Central Management Console

Centralized OT and IoT Security and Visibility for Distributed Sites

Nozomi Networks' Central Management Console™ (CMC) delivers centralized OT and IoT security management—no matter how large or distributed your business is.

Whether you're consolidating visibility and risk management at the edge or in the cloud, the CMC is fast and simple to deploy.

See
What's on your networks and how they're behaving

Detect
Cyber threats, risks and anomalies for faster response

Unify
Security, visibility and monitoring across all your assets
Consolidate
Unified OT, IoT and IT Security

Centrally Monitor
Your Distributed Sites

- Single Console Access from the Cloud or at the Edge
  - Delivers aggregated summaries with drilldown to detailed information by site
  - Answers questions fast with powerful queries about any and all OT/IoT data
  - Deploys in the cloud (AWS or Azure), or at the edge, for anytime, anywhere access

Easily Streamlines
SOC/IT Workflows

- Unified Security Monitoring
  - Integrates quickly with asset, ticketing and identity management systems, and SIEMs
  - Streamlines security processes across IT/OT and harmonizes security data
    nozominetworks.com/integrations

- Enterprise OT/IoT Risk Monitoring
  - Maps your Guardian appliances and shows risk level by site
  - Delivers fast insight into key metrics, alerts, incidents, vulnerabilities and more
  - Manages Nozomi Networks appliances and services

Enterprise-level Best Practices

- Leverages enterprise single sign-on (SSO) credentials for fast access to OT and IoT information
- Provides deep role-based access control (RBAC) “least privilege” permission options for maximum security

The CMC showing a geographic map of your Guardian appliances.
Visualization: Enterprise-wide Visibility

**Instantly See Your Networks**
- Real-time Network Visualization
  - Delivers instant awareness of OT/IoT networks and their activity patterns
  - Captures key data such as traffic throughput, TCP connections, protocols used between zones and more
  - Accelerates incident response and troubleshooting efforts

**Quickly Know Your Assets and Their Risks**
- Summarized Asset Information
  - Aggregates asset inventories that are automatically generated by Guardian at each site
  - Provides key information such as:
    - OT asset inventory
    - IoT asset inventory
    - Vulnerabilities by asset type, vendor or location

**Flexible Navigation and Filtering**
- Shows macro views of multiple sites, individual sites and detailed information on nodes and connections
- Filters by subnet, type, role, zone and topology
- Groups assets visually, in lists and detailed single asset views

**Drilldown to Individual Assets**
- Enables access to local Guardian appliances and individual asset details, such as:
  - Operating system
  - MAC vendor
  - MAC address
  - Installed software
  - Vulnerabilities
  - Captured URLs/files
  - IP
  - Subnet
  - Zone
  - Role
  - Alerts

Portion of interactive Network Visualization Graph.
Data Sheet for Central Management Console

**Rapidly Respond to OT and IoT Risks**

- **Detect and Disrupt Emerging Threats**
  Aggregates cybersecurity and process reliability threats
  Reports attacks in process, reducing the mean-time-to-detection (MTTD)
  Consolidates vulnerability assessment across sites

- **Unified OT and IoT Threat Detection**
  Combines behavior-based anomaly detection with signature-based threat detection for complete coverage
  Integrates quickly with ticketing systems and SIEMs for streamlined security processes

**Optimize Troubleshooting and Forensic Efforts**

- **Powerful Tools for Fast Analysis**
  Decodes incidents with Time Machine™ before and after system snapshots
  Provides fast answers with a powerful ad hoc query tool

- **Smart Incidents Speed Up Forensics**
  Decreases response time with Smart Incidents™ that:
  - Correlate and consolidate alerts
  - Provide operational and security context
  - Supply automatic packet captures

---

**Smart Incident** showing related alerts and security context.
Scale
Unified Security for Thousands of Distributed Sites

Attain High Performance for Multinational Deployments

Centralized Monitoring of OT Risks
Consolidates information for thousands of sites and devices
Quickly scales for enterprise-wide deployment with optimum performance
Adapts to all sites, with multiple appliance models and flexible deployment options

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

Realize Rapid Time to Value

Swift Deployment
Installs as a proven, plug-and-play, ISO 9001: 2015 certified product
Deploys in the cloud on AWS or Azure, and at the edge on virtual and physical appliances
Rolls out to numerous of sites within weeks

Immediately Valuable
Improves visibility, cybersecurity and reliability
Integrates with existing tools and workflows for fast adoption and high productivity
Accelerates IT/OT collaboration

Sample Deployment Map - Centrally Monitor and Secure Many Facilities
Flexible Deployment and Licensing

You can deploy the Nozomi Networks solution in a wide variety of mixed environments for rapid asset discovery, network visualization and accelerated security.

Industrial Strength OT and IoT Security and Visibility

Multiple Licensing Options

Nozomi Networks offers a range of licensing options to fit your organization’s preferences, including:

- Subscription licenses
- Enterprise license agreements (ELAs)
- Perpetual licenses

Please contact your Nozomi Networks Sales Director for more information.
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 appliances, and integrations with other systems.

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
- **SI/VAR relationships** with 200+ prominent organizations around the world

Visit nozominetworks.com/partners for more information.
CMC Appliances
in the Cloud or at the Edge

Cloud or Virtual

Virtual appliance for centralized management of multi-tier, distributed deployments.

Unlimited Max. Managed Appliances*

<table>
<thead>
<tr>
<th>Deployment Options - Cloud</th>
<th>Amazon AWS and Microsoft Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Options - Virtual</td>
<td>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 the infrastructure

NCMC-100 Series

Rack-mounted appliance for centralized management of multi-tier, distributed deployments.

50 Max. Managed Appliances

<table>
<thead>
<tr>
<th>Max. Managed Appliances</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. Throughput</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Management Ports</td>
<td>5x1000BASE-T</td>
</tr>
<tr>
<td>Expansion Slots</td>
<td>Not available</td>
</tr>
<tr>
<td>Storage</td>
<td>256 Gb</td>
</tr>
<tr>
<td>Form Factor</td>
<td>1 Rack Unit</td>
</tr>
<tr>
<td>Max. Power Consumption</td>
<td>360W</td>
</tr>
<tr>
<td>Power Supply Type</td>
<td>100-240V AC - 50/60 Hz</td>
</tr>
<tr>
<td>Temperature Range</td>
<td>0 / +45 °C</td>
</tr>
<tr>
<td>HxWxL (mm/in)</td>
<td>44 x 429 x 438 / 1.73 x 16.89 x 17.24</td>
</tr>
<tr>
<td>Weight</td>
<td>14 kg</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
PRODUCT

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 solution. Guardian accelerates security and simplifies IT/OT convergence.

SERVICE

Threat Intelligence
The Threat Intelligence subscription delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of the dynamic threat landscape, and reduce your mean-time-to-detection (MTTD).

SERVICE

Asset Intelligence
The Asset Intelligence subscription delivers ongoing OT and IoT asset intelligence for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-response (MTTR).

GUARDIAN ADD-ON

Smart Polling
Smart Polling adds low-volume active polling to Guardian’s passive asset discovery for enhanced asset tracking, vulnerability assessment and security monitoring.

GUARDIAN ADD-ON

Remote Collectors
Remote Collectors capture data in remote, distributed locations and send it to Guardian for analysis, improving visibility while reducing deployment costs.

PRODUCT

Central Management Console
The Central Management Console (CMC) consolidates OT and IoT risk monitoring and visibility across many distributed sites, at the edge or in the cloud. It integrates with IT security infrastructure for streamlined workflows and faster response to threats and anomalies.
Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.