NOZOMI NETWORKS

PRODUCT OVERVIEW

Vantage

SaaS-Powered Security and Visibility of OT and IoT Networks

Nozomi Networks **Vantage™** leverages the power and simplicity of software as a service (SaaS) to deliver unmatched security and visibility across your OT, IoT, and IT networks.

Vantage accelerates digital transformation for the largest and most complex distributed networks.

You can protect any number of OT, IoT, IT, edge and cloud assets, anywhere.

Its scalable SaaS platform enables you to consolidate all of your security management into a single application, even as your networks quickly evolve.

Vantage delivers the immediate awareness of cyber threats, risks, and anomalies you need to detect and respond quickly and ensure cyber resilience.
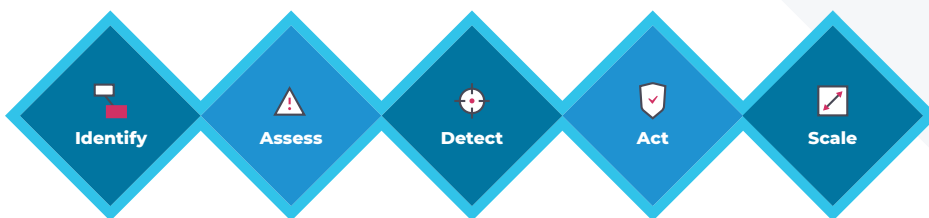
Identify   **Assess**   **Detect**   **Act**   **Scale**

See

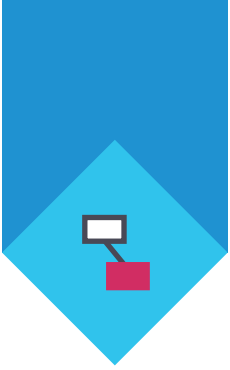All OT and IoT assets and behavior on your networks for unmatched awareness

Detect

Cyber threats, vulnerabilities, risks and anomalies for faster response

Unify

Security, visibility and monitoring across all your assets for improved resilience

Identify

Asset Discovery and Network Visualization

Automatically Track Your OT and IoT Assets

Up-to-Date Asset Inventory

Eliminates blind spots and increases awareness with automated asset inventory

Intuitive Dashboards

Generates macro views as well as detailed information on assets and connections
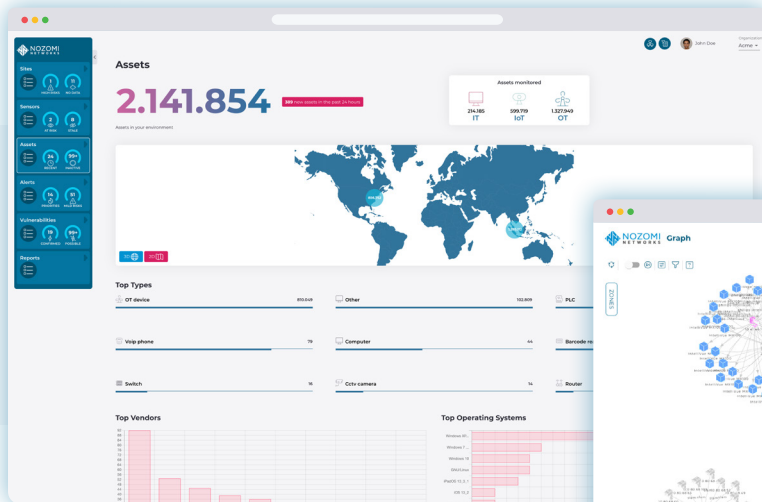
Immediately Understand Your Networks

Identifies All Communicating Devices

Provides extensive node information including name, type, and firmware version

Reduced Risk Through Network Visualization

Delivers detailed insight into your OT/IoT networks including asset behavior, roles, protocols, and data flows

Vantage Assets View summarizes all asset activity on your network for rapid assessment.
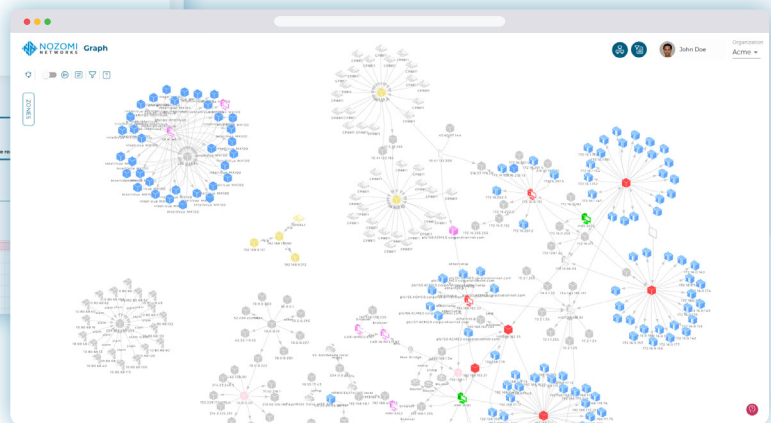
Network Visualization View displays all assets communicating on your network for real-time awareness.

Assess

Vulnerability Assessment and Risk Monitoring

Rapidly Identify Your Vulnerability Risks

Automated Vulnerability Assessment

Presents risk information including security alerts, missing patches and vulnerabilities

Correlates known vulnerabilities to Common Vulnerabilities Exposure (CVE) reports to quickly research root cause and potential impact

Efficient Prioritization and Remediation

Speeds response with vulnerability dashboards and drilldown capability

Prioritizes remediation by focusing efforts on high-impact risk reduction

Continuously Monitor Your Networks and Automation Systems

Continuous Monitoring

Continuous monitoring of all supported protocols: OT, IoT and IT

No critical blind spots in protection caused by limited monitoring or inadequate protocol support
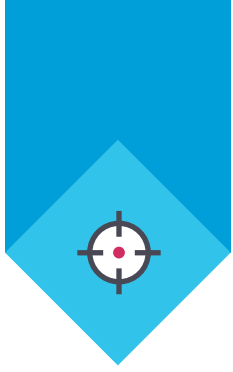
Easy Access to OT/IoT Risk Data

Summarizes OT and IoT risk information and highlights indicators of reliability issues, such as unusual process values

Supports drilldown on visual indicators for more detailed information
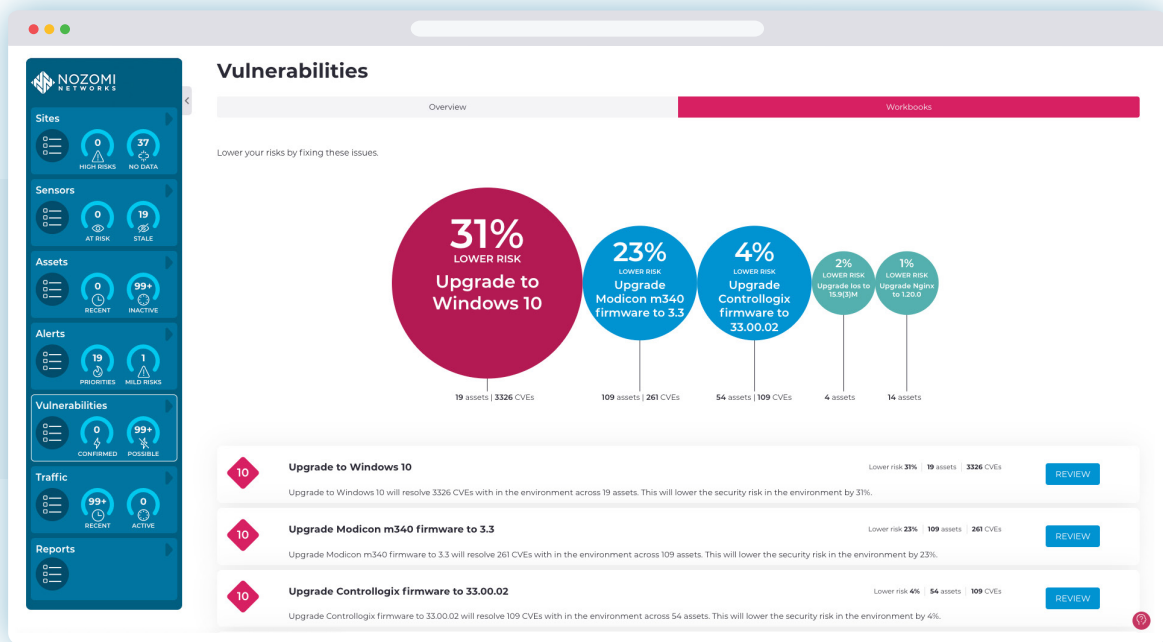
Vantage Workbooks show which vulnerabilities create the highest risk exposure and how to prioritize efforts for the greatest impact.

Detect

Advanced Anomaly and Threat Detection

Quickly Detect and Disrupt Threats and Anomalous Behavior

Constantly Updated Threat Detection

Identifies cybersecurity and process reliability threats

Detects early stage and late stage advanced threats and cyber risks

Superior OT and IoT Threat Detection

Combines behavior-based anomaly detection with signature-based threat detection for comprehensive risk monitoring

Effectively Monitor Mixed Environments

SUBSCRIPTION
Threat Intelligence

Ensures up-to-date threat detection and vulnerability identification using indicators created and curated by Nozomi Networks Labs

SUBSCRIPTION
Asset Intelligence

Powers breakthrough anomaly detection accuracy for OT and IoT devices, accelerating incident response

Breakthrough Anomaly Detection for OT and IoT

Rapid Identification of Assets

▼

Ensures Precise Asset Inventory

Accurate Anomaly Alerts

▼

Accelerates Incident Response

Asset Intelligence for Dynamic Networks

▼

Sustains Accurate Inventory & Detection

Act

Accelerated Global Incident Response

Significantly Improve OT and IoT Risk Management

User-Centric Design Accelerates Response

Focuses attention on critical vulnerabilities and prioritizes activities that can maximize risk reduction

Improves response time and productivity with pre-defined playbooks that guide remediation efforts for specific teams against each type of threat

Detailed Alerts Provide Global Perspective

Consolidates data to create accurate high-priority alerts across a global network in a centralized dashboard

Greatly Reduce Time-Consuming Research

### Clear Explanation of Incidents

Describes what happened, possible causes and suggested solutions for every alert, reducing the need for additional investigation

Automatic Consolidation of Alerts

Groups alerts into incidents, providing security and operations staff with a simple, clear, consolidated view of what's happening on your networks
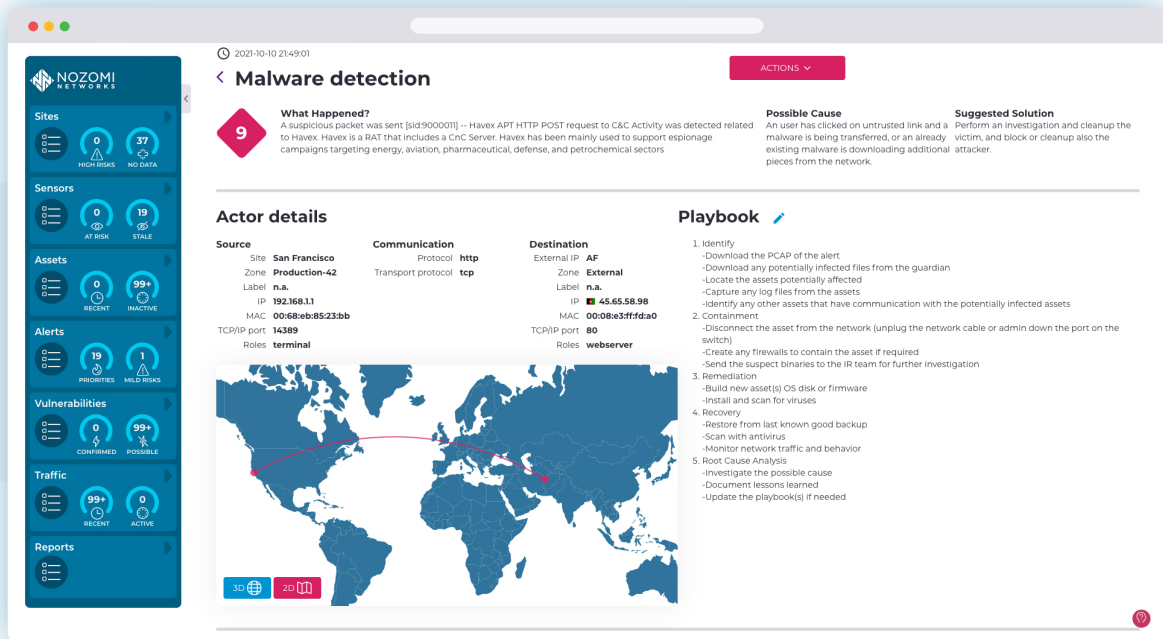
Vantage Alerts and **Playbooks** script guided remediation efforts to accelerate response.
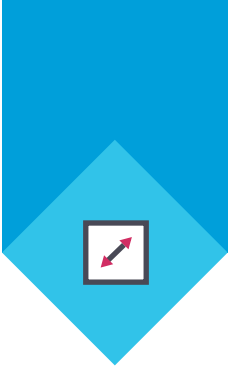
Scale

Unified Security for All of Your Sites with the Power of SaaS

Readily Scale with Optimal Performance

Exceptional Global Visibility

Aggregates data from any number of Guardian sensors, deployed anywhere

Delivers customizable summaries of essential information with drill-down to individual sites or assets

Consolidated Monitoring of All Facilities

Enables centralized security risk management for all sites

Provides visibility into all OT/IoT environments

Easily Integrate with SOC/IT Environments

Integrated Security Infrastructure

Streamlines security processes across IT/OT for cohesive response

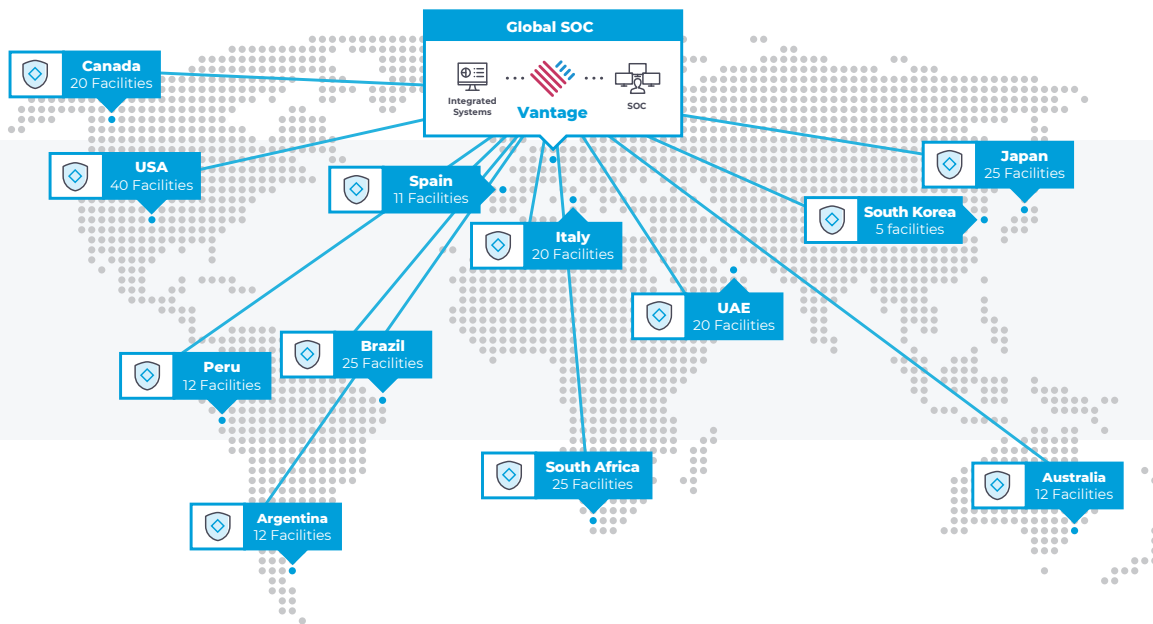Includes built-in integrations for asset, ticket and identity management systems, as well as SIEMs

nozominetworks.com/integrations

Broad Protocol Support

Supports hundreds of OT, IoT and IT protocols

Includes Protocol SDK and on-demand engineering services for new protocol support

nozominetworks.com/integrations

Global SOC

Integrated Systems | **Vantage** | SOC

Canada — 20 Facilities

USA — 40 Facilities

Spain — 11 Facilities

Japan — 25 Facilities

South Korea — 5 facilities

Italy — 20 Facilities

UAE — 20 Facilities

Peru — 12 Facilities

Brazil — 25 Facilities

South Africa — 25 Facilities

Australia — 12 Facilities

Argentina — 12 Facilities

Vantage protects any size network.

OT and IoT Security and Visibility

Industrial Strength Cyber and Operational Resilience

Vantage's scalable SaaS platform protects any number of OT, IoT, IT, edge, and cloud assets, anywhere.

Every Vantage license includes an unlimited number of Guardian virtual sensor licenses, enabling you to deploy Guardian sensors wherever you want to increase your visibility and security.
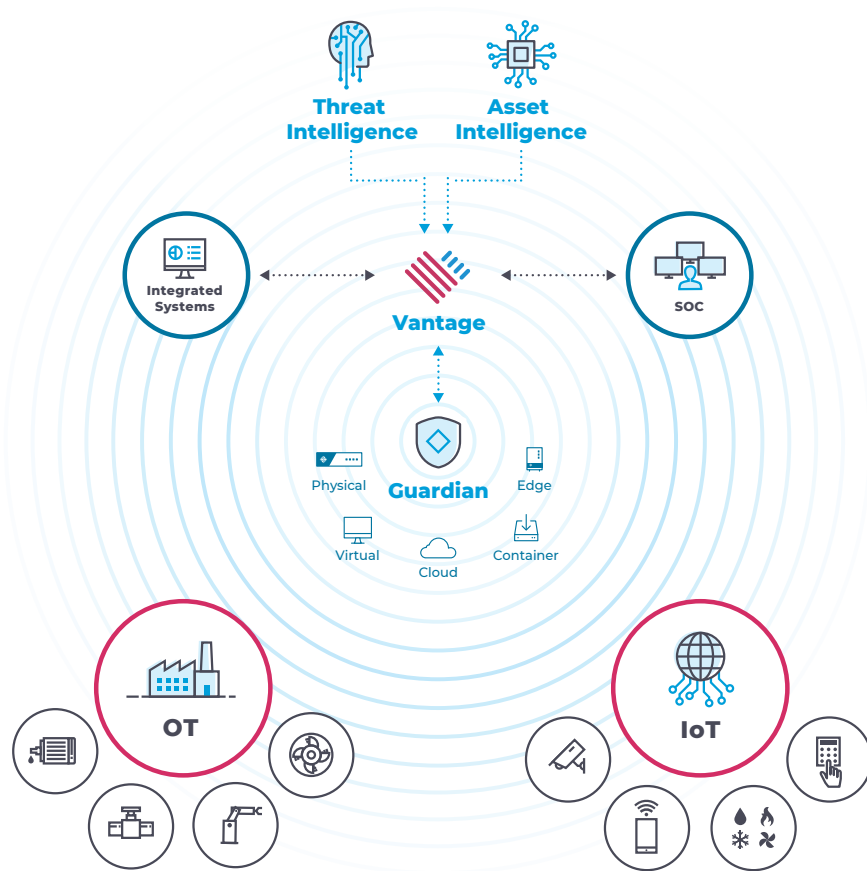
Respond to Incidents Faster

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 needed to understand and respond to threats before data theft or operational disruptions occur. Remediation efforts are prioritized by the highest impact vulnerabilities and risk exposure, and pre-defined playbooks can script remediation efforts to accelerate incident response.

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.
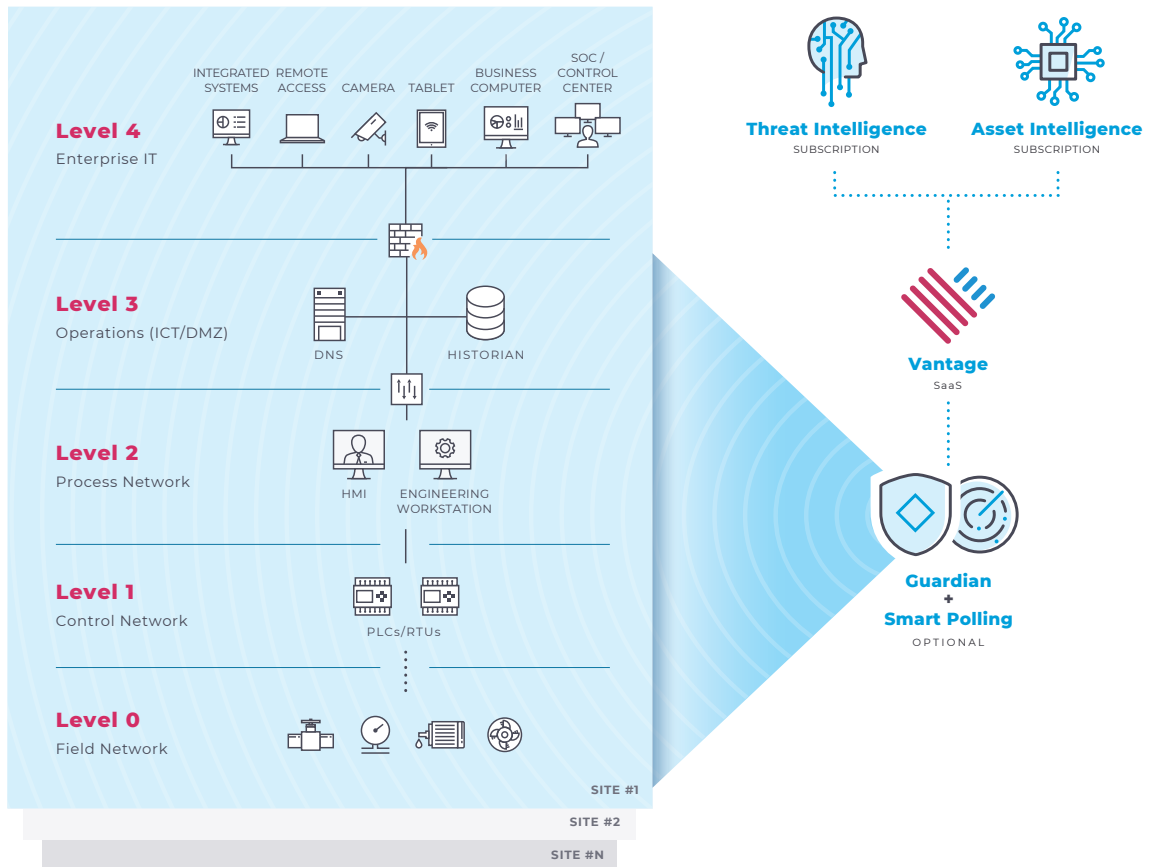
World Class Partners

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.

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