CASE STUDY_

Major Financial Institution Defends Against Nation-State Threats with Eclypsium Endpoint Firmware Security

THE CHALLENGE_

A Systemically Important Financial Institution with several hundred thousand employees worldwide faced growing concerns about firmware-level vulnerabilities in endpoint devices from a specific vendor widely deployed across their organization. As nation-state threat actors—particularly those associated with the People's Republic of China—increasingly target financial institutions through sophisticated supply chain attacks, the bank required comprehensive visibility into chip-level and firmware-level security across their distributed workforce.

Traditional endpoint security solutions failed to detect firmware-level compromises, leaving the organization vulnerable to attacks that could persist undetected even after device reimaging. The bank needed assurance that known attack tactics associated with PRC APT groups could not be used to achieve intrusion or establish persistence within their systems.

Customer Needs	Eclypsium Results
Comprehensive firmware monitoring across hundreds of thousands of employee laptops to detect vulnerabilities and threats at the chip and firmware level.	**Complete visibility** into firmware components including CPU, BIOS, UEFI, Intel ME/AMT, TPM, NICs, and peripheral devices across the entire endpoint fleet with automated scanning and continuous monitoring.
Nation-state threat detection specifically focused on PRC APT tactics, techniques, and procedures targeting financial institutions.	**Advanced threat detection** using the industry's largest firmware reputation database with 10M+ hashes across 30+ hardware vendors, specifically designed to identify implants, backdoors, and rootkits used by state-sponsored actors.
Scalable monitoring solution capable of protecting a distributed workforce without impacting device performance or user productivity.	**Cloud-based platform** with configurable scanning frequency and automated alerting that scales to monitor hundreds of thousands of endpoints while maintaining minimal system overhead.
Rapid vulnerability response to protect against newly disclosed threats and zero-day exploits targeting firmware components.	**Real-time alerting** and detailed remediation guidance with CVSS scoring, vendor advisory mapping, and automated firmware update recommendations for immediate threat response.

PROTECTING AGAINST SOPHISTICATED NATION-STATE FIRMWARE ATTACKS_

The financial institution's implementation of Eclypsium's endpoint firmware protection addresses critical gaps in traditional security monitoring. Eclypsium extends visibility and protection to all the components that make up this internal attack surface including processors, network interface cards, UEFI and EFI firmware, Baseboard Management Controllers (BMCs), Intel Security Management Engine, and more.

Defending Against Known PRC APT Tactics

Eclypsium's platform specifically addresses tactics employed by Chinese threat actors targeting financial institutions:

- **Firmware Implant Detection:** Eclypsium checks the system for the presence of any known implants based on our industry research and intelligence and monitors devices and the behavior of their firmware to identify risky behavior.
- **Supply Chain Compromise Protection:** Eclypsium detects signs of of tampered firmware that could have been compromised during manufacturing or distribution.

CONTINUOUS PROTECTION ACROSS A DISTRIBUTED WORKFORCE_

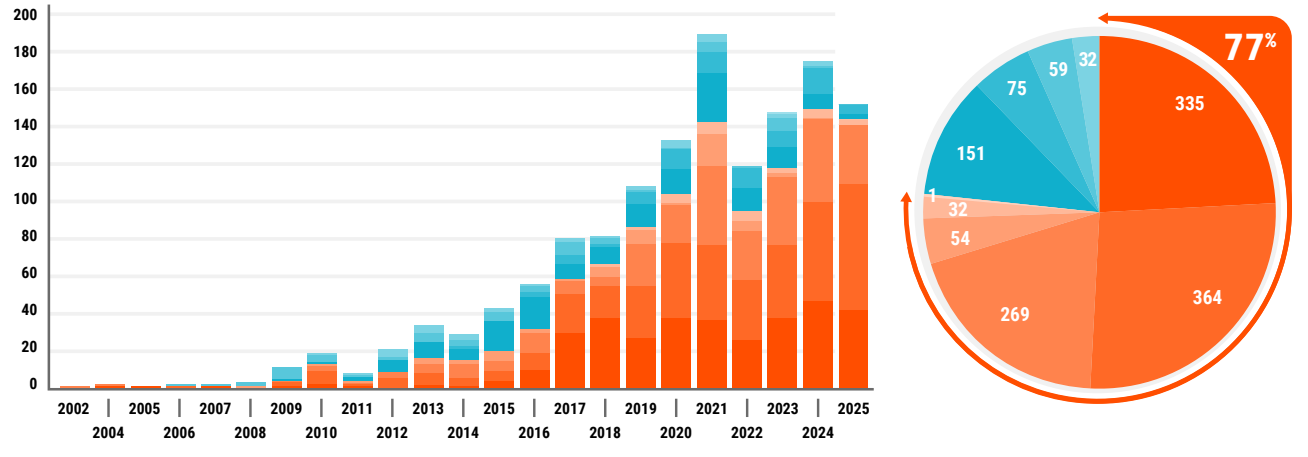
The bank's implementation will grow to provide comprehensive coverage across their global operations. Eclypsium's monitoring capabilities include:

- **Pre-Deployment Validation:** Ensuring new devices haven't been compromised before deployment to employees.

Sample dashboard of Eclypsium tracking integrity, vulnerability, and firmware version. Not real customer data.

- **Continuous Monitoring:** Regular firmware scans with configurable frequency based on threat levels and device criticality.
- **Incident Response Integration:** Real-time alerts to security teams when critical events such as failed integrity checks or threats are detected

THE RISE IN FIRMWARE VULNERABILITIES_



The number of vulnerabilities in firmware and other below-the-OS components listed on CISA's Known Exploited Vulnerabilities catalog has risen sharply in recent years. Firmware vulnerabilities introduced through the IT supply chain are a powerful tool in nation state hacker toolboxes. The traditional approach of focusing solely on operating system-level security is insufficient against these advanced threats. By implanting malicious code in firmware, the threat is able to sit below the level of the operating system, enabling the threat to easily subvert traditional security controls and gain near omnipotent power and visibility over the infected system.

EXPANDING PROTECTION BEYOND ENDPOINTS_

Building on the success of their endpoint protection program, the bank is extending Eclypsium's capabilities to:

- **Server Infrastructure:** Continuous monitoring of data center servers for firmware integrity and vulnerability management.
- **Network Infrastructure:** Protection of routers, switches, and firewalls from firmware-level compromises.
- **AI Infrastructure:** As the bank expands machine learning capabilities, extending firmware monitoring to GPU servers and specialized AI hardware.

ABOUT ECLYPSIUM_

Eclypsium's cloud-based and on-premises platform provides digital supply chain security for critical software, firmware and hardware in enterprise infrastructure. Eclypsium helps enterprises and government agencies mitigate risks to their infrastructure from complex technology supply chains. The company has been named a Gartner Cool Vendor, a TAG Cyber Distinguished Vendor, one of the World's 10 Most Innovative Security Companies by Fast Company, a CNBC Upstart 100, a CB Insights Cyber Defender, and an RSAC Innovation Sandbox finalist.