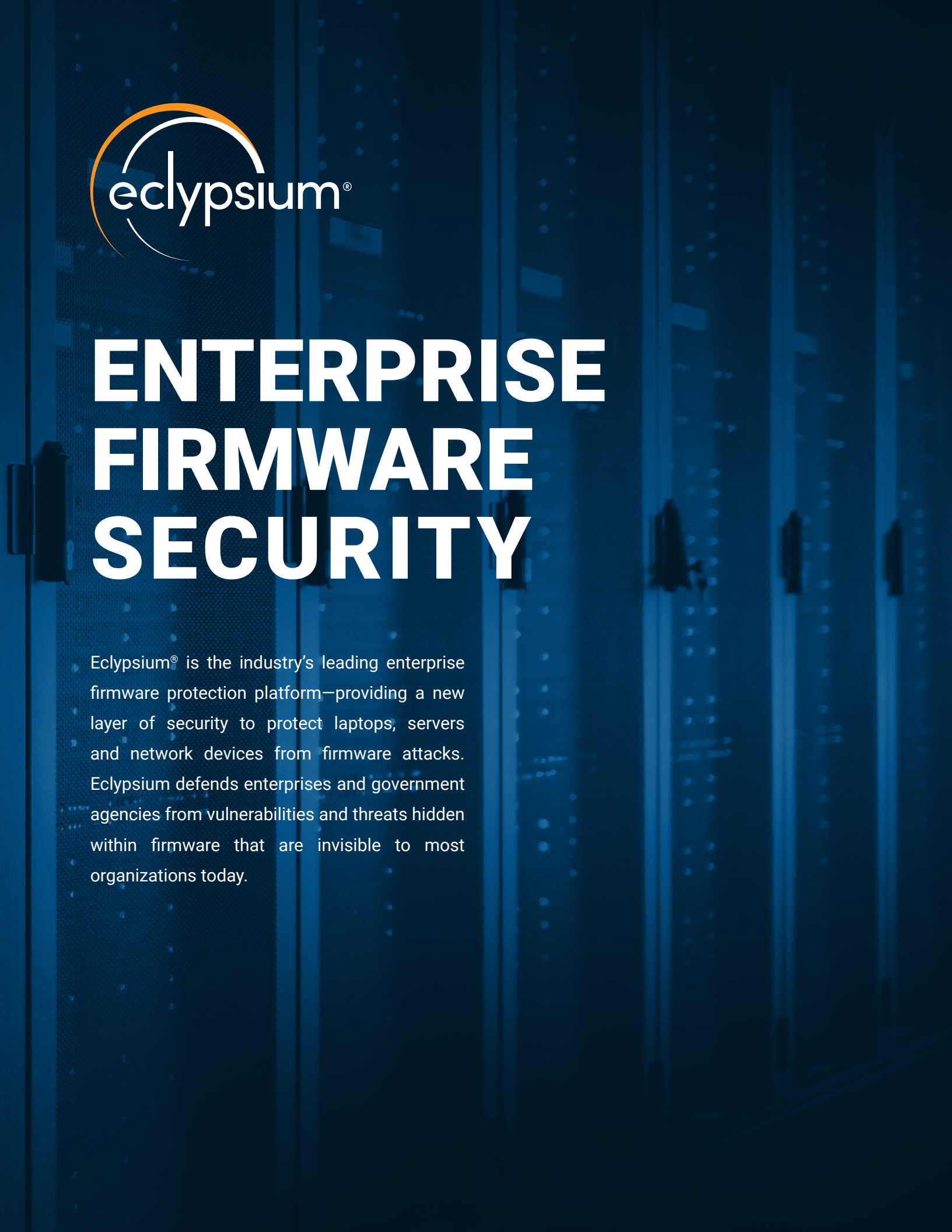


ENTERPRISE FIRMWARE SECURITY

Eclypsium® is the industry's leading enterprise firmware protection platform—providing a new layer of security to protect laptops, servers and network devices from firmware attacks. Eclypsium defends enterprises and government agencies from vulnerabilities and threats hidden within firmware that are invisible to most organizations today.

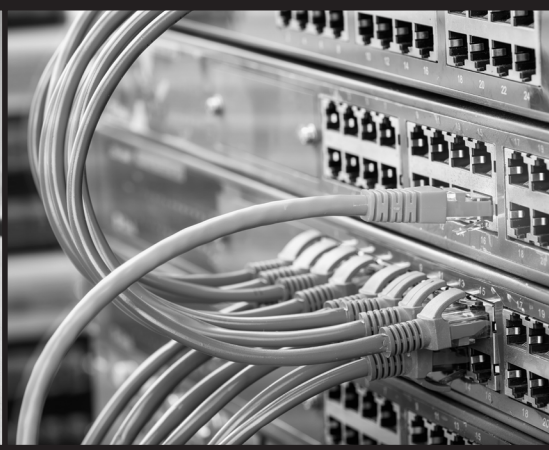
THE FIRMWARE SECURITY CHALLENGE

Firmware is the unguarded attack surface of the enterprise. Today's servers, laptops and networking equipment include dozens of components, each of which has their own complex software programming with millions of lines of code. Known as firmware, this ubiquitous component-level software is developed by a wide variety of manufacturers, runs independently from the operating system and is essential to the proper functioning of system hardware. As firmware has become more sophisticated, manufacturers have added new methods of maintaining and updating it, and that has introduced new attack vectors into enterprise devices.

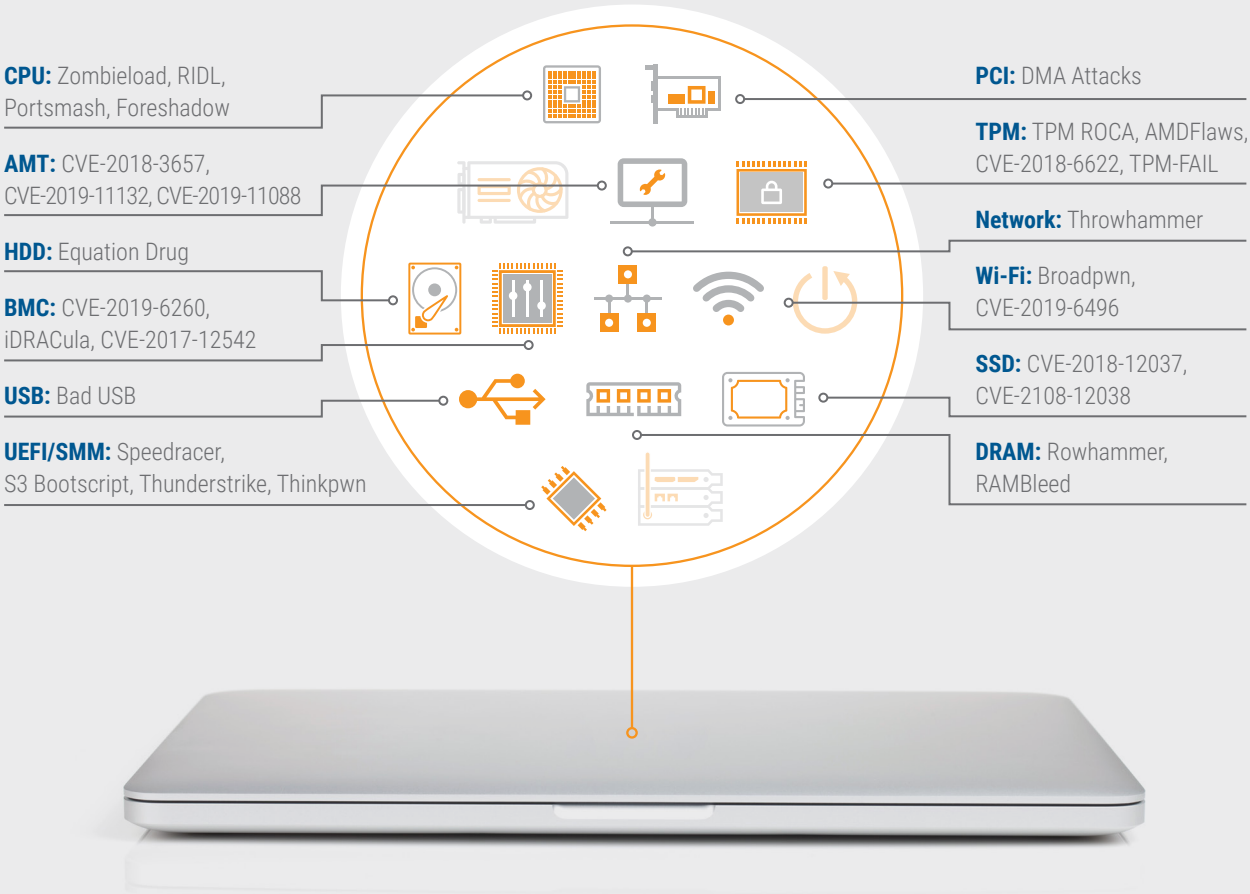
Most organizations lack visibility into this attack surface. They can't see what version of firmware is running in each component of an enterprise device, or determine whether it is vulnerable to known threats, much less detect a hidden implant or backdoor. Once compromised, this blind spot allows attackers to subvert traditional security controls and persist undetected, leaving you exposed to device failures, ransomware and data breaches.

That's why global financial services firms, critical infrastructure providers, leading manufacturers, and the US federal government have turned to Eclypsium. We provide the most complete defense against firmware attacks available - enabling you to see and manage risk across enterprise devices, and stop active threats from device-level implants and backdoors.





THE FIRMWARE SECURITY LANDSCAPE



Firmware is the bedrock of every device and all computing from an employee's laptop to the servers underlying cloud-based infrastructure. Firmware governs how a device boots, has the ability to modify the operating system, and largely runs in a layer that the operating system doesn't see or control. If compromised, malicious firmware can enable an attacker to subvert traditional security and silently persist without detection, even surviving a complete re-imaging of the device or installation of a new drive.

Just as importantly, firmware exists in virtually every component of a device from its chipset and processor, to drives, network adapters, graphics cards, memory, USB and PCI buses, and more. All of these components can be subject to attack. Compromises at this level can provide attackers with near unlimited power to see and modify data or disable devices completely.

FIRMWARE IS UNDER ATTACK

Firmware backdoors and implants have been a tool of choice for sophisticated attackers for years. However, in recent years firmware threats have become far more widespread due to the ready availability of tools, firmware knowledge, and a wealth of vulnerabilities for attackers to target.

FBI cybersecurity expert James Morrison recently cited vulnerabilities in firmware and hardware as one of the top growing cyberthreats as sophisticated criminals seek new ways to make money.

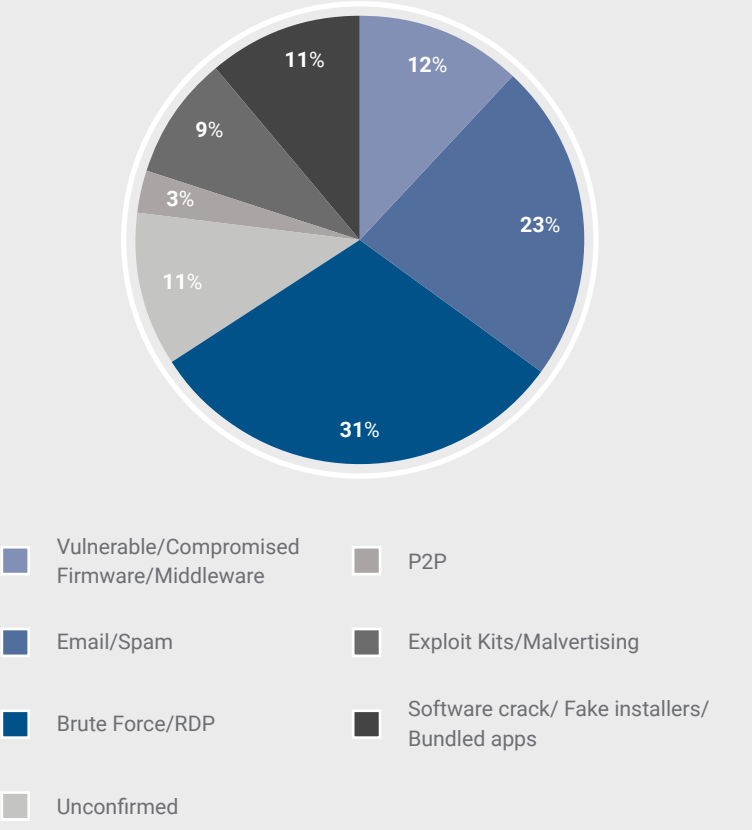
Recent analysis from F-Secure found that compromised firmware was the 3rd most common infection vector in 1H 2019, accounting for 12% of attacks disrupting companies, public entities and other organizations.

Widespread malware campaigns such as Lojax have used firmware to maintain persistence on infected devices, and a wealth of new vulnerabilities have enabled even unsophisticated attackers to target firmware.

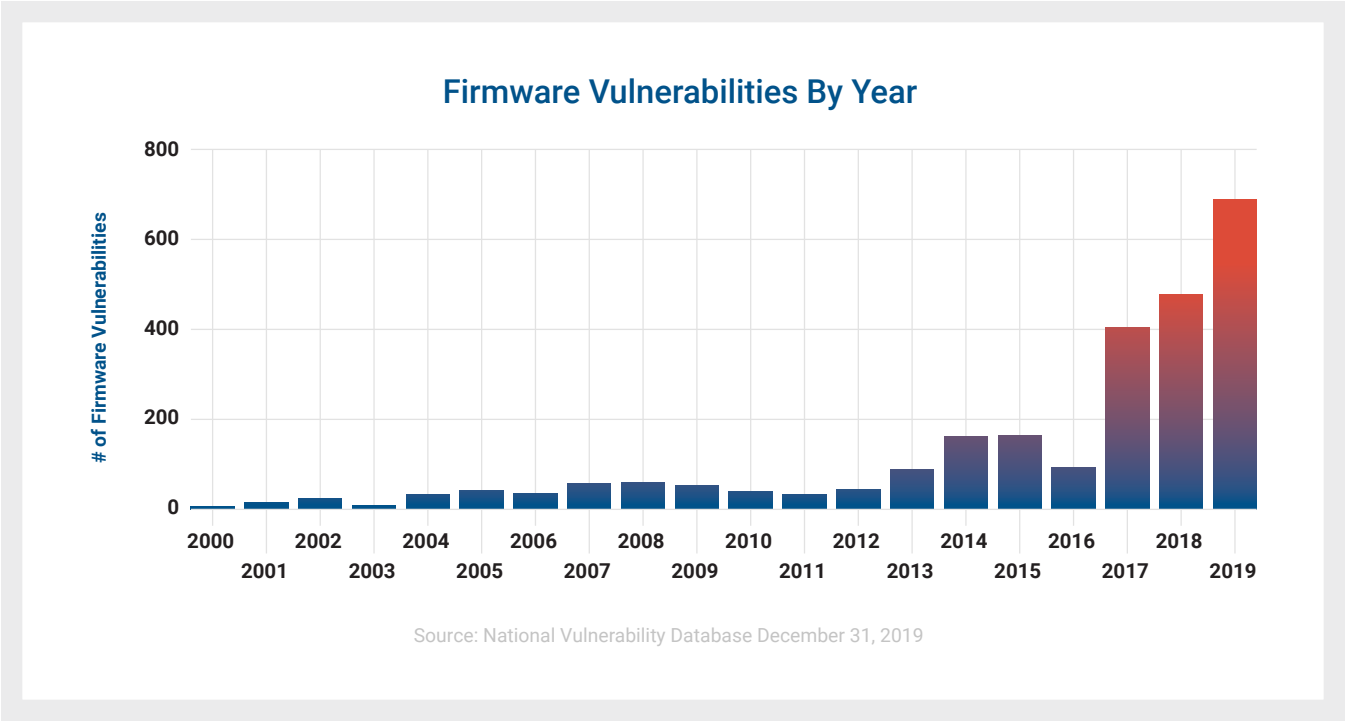
The FBI has warned that high-impact ransomware attacks threaten US businesses, organizations, and advised patching operating system, software, and firmware on devices as part of cyber defense best practices.

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

Ransomware Distribution Methods
(January-May 2019)



Source: F-Secure Attack Landscape H1 2019



FIRMWARE SECURITY IS ESSENTIAL

Compliance standards like the NIST Cyber Security Framework and PCI DSS repeatedly underscore the importance of firmware security as part of a modern security program. Yet, this area remains one of the most overlooked and poorly understood areas of risk within government agencies and enterprise security teams.

The number of firmware vulnerabilities reported to the National Vulnerability Database in 2019 is up more than 30% from last year, and is six times larger than three years ago. For IT teams tasked with protecting infrastructure from attack, the challenge of keeping up with firmware updates has grown significantly, and the severity of the issues demonstrates how big the gaps are in firmware security.

These trends have not gone unnoticed by industry analysts, with Gartner predicting that by 2022, 70% of enterprises without a firmware upgrade plan will be breached due to a firmware vulnerability. As firmware risks and threats become mainstream, it is incumbent on organizations to build the appropriate defenses to meet this growing area of risk.

BUSINESS VALUE

As your firmware security partner, Eclypsium provides both unmatched security technology and talent to ensure your security operations remain highly effective and efficient. Here are a few key benefits that Eclypsium can bring to any organization:

Reduce Hidden Risk—With 99% of devices containing at least one vulnerability, Eclypsium reveals the hidden attack surface that attackers see but are 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 finds firmware threats whether they are known or unknown.

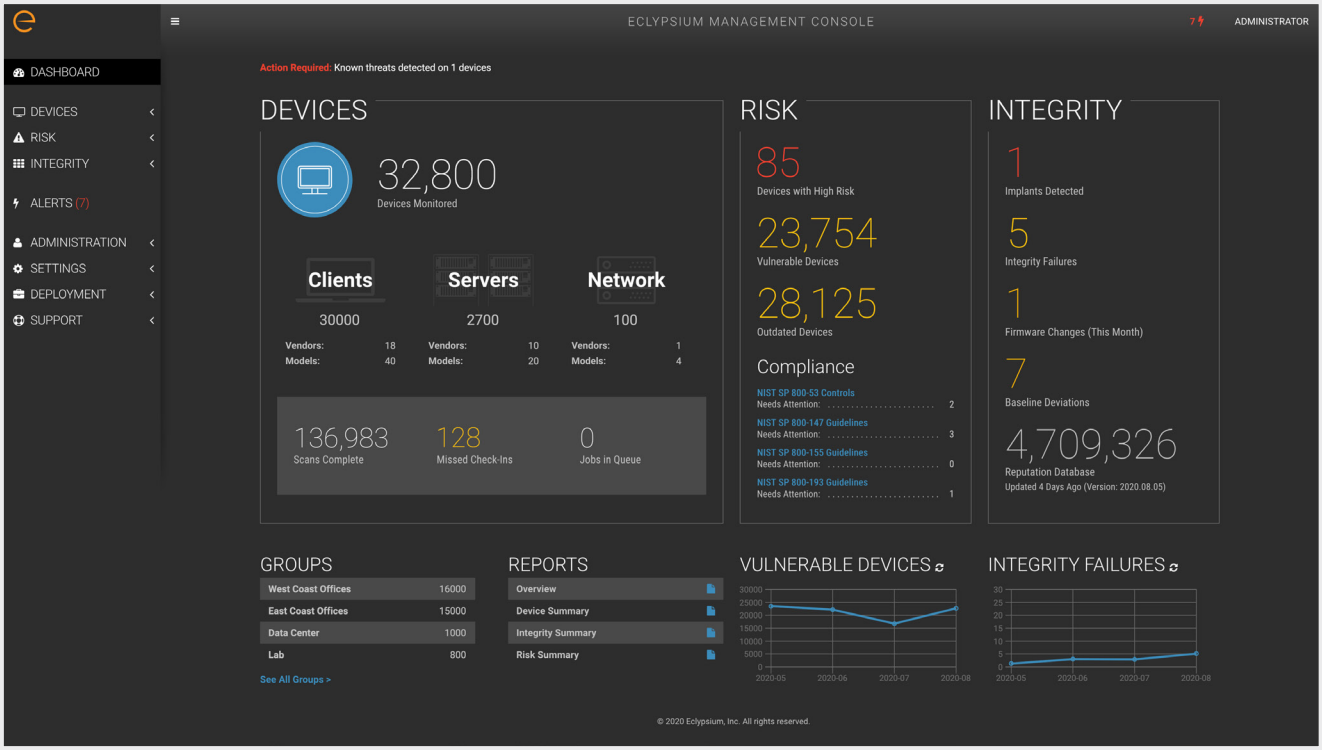
Break the Cycle of Re-Infection—Firmware threats survive re-imaging so that attackers can immediately re-infect the host. Eclypsium provides simple, automated tests to ensure that devices are truly clean before they are returned to operation.

Proactively Verify Your Supply Chain—Most supply chain security efforts are passive, such as choosing reputable vendors. Eclypsium lets you take proactive action to assess your prospective vendors and all new devices to verify their integrity and detect tampering.

Save Time and Effort—Without Eclypsium, managing firmware 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.

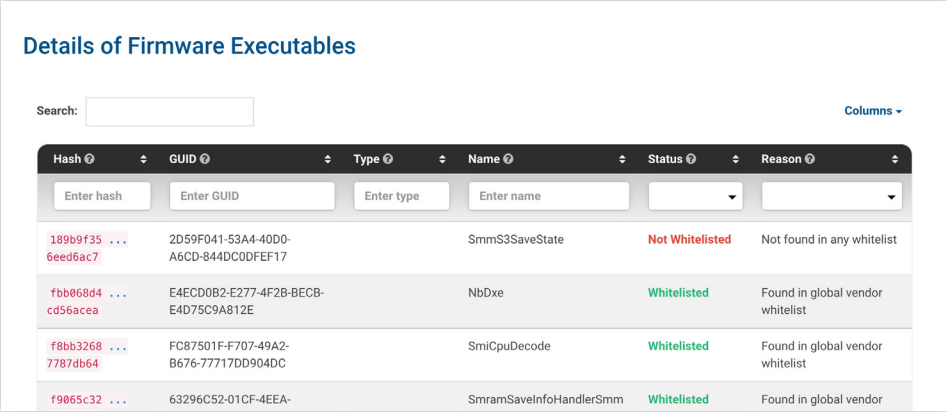
Built-in Firmware Experts—Security talent is in short supply, and firmware security skills are some of the hardest to find. If you find suspicious firmware, Eclypsium experts are there to analyze it for you.

THE ECLYPSIUM PLATFORM



Eclypsium provides a new layer of security to defend the unprotected firmware and hardware layer of the enterprise—including laptops, servers, and networking infrastructure. Modern attackers know that traditional security tools lack visibility into firmware both at the system level and within hardware components, and are increasingly using firmware implants and backdoors to bypass security controls, persist and disrupt an organization's infrastructure. Eclypsium closes this gap by finding and mitigating the weaknesses and threats in firmware that traditional security misses.

THE ECLYPSIUM PLATFORM PROVIDES:

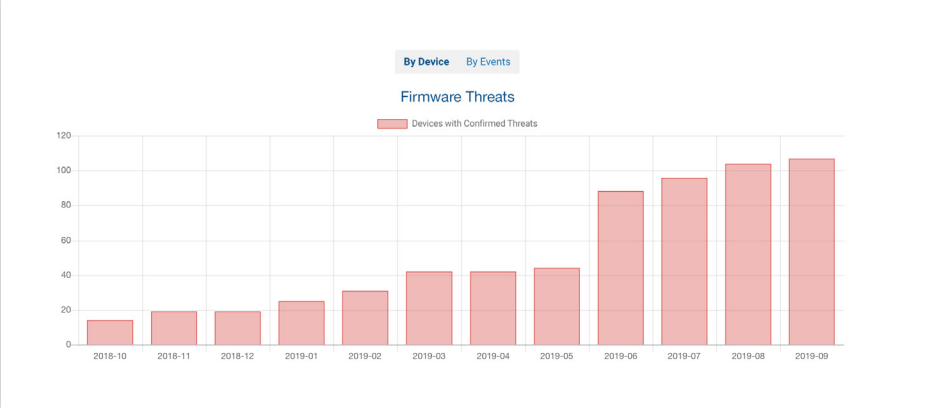


The Industry's Largest Global Firmware Reputation Database

Unlike traditional software, which is always changing, firmware should remain predictable and in "known good" states. The Eclypsium Cloud 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.

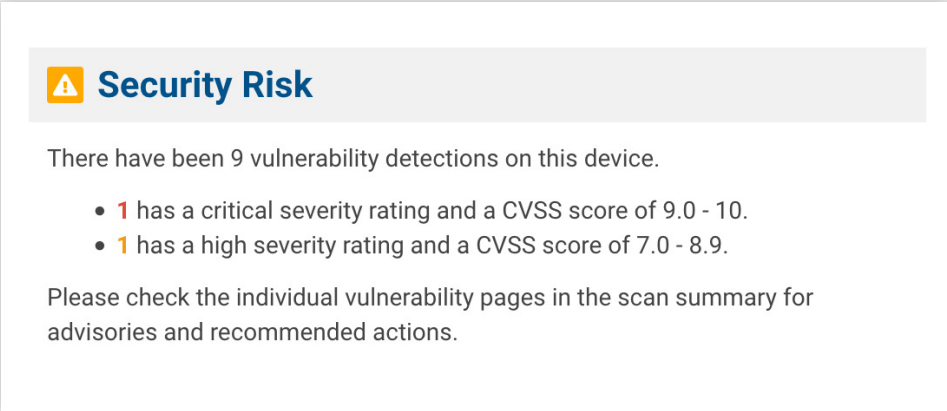
Firmware Risk and Vulnerability Scanning

Schedule regular scans or perform 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.



Firmware 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.

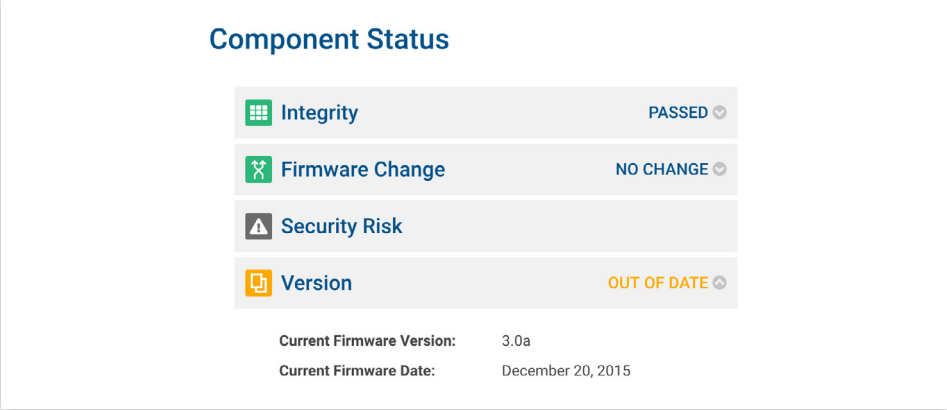


Comprehensive Firmware Monitoring

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

Firmware 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 servers, networking gear (switches, routers, firewalls), and user laptops. 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.

BRING FIRMWARE SECURITY INTO THE MODERN AGE

For most organizations, the firmware layer is the weak link in their security program where standard security practices are not applied. Eclypsium is dedicated to changing that. While most organizations lack the time and in-house expertise to manually secure their firmware, Eclypsium consolidates decades of experience into software to automatically find hidden weaknesses and threats within laptops, servers, and networking infrastructure.

Enterprise Firmware Today	Firmware Security With Eclypsium
Unprotected by Traditional Security Firmware attacks can exist undetected in your IT infrastructure, subverting OS and traditional security controls, and even surviving reimaging, poised to damage your systems and compromise your security.	**Protected from Firmware Threats** Alerts warn you when implants and backdoors have compromised your IT infrastructure. You get advance warning of firmware vulnerabilities and expert guidance on mitigation.
Hard to Manage New firmware vulnerabilities are common, but nearly impossible to manage without knowing which of your devices are affected. And misconfigured hardware settings can leave you open to attacks that are easily prevented.	**Firmware Management Simplified** At a glance, you can see the impact of a new vulnerability across all your devices, assess the severity of threats, identify misconfigured hardware settings or out of date firmware, and get guidance on mitigation.
Out of Compliance NIST and other standards identify firmware as a critical part of a security program. Although most compliance requirements already apply to firmware, many organizations lack the tools and experience to assess and measure compliance.	**Meet Firmware Security 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, PCI, or FISMA requirements down to the firmware and hardware level.
Behind the Attack Curve Firmware security is constantly changing with new vulnerabilities every day and new threats from advanced actors as well as large-scale opportunistic campaigns. Most organizations lack the expertise to assess and defend against active firmware attackers.	**A Step Ahead of Attackers** Eclypsium's world-class firmware security researcher team leads the industry in identifying threats and vulnerabilities that impact enterprise devices. Their insights power the Eclypsium Platform, putting you ahead of the curve on firmware security.

TOP ECLYPSIUM USE CASES

Firmware is everywhere in the enterprise and as a result Eclypsium provides value in a wide variety of ways. The list below provides just some of the ways that organizations are using Eclypsium to enhance their security practice:

Firmware Visibility, Risk Assessment and Patching: While software vulnerability scanning is standard in most enterprises, firmware scanning is not. Eclypsium quickly shows the firmware you have in your environment, finds outdated firmware, vulnerabilities, missing protections, and facilitates firmware patching process.

Firmware Monitoring, Detection, and Response: Traditional security has limited visibility below the operating system. Eclypsium checks for any changes in device integrity, and detects the presence of both known and unknown firmware threats both at the system level and within device components.

Supply Chain Risk Management: Eclypsium gives organizations the necessary tools to verify their supply chain and make informed buying decisions. Eclypsium can scan prospective vendor devices to identify hidden weaknesses or vulnerabilities during the evaluation phase. As new devices are delivered they can be scanned to verify that their integrity has not been compromised before delivery.

Incident Response and Threat Hunting: Attackers use implants in firmware to survive device re-imaging and silently persist in the network. Eclypsium let's IR and recovery teams verify that devices are truly clean before returning them to action, while threat hunters can use Eclypsium to uncover advanced threats that are invisible to traditional security tools.

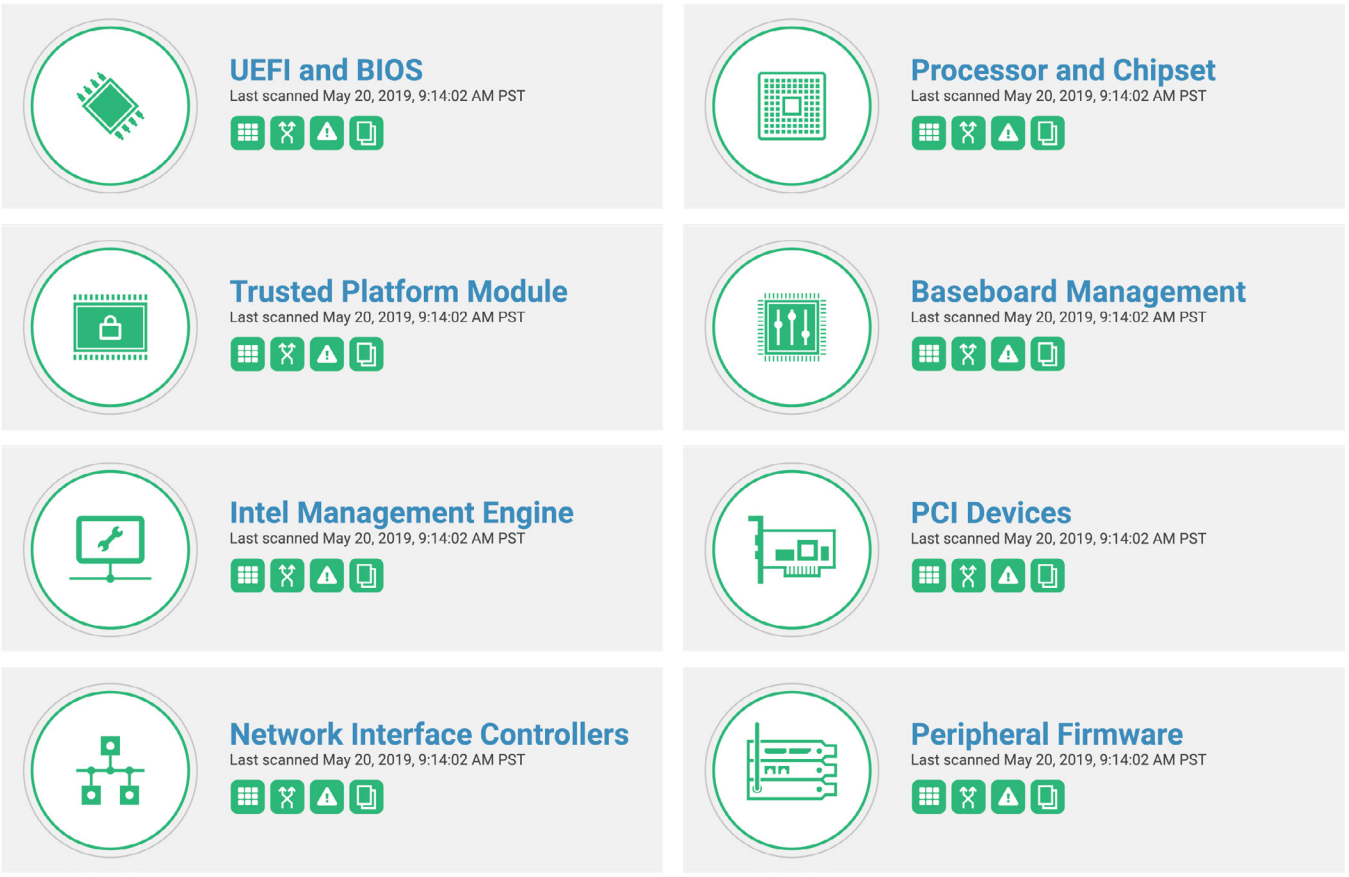
Global Travel Protection: Organizations often have employees who work in or need to travel to areas that are at higher risk for cyberattacks or espionage. Eclypsium can baseline all devices, alert in real-time to any changes in integrity, and ensure devices are clean during the device recovery process.

ECLYPSIUM PLATFORM ARCHITECTURE

Eclypsium easily plugs into your environment for fast, automated visibility and defense. Your firmware information is analyzed by the Eclypsium platform, which can be deployed in the cloud or on premise. The analytics server is constantly updated based on industry-leading threat and vulnerability research. A rich web-based user interface provides easy access to information from any location, and integration with other security and orchestration tools is available. The solution can be deployed as a targeted dissolvable scan to uncover integrity issues upon delivery of hardware or run as a periodic scan to identity threats in real time.

BROADEST COVERAGE OF FIRMWARE RISKS & THREATS

Virtually every component within a modern device has its own firmware that can be compromised in an attack. Eclypsium extends visibility and protection to all the components that make up this internal attack surface. This reach and level of granularity ensures visibility into areas most enterprises cannot see, exposing risk due to vulnerabilities and misconfigurations, unpatched firmware and compromise from implants and backdoors.



ECLYPSIUM RESEARCH

Eclypsium solutions are driven by years of experience and ongoing cutting-edge research into the foundations of computing systems and threats that target them. By deeply understanding attacks against firmware and hardware, we are able to develop mechanisms that enable detection, protection, and response.

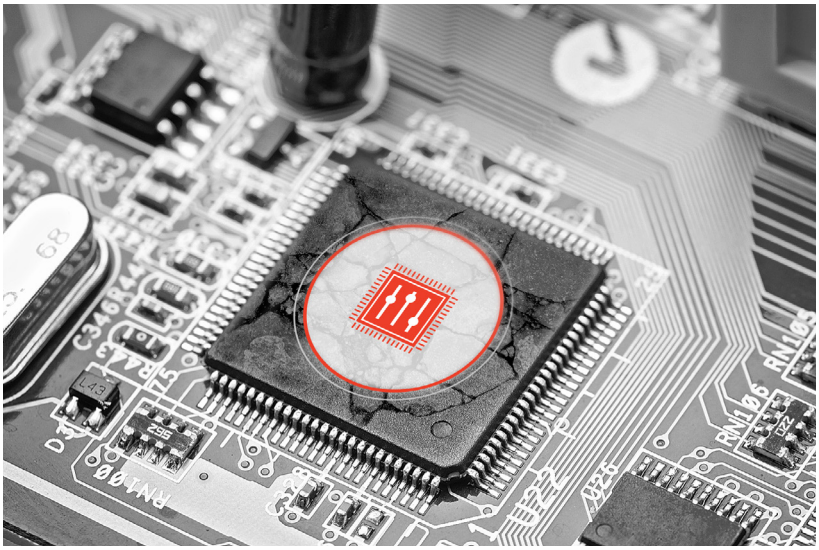
Eclypsium researchers have been credited with some of the most important recent hardware and firmware security discoveries in the industry. And in addition to being one of the most insightful teams in security, it is also one of the most prolific. The summaries below provide just a sample of some of Eclypsium's notable research.

USBAnywhere BMC Vulnerability Opens Servers to Remote Attack

Research published by Eclypsium identified 47,000 servers with BMCs exposed to the Internet that are vulnerable to remote attacks. The USBAnywhere vulnerability allows an attacker to easily connect to a server and virtually mount any USB device of their choosing to the server remotely over any network including the Internet. **Learn More >**

Screwed Drivers—Signed, Sealed, Delivered

Eclypsium researchers demonstrated that a common design flaw found in dozens of Windows drivers allows attackers to turn the very tools used to manage a system into powerful threats that can escalate privileges and persist invisibly on the host. The problem affects more than 40 drivers from at least 20 vendors. Worse yet, all the vulnerable drivers were certified by Microsoft. **Learn More >**



Vulnerable Firmware in the Supply Chain of Enterprise Servers

Research from Eclypsium shows how BMC firmware vulnerabilities in the supply chain of major server manufacturers put customers at risk of data loss and attack. Weaknesses in a BMC firmware supplier affected at least 8 server manufacturers, highlighting a problem that is industry-wide. As attackers and nation-states target higher-value assets, BMC and other firmware inside critical servers provide a particularly strategic target, which can be used to irrevocably "brick" the server and its contents. **Learn More >**

The Missing Security Primer for Bare Metal Cloud Services

Organizations turn to bare-metal cloud services when they need the highest levels of security and performance for their applications. However, Eclypsium research shows these offerings can inadvertently make the firmware layer easier to attack. **Learn More >**

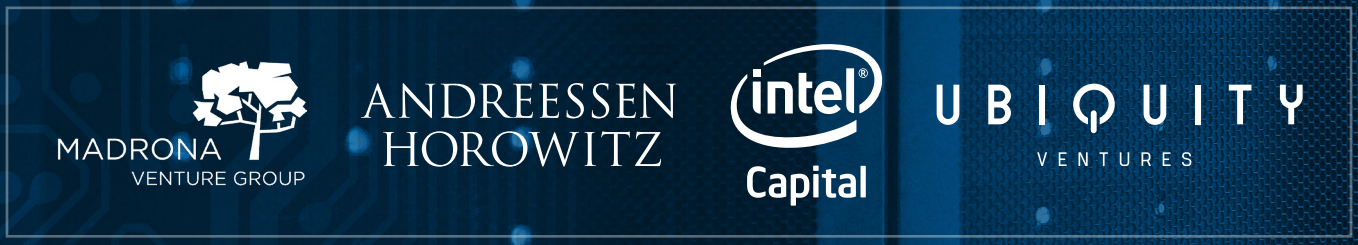
TRAINING

Eclypsium provides training for organizations on firmware security and threat prevention and assistance to security teams to investigate potential compromise. This training is targeted for individuals and teams in IT security, infrastructure, SOC, PSIRT, CSIRT, forensics, red teams, and penetration testing. These one- or two-day sessions will teach trainees about security at the hardware and firmware levels, understanding attacks against system firmware and how to mitigate them, and how to identify vulnerabilities and perform basic forensics on different firmware components. Our threat intelligence and research teams can assist customers to triage issues as part of incident response or forensics in case of a compromise.

COMPANY

Headquartered in Portland, Oregon, Eclypsium brings together an unmatched combination of talent and expertise dedicated to stopping the threats that subvert traditional security. With the backing of top tier investors, Eclypsium has assembled a team of the industry's preeminent firmware security experts and researchers with decades of real-world experience in commercial and government environments as well as open-source projects. These skills are paired with experienced and proven security industry veterans who have repeatedly shown the ability to deliver truly innovative, usable, and reliable security products for enterprises.

INVESTORS



READY TO LEARN MORE?

The Eclypsium team is here to help when you are ready to secure the firmware layer of your organization. To learn more, see a demonstration, or schedule a proof of concept at your location, please contact us at **info@eclypsium.com** or call 1-833-FIRMSEC.