SOLUTION BRIEF

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.

THE LEADER OF INDUSTRIAL CYBER SECURITY
Nozomi Networks is accelerating the pace of digital transformation by pioneering innovation for industrial cyber security and operational control.

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

In a single solution, Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest critical infrastructure and industrial sites around the world.

Through the innovative use of artificial intelligence (AI), our solution automates the hard work of inventorying, visualizing and monitoring your industrial control networks.

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

ENGAGED WITH GLOBAL INDUSTRY LEADERS

Electric Utilities
Automotive Manufacturing
Oil & Gas
Pharmaceuticals
Mining
Chemicals
Food & Consumer Goods
Water/Wastewater
Leverage Our Global Expertise

1,400+
Installations Across 5 Continents

625,000+
Devices Supported

100+
System Integrators and VARs

250+
Trained and Certified Professionals

WORLDWIDE OFFICES

Australia, Brazil, Canada, Denmark, Germany, Italy, Mexico, Netherlands, Portugal, Singapore, Spain, Switzerland, United Arab Emirates, United Kingdom and the United States.

STRATEGIC PARTNERS

accenture
Atos
FireEye™
GE Power
IBM Security
Schneider Electric
NTT Security

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

It monitors network communications and behavior for risks that threaten the reliability of your systems, and provides the information you need to respond quickly.

The award winning Nozomi Networks solution improves cyber resiliency and reliability via a modular, extensible and scalable architecture.
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 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

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

Multiple Appliance Formats for Every Type of Deployment

<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>750</td>
<td>250</td>
</tr>
<tr>
<td></td>
<td>250</td>
<td>100</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td>150</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Image</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Rack-mounted appliances for real-time industrial network visibility, cyber security and monitoring</td>
<td>Rack-mounted appliances for real-time industrial network visibility, cyber security and monitoring</td>
<td>Ruggedized appliances for real-time industrial network visibility, cyber security and monitoring</td>
</tr>
<tr>
<td>Monitoring Ports</td>
<td>7 RJ45 + 4 SFP</td>
<td>7 RJ45 + 4 SFP</td>
<td>5 RJ45</td>
</tr>
<tr>
<td>Max. Protected Nodes</td>
<td>10,000</td>
<td>2,500</td>
<td>750</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
</tr>
<tr>
<td>V1000</td>
</tr>
<tr>
<td>V750</td>
</tr>
<tr>
<td>V250</td>
</tr>
<tr>
<td>V100</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>For enterprise scenarios</td>
</tr>
<tr>
<td>For large scenarios</td>
</tr>
<tr>
<td>For medium scenarios</td>
</tr>
<tr>
<td>For small scenarios</td>
</tr>
<tr>
<td>Max. Protected Nodes</td>
</tr>
<tr>
<td>10,000</td>
</tr>
<tr>
<td>2,500</td>
</tr>
<tr>
<td>750</td>
</tr>
<tr>
<td>300</td>
</tr>
<tr>
<td>300</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Embedded container appliance for switches, routers and other security infrastructure</td>
</tr>
<tr>
<td>Fast, flexible deployment option that leverages existing hardware units</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Container Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Low resource appliances that collect asset and network data in remote locations and send it to Guardian for further analysis</td>
</tr>
</tbody>
</table>

See nozominetworks.com/techspecs for current and complete appliance details.
PRODUCT

Central Management Console

Centralized OT Visibility and Cyber Security for Distributed Deployments

The Central Management Console™ (CMC) makes it easy to monitor and manage cyber security across distributed industrial sites. A single console provides consolidated access to data from all Guardian deployments in the field or on the plant floor.

Centralized Monitoring of Your Distributed Industrial Facilities

- **Aggregated Summaries Plus Details by Remote Site**
  - Shows a geographic map of Guardian 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

| Description                           | Virtual appliance for centralized management of multi-tier, distributed deployments  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregates</td>
<td>Aggregates all ICS assets, vulnerabilities, and alerts in a single console</td>
</tr>
<tr>
<td>Installation Specs</td>
<td>Amazon 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>
<tr>
<td>Storage</td>
<td>100+ GB</td>
</tr>
</tbody>
</table>

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

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 and data exchange
- ICS Data Enhancement
  - Export data for further analysis or presentation in other applications
- Current Details Available Online
  - See nozominetworks.com/techspecs

SECURITY SERVICE PROVIDER SOLUTION

Nozomi Networks Solution for MSS and MDR Service Providers

Nozomi Networks is the multitenant OT cyber security and visibility vendor of choice for MSS (Managed Security Service) and MDR (Managed Detection and Response) service providers.

We thoroughly understand industrial networks and processes and our solution is optimized for ICS.

Flexible Scalable Architecture
- Multitenant application designed for powering service offerings with shared infrastructure
- High Availability (HA) solution
- Flexible Deployment Options (Physical, Virtual and Container appliances)
- Easy-to-use OpenAPI

Confidently Use a Solution Designed Specifically for OT
Quickly Monitor ICS Networks and Processes with Real-time Insights
Rapidly Detect & Hunt Cyber Threats Using a Best-in-Class Solution
Efficiently Act on ICS Cyber Security Threats and Risks
Easily Provide Exceptional Forensics and Troubleshooting Services
**GUARDIAN ADD-ON MODULE**

**Smart Polling**

*Active Asset Discovery for Comprehensive Asset Details*

*Smart Polling™* extends Guardian’s built-in asset discovery functionality with active capabilities that deliver comprehensive and precise details about each asset in your network.

**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
- Uses a full set of ICS data for advanced anomaly detection
- Integrates with OT ThreatFeed for up-to-date threat detection

**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

---

**The Asset Visibility You Need for Cyber Resiliency**

*SANS 2019 State of OT/ICS Cybersecurity Survey:*

<table>
<thead>
<tr>
<th>Top Threat Concern</th>
<th>State of OT Asset Inventory</th>
<th>SANS’ Advice</th>
<th>Top Planned Security Technology Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices and “things” (that cannot protect themselves) added to network</td>
<td>Less than half of asset owners have inventoried their control systems devices</td>
<td>Establish an inventory of OT assets, maintain the OT/ICS asset inventory over time</td>
<td>OT/ICS network security monitoring and anomaly detection solutions</td>
</tr>
</tbody>
</table>
GUARDIAN ADD-ON SUBSCRIPTION

OT ThreatFeed
Detect Threats and Vulnerabilities with ICS Threat Intelligence

OT ThreatFeed™ delivers up-to-date industrial threat intelligence to the Nozomi Networks solution, making it easy to detect threats and vulnerabilities in your environment.

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
- Identifies assets with vulnerabilities and at risk of attack
- Provides valuable security and operational context regarding detected risks
- Generates real-time alerts about suspicious activity

Continuous Threat Research that Reduces OT Cyber Risk
- 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
- Reduces security management costs as a single, comprehensive ICS threat detection tool

Threat Intelligence You Can Rely On

OT ThreatFeed is produced and curated by Nozomi Networks Labs, a team of expert ICS security researchers.

Nozomi Networks customers received LockerGoga malware signatures within 48 hours of an attack on a major aluminum producer.

Hot Company for Threat Intelligence, Best Product for ICS/SCADA Security
Cyber Defense Magazine InfoSec Awards 2019
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.

Additionally, Remote Collectors™ can be added to Guardian appliances to capture data from remote and offsite locations.
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 choosing a cyber security solution and vendor for your organization, make sure they have the advantages shown here.

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

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?

- Guardian
- Central Management Console
- OT ThreatFeed

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

#thosewhoknowpicknozomi