The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks accelerates digital transformation by providing exceptional network visibility, threat detection and operational insight for OT and IoT environments.

We make it possible to tackle escalating cyber risks to operational networks while modernizing your business to succeed in the future.

Let us put our passion for innovation and customer success to work for you, helping you ensure high cyber resiliency and reliability.

See
What’s on your network and how it’s behaving

Detect
Cyber threats, risks and anomalies for faster response

Unify
Security, visibility and monitoring across all your assets

Securing the World’s Largest Organizations

6 of Top 20 Oil & Gas

5 of Top 10 Pharma

4 of Top 10 Mining

4 of Top 10 Utilities

Chemicals
Electric Utilities
Manufacturing
Mining
Oil & Gas
Pharma
Water

Airports
Automotive
Building Automation
Food & Retail
Logistics
Smart Cities
Transportation
Global Footprint

2,600,000+
OT, IoT and IT Devices Monitored

2,250+
Installations Worldwide

Worldwide Offices

Partnering to Accelerate OT and IoT Security

200+
System Integrators and VARs

500+
Trained and Certified Professionals
Guardian

Industrial Strength OT and IoT Security and Visibility

Nozomi Networks Guardian™ unlocks visibility across OT, IoT, and IT for accelerated security and digital transformation.

It reduces OT risks for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world.

Identify
Asset Discovery and Network Visualization

Assess
Vulnerability Assessment and Risk Monitoring

Detect
Advanced Anomaly and Threat Detection

Act
Time-Saving Dashboards and Forensic Tools

Scale
Unified Security for Thousands of Distributed Sites

Single Asset View with extensive information.

Portion of interactive Network Visualization Graph.
Automatically Track and Visualize Your Assets

Up-to-Date Asset Inventory
Enhances cyber resiliency and saves time with automated asset inventory
Provides extensive node information and identifies risks such as alerts and vulnerabilities

Quickly Detect Threats and Anomalous Behavior

Up-to-the-Minute Threat Detection
Identifies cybersecurity and process reliability threats
Detects early stage and late stage advanced threats and cyber risks

Reduced Risk Through Network Visualization
Provides instant awareness of your OT/IoT networks and their activity patterns
Presents key data such as traffic throughput, TCP connections and protocols used between nodes and zones

Guardian Appliances for any Environment

Large Enterprises
- 300,000 - 500,000 Nodes
- 3 - 6 Gbps Max. Throughput

Mid-enterprises
- Up to 40,000 Nodes
- 250 Mbps - 1 Gbps Max. Throughput

Ruggedized Environments
- 500 - 1,000 Nodes
- 100 - 250 Mbps Max Throughput

Portable Scenarios
- 2,500 Nodes
- 200 Mbps Max. Throughput

Remote Site Data Collectors
- 250 Nodes
- 1 Mbps Max. Throughput
- Sends data to Guardian for analysis
- A Virtual Appliance is also available

Virtual Environments and Containers

VIRTUAL APPLIANCE
- 1,000 - 40,000 Nodes
- 1 Gbps Max. Throughput

CONTAINER EDITION
- Cisco Catalyst
- Siemens RUGGEDCOM

For more details, visit: nozominetworks.com/techspecs.
Central Management Console

Centralized OT and IoT Security and Visibility for Distributed Sites

Nozomi Networks’ Central Management Console™ (CMC) delivers centralized OT and IoT security and visibility—no matter how large or globally distributed your business is.

Whether you’re consolidating visibility and risk management at the edge or in the cloud, the CMC is fast and simple to deploy.

Consolidate
Asset Discovery and Network Visualization

Visualize
Vulnerability Assessment and Risk Monitoring

Respond
Advanced Anomaly and Threat Detection

Scale
Unified Security for Thousands of Distributed Sites

Sample deployment map for centrally monitoring and securing many facilities.
Centrally Monitor Your Distributed Sites

Single Console Access
Maps your Guardian appliances and shows risk level by site
Delivers aggregated summaries with drilldown to detailed information by site
Deploys in the cloud (AWS or Azure), or at the edge, for anytime, anywhere access

Unified Security Monitoring
Integrates quickly with security infrastructure including with asset, ticketing and identity management systems, and SIEMs
Streamlines security processes across IT/OT
Makes it easy to harmonize data for cohesive response, see: nozominetworks.com/integrations

Optimize Troubleshooting and Forensic Effort

Smart Incidents Speed Up Forensics
Reduces response time with Smart Incidents™ that:
• Correlate and consolidate alerts
• Provide operational and security context
• Supply automatic packet captures

Fast Forensic Analysis
Decodes incidents with Time Machine™ before and after system snapshots
Provides fast answers with a powerful ad hoc query tool

High Performance for Multinational Deployments

Fast, Flexible Deployment
Quickly scales for enterprise-wide deployment with optimum performance
Adapts to all sites, with multiple appliance models and flexible deployment options

High Availability, High Security
Ensures continuous OT and IoT monitoring with high availability configuration
Connects with field appliances using encrypted, bandwidth optimized data transfers

CMC Appliances
In the Cloud or at the Edge

Mid-enterprises

PHYSICAL APPLIANCE
◆ 50 Max. Managed Guardian Appliances
◆ 250 Mbps–1 Gbps Max. Throughput

Cloud or Virtual Environments

CLOUD
◆ Amazon AWS
◆ Microsoft Azure

VIRTUAL
◆ Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+
◆ Unlimited* Max. Managed Appliances
◆ 100+ GB Storage

*Based on the infrastructure. For complete and current tech specs, visit nozominetworks.com/techspecs.
Flexible Deployment and Licensing

You can deploy the Nozomi Networks solution in a wide variety of mixed environments for rapid asset discovery, network visualization and accelerated security.

Multiple Licensing Options

Nozomi Networks offers a range of licensing options to fit your organization's preferences, including:

- Subscription licenses
- Enterprise license agreements (ELAs)
- Perpetual licenses

Please contact your Nozomi Networks Sales Director for more information.
Sample Deployment Architecture

Purdue Model Example

You can tailor the Nozomi Networks solution to meet your needs by utilizing its flexible architecture, extensive range of appliances, and integrations with other systems.

World Class Partners

Nozomi Networks partners deeply with the IT/OT services and technology companies you trust. These include:

- **Strategic alliances** with enterprise IT and managed security providers
- **Technology integrations** with leading IT/OT solutions
- **SI/VAR relationships** with 200+ prominent organizations around the world

Visit [nozominetworks.com/partners](http://nozominetworks.com/partners) for more information.
Enhance Guardian for Expanded Visibility and Threat Detection

**GUARDIAN ADD-ON**

**Smart Polling**

- Adds low-volume active polling to Guardian’s passive asset discovery
- Identifies non-communicating assets and rogue devices
- Delivers accurate vulnerability assessment for fast and efficient response

Complete details available at: [nozominetworks.com/smart-polling](http://nozominetworks.com/smart-polling)

**GUARDIAN ADD-ON**

**Remote Collectors**

- Supplement Guardian data via low-resource appliances for distant and distributed locations
- Collect data and send it to Guardian for further analysis
- Reduce deployment costs for wilderness, off-shore or desert locations

Complete details available at: [nozominetworks.com/techspecs](http://nozominetworks.com/techspecs)

**SERVICE**

**Threat Intelligence**

- Reduces risks by shrinking the mean-time-to-detection (MTTD), minimizing impacts
- Delivers ongoing OT and IoT threat and vulnerability intelligence for rapid risk detection
- Consists of rules, signatures and vulnerability updates created and curated by Nozomi Networks Labs, a team of expert security researchers

Complete details available at: [nozominetworks.com/threat-intelligence](http://nozominetworks.com/threat-intelligence)

**SERVICE**

**Asset Intelligence**

- Reduces risk by eliminating anomaly alert overload and focusing your attention on critical incidents, decreasing the mean-time-to-respond (MTTR)
- Delivers ongoing OT and IoT asset intelligence for rapid asset identification and precise anomaly detection
- Updates Guardian’s anomaly detection technology with device profiles and behavior data based on analysis of millions of devices in use at sites around the world

Complete details available at: [nozominetworks.com/asset-intelligence](http://nozominetworks.com/asset-intelligence)
What to Look for in an OT and IoT Security and Visibility Solution

Technology advancements, such as those found in the Nozomi Networks solution, can dramatically improve security and reliability.

When choosing a solution, look for the following characteristics:

- Comprehensive OT and IoT and visibility
- Advanced threat detection
- Accurate anomaly alerts
- Proven scalability across thousands of sites
- Easy IT/OT integration
- Global partner ecosystem
- Exceptional customer engagement and support

See the Nozomi Networks Solution in Action

If you would like to see our solution in action, and experience how easy it is to work with Nozomi Networks, please contact us at nozominetworks.com/contact

Want to Know More?

DATA SHEET Guardian
DATA SHEET Central Management Console
DATA SHEET Threat Intelligence
DATA SHEET Asset Intelligence

DOWNLOAD DOWNLOAD DOWNLOAD DOWNLOAD
Nozomi Networks

The Leading Solution for OT and IoT
Security and Visibility

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate
digital transformation by unifying cybersecurity visibility for the largest critical
infrastructure, energy, manufacturing, mining, transportation, building automation
and other OT sites around the world. Our innovation and research make it possible
to tackle escalating cyber risks through exceptional network visibility, threat
detection and operational insight.