NOZOMI NETWORKS | SecuriOT

CASE STUDY

European Heating Supply Company Monitors Over 200 Sites With a Single Device

A single Guardian sensor monitors the OT network supplying heat to over 300,000 customers, identifying device vulnerabilities and other operational reliability risks.

Customer Profile

- District heating supply, waste and recycling
- Centralized heating for 300K+ customers
- 400+ employees

Goals & Challenges

- Actionable insight into OT device vulnerabilities
- Increased cybersecurity resilience and maturity
- Compliance with anticipated NIS regulations/IEC standards

Results

- Real-time visibility into activity across the entire heating system infrastructure
- Detailed insight into PLC vulnerabilities and inbound/outbound network connections
- Ability to demonstrate good cybersecurity practice and fulfil objectives of the NIS Directive

> This heating provider is able to create a detailed overview of the OT infrastructure with only one Guardian sensor – including asset inventorying, network monitoring, vulnerability assessment, and anomaly and threat detection. It's an incredibly powerful and cost effective security solution for them.

Jørgen Hartig
CEO & Partner, SecuriOT

Guardian

Unlock Visibility Across OT/IoT Networks for Continuous Cybersecurity and Reliability Monitoring

The Challenge: Identifying OTIoT Device Vulnerabilities

The heating supply company's OT Network Administrator is responsible for ensuring that heat continues to flow to the company's 300,000+ customers in this Nordic country.

While the Administrator had a good understanding of the quantity and types of devices on the infrastructure, he was concerned about potential cyber threats. He knew that the network contained a large number of programmable logic controllers (PLCs) known to be vulnerable to the Stuxnet virus. While Stuxnet enters via an IT network, it ultimately targets the supervisory control and data acquisition (SCADA) systems on the OT side.

To prevent cross-infection, the Administrator maintained a gap between the organizations's OT and IT systems. However, because heating substation data flowed through a centralized SCADA service, every time a computer inside the network made a connection to the outside, it increased the organization's vulnerability to malicious malware.

To reduce the level of risk, the Administrator wanted to continually monitor his OT network for vulnerabilities that could disrupt heating operations in any way, and quickly remediate any issues found.

Guardian

Unlock Visibility Across OT/IoT Networks for Continuous Cybersecurity and Reliability Monitoring

The Solution: Automated Network Monitoring and Rapid Identification of Vulnerabilities

The OT Network Administrator was intrigued when he learned about the comprehensive capabilities of the Nozomi Networks OT and IoT visibility and security solution from a former colleague.

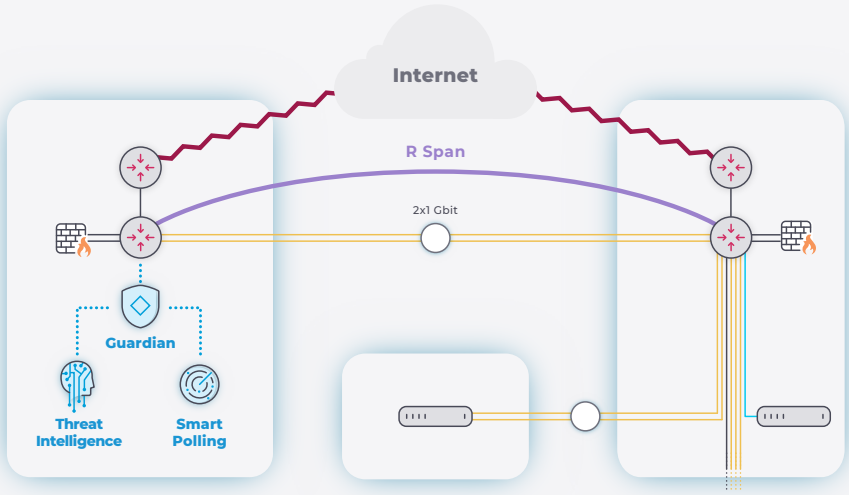
It seemed to offer much of what he needed, starting with the ability to identify OT and IoT assets on his network. This would help him maintain the vital gap between OT and IT systems. The solution also provided much-needed insight into which PLCs and other assets were vulnerable to exploitation by cyber attackers.

The OT Network Administrator worked with Nozomi Networks local system integration partner SecuriOT to spin up a security assessment Proof of Concept (PoC) at the core site of the organization. The OT cyber experts from SecuriOT were able to demonstrate the value of the solution almost immediately.

Upon deployment, the Guardian appliance inventoried the OT and IoT assets on the site's local network and identified all communicating devices. This included those used by third party suppliers connecting and interacting with the heating infrastructure. Guardian then conducted a vulnerability assessment and provided detailed information on PLCs that were open to cyber threats.

The heating supplier's executive team was excited by what they saw, and quickly gave the Network Administrator approval to deploy the Nozomi Networks solution, including Smart Polling and Threat Intelligence services, across the organization's entire 200-site infrastructure.

While each of the 200+ heating system sites has its own local network, the heating supplier's centralized SCADA infrastructure consolidates all PLC communications, and routes the data to a single Guardian sensor for monitoring.



Nozomi Networks

Helping Critical Infrastructure Address IEC 62443 Standards and NIS Regulations

The Challenge: Getting a Head Start on Compliance Before Regulations and Standards Become Mandatory

The heating company's Network Administrator was also looking for an efficient way to prepare for the security regulations he believed were coming to suppliers in the region.

The Directive on Network and Information Systems (NIS Directive - EU) went into effect in 2018, and a new version, the NIS2 Directive, is on its way. The initiative is designed to ensure that operators of essential services (OES) are equipped to deal with increasing cyber threats. When applied consistenty, NIS principles can help critical infrastructure providers achieve and maintain a high level of network and information system security.

A second set of industry guidelines and standards, IEC 62443, provides a framework for addressing and mitigating security vulnerabilities in industrial automation and control systems. It outlines technical standards for the life cycle of cybersecurity in OT environments, including technical requirements, and requirements for policies, procedures and components used in industrial control systems, including embedded devices like PLCs, as well as network assets and software.

While this Nordic country has yet to mandate that heating companies comply with NIS Regulations or IEC 62443 Standards, the heating supplier wanted to understand what they entailed, and get in front of the compliance curve.

"The centralized design and network architecture of this organization's heating system infrastructure is quite common for this type of utility service. Therefore it was possible to use just one Guardian sensor to monitor all 200 sites. Adding the Nozomi Networks Threat Intelliegence Service, which continually updates Guardian with ongoing threat and vulnerability intelligence, completes the picture with visibility, security and peace of mind."

Jørgen Hartig
CEO and Partner, SecuriOT

Nozomi Networks and SecuriOT

Delivering Real-time Visibility Across the Entire Infrastructure

The Solution:
Taking a Proactive, Risk-based Approach to Cybersecurity

The comprehensive visibility, monitoring and risk identification capabilities of the Nozomi Networks solution support a structured approach to compliance with cybersecurity regulations and standards.

For example, Guardian's OT/IoT security and visibility functionality provides real-time network intelligence, monitoring and AI-powered threat detection. This allows the heating supplier to proactively manage security risk and protect itself against cyberattacks, as outlined in NIS objectives. The Nozomi Networks solution also provides real-time alerts for behavioural anomalies and threats it identifies within industrial control networks. All monitoring and assessment information is displayed in an intuitive interface that streamlines reporting and operational oversight.

Thanks to the Nozomi Networks solution, this European heating provider is proactively embedding cybersecurity into its operational processes and improving its cyber resiliency. The company is well on its way to developing a level of security maturity that demonstrates compliance with the NIS Directive.

The Results:
Addressing Multiple OT Security Needs With a Single, Comprehensive Solution

The heating supply company was able to cost-effectively deploy a mature OT visibility solution across its 200-site heating system infrastructure.

Thanks to a single Guardian sensor and the extensive cybersecurity knowledge of the SecuriOT team, the organization can now automatically monitor its operational processes and identify vulnerabilities, all with an OT team of one.

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

SecuriOT

About SecuriOT

SecuriOT has deep expertise in cybersecurity for industrial control networks. We help our customers on the journey in OT Security (Operational Technology Security). An important foundation for SecuriOT's business approach is that OT-security is not just fixed with a quick analysis or a new network component. It is a continuous process to keep security at the right level. It requires a new mindset in the organisation, greater visibility and an better understanding of the cyber threats against your production floor. Often the security in automation systems is set aside with old unpatched computers, wrongly connected networks, unsecure remote access, nonexistent OT policies and procedures etc. We have knowledge in all these areas and will be the natural partner in OT security.

SecuriOT is part of the Novotek Group. Novotek is the leading creator of innovative solutions for Automation and Industrial IT in the Nordic countries, Benelux, Switzerland, United Kingdom, Austria, Germany and Ireland. Learn more about SecuriOT at **securiot.dk**

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