NOZOMI NETWORKS

Guardian

Industrial Strength OT and IoT Security and Visibility

Nozomi Networks **Guardian™** unlocks visibility across your OT, IoT, IT, edge and cloud assets, for accelerated security and digital transformation.

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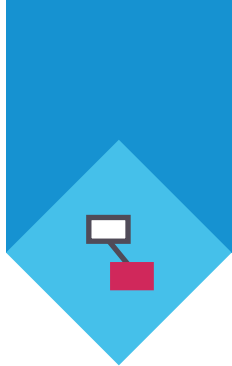
IDENTIFY

ACT **SCALE** **ASSESS**
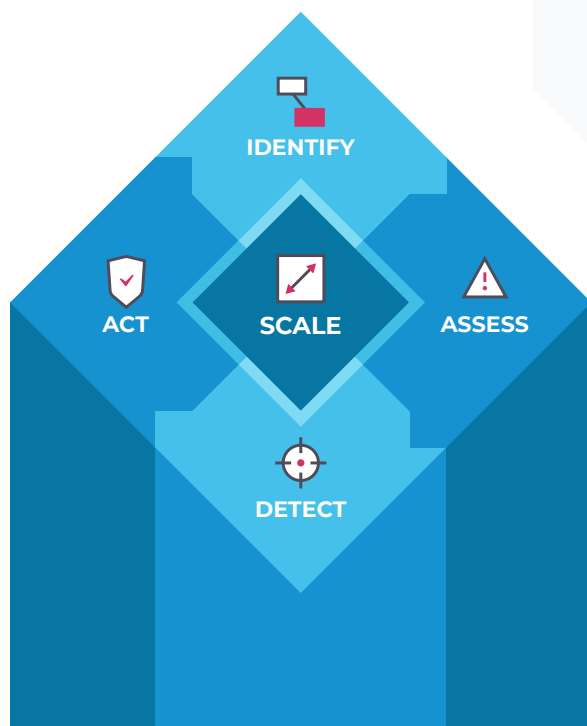
DETECT

See

All OT and IoT assets and behavior on your networks for unmatched awareness

Detect

Cyber threats, vulnerabilities, risks and anomalies for faster response

Unify

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

Identify

Asset Discovery and Network Visualization

Automatically Track Your OT and IoT Assets

Up-to-Date Asset Inventory

Enhances cyber resilience and saves time with automated asset inventory

Identifies all communicating assets

Provides extensive node information including name, type, serial number, firmware version and components

Presents risk information including security and reliability alerts, missing patches and vulnerabilities

ADD-ON
Smart Polling

Expands Guardian's built-in passive asset discovery with low-volume active polling, see:

nozominetworks.com/smart-polling

SUBSCRIPTION
Asset Intelligence

Accelerates the asset learning process and keeps asset profiles and behavior data up-to-date, see:

nozominetworks.com/asset-intelligence

Immediately Understand Your Networks

Reduced Risk Through Network Visualization

Provides instant awareness of your OT/IoT network and its activity patterns

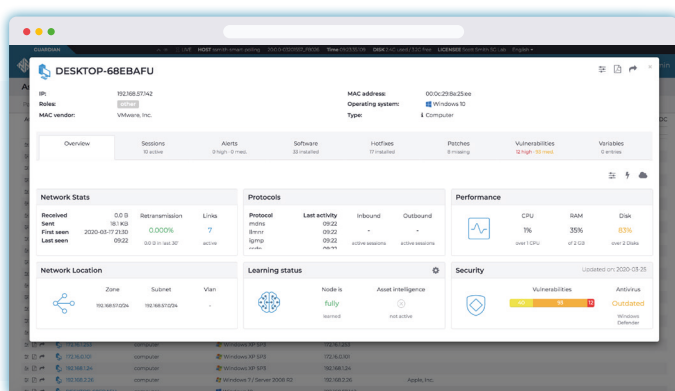Presents key data such as traffic throughput, TCP connections, and protocols

Improves your understanding of 'normal' operations

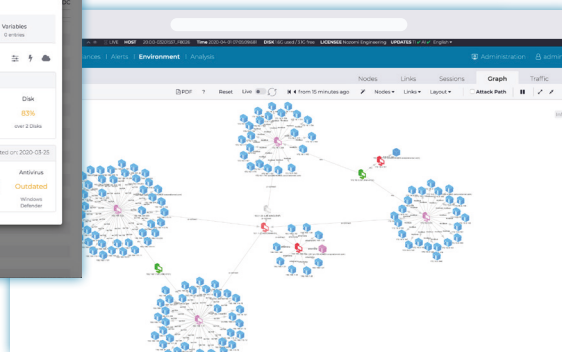### Intuitive Dashboards and Reports

Explore macro views as well as detailed information on endpoints and connections

Filter by subnets, type, role, zone and topologies

Group assets visually, in lists and detailed single asset views

Single **Asset View** with extensive information.

Portion of interactive **Network Visualization Graph**.

Assess

Vulnerability Assessment and Risk Monitoring

Rapidly Identify Your Vulnerability Risks

Automated Vulnerability Assessment

Identifies which vendors' devices are vulnerable

Utilizes the U.S. government's National Vulnerability Database (NVD) for standardized naming, description and scoring

Efficient Prioritization and Remediation

Speeds response with vulnerability dashboards, drilldowns and reports

Answers questions like:
- "Are my assets running vulnerable firmware?"
- "Are assets from Vendor X vulnerable?"

Continuously Monitor Your Networks and Automation Systems

Continuous Monitoring

Continuous monitoring of all supported protocols: OT, IoT and IT

No critical blind spots in protection caused by limited monitoring or inadequate protocol support

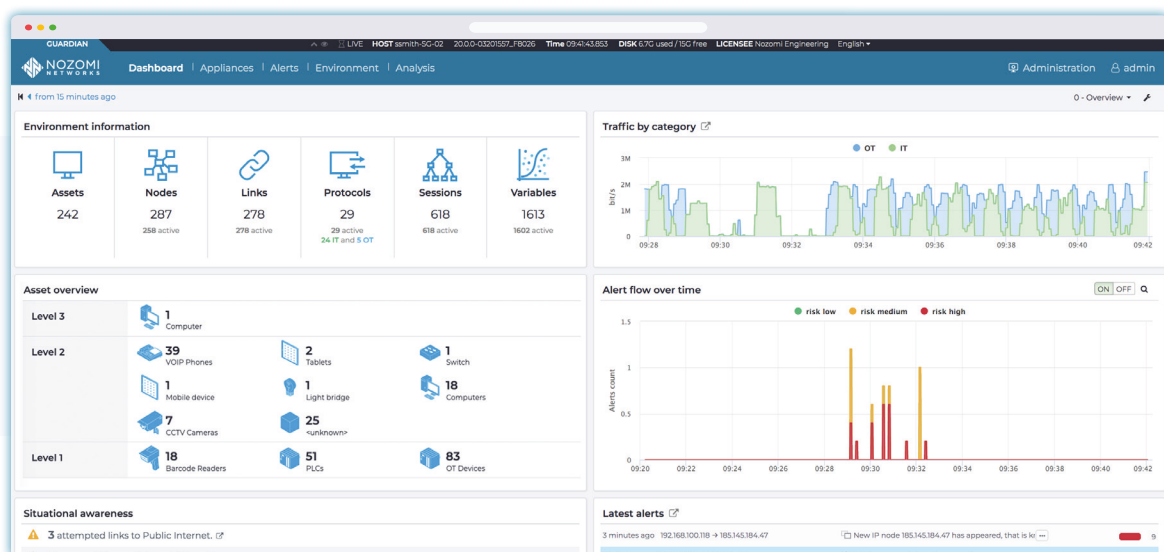Monitors assets from all vendors and all network communications
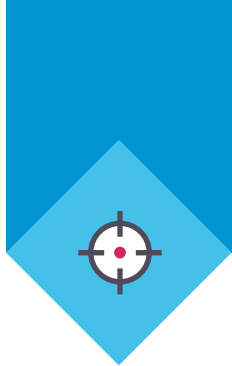
Easy Access to OT Data

Summarizes OT and IoT risk information for customizable date and time ranges

Highlights indicators of reliability issues, such as unusual process values

Queries any aspect of your network or control system performance, reducing data collection and spreadsheet work

Portion of customizable **Guardian Dashboard**.

Detect

Advanced Anomaly and Threat Detection

Quickly Detect and Disrupt 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

Blocks attacks when integrated with compatible firewalls and endpoint security products

Superior OT and IoT Threat Detection

Combines behavior-based anomaly detection with signature-based threat detection for comprehensive risk monitoring

Provides detailed threat information as Yara rules, packet rules, STIX indicators, threat definitions, a threat knowledgebase and vulnerability signatures

Effectively Monitor Mixed Environments

SUBSCRIPTION
Threat Intelligence

Ensures up-to-date threat detection and vulnerability identification using indicators created and curated by Nozomi Networks Labs

Delivers ongoing OT, IoT and IT threat and vulnerability intelligence

SUBSCRIPTION
Asset Intelligence

Powers breakthrough anomaly detection accuracy for OT and IoT that filters out alerts for benign behavior, accelerating incident response

Delivers ongoing OT and IoT asset profile and behavior data

Breakthrough Anomaly Detection for OT and IoT

Rapid Identification of Assets
▼
Ensures Precise Asset Inventory

Accurate Anomaly Alerts
▼
Accelerates Incident Response

Asset Intelligence for Dynamic Networks
▼
Sustains Accurate Inventory & Detection

Act
Time-saving Dashboards and Forensic Tools

Significantly Improve OT and IoT Risk Management

Dashboards and Customizable Reports Highlight Risks

Focuses attention on key concerns by summarizing risks and threats

Built-in reports are customizable. You can select from predefined widgets to add exactly the information you need

Detailed Alerts Provide Key Information

Generates detailed, accurate alerts

Identifies security and reliability risks

Groups alerts into incidents, providing security and operations staff with a simple, clear, consolidated view of what's happening on their network

Greatly Reduce Troubleshooting and Forensic Efforts

Accelerated Incident Response

Combines Guardian's breakthrough anomaly detection for OT and IoT with the **Asset Intelligence™** service for focused, actionable alerts

Understands normal behavior for assets with frequent behavior changes, eliminating alerts for benign anomalies

Improves response time and productivity with precise alerts that are easy to prioritize

Fast Forensic Analysis
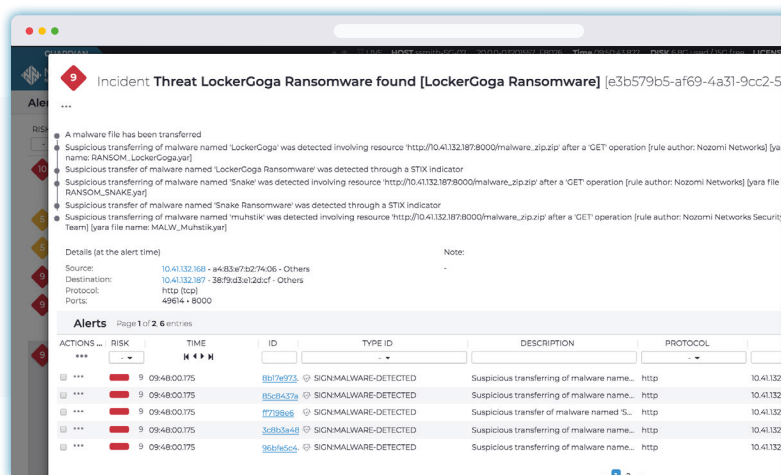
Focuses effort with Smart Incidents™ that:
- Correlate and consolidate alerts
- Provide operational and security context
- Supply automatic packet captures

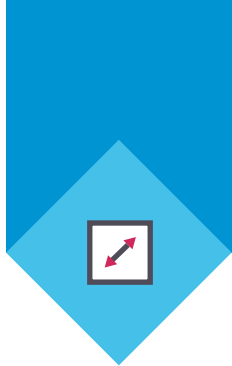Decodes incidents with Time Machine™ before and after system snapshots

Provides answers fast with a powerful ad hoc query tool

Smart Incident showing related alerts and security context.

Report summarizing alerts for a site.

Scale

Unified Security for Hundreds of Thousands of Assets

Readily Scale with Optimal Performance

Exceptional Local & Global Performance

Processes data for up to 500,000 assets in real-time

Generates network visualizations, dashboards and reports quickly

Speeds up threat detection and response with local processing of threat and asset intelligence

Consolidated Monitoring of All Facilities

Aggregates data from multiple sites when used with **Vantage™**

Enables centralized security risk management for all sites

Provides visibility into all OT/ IoT environments

Easily Integrate with SOC/IT Environments

Integrated Security Infrastructure

Streamlines security processes across IT/OT

Makes it easy to harmonize security data for cohesive response

Includes built-in integrations for asset, ticket and identity management systems, as well as SIEMs

nozominetworks.com/integrations

Broad Protocol Support

Supports hundreds of OT, IoT and IT protocols

Utilizes Nozomi Networks' deep expertise in OT protocols for accurate analysis

Includes Protocol SDK and on-demand engineering services for new protocol support

nozominetworks.com/techspecs
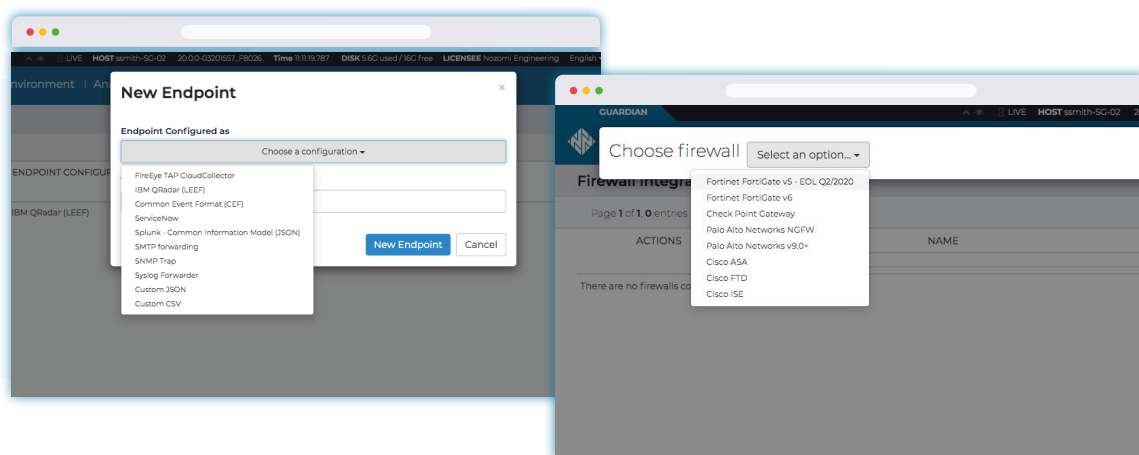
Built-in integrations make it easy to streamline security processes.

OT and IoT
Security and Visibility

Industrial Strength Cyber and Operational Resilience

You can protect a wide variety of mixed environments with rapid asset discovery, network visualization and accelerated security.
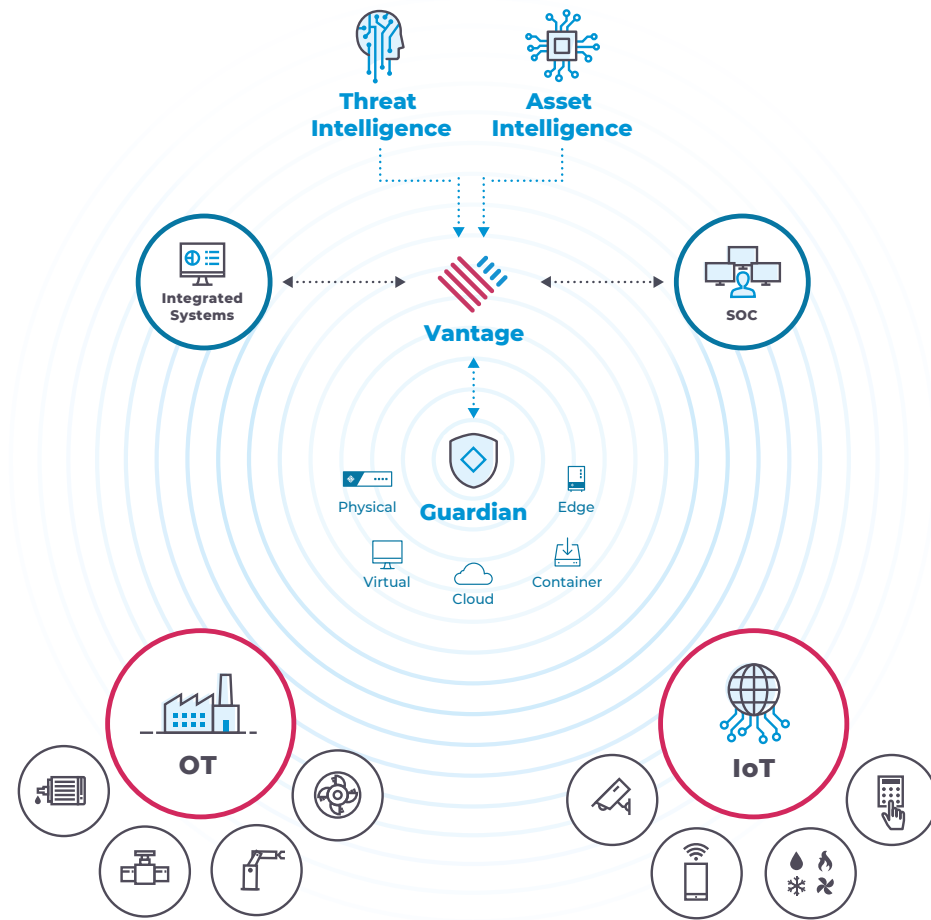
Respond to Incidents Faster

For the first time you can see all the assets on your network and know their behavior.

Our technology quickly and accurately detects malicious and anomalous activity.

You have the insights you need to understand and respond to threats before data theft or operational disruptions occur.

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 sensors, and integrations with other systems.
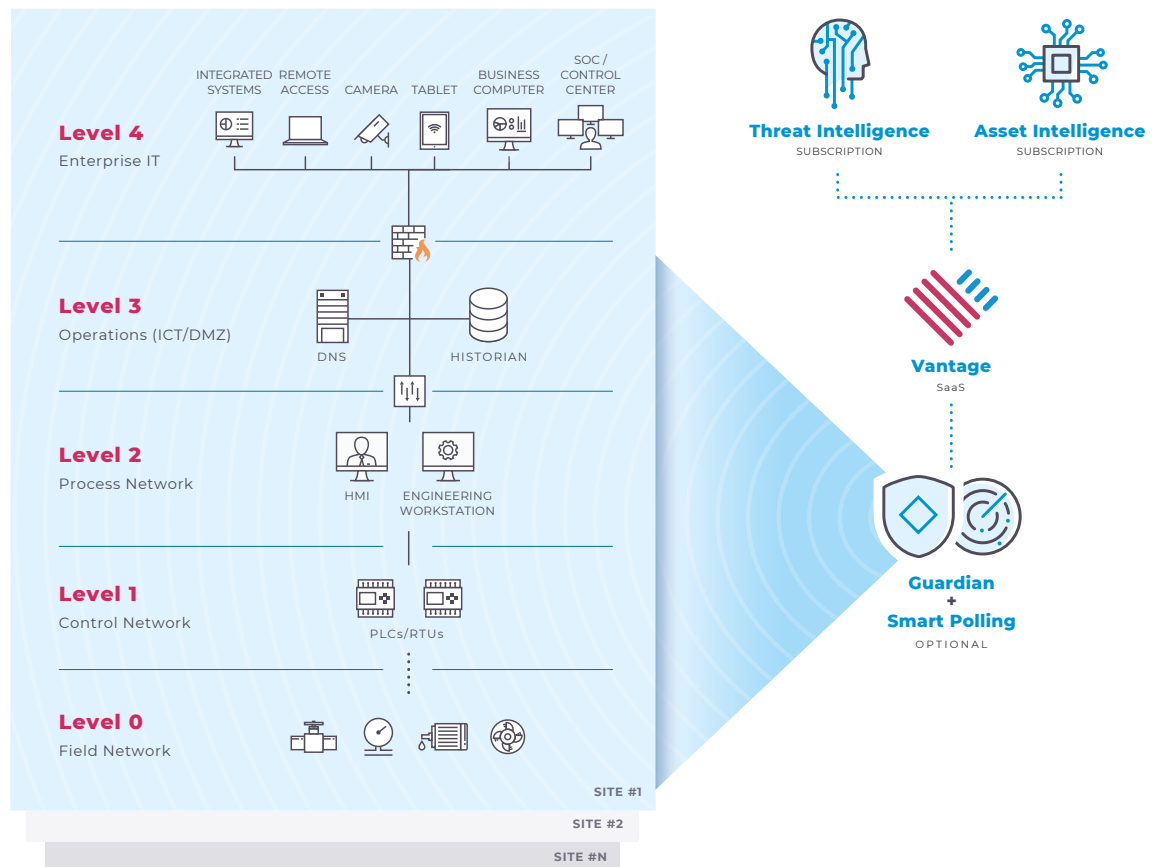
World Class Partners

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
- **Global network** of SI, VAR and distribution partners

Visit **nozominetworks.com/partners** for more information.

Enhance Guardian for Expanded Visibility and Threat Detection

SUBSCRIPTION
Threat Intelligence

Reduces risks by shrinking the mean-time-to-detect (MTTD), minimizing impacts

Delivers regular updates to detect emerging threats and new vulnerabilities

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

SUBSCRIPTION
Asset Intelligence

Reduces risks by decreasing the mean-time-to-respond (MTTR) to operational anomalies

Delivers regular updates for faster and more accurate anomaly detection

Updates Guardian's anomaly detection technology with device profiles and behavior data based on analysis of millions of assets in use at sites around the world

Complete details available at:
nozominetworks.com/asset-intelligence

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

GUARDIAN ADD-ON
Remote Collectors

Supplements Guardian's data via low-resource sensors for distributed locations

Collects data and sends it to Guardian for further analysis

Reduces deployment costs for wilderness, off-shore or other isolated locations

Complete details available at:
nozominetworks.com/techspecs

Guardian Sensors

for the Large Enterprise

NSG-HS Series

Rack-mounted sensors for real-time OT/IoT visibility, cybersecurity and monitoring.

◆ **300,000 - 500,000 Nodes**

◆ **6 Gbps Max. Throughput**

NSG-H Series

Rack-mounted sensors for real-time OT/IoT visibility, cybersecurity and monitoring.

◆ **100,000 - 200,000 Nodes**

◆ **3 Gbps Max. Throughput**

	NSG-HS 3500	NSG-HS 3000	NSG-H 2500	NSG-H 2000
Max. Protected Nodes	500,000	300,000	200,000	100,000
Max. Virtual RTUs*	3,000,000	1,800,000	1,200,000	600,000
Max. Throughput	6 Gbps		3 Gbps	
Max. Remote Collectors**	50		50	
Monitoring Ports	Modular up to 16+1		Modular up to 8+1	
Management Ports	1x1000Base-T		1x1000Base-T	
Expansion Slots	4 slots available: 4x1000BaseT | 4xSFP | 4xSFP+		2 slots available: 4x1000BaseT | 4xSFP | 4xSFP+	
Storage	512 GB		512 GB	
Form Factor	1 rack unit		1 rack unit	
Max. Power Consumption	750 W		750 W	
Power Supply	100-240V AC - 50/60Hz 36-72V DC Dual		100-240V AC - 50/60Hz 36-72V DC Dual	
Temperature Range	0 / +40° C		0 / +40° C	
HxWxL (mm/in)	44 x 438 x 600 1.73 x 17.24 x 23.60		44 x 438 x 600 1.73 x 17.24 x 23.60	
Weight	18 Kg		17 Kg	

* Virtual RTUs can either be subRTUs or smart meters reachable through direct or serial communication. ** See Remote Collector tech specs for more details. For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Guardian Sensors

for the Mid-Enterprise

NSG-M Series

Rack-mounted sensors for real-time OT/IoT visibility, cybersecurity and monitoring.

- ◆ **10,000 - 40,000 Nodes**
- ◆ **1 Gbps Max. Throughput**

NSG-L Series

Rack-mounted sensors for real-time OT/IoT visibility, cybersecurity and monitoring.

- ◆ **1,000 - 5,000 Nodes**
- ◆ **250 - 500 Mbps Max. Throughput**

	NSG-M 1000	NSG-M 750	NSG-L 250	NSG-L 100
Max. Protected Nodes	40,000	10,000	5,000	1,000
Max. Throughput	1 Gbps		500 Mbps	250 Mbps
Max. Remote Collectors*	50		20	
Monitoring Ports	7x1000BASE-T + 4xSFP		5x1000BASE-T	
Management Ports	1x1000Base-T		1x1000Base-T	
Expansion Slots	1 slot available: 4x1000Base-T | 4xSFP | 4xSFP*		1 slot available: 4x1000Base-T | 4xSFP	
Storage	256 GB		64 GB	
Form Factor	1 rack unit		1 rack unit	
Max. Power Consumption	360W		250W	
Power Supply	100-240V AC - 50/60 Hz Single		100-240V AC - 50/60 Hz Single	
Temperature Range	0 / +45° C		0 / +45° C	
HxWxL (mm/in)	44 x 429 x 438 1.73 x 16.89 x 17.24		44 x 438 x 300 1.7 x 17.2 x 11.8	
Weight	14 Kg		8 Kg	

* See Remote Collector tech specs for more details. | For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Guardian Sensors
for Specialized Requirements

NSG-R Series

Ruggedized sensors for real-time OT/IoT visibility, cybersecurity and monitoring.

◆ **500 - 1,000 Nodes**

◆ **100 - 250 Mbps Max. Throughput**

Portable

Portable sensor for real-time OT/IoT visibility, cybersecurity and monitoring.

◆ **2,500 Nodes**

◆ **200 Mbps Max. Throughput**

	NSG-R 150	NSG-R 50	P550
Max. Protected Nodes	1,000	500	2,500
Max. Throughput	250 Mbps	100 Mbps	200 Mbps
Max. Remote Collectors*	20	10	Not available
Monitoring Ports	7x1000BASE-T	4x1000BASE-T	5x1000BASE-T
Management Ports	1x1000Base-T		1x1000Base-T
Expansion Slots	Not available		Not available
Storage	64 GB		256 GB
Form Factor	2 rack unit	DIN mountable	Desktop with wall mount kit
Max. Power Consumption	250W	60W	38W
Power Supply	100-240V AC 100-240V DC Dual	100-240V AC 12-36V DC Single	90-240V AC 12-30V DC Single
Temperature Range	-40 / +70° C	-40 / +75° C	0 / +60° C
HxWxL (mm/in)	88 x 440 x 301 3.46 x 17.32 x 11.86	80 x 130 x 146 3.15 x 5.11 x 5.74	70 x 180 x 240 2.75 x 7.08 x 9.44
Weight	6 Kg	3 Kg	2.5 Kg

* See Remote Collector tech specs for more details. | For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Guardian Sensors

for Remote Sites

Remote Collector

Low-resource sensors that collect asset and network data in remote locations and send it to Guardian for further analysis.

◆ **Up to 15 Mbps Throughput**

	NRC-5
Max. Throughput	Up to 15 Mbps
Remote Collector Support	Not available
Monitoring Ports	2x1000Base-T, 1xSFP
Management Ports	1x1000Base-T
Expansion Slots	Not available
Storage	8 GB
Form Factor	DIN mountable
Max. Power Consumption	12W
Power Supply	12-36V DC Single
Temperature Range	-40 / +70° C
Heat Generation	55.44 BTU/hr
HxWxL (mm/in)	41.5 x 170 x 138 / 2.71 x 6.67 x 5.00
Weight	1.2 Kg
Compliance	RoHS
Certifications	CE, FCC, UL
	Virtual Remote Collector
Max. Throughput	15 Mbps
Deployment Options	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+

For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Guardian Sensors
for Virtual Environments and Containers

Virtual Series

Virtual sensors for real-time OT/IoT visibility, cybersecurity and monitoring.

◆ **1,000 - 40,000 Nodes**

◆ **1 Gbps Max. Throughput**

	V1000	V750	V250	V100
Max. Protected Nodes	40,000	10,000	5,000	1,000
Max. Throughput*	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Scenarios	Enterprise	Large	Medium	Small
Deployment Options	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+			
Max. Remote Collectors**	50	50	20	20

* Performance is dependent upon hardware configuration and resource allocation. ** See Remote Collector tech specs for details.

Container Edition

Embedded container sensor for switches, routers and other security infrastructure.
Fast, flexible deployment option that leverage your existing devices.

◆ **Available for Guardian with the Smart Polling add-on module only**

	Container
Embedded Offerings	Gatewatcher, Siemens RUGGEDCOM
Add-ons	Smart Polling module: *included* | Threat Intelligence and Asset Intelligence subscriptions: *can be added*
Remote Collector Support	Not available

For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Multiple Deployment and Support Options

Here are several options for deployment and support assistance:

· **Nozomi Networks Global Strategic Alliance Partners**

· **Nozomi Networks SI/VARs**

· **Nozomi Networks Professional Services**

· **Nozomi Networks Global Customer Support**

Products and Services

SAAS
Vantage

Vantage accelerates digital transformation with unmatched security and visibility across your OT, IoT, and IT networks. Its scalable SaaS platform enables you to protect any number of assets, anywhere. You can respond faster and more effectively to cyber threats, ensuring operational resilience.

Requires Guardian sensors.

EDGE OR PUBLIC CLOUD
Guardian

Guardian provides industrial strength OT and IoT security and visibility. It combines asset discovery, network visualization, vulnerability assessment, risk monitoring and threat detection in a single application. Guardian shares data with both Vantage and the CMC.

EDGE OR PUBLIC CLOUD
Central Management Console

The Central Management Console (CMC) consolidates OT and IoT risk monitoring and visibility across your distributed sites, at the edge or in the public cloud. It integrates with your IT security infrastructure for streamlined workflows and faster response to threats and anomalies.

SUBSCRIPTION
Asset Intelligence

The Asset Intelligence service delivers regular profile updates for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-respond (MTTR).

SUBSCRIPTION
Threat Intelligence

The Threat Intelligence service delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of emerging threats and new vulnerabilities, and reduce your mean-time-to-detect (MTTD).

GUARDIAN ADD-ON
Smart Polling

Smart Polling adds low-volume active polling to Guardian's passive asset discovery, enhancing your asset tracking, vulnerability assessment and security monitoring.

GUARDIAN ADD-ON
Remote Collectors

Remote Collectors are low-resource sensors that capture data from your distributed locations and send it to Guardian for analysis. They improve visibility while reducing deployment costs.

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.

nozominetworks.com