OVERVIEW

Nozomi Networks Platform

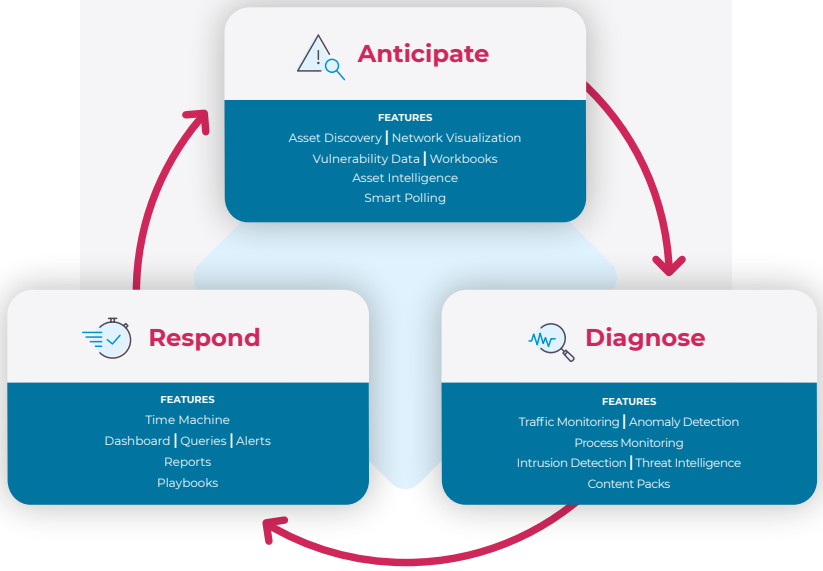
Cybersecurity and Analytics for Industrial Control, OT and IoT Networks

As network connectivity and automation proliferate for our online processes, security concerns have skyrocketed. For many, risk management and maintaining operational efficiency begin with vulnerability assessments and threat detection.

Deep, intelligent analysis of vulnerabilities, network anomalies, active threats and industrial process issues all lead to reduced security risk, process optimization and improvements, and rapid remediation for the complex OT/IoT landscape. Nozomi Networks is your partner for OT and IoT visibility and cybersecurity solutions for a wide variety of industrial processes and critical infrastructure industries.

The Nozomi Networks platform methodology revolves around the process analysis steps of Anticipate, Diagnose and Respond.

Our platform provides key features to support typical administrative, security and networking tasks for each of the process steps as described below.



Anticipate

Unparalleled OT and IoT visibility helps you foresee potential security and reliability threats long before they impact operations.

The first phase of cybersecurity maturity is understanding what is on your network and anticipating where risks may arise.

Nozomi Networks provides visibility to all your endpoints with deep data collection that can expose vulnerabilities and highlight where to focus risk management efforts. Visualize your device connections and traffic patterns to facilitate research and compliance efforts. Anticipate security threats before they impact your operations, while reducing risk and compliance efforts.

Network view provides an interactive vizualization of your network.

Key Platform Features

Passive Asset Discovery

Asset discovery in OT and IoT environments can be completely passive based on observing mirrored traffic to not disrupt critical processes, trigger alarms, or generate additional traffic.

Network Visualization

Get a complete view of communicating devices and traffic patterns to build a visualization map that can accelerate research and quickly identify anomalies and incidents.

Vulnerability Database

To help you identify risks and patch priorities, we manage one of the most extensive databases of known vulnerabilities from researchers and security bodies across the globe.

Workbooks

Workbooks prioritize remediation efforts by highlighting the most critical endpoint vulnerabilities.

Asset Intelligence SUBSCRIPTION

Our Asset Intelligence subscription service keeps organizations up-to-date with latest vulnerability research, current OS and firmware patch levels and recent breaches.

Smart Polling ADD-ON

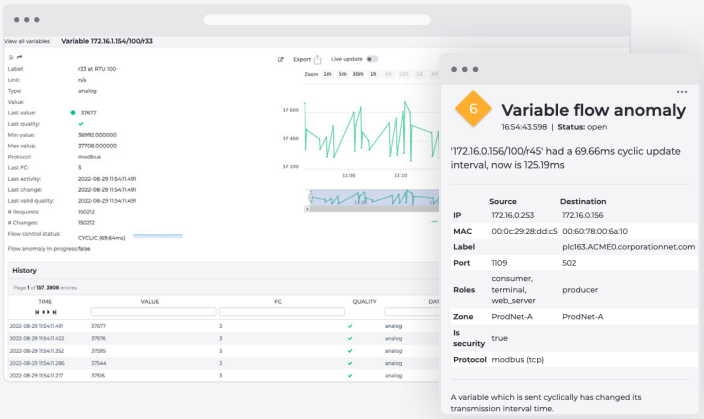
This asset reconnaissance feature proactively checks devices and gathers critical endpoint information for enhanced security. Polling parameters can be set to minimally impact existing traffic and devices below alarm thresholds.

Diagnose

We go beyond OT and IoT anomaly detection to help you diagnose the root causes of unexpected process changes and deviations from baseline behavior.

Reducing risk and anticipating potential issues is no guarantee that you will eliminate every new threat. Continuous process and traffic monitoring are critical to identifying and diagnosing threats or understanding process anomalies.

Nozomi Networks applies its artificial intelligence/machine learning engine to deliver industry-leading insights and analytics. Our threat intelligence data keeps you up-to-date with signatures and indicators of compromise (IOC) from the latest zero-day attacks and ransomware trends.



Process variables can be tracked for anomalies which could stem from an attack, human error, or potential mechanical failure.

Key Platform Features

Monitoring

Compare network traffic and process trends over time to identify potential threats and keep industrial processes running at peak efficiency.

Content Packs

Content Packs provide insights for common issues and emerging threats, like Industroyer2 vulnerabilities or IEC 62443 compliance.

Threat Intelligence SUBSCRIPTION

Detect more threats to more devices with our intrusion detection capabilities and support of the widest range of industrial devices and protocols. Threat Intelligence keeps you up-to-date with emerging malware and IOCs specific to industrial processes and IoT devices. Our feed is also available in an open format for use in other security platforms.

Anomaly Detection

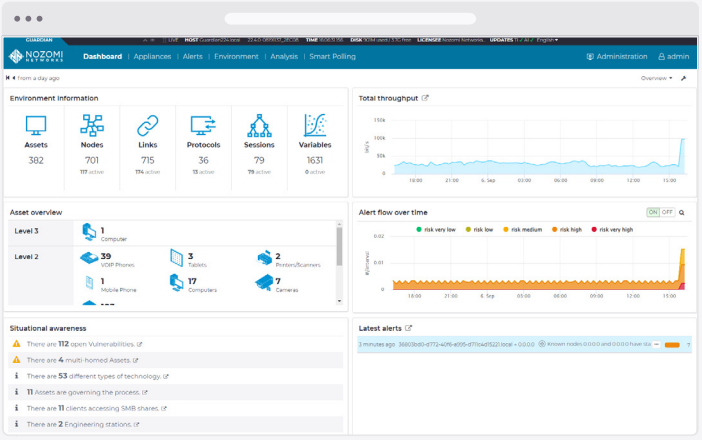
Our learned behavior over time helps eliminate false alerts and provides deeper insight into process trends. Go beyond traditional anomaly detection metrics of network traffic to trendlines of process variables and control system data to identify more issues and expand root cause analysis.

Respond

Actionable intelligence and guided remediation provide the insight you need to accelerate your response to critical OT and IoT security breaches and process control issues.

When it's time to respond to a security breach or a process control issue, you need actionable intelligence to address the problem with the minimum cost and impact to your operations. Nozomi Networks gives you all the information and insight to remediate issues, dive into further research and guide or coordinate an appropriate response. The Nozomi platform aggregates an enormous amount of data from devices and network traffic across the organization and over time.

In fact, we can do this at nearly infinite scale with our elastic cloud offering, Vantage. Making this data available, useful and accessible from a number of different angles is the power of the platform's user interface design, alert dashboards, query capabilities and forensic tools.



Customizable dashboards provide the important data you need to know in one location.

Key Platform Features

Time Machine

Time Machine allows users to replay network events around an incident to help isolate the root cause and visualize the impact to reduce mean time to repair (MTTR).

Reports

Reports are easily generated for turnkey, repeatable forensic or compliance reporting efforts. Queries and reports can be packaged into Content Packs or leverage existing Content Packs from Nozomi Networks and partners.

Dashboards and Alerts

Nozomi Networks dashboards are designed to give you a high-level, actionable view of events, systems, assets, security issues and alerts across a large organization. Filtering up a potentially enormous amount of information while keeping it fully organized and accessible saves time and effort for admin teams while focusing on real issues. Build queries across the environment to quickly isolate vulnerabilities, incidents or identify and inventory assets.

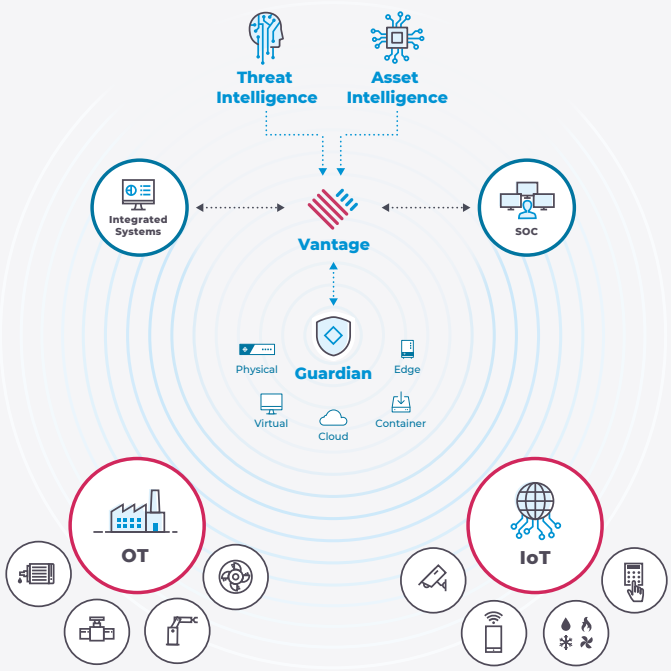
Playbooks

Playbooks are critical to coordinate a rapid response to an incident or outage. Nozomi Networks allows you to import or design your own security playbooks to define the remediation steps for any type of incident. Steps can be customized to include specific admins or executives based on incident type or location. Track Playbook steps to coordinate incident response as a workflow and integrate with ticketing systems.

Build Your Solution

The Nozomi platform provides a wide range of components and form factors to flexibly deploy and scale in a wide range of industrial and corporate environments.

We allow you to choose how and what to deploy on-premises and in the cloud for the most efficiency.



Vantage

SAAS

Nozomi Networks Vantage™ is a SaaS solution that scales security monitoring and visibility for large multi-site enterprises, while offering the cost benefits and flexibility of a cloud-hosted solution. It provides unified visibility and security monitoring for an unlimited number of nodes and systems for high volume traffic and asset infrastructure. It can simplify the deployment of on-premises Guardian sensors and reduces the complexity of managing multiple CMC devices.

nozominetworks.com/products/vantage

Guardian

EDGE PUBLIC CLOUD

Nozomi Networks Guardian™ sensors are on-premises sensors that collect and analyze your operational data. They eliminate blind spots in your operational environment with asset, data flow and network visibility for OT and IoT environments. Guardian sensors detect cyber and operational threats, plus vulnerabilities, providing situational awareness that is critical for ensuring security and compliance.

Guardian sensors can be run as virtual machines on a range of operating platforms, as a dedicated hardware appliance appropriate for the scale and complexity of the local environment, or on third-party devices designed for specific industrial processes. They are effective for all operational systems/subsystems including industrial controllers, IoT sensors, CCTV, building automation systems and ruggedized environments.

nozominetworks.com/products/guardian

Arc Sensor

EDGE PUBLIC CLOUD

Nozomi Arc™ endpoint sensors are endpoint executable that runs on either Windows, Linus or macOS hosts in mission critical networks. Customers can now easily identify compromised hosts with malware, rogue applications, unauthorized USB drives and suspicious user activity. Collected data can be sent to either Guardian or Vantage.

nozominetworks.com/products/arc

Central Management Console (CMC)

EDGE PUBLIC CLOUD

The Nozomi Networks Central Management Console™ (CMC) consolidates OT and IoT security and visibility across networks, making it easy to monitor and prioritize vulnerabilities and risks. It helps detect and disrupt emerging threats and answers questions fast through powerful queries about any operational data.

nozominetworks.com/products/central-management-console

Remote Collectors

ADD-ON

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.

Smart Polling

ADD-ON

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

nozominetworks.com/products/smart-polling

Asset Intelligence

SUBSCRIPTION

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).

nozominetworks.com/products/asset-intelligence

Threat Intelligence

SUBSCRIPTION

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).

nozominetworks.com/products/threat-intelligence

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.

NOZOMI NETWORKS

nozominetworks.com