Real-time Cyber Security and Visibility for Industrial Control Networks
See and Secure Your Industrial Networks

Superior Operational Visibility
Accurately visualize your industrial networks and improve resilience with real-time asset inventory and network monitoring.

Best-in-Class ICS Threat Detection
Rapidly manage cyber threats and process risks with a solution that correlates multiple, advanced detection techniques.

Most Global Installations
Centrally monitor hundreds of facilities with a solution proven to scale across continents and integrate with IT/OT systems.

Nozomi Networks is the leader of industrial cyber security, delivering the best solution for real-time visibility to manage cyber risk and improve resilience.

With one solution, our customers gain:

- Advanced cyber security
- Improved operational reliability
- Easy IT/OT integration

Through the innovative use of artificial intelligence (AI), we help the largest industrial facilities around the world See and Secure™ their critical control networks.

Today Nozomi Networks supports over a quarter of a million devices in sectors such as:

- Critical Infrastructure
- Manufacturing
- Transportation
- Energy
- Mining
- Utilities

Let our advanced solution automate the hard work of inventorying, visualizing and monitoring your industrial control networks.

You benefit from the real-time visibility and threat detection needed to ensure high cyber resiliency and reliability.

#thosewhoknowpicknozomi
Leverage Our **Global Expertise**

- **1,000+** Installations Across 5 Continents
- **300,000+** Devices Supported
- **40+** System Integrators and VARs
- **100+** Trained and Certified Partners

**OUR OFFICES**

**Expert Staff**
Around the World

**FORTUNE 500 CUSTOMERS**

- **#1** Global Electric Utility
- **Top 3** Energy Companies
- **Major** Multinational Deployments

**FORTUNE 500**

**STRATEGIC PARTNERS**

- **accenture**
- **Atos**
- **cisco**
- **GE Power**
- **IBM Security**
- **...and more**
SCADAguardian™ protects your control networks from cyber attacks and operational disruptions.

It provides superior operational visibility and rapid detection of cyber threats plus process risks through passive network traffic analysis.

Nozomi Networks Solution Architecture - SCADAguardian Edition

The award winning Nozomi Networks solution improves cyber resiliency and reliability via a modular, extensible and scalable architecture.
Multiple Appliance Formats for Every Type of Deployment

- **Real-time Network Visualization**
  - Improves system awareness and understanding of network structure and activity
  - Displays key information such as traffic throughput and TCP connections

- **Flexible Navigation and Filtering**
  - Shows macro views + detailed information on endpoints and connections
  - Filters by subnets and network segments, or presents topologies

- **Quickly Detect Threats to Your ICS or SCADA System**
  - **Up-to-the-Minute Threat Detection**
    - Identifies cyber security and process reliability threats at all times
    - Detects attacks in process, early stage advanced threats and cyber risks
  - **Best-in-Class ICS Threat Detection**
    - Uses multiple, hybrid techniques for comprehensive risk detection
    - Ensures current monitoring when integrated with optional OT ThreatFeed™

### Physical Appliances

<table>
<thead>
<tr>
<th>Series</th>
<th>NSG-M</th>
<th>NSG-L</th>
<th>NSG-R</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>1000</td>
<td>250</td>
<td>150</td>
</tr>
<tr>
<td>Description</td>
<td>Rack-mounted appliances for large scenarios</td>
<td>Rack-mounted appliances for medium scenarios</td>
<td>Ruggedized appliances for medium or small scenarios</td>
</tr>
<tr>
<td>Monitoring Ports</td>
<td>7 RJ45 + 4 SFP</td>
<td>5 RJ45</td>
<td>7 RJ45</td>
</tr>
<tr>
<td>Max. Protected Nodes</td>
<td>10,000</td>
<td>750</td>
<td>500</td>
</tr>
</tbody>
</table>

### Virtual Appliances

<table>
<thead>
<tr>
<th>Model</th>
<th>V1000</th>
<th>V750</th>
<th>V250</th>
<th>V100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A powerful appliance for very large, demanding scenarios</td>
<td>A virtual appliance for medium scenarios</td>
<td>A virtual appliance for small scenarios</td>
<td></td>
</tr>
<tr>
<td>Monitoring Ports</td>
<td>Unlimited</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Max. Protected Nodes</td>
<td>10,000</td>
<td>2,500</td>
<td>750</td>
<td>300</td>
</tr>
</tbody>
</table>

A portable appliance, suitable for temporary scenarios, is also available. **Contact us** for more information. See [nozominetworks.com/techspecs](http://nozominetworks.com/techspecs) for current and complete appliance details.
SCADAguardian Advanced™ extends the significant value obtained with SCADAguardian, with the use of Smart Polling™. This precise, low volume, active technique provides a full asset inventory, exact vulnerability assessment and advanced ICS network monitoring.

Smart Polling safely identifies a full set of ICS data, improving asset inventory, vulnerability assessment and network monitoring.
Automatically Track Your Industrial Assets and Know Your Vulnerability Risks

- **Full Asset Inventory**
  - Provides a full set of asset inventory providing accurate deep details
  - Identifies firmware versions and their patch levels

- **Automated Vulnerability Assessment**
  - Identifies and confirms which vendors devices are vulnerable
  - Optimizes workflows with informative dashboards and drilldowns

**Compare SCADAguardian Advanced to SCADAguardian**

<table>
<thead>
<tr>
<th>Functionality</th>
<th>SCADAguardian Advanced</th>
<th>SCADAguardian</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Analysis</td>
<td>Passive + Active Smart Polling</td>
<td>Passive</td>
</tr>
<tr>
<td>Asset Inventory</td>
<td>Identifies All Assets</td>
<td>Identifies Communicating Assets</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>Confirms Vulnerabilities</td>
<td>Identifies Vulnerabilities</td>
</tr>
<tr>
<td>Network Monitoring &amp; Threat Detection</td>
<td>for All Assets &amp; ICS Data</td>
<td>for Communicating Assets &amp; ICS Data</td>
</tr>
<tr>
<td>Deployment</td>
<td>Assigned IP Address - Installed on Switch or Router Port - Routing for Selected IPs Enabled</td>
<td>No IP Address - Installed on SPAN or Mirror Ports - No Routing Required</td>
</tr>
</tbody>
</table>

**Multiple Appliance Formats for Every Type of Deployment**

**Physical Appliances**

<table>
<thead>
<tr>
<th>Series</th>
<th>NSG-M</th>
<th>NSG-L</th>
<th>NSG-R</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>1000A</td>
<td>250A</td>
<td>150A</td>
</tr>
<tr>
<td>Description</td>
<td>Rack-mounted appliances for large scenarios</td>
<td>Rack-mounted appliances for medium scenarios</td>
<td>Ruggedized appliances for medium or small scenarios</td>
</tr>
<tr>
<td>Monitoring Ports</td>
<td>7 RJ45 + 4 SFP</td>
<td>5 RJ45</td>
<td>7 RJ45</td>
</tr>
<tr>
<td>Max. Protected Nodes</td>
<td>10,000</td>
<td>750</td>
<td>500</td>
</tr>
</tbody>
</table>

**Virtual Appliances**

<table>
<thead>
<tr>
<th>Model</th>
<th>V1000A</th>
<th>V750</th>
<th>V250A</th>
<th>V100A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A powerful appliance for very large, demanding scenarios</td>
<td>A virtual appliance for large scenarios</td>
<td>A virtual appliance for medium scenarios</td>
<td>A virtual appliance for small scenarios</td>
</tr>
<tr>
<td>Monitoring Ports</td>
<td>Unlimited</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Max. Protected Nodes</td>
<td>5,000</td>
<td>1,000</td>
<td>500</td>
<td>200</td>
</tr>
</tbody>
</table>

**SCADAguardian Advanced Container Edition**

- **Description**
  - Embedded container application for switches, routers and other security infrastructure. Fast, flexible deployment option that leverages hardware units.

**Continuously Monitor Your Network and ICS**

- **Real-time Network Visualization**
  - Improves situational awareness and speeds troubleshooting
  - Shows macro views of the network plus detailed information

- **Advanced ICS Network Monitoring**
  - Monitors assets and network behavior for cyber security and reliability risks
  - Uses full ICS data to monitor for threats and anomalies
Central Management Console

Consolidated OT Cyber Security and Visibility
Across Distributed Industrial Sites

Easily manage cyber security for hundreds of distributed industrial installations with the **Central Management Console™ (CMC)**.

It provides consolidated and remote access to your ICS data from SCADAguardian and SCADAguardian Advanced appliances.

---

**Centralized Monitoring of Distributed Industrial Facilities**

**Aggregated Summaries / Details by Remote Site**

- Shows a geographic map of your SCADAguardian and SCADAguardian Advanced appliances, including risk level by site
- Enables a fast understanding of key metrics, such as alerts, incidents, vulnerabilities and more
- Supports drilldown on visual indicators for detailed information
- Displays dashboards, charts and queries relevant to your organization

---

**The Virtual, Multitenant CMC is Easy to Deploy and Scale**

<table>
<thead>
<tr>
<th>Summary</th>
<th>Consolidated and remote ICS cyber security and visibility for distributed industrial sites.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Specs</td>
<td>Amazon AWS AMI, Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+</td>
</tr>
<tr>
<td>Max. Managed Appliances</td>
<td>Unlimited (*)</td>
</tr>
</tbody>
</table>

(*) Based on infrastructure. See nozominetworks.com/techspecs for current and complete appliance details.
OT ThreatFeed

OT ThreatFeed is an optional subscription that delivers threat updates, making it easy for IT/OT teams to stay on top of current ICS risks.

Convenient OT ThreatFeed Service

☐ Timely Threat Updates
  • Provides indicators of known and emerging threats and vulnerabilities
  • Curates, tests and adapts ICS threat information from multiple sources, including threats and vulnerabilities discovered by Nozomi Networks

☐ Actionable Threat Remediation Insights
  • Decreases response time with Smart Incident™, which correlates alerts, provides operational context and delivers automatic packet captures

Easily Integrate / Share Information with IT/OT Environments

• Includes built-in integrations for asset management systems, firewalls, identity management systems, SIEMs and more
• Supports dozens of IT/OT protocols
• Extends further with Open API and Protocol SDK
• See website for current details

Central Management Console

Regularly Receive OT Threat and Vulnerability Updates

Quickly Identify New Risks to Your Industrial Systems

Rapidly Respond with Actionable Insights

Sample Deployment Map: Centrally Monitor and Secure Many Facilities

EXAMPLE
GLOBAL INSTALLATIONS

500+
Hydro-generation plants on five continents

420+
Gas distribution locations

300+
Electric distribution sites

OT ThreatFeed

Regional distributions: Canada, USA, Spain, Italy, China, Japan, Brazil, Argentina, Africa, Australia.
Nozomi Networks Solution
Sample Deployment Architecture

Shown above 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.
What to Look for in a Real-time ICS Visibility and Cyber Security Solution

While increasing cyber threats dominate the news, there is reason to be optimistic.

New technology, such as the Nozomi Networks solution, is easy and safe to deploy, dramatically improves OT cyber security and integrates seamlessly with IT infrastructure.

When considering such a solution, make sure it has the advantages shown here.

- Accurate OT Operational Visibility
- Advanced ICS Threat Detection
- Proven, Large-Scale Global Installations
- Swift Deployment Across Many Sites
- Global Partner Ecosystem
- Easy IT/OT Integration
- Extraordinary Customer Care

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?

For detailed information about our products, visit www.nozominetworks.com

#thosewhoknowpicknozomi