Building a Cyber Fortress: Preparedness and Resilience in Critical Infrastructure

Foteini Papagiannaki
Cyber Security Division Manager, ADAPTIT SA

Agenda

01   **Market Challenges**

02   **Introduction** to Nozomi Networks

03   **Nozomi Networks Solution**

04   **Nozomi Networks+ADAPTIT Offerings**

05   **Market Momentum / Partner Ecosystem**

Market
Challenges

Market Forces Driving Change

Digital Transformation

- New technologies, new use cases in every industry

IT/OT Convergence

- Integrated teams and workflows need a single view

Internet of Everything

- Juniper Research: 83 billion IoT connections by 2024; 70% in Industrial sector

Threat & Risk Management

- Frequency and cost of targeted attacks continue to increase

> **5G is accelerating digital transformation across all sectors — everyone is connected to everything, and new use cases are speeding OT, IoT and IT convergence.**
>
> Andrea Carcano, Co-founder and CPO, Nozomi Networks

How OT Security Differs from IT Security

Safety and Reliability of critical systems that operate 24/7/365 and involve processes with significant safety risks.
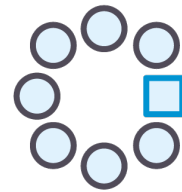
Heterogeneous/Legacy Systems Industrial networks include diverse assets, and often consist of multiple connected architectures.
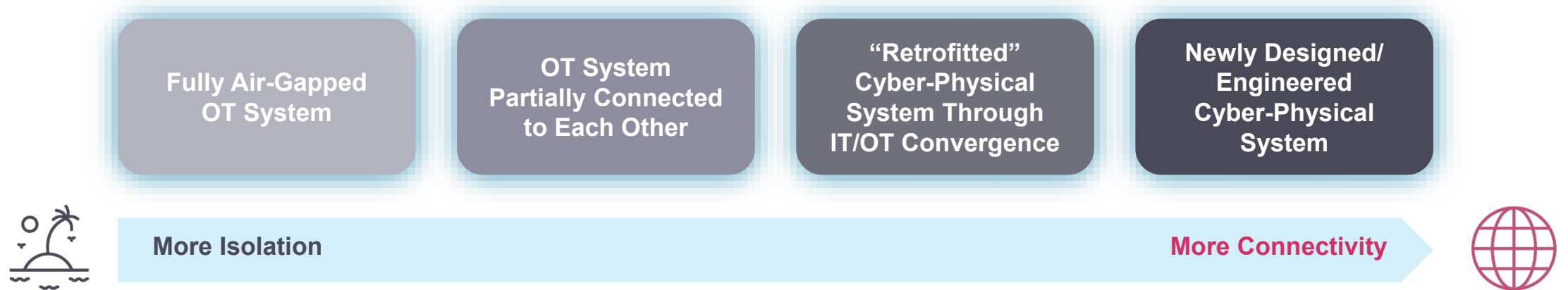
Industrial Protocols are often unknown in the IT world, and that are inherently insecure.

Volume of IoT/OT Devices will grow to billions worldwide vs millions in IT.

OT Systems Evolution

| Fully Air-Gapped OT System | OT System Partially Connected to Each Other | "Retrofitted" Cyber-Physical System Through IT/OT Convergence | Newly Designed/ Engineered Cyber-Physical System |

More Isolation ———————————————————————→ **More Connectivity**

Examples of Traditional OT Systems

- Supervisory Control and Data Acquisition (SCADA)
- Industrial Control Systems (ICS)
- Programmable Logic Control (PLC)
- Process Control Networks (PCN) – Including Safety Instrumented Systems (SIS), Engineer Workstation and Human Machine Interface (HMI)
- Distributed Control Systems (DCS)
- Computer Numerical Control (CNC)

Examples of OT-Related Cyber-Physical Systems

- Industrial Robots
- Virtual Reality Manufacturing Simulation Systems
- Self-Optimizing Press-Bending and Roll-Forming Machine
- Adaptable Production Systems
- Energy-Efficient Intralogistics Systems
- Connected 3D Printers
- Smart Grids

The High Cost of a Cybersecurity Incident

1.7M USD
Average estimated cost of cyberattack

"Cyberattacks on critical infrastructure have become the new normal and are one of the top five global risks."

World Economic Forum
Global Risk Report, 2020

	Organization	Issue/Attack	Cost (USD)
2020	Cognizant	Maze Ransomware	70m
	Honda	COVID-related Ransomware	Unknown
2019	Norsk Hydro	LockerGoga Ransomware	70m
	Duke Energy	Compliance Violation	10m
2018	Saudi Petrochem	Triton	Unknown
	UK NHS	WannaCry	100m
2017	Merck	NotPetya	870m
	FedEx (TNT Express)	NotPetya	400m
	Maersk	NotPetya	300m
	Mondelēz	NotPetya	188m
2016	Ukrenergo	Industroyer/Crashoverride	Outage
2012	Saudi Aramco	Shamoon	1 Billion

Sources: Wired, Wall Street Journal, UK Telegraph, Threatpost, Forbes

Introduction to
Nozomi Networks

Global Leadership Footprint
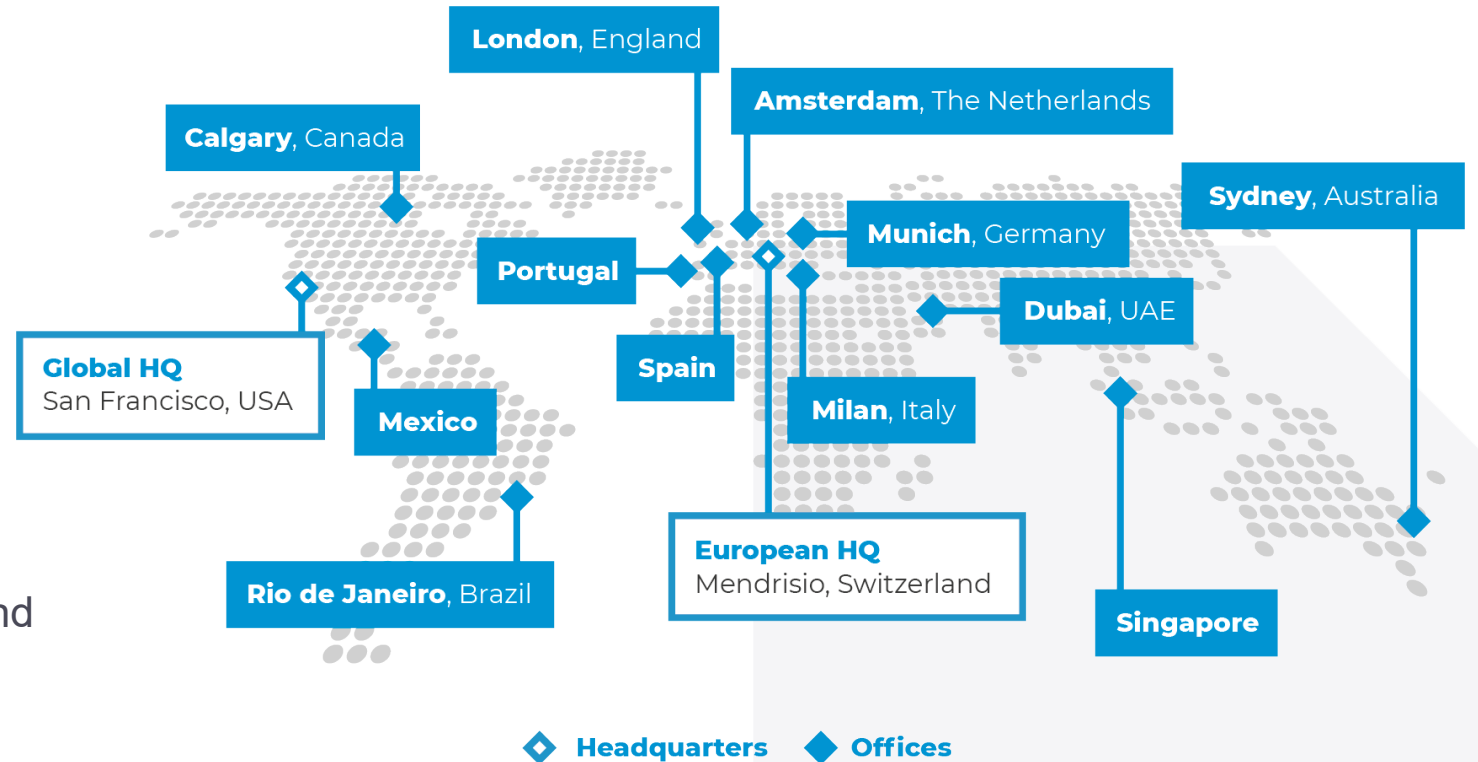
Global Customer Base
5.0K Installations

57.2M Devices Monitored
Across Converged OT/IoT

Scalable Deployments
Across **6 Continents**

Global Expertise
Worldwide Network of Partners and
1,000+ Certified Professionals

London, England

Amsterdam, The Netherlands

Calgary, Canada

Sydney, Australia

Munich, Germany

Portugal

Dubai, UAE

Global HQ
San Francisco, USA

Spain

Mexico

Milan, Italy

European HQ
Mendrisio, Switzerland

Rio de Janeiro, Brazil

Singapore

◇ **Headquarters** ◆ **Offices**

NOZOMI NETWORKS | ADAPTIT GROUP OF COMPANIES

NOZOMI NETWORKS

100% Customer **retention**

100% Customer **growth**

83% **win rate** for PoCs*

90% of the time, **vulnerabilities/ threats** found within 24 hours of installation

Industry-1st SaaS solution for OT/IoT cybersecurity: **Vantage**™

Industry Leader for 3rd consecutive year in **Gartner Peer Insights Reviews**

Unrivaled Partner Ecosystem adding Honeywell, Telefónica, ABB, AWS, Honeywell, Siemens, Google, Service Now, Yokogawa, and other

Strategic Investments from In-Q-Tel, Telefónica and Forward Investments

2020
Growth

Securing the World's Largest Organizations
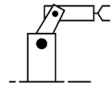
9 of Top 20 **Oil & Gas**

7 of Top 10 **Pharma**

5 of Top 10 **Mining**
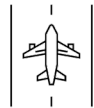
5 of Top 10 **Utilities**

Chemicals
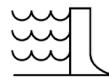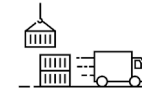
Manufacturing

Automotive

Airports

Water

Building Automation
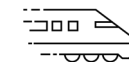
Food & Retail

Logistics

Smart Cities

Transportation

This seems to be a joke but this is reality !!!

Nozomi Networks Strengths

Proven Scalability

Central Management & Analysis
Manage any number of sites & assets

Cloud Multi-tier Architecture
SaaS platform monitors any number of assets and locations from anywhere

Agentless Protection
Single Guardian sensor can monitor over 500K assets

Faster Deployment

Sensor Options to Fit Your Environment
Physical, virtual, cloud, edge, container sensors

Cloud Architecture
SaaS platform speeds onboarding, eliminates sizing issues

Industry's Largest Partner Ecosystem and Open API
Minimizes integration complexity

Always-On Monitoring

Continuous Monitoring of All Supported Protocols: OT, IoT and IT
No critical blind spots

Unmatched Detection & Visibility
Prevents operational disruptions

Audit-ready Default Configuration
Avoids findings due to misconfiguration

Full Stack Solution

No Reliance on Other Vendors
Avoids EOL impacts or waiting for patches

Rigorous QA Ensures Interoperability and Stability
Improves hardening, scalability, rollback, data analysis

Integrated Development
Extracts the best performance from hardware and software

Nozomi Networks+ADAPTIT
Offerings

Nozomi Networks Key Differentiators

See
All assets and behaviors on your OT/IoT networks for comprehensive awareness
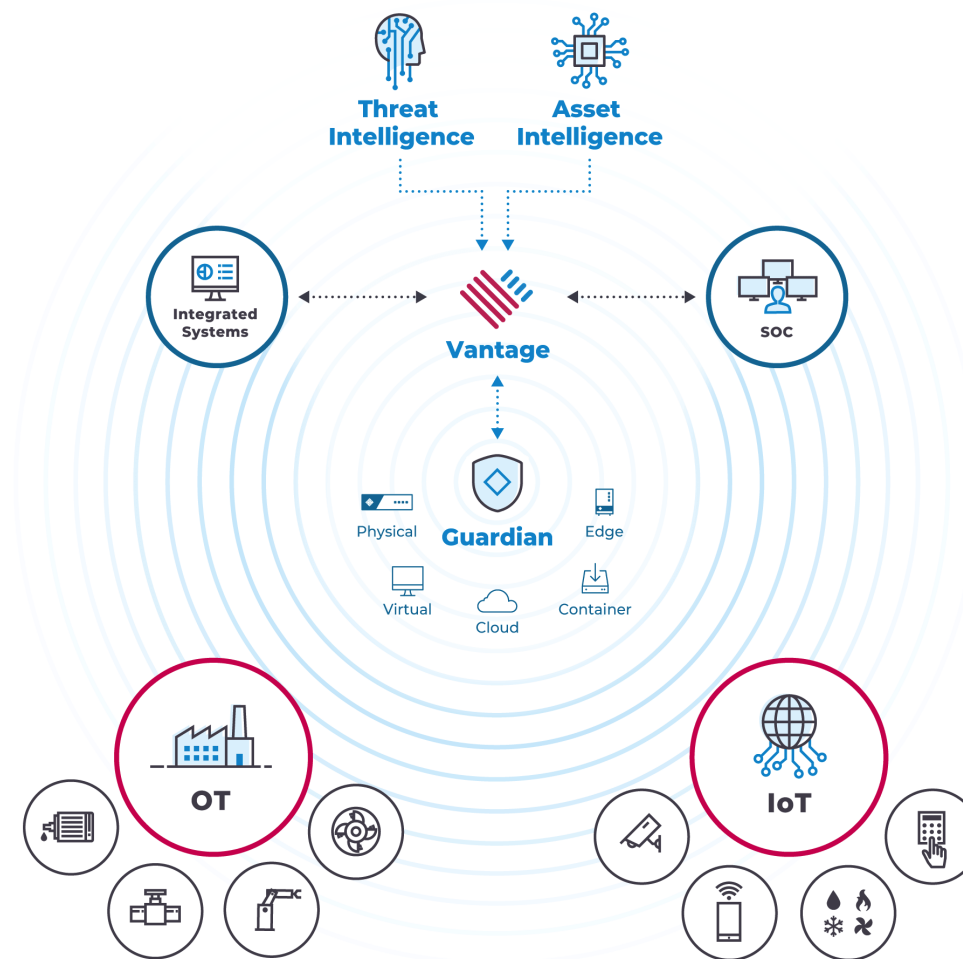
Detect
Cyber threats, vulnerabilities, risks and anomalies for faster response

Unify
Security, visibility and monitoring across all your assets for improved operational resilience

Nozomi Networks + ADAPTIT Offerings

ADAPTIT uses Nozomi Network products for asset inventory and ICS assessments to passively identify and map networked assets in customers' ICS and surrounding networks.

ADAPTIT assists with deploying the Nozomi Networks solution, gaining immediate network visibility, and building an interactive visualization of every device on the network.

ADAPTIT uses Nozomi products to accelerate Detection and Response, thus improving Operations and Security Teams' Efficiency.
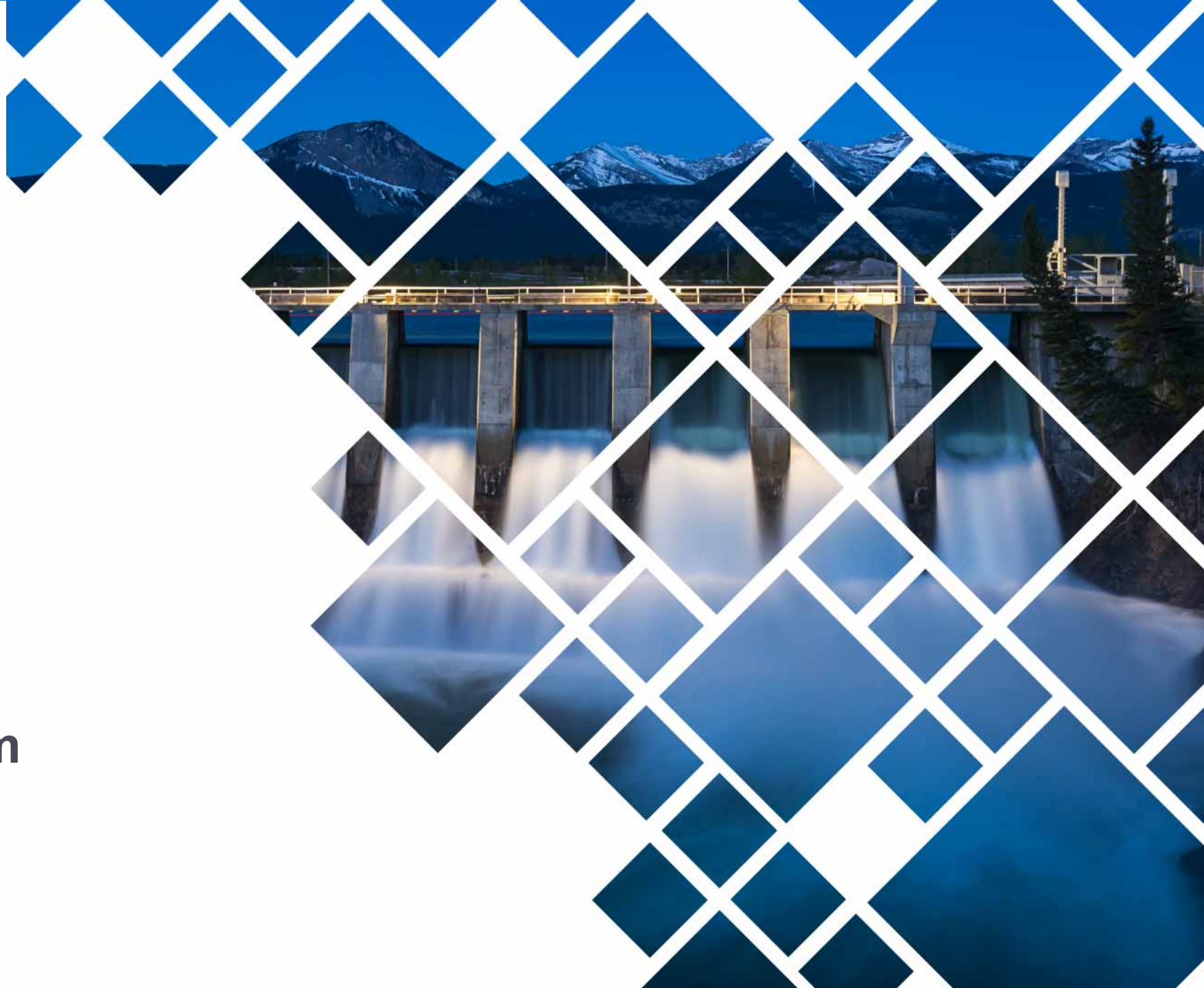
Adaptit leverages the experience of the Nozomi Networks Threat Operations Center (TOC) for extended ICS knowledge, training, and intelligence to better support customers' risk evaluations and managed service needs.

Nozomi Networks
Market Momentum

Technology Alliance Ecosystem

Integrations and Interoperability with Controls, Security, Network & Cloud Architectures

SIEM, SOAR and Data Integrations
- ArcSight
- Atos Codex
- exabeam
- FORTINET
- IBM Security
- LogRhythm — The Security Intelligence Company
- splunk>
- SWIMLANE

OT / ICS Interoperability
- ABB
- GE Power
- Honeywell
- MITSUBISHI
- OMRON
- Rockwell Automation
- Schneider Electric
- SEL — SCHWEITZER ENGINEERING LABORATORIES
- SIEMENS
- YOKOGAWA

Other Network / IT and Security Technologies
- Allied Telesis
- CISCO
- FORTINET
- GARLAND TECHNOLOGY — See every bit, byte, and packet
- GATEWATCHER
- Gigamon
- KEYSIGHT TECHNOLOGIES
- paloalto NETWORKS
- tdi
- Tempered
- WATERFALL — Stronger Than Firewalls
- ZEDEDA

Cloud Services Platforms
- aws
- Google Cloud
- Microsoft Azure
- servicenow

Our solution provides extensive support for OT/IoT and IT protocols and is frequently updated. See the latest **Protocol List**.

Five Star Customer Reviews

100% Customer Retention

★★★★★

"The Guardian appliance Is powerful, their team is skilled, they solved our problem."

Senior Program Manager
Manufacturing Industry

★★★★★

"Innovative, easy to implement and even easier to maintain."

Systems Specialist
Services Industry

★★★★★

"Once you try Nozomi and its rich feature set you cannot imagine operating without it!"

Security Analyst
Manufacturing Industry

★★★★★

"We wanted the most advanced technology available."

Manager, Cyber Security
Oil & Gas Industry

★★★★★

"This product keeps its promises."

System Administrator
Energy and Utilities Industry

★★★★★

"Exceeded expectations. Deeper visibility than expected."

Senior Industrial Security Manager
Manufacturing Industry

What Partners Say

Atos

Working with Nozomi Networks allows us to take advantage of their artificial intelligence-powered software to map, monitor and identify threats in some of the largest industrial installations around the world.

JEROME SANDRINI
Head of Big Data and Security Atos North America

Honeywell

Our partnership delivers the industry's most complete, vendor-neutral OT cybersecurity portfolio, strengthened by Honeywell global professional and managed security services.

JEFF ZINDEL
Vice President and General Manager, Honeywell Connected Enterprise Cybersecurity

---

IBM Security

Teaming with Nozomi Networks, our customers immediately gain market-leading OT network monitoring and threat detection technology that is fully integrated with key IBM Security services and platforms such as QRadar.

CHRIS MCCURDY
Vice President Worldwide, IBM Security

Schneider Electric

We tested a number of different vendors, and Nozomi came out on top … Guardian also learns the system, tells you all the assets, and will tell you about unusual activity … They will help us address threats we can't even quantify.

GARY WILLIAMS
Senior Director, Schneider Electric

What Partners Say

Gartner

Gartner's recognizes Nozomi Networks Vantage as a SaaS-based Multiplatform OT Security Platform — urges security and risk management leaders to "seize the opportunity to support their organizations' efforts to improve operational resilience.

GARTNER MARKET GUIDE
For Operational Technology Security, January 2021

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 ...

SANKARA NARAYANAN
Senior Industry Analyst Frost & Sullivan

IDC ANALYZE THE FUTURE

Nozomi Networks has grown to become a leader in industrial cybersecurity ... with deployments worldwide at many of the biggest players in industries such as oil and gas, pharmaceuticals, utilities, and mining.

MARK CHILD
Research Manager, European Security, IDC

ROMAIN FOUCHEREAU
Manager, Security Appliance Program, IDC

---

451 Research

Nozomi's flagship Guardian product comes at a pivotal time in the development of the ICS security market and reflects several of the trends we are seeing across ICS security …

PATRICK DALY
Associate Analyst 451 Research

Industry Awards

...and more!

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