitoring

Maintain a complete view of your entire environment or focus on a specific group of devices, with insight into firmware and components so that you know your security posture at all times.

Gain visibility into weaknesses and threats to detect risks associated with hardware profile changes, tampering and compromise.

Device Risk and Vulnerability Scanning

Schedule regular or ad-hoc scans of devices for firmware vulnerabilities, outdated versions, hardware misconfigurations, and missing protections. Based on scan results take actions such as applying updates or quarantining devices.

Advanced Threat Detection

Detect and alert on threats such as hardware implants, backdoors and other malicious code. Leverage IOCs, static, behavioral, and heuristic analysis to find known or unknown threats or changes to firmware integrity.

The Industry's Largest Global Firmware Reputation Database

The Eclypsium Platform checks firmware against millions of firmware hashes across dozens of enterprise hardware vendors to identify changes to baselines, find outdated firmware, and expose tampering.

Device Analysis and Forensics

Detailed analysis & reporting of any firmware image enables digital forensics to gather evidence to investigate the context of any attack as well as identifying and limiting the exposure of a breach, as part of a complete incident response playbook. Easily share firmware samples with Eclypsium for expert analysis.

Firmware Patch Management

Eclypsium accelerates patching and update efforts, enabling staff to address weaknesses and save time. When threats are encountered, the platform can prevent damage, and robust APIs enable automated orchestration efforts such as quarantine of affected devices.

Protection For All Your Devices

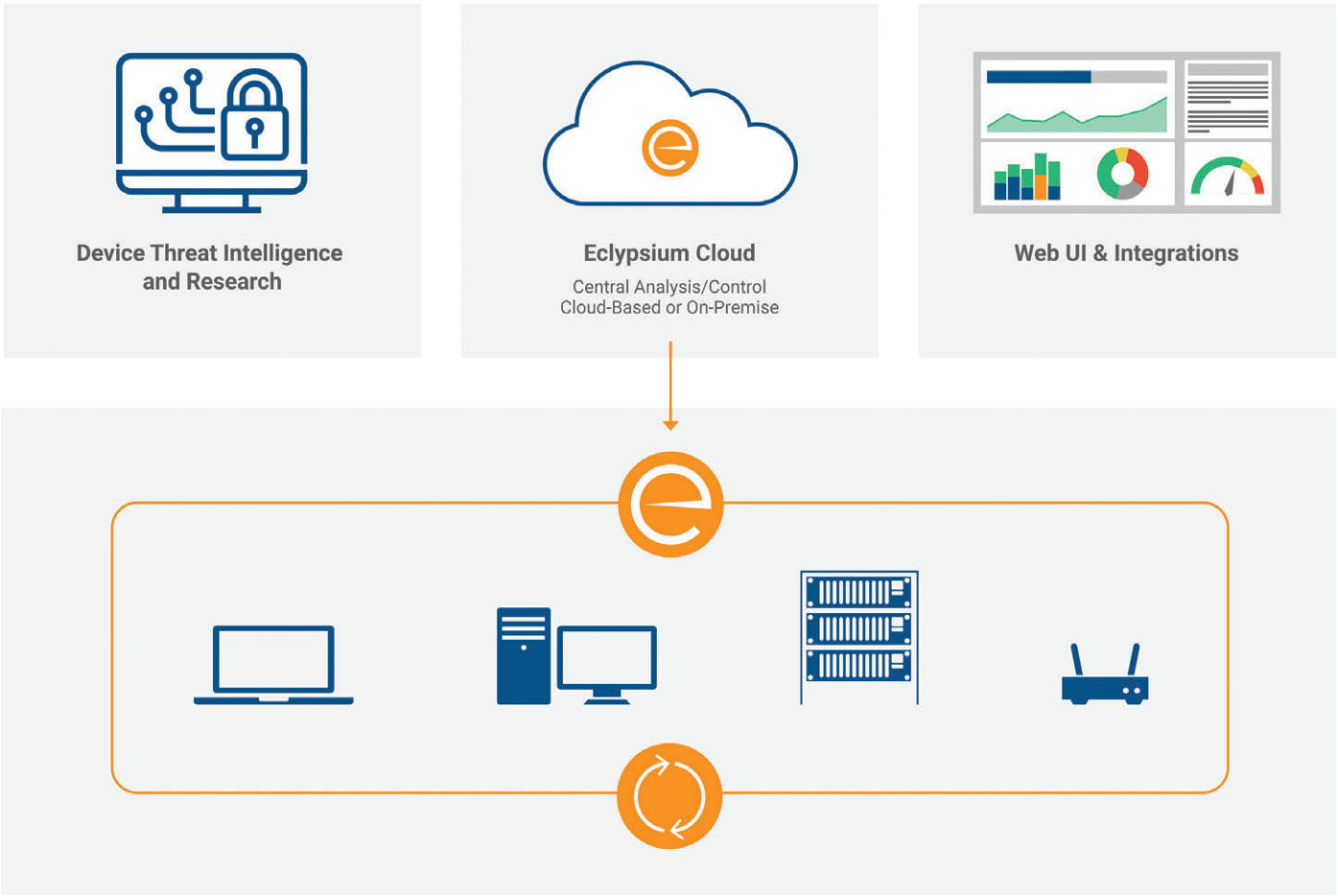
Eclypsium ensures all your critical devices are protected including laptops, servers, switches, routers and other systems. The platform supports a wide range of operating systems including Linux, Windows, MacOS, Cisco IOS, and more.

Broad Coverage For Components

Every device has dozens of components that all rely on firmware and have their own unique vulnerabilities and threat models. Eclypsium ensures you have the same visibility and security for these components including system UEFI and BIOS, processors and chipsets, PCI devices, server BMCs, networking components, peripheral devices, Trusted Platform Module, Intel's Management Engine and more.

Seamless Enterprise Integrations

Deploy Eclypsium with tools such as Microsoft SCCM, Intune or Tanium and manage access with popular SSO providers. Visualize event data through syslog or major SIEM providers including Splunk and QRadar. The Eclypsium Platform also provides a rich set of REST APIs for integration into your existing security solutions.



“We went from 0% work from home to 99% work from home and wanted to cover our remote access laptops as we consider all of them high risk assets at present.”

—Eclypsium Customer

Reduce Hidden Risk

With most devices containing at least one vulnerability, Eclypsium reveals the hidden attack surface that attackers see but that is invisible to traditional vulnerability scanners.

Find the Threats You've Been Missing

Attackers use firmware implants and backdoors because they are so successful at evading traditional security. Eclypsium detects the most stealthy and persistent threats.

Break the Cycle of Re-Infection

Firmware threats survive re-imaging so that attackers can immediately re-infect the host. Eclypsium provides simple, automated tests to ensure that devices are truly clean before they are returned to operation.

Meet Compliance Standards

Eclypsium equips you with the tools you need to assess your firmware security vulnerabilities and risks, take action and demonstrate your compliance with NIST and other requirements down to the firmware and hardware level.

Save Time and Effort

Without Eclypsium, managing devices is a slow, laborious process that can easily overwhelm staff. Eclypsium automates the task of scanning and maintaining visibility, and accelerates the process of applying needed updates.

Stay Ahead of Attackers

Eclypsium's world-class firmware security research team leads the industry in identifying threats and vulnerabilities that impact enterprise devices. Their insights put you ahead of the curve on device security.

ABOUT ECLYPSIUM

The Eclypsium Platform is driven by years of experience and ongoing research into modern devices and the threats that target them. By deeply understanding attacks against firmware and hardware, we develop effective mechanisms to protect enterprise infrastructure. Headquartered in Portland, Oregon, our team includes many of the world's leading device security researchers.

That's why global financial services firms, critical infrastructure providers, leading manufacturers, and the US federal government rely on Eclypsium for comprehensive device management and security.

To learn more visit eclypsium.com or contact us at (833) FIRM-SEC.