WHAT WE DO

Eclypsium defends the firmware and hardware layers of the enterprise where traditional security fails and attackers are the most sophisticated. Our software proactively finds weaknesses in your laptops, servers, and networking infrastructure, helps mitigate the risks, and proactively defends against advanced threats like firmware implants and backdoors. Eclypsium provides security assurance for the entire hardware lifecycle: from supply chain to travel and remote use, as well as in operations.

Enterprise IT Infrastructure	Information Security	Incident Response

Supply Chain and Travel Scan

Continuous or On Demand Scanning

Ensure Device Integrity	Monitor Firmware & Hardware Risk	Manage Firmware Updates
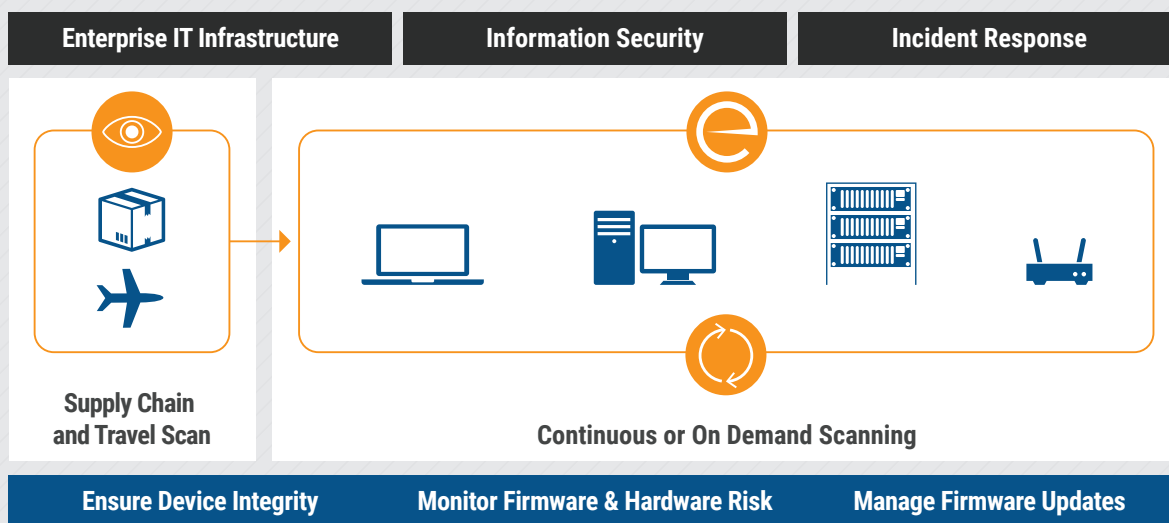
THE NEWLY EXPOSED GAP IN SECURITY

While traditional enterprise security begins at the operating system and works up, attackers are increasingly subverting these defenses by attacking the underlying firmware that controls the system itself and virtually every hardware component such as hard drives, network cards, and the processors themselves.

And while advanced actors have relied on these attack vectors for years, a new wave of vulnerabilities, exploits, and toolkits is making firmware attacks more accessible and commonplace. Servers, network devices, and laptops are now all remotely exploitable at the firmware level, and so-called "evil maid" attacks can allow anyone with a USB drive to compromise the firmware of a vulnerable system. As a result, attackers increasingly have the tools, techniques, and procedures to attack organizations where they are vulnerable, and lack visibility and protection.

THE ECLYPSIUM SOLUTION

Eclypsium is delivering the industry's first enterprise-grade software platform that can detect, defend and mitigate firmware weaknesses and threats. Our technology allows you to:

MANAGE HARDWARE ASSETS AND RISKS

- See your hardware attack surface for all hardware components (drives, CPU, etc)
- Discover and update all outdated firmware
- Discover vulnerable devices/firmware and patch critical vulnerabilities

PROTECTION FROM FIRMWARE THREATS

- Detect and mitigate firmware implants and backdoors
- Protect your IT infrastructure, including servers, endpoints, and networking devices from damage
- Ensure newly acquired hardware was not tampered with in the supply chain / manufacturing phase
- Protect laptops during travel and ensure they were not compromised upon return

THE ECLYPSIUM TEAM

We are security researchers and practitioners working at the forefront of the most insecure and unguarded attack surface in the IT landscape today. With decades of collective experience leading Intel's Advanced Research teams and founding CHIPSEC, the industry's only open-source security assessment framework for hardware platforms, we have discovered many new firmware exploits and analyzed the world's most advanced attackers.

Founded in 2017, Eclypsium is devoted to delivering the first enterprise firmware protection platform that can help our customers detect, defend and mitigate known and unknown risks at the firmware and hardware layer across their IT infrastructure, from endpoints to servers to cloud. Our investors include Madrona Venture Group, Andreessen Horowitz, Intel Capital and Ubiquity Ventures.

Connect with Eclypsium at **info@eclypsium.com** to learn more about how to defend the foundation of your organization and to see a live demonstration of the platform.