NOZOMI NETWORKS | COPT DEFENSE PROPERTIES

CASE STUDY

COPT Defense Achieves Centralized Visibility Across Mission-Critical Facilities

The Customer: COPT Defense Properties

COPT Defense Properties is a real estate investment trust (REIT) that owns, develops and operates mission-critical facilities, including 200+ properties and 30+ data centers that support U.S. government agencies and defense contractors.

Its portfolio is strategically located near key defense installations and technology hubs, providing secure, high-performance environments for government and defense organizations. Given the sensitive nature of their national security and intelligence-related missions, visibility and reliability into all cyber assets and networks is critical for COPT Defense.

How can mission-critical facilities be monitored and secured across hundreds of distributed buildings?

As COPT Defense expanded its portfolio of mission-critical facilities, managing their operational technology (OT) environments became increasingly complex. Each building operates its own building automation systems (BAS), creating a fragmented landscape that limited visibility across sites.

COPT Defense lacked insight into what devices existed on its networks, how those devices communicated and whether behavior aligned with expected baselines. As a result, identifying anomalies or potential issues was difficult.

Prior to their search for an OT security solution, COPT Defense relied on traditional networking tools and the expertise of building systems

Company Profile

Industry: Real Estate/Government

Employees: <1,000

Location: United States

Challenges

- **Limited visibility into OT and IoT devices,** traffic and baseline communications
- **Fragmented monitoring** across geographically distributed facilities
- **Lack of centralized asset inventory** and independent validation

Results

- **Centralized visibility** across 130+ sites
- **Improved asset discovery** and inventory accuracy
- **Enhanced ability to detect anomalies** and validate configurations

teams and OT integrators. However, this approach limited their ability to independently validate system integrity and proactively detect issues.

"You have to know what you have in order to defend it," said Ken Kurz, VP of IT and CIO at COPT Defense Properties. *"That gap in visibility and not knowing will keep any security leader up at night."*

Deploying a Hybrid Nozomi Networks Solution for Centralized Visibility Across Distributed OT Environments

To address these challenges, COPT Defense evaluated OT security solutions that could provide deep visibility across distributed environments while meeting strict operational requirements. The team needed a flexible architecture that could support both cloud-connected sites and secure, air-gapped environments where sensitive operations required local control. Nozomi was the only vendor that offered that hybrid deployment model, combining comprehensive OT and IoT visibility with the ability to adapt to each facility's requirements.

"We wanted an on-premises solution that we could leverage from the cloud, but other vendors forced you down a direction where you had to be connected to the internet," said Kurz.

Across more than 130 sites with varying operational and security requirements, COPT Defense deployed Nozomi in a hybrid architecture. For cloud-connected facilities, remote collectors, virtual Guardian sensors and the Vantage cloud platform provide a centralized, accurate view of OT and IoT assets. For secure air-gapped environments, remote collectors and physical Guardians connect to an on-premises management console, giving COPT Defense consistent visibility while maintaining the segmentation and local control required for sensitive facilities.

With OT- and IoT-native visibility, the team has been able to identify legacy components in systems they thought had been fully upgraded and uncover other hidden risks. They also use the Vantage IQ AI assistant to get instant answers to plain-language questions about their environment, including clear advice on what to do next across their entire portfolio.

Strengthening Operational Resilience with Scalable Visibility and a Trusted Partnership

With the Nozomi platform in place, COPT Defense has transformed how it monitors and manages building systems across its distributed environment. They now have a centralized, accurate view of OT and IoT assets across their facilities, giving their teams visibility into what exists in each building and how those systems are behaving.

"Nozomi has given us insight into our OT systems that we didn't have previously. We can now provide an accurate inventory of what exists in each building and see how those systems are actually communicating," said Thomas Jacobs, Security Engineer at COPT Defense Properties. This visibility enables COPT Defense to more effectively identify vulnerabilities and outdated software, strengthening their overall security posture.

Beyond improving visibility, the Nozomi platform has enhanced oversight and accountability across

COPT Defense's building environments. They can now independently validate that their systems are configured correctly, and that third-party vendors are adhering to required standards. This visibility has already helped the team identify and address previously unseen issues within their environment.

"We were able to identify unmanaged switches in our buildings and give our field teams a starting point, instead of just having them search blindly," said Jacobs. By enabling more targeted investigations, Nozomi has helped streamline how field teams assess and resolve issues across facilities while reinforcing operational controls.

By deploying a hybrid solution for OT and IoT cybersecurity, COPT Defense is better equipped to maintain uptime and reliability in the mission-critical environments it supports. Their team can identify anomalies faster, respond more effectively and ensure systems continue to operate as expected across a growing portfolio of properties.

Kurz credits much of their success to the strong partnership with Nozomi Networks, defined by ongoing engagement, regular check-ins and hands-on expertise to optimize the deployment and drive continued value.

"From the start, it wasn't a hard sales pitch; it was about understanding what we needed and helping us get it right. That trust is just as important as the technology," said Kurz.

As COPT Defense continues to expand, Nozomi provides a scalable foundation for consistent visibility and monitoring across new facilities, helping the organization maintain control, reduce risk, and support its mission-critical operations with confidence.

> "You have to know what you have in order to defend it. That gap in visibility and not knowing will keep any security leader up at night.
>
> **Ken Kurz**
> VP of IT and CIO, COPT Defense Properties

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com