NOZOMI NETWORKS

EBOOK

~~Un~~certainty, ~~Un~~done.

An OT/IoT Cybersecurity Strategy for Converged Environments

Table of Contents

1. Introduction

In 2026, AI-Powered Cybersecurity for OT & IoT Is Table Stakes.

Last year was a tipping point for OT cybersecurity, in terms of risk consolidation under the CISO. According to a Fortinet survey, more than half (52%) of surveyed organizations assigned CISO/CSO responsibility for OT in 2025, up from just 16% in 2022. As owners of enterprise risk, corporate CISOs must deliver on holistic strategies designed not only to protect data integrity and availability but also to ensure cyber-physical resilience — and articulate progress to their boards. Regulatory pressures to consolidate cybersecurity risk have accelerated this trend.

52% of organizations gave the CISO/CSO responsibility for OT in 2025, **up from just 16%** in 2022.

Whether you're a CISO newly assigned responsibility for OT and IoT risk, an analyst trying to make sense of OT and IoT alerts in a newly merged SOC, or a plant operator grappling with how to square new cybersecurity controls with safety and efficiency concerns, the industrial cybersecurity curve can be steep, especially since AI is changing the rules of engagement.

This eBook provides a primer on OT and IoT security, focusing on four essential ways to leverage AI to build resilience:

100% asset visibility with endpoint and wireless sensors

Holistic threat intelligence that connects the dots

Risk management for complex OT/IoT environments

SOC efficiency that closes the OT security skills gap

2. OT & IoT: The Fastest-Growing Contributors to Enterprise Cyber Risk

Across industries, OT and IoT devices are a growing percentage of total digital assets. A 2024 survey found that OT, IoT and other specialized systems comprise 42% of enterprise assets — and account for 64% of mid- to high-level enterprise risk.

In other words, the fastest-growing part of the enterprise attack surface is the part CISOs understand the least and have invested in the least, because IT cybersecurity tools don't work in OT and IoT environments. This explosion is raising questions from key stakeholders.

INDUSTRY INSIGHT

OT, IoT and other specialized systems comprise **42% of enterprise assets** - and **account for 64% of mid- to high-level** enterprise risk.

Top OT/IoT Cybersecurity Questions Being Asked

CISO:
What strategies and tools will help us prevent and contain incidents?

SOC Analyst:
What do these alerts mean? Which ones do I pay attention to?

Plant Operator:
How do I know your poeple and tools won't break something or cause downtime?

Board of Directors:
What's our risk? Could this happen to us? Translate that into business terms.

3. How Is OT Security Different From IT Security?

Here are the main ways that OT networks and devices are different and why IT security tools don't work with them:

Physical consequences:

IT manages information. OT controls physical processes, including the crown jewels that drive revenue or provide essential public services. Often, they operate continuously. If OT fails or is attacked, the stakes are higher, especially for critical infrastructure.

Cybersecurity goals:

Forgotten-once-deployed, internet-exposed devices with no encryption and unpatchable firmware are ideal pivot points to bypass perimeter defenses.

OT nuances:

IT solutions use standard operating systems, have frequent, automated updates and are upgraded or replaced every 3 to 5 years. OT assets are built to last 10 to 15 years and are "insecure by design." Patches, if available, are infrequent, and updates must occur during maintenance windows.

IT security tools don't work because they can't read hundreds of proprietary OT protocols, can't perform deep packet inspection (DPI) and can't baseline normal behavior to detect anomalies. Moreover, IT endpoint agents that are standard for antivirus protection and patching don't work on OT devices: they're heavyweight, disruptive and aren't trained on OT environments so detect the wrong threats.

4. How Is IoT Security Different From IT Security?

The Internet of Things is the ecosystem of internet-connected devices that collect, share and act on data to make the modern world hum. IoT devices are everywhere and, like OT devices, they're typically insecure by design. Added challenges call for security approaches more similar to OT than IT. For example:

Proliferation of diverse devices:

An ever-expanding number and array of IoT devices, many wireless, use stripped-down OSs and disparate protocols — and are often deployed ad hoc.

Devices that are unmanaged and insecure by design:

Forgotten-once-deployed, internet-exposed devices with no encryption and unpatchable firmware are ideal pivot points to bypass perimeter defenses.

Weak identity and access controls:

Use of default passwords and lack of strong authentication procedures, including for remote access, make IoT devices easy to exploit.

The sheer volume of diverse IoT devices — many of them wireless — combined with weak or nonexistent security controls render traditional IT security tools ineffective.

5. Asset Visibility: The Starting Point of Your OT/IoT Cybersecurity Strategy

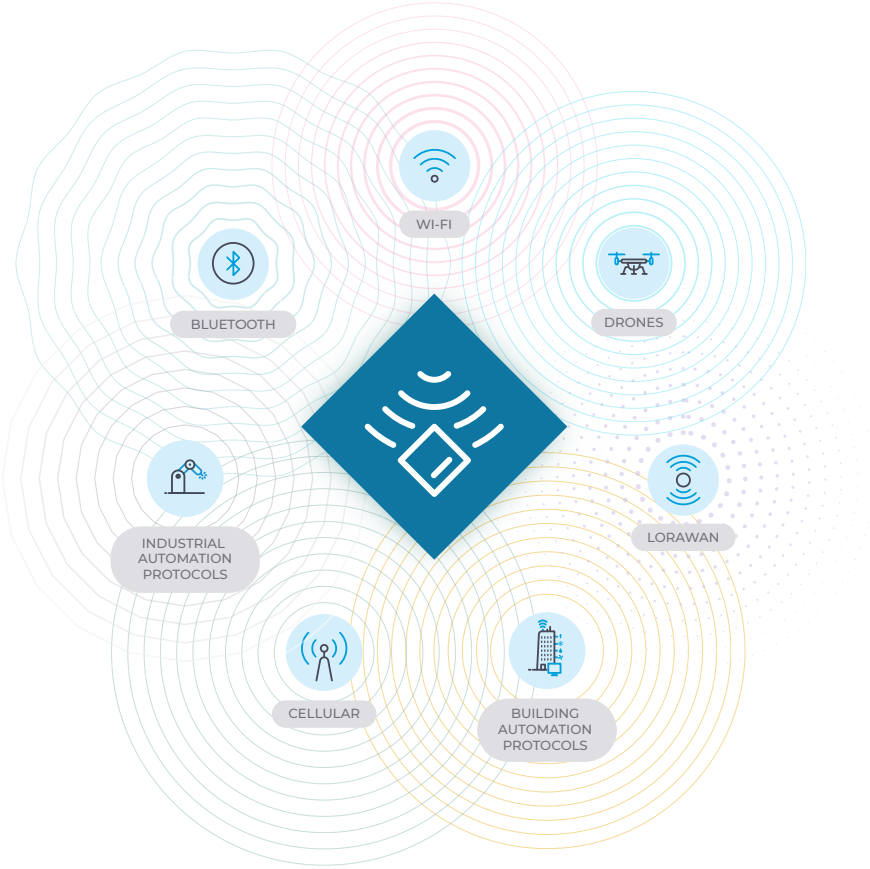
Knowing what assets you have is the foundation of all cybersecurity frameworks, regulations or programs. Indeed, full asset visibility is the starting point for effective anomaly detection, vulnerability management and, ultimately, risk management. To build a strong OT/IoT strategy for converged environments, you need a complete, automated inventory of wired and wireless OT, IoT and IT assets, with deep insights into their behavior and communications.

That requires a combination of endpoint-to-air sensors, passive and active data collection, OT/IoT protocol fluency and third-party IT asset data — using AI to fill in missing details based on matching devices, so you understand their risk.

5.1 Don't Overlook Wireless Security Sensors!

Industrial organizations increasingly rely on wireless communications for logistics, autonomous transport and monitoring, yet they're often the biggest remaining blind spot, even in mature organizations. Intermittent operation of wireless devices makes baselining normal behavior even harder.

OT/IoT wireless sensors can read protocols such as Bluetooth and cellular but also LoRaWAN and ODID, and detect wireless threats such as a deauth attack, rogue wireless access point (WAP) or wireless network infiltration using compromised credentials.



In addition to gaining visibility of your wireless network, seeing your endpoints is just as important. From there, AI-powered asset matching ensures asset inventory accuracy. Let's take a closer look.

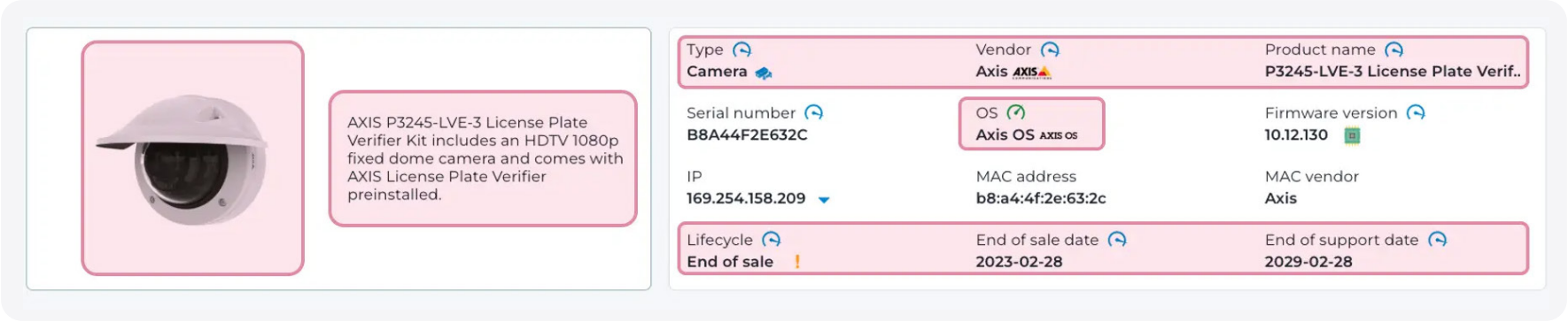
5.2 Endpoint Security Sensors

In IT security, endpoint agents are ubiquitous for anti-virus protection and patching, but negative experiences deploying them on OT devices have led to scarce adoption. Purpose-built OT endpoint sensors overcome those objections, but they must do more than collect asset details. They should also detect who's logged onto what machine when. Human interface devices (HIDs), human-machine interfaces (HMIs) and other devices are where people (including remote, third-party technicians) interact, and thus where suspicious activity happens.

5.3 AI-Powered Asset Matching

AI is indispensable for enriching asset profiles to achieve near 100% asset inventory accuracy. It can augment sensor-collected data by inferring asset types and roles based on traffic patterns and tapping a trove of details from matching devices to fill in missing data fields.

Closing these gaps helps you zero in on essential information for identifying the riskiest assets, such as which ones have known exploited vulnerabilities (KEVs).



Information outlined in red is populated from AI-powered asset matching.

6. Actionable Threat Intelligence That Covers IT, IoT and OT Threats

Most attacks impacting industrial environments originate from IT compromises before pivoting into OT. IT threat intelligence is an InfoSec staple, but it won't detect the downstream impact of a breach on OT and IoT assets.

Today's industrial and critical infrastructure environments rely on a mix OT, IT and IoT networks, so the threat detection tools monitoring them need a steady feed of high-quality, holistic threat intelligence. Insecure, unmanaged and internet-facing IoT devices are a favorite attack vector for hacktivists.

Direct attacks on OT, while less common, are on the rise due to advanced persistent threat groups and geopolitical tensions.

6.1 Curated Insights That Connect the Dots

Just as asset visibility requires more than a static database or list of IP addresses, threat intelligence is more than a raw feed of indicators of compromise (IOCs). Threat detection tools are only as good as the threat intelligence that informs them. They need detailed information in the form of Yara, packet and Sigma rules as well as STIX and vulnerability indicators specific to OT and IoT processes and devices.

As the term implies, the intelligence should be curated to deliver actionable insights into behaviors and tactics of threat actors who are actively targeting industrial environments.

6.2 Vulnerability Risk Scoring for When You Can't Patch Everything

IT has its Patch Tuesday. In OT and IoT, it's Patch Never, Next or Now. You can't patch everything, and sometimes you can't patch at all. That makes vulnerability management much more challenging.

AI-powered risk scoring is essential for prioritizing remediation. In addition to identifying KEVs, it can factor in asset criticality, exposure and what controls are already in place.

7. Risk Management for OT/IoT Environments

OT/IoT cyber risk is the potential for loss of life, injuries, equipment damage, environmental damage, revenue loss, and operational disruptions caused by the failure, misuse, or cyber compromise of connected OT/IoT systems that support industrial and critical infrastructure operations. Managing risk for complex OT/IoT environments requires a different strategy. **There are four main differences between how you assess IT risk vs. OT/IoT risk:**

1

Cyber and operational risk

In industrial environments we must account for both cyber and operational risk, including process risk, because operational anomalies unrelated to a cyber threat are far more common.

Until investigated, you don't know whether they involve a cyberattack or not.

2

Consequence-based risk

In OT, risk assessment is almost entirely focused on consequences such as physical safety, the environment and continuity of operations — all of which impact revenue. Whether you're assessing risk in a warehouse or on a cargo ship, with OT you're always planning for your worst day.

3

Interconnected risk

Every component in an OT network is part of a larger process in a distributed environment. If one machine has a problem, you need to know what it depends on and what is depending on it. From there, what are the consequences of an emergency shutdown?

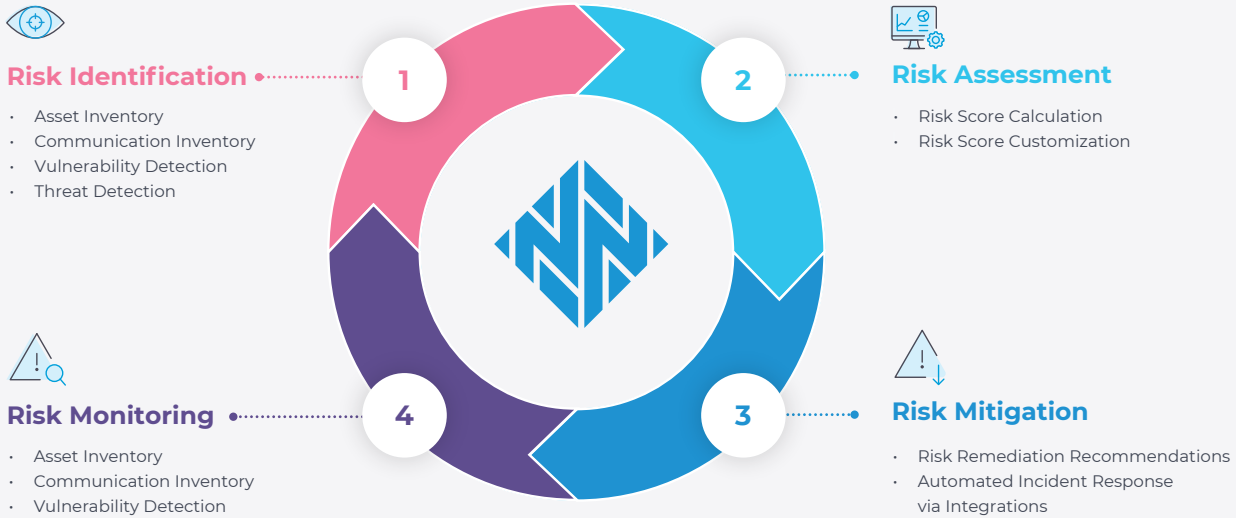
4

Vulnerabilities-only vs. multi-dimensional risk

In IT, device risk is based solely on vulnerabilities, and you can practically eliminate risk with patching. In OT, it's multilayered — and patching isn't always an option. In addition to vulnerabilities, you need to consider alert risk, communication risk, device risk, asset criticality and compensating controls.

8. The Four Steps to Continuous OT/IoT Cyber Risk Management

There are four steps to continuous OT/IoT cyber risk management: Risk Identification, Risk Assessment, Risk Mitigation and Risk Monitoring. The Nozomi Networks platform simplifies each phase in the cycle, enabling you to detect threats before they can cause harm, mitigate vulnerabilities before they can be exploited and minimize damage should an incident occur. In doing so, it helps operators and SOC teams collaborate to prioritize efforts and take the most impactful actions to reduce risk and increase resilience.



9. SOC Efficiency: Close the OT/IoT Cybersecurity Gap

If anyone needs an “easy button,” it’s the overwhelmed SOC analyst new to OT and IoT security. When AI infuses every aspect of your cybersecurity platform — from asset inventory to behavior baselining to threat and anomaly detection to vulnerability management — those capabilities culminate in the SOC, where the most critical information must be surfaced so analysts never miss a critical issue. Not just displayed but continuously refreshed, correlated and prioritized by risk, with drill-down access to more insights and what to do next.

Offloading the tedious tasks of reviewing, correlating and prioritizing thousands of data points to a tireless AI engine can potentially eliminate the need for Tier 1 SOC analysts and other junior positions altogether. No more sifting through the noise for a few alerts that matter. No more being stumped about what to do, not just about this one alert but to reduce the most risk overall.

Hello, Ask Me Anything About Your Environment

AI assistants have taken off because they provide instant answers to plain-language questions that might otherwise require hours of research. No doubt SOC analysts are turning to commercial chatbots for help, but for reliable answers they need an AI assistant they can engage with that is OT and IoT aware and can respond contextually based on what’s happening in their environment.

Instead of just asking a general compliance question about, say, NIS2 or IEC 62443 requirements, **they can ask whether their specific environment is compliant and, if not, what to do in what order.**

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.

© 2026 Nozomi Networks, Inc. | All Rights Reserved.

nozominetworks.com

NN-OT-IoT-STRATEGY-EBOOK-001