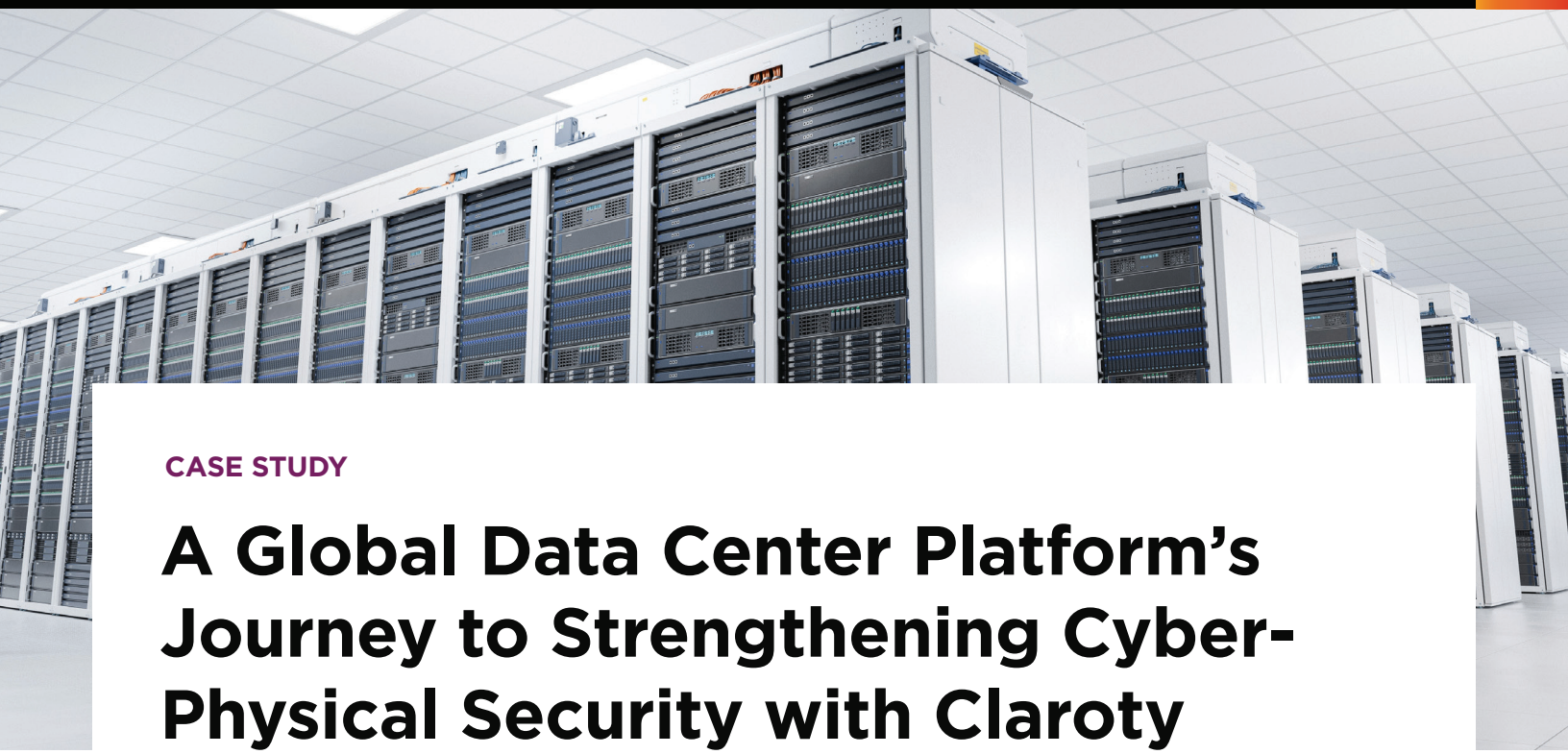

CASE STUDY

A Global Data Center Platform's Journey to Strengthening Cyber-Physical Security with Claroty

Introduction

A leading global provider of data centers, co-location services, and interconnection solutions, is committed to providing reliable, secure infrastructure for their clients, including some of the world's largest companies. With an increasingly complex IT and cyber-physical systems (CPS) environment of 300+ sites, this data center provider faced the challenge of ensuring the security and visibility of OT, IoT, and BAS assets across its diverse network of data centers.

CPS are essential to any data center cybersecurity program because they bridge physical processes—such as cooling, power distribution, and access controls—with digital networks and control systems. Unlike traditional IT cybersecurity programs, which focus primarily on protecting data and digital services, the prevalence of CPS in data centers expands the attack surface and demands close attention to the operational integrity and safety of physical processes. Data centers are high-value targets for cyber-physical attacks because they rely on interconnected CPS systems such as power, cooling, and access control. If compromised, these systems can cause widespread disruption. Effective CPS cybersecurity requires a holistic approach that combines traditional IT security with specialized protections for physical infrastructure to ensure safety, operational continuity, and business resilience.

Key Highlights

- **Comprehensive OT asset visibility** across global data centers.
- **Seamless integration with existing systems** (SolarWinds, Cisco DNA).
- **Contractual compliance** preventing tens of millions in penalties.
- **Risk posture tracking** with real-time remediation data and risk scoring.
- **True partnership** with Claroty's proactive and committed team.

The Challenge

As a company that operates highly sensitive, business-critical infrastructure, this data center provider's CPS environment includes numerous assets, from cooling and power systems to backup generators. However, a lack of visibility and outdated security practices posed risks to both operational efficiency and regulatory compliance.

Moreover, key data center clients required timely vulnerability patching, with contractual penalties for non-compliance, potentially costing millions of dollars. At the same time, the data center provider realized that the visibility of their OT assets was fragmented, and with acquisitions, legacy systems, and overlapping networks, they needed a comprehensive, scalable solution to gain full visibility into all their OT assets and vulnerabilities. The data center provider sought a robust solution that would provide real-time asset visibility, integrate seamlessly with existing systems, and allow for proactive vulnerability management. After evaluating multiple vendors, they chose Claroty to address their unique challenges.

The Solution

Tailored Visibility at Global Scale

With more than 320 global sites (and over 60 new data centers coming online each year), this global data center provider needed a scalable, accurate way to see and manage their OT environments. Claroty xDome replaced error-prone spreadsheets with an automated, always up-to-date asset inventory, delivering weekly insights across distributed locations without requiring hardware-heavy deployments.

By integrating with existing tools like SolarWinds and Cisco DNA, xDome eliminated visibility gaps caused by overlapping subnets and complex network topologies. It captured everything from physical devices to critical cooling and power systems. For the first time, the organization had a single source of truth for its OT asset inventory.

Claroty's Edge technology provided a comprehensive asset inventory across all global sites without requiring network changes or physical hardware.

This foundational visibility didn't just improve daily operations, it became a strategic enabler. It empowered the organization to launch a targeted risk reduction program and respond effectively in moments of crisis. For example, after a battery-related fire impacted a Singapore facility, teams used Claroty's asset data to quickly identify affected devices by model, firmware, and serial number, enabling rapid, precise remediation without relying on outdated records. Within hours, they had a complete, trustworthy picture of what needed to be replaced, minimizing downtime and reinforcing the value of an accurate inventory.

Enabling Informed and Prioritized Risk Reduction

With a single, trusted view of their OT assets in place, the organization was finally able to make informed decisions about which risks to remediate, defer, or accept. This transformed risk reduction from an overwhelming challenge into a manageable and strategic effort.

Claroty xDome provided centralized, real-time visibility into OT vulnerabilities along with customized risk scoring. This allowed security, operations, and risk teams to collaborate more effectively and base decisions on shared, trustworthy data.

With this foundation, the team launched targeted remediation programs that included patching firmware vulnerabilities and replacing outdated assets. Prioritization was guided by business impact and contractual requirements, as many data center clients mandate timely resolution of known vulnerabilities to avoid multi-million dollar penalties.

Claroty's risk scoring data now powers remediation reports that track progress site by site. This visibility has helped secure executive alignment and support for a 12-month roadmap to address 90 percent of known asset risks across critical global locations. With clear tracking and measurable results, OT risk reduction has shifted from a reactive task to an operational priority informed by strategic insight.

A Collaborative Partnership

Claroty quickly distinguished itself not just as a software vendor, but as a committed partner invested in the organization's success. As the team navigated inherited network complexity, including overlapping IP ranges from past acquisitions, Claroty provided hands-on support to close visibility gaps through integrations with existing tools like SolarWinds and Cisco DNA. This collaboration enabled smoother asset correlation and established a stronger foundation for risk reduction efforts.

According to the customer's OT security lead, what set Claroty apart was the team's consistent, pragmatic approach. Based on prior experience with other cybersecurity vendors, he noted that where others may have dismissed challenges, Claroty provided real solutions. Their responsiveness and willingness to problem-solve reinforced confidence in the five-year partnership and contributed meaningfully to the program's early success.

> "Every time we encountered a challenge, the entire Claroty team showed up and proposed solutions. That has been, again and again, the reassurance that the five-year commitment we gave Claroty was the right choice."

Conclusion

This global data center provider's journey with Claroty highlights the impact of a collaborative partnership grounded in visibility, trust, and shared objectives. By replacing outdated spreadsheets with accurate asset inventories, the organization laid the foundation for a scalable OT vulnerability remediation program.

Claroty's safe queries, tailored integrations, and hands-on support enabled the team to manage risk, maintain uptime, and meet strict contractual and regulatory obligations. With a clear roadmap to remediate 90 percent of asset risks and growing internal alignment, the organization is well-positioned to advance its OT security maturity. Claroty's support has been a key contributor to that progress.