NOZOMI NETWORKS

CASE STUDY

Global Medical Technology Company Gains Deep Visibility into its Manufacturing Processes

The Nozomi Networks platform supports the company's advanced security program across manufacturing plants and engineering lab environments worldwide.

Customer Profile

- Global medical technology and digital solutions
- Operating in over 150 countries
- 50K+ employees

Goals & Challenges

- Expand visibility into global manufacturing and engineering processes
- Prevent and minimize downtime due to operational disruptions or security incidents
- Accelerate enterprise-wide security maturity

Results

- Consolidated visibility across global manufacturing facilities
- Real-time insights into OT/IoT vulnerabilities and risks
- Accelerated response to potential operational disruption

"The solution began delivering value in the first hour it was deployed. Its detailed OT network topology, advanced monitoring capabilities, extensive integrations and outstanding scalability give our Security Operations Center enterprise-level visibility with no disruption to ongoing operations.

Director of Cybersecurity, Medical Technology Company

Guardian

Unlocks Visibility Across OT and IoT for Accelerated Digital Transformation

The Challenge: Gaining Visibility Across Globally Distributed Manufacturing Processes

This healthcare company's intelligent medical technologies are redefining patient care. Its expertise in diagnostics, research and biopharmaceutical solutions are helping physicians detect disease earlier and create personalized treatment plans for patients.

The organization's manufacturing facilities, spread around the world, had varying levels of security maturity. Some had visibility into the mixed environment of OT and IoT devices being used in plant operations, while others didn't. Inconsistent situational awareness and insight made it difficult to monitor and manage manufacturing processes efficiently. It also made it challenging to identify production line availability risks, and quickly troubleshoot problems.

The Solution: An Automated Asset Inventory and Real-time OT/IoT Network Visualization

The first step towards building a stronger OT and IoT security posture involves tracking the devices operating on the network, and how they're interacting.

Upon deployment, Nozomi Networks Guardian immediately generated an interactive network visualization map displaying all assets and lines of communications. It also created a comprehensive inventory, complete with name, type, serial number, firmware version, components and more.

The solution then analyzed network traffic and established a baseline for legitimate activity and behavior. The breadth and depth of information gave plant managers and the cybersecurity team extensive visibility into the operational environment, including:

- A macro view of its entire OT and IoT network
- The protocols used to communicate between nodes and zones
- Network traffic information such as throughput, protocols and open TCP connections
- Detailed attributes of endpoints and connections
- A solid foundation for identifying system vulnerabilities and anomalies

> "We invited each of our business units to do their own review of the Nozomi Networks solution and team. The level of engagement during pre-sale discussions, solution training, and post-sale deployment has been exemplary. When combined with the system's maturity and scalability, it was easy to get to a unanimous decision that this was the right solution for us worldwide."
>
> **Director of Cybersecurity, Medical Technology Company**

Anomaly & Threat Detection

Quickly Identify Process Reliability and Cybersecurity Threats

The Challenge: Preventing Production Line Disruption

When COVID-19 hit and global demand for ventilators skyrocketed, this medical technology provider quickly scaled up its manufacturing lines to produce triple its usual output.

One critical step involved engaging the network team responsible for new product line and manufacturing systems infrastructure. The team needed to ensure that ramp up could be done securely, without introducing any risk to plant floors.

Fortunately, when the company first started looking for an ICS vulnerability and incident response platform, its selection criteria included the ability to monitor production processes and identify vulnerabilities and behavioral anomalies. Other priorities included the ability to automatically alert operators to reliability issues, filter out noise and provide context that would allow them to proactively address the issues before downtime occurred.

The Solution: Ongoing Vulnerability Assessment + Advanced Threat Detection

The Nozomi Networks solution was in place when the pandemic began to wreak havoc around the world. This meant that the company was already monitoring its network for operational anomalies that could bring critical production lines down. The solution's precise alerts, which exclude benign anomalies, helped focus the company's attention on high-priority risks and improved its mean-time-to-response (MTTR).

The cybersecurity team was well armed with the tools it needed to detect threats, thanks to the large number of ICS and IT protocols monitored by the Nozomi Networks solution. The products also integrate with a roster of third-party security tools such as SIEMs and asset and log management systems. Integrations with firewalls allowed the team to automatically block attacks.

The medical technology company also leveraged the Nozomi Networks Threat Intelligence service. It continually updates Guardian sensors with rich data and analytics, and correlates threat intelligence information with broader environmental behavior. This provided an added layer of security and operational insight to its risk management program. It also helped the company confidently scale up production to address changing market demand.

Guardian

Unified Visibility, Monitoring and Security Across Distributed Operations

The Challenge: Accelerating Security Maturity Across the Manufacturing Supply Chain

Given the critical nature of its business, the company had invested significant resources in establishing a solid framework for its security program, complete with best practices, employee training, ongoing audits, and much more. With the infrastructure in place, the cybersecurity team felt it was time to ramp up security maturity across its entire manufacturing supply chain. To achieve this, it needed a proven ICS visibility and security solution that could easily scale to support globally-distributed manufacturing processes that were interconnected, automated and IoT-enabled.

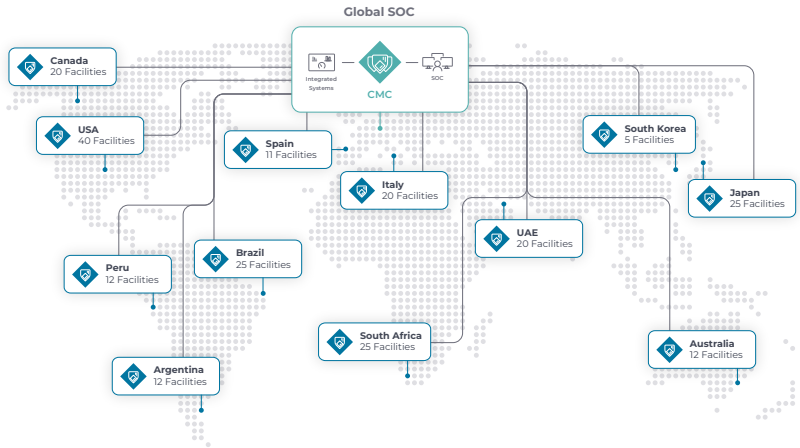
The Solution: A Highly Scalable Solution Built to Deliver Outstanding Regional and Global Insight

The Nozomi Networks solution was built for scalability. Guardian sensors come in physical, virtual, ruggedized, portable and container versions to fit all deployment scenarios, and a single Guardian sensor can monitor up to 500,000 assets in real-time. In addition, Guardian's large enterprise series, including the powerful 750 and 1,000 models deployed by the medical technology company, can be easily customized to meet the network needs of specific sites, including 1G and 10G deployments.

The company deployed virtual Central Management Consoles (CMCs) in North America, EMEA and APAC to aggregate data from in-region manufacturing and engineering operations. It now feeds this information to a global OT Security Operations Center (SOC) located in North America.

Built-in integrations with asset, identity management and other systems made it easy to streamline security processes across IT and OT, and around the world.

As a result, the medical technology manufacturer now has consolidated OT/ IoT visibility and security risk management within a single pane of glass.



Sample deployment map showing the global Security Operations Center (SOC) receiving feeds from Nozomi Networks Central Management Consoles (CMCs) and in-region Guardian sensors.

The Result:
Fast, Easy Deployment Delivers Immediate Value to Cybersecurity Team

This multi-national medical technology company was able to quickly roll out a mature OT and IoT security solution across operations in multiple countries. It can now continuously monitor its manufacturing and engineering processes for vulnerabilities and risks. The company can also quickly spot and respond to anomalies that could disrupt availability. Even better, it can do all this and more from a central location managed by a small team of security experts.

As of October 2020, Nozomi Networks' industry leading solution for network visibility and threat detection was monitoring over 17,000 devices and network connections for the company's facilities in North America, Europe and Asia. To further strengthen its cyber resilience, this innovative medical technology company plans to more than double its deployment of Guardian sensors within its manufacturing and engineering operations in 2021.

The Nozomi Networks Advantage

Securing the World's Largest Organizations

Accelerating your digital transformation by reducing cyber risk.

Unifying Cybersecurity Visibility

Innovating visibility and threat detection across your OT, IoT, IT and cyber-physical systems.

Partnering to Accelerate IT/OT Convergence

Deeply aligned with the OT, IoT and IT partners you trust.

Take the next step.

Discover how easy it is to identify and respond to cyber threats by automating your IoT and OT asset discovery, inventory, and management.

Learn More

nozominetworks.com

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.

NOZOMI NETWORKS

nozominetworks.com