NOZOMI NETWORKS

EBOOK

# Manufacturing: Improving Operational Resilience

# **Manufacturing:** An Industry in Transition

Faced with tough competitive pressures and looking for improved efficiencies at scale, manufacturing companies are embracing digital transformation. Investments span greenfield and brownfield facilities, from the production floor to newly added IoT devices.

Industry 4.0 is taking place in a world of uncertainty. Pandemic effects, supply chain disruption, climate change and political factors are making constant change the new normal.

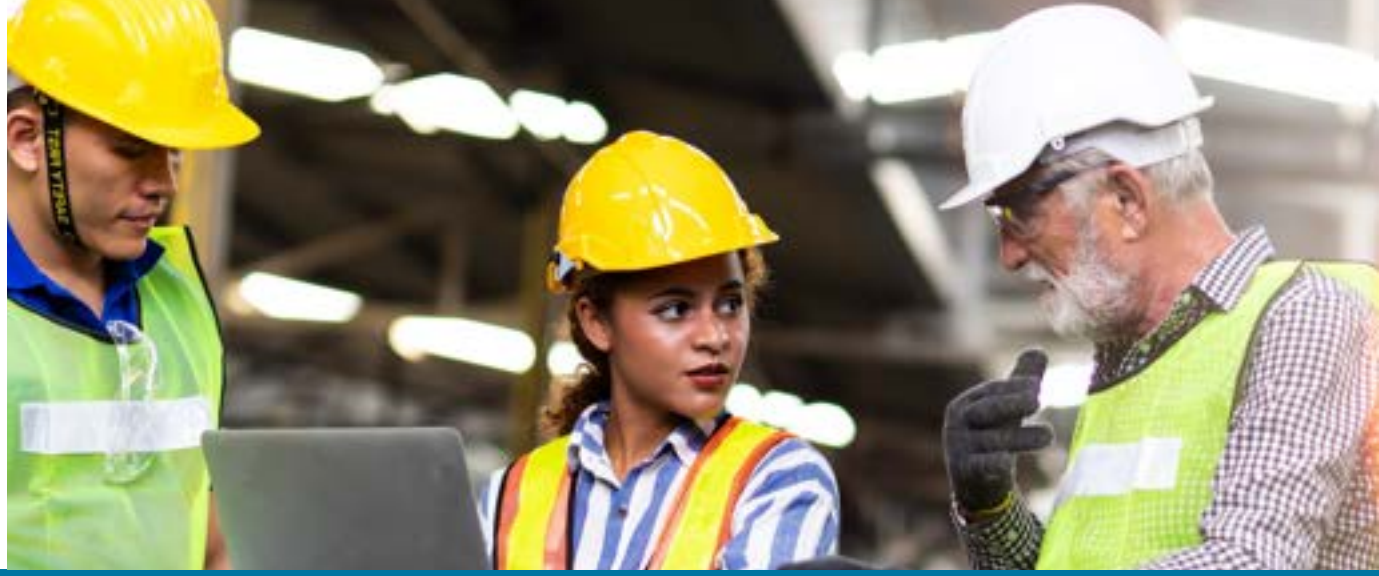
Skilled worker shortages and further reliance on remote work are adding new levels of complexity.

How do you navigate all this change and ensure business continuity? To ensure operational resilience, you need visibility and cybersecurity for all your plant networks—using a solution and vendor with deep manufacturing expertise.

Read more about **Manufacturing Industry Trends →**

# The Transition to Industry 4.0 is Complicated and Involves:



### Transformation of processes and systems

Manufacturing industrial control systems (ICS) can be very complex, often consisting of disparate networks, assets, and protocols. A shortage of specialists with deep OT knowledge makes Industry 4.0 projects particularly challenging.

### Increased use of IoT technologies

IoT technologies are a key element of smart factories, expected to optimize operations, increase productivity, cut costs and ensure high product quality. Advances in robotics, cloud computing, and the deployment of 5G are going to expand reliance on IoT. In addition to productions systems, other systems that impact a facility's availability such as access control, fire, lighting and HVAC, contain more and more IoT endpoints.

### The OT network is no longer just an OT network

As more IT and IoT devices are added to OT networks, the lines between IT and OT become blurred. IT departments must now monitor and secure not only IT systems, but also operational environments, which include rapidly multiplying IoT devices—and their vast attack surface.

# **The Challenge:** Transforming While Ensuring Business Continuity and Cyber Resilience

For manufacturers, digital transformation is a double-edged sword. On one hand, it's the only path towards maintaining a competitive edge. On the other hand, it makes smart factories more vulnerable to cyber risks and downtime threats. Companies with a mix of brownfield and greenfield sites need a solution that reduces cyber risk and improves operational resilience—at scale.

**Manufacturers face three major challenges:**

**Increased cyber risk**

**Threat of downtime**

**Legacy equipment**

> *The traditional network-centric, point solution security tools originally deployed in critical infrastructure operations are **no longer adequate** to account for the speed and complexity of the emerging threat environment.*
>
> ***Gartner, November 10, 2021***

## Increased Cyber Risk

Threat of Downtime

Legacy Equipment

**#2** Manufacturing is **the number two most targeted** sector for ransomware attacks.[1]

As cyber threats continue to escalate, manufacturing is increasingly a target. More and more connected systems create more exposure to cyberattacks. Motivated by the need to avoid a data breach or successful ransomware attack and keep business running, security and risk management has become a top focus of boards of directors.

When a cyberattack strikes, it might not be just the IT networks that are impacted; production can come to a standstill. OT and IoT systems might be compromised or taken offline to protect them.

Converging OT, IoT and IT systems can lead to resilience issues caused by lack of visibility and limited access to real-time operational data. Manufacturers need contextual asset, vulnerability, threat and anomaly information to prioritize and mitigate risks to their vital production and facility networks.

*1. Crowdstrike 2021 Global Threat Report*

Increased Cyber Risk

**Threat of Downtime**

Legacy Equipment

**As new systems are added,** the potential for network instability, manufacturing process anomalies and failing equipment increases.

In addition to cyberattacks, factory automation puts operational reliability at risk. Unplanned downtime can happen for multiple reasons—a component breaks down; a networking change impacts the production lines; or a cyber incident disrupts communication. While you are figuring out what happened and how to fix the problem, valuable production time is lost.

Manufacturers need process and stability monitoring for production and automation systems. Such monitoring gives early warning of failing equipment, unusual variable values, and networking communication anomalies. Engineers and networking specialists can then act to resolve issues before they impact manufacturing output or quality.

Increased Cyber Risk

Threat of Downtime

**Legacy Equipment**

Legacy systems were not built to withstand **today's sophisticated cyber threats.**

As manufacturers transform, they uncover a vast quantity of operational assets in their legacy manufacturing networks that must now be identified, monitored, and secured. Many are beginning to understand the extent of what they don't know.

Securing aging control systems is difficult because most assets lack intrinsic security and are sensitive to network and firmware changes. Many ICS assets communicate using proprietary protocols that must be deeply and carefully analyzed to identify suspicious or anomalous behavior.

Staff with deep OT knowledge are essential to securing older systems comprehensively and efficiently, yet such specialists are in short supply.

# **The Opportunity:**
# See, Detect, Respond

Fully connected smart factories have a large attack surface and are increasingly the target of threat actors. Geographically dispersed operations, diverse equipment, and quickly evolving IoT systems require monitoring that is scalable to keep up with a growing and evolving organization.

The only way to increase situational awareness and fix issues before they cause disruption is with accurate and deep IT, OT and IoT visibility and security.

**To stay ahead of cyber threats and ensure operational resilience, you need to:**

## See

Comprehensive OT, IoT and IT visibility

## Detect

Stability, threat and anomaly detection

## Respond

Actionable intelligence and playbooks

**See**

Detect

Respond

## Comprehensive, Real-time Visibility

*Do you really know what devices are on your network and how many there are? Which ones are actively communicating and what protocols they are using? Would you know if someone intentionally or accidentally changed the configuration on a PLC or deleted a log file?*

To spot and troubleshoot networking and communication issues that threaten reliability, you need real-time visibility into your assets, connections, communications, protocols and more.

By automating asset inventory, you eliminate blind spots and reveal assets that might have been previously missed. You save time and money by using a solution that builds always up-to-date inventory vs. relying on snapshots of data.

What's needed is a vendor that provides extensive depth and breadth of protocol support, including deep, accurate analysis of ICS protocols. You want maximum coverage of all your OT, IoT and IT assets from all systems—no matter their age, vendor or function.

For many manufacturers, updating their asset inventory requires time-consuming manual data collection and spreadsheet work. This was the case at a building materials manufacturer who believed they had 3,000 assets in one section of a plant. **Minutes into deployment of the Nozomi Networks solution they were shocked to see they had 15,000+ assets.**

See

**Detect**

Respond

## Advanced Threat and Anomaly Detection

*In manufacturing, one small change or networking issue can have a significant effect—on product quality, production uptime, and even on plant safety. Staying on top of what's happening in your industrial control network, including visibility into assets, connections, communications, protocols and more, helps improve stability.*

At the same time, continuous detection of vulnerabilities, threats, and anomalies allows you to evaluate and address cyber and operational threats before they cause harm.

Manufacturers need a solution that identifies threat indicators of compromise, or variable values never seen before—so you can mitigate risks as soon as possible.

**A pharma manufacturer that deployed the Nozomi Networks solution reduced time to visibility by 99%.** The customer was able to identify and locate vulnerable assets for all facilities across the enterprise in ~2 minutes, instead of approximately 4.5 hours of data gathering. The increased visibility reduced the mean time to respond (MTTR), thereby improving operational resilience.

See

Detect

**Respond**

**Time-Saving Playbooks and Forensic Tools**

*As important as it is, situational awareness is not enough. You need to know how to treat the alerts that signal cyber risk or anomalous behavior.*

A system that summarizes and prioritizes risks, with actionable intelligence and playbooks for remediation, helps you efficiently and systematically make your facility more secure.

And, to analyze potentially problematic network changes over time, or execute fast incident response, strong, forensic timeline analysis and query tools are needed. For manufacturers, this translates into maximized uptime, and consistent product quality and production volumes.

A defense manufacturer needed to track network changes over time. Digging through various sources of data resulted in “analysis paralysis.” **The Nozomi Networks TimeMachine™ capability resulted in a 90% reduction in time to visibility and forensic analysis with reduced use of resources.**

# Taking Action

Manufacturers who understand these challenges, and recognize that the right vendor can help mitigate risk while ensuring business continuity, will be the ones that come out ahead.

**Here are three strategies you can act on now:**

## Bridge the IT/OT divide

## Leverage existing technology investments

## Scale up

## Learn more about our products

### Guardian™

**What is it?** Sensors that analyze and visualize data from manufacturing networks.

Learn More

### Vantage™

**What is it?** SaaS that scales security monitoring and visibility for global manufacturing OT, IoT and IT environments.

Learn More

***Effective not only for production systems, but all systems needed to keep facilities operating, including CCTV, access control, fire systems, lighting and HVAC systems.***

## Bridge the IT/ OT divide

Leverage existing technology investments

Scale up

*Attackers know how to exploit IT/OT defense gaps. To reduce risk, it's essential that IT and OT teams combine forces.*

*IT personnel generally have better cybersecurity and cloud expertise, whereas OT staff know how to keep cyber-physical processes running. A solution that improves the effectiveness of both teams and helps them collaborate is one that accelerates operational resilience.*

OT needs a "no process risk" solution that provides comprehensive visibility and monitoring for all systems and assets. A system that helps maximize production uptime and provides insight into risks such as failing equipment and unusual variable values is ideal.

IT needs to secure operational environments, starting with visibility into OT and automation systems, and their cybersecurity gaps. A system that consolidates information from all facilities, prioritizes vulnerabilities and threats, and expedites response with actionable intelligence is ideal.

**Read our manufacturing solution infographic to see how Nozomi Networks delivers smart cybersecurity for smart factories.**

**Download**

Bridge the IT/ OT divide

**Leverage existing technology investments**

Scale up

*A cybersecurity solution for manufacturers needs to not only help OT and IT do their jobs more effectively, but seamlessly integrate with key applications across the enterprise IT/IoT/OT ecosystem*.

Companies make significant investments in technology solutions. Using and maintaining all technologies requires significant commitment and resources, which is why CISOs are streamlining their vendor line-ups.

In the case of manufacturing network visibility and security, it's necessary to use a "no process risk" solution specifically designed for operational environments, with extensive built-in ICS and protocol expertise.

At the same time, such a solution needs to integrate seamlessly with other IT/OT applications, including SIEMs, asset management systems, IAMs, firewalls, and ticketing systems. Holistic integrations improve data analytics as well as resource and workflow efficiency.

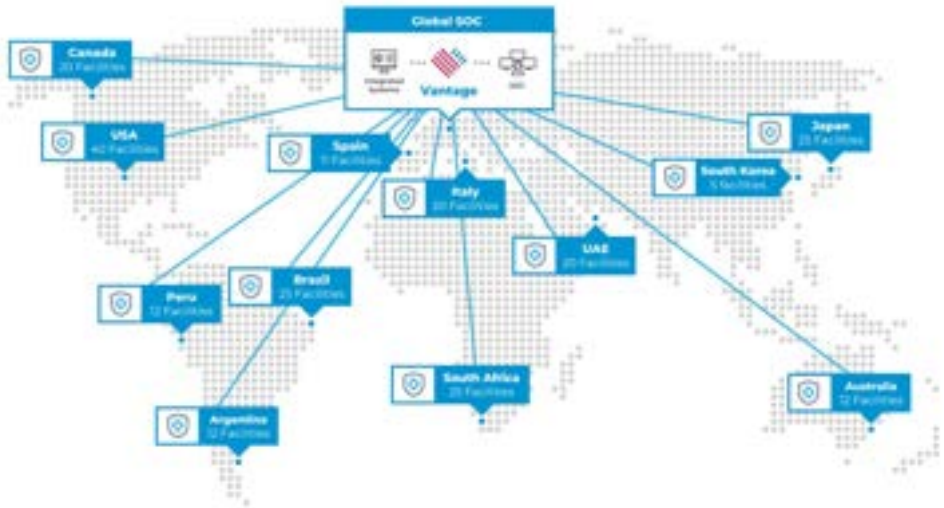
Bridge the IT/ OT divide

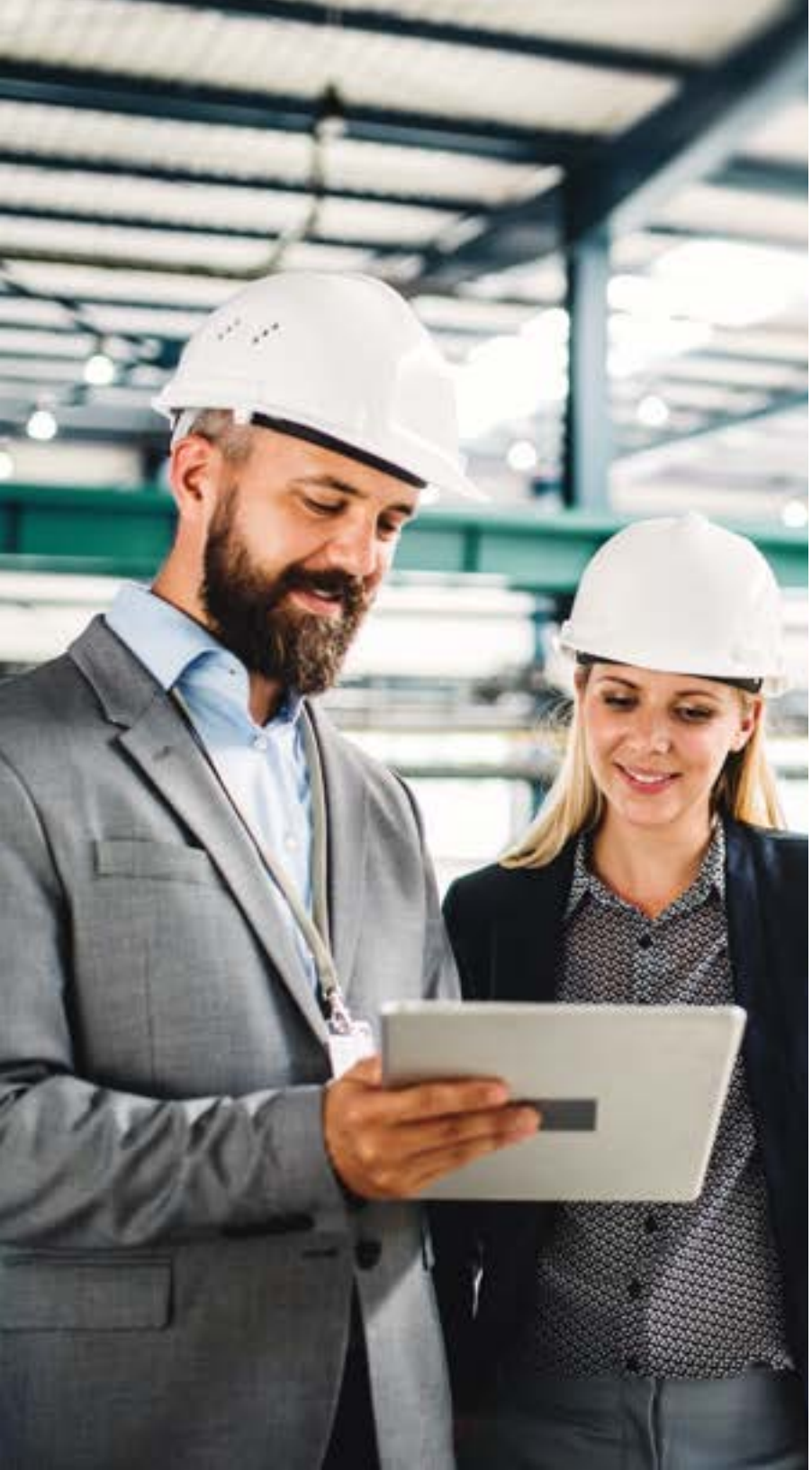
Leverage existing technology investments

## Scale up

*Geographically dispersed operations and quickly-evolving IoT systems require monitoring at scale. It's critical to implement a solution that can protect any number of OT, IoT, IT, edge and cloud assets.*

A SaaS-powered application provides a single pane of glass view of aggregated and prioritized risks across all facilities. It scales quickly and reduces complexity and cost. Paired with a wide range of onsite sensors, such a system meets the needs of any factory ecosystem.





# What Does **Success Look Like?**

**Case Studies:**

- Industrial equipment manufacturer
- Pharma manufacturer
- Medical technology company

# Industrial Equipment Manufacturer

## The Challenge:

### A Fortune 500 industrial equipment manufacturer realized:

IT security was not able to protect their plant networks

They lacked visibility into each facility's mix of unsupervised IT and OT networks

They needed to secure hundreds of plants all over the world

## The Result:

### The Nozomi Networks solution was deployed in 120+ plants, with more scheduled. The results include:

A comprehensive asset inventory of OT networks

Improved network understanding which has facilitated network segmentation efforts

Implementation of vulnerability management and OT network monitoring

Initiation of threat detection and incident response procedures

Planning for Vantage™ deployment for centralized management and increased global asset/alert correlation

# Pharma Manufacturer

## The Challenge:

### A global pharma company headquartered in Europe wanted to:

Improve supply chain visibility

Integrate isolated data into the SOC

Gain visibility into acquired network operations

Satisfy regulatory requirements

## The Result:

### After deploying the Nozomi Networks solution in 15 countries, including SIEM, IAM and firewall integration, the company achieved:

Improved supply chain visibility

Automated detection of operational anomalies

Accelerated response to potential disruptions to supply chain

# Medical Technology Company

## The Challenge:

**A global medical technology company, headquartered in the U.S., wanted to:**

Improve visibility into global manufacturing processes

Protect production lines against downtime

Minimize the impact of potential security incidents

## The Result:

**After deploying the Nozomi Networks solution (100+ Guardian appliances) in several countries, the company was able to:**

Achieve a more mature security posture

Build a robust defense against cyberattacks

Improve the availability and reliability of the manufacturing process

Establish a Corporate Security Center of Excellence.

# Manufacturing Customer Reviews
# Gartner Peer Insights

★★★★★

**ROLE:** CISO EMEA
**INDUSTRY:** MANUFACTURING
**COMPANY SIZE:** 10B – 30B USD

## 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.

★★★★★

**ROLE:** MAINTENANCE COORDINATOR
**INDUSTRY:** MANUFACTURING
**COMPANY SIZE:** 250M – 500M USD

## OT Visibility

It significantly opened up our vision of security and identified hundreds of fails that were hidden. The process of discovering hidden things was extremely interesting, many fails were solved through use.

★★★★★

**ROLE:** SECURITY ANALYST
**INDUSTRY:** MANUFACTURING
**COMPANY SIZE:** 1B – 3B USD

## 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.



More **Reviews** from Manufacturing Customers

NOZOMI NETWORKS

# Next Steps

Find out how Nozomi Networks can help you improve operational resilience, visibility and security at your manufacturing facilities:

Manufacturing Webpage

Request a Demo

# Want to **Learn More?**

## About Nozomi Networks and Manufacturing

Nozomi Networks is the leading provider of OT, IoT and IT visibility and security solutions for industrial manufacturers. Our deep OT expertise and extensive protocol coverage provides more asset coverage than any other vendor. This results in accurate detection of cyber threats, risks, and anomalies, and improves operational resilience—no matter the age of the facility or the scale of the challenge.

## Additional Resources:


Industry Trends


Solution Infographic


Industry Brief – Manufacturing


Industry Brief - Pharmaceutical


Case Study


White Paper

NOZOMI NETWORKS

# Thank You!

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

**nozominetworks.com**

EBOOK-MFG-Improving-Op-Res-8.5x11-001