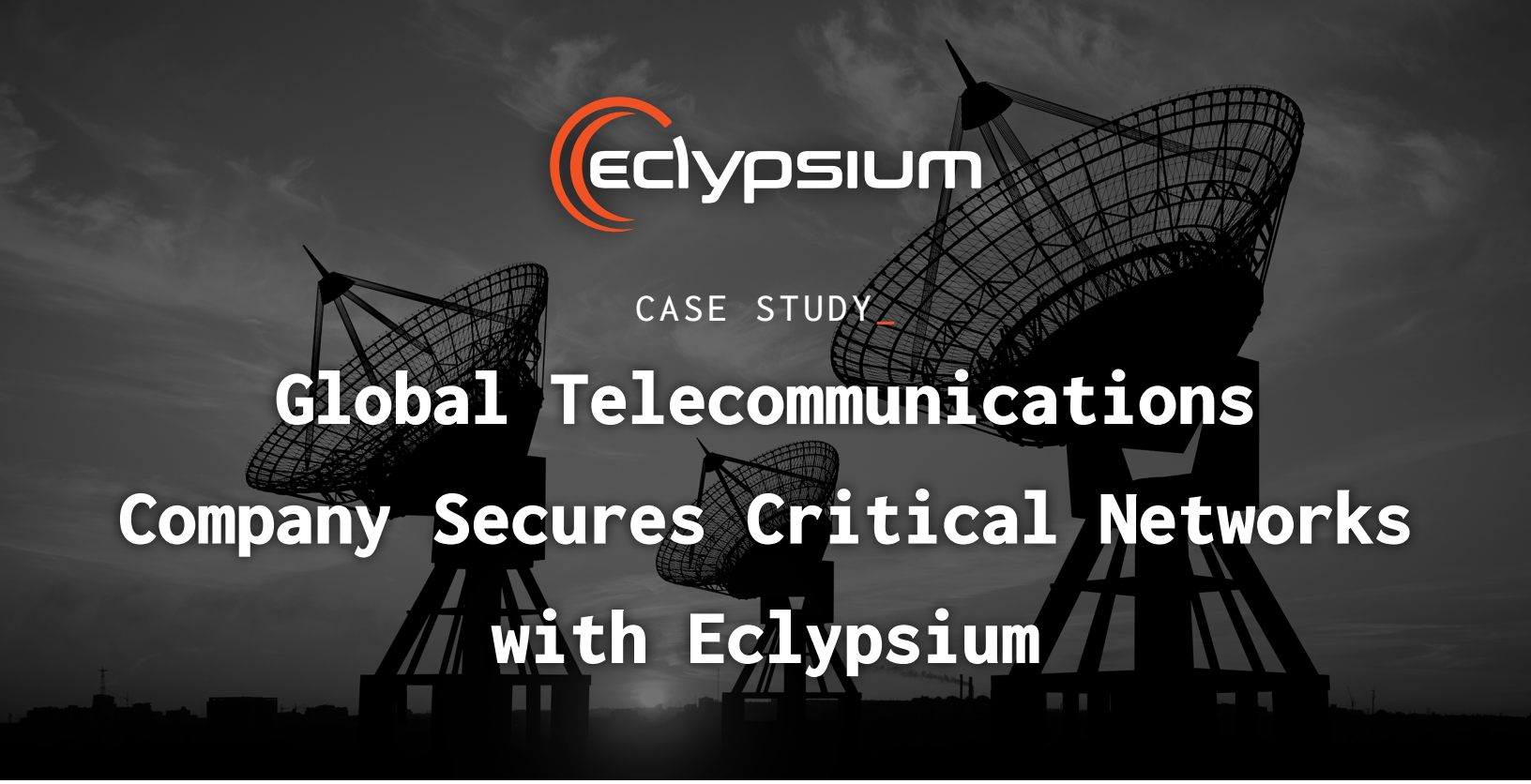


CASE STUDY_

Global Telecommunications Company Secures Critical Networks with Eclypsium

THE CHALLENGE_

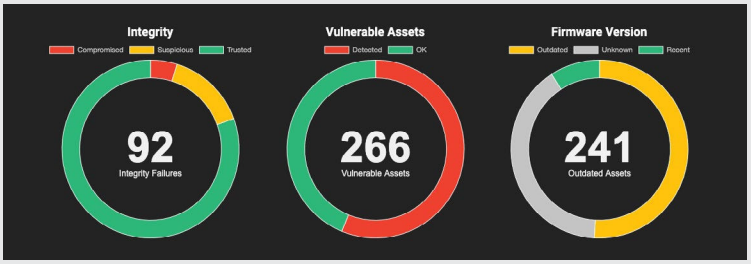
A leading global telecommunications company with large integrated satellite and terrestrial networks provides diverse services to telecommunications operators, enterprises, media companies, and government entities. They chose Eclypsium to provide better visibility and vulnerability management on thousands of Cisco and Juniper network devices critical to their global operations.

Within 1-2 months, Eclypsium was able to deliver on the company's foundational security needs, and build a roadmap for even more visibility and hardening of network assets over time.

Customer Needs	Eclypsium Results
Vulnerability management in network infrastructure that was not effectively monitored by their existing vulnerability management solution.	**750+** Vulnerabilities, and **32 Critical Unique Vulnerabilities** discovered in their network environment.
Network device inventory with firmware version and update tracking across thousands of devices from multiple vendors.	**65%** Assets with outdated firmware discovered.
Device hardening, integrity monitoring, and configuration change detection in firmware across critical network devices.	Security configurations mapped, with detailed information about their security and support status across all assets. Eclypsium discovered numerous configuration and integrity challenges, including certificate misalignment on critical network devices.

CONTINUOUS, COMPREHENSIVE REPORTING_

Eclypsium continuously monitors assets and identifies risks, integrity failures, configuration changes, vulnerabilities, and indicators of compromise, providing peace of mind to this global satellite network operator that their network infrastructure is secure.



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

HOW ECLYPSIUM PLATFORM DEFENDS AGAINST GROWING NETWORK ATTACKS_

The number of attacks and vulnerabilities targeting network devices from Cisco, Juniper, and other major network infrastructure providers is on the rise. 2024 and 2025 saw major disclosures of China-sponsored attackers given the "Typhoon" moniker targeting telecoms. Eclypsium delivers inventory, hardening, and detection and response to protect undermonitored network infrastructure that is increasingly under attack by nation states and ransomware gangs.

INVENTORY_

Dynamic inventory of production assets - Build an inventory of every piece of enterprise IT infrastructure, down to the hardware, firmware, and software level.

On-demand SBOMs - Generate software bills of material on demand, including hardware and firmware components of devices.

Assess product risk - Equip security and procurement teams to understand the risk inherent in those products before purchase.

HARDEN_

Prioritize infrastructure vulnerabilities - Gain insights into low-level vulnerabilities in hardware, firmware, and software components.

Simplify compliance - Track issues at the hardware and firmware levels in frameworks such as NIST 800-53.

Automate firmware updates - Schedule and automatically apply critical firmware patches.

DETECT & RESPOND_

Detect threats that evade EDR - Alert on implants and other indicators of compromise for low-level components of your IT infrastructure.

Defend against tampering and counterfeit components - Validate that assets have not been tampered with and have authentic components.

Correlate with other data - Send alerts to SIEM and SOAR to give analysts improved context.

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.