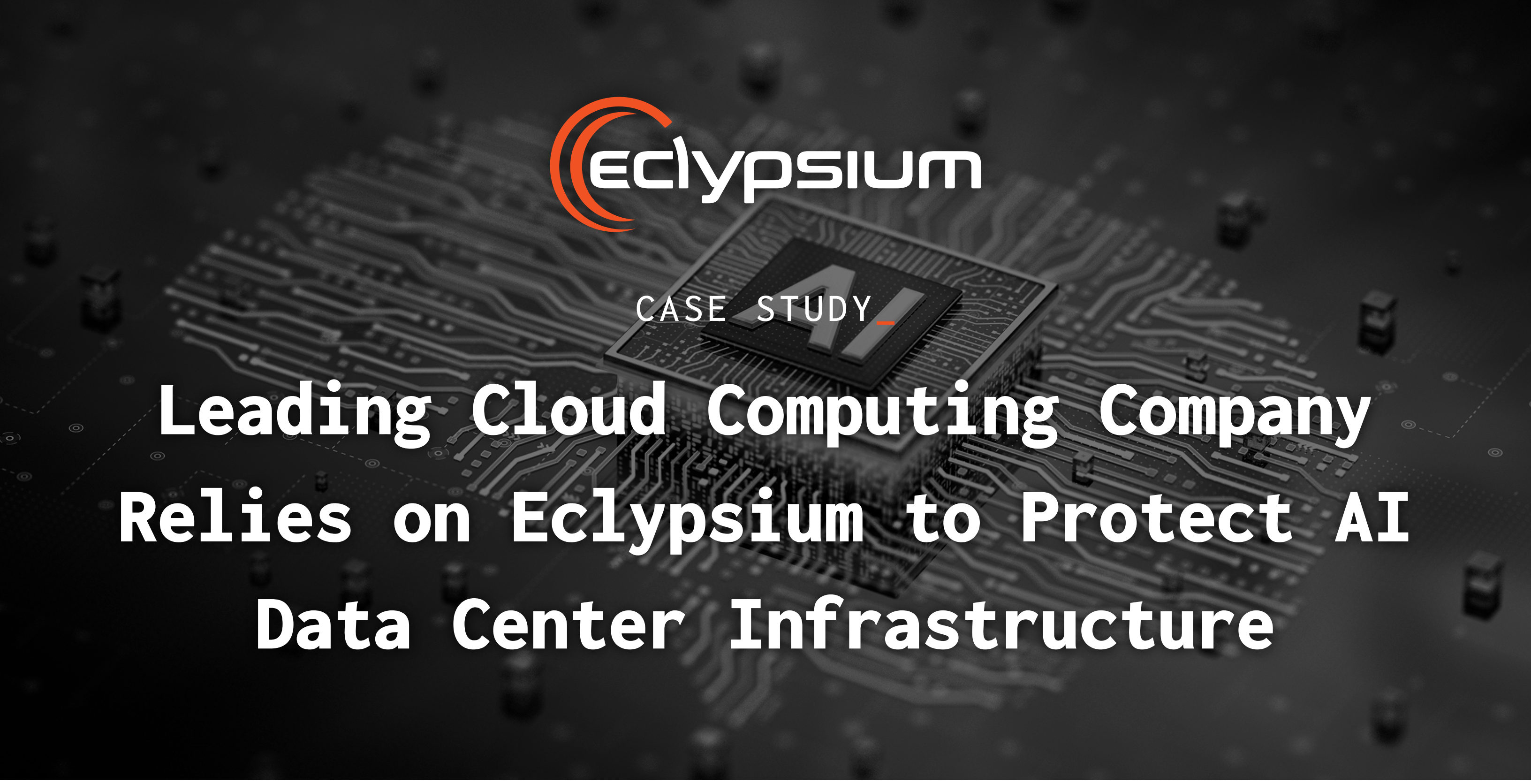


Eclypsium

CASE STUDY_

Leading Cloud Computing Company Relies on Eclypsium to Protect AI Data Center Infrastructure

This organization provides a new breed of cloud services, purpose-built for the needs of AI and the next generation of computing. With industry-leading innovation, close ties to industry titans such as NVIDIA, Microsoft and OpenAI, and meteoric growth across the US and Europe, they have become one of hottest cloud platform providers in the industry.

But this rise naturally comes with challenges. The company's services rely on a rapidly growing fleet of highly specialized server hardware and AI GPUs, and it is up to the security team to ensure the integrity and security posture of the hardware and components at the heart of the platform.

By partnering with Eclypsium, the organization was able to harness a turn-key solution for the assessment and ongoing monitoring of their servers and internal components such as UEFI firmware, NVIDIA GPUs, Intel CPUs, and more. This enabled their team to proactively verify technology supply chains while ensuring the highest levels of security for their customers.

Business Needs

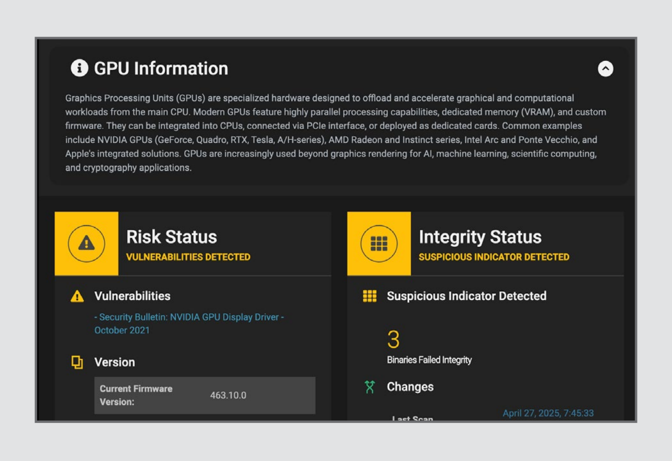
- Verify the integrity of firmware in AI server infrastructure and components and proactively alert on any changes.
- Firmware-specific vulnerability management, updating, and configuration management.
- Support fast, efficient rollout while minimizing costs and impact to staff.

Eclypsium Benefits

- Deep vendor-agnostic visibility into AI servers and components including NVIDIA GPUs
- Automated assessments to identify vulnerabilities, threats, or changes to device firmware and proactively verify firmware and supply chain integrity.
- Simple, easy-to-deploy solution at a significantly lower cost than developing custom solutions for each vendor.

ENABLING THE AGE OF AI

To efficiently harness the power of AI, organizations need to focus on their business without getting bogged down in the minutia of building out AI infrastructure. As a new class of cloud platform, this Eclypsium customer provides enterprises and AI labs with easy, cost-effective access to next-generation software and infrastructure designed specifically for the most compute-hungry projects.



GPU Information

Graphics Processing Units (GPUs) are specialized hardware designed to offload and accelerate graphical and computational workloads from the main CPU. Modern GPUs feature highly parallel processing capabilities, dedicated memory (VRAM), and custom firmware. They can be integrated into CPUs, connected via PCIe interface, or deployed as dedicated cards. Common examples include NVIDIA GPUs (GeForce, Quadro, RTX, Tesla, A/H-series), AMD Radeon and Instinct series, Intel Arc and Ponte Vecchio, and Apple's integrated solutions. GPUs are increasingly used beyond graphics rendering for AI, machine learning, scientific computing, and cryptography applications.

Risk Status
VULNERABILITIES DETECTED

Vulnerabilities
- Security Bulletin: NVIDIA GPU Display Driver - October 2021

Version
Current Firmware Version: 463.10.0

Integrity Status
SUSPICIOUS INDICATOR DETECTED

Suspicious Indicator Detected
3
Binaries Failed Integrity

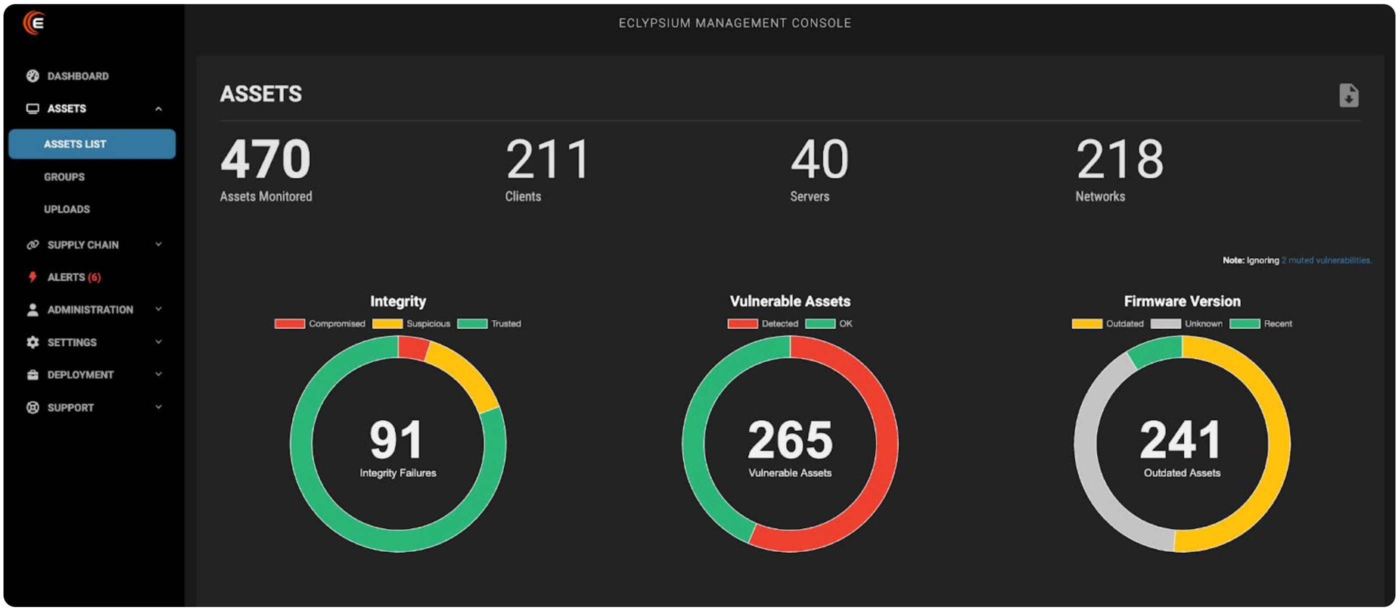
Changes
Last Scan April 27, 2025, 7:45:33

SHARED RESPONSIBILITY FOR SECURITY

Like other platforms-as-a-service (PaaS), this technology offering has a shared responsibility model when it comes to security. Customers are responsible for securing their own code and projects, while the cloud hosting provider is responsible for the security of the infrastructure from the VMs and containers all the way down to the physical servers and components that run the workloads.

SUPPLY CHAIN RISKS AND CHALLENGES

As a result, this organization knew early on that firmware and supply chain security would play a critical role in their security program. The team needed to audit and monitor a wide range of highly specialized assets. This included AI servers and all their critical code and components such as UEFI firmware and bootloaders, the NVIDIA GPUs that power AI workloads, Intel CPUs, external PCIe devices, and other system components.



ASSETS

470 Assets Monitored
211 Clients
40 Servers
218 Networks

Note: Ignoring 2 muted vulnerabilities.

91 Integrity Failures
265 Vulnerable Assets
241 Outdated Assets

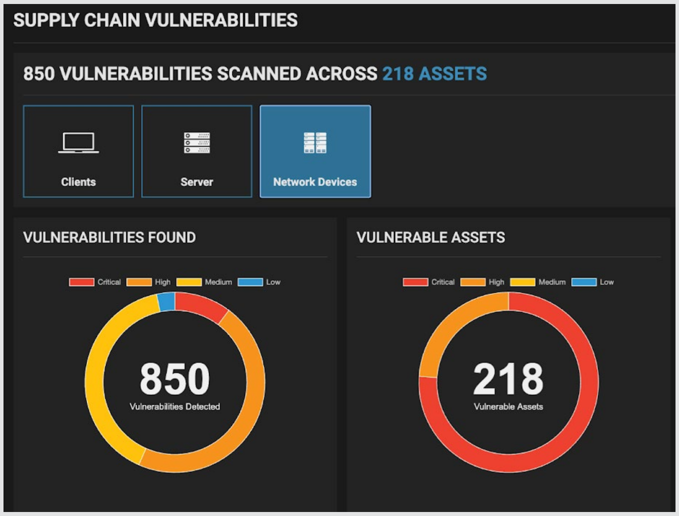
Teams needed to know that every piece of code was valid, unaltered, and free of threats or implants. They needed to know if there were vulnerabilities and to apply updates if needed. And on an ongoing basis, they needed to know if there were any changes, whether malicious or otherwise that could put a device or component at risk. And they needed to do all of this without slowing down their massive growth and expansion or overburdening technical or security staff. They were able to leverage Eclypsium to validate that all systems are running the level of code they are expecting to ensure devices are running the “gold” firmware binaries.

THE ECLYPSIUM SOLUTION_

Using the Eclypsium Platform, they were able to quickly roll out a comprehensive strategy for firmware and supply chain security. Eclypsium was able to provide value in the following key areas.

Security Capabilities

- **Firmware integrity checks** - Eclypsium scans were used to verify that all firmware was valid, unaltered, and free from threats such as implants and backdoors. Systems were also checked for threats such as malicious bootloaders.
- **Firmware baselines and change monitoring** - Next, Eclypsium was able to establish an auditable baseline of all critical firmware and components. Any changes to these established baselines would then trigger alerts to the firm's SIEM for further investigation and response.
- **Vulnerability management and flaw remediation** - Eclypsium was able to provide simple automated vulnerability assessments for low-level components that are typically missed by traditional scans. This included detecting misconfiguration or missing protections between various system components. When problems were identified, Eclypsium helped the team to apply corrective changes or updates.
- **Additional context and enrichment for investigations** - Using the Eclypsium API, the team was able to pull in low-level device details for servers and components to assist with other investigations.



SUPPLY CHAIN VULNERABILITIES

850 VULNERABILITIES SCANNED ACROSS 218 ASSETS

VULNERABILITIES FOUND

VULNERABLE ASSETS

Cost-Effective and Simple

- **Simple evaluation and deployment** - Within just a few hours, the team was able to install the Eclypsium platform and begin seeing results on their server infrastructure.
- **Broad support for the latest AI technology** - Eclypsium provided consistent coverage across a wide range of vendors and asset types.
- **Automated assessments and guidance** - Eclypsium assessments were able to automatically identify and explain firmware and supply chain risks without the need to hire firmware specialists. Staff could simply scan their devices and quickly detect and remediate threats.

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. Eclypsium 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.