

## Complete Cyber Security and Visibility for ICS Environments



Immediately  
Visualize and Explore  
Industrial Networks



Automatically Track  
Industrial Assets and Know  
Their Cyber Security Risks



Continuously  
Monitor ICS Risks  
and Processes



Quickly Identify  
and Address  
Vulnerabilities



Rapidly Detect Cyber  
Threats/Risks and  
Process Anomalies



Easily Integrate  
with SOC/IT Tools  
and Workflows

**Guardian™** protects your control networks from cyberattacks and operational disruptions by providing complete ICS visibility and security in a single, unified solution.

Its advanced technology automatically maps and visualizes your entire industrial network, including assets, connections, and protocols. Guardian monitors network communications and behavior for risks that threaten the reliability of your systems, and provides the information you need to respond quickly.

Available as a passive monitoring solution, or a low-impact active solution with the **Smart Polling™** add-on, Guardian allows you to choose the asset discovery approach that best fits your organization.

### Guardian delivers:

- Superior asset identification, network visualization and ICS risk monitoring
- Real-time ICS threat, anomaly and vulnerability detection
- Enterprise-class scalability when deployed with the **Central Management Console™ (CMC)**
- Seamless integration with other security and IT tools

Find out how customers improve the reliability, cyber security and operational efficiency of their facilities with Guardian.

Contact us today at [nozominetworks.com/contact](https://nozominetworks.com/contact)

### Superior Operational Visibility

- Intuitive network visualization
- Automated asset inventory
- Real-time network monitoring

### The Best ICS Threat Detection

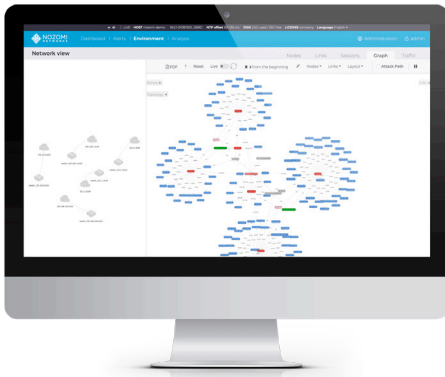
- Behavior-based anomaly detection
- Rules and signature-based threat detection
- Advanced correlation for detailed insights and rapid remediation
- **OT ThreatFeed™** subscription ensures rapid detection of emerging risks

### Extensive Global Installations

- Multinational deployments with hundreds of facilities and thousands of devices
- Monitors and reduces OT risks in sectors such as critical infrastructure, energy, manufacturing, mining, transportation and utilities

### Time-Saving Forensic Tools

- Dynamic Learning™ that reduces false alerts
- Automatic packet capture
- TimeMachine™ system snapshots
- Real-time ad hoc query tool



## Immediately Visualize Your Industrial Network

### Real-time Network Visualization

- Improves system awareness and understanding of network structure and activity
- Displays key information such as traffic throughput, TCP connections, and the protocols used between nodes and zones
- Speeds incident response and troubleshooting efforts

### Flexible Navigation and Filtering

- Shows macro views plus detailed information on endpoints and connections
- Filters by subnets, network segments and topologies

## Automatically Track Your Industrial Assets

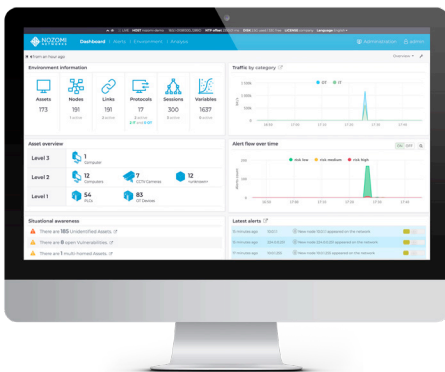
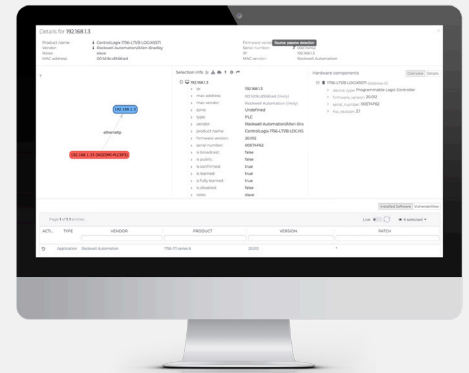
### Up-to-Date Asset Inventory

- Advances cyber resiliency and saves time with automated asset inventory
- Provides detailed and verified asset information
- Identifies communicating assets using built-in passive network monitoring

### Enhance Asset Tracking with Smart Polling Add-on Module

- Discovers silent and rogue assets with active discovery
- Includes firmware versions, patch levels and more

See *Smart Polling* section, page 5, for more details.



## Continuously Monitor Your Network and ICS

### Comprehensive Cyber Security and Reliability Monitoring

- Improves network security and productivity through dashboards, charts and queries relevant to your organization
- Monitors assets from all vendors and all network communications

### Clear Presentation of Key Metrics

- Displays summarized data related to alerts, incidents, vulnerabilities, etc.
- Includes indicators of reliability issues such as unusual process values

### Easy Access to ICS Data

- Summarizes ICS risk information for selected date and time ranges
- Supports drilldown on visual indicators for detailed information
- Queries any aspect of your network or ICS performance, reducing data collection and spreadsheet work



## Quickly Detect Threats to Your ICS or SCADA System

### Up-to-the-Minute Threat Detection

- Identifies cyber security and process reliability threats in real-time
- Detects attacks in process, early stage advanced threats and cyber risks
- Blocks attacks when integrated with compatible firewalls

### Best-in-Class ICS Threat Detection

- Uses anomaly and signature-based threat detection for comprehensive risk detection
- Ensures current monitoring when integrated with OT ThreatFeed subscription

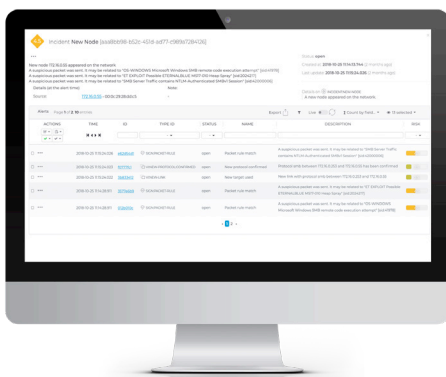
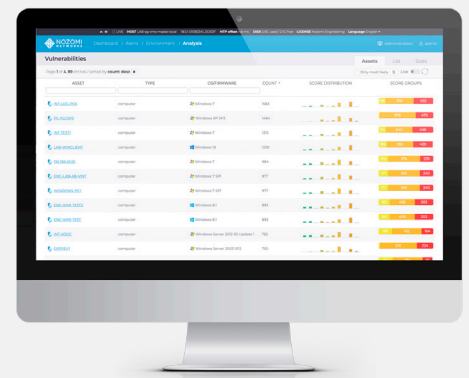
## Rapidly Identify Your Vulnerability Risks

### 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 workflows with vulnerability dashboards and drilldowns
- Addresses questions like "Do certain devices have vulnerable firmware?"



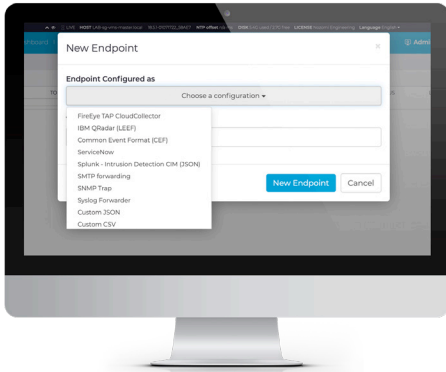
## Reduce Troubleshooting and Forensic Efforts

### Effective, Efficient Incident Response

- Minimizes false positives with AI-powered Dynamic Learning
- Decreases response time with Smart Incident™, which correlates alerts, provides operational context and delivers automatic packet captures

### Informative Forensics

- Decodes incidents with Time Machine™ system snapshots and diff reports (Snapshots are dynamic, allowing drilldown into rich ICS data.)
- Provides answers fast with a powerful ad hoc query tool



## Easily Integrate with SOC/IT Environments

### ✓ Integrated Security Infrastructure

- Includes built-in integrations for asset, ticket and identity management systems, SIEMs and more
- Extends further with OpenAPI for additional integrations

### ✓ Broad Protocol Support

- Supports hundreds of ICS and IT protocols
- Includes Protocol SDK and on-demand engineering services for quick creation of new protocol support

### ✓ Complete Details Available Online

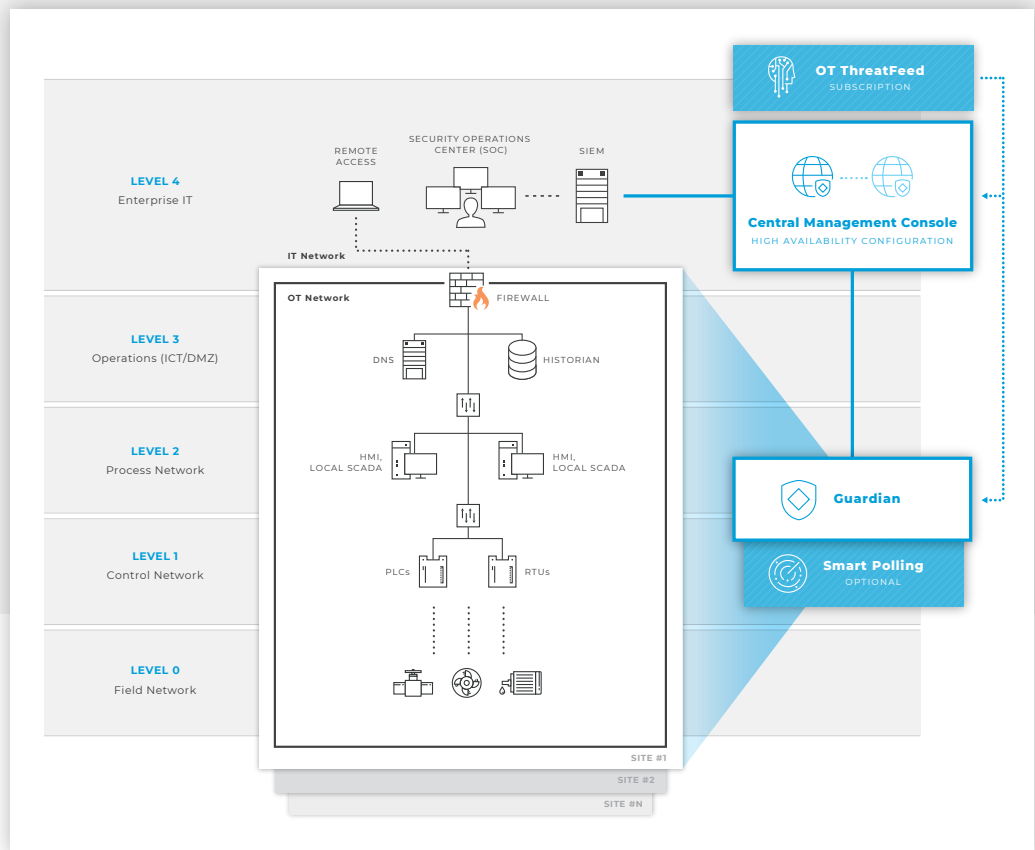
- See [nozominetworks.com/techspecs](https://nozominetworks.com/techspecs)

## Sample Deployment Architecture

This is a general example of how the Nozomi Networks solution can be deployed.

A wide variety of appliances, a flexible architecture, and integrations with other systems allow us to provide a solution tailored to meet the needs of your organization.

Additionally, **Remote Collectors™** can be added to Guardian appliances to capture data from remote and offsite locations.



# Enhance Guardian for Complete OT Visibility & Threat Detection

## GUARDIAN ADD-ON MODULE



### Smart Polling for Active Asset Inventory



#### Hybrid Passive + Active Asset Discovery Enhances Guardian

- Adds low volume, active technologies to Guardian's passive asset discovery
- Provides precise asset details, a complete asset inventory, exact vulnerability assessment and advanced ICS security monitoring



#### Comprehensive ICS Asset Details

- Identifies non-communicating assets and rogue devices
- Detects USB devices on Windows systems
- Gathers details about changes in process flows and variables
- Discovers operating system information, firmware, patch levels and more
- Delivers accurate vulnerability assessment for fast and efficient response



#### Enhanced Network Monitoring and Threat Detection

- Uses a full set of ICS data for enhanced anomaly detection
- Integrates with OT ThreatFeed for up-to-date detection of emerging threats and zero-days



#### Flexible Usage Options

- Applies across your entire network or only to targeted segments or assets

## GUARDIAN ADD-ON SUBSCRIPTION



### OT ThreatFeed for Up-to-Date Threat Intelligence



#### Stay on Top of the Dynamic Threat Landscape

- Makes it easy and efficient to stay on top of current ICS risks
- Delivers up-to-date threat intelligence for ICS environments



#### Timely Threat Updates

- Provides emerging threats, zero-day, and vulnerability information, curated by Nozomi Networks Labs
- Includes threat detection tools such as Packet rules, Yara rules, vulnerability signatures, STIX indicators and a threat knowledgebase



#### Threat Insights that Strengthen Cyber Resiliency

- Provides full network visibility with integrated threat intelligence
- Extensive protocol support and many integrations for SOC/IT/OT environments are available.
- Generates real-time alerts about suspicious activity
- Reduces security management costs as a single, comprehensive ICS threat detection tool

## GUARDIAN ADD-ON APPLIANCE



### Remote Collectors for Expansive Visibility and Cyber Security





#### Low-Resource Appliances for Distant and Distributed Installations

- Collect data from remote locations and send it to Guardian for further analysis
- Reduce deployment costs for wilderness, off-shore or desert installations

# Multiple Guardian Appliance Formats to Meet Your Needs

## NSG-M Series

Rack-Mounted Appliances for Monitoring 2,500–10,000 Nodes



Product Descriptions		
Model	NSG-M 1000	NSG-M 750
Image		
Description	Rack-mounted appliances for real-time industrial network visibility, cyber security and monitoring	
Form Factor	1 rack unit	1 rack unit
Monitoring Ports	7 RJ45 + 4 SFP	7 RJ45 + 4 SFP
Maximum Protected Nodes	10,000	2,500
Maximum Remote Collectors*	20	20
Additional Interfaces		
Expansion Slots**	1	1
Maximum Throughput	1 Gbps	500 Mbps
Storage	256 Gb	256 Gb
Power Requirements		
Maximum Power Consumption	360W	360W
Power Supply Type	100-240V AC - 50/60 Hz	100-240V AC - 50/60 Hz
Ambient Conditions		
Temperature Range	0 / +45° C	0 / +45° C
Mechanical Construction		
HxWxL (mm/in)	44 x 429 x 438 / 1.73 x 16.89 x 17.24	44 x 429 x 438 / 1.73 x 16.89 x 17.24
Weight	14 Kg	14 Kg

\* See Remote Collector tech specs for more details.

\*\* Expansion slot can host either 4 additional RJ45 ports OR 4 additional SFPs.

## NSG-L Series

Rack-Mounted Appliances for Monitoring 300–750 Nodes



Product Descriptions		
Model	NSG-L 250	NSG-L 100
Image		
Description	Rack-mounted appliances for real-time industrial network visibility, cyber security and monitoring	
Form Factor	1 rack unit	1 rack unit
Monitoring Ports	5 RJ45	5 RJ45
Maximum Protected Nodes	750	300
Maximum Remote Collectors	Not available	Not available
Additional Interfaces		
Expansion Slots*	1	1
Maximum Throughput	200 Mbps	100 Mbps
Storage	64 Gb	64 Gb
Power Requirements		
Maximum Power Consumption	250W	250W
Power Supply Type	100-240V AC - 50/60 Hz	100-240V AC - 50/60 Hz
Ambient Conditions		
Temperature Range	0 / +45° C	0 / +45° C
Mechanical Construction		
HxWxL (mm/in)	44 x 438 x 300 / 1.7 x 17.2 x 11.8	44 x 438 x 300 / 1.7 x 17.2 x 11.8
Weight	8 Kg	8 Kg

\* Expansion slot can host either 4 additional RJ45 ports OR 4 additional SFPs.

# Readily Tailor Your Solution Using Multiple Appliance Formats

## NSG-R Series

Rugged Appliances for Monitoring 200–500 Nodes

Product Descriptions		
Model	NSG-R 150	NSG-R 50
Image		
Description	Ruggedized appliances for real-time industrial network visibility, cyber security and monitoring	
Form Factor	2 rack units	DIN mountable
Monitoring Ports	7 RJ45	4 RJ45
Maximum Protected Nodes	500	200
Maximum Remote Collectors	Not available	Not available
Additional Interfaces		
Expansion Slots	Not available	Not available
Maximum Throughput	200 Mbps	50 Mbps
Storage	64 Gb	64 Gb
Power Requirements		
Maximum Power Consumption	250W	60W
Power Supply Type	Dual power mode: 100-240V AC / 100-240V DC	12-36V DC / 100-240V AC (Provided power supply)
Ambient Conditions		
Temperature Range	-40 / +70° C	-40 / +70° C
Mechanical Construction		
HxWxL (mm/in)	88 x 440 x 301.2 / 3.46 x 17.3 x 118.58	80 x 130 x 146 / 3.15 x 5.11 x 5.74
Weight	6 Kg	3 Kg

## Virtual Appliances

Virtual appliances for Monitoring 300–10,000 Nodes

Model	V1000	V750	V250	V100
Description	A powerful appliance for enterprise scenarios	A virtual appliance for large scenarios	A virtual appliance for medium scenarios	A virtual appliance for small scenarios
Deployment Options	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+			
Max. Throughput*	1,000 Mbps	1,000 Mbps	1,000 Mbps	1,000 Mbps
Max. Protected Nodes	10,000	2,500	750	300
Maximum Remote Collectors**	20	20	Not available	Not available

\* Performance is dependent upon hardware configuration and resource allocation.

\*\* See Remote Collector tech specs for details.

## Container Appliances


Description*	Embedded container appliance for switches, routers and other security infrastructure Fast, flexible deployment option that leverages existing hardware units
Embedded Offerings	Cisco Catalyst / Siemens RUGGEDCOM

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

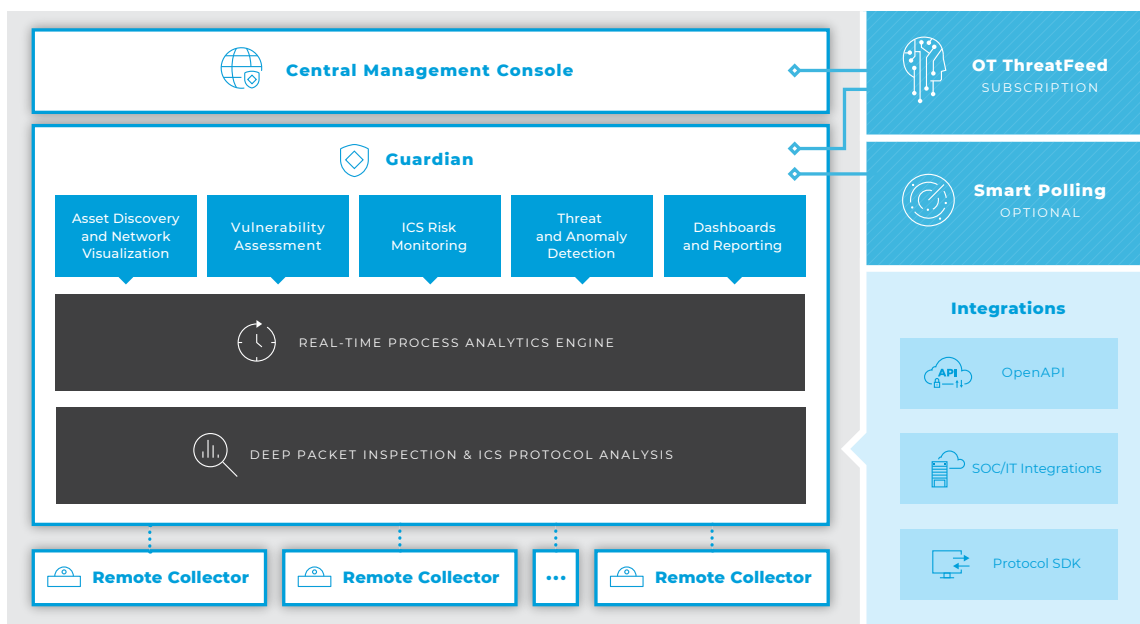
## Remote Collectors

Description	Low-resource appliances that collect asset and network data in remote locations and send it to Guardian for further analysis
Deployment Options*	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+
Max. Throughput	250 Kbps
Storage	10 Gb

\* Physical appliance deployment options are also available, [contact us](#) for details.

	<b>Protocols and Integrations</b> Extensive protocol support and many integrations for SOC/IT/OT environments are available. For complete and current tech specs, visit: <a href="https://nozominetworks.com/techspecs">nozominetworks.com/techspecs</a> , or <a href="#">contact us</a> .
---	---

# Nozomi Networks Solution Architecture



## Nozomi Networks Products and Services



**Guardian** provides complete visibility and cyber security for ICS environments by combining asset discovery, vulnerability assessment, threat detection, and anomaly detection in a single, unified solution.



**Central Management Console (CMC)** enables centralized security visibility and management for multi-tier, distributed OT deployments across the world.



**OT ThreatFeed** delivers up-to-date threat intelligence to effectively detect threats and identify vulnerabilities in ICS environments.

## About Nozomi Networks

Nozomi Networks is accelerating the pace of digital transformation by pioneering innovation for industrial cyber security and operational control. Leading the industry, we make it possible to tackle escalating cyber risks to operational networks. In a single solution, Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest critical infrastructure, energy, manufacturing, mining, transportation and other industrial sites around the world.



[www.nozominetworks.com](http://www.nozominetworks.com)

 [@nozominetworks](https://twitter.com/nozominetworks)

© 2019 Nozomi Networks, Inc.

All Rights Reserved.

DS-G-8.5x11-008