NOZOMI NETWORKS

EBOOK

Cyber-physical Security for Data Centers

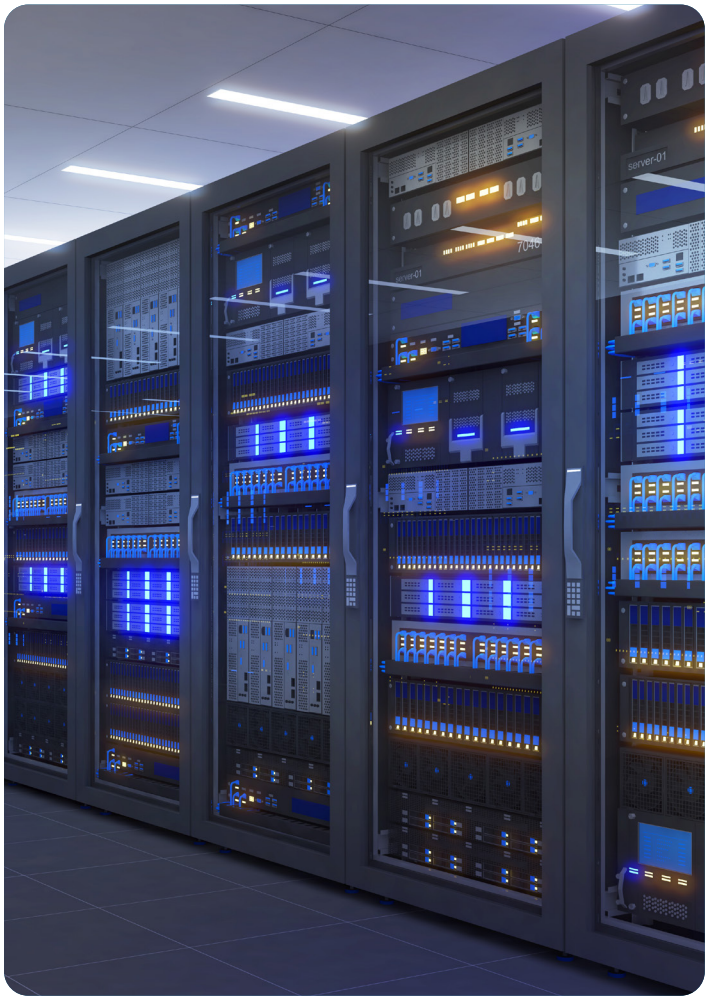
Securing the Infrastructure that Powers AI

Data Center Infrastructure: The Overlooked Attack Surface

Data center construction is booming, driven by cloud migration and the surge in AI workloads that demand massive compute power, storage space, network bandwidth — not to mention precise environmental control to ensure uninterrupted uptime.

Given their business criticality, data centers have become high-value targets for sophisticated cyberattacks. But cybersecurity priorities focus on protecting the crown jewels; that is, the rows and rows of always-on servers, often tenant-owned but under the data center's watch. Meanwhile, the building management, physical security and OT systems that control power and cooling to keep data centers humming remain a blind spot.

Whether you're responsible for the end-to-end performance of the data center or its overall cyber risk posture, securing the OT, IoT and building management systems that ensure high availability and precise environmental conditions must be in scope.



THE CHALLENGE

Reducing Cyber Risk and Maintaining Operational Resilience

Data centers face three primary cyber-physical security challenges:

Vast unprotected OT/IoT attack surfaces

Dependence on a stable energy supply

Critical infrastructure regulatory requirements

The Connected Data Center

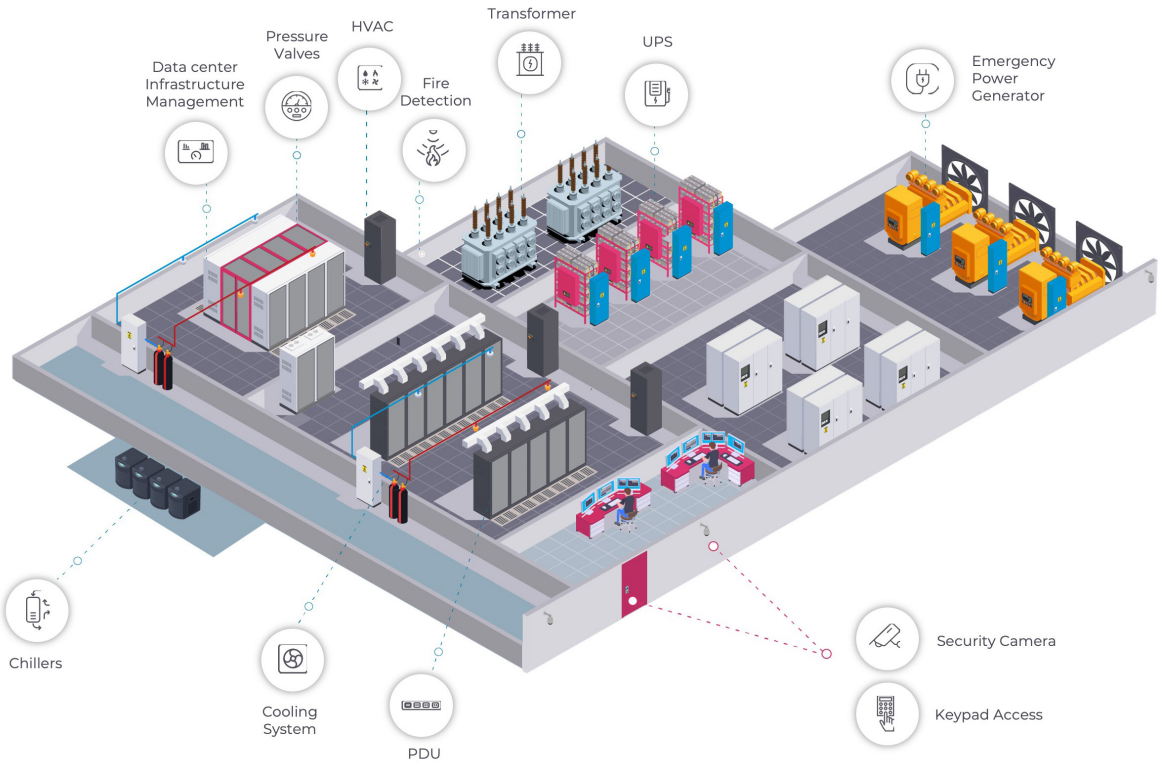
Large data centers commonly rely on thousands of OT/IoT controls to function reliably. These systems are increasingly connected for centralized monitoring, energy optimization, remote access and predictive maintenance, significantly expanding the attack surface.

Data Center IoT Assets

- Video Monitoring
- Printers and other devices
- Fire Detection and Suppression
- Smart Displays and Server Screens
- Biometric Access Points
- Access Monitoring
- Core networking switches
- End-point devices (terminals, computers)

DCIM / Building OT Assets

- Alarm systems
- CCTV/NDR
- Power/Emergency power generator
- Smart thermostats
- HVAC systems for bank building and data center heating/ cooling
- Fire detection
- Lighting control
- Door locks/keypad access/badge systems
- Data center cooling system



Cybersecurity Across Converged OT, IoT and IT Systems

IT cyber incidents may affect data confidentiality, integrity or availability, but attacks on OT and IoT systems can have harmful physical consequences.

Modern data centers leverage hundreds of cyber-physical systems to monitor and manage everything from heating ventilation to cooling systems to the uninterrupted power supply systems. Add to this CCTVs, badge access, fire suppression and other IoT systems found throughout the data center campus. These systems are more connected than ever to both IT networks and the internet, often unknowingly and with default credentials unchanged. Many of them are managed and maintained remotely by third-party vendors with round-the-clock access. Others may not be maintained at all.

When not managed as part of holistic data center cyber risk, this complex network can easily be exploited by threat actors intent on triggering cascading failures. For example, a compromise in the cooling system could overload circuits, requiring a shutdown.

Top Cyber-Physical Risks for Data Centers

As geopolitical crises morph into chronic tensions, cyberattacks on critical infrastructure meant to disrupt services and undermine public trust have become the norm.

Increasingly connected, remotely serviced and internet exposed, OT and IoT assets and networks provide access points and attack paths for threat actors that bypass IT controls, potentially causing disruption or widespread outages.

Internet-exposed DCIMs at the core of operations

The data center infrastructure management system (DCIM) integrates IT and facility management systems to monitor power, cooling, server racks and environmental sensors. Because it sits in a gray zone, it's often overlooked – and often exposed to the internet.

Cooling systems that maintain precise conditions

Whether related to a cyberattack or malfunction, a cooling system outage would lead to a rapid temperature increase, allowing just 15 or 20 minutes to shut down servers before they're damaged beyond repair.

Exploitable OT/IoT devices

Assets like CCTV cameras and temperature sensors use stripped-down OSs and minimal encryption or authentication, enabling hackers to bypass perimeter controls to gain initial access and pivot to critical systems.

Remote maintenance by third-party vendors

Dozens of vendors have remote access to OT and IoT systems throughout the data center. On any given day, there's a steady stream of technicians logging into the network for maintenance, with scant security.

Cybersecurity Regulatory Compliance for Critical Infrastructure

Data centers are now formally classified or regulated as critical infrastructure/critical national infrastructure (CNI) across most major economies. Cybersecurity oversight and regulations are common everywhere that data centers are common.

EMEA

EU - Treated as Essential Entities under the NIS2

UK - Designated as CNI, regulated under the Cyber Security and Resilience Bill

Saudi Arabia - Subject to the NCA's Essential Cybersecurity Controls and Critical Systems Cybersecurity Controls

UAE - Treated as critical infrastructure under Information Assurance standards

APJ

Australia - Subject to the SOCI Act

Singapore - Regulated under the Cybersecurity Act, with a Digital Infrastructure Act proposed to bring data centers and cloud into scope

Japan - Relevant under the Economic Security Promotion Act, which regulates designated essential-infrastructure operators

South Korea - Covered under the Act on the Protection of Information and Communications Infrastructure

India - Designated as "Protected Systems" under the IT Act

Americas

U.S. - CISA oversight as critical infrastructure; FedRAMP certification required for federal cloud providers

Canada - Covered under the Critical Cyber Systems Protection Act (Bill C-8, the successor to Bill C-26)

Brazil - Included under the National Critical Infrastructure policy

Securing the Substation that Powers AI

Data centers need a continuous and stable supply of energy to operate, namely because AI workloads are extremely energy intensive. To meet this insatiable demand, larger data centers need a dedicated power grid that they can control, especially regarding redundancy, uptime and cost.

Hyperscale data centers almost always have their own purpose-built substation. A single hyperscale campus can demand city-scale power. Colocation facilities may also build and operate their own substations. In both scenarios, data center operators must satisfy additional cyber regulations for utilities such as NERC CIP in North America, which requires ongoing, defensible proof of compliance.

> “Cybersecurity requires visibility across the system of systems. The power plant, backup power, cooling and physical access systems each have potential for misuse that could affect data center and grid stability.”
>
> **– World Economic Forum**

THE SOLUTION

A Complete Platform for OT/IoT Cyber Resilience

To achieve operational resilience and meet compliance requirements, data center owners and operators need:

Asset visibility and vulnerability management

Continuous threat and anomaly detection

Prioritized remediation for measurable risk reduction

The Leading AI-powered Platform for OT and IoT Visibility and Security

The Nozomi platform helps data centers comply with regulations and meet uptime guarantees by providing a complete, accurate inventory of OT and IoT assets, risk-based vulnerability management, continuous threat and anomaly detection, and AI-powered SOC assistance to keeps analysts focused on what matters most.

Gain Context with Unparalleled Asset Visibility and Vulnerability Management

- Build an accurate, real-time asset inventory with passive and active discovery techniques for wired and wireless networks and fluency in over 200 OT and IoT protocols, along with active scanning on sensitive OT endpoints that IT security agents may damage.
- Asset profiles are enriched via data integrations and an AI engine that learns from millions of globally monitored assets to fill in information and provide complete visibility into asset status and behavior.
- Automatically detect and assess vulnerabilities in “insecure-by-design” OT and IoT devices, many of which lack authentication, encryption and other security standards. Benefit from regularly updated vulnerability databases and OT and IoT security research from Nozomi Networks Labs.

Prevent Incidents from Becoming Outages with Continuous Threat and Anomaly Detection

- Leverage signature-based threat detection and the Nozomi Threat Intelligence feed to detect known threats, with sensors continuously updated with emerging malware and IOCs specific to OT and IoT
- Use AI-powered behavior-based anomaly detection techniques, including deep packet inspection, to detect operational anomalies and zero-days.

Prioritize Remediation Efforts So SOC Teams Never Miss a Critical Issue

- Calculate risk by asset, sensor, zone, site and enterprise using weighted risk factors that reflect asset criticality and exploitability, including CVSS, EPSS and KEV scores and more.
- Reduce alert fatigue with an AI engine that continuously identifies, analyzes, correlates and prioritizes issues across your environment, focusing attention on the threats with the greatest potential impact.

SOC Efficiency: Closing the OT/IoT Cybersecurity Gap

If anyone needs an “easy button,” it’s the overwhelmed SOC analyst new to OT and IoT security. Nozomi’s AI-powered assistant provides deep insights and clear remediation advice specific to your environment in response to prompts like these:

Show me every OT and IoT device on my network that isn't in my CMDB or asset inventory. Group them by site and by the critical system they support — cooling, power, physical access or fire suppression."

Find any device in my IT environment communicating with OT systems that control power, cooling, or physical access. Flag flows that violate my Purdue model or segmentation policy, and rank by potential blast radius to tenant SLAs."

Which external vendors have connected to my BMS, UPS, PDU, or HVAC controllers in the last 30 days? Show me the session duration, protocols used, and any commands executed on safety-critical devices."

List all OT and IoT devices running firmware with vulnerabilities on CISA's Known Exploited Vulnerabilities list. Rank by criticality to power and cooling availability, and tell me which ones have a patch available versus require compensating controls."

Where Are You on Your OT/IoT Cyber Journey? Where Do You Need to Be?

PROACTIVE

MANAGED

AD-HOC

Actively Manage Vulnerabilities

- Classify and prioritize vulnerabilities based on asset criticality and exploitability
- Exposure, vulnerability trends, and predicted risks are tracked

Have Continuous Asset Discovery

- AI-powered asset enrichment
- Targeted active queries to collect OS, firmware, patch level, etc. safely.

Proactive OT/IoT Incident Response

- Automated remediation
- AI-assisted incident response
- SOC integrated IR playbooks
- Detect and respond to wireless threats
- Threat intel is presented via threat actor profiles with recommended mitigations

OT/IoT Risk Identification, Prioritization, & Reduction

- Can communicate OT/IoT risk in business terms to the board
- Investments are prioritized based on quantified risk reduction

Automated & Centralized Asset Tracking

- Have basic vulnerability mapping
- Can visualize basic network topology, zones, and protocol use
- Global asset database
- Wired, wireless, & endpoint sensors
- CMDB integrations

Intel-driven OT/IoT SecOps

- OT/IoT specific threat intel integrated into SOC workflows
- Have deployed OT/IoT detections
- Have operational baselining of our environment

Regulatory & Standards Compliance Reporting & Tracking

- Produce auditor-ready reports for site-level and enterprise-level controls
- Can map detections and dashboards to specific controls
- Maintain customizable, multi-level risk scoring by asset, zone, site

Assets Tracked Manually

- Excel-based
- Sales orders

Fragmented OT/IoT Threat Response

- Rely on IT scanners that lack OT/IoT context
- Response playbooks are informal or inconsistent

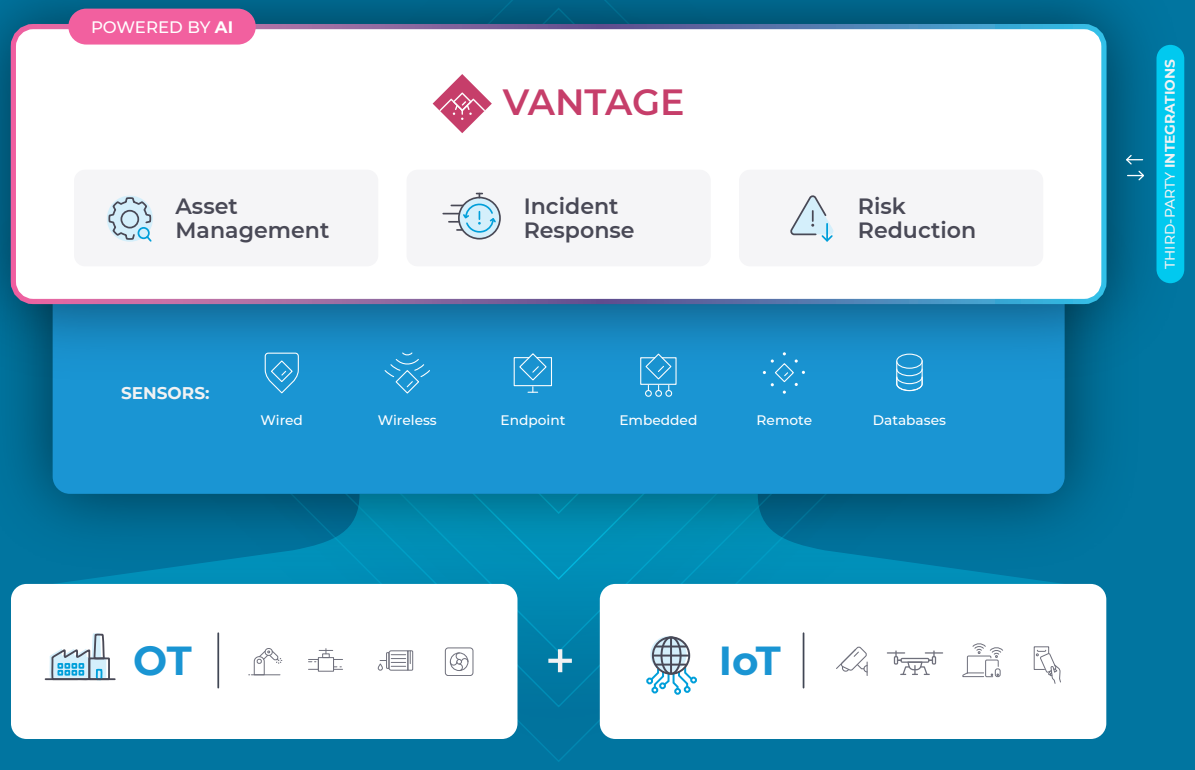
Policy & Rule Management

- OT security policies exist but are not actively implemented or audited
- Audit evidence is difficult to collect

Asset Visibility | Incident Response | Risk Management

A Complete Platform for OT/IoT Cyber Resilience

The Nozomi platform gives data centers the context, control and confidence to withstand cyber threats and keep running smoothly.



Unparalleled visibility - the foundation for operational and cyber resilience

Prevent incidents from becoming outages with OT/IoT-specific threat intel, detections and proactive response

Quantify, improve and communicate OT/IoT risk for continued cyber resilience

The only hybrid & resilient architecture that scales with your business and an evolving threat landscape

Powered by **purpose-built AI** that transforms OT/IoT telemetry into actionable intelligence

Next Steps

Find out how Nozomi Networks can help you gain context, control and confidence to withstand cyber threats — without impacting reliability and safety.

View Platform

Request a Demo

NOZOMI NETWORKS

Cybersecurity for OT, IoT and Critical Infrastructure

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.

nozominetworks.com

NN-OT-DATA-CENTER-EBOOK-001