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.

The CMC helps manage OT cyber risk across the enterprise with a scalable solution that is fast and simple to deploy.

**The CMC delivers:**

- Centralized visibility of all OT assets, vulnerabilities and alerts across the organization
- Superior operational visibility and ICS threat detection
- Easy drilldown to connected Guardian deployments for deeper analysis and investigation
- Centralized management of Nozomi Networks appliances and **OT ThreatFeed™** updates
- Seamless integration with security and IT tools

Find out how customers centralize ICS cyber security monitoring using the CMC, improving reliability, cyber resiliency and operational efficiency.

Contact us today at nozominetworks.com/contact

**Superior Visibility and Threat Detection**

- Actionable dashboards show key cyber security and process threats
- Real-time network visualization improves situational awareness
- Best-in-class OT threat detection and advanced correlation provide rapid insights
- OT ThreatFeed subscription ensures rapid detection of emerging risks

**Scalable, Flexible Architecture**

- Readily scales to numerous industrial facilities with optimal performance
- Flexible ICS data consolidation using multi-tier aggregations

**Extensive Global Installations**

- Centralized OT visibility and cyber security for multinational deployments
- Fast deployments with immediate ROI
- Easy integration with IT and security infrastructure
- Common platform to drive IT/OT convergence
Superior ICS Network and Operational Visibility

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

Immediately Visualize Your Industrial Networks

- Real-time Network Visualization
  - Improves system awareness and understanding of industrial networks, including their structures and activities
  - 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 of multiple sites, individual sites and detailed information on endpoints and connections
  - Filters by subnets, networks segments and topologies

Consolidated, Comprehensive OT Threat Monitoring

- Up-to-the-Minute Threat and Vulnerability Detection
  - Aggregates cyber security and process reliability threats in real-time, reducing the mean time to detection (MTTD)
  - Reports attacks in process, early stage advanced threats and cyber risks
  - Consolidates vulnerability assessment across sites

- Best-in-Class ICS Threat Detection
  - Delivers comprehensive risk monitoring using advanced threat detection
  - Ensures current detection when integrated with OT ThreatFeed subscription
Immediate Value Delivered to Multinational Organizations

Reduce Troubleshooting and Forensic Efforts

- **Effective, Efficient Incident Response**
  - Decreases the mean time to respond (MTTR) using Smart Incident™, which groups related alerts and provides context about the threat lifecycle
- **Informative Forensics**
  - Provides answers fast with a powerful ad hoc query tool

 Quickly Achieve a Fast ROI with Our Easy-to-Deploy Solution

- **Swift Deployment**
  - Installs as a proven, plug-and-play, ISO 9001: 2015 certified product
  - Rolls out across multiple sites in weeks
- **Immediately Valuable**
  - Improves ICS visibility, cyber security and reliability
  - Reduces cyber security workforce requirements
  - Increases productivity and IT/OT collaboration

Virtual Appliance is Easy to Deploy and Scalable

<table>
<thead>
<tr>
<th>Description</th>
<th>Virtual appliance for centralized management of multi-tier, distributed deployments. Aggregates all ICS assets, vulnerabilities, and alerts in a single console.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Options</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. Visit [nozominetworks.com/techspecs](http://nozominetworks.com/techspecs) for the latest technical specifications.
Sample Deployment Map: Centrally Monitor and Secure Many Facilities

A single installation of the CMC can monitor, manage and remediate threats for numerous industrial facilities.

High Performance and Scalability for Multinational Deployments

- **Centralized Monitoring of OT Risks**
  - Consolidates information for hundreds of sites and thousands of devices
  - Leverages centralized cyber security expertise

- **Enterprise Ready**
  - Scales for enterprisewide deployment with optimum performance
  - Adapts to all sites, with multiple appliance models and flexible deployment options

- **High Availability, High Security**
  - Ensures continuous OT monitoring with high availability or multitenant CMC configurations
  - Connects with field appliances using encrypted, bandwidth optimized data transfers

**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

- **Complete Details Available Online**
  - See nozominetworks.com/techspecs
Sample Deployment Architecture: Flexibly Consolidate ICS Data

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.
Nozomi Networks **Solution Architecture**

---

**Central Management Console**

**Guardian**
- Asset Discovery and Network Visualization
- Vulnerability Assessment
- ICS Risk Monitoring
- Threat and Anomaly Detection
- Dashboards and Reporting

**Ot ThreatFeed**
- Subscription

**Smart Polling**
- Optional

**Integrations**
- OpenAPI
- SOC/IT Integrations
- Protocol SDK

---

**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