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.

Figure 1 - Network view provides an interactive visualization 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
Nozomi Networks manages one of the most extensive databases of known vulnerabilities from researchers and security bodies around the globe. Compare to your environment to identify risks and patch priorities.

Workbooks
Workbooks prioritize remediation efforts by highlighting the most critical endpoint vulnerabilities.
Asset Intelligence [SUBSCRIPTION]

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.

Smart Polling [ADD-ON]

Smart Polling is an asset reconnaissance feature that proactively checks devices and gathers critical endpoint information for enhanced security. Organizations can set polling parameters (frequency and to which critical devices) to minimally impact existing traffic and devices below alarm thresholds. Combining passive asset discovery and Smart Polling provides the best and most accurate sensing and data capture possible.

Figure 2 - Workbooks highlight the corrections that can quickly improve your overall risk posture.
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.

Nozomi Networks goes beyond simple network anomaly detection to drill down into unexpected process changes and deviations from established baseline patterns to quickly diagnose root cause conditions and provide actionable intelligence to operators for fast remediation.

Figure 3 - 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.

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.
**Threat Intelligence**  
Detect more threats to more devices with our intrusion detection capabilities and support of the widest range of industrial devices and protocols. Threat Intelligence data keeps you always up-to-date with emerging malware and IOCs specific to industrial processes and IoT devices. Our Threat Intelligence feed is also available in an open format for use in other security platforms such as firewalls and security orchestration automation and response (SOAR) solutions that can update device policies based on the latest threat intelligence.

**Content Packs**  
Content Packs are readily available for the most common issues and emerging threats to provide specific insights, such as Industroyer2 vulnerabilities across your network, IEC 62443 compliance, and a lot more.

**Figure 4**  
Nozomi Networks Labs provides a combination of Packet and Yara rules along with STIX indicators and vulnerability detection to stay on top of the latest threats.
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. Security breaches and process outages happen to even the most sophisticated and prepared organizations. Nozomi Networks accelerates your response and manages the remediation efforts to reduce the incident cost and the administrative overhead involved.

**Figure 5** - 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. Repeatable or common query and report combinations can be packaged into Content Packs or leverage existing Content Packs available 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 in our system to define the remediation step process for any type of incident. The Playbook feature allows customization of playbook steps 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.

Figure 6 - Time Machine can be used to quickly highlight the changes in the network from one point in time to another.
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.

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

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.

A broad range of sensors ensures a fit with any size and location of network, including isolated or remote networks. They are effective for all operational systems/subsystems including industrial controllers, IoT sensors, CCTV, building automation systems and ruggedized environments. 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.

nozominetworks.com/products/guardian
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.

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).

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).

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.

CMC can be run on physical or virtual appliances that aggregate data from Guardian sensors, providing risk monitoring across diverse and dispersed networks. The CMC scales to hundreds of thousands of nodes and integrates with IT security infrastructure for streamlined workflows and faster response to threats. It can be run on-premises to support individual sites, or as a virtual workload in a virtual private cloud.

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.