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.

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

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.

DATA SHEET
Guardian
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
**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.

**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

**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

**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.
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

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

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

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](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

**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

**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 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**

<table>
<thead>
<tr>
<th>Model</th>
<th>NSG-HS 3500</th>
<th>NSG-HS 3000</th>
<th>NSG-H 2500</th>
<th>NSG-H 2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. Protected Nodes</td>
<td>500,000</td>
<td>300,000</td>
<td>200,000</td>
<td>100,000</td>
</tr>
<tr>
<td>Max. Protected Network Elements¹</td>
<td>2,000,000</td>
<td>1,500,000</td>
<td>1,200,000</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Max. Protected Smart IoT Devices²</td>
<td>3,000,000</td>
<td>1,800,000</td>
<td>1,200,000</td>
<td>600,000</td>
</tr>
<tr>
<td>Max. Throughput³</td>
<td>6 Gbps</td>
<td>3 Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max. Remote Collectors⁴</td>
<td>50</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring Ports</td>
<td>Modular up to 16+1</td>
<td>Modular up to 8+1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Ports</td>
<td>1x1000Base-T</td>
<td>1x1000Base-T</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expansion Slots</td>
<td>4 slots available: 4x1000BaseT</td>
<td>4xSFP</td>
<td>4xSFP+</td>
<td>2 slots available: 4x1000BaseT</td>
</tr>
<tr>
<td>Storage</td>
<td>512 GB</td>
<td>512 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Form Factor</td>
<td>1 rack unit</td>
<td>1 rack unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max. Power Consumption</td>
<td>750 W</td>
<td>750 W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Supply</td>
<td>100-240V AC - 50/60Hz, 36-72V DC, Dual</td>
<td>100-240V AC - 50/60Hz, 36-72V DC, Dual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temperature Range</td>
<td>0 / +40º C</td>
<td>0 / +40º C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HxWxL (mm/in)</td>
<td>44 x 438 x 600 / 173 x 17.24 x 23.60</td>
<td>44 x 438 x 600 / 173 x 17.24 x 23.60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>18 Kg</td>
<td>17 Kg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certifications</td>
<td>CE, FCC, UL</td>
<td>CE, FCC, UL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ Network Elements: The sum of nodes, links, variables. ² Smart IoT Devices: The concept of “Smart IoT device" covers devices communicating in an intermittent way and resulting in low throughput. ³ All performance values are "up to" and vary depending on the analyzed traffic. ⁴ 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**

<table>
<thead>
<tr>
<th></th>
<th>NSG-M 1000</th>
<th>NSG-M 750</th>
<th>NSG-L 250</th>
<th>NSG-L 100</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max. Protected Nodes</strong></td>
<td>40,000</td>
<td>10,000</td>
<td>5,000</td>
<td>1,000</td>
</tr>
<tr>
<td><strong>Max. Protected Network Elements</strong>&lt;sup&gt;1&lt;/sup&gt;</td>
<td>600,000</td>
<td>200,000</td>
<td>90,000</td>
<td>20,000</td>
</tr>
<tr>
<td><strong>Max. Protected Smart IoT Devices</strong>&lt;sup&gt;2&lt;/sup&gt;</td>
<td>200,000</td>
<td>50,000</td>
<td>20,000</td>
<td>5,000</td>
</tr>
<tr>
<td><strong>Max. Throughput</strong>&lt;sup&gt;3&lt;/sup&gt;</td>
<td>1 Gbps</td>
<td></td>
<td>500 Mbps</td>
<td>250 Mbps</td>
</tr>
<tr>
<td><strong>Max. Remote Collectors</strong>&lt;sup&gt;4&lt;/sup&gt;</td>
<td></td>
<td></td>
<td>20</td>
<td></td>
</tr>
<tr>
<td><strong>Monitoring Ports</strong></td>
<td>7x1000BASE-T + 4xSFP</td>
<td></td>
<td>5x1000BASE-T</td>
<td></td>
</tr>
<tr>
<td><strong>Management Ports</strong></td>
<td>1x1000Base-T</td>
<td></td>
<td>1x1000Base-T</td>
<td></td>
</tr>
<tr>
<td><strong>Expansion Slots</strong></td>
<td>1 slot available: 4x1000Base-T</td>
<td>4xSFP</td>
<td>4xSFP</td>
<td>1 slot available: 4x1000Base-T</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>256 GB</td>
<td></td>
<td>64 GB</td>
<td></td>
</tr>
<tr>
<td><strong>Form Factor</strong></td>
<td>1 rack unit</td>
<td></td>
<td>1 rack unit</td>
<td></td>
</tr>
<tr>
<td><strong>Max. Power Consumption</strong></td>
<td>360W</td>
<td></td>
<td>250W</td>
<td></td>
</tr>
<tr>
<td><strong>Power Supply</strong></td>
<td>100-240V AC - 50/60 Hz, Single</td>
<td></td>
<td>100-240V AC - 50/60 Hz, Single</td>
<td></td>
</tr>
<tr>
<td><strong>Temperature Range</strong></td>
<td>0 / +45º C</td>
<td></td>
<td>0 / +45º C</td>
<td></td>
</tr>
<tr>
<td><strong>HxWxL (mm/in)</strong></td>
<td>44 x 429 x 438 / 1.73 x 16.89 x 17.24</td>
<td></td>
<td>44 x 438 x 300 / 17 x 17.2 x 11.8</td>
<td></td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>14 Kg</td>
<td></td>
<td>8 Kg</td>
<td></td>
</tr>
<tr>
<td><strong>Certifications</strong></td>
<td>CE, FCC, UL</td>
<td></td>
<td>CE, FCC, UL</td>
<td></td>
</tr>
</tbody>
</table>

<sup>1</sup> Network Elements: The sum of nodes, links, variables.
<sup>2</sup> Smart IoT Devices: The concept of “Smart IoT device” covers devices communicating in an intermittent way and resulting in low throughput.
<sup>3</sup> All performance values are “up to” and vary depending on the analyzed traffic.
<sup>4</sup> See Remote Collector tech specs for more details. For complete and current tech specs, visit [nozominetworks.com/techspecs](http://nozominetworks.com/techspecs), or contact us.
# Guardian Sensors

## Ruggedized Series

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

- **500 - 5,000 Nodes**
- **100 - 250 Mbps Max. Throughput**

<table>
<thead>
<tr>
<th></th>
<th>NG-500R</th>
<th>NSG-R 50</th>
<th>P550</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max. Protected Nodes</strong></td>
<td>5,000</td>
<td>500</td>
<td>2,500</td>
</tr>
<tr>
<td><strong>Max. Protected Network Elements</strong></td>
<td>80,000</td>
<td>10,000</td>
<td>50,000</td>
</tr>
<tr>
<td><strong>Max. Protected Smart IoT Devices</strong></td>
<td>30,000</td>
<td>2,500</td>
<td>12,500</td>
</tr>
<tr>
<td><strong>Max. Throughput</strong></td>
<td>800 Mbps</td>
<td>100 Mbps</td>
<td>200 Mbps</td>
</tr>
<tr>
<td><strong>Max. Remote Collectors</strong></td>
<td>30</td>
<td>10</td>
<td>Not available</td>
</tr>
<tr>
<td><strong>Monitoring Ports</strong></td>
<td>3x1000BASE-T</td>
<td>4x1000BASE-T</td>
<td>5x1000BASE-T</td>
</tr>
<tr>
<td><strong>Management Ports</strong></td>
<td>1x1000Base-T</td>
<td>1x1000Base-T</td>
<td>1x1000Base-T</td>
</tr>
<tr>
<td><strong>Expansion Slots</strong></td>
<td>2</td>
<td>Not available</td>
<td>Not available</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>256 GB (Redundant Data Partition)</td>
<td>64 GB</td>
<td>256 GB</td>
</tr>
<tr>
<td><strong>Form Factor</strong></td>
<td>3 rack unit</td>
<td>DIN mountable</td>
<td>Desktop with wall mount kit</td>
</tr>
<tr>
<td><strong>Max. Power Consumption</strong></td>
<td>115W</td>
<td>60W</td>
<td>38W</td>
</tr>
<tr>
<td><strong>Power Supply</strong></td>
<td>100-240V AC, 100-240V DC, Dual</td>
<td>100-240V AC, 12-36V DC, Single (External PSU)</td>
<td>90-240V AC, 12-30V DC, Single (External PSU)</td>
</tr>
<tr>
<td><strong>Temperature Range</strong></td>
<td>-40º C / +70º C (Max 40º C with SFP NIC)</td>
<td>-40 / +75º C</td>
<td>0 / +60º C</td>
</tr>
<tr>
<td><strong>HxWxL (mm/in)</strong></td>
<td>131.8x438x300.1</td>
<td>80 x 130 x 146</td>
<td>70 x 180 x 240</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>8.5 Kg / 18.74 Lb</td>
<td>3 Kg</td>
<td>2.5 Kg</td>
</tr>
<tr>
<td><strong>Certifications</strong></td>
<td>CE, FCC, UL</td>
<td>FCC</td>
<td>FCC</td>
</tr>
</tbody>
</table>

1 Network Elements: The sum of nodes, links, variables. 2 Smart IoT Devices: The concept of “Smart IoT device” covers devices communicating in an intermittent way and resulting in low throughput. 3 All performance values are “up to” and vary depending on the analyzed traffic. 4 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

<table>
<thead>
<tr>
<th></th>
<th>NRC-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. Throughput</td>
<td>Up to 15 Mbps</td>
</tr>
<tr>
<td>Remote Collector Support</td>
<td>Not available</td>
</tr>
<tr>
<td>Monitoring Ports</td>
<td>2x1000Base-T, 1xSFP</td>
</tr>
<tr>
<td>Management Ports</td>
<td>1x1000Base-T</td>
</tr>
<tr>
<td>Expansion Slots</td>
<td>Not available</td>
</tr>
<tr>
<td>Storage</td>
<td>8 GB</td>
</tr>
<tr>
<td>Form Factor</td>
<td>DIN mountable</td>
</tr>
<tr>
<td>Max. Power Consumption</td>
<td>12W</td>
</tr>
<tr>
<td>Power Supply</td>
<td>100-240VAC, 12-36V DC, Single (External PSU)</td>
</tr>
<tr>
<td>Temperature Range</td>
<td>-40 / +70º C</td>
</tr>
<tr>
<td>Heat Generation</td>
<td>55.44 BTU/hr</td>
</tr>
<tr>
<td>HxWxL (mm/in)</td>
<td>78 x 146 x 127 / 3.07 x 6.67 x 5.00</td>
</tr>
<tr>
<td>Weight</td>
<td>1.2 Kg</td>
</tr>
<tr>
<td>Compliance</td>
<td>RoHS</td>
</tr>
<tr>
<td>Certifications</td>
<td>CE, FCC, UL</td>
</tr>
</tbody>
</table>

Virtual Remote Collector

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. Throughput</td>
<td>15 Mbps</td>
</tr>
<tr>
<td>Deployment Options</td>
<td>Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th></th>
<th>V1000</th>
<th>V750</th>
<th>V250</th>
<th>V100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. Protected Nodes</td>
<td>40,000</td>
<td>10,000</td>
<td>5,000</td>
<td>1,000</td>
</tr>
<tr>
<td>Max. Protected Network Elements¹</td>
<td>400,000</td>
<td>200,000</td>
<td>100,000</td>
<td>20,000</td>
</tr>
<tr>
<td>Max. Protected Smart IoT Devices²</td>
<td>200,000</td>
<td>100,000</td>
<td>25,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Max. Throughput³</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Scenarios</td>
<td>Enterprise</td>
<td>Large</td>
<td>Medium</td>
<td>Small</td>
</tr>
<tr>
<td>Deployment Options</td>
<td>Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max. Remote Collectors⁴</td>
<td>50</td>
<td>50</td>
<td>20</td>
<td>20</td>
</tr>
</tbody>
</table>

¹ Network Elements: The sum of nodes, links, variables. ² Smart IoT Devices: The concept of “Smart IoT device” covers devices communicating in an intermittent way and resulting in low throughput. ³ Performance is dependent upon hardware configuration and resource allocation. ⁴ See Remote Collector tech specs for more details. For complete and current tech specs, visit: nozominetworks.com/techspecs, or contact us.

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**

<table>
<thead>
<tr>
<th></th>
<th>Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Offerings</td>
<td>Gatewatcher, Siemens RUGGEDCOM</td>
</tr>
<tr>
<td>Add-ons</td>
<td>Smart Polling module: included</td>
</tr>
<tr>
<td>Remote Collector Support</td>
<td>Not available</td>
</tr>
</tbody>
</table>

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 security response with unmatched threat detection 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

**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.

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.
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.