NOZOMI NETWORKS

EXECUTIVE BRIEF

Business Leaders Need to Quickly Shift Focus to Industrial Cybersecurity

Cyberattacks on critical infrastructure and strategic industrial assets are one of the top five global risks, according to the executives and world leaders who participated in the World Economic Forum's 2020 Global Risk Report.[1]

To keep critical systems running and protect the financial results and reputation of your organization, it is essential to improve industrial cybersecurity. Cyberattacks have cost companies millions of dollars through the disruption of services and critical operations. Without visibility and cybersecurity, customer and employee safety are at risk.

Today's business leaders are expected to protect the entire organization beyond enterprise IT systems, including operational technology (OT) environments.

Frost & Sullivan

"With an impressive understanding of the expanding markets it serves, Nozomi Networks is transforming traditional ICS cybersecurity to pinpoint OT and IoT threats in real-time and address an even broader set of customers with solutions that unify OT, IoT and IT security monitoring."

ARC Advisory Group

"Nozomi Networks is a leading supplier of continuous OT network monitoring solutions. Organizations around the world use the company's security platform to protect critical infrastructure."

Enel, Global Energy Provider

"With Nozomi Networks Guardian we can now detect and collect operational and cybersecurity issues in real-time and take corrective actions before the threat can strike."

Head of Cybersecurity Design, Enel

Focus on Industrial Cybersecurity

Two of the most important measures you can take to mitigate OT risk are to bring together your IT and OT teams and invest in new technology designed to improve the visibility and cyber resilience of industrial networks.

Why align IT and OT? Because the technologies they use are converging and their systems are becoming more and more connected. When IT and OT join forces, there is an opportunity to reduce risk and cost, and speed projects.

Why invest in new OT technology? Because it improves reliability and cybersecurity, as well as staff productivity and teamwork – and it is much simpler than you might expect, delivering nearly immediate ROI.

Learn how taking these two important steps can help you proactively reduce cyber risks, including damage that could be caused by cyberattacks.

Nozomi Networks Leads OT and IoT Security

The **best solution** to manage cyber risk and improve resilience for industrial operations

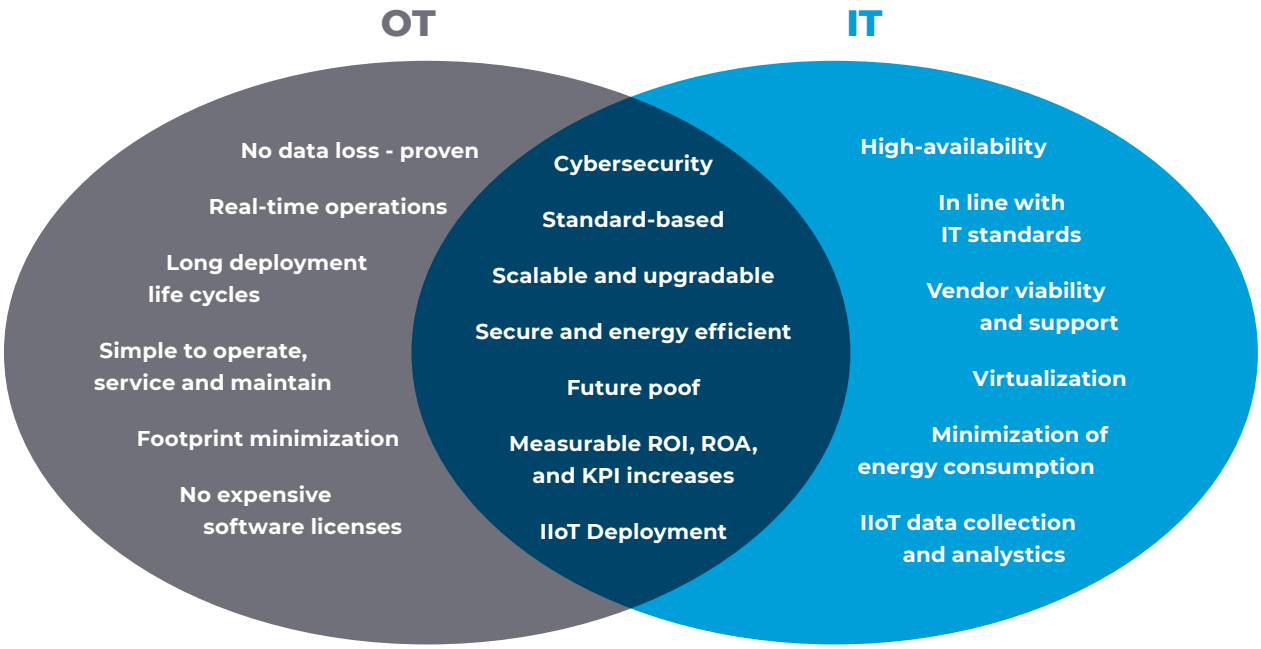
3,700+ installations worldwide in sectors such as critical infrastructure, energy, manufacturing, mining, transportation and utilities

47.7M+ OT, IoT and IT devices monitored

Gartner Peer Insights

Nozomi Networks has earned a 4.9 out of 5 star overall ranking in OT security from Gartner's real-world user peer review program

Align OT/IT Priorities to Improve Cybersecurity



Source: Craig Resnick, ARC Advisory Group – reprinted with permission.

What Drives IT/OT Convergence?

The Industrial Internet of Things

The computing landscape of today is characterized by increasing connectivity and data sharing between disparate systems. It also involves data flows between local applications and cloud-based applications, where sophisticated analytics may be done.

Similarly, the Industrial Internet of Things (IIoT) and Industry 4.0 are both trends that involve connecting smart devices and sharing the data they produce to improve existing business models and enable new ones. Benefits include reduced costs, improved productivity, energy savings and faster response to customer demand.

While bringing many benefits, the IIoT also increases cyber risks. Traditionally insecure industrial systems, which include many legacy assets, are now exposed to the type of threats that IT has been dealing with for years. Complicating the picture is the dramatic rise in cyberattacks specifically targeting critical infrastructure and manufacturing systems.

Executive Concerns about Cyber Risks Are Increasing

A 2018 Marsh report[2] found three-quarters of energy executives worry about cyberattacks interrupting their business operations. Physical damage is the cyber loss scenario of greatest concern. As a consequence, most of the executives surveyed are preparing to increase their investments in cyber risk management.

And, both the U.S. and U.K. governments have issued warnings around state-sponsored attacks targeting critical network infrastructure.

Other examples of the business costs related to cyberattacks on industrial networks include:

- Merck: $780M losses from production shutdown, lost sales and remediation costs[3]
- Maersk: $300M losses from business interruption, lost revenues and remediation costs[4]
- FedEx: $300M in lost earning for one quarter, with additional losses to follow[5]

With the IIoT trend increasing cyber exposure for industrial networks, and cyberattacks increasingly becoming the tool of choice for nation states and cyber criminals, losses continue to increase.

Countering Cyber Risk with IT/OT Convergence

To reduce cyber risks related to industrial systems, it is 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. Collaboration between the groups reduces cybersecurity blind spots and costs.

However, as any initiative that involves people and process, making it happen takes strong direction and ongoing leadership commitment.

Depending upon an organization's convergence maturity level, executives should set appropriate goals. This can include things like having one executive responsible for both IT and OT, facilitating cross-training, and insisting on as much common technology between the groups as possible.

80% of the industrial facilities we visit do not have up-to-date lists of assets or network diagrams. The first step to better cybersecurity is better visibility of OT infrastructure. Our solution is easy to deploy and combines superior operational visibility and best-in-class threat detection. The ROI is very fast, delivered through increased productivity, enhanced cybersecurity and the use of a common tool for both IT and OT.

EDGARD CAPDEVIELLE — CEO, Nozomi Networks

Why Invest in the Nozomi Networks Solution?

Solution Designed for OT, Benefits OT, IoT and IT
As the cybersecurity risk to critical infrastructure and manufacturing organizations increases, it is important for enterprises to actively monitor and secure OT networks.

An important aspect of this is having complete visibility to OT networks and assets and their cybersecurity and process risks.

IT solutions do not apply as they do not meet the unique challenges of managing 24/7/365 operational systems where availability is often a bigger concern than confidentiality or integrity.

Nozomi Networks is the OT and IoT security and visibility vendor of choice because we thoroughly understand industrial networks and processes. Our technology is completely safe for industrial control systems (ICS) and delivers superior visibility, real-time network monitoring and threat detection in a passive, non-intrusive manner. It also integrates seamlessly with IT infrastructure, easily sharing data with existing applications and assets.

Our company has innovated the use of artificial intelligence to automate inventorying, visualizing, monitoring and identifying threats to OT networks. The result is improved cyber resiliency and reliability.

Immediate Value Delivered to Multinational Organizations
Unlike some enterprise-class applications, deployment of the Nozomi Networks solution is straightforward and starts providing ROI quickly. Here is why:

- It is a passive solution that is completely safe for industrial networks and processes.
- It is a mature, 4th generation solution that is ISO9001:2105 certified and quick to deploy.
- It immediately brings benefits by identifying existing threats in the industrial network and improving the productivity of operations and IT staff.

Example Time Savings of One Employee

- It readily scales to monitor hundreds of facilities and thousands of devices from a central location.
- It integrates easily with IT/OT infrastructure, supporting existing investments in technology and skills.

> I slashed ICS administration and cybersecurity labor hours by 10 to 12 hours a week using the Nozomi Networks solution.
>
> **Kris Smith, Vermont Electric Cooperative**

Nozomi Networks Benefits for OT and IT: A Safe Solution for OT Visibility and Detection for IT

OT

- A "no process risk" solution that provides comprehensive visibility to all ICS assets
- Rapid identification of threats, policy violations and risks to reliability
- Unique process views monitor variables such as pump speed or temperature
- Faster troubleshooting, as network information is easy to see and drill into
- Single application that monitors devices from all vendors
- A common platform to drive IT/OT convergence

IT

- Complete visibility to OT networks and their risk exposure
- Consolidated information from multiple industrial facilities via one monitoring tool, when using the CMC
- Shows IT-allowed protocols and alerts when disallowed protocols are in use
- Faster troubleshooting of OT incidents with ICS-specific dashboards and forensic tools
- Seamless integration with SIEMs and other IT applications
- A common platform to drive IT/OT convergence

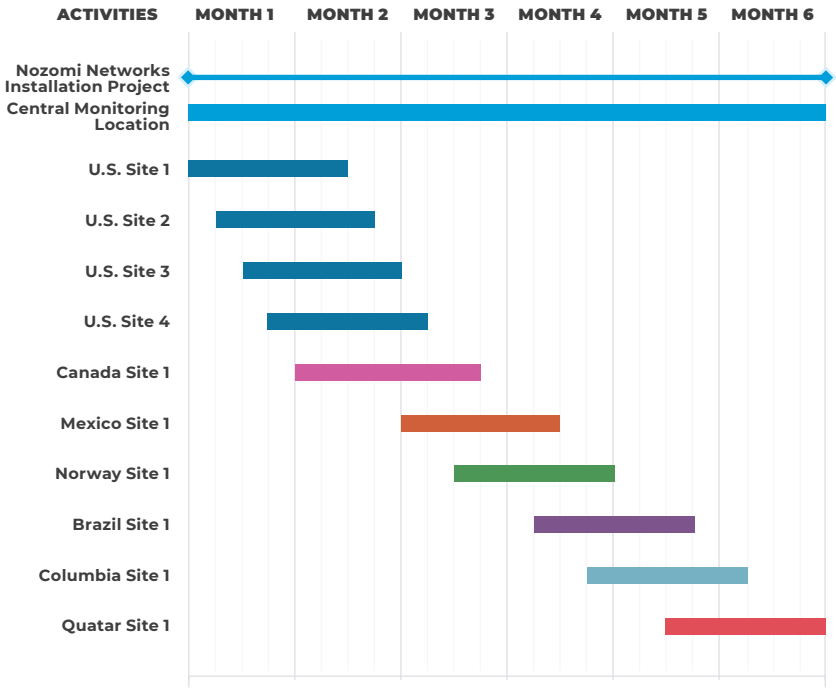
Fast Deployment and ROI for the Nozomi Networks Solution

Sample Deployment

Central Monitoring Location	1
Industrial Facilities	10
Countries	7
Project Duration (months)	6

Implementing the Nozomi Networks solution is time and cost effective, improving:

- OT visibility and cybersecurity
- Reliability
- Productivity
- IT/OT collaboration



Securing the World's Largest Organizations

9 of Top 20 Oil & Gas

7 of Top 10 Pharma

5 of Top 10 Mining

5 of Top 10 Utilities

- Chemicals
- Manufacturing
- Automotive
- Airports
- Water
- Building Automation
- Food & Retail
- Logistics
- Smart Cities
- Transportation

Why Choose Nozomi Networks?

“Nozomi Provides The Right Level Of Cybersecurity Insights For My OT Domain.

The Nozomi Team has been very hands on with our large-scale deployment. They have shown their commitment by providing the right level of expertise and localization. Their extensive networks have allowed us to continue our deployments despite the global pandemic.

Principal Engineer, Energy & Utilities Industry ›

“The Guardian Appliance Is Powerful. Their Team Is Skilled, They Solved Our Problem.

Nozomi has provided a high level of customer service and expertise throughout our procurement and implementation process. Their sales, engineering, and support teams are excellent and their product is best in class.

Sr. Program Manager, Manufacturing Industry ›

References

1. **“The Global Risks Report 2020,”** World Economic Forum, 2020.
2. **“Could Energy Industry Dynamics Be Creating and Impending Cyber Storm?,”** Marsh, 2018.
3. **“NotPetya Ransomware Outbreak Cost Merck More Than $300M per Quarter,”** TechRepublic, 2018.
4. **“Petya Ransomware: Cyberattack Costs Could Hit $300M for Shipping Giant Maersk,”** ZDNet, 2017.
5. **“FedEx Lost $300 Million During Petya Attack on TNT Express,”** CIO Bulletin, 2017.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

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.

EB-BUS-LEADERS-8.5x11-004

nozominetworks.com