SOLUTION BRIEF_

SECURING AI DATA CENTERS

Continuous monitoring and hardening AI factories, AI infrastructure and supply chains

THE GROWING CHALLENGE_

The global AI arms race is accelerating, and AI data centers are now critical infrastructure, vital to national security and defense. AI data centers are uniquely challenging to secure. They process high volumes of sensitive data on complex compute infrastructure where capacity is rapidly swapped between different customers. Any attack can cause loss of data, leaking of intellectual property, poisoning of model weights, causing significant harm to any nation's battle for AI supremacy.

The urgency of proactive cybersecurity for AI data centers could not be higher.

AI INFRASTRUCTURE RISKS FOR DATA CENTERS_

From AI Servers, to GPUs, to network infrastructure and other foundational tech, increased security and continuous protection is needed. NIST SP 800-223 identifies numerous cyber risks facing High Performance Compute (HPC) which includes AI data centers. Risks include:

- **Attacks on critical hardware components** and software manipulation to gain unauthorized access.
- **Rapidly changing infrastructure for HPC firmware and hardware components**, increasing supply chain risk
- **Compute Node Sanitization challenges**, such as validating firmware between task runs on shared compute infrastructure.

Private sector AI leaders are also increasing focus on secure AI infrastructure. OpenAI published a list of six core security practices for securing advanced AI, including:

I. Trusted computing for AI accelerators
II. Network and tenant isolation guarantees
III. Innovation in operational and physical security for datacenters
IV. AI-specific audit and compliance programs
V. AI for cyber defense
VI. Resilience, redundancy, and research

Eclypsium supports many requirements of NIST SP 800-223, as well as the recommendations in OpenAI's guidance for rethinking secure AI infrastructure.

ECLYPSIUM DELIVERS PROACTIVE SECURITY FOR AI INFRASTRUCTURE_

Leading cloud computing companies already rely on Eclypsium to protect AI DC Infrastructure with capabilities such as:

AI Server & GPU Risk Analysis

Inventory, **manage**, and **secure critical assets** across numerous AI servers and components, including NVIDIA GPUs.

Proactively validate integrity of GPUs before installing or leasing to new customers.

AI Infrastructure Integrity

Verify firmware integrity in AI Server Infrastructure and supply chain components.

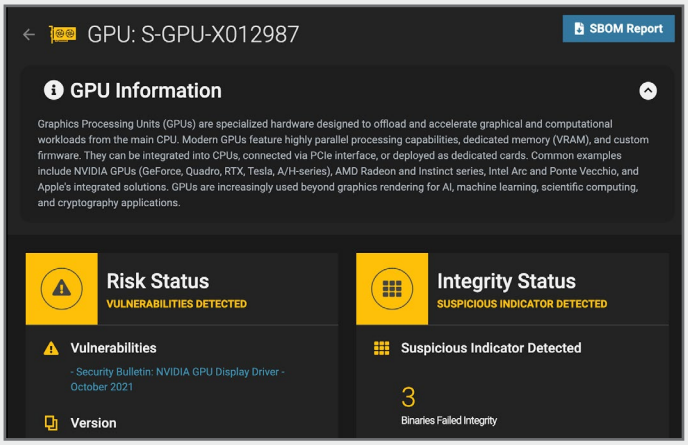
Proactively alert on changes in components and configurations.

Scan and verify all production GPUs and connected infrastructure to assure known-good firmware and configurations.

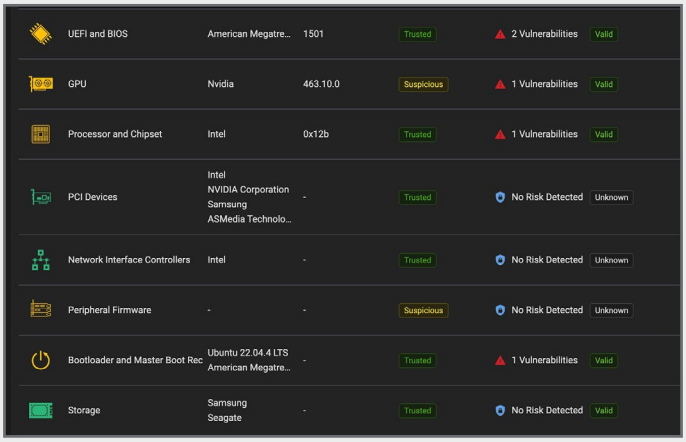
Vulnerability Management & Threat Detection

Discover vulnerabilities other scans miss, deep in the firmware of AI data center servers, chips and components.

Proactively detect threats and attacks other tools miss.



Eclypsium delivers actionable summaries of vulnerabilities and integrity failures for individual GPUs, or all GPUs throughout a data center.



Eclypsium delivers complete inventory and vulnerability analysis of each component in a device, GPU, server, or connected network appliance. Identify vulnerabilities, outdated firmware, vulnerable GPU drivers, and other hardware and component level risks in AI data centers.

FAST. SIMPLE. COMPLETE_

The Eclypsium platform rolls out quickly, with minimal deployment burden, and works across the entire environment. With Eclypsium, AI data center teams don't have to worry about the security of your infrastructure, and can focus on delivering the best service to your customers.

- **Simple evaluation and deployment before, during, and after** - Data center teams can install the Eclypsium platform and quickly begin seeing results on their AI data center infrastructure at any time in its lifecycle, from before deploying gear to between training runs to asset disposition.
- **Broad support for the latest AI technology** - Eclypsium provides consistent coverage across a wide range of vendors and asset types, from x86 and ARM servers and GPUs to firewalls, routers, switches, and other data center infrastructure, minimizing tools needed to mitigate risk.
- **Automated platform analytics and guidance** - Eclypsium assessments automatically identify and explain firmware and supply chain risks without the need to hire firmware specialists.