DATA SHEET

Central Management Console

Centralized OT and IoT Security and Visibility for Distributed Sites

Nozomi Networks **Central Management Console™** (CMC) appliances deliver centralized edge or public cloud-based monitoring of Guardian sensors–no matter how 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.

CONSOLIDATE

RESPOND

SCALE

VISUALIZE
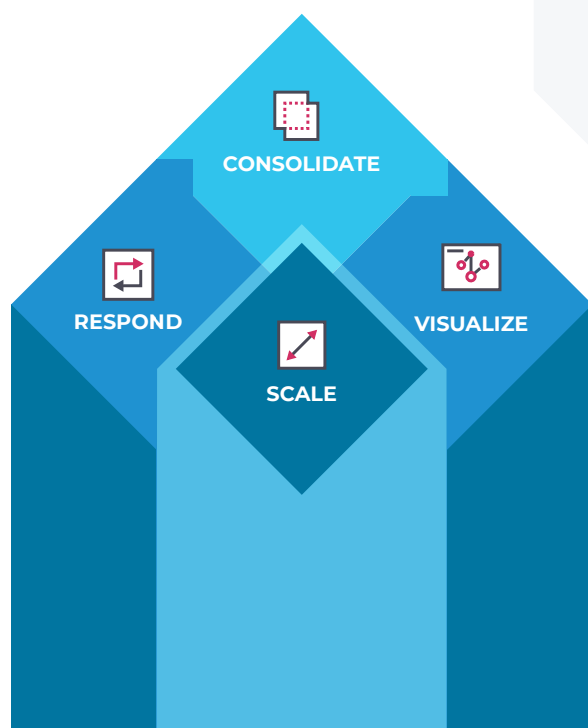
See

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

Consolidate
Unified OT, IoT and IT Security

Centrally Monitor Your Distributed Sites

Single Console Access from the Public 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

Enterprise OT/IoT Risk Monitoring

Maps your **Guardian™** sensors and shows risk level by site

Delivers fast insight into key metrics, alerts, incidents, vulnerabilities and more

Manages Nozomi Networks sensors and services

Easily Streamline SOC/IT Workflows

Unified Security Monitoring

Integrates quickly with asset, ticketing & identity management systems, and SIEMs

Streamlines security processes across IT/OT and harmonizes security data

nozominetworks.com/integrations

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
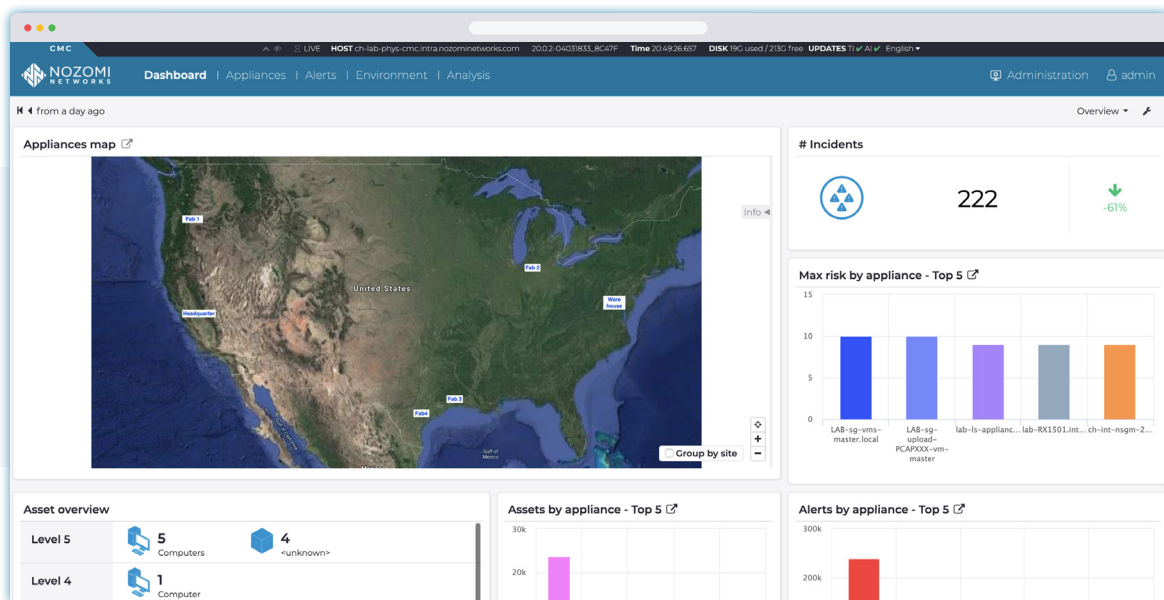
The **CMC** showing a geographic map of your Guardian sensors.

Visualize

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

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

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

Drilldown to Individual Assets

Enables access to local Guardian sensors and individual asset details, such as:

- Operating system
- MAC vendor
- MAC address
- Installed software
- Vulnerabilities
- Captured URLs/files

- IP
- Subnet
- Zone
- Role
- Alerts
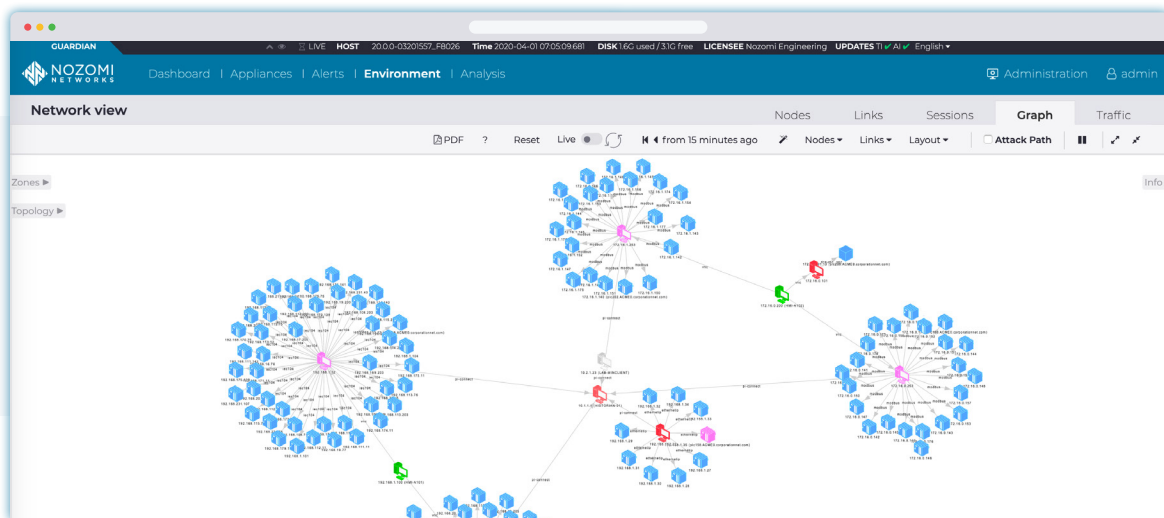
Portion of interactive **Network Visualization Graph**.

Respond

Time-saving Threat Summaries and Forensic Tools

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 Forensicss

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.
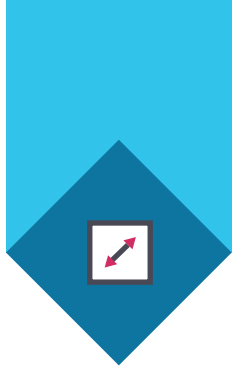
Scale

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 assets

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 sensors 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

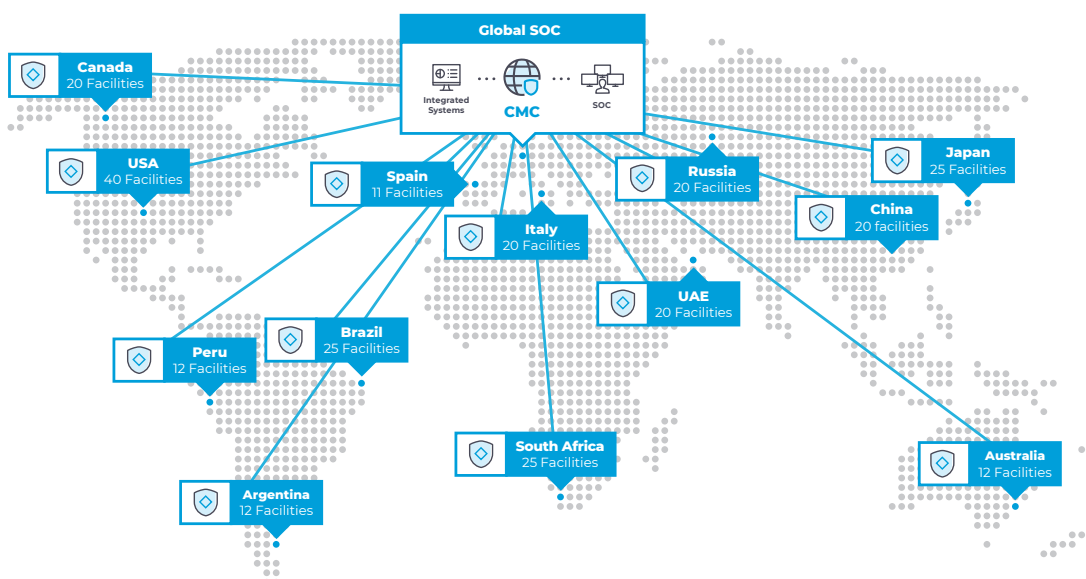Deploys in the cloud on AWS or Azure, and at the edge on virtual and physical appliances

Rolls out to numerous 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 for centrally monitoring and securing many facilities.

OT and IoT
Security and Visibility

Industrial Strength Cyber and Operational Resiliency

You can deploy the CMC and Guardian Sensors in a wide variety of mixed environments for rapid asset discovery, network visualization and accelerated security.
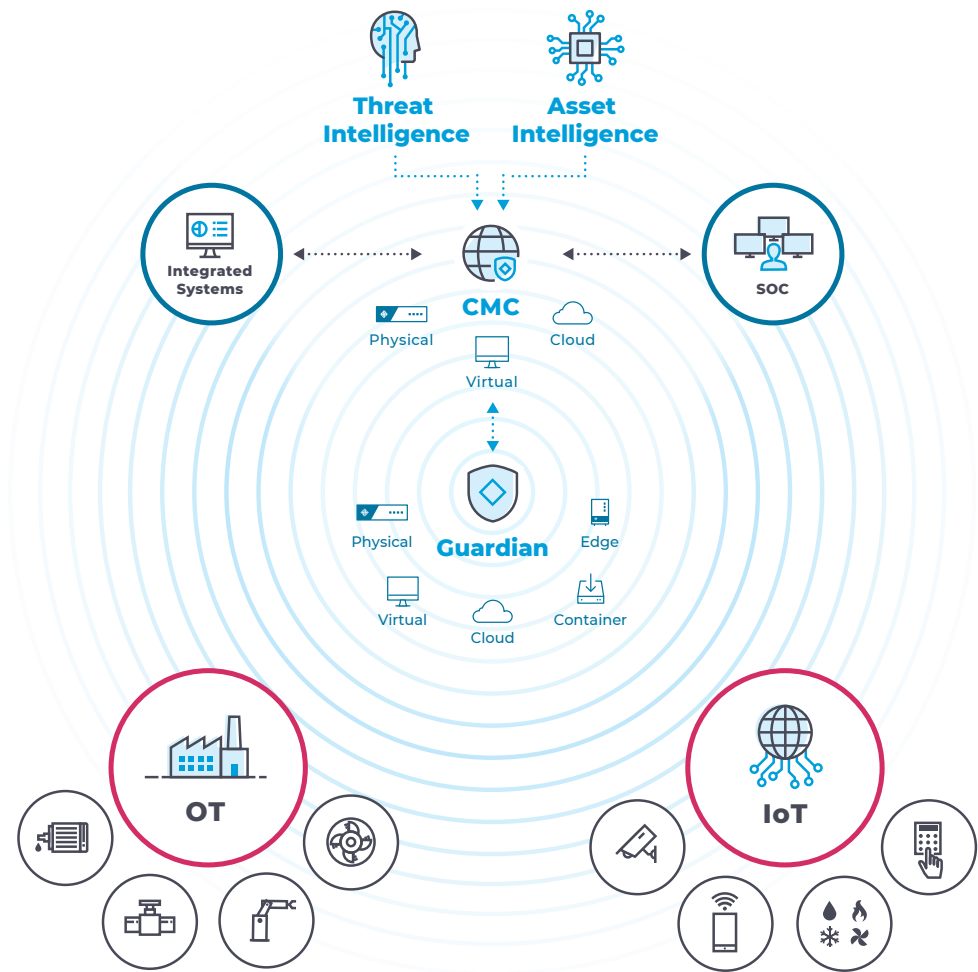
Respond to Incidents Faster

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 and integrations with other systems.
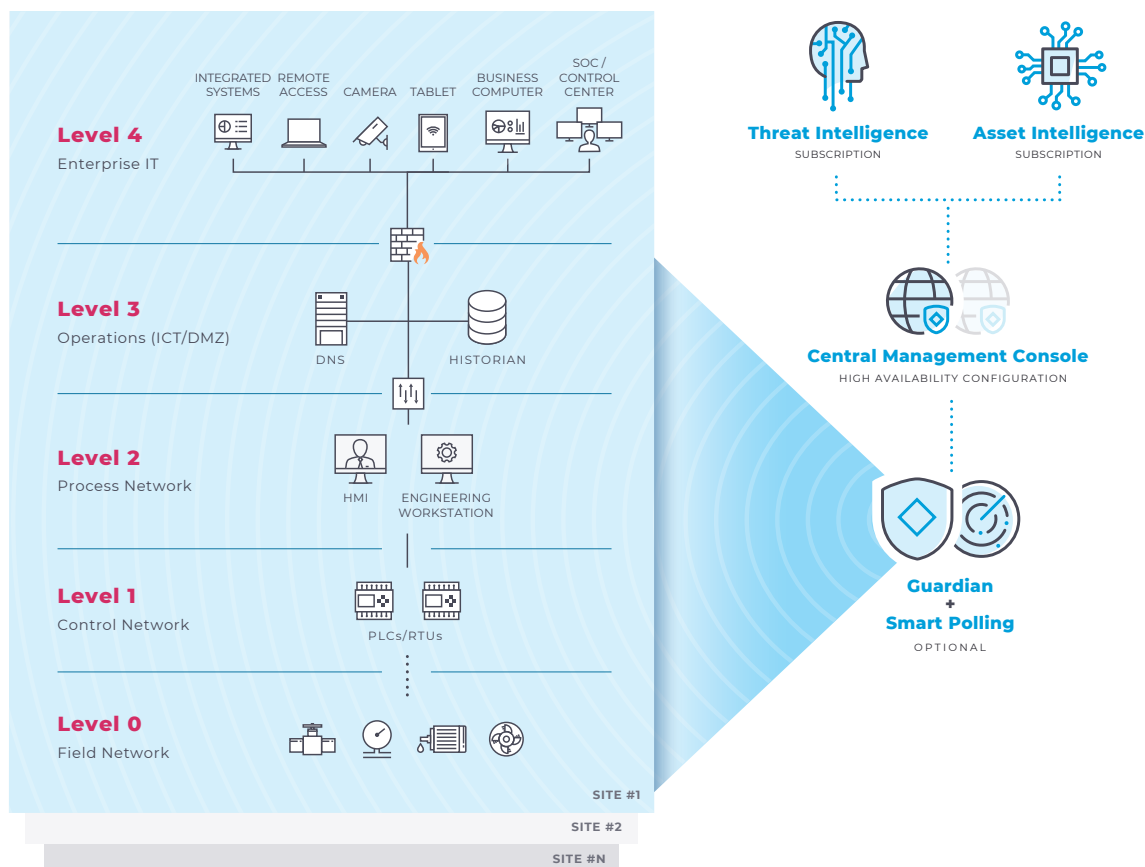
World Class Partners

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** for more information.

CMC Appliances
in the Public Cloud or at the Edge

Cloud or Virtual

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

◆ **400 Max. Managed Guardian Sensors**

	Virtual Central Management Console
Deployment Options - Cloud	Amazon AWS and Microsoft Azure
Deployment Options - Virtual	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+
Max. Managed Sensors[1]	400[1]
Max. Protected Network Elements[2]	2,000,000[1]
Storage	100+ GB

[1] Depending on the existing virtual infrastructure and deployment architecture. [2] Network Elements: The sum of nodes, links, variables. For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

NCMC-100 Series

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

◆ **50 Max. Managed Guardian Sensors**

	NCMC-100
Max. Managed Sensors[1]	50[1]
Max. Protected Network Elements[2]	600,000[1]
Max. Throughput	1 Gbps
Management Ports	4x1000BASE-T
Expansion Slots	Not available
Storage	256 GB
Form Factor	1 rack unit
Max. Power Consumption	360W
Power Supply	100-240V AC - 50/60 Hz, Single
Temperature Range	0 / +45 °C
HxWxL (mm/in)	44 x 429 x 438 / 1.73 x 16.89 x 17.24
Weight	14 kg

[1] Depending on the existing deployment architecture. [2] Network Elements: The sum of nodes, links, variables. 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
Smart Polling

Smart Polling adds low-volume active polling to Guardian's passive asset discovery, enhancing your asset tracking, vulnerability assessment and security monitoring.

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.

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.

nozominetworks.com