NOZOMI NETWORKS

EXECUTIVE BRIEF

Closing IoT Security Gaps in Your Operations

Industrial networks are quickly adopting Internet of Things (IoT) technologies to reduce costs and deliver more value to customers and shareholders. Unfortunately, this trend is creating new security risks, as many organizations lack the ability to monitor and secure their IoT assets.

The challenges will only increase over the next few years as industrial organizations deploy 5G with the capacity to support hundreds of thousands of IoT assets in their global operations.

Business and security leaders need to get ahead of the risks and challenges coming their way. This brief provides insight into the issues involved in securing IoT assets and effective ways to overcome them in your OT environments.

> **The IoT Security Dilemma** - Today, you cannot secure an OT network without also securing the IoT devices on it. IoT usage is surging, expanding the attack surface and exponentially increasing the volume of devices and data that needs monitoring. My main recommendation for securing OT infrastructure is to embrace a cloud-based OT/IoT security strategy that delivers flexibility, scalability and simplicity – now.

Andrea Carcano, Co-founder and CPO, Nozomi Networks

Industrial IoT Will Account for 70% of All IoT Connections

Juniper Research predicts that there will be **83 billion IoT connections** by 2024, a 130% increase over 2020.[1]

The industrial sector, including manufacturing, retail and agriculture, will account for over **70% of all IoT connections** by 2024.

Every OT Network Is an IoT Network

IoT Adds Value To Any OT Environment

A 2019 report surveying over 3,000 IT decision-makers and developers found that 94% of businesses expect to be using IoT by the end of 2021.[2]

The five most common reasons for the adoption of IoT were:

- Operations Optimization
- Employee Productivity
- Safety and Security
- Supply Chain Management
- Quality Assurance

The improved communication, instrumentation and analytics enabled by IoT technology adds value in virtually any OT environment.

For example, the report found that the top three IoT use cases in the manufacturing industry were to improve automation, increase quality and compliance, and improve production planning.

By gaining visibility into production equipment performance, manufacturers can identify problems and take action to prevent maintenance-related disruption. Detailed operations data can also be used to improve safety and inventory management, and adapt quickly to changing demand.

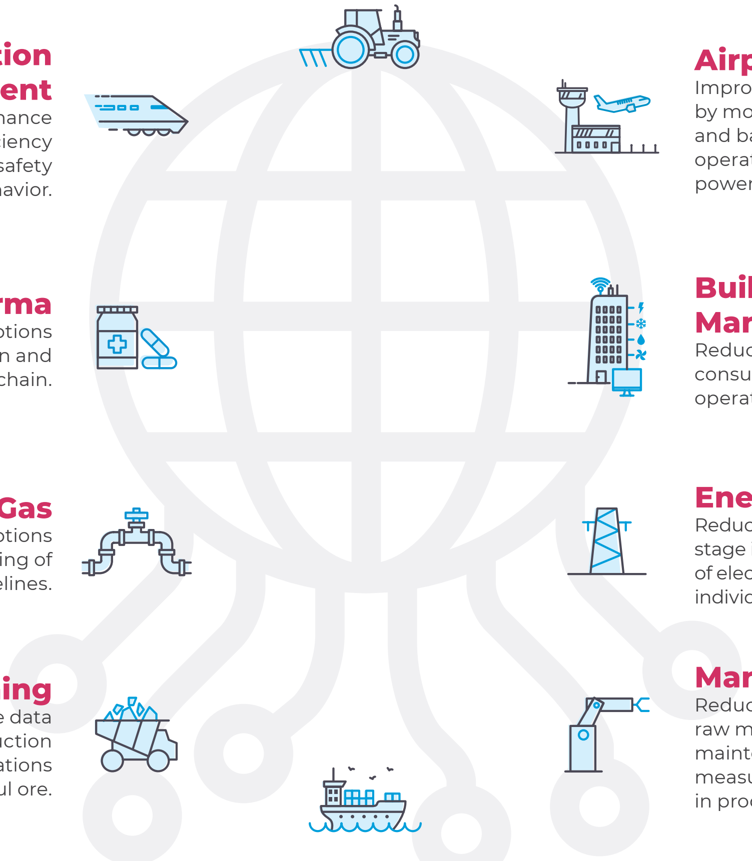
IoT technology helps industrial organizations realize many benefits, including lower production and energy costs, among others.

> Gartner
>
> As cyber-physical systems continue to multiply due to IT/OT convergence or IoT-/industrial IoT (IIoT)-type deployments, they increase and blend risks in the cyber and physical worlds. **As a result, the siloed nature of today's security disciplines becomes its own risk and a liability to the organization.**
>
> ***Predicts 2021: Cybersecurity Program Management and IT Risk Management, Gartner, 2021***

Unlimited IoT Use Cases in Every Industry

Agriculture

Increase productivity by measuring ground humidity, precipitation, and amount of sunlight.



Transportation Fleet Management

Lower costs and reduce maintenance disruptions by monitoring fuel efficiency and engine performance; Improve safety record by monitoring driver behavior.

Pharma

Reduce manufacturing disruptions by monitoring production and distribution supply chain.

Oil & Gas

Reduce unplanned disruptions through improved monitoring of pumps and pipelines.

Mining

Improve the accuracy of ore data during drilling to increase production efficiency; Automate fleet operations with driverless trucks to haul ore.

Airport

Improve passenger experience by monitoring security queue and baggage handling; Reduce operational costs by optimizing fleet, power grid and building management.

Building Automation Management

Reduce costs by optimizing energy consumption and maintenance operations.

Energy

Reduce disruptions by monitoring every stage in transmission and consumption of electricity, from substation to individual meter.

Manufacturing

Reduce downtime by monitoring raw material supply chains; Reduce maintenance-related disruptions by measuring equipment performance in production processes.

Maritime/Ports

Improve flow of containers by monitoring location of vehicles and goods, status of cargo, local terminal parking and traffic congestion.

> **Gartner**
>
> Organizations need to better understand and assess the existence and impact of IoT devices connecting to their infrastructures, **and the potential vulnerabilities these devices may present.**
>
> ***Market Trends: IoT Edge Device Security, Gartner, 2020***

What Drives the IoT Security Gaps in Industrial Networks?

The Challenges of an Expanding Digital Footprint

Ongoing OT/IT convergence in pursuit of competitive advantage is accelerating the consolidation of two formerly separate networks:

- OT (the systems that monitor and control physical processes)
- IT (the systems that transmit, manage, and store data)

Greater access between internet-facing IT networks and OT networks means that threat actors are targeting OT/IoT assets more frequently.

- IBM Security reported a **2,000% increase in incidents targeting OT in 2019**[3]
- Nozomi Networks Labs reported that 2020 saw an increase in IoT botnet, ransomware and COVID-19-themed attacks on OT and IoT networks[4]

In other words, the significant benefits offered by adding IoT assets to your network also bring significant risks. IoT assets can expose your networks to a range of challenges, including:

- Seeing all your assets, their connections and behavior
- Assessing risks and ensuring high cyber resilience
- Implementing a visibility and security solution that scales sufficiently

Limited Visibility of Assets and Behaviors

The significant increase in the number of IoT assets in your OT networks – and the volume of data they generate – can create monitoring and security challenges for your operations and security teams.

In addition, the IoT assets in your OT environments communicate with different protocols than OT assets. Most network monitoring and security controls used in OT environments are designed to analyze only the proprietary protocols and device behavior of OT assets. They're not designed to monitor IoT protocols or IoT device behavior, and consequently have only limited visibility of IoT assets on the network.

Conversely, monitoring OT environments using security controls designed for IoT networks provides only limited value to operations or security teams. These tools frequently lack understanding of OT protocols or device behavior, preventing them from detecting anomalous or malicious behavior.

“

Gartner

> While most organizations are still in the awareness phase, Gartner interactions show that when they deploy asset discovery tools, most organizations are shocked by the number of connected assets they were not aware of... **Most are equally shocked at the security posture of these assets...**

Predicts 2021: Cybersecurity Program Management and IT Risk Management, Gartner, 2021

Limited Security and Scalability Widen the Gaps

Limited IoT Security

Your security teams may also find it challenging to secure the IoT assets they have already deployed. IoT devices often present security teams with several challenges, including:

- Vulnerable firmware that can't accept patches
- Weak default passwords
- Limited capacity that prevents installation of endpoint protection agents
- Non-hardened operating systems that are susceptible to code insertion
- Unknown software component supply chain that is subject to vulnerabilities

In their 2020 survey of 200 organizations in North America and Europe that had deployed IoT assets, Syniverse/Omdia reported that "50% of enterprises report that ensuring data, network and device security is their biggest challenge when adopting IoT solutions."[5]

The top three IoT security concerns were:

58%	**Protect against malware/ransomware**
55%	**Protect against theft of data/financial loss**
52%	**Prevent accidental leakage of confidential data/intellectual property**

Those concerns had a direct effect on the success of their IoT initiatives. The same survey found that "86% of enterprises using IoT reported their IoT deployments have been delayed or constrained by security concerns."

Additionally, not following best practices in the deployment of IoT devices can create significant risks. In a 2018 SANS survey, 32% of respondents stated that their industrial IoT assets connect directly to the internet, bypassing traditional IT security layers.

Harder to Scale

As you deploy IoT assets at scale, your security team may find that it can't monitor and analyze the data from thousands of new assets for anomalous or malicious behavior.

Many industrial organizations discover that their on-premises monitoring and security technologies lack the capacity to analyze all the data generated by widespread deployment of IoT sensors.

This monitoring problem will only increase with the adoption of 5G technology. It will increase asset capacity from approximately 100K per square kilometer under 4G LTE technology to approximately 1 million per square kilometer under 5G, with higher data transfer speeds (up to 100 times faster than 4G) and lower latency.[6]

Achieving Visibility and Security at Scale

Nozomi Networks Closes Your IoT Security Gaps

Nozomi Networks accelerates your digital transformation by providing exceptional network visibility, threat detection and operational insight into your OT and IoT environments. We help many of the world's largest and most successful companies unify their cybersecurity visibility and monitoring.

We designed Vantage™ to leverage the power and simplicity of software as a service (SaaS) to help you close your IoT security gaps. It delivers unmatched security, visibility and scalability across your OT, IoT, and IT networks.

Visibility

Vantage allows you to centrally monitor your networks without deploying agents. Our sensors detect and monitor the behavior of all OT, IoT and IT assets connected to your OT network, delivering critical visibility of every asset in your network.

Security

You can protect any number of OT, IoT, IT, edge, and cloud assets, anywhere. The platform's comprehensive approach unifies essential security technologies: vulnerability assessment, risk monitoring, anomaly and threat detection. The result is the detailed awareness of cyber threats, risks, and anomalies you need to detect and respond quickly and ensure cyber resilience.

Scalability

The power of SaaS enables you to scale quickly with cloud-based management and analytics that support any size network any number of locations. The simplicity of SaaS enables you to consolidate all OT and IoT monitoring and security management into a single application, accessible from anywhere in the world.

With Vantage, it is possible for you to realize the benefits of IoT devices *and* close your IoT security gaps.

You can use Nozomi Networks Vantage to improve security and visibility across your OT, IoT and IT networks. Visit: **nozominetworks.com/vantage**

Customer Reviews

Customers Give Nozomi Networks Top Score

★★★★★

Good For Both Operational Insights And Visibility Over Security Breaches

A robust solution that gives us all the insights we need about our OT network security. Visibility over the OT network and the automatically illustrated topology diagram, it shows us devices even we aren't aware of and their corresponding connectivities and communications. It is also easy to deploy and configure.

Services Technical Director ›

Increase OT Cybersecurity Posture Through Network Visibility

Nozomi Networks Guardian allows to increase visibility of OT environment, identifying IT and OT devices connected to the network, and highlighting vulnerabilities and anomalies. The solution gathers information analyzing network connections and provides aggregated results in a simple and intuitive interface.

Chief Information Security Officer ›

Once You Try Nozomi And Its Rich Feature Set You Cannot Imagine Operating Without It!

We put Nozomi head to head against other similar products and the Nozomi platform was able to pick out and properly categorize more L2 devices than any other tool in the market place at the time of test.

Security Analyst ›

For more reviews, visit **our website.**

See All Reviews

References

1. **"IOT ~ THE INTERNET OF TRANSFORMATION 2020,"** Juniper Research, Markus Rothmuller, Sam Barker, April 2020.
2. **"IoT Signals Report,"** Microsoft Azure, November 2020.
3. **“IBM X-Force Threat Intelligence Index 2020,”** IBM, February 2020.
4. **“OT/IoT Security Report 2020 1H,"** Nozomi Networks, September 2020.
5. **"Connected Everything: Taking the I out of IoT,"** Syniverse/Omdia, Alexandra Rehak, Pablo Tomasi, April 2020.
6. **"Telecom Experts Plot a Path to 5G,"** IEEE Spectrum, October 2015.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

EB-CLOSING-IOT-SEC-GAPS-8.5x11-002

nozominetworks.com