NOZOMI NETWORKS



WHITE PAPER

Advancing OT & IoT Visibility and Cybersecurity with the Nozomi Networks Solution

Table of Contents

1. Introduction 1

2. Improving Network and Operational Visibility and Security 2

2.1 How OT Security Differs from IT Security 2
2.2 Diagram: OT and IoT Security and Visibility 3
2.3 Deployment Architecture: Purdue Model Example 4
2.4 Nozomi Networks Products and Services 5
2.5 Network Visualization Improves Situational Awareness and Speeds Troubleshooting 6
2.6 Superior Asset Inventory Enhances Cybersecurity and Saves Time 9
2.7 Dynamic Learning Reduces Deployment Time and False Alerts 11
2.8 Deep Protocol Support Recognizes Improper Communications 11
2.9 Vulnerability Assessment Helps Manage Risk Exposure 12
2.10 Process Views Improve Reliability Without Requiring Access to a Historian 13
2.11 Comparison of Guardian and Guardian with Smart Polling 14
2.12 Dashboards and Queries Enhance Risk Management and Staff Productivity 14

3. Detecting OT and IoT Cyber and Process Risks 17

3.1 Hybrid Threat Detection for Best-in-Class OT and IoT Security 17
3.2 OT Risk Management for Proactive Security and Reliability 20
3.3 Early Warning for Neutralizing Advanced Threats 23
3.4 Attack Detection for Rapid Mitigation 25
3.5 Blocking Attacks for Maximum Protection 25

4. Facilitating Rapid Threat Response 26

4.1 Detailed Alerts and Incidents Improve Risk Management 26
4.2 Forensic Tools Reduce Mean Time to Resolution and Improve Staff Productivity 28
5. Enabling Enterprise OT and IoT Risk Monitoring 30
5.1 High Performance and Scalability for Large Distributed Installations 30
5.2 Designed for Industry Skill Levels and Best Practices 31
5.3 Fast, Flexible Deployment for Immediate ROI 32
5.4 Easy IT/OT Integration for a Complete Solution 33

What to Look for in an OT and IoT Security and Visibility Solution 34

Want to Know More? 34

6. References 35

1. Introduction

Securing Industrial Networks and Improving Cyber Resilience

The Nozomi Networks solution improves reliability for converged OT and IoT systems. It does this by providing superior network and asset visibility and by rapidly identifying cybersecurity and process risks. It significantly reduces OT/IoT monitoring and threat response efforts and results in improved availability and cyber resilience.

The industrial sector is digitizing and automating processes at an increasingly rapid rate. While connected systems deliver new value and improved productivity, they also heighten cyber risk.

All this is happening against a backdrop of accelerating concern about cyber threats by world leaders and the C-suite:

> WORLD ECONOMIC FORUM
>
> Cyberattacks on critical infrastructure— rated the fifth top risk in 2020 by our expert network—have become the new normal across sectors such as energy, healthcare, and transportation. Such attacks have even affected entire cities. Public and private sectors alike are at risk of being held hostage.
>
> **World Economic Forum, The Global Risks Report 2020**[1]

In the face of escalating cyber risks, organizations are reinforcing their cyber defenses with the adoption of new technology. The SANS Institute emphasizes that:

> SANS
>
> [There is a] need to understand and chart the ICS environment. Internet connectivity has opened ICS network boundaries that historically were closed, well-defined and documented, resulting in the desire and need for visibility into critical communication links—especially wireless extensions to the ICS architecture.
>
> **SANS 2019 State of OT/ICS Cybersecurity Survey**[2]

Read this paper to learn how to gain reliability, visibility and security for OT and IoT networks using the Nozomi Networks solution.

2. Improving Network and Operational Visibility and Security

2.1 How OT Security Differs from IT Security

Providing visibility and security to operational networks is not simply a matter of implementing IT tools and practices. Unique requirements must be met:

Safety and Reliability

Many industrial systems operate 24/7/365 and involve processes with significant safety risks. Network interruptions or system failures may harm people, cause service or production interruptions, and result in negative economic consequences.

Cybersecurity tools that generate significant network traffic, for example, are not suitable because repeated queries can cause industrial devices to fail, or they introduce latency, which can also disrupt the industrial process.

Industrial Protocols

OT/ICS systems use many protocols that are unknown in the IT world, and that are inherently insecure. Analyzing communications using these protocols for security threats requires specialized evaluation techniques and must done at a very detailed level.

Heterogeneous and Legacy Systems

Industrial networks are usually large, include many diverse assets, and often consist of multiple connected architectures. In the age of the Industrial Internet of Things (IIoT), they are also adjusted frequently, with devices being added, and changed, all the time.

The Nozomi Networks solution poses no risk to safety and reliability.

- It can be installed as a passive solution
- It observes network traffic via a SPAN or mirror port

The Nozomi Networks solution supports dozens of industrial protocols.

- It has extensive understanding of industrial protocols
- It easily extends to proprietary protocols via a Protocol SDK

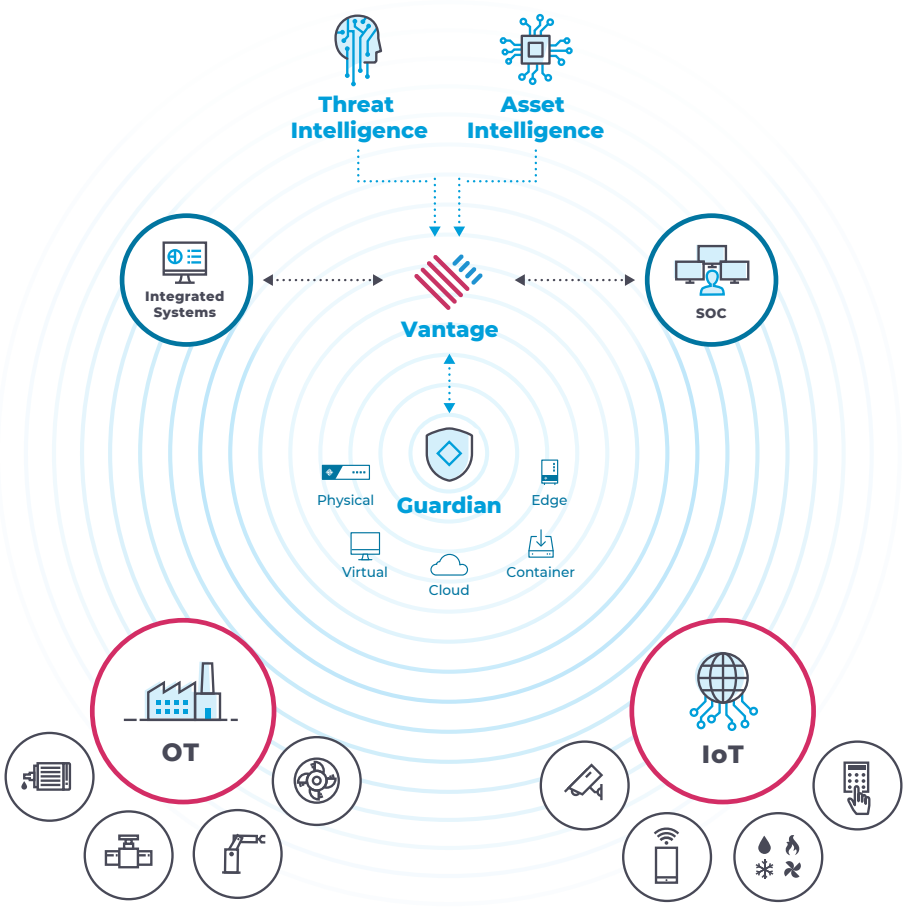
The Nozomi Networks solution tracks all types of assets & networks.

- It identifies devices from all vendors, including legacy assets
- It automatically maps network segments and topologies

2.2 Diagram: OT and IoT Security and Visibility

Industrial Strength Cyber and Operational Resilience

You can protect a wide variety of mixed environments with 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.

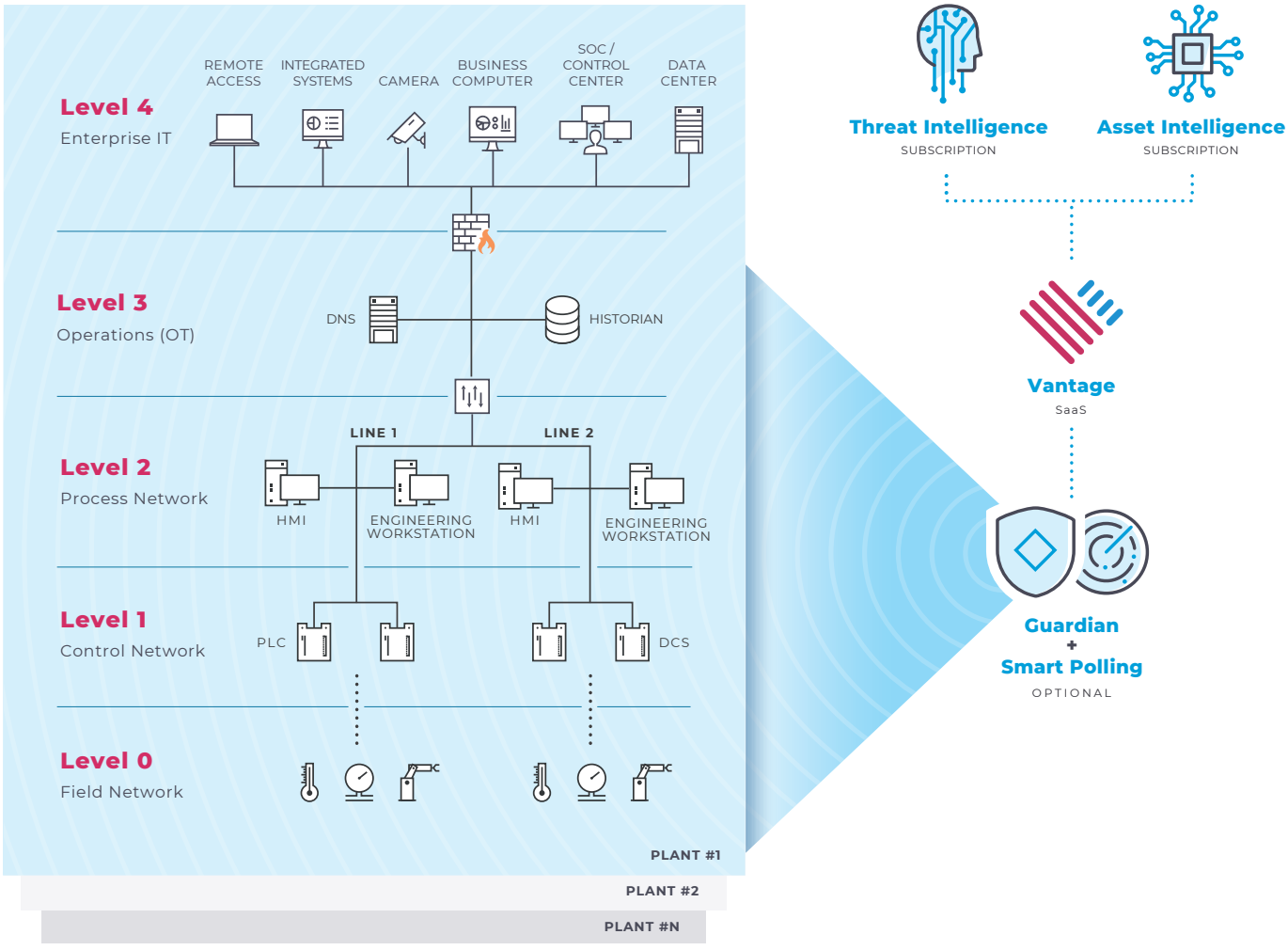
Our technology quickly and accurately detects malicious and anomalous activity.

You have the insights you need to understand and respond to threats before data theft or operational disruptions occur.

2.3 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.

Additionally, **Remote Collectors**™ can be added to Guardian sensors to capture data from remote and offsite locations.



2.4 Nozomi Networks Products and Services

SAAS

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

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

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

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.

EDGE OR PUBLIC CLOUD

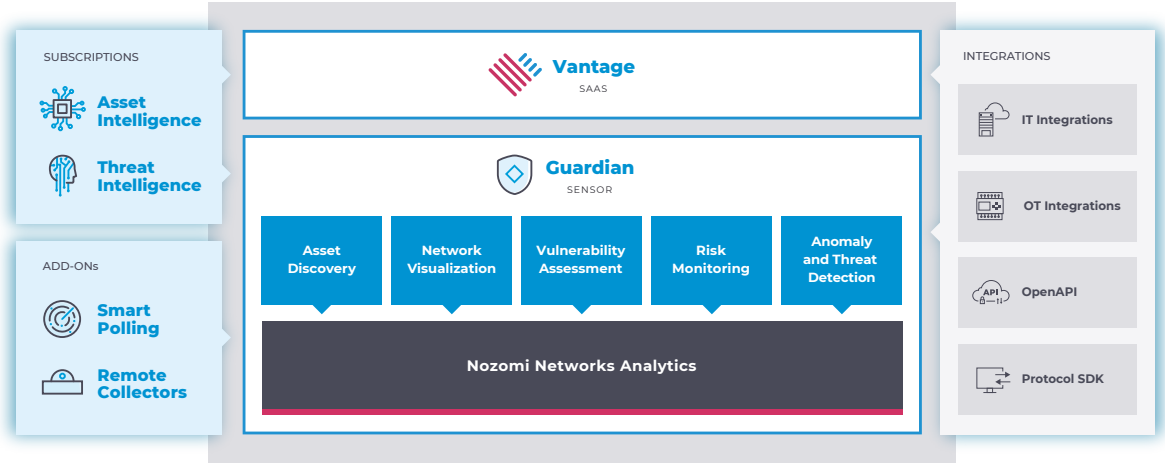
Guardian provides industrial strength OT and IoT security and visibility. It combines asset discovery, network visualization, vulnerability assessment, risk monitoring and threat detection in a single application. Guardian shares data with both Vantage and the CMC.

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).

GUARDIAN ADD-ON

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



The Nozomi Networks solution improves cyber resilience and reliability via a unified and scalable architecture.

2.5 Network Visualization Improves Situational Awareness and Speeds Troubleshooting

Industrial operators and cybersecurity staff often face the difficult task of managing and monitoring a system that is not thoroughly documented or easy to visualize.

As soon as the Nozomi Networks solution starts analyzing the traffic on a network, it builds an interactive, live visualization of the system.

Time and time again, when prospects and customers experience the smooth installation of the solution and see the immediate picture it provides, they are delighted. They quickly perceive aspects of their OT/IoT network that they were not previously aware of, and they can easily drill down to find more information.

Plug and Play Installation

Nozomi Networks fourth generation technology is ISO 9001: 2015 certified.
Its installation and functioning are not dependent on any operating system or software libraries because the technology is completely self-contained ("full stack"). The maturity of the Nozomi Networks solution makes it easy to deploy, delivering immediate value with rapid asset discovery and threat detection.

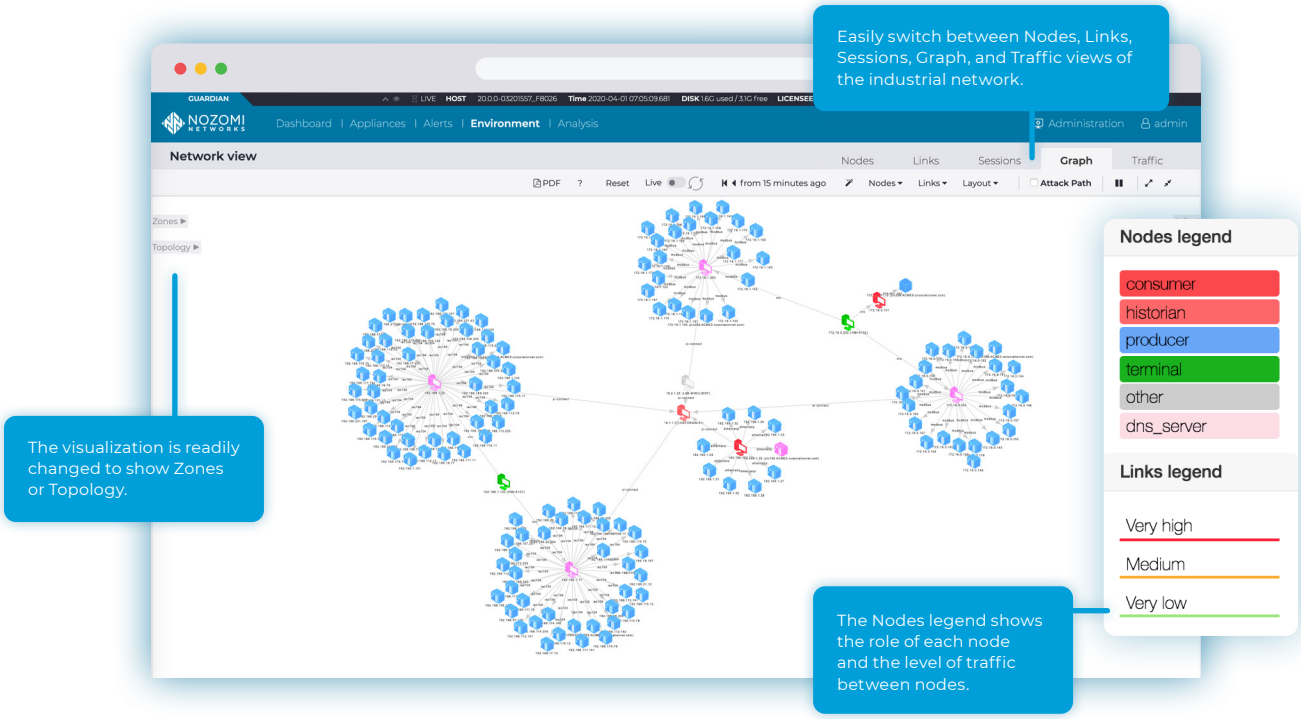


Figure 2 - Network Visualization Graph (Guardian)
Within minutes of deployment, the nodes of the industrial network are displayed in a live interactive visualization.

An extensive amount of use information is available from the real-time network visualization:

- A macro view of the entire industrial network
- The ability to navigate and filter by different subnets and network segments.
- The ability to drill down on any endpoint or connection to see detailed attributes

Deep Device Identification for Superior Visibility

The Nozomi Networks solution identifies all entities that communicate over the network, including:

- Entities with an IP or MAC address
- Devices without IP addresses, such as those that communicate at Layer 2 of the OSI model. An example is a substation device that uses the GOOSE protocol.
- Serial devices nested behind networking equipment such as gateways

The depth of assets identified is a differentiating capability that ensures that all communicating devices are monitored for cybersecurity and reliability risk.

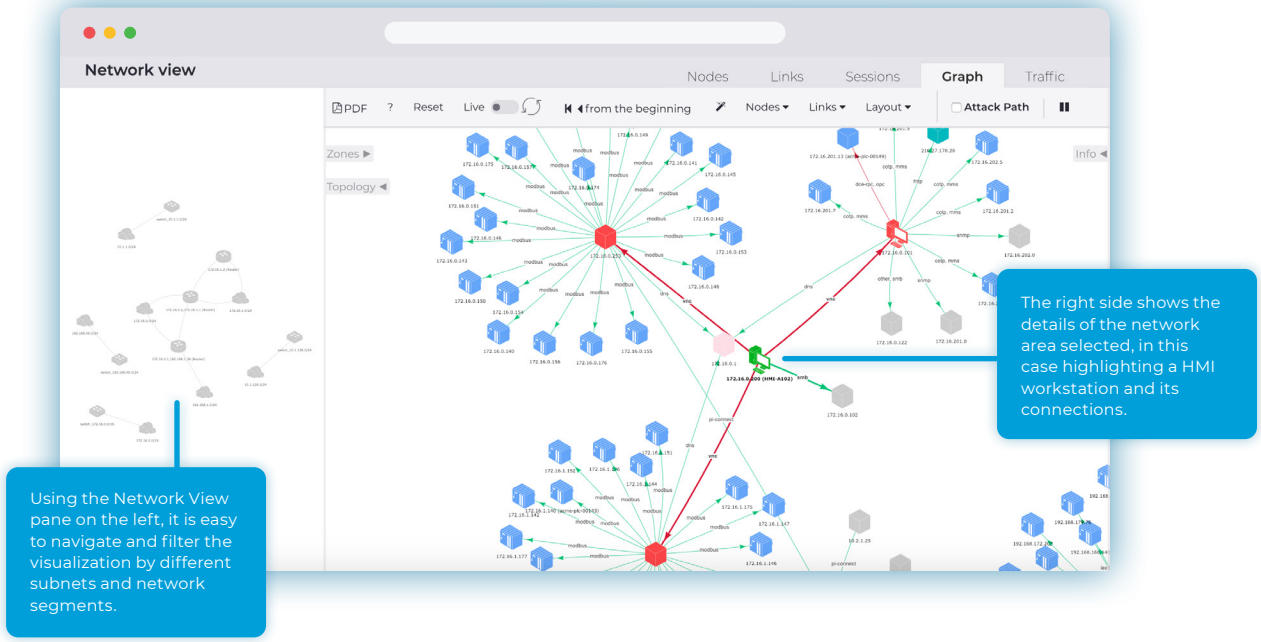


Figure 3 - Network Visualization: Topology (Guardian)

Other network visualization capabilities include:

- A display showing the protocols used to communicate between nodes and between zones
- Network traffic information such as throughput, protocols and open TCP connection
- Visualization of multiple, geographically distributed sites, when deployed with the Central Management Console
- Printable and exportable versions of the network structure and its details, in multiple file formats

Network Visualization Features and Benefits

OT

- A "no process risk" solution that provides comprehensive visibility to all ICS assets
- Rapid identification of threats, policy violations and risks to reliability
- Unique process views monitor variables such as pump speed or temperature
- Faster troubleshooting, as network information is easy to see and drill into
- Single application that monitors devices from all vendors
- A common platform to drive IT/OT convergence

IT

- Complete visibility to OT networks and their risk exposure
- Consolidated information from multiple industrial facilities via one monitoring tool, w hen using the CMC
- Shows IT-allowed protocols and alerts when disallowed protocols are in use
- Faster troubleshooting of OT incidents with ICS-specific dashboards and forensic tools
- Seamless integration with SIEMs and other IT applications
- A common platform to drive IT/OT convergence

> Nozomi Networks Guardian is now a fundamental element of our network infrastructure and an essential tool for our daily activities.
>
> **FEDERICO BELLIO, Head of Power Generation Remote Control System - Enel, Global Energy Company**

2.6 Superior Asset Inventory Enhances Cybersecurity and Saves Time

Developing and maintaining a centralized OT/IoT system inventory can be a difficult and time-consuming project. Guardian addresses this challenge by identifying assets, keeping them up-to-date, and monitoring them in real-time.

Guardian makes it easy to address questions like:

- Is it possible to quickly review all my assets?
- What is the firmware version of my PLCs?
- Can I monitor and be alerted to changes in my hardware/software?

Dedicated Asset Views make it easy to visualize, find and drill down into asset information. Assets, including common industrial devices, are presented:

- Grouped visually, as per the Purdue model
- In list views
- In detailed, single asset views

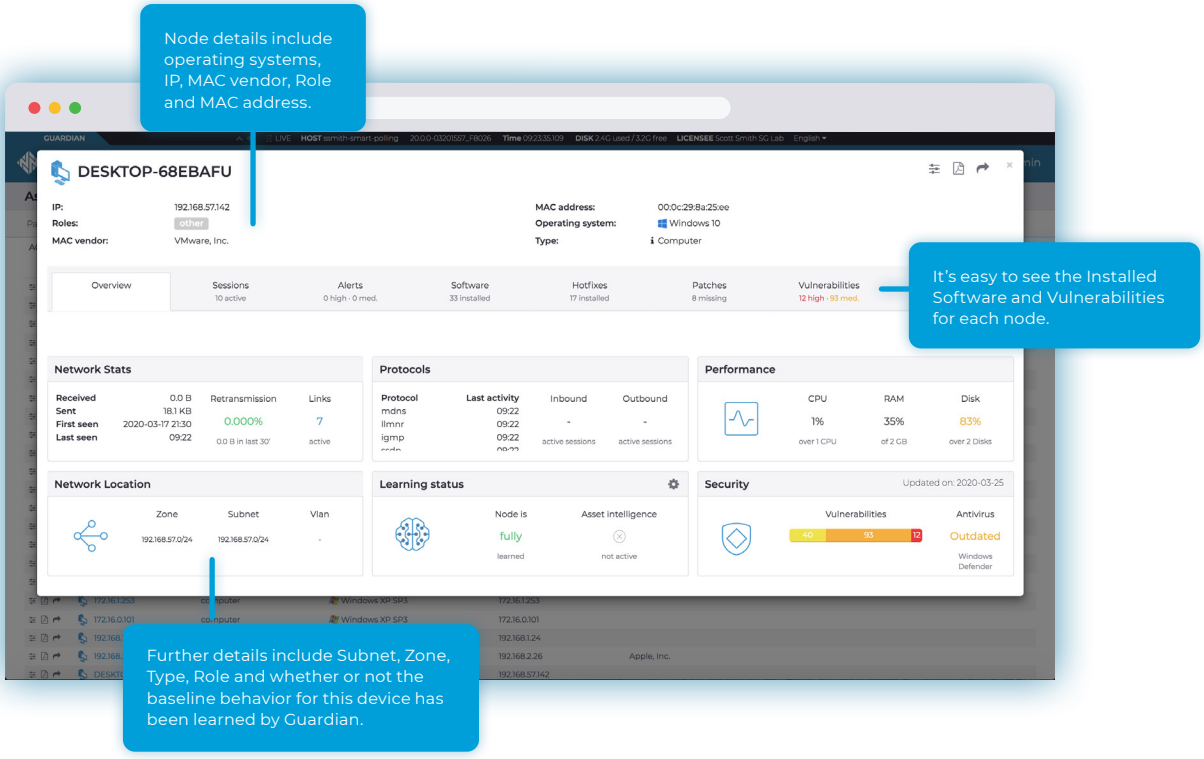


Figure 4 - Network Node Detail Screen (Guardian)
The amount of information shown for each node is extensive and includes vulnerabilities and installed software.

Many attributes are tracked per asset, including device name, type, serial number, firmware version, product name and components. It is also easy to add metadata for assets, such as location or site.

Guardian also captures context about each device, such as how it is being used. For example, if a Cisco switch (as indicated by its MAC address) is a being used as a Siemens Scalence Switch (the PROD vendor), Guardian is aware of it. This important attribute leads to lower false positives in anomaly detection and vulnerability identification, as compared to products that do not recognize encompassing systems.

Changes to hardware, software and devices are communicated via alerts which quickly bring potential cyber incidents or process risks to the attention of appropriate staff.



How Guardian's Accuracy in Identifying Assets Stands Out

Nozomi Networks believes that asset accuracy is important as a basis for cybersecurity alerts and policies. Thus, our solution does not infer information about assets, instead it validates details and provides precise descriptions.

If asset identification is deduced rather than validated, it undermines the credibility of the cybersecurity and risk information provided by a solution.

In comparison with other passive OT and IoT monitoring systems, Guardian stands out in terms of:

- Providing a high level of detail about each asset
- Completely validating the details of an asset, such as the manufacturer, before naming it
- Identifying components as being part of another system, such as a control system

Guardian is a passive solution and it identifies all assets that communicate on the industrial network.

If identifying non-communicating or rogue assets is important to your operation, however, you should consider Guardian with the Smart Polling add-on module. It uses a low volume, active approach to provide precise asset details including operating system information, firmware, patch levels and more.

2.7 Dynamic Learning Reduces Deployment Time and False Alerts

The network visualization of Guardian is generated during the product's learning phase, by using artificial intelligence and machine learning techniques to model the network. Once the modeling is complete, protection mode is enabled and Guardian begins monitoring for changes that may indicate threats to security or reliability.

The automatic switching of modes is called Dynamic Learning™. Its advantages are:

- Protective monitoring of stable nodes and network segments happens quickly. Threat and anomaly detection for parts of the network are not delayed because some nodes or network segments are less stable.
- No configuration change, manual work or guesswork is involved in changing the mode.
- The learning of normal behavior is very accurate and reduces false alerts.

Although baselines are established automatically, it can be helpful to incorporate the knowledge of onsite system experts. For example, you may need to adjust the baseline for things such as rogue PCs or dual-homed devices that have an explicit purpose.

2.8 Deep Protocol Support Recognizes Improper Communications

When learning a network, Guardian analyzes communications utilizing its extensive understanding of dozens of OT, IoT and IT protocols. Not only is its built-in protocol support broad, new protocols are added on a regular basis and can be readily extended using the Nozomi Networks Protocol SDK.

A complete list of currently supported protocols is available at **nozominetworks.com/techspecs**.

Guardian provides rapid alerts if it detects unusual or disallowed protocols. And, regarding protocols that are unique to industrial environments, including proprietary and open source ones, Guardian does a thorough analysis of their communications.

This is done using protocol-specific Deep Packet Inspection* (DPI) techniques, which include:

- Examining packets in all 7 layers of the OSI model
- Knowing the official syntax and grammar for each protocol
- Understanding the customizations used by specific industry sectors
- Using a high performing analysis algorithm to evaluate possibilities in real-time

The benefit of protocol-specific DPI is the accurate identification of improper communications that could indicate new threats or risks. OT and IT staff are quickly alerted, and problematic situations can be quickly handled.

* Protocol-specific Deep Packet Inspection (DPI) validates a protocol's structure, the sequence of packets, proper byte values and more. It is different from signature-based DPI used in IT (often by internet service providers) as it can identify previously unknown threats or risks.

2.9 Vulnerability Assessment Helps Manage Risk Exposure

Another challenging aspect of OT security and process reliability is knowing which devices are vulnerable and require updates or special protection. For example, engineering and cybersecurity staff might want to know:

- Are the assets from Vendor X vulnerable?
- How many assets are still running Windows XP?
- Do I need to update certain network devices because their firmware is vulnerable?

Guardian automatically identifies devices with vulnerabilities using updates from the Threat Intelligence service. Vulnerability naming and descriptions use standardized conventions, as defined by the NVD (National Vulnerability Database).

As a passive product, Guardian identifies what vulnerabilities may exist on an asset, but does not know if patches have been applied. When used with the Smart Polling add-on module, however, Guardian confirms vulnerabilities, providing accurate vulnerability assessment for fast and efficient response.

Using dedicated views, vulnerabilities and their severities can be identified by vendor or other attributes and prioritized for remediation. This supports proactive mitigation of cyber risks, improving network resilience.

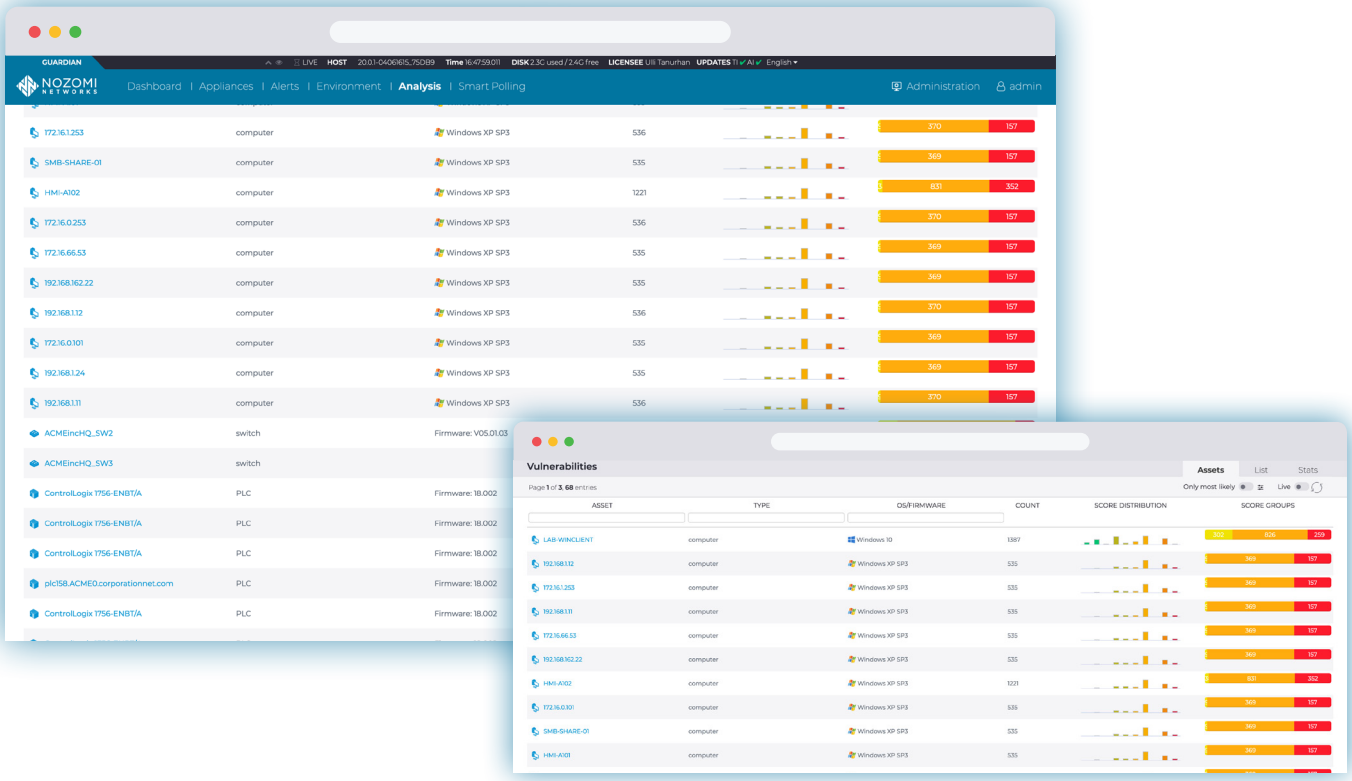


Figure 5 (left) - List of Vulnerabilities by Severity Level (Guardian)
Shown above are the vulnerabilities present on a facility's industrial assets.
Figure 6 (right) - List of Assets with Confirmed Vulnerabilities (Guardian with Smart Polling)

2.10 Process Views Improve Reliability Without Requiring Access to a Historian

A very important part of monitoring an ICS system is knowing normal values for process variables and recognizing when they are moving towards a critical state. Guardian not only identifies and baselines process variables, it models their behavior and correlates multiple types of data to detect when they are moving to a state that will disrupt normal operations.

This is an important way of detecting behavior that might be related to a malware attack early in its kill chain, or determining an operational reliability issue.

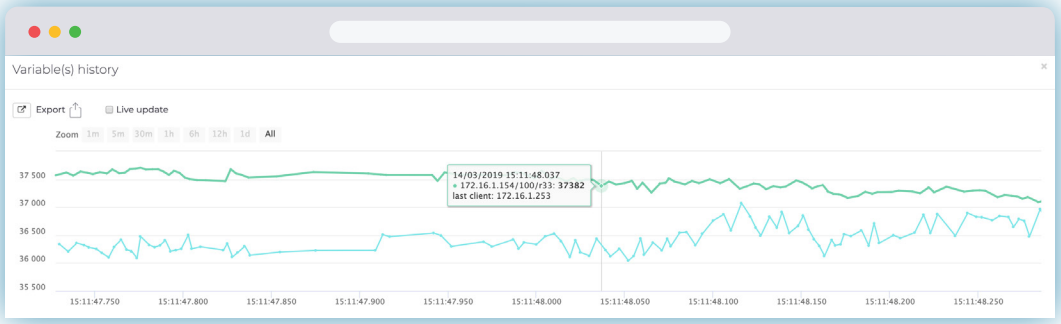


Figure 7 - Variables History Chart
The chart shows increasing, erratic pressure for gas flowing through a pipeline (lower line), compared to the normal flow rate (upper line). Rapid identification and investigation of this pattern would, in this case, alert operators of a slow seepage problem.

Guardian's Process Views and Alerts

Guardian's Process Views and the way it uses process variable information for cybersecurity and reliability monitoring is a unique capability.

For example, alerts automatically include information that makes it easy to view process variable trends and see how they are deviating from normal states. There is no need to manually guess how an alert is related to a specific process, through a method such as associating a controller memory location to a process (see Figure 15, page 20).

2.11 Comparison of Guardian and Guardian with Smart Polling

When considering asset inventory, vulnerability assessment and network monitoring needs, the Nozomi Networks solution provides two options. Guardian is passive and provides a high proportion of asset and vulnerability information.

Guardian with Smart Polling builds on the passive information, using precise, active technologies for additional details.

Functionality	Guardian	Guardian with Smart Polling
Network Analysis	Passive	Passive + Active Smart Polling
Asset Inventory	Identifies Communicating Assets	Identifies All Assets
Vulnerability Assessment	Identifies Vulnerabilities	Confirms Vulnerabilities
Network Monitoring & Threat Detection	for Communicating Assets & ICS Data	for All Assets & ICS Data
Deployment	No IP Address · Installed on SPAN or Mirror Ports · No Routing Required	Assigned IP Address · Installed on Switch or Router Port · Routing for Selected IPs Enabled

Figure 8 – Comparison of Guardian to Guardian with Smart Polling

If visibility and cybersecurity needs require the functionality of Guardian with Smart Polling, be aware that the product provides control over the extent of Smart Polling done.

A default configuration can be used, or manual options can be set that limit its use to specific devices and network segments.

2.12 Dashboards and Queries Enhance Risk Management and Staff Productivity

The Nozomi Networks solution is designed to improve both risk visibility and staff productivity. One of the ways it achieves this is via dashboards that quickly and accurately extract and organize key network and process insights. Information that has been consolidated to show internal metrics and policies saves time and speeds response times.

The dashboards included with Guardian and the CMC highlight critical information. They are also flexible and customizable.

Guardian dashboards summarize OT and IoT risk information for selected date and time ranges. For example, they can show:

- The number of alerts detected in a specific period of time
- Critical performance indicators, including current data and variance from the previous period
- The nodes most at risk, including related alerts
- Visual markers that blink if the number of alerts is increasing

Following are two dashboard examples.

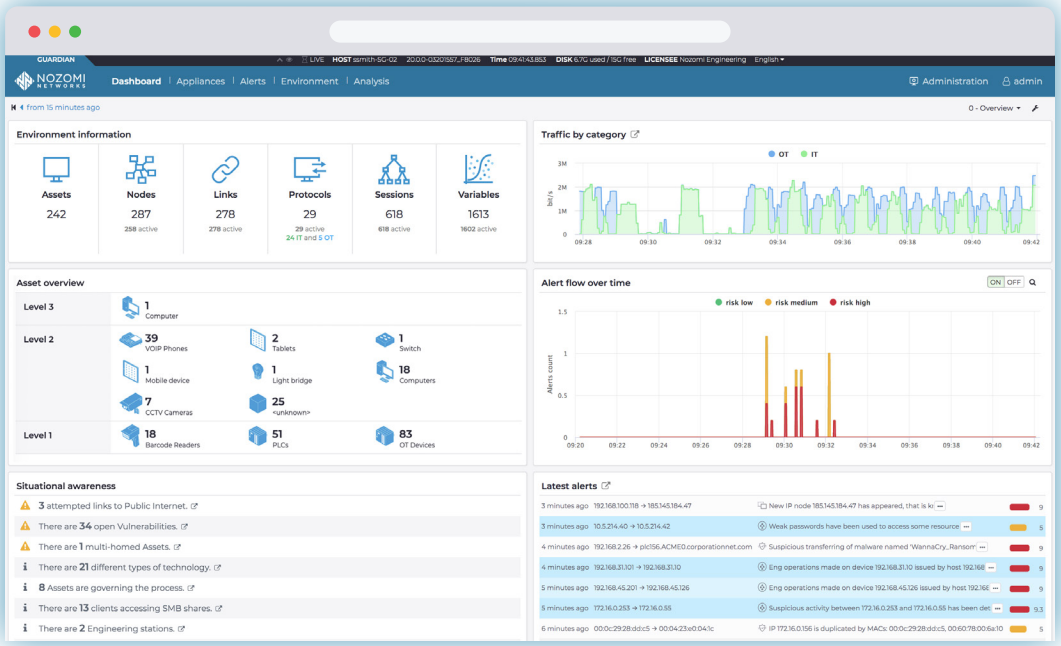


Figure 9 – Dashboard Showing Real-time Network Throughput (Guardian)
The high amount of VNC traffic might be normal or alarming, depending on the industrial network.

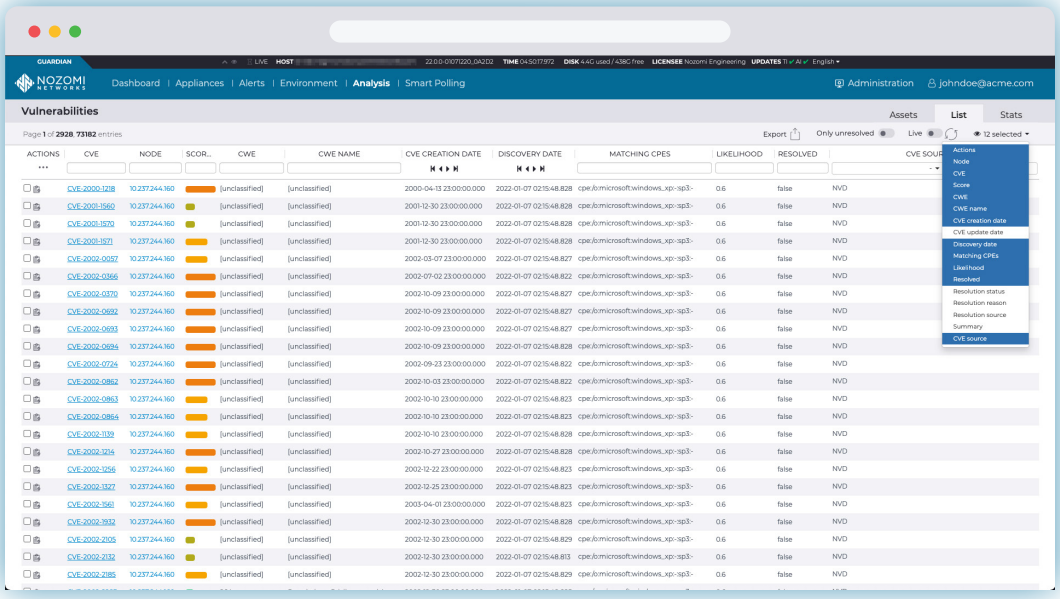


Figure 10 - Key Vulnerability Scoring and Details (Guardian)
Using this data, vulnerability work can be prioritized, maximizing cyber resiliency enhancements per work hour of effort.

Queries Answer Real-time OT and IoT Questions

The Nozomi Networks query tool provides real-time information on any aspect of device attributes, network communication, cyber risks and process variables. It is a powerful way to monitor and investigate system performance.

Queries can be simply posed and an answer returned, or they can be used to build tables, graphs and widgets.

Building on queries, assertions are rules that check for certain conditions, such as policy violations. They generate alerts, or communicate with other applications, when the conditions are either met or not met.

For example, when wanting to check whether an Indicator of Compromise (IOC) exists in the system, an operator could:

- Use a Query to check whether the IOC exists right now
- Use an Assertion to regularly check that the IOC does not exist (see Figure 13, page 18). If it is found, generate an alert. The alert could also be sent to another security application, such as a SIEM.

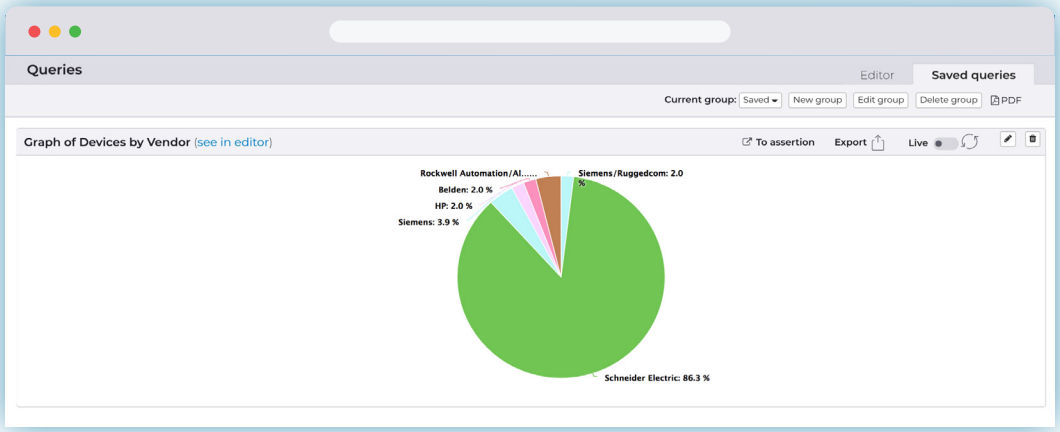


Figure 11 – Query Result Showing a Graph of Device Vendors
This widget can be included in dashboards, reports and API queries.

Nozomi Networks Customer Efficiently Checks for IOCs

Mr. Smith is describing how he uses Nozomi Networks queries and assertions to check for IOCs that are provided to him through E-ISAC (Electricity Information Sharing and Analysis Center) and other sources.

"I've also added IOCs as I get them through the cybersecurity community. So, in a matter of moments, I can identify, and promptly address, any issues."

Kris Smith, Manager Operations Engineering, Vermont Electric Cooperative

3. Detecting OT and IoT Cyber and Process Risks

Guardian uses a hybrid approach to detect risks and threats. This includes behavior-based anomaly detection and multiple types of signature and rules-based detection provided by the Threat Intelligence service. Furthermore, anomaly detection and signature detection results are correlated with operational context to provide rapid insight into what is happening, reducing mitigation and forensic analysis time.

3.1 Hybrid Threat Detection for Best-in-Class OT and IoT Security

Behavior-based Anomaly Detection for Identifying Unknown Threats and Risks

A foundational capability of Guardian is its ability to learn normal network and process behavior. It achieves this by building a baseline OT and IoT virtual image of an industrial installation, which serves as a logical and comprehensive model of its physical processes and network deployment. Then, to rapidly identify anomalies and correlate them with process data readings, it uses:

- advanced industrial network behavioral analytics
- artificial intelligence techniques, and
- continuous real-time assessment.

Examples of anomalies include changed or added devices within the network, irregular commands, and communication issues such as bandwidth and latency threats. Anomalies are categorized according to threat category, risk level and location within the network.

An important risk type that anomaly detection can help identify is a zero-day attack on an unknown vulnerability. Signatures do not yet exist for such malware, but using communication and behavioral anomalies, the threat can be identified and stopped or mitigated before damage is done.

Signature-Based Analysis for Identifying Known Malware and IOCs

Signature-based threat analysis immediately identifies known malware present in industrial environments. It is a proactive way to identify any threats currently present including early stage attacks that have not yet caused harm.

Yara Rules for Up-to-Date and Time Saving Threat Hunting

Yara rules are a library of advanced scripts that check for the presence of malware IOCs. They aggregate checking for multiple IOCs for a particular malware, reducing manual threat detection work.

Guardian embeds Yara rules in its platform that have been curated or built by the Nozomi Networks Labs team. This ensures the rules are accurate and high quality, saving your organization the time involved in evaluating new Yara rules.

Packet Rules for Granular Threat Hunting

SNORT-like packet rules examine subsets of files for malware and cyber threats unique to the industrial environment. Packet rules harness the power of Guardian's DPI and analytics engine to evaluate packets within the control network for operational anomalies and malware profiles that are known indicators of defined threats.

For example, packet rules can identify a malware attack in process by examining known malicious protocol behavior between devices within the ICS network, such as irregular command structures.

STIX Indicators

STIX indicators identify elements of threat indicators, such as an IP address or a file hash, and are used to observe

patterns or behaviors of interest within a cybersecurity context. Guardian correlates STIX indicators with other information to assess and alert on threats.

Threat Intelligence

Nozomi Networks Threat Intelligence service continuously updates Guardian sensors with rich data and analysis so you can detect and respond to vulnerabilities and emerging threats faster.

Guardian correlates Threat Intelligence information with broader environmental behavior to deliver maximum security and operational insight.

Asset Intelligence

Nozomi Networks Asset Intelligence service continuously updates Guardian sensors with rich OT and IoT device data so you can identify and respond to the most important security alerts faster.

Guardian's anomaly detection for IoT leverages millions of OT and IoT asset profiles for asset identification and anomaly alerting at enterprise scale



Continuous Threat Research reduces the time to detect active threats and vulnerabilities.

Rapid response is facilitated by the products' time-saving forensic tools. This includes Smart Incident™, which correlates incidents with operational context for rapid insight. Other tools include automatic packet captures, Time Machine™ system snapshots and an ad hoc query tool. For more information, see section 4.

Assertions for Custom Threat Hunting and Risk Identification

Assertions are rules that each organization, or their trusted providers, create to detect data and specific events from a stream of network traffic. They are particularly useful in addressing new malware attacks because they are an adaptive threat hunting tool. As hackers become more innovative, assertions can be updated, or new ones written to check various data flows for signs of infection and irregular behavior. Assertions allow organizations to be as proactive as possible in changing security environments.

An example is related to the critical incident detected shown in Figures 18 and 19, on page 26. Dragonfly files have been identified on the network, but has the malware been launched? Has a connection with a Command and Control (C2) server occurred? Assertions can be set-up to check for connections with the known IP addresses of malware, as shown below.

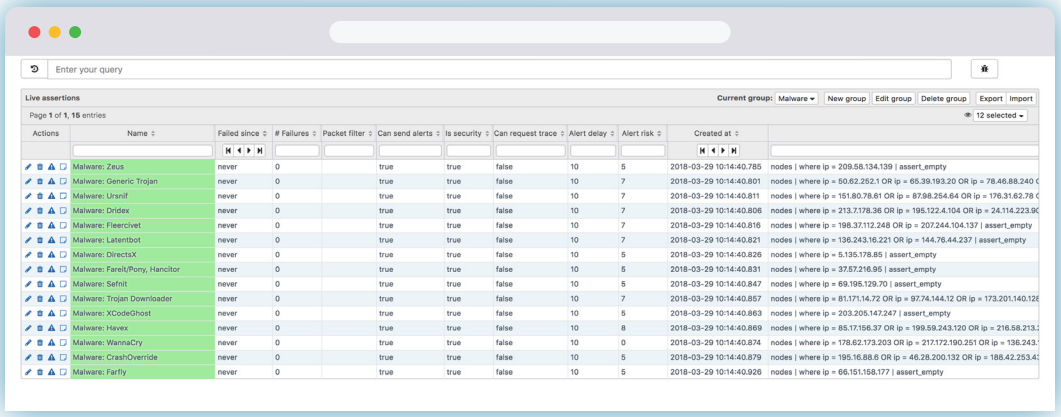


Figure 13 - List of Assertions that Check for Malware Communications with External Servers
If such communication occurs it indicates a compromise and requires an immediate response. In such a case the assertion automatically triggers an urgent alert.

Other uses of assertions include monitoring for operational conditions of interest or helping diagnose equipment or communication problems. An assertion could be written to check whether compressors are operating outside of a certain range, and if they are, notify operators with an alert.

3.2 OT Risk Management for Proactive Security and Reliability

Identifying Network Risks for Ongoing Improvements to Cyber Resilience

The Nozomi Networks solution proactively identifies risks that threaten the security and reliability of industrial networks. Identifying these risks and scoring them helps operators act to improve cyber resilience on an ongoing basis, strengthening defenses against deliberate or accidental cyberattacks. Examples include detecting:

- Assets with vulnerabilities
- Cleartext or weak passwords
- Device state change
- New connections to the enterprise network
- New communications
- Policy violation
- Used ports of assets
- Unauthorized cross level communication
- Bad configurations (NTP/DNS/DHCP, etc.)
- Corrupted OT packets
- IP conflicts
- New connections to the Internet
- New nodes
- New remote access
- Non-responsive assets
- Unencrypted communications (Telnet)

Identifying Operational Risks for Ongoing Improvement to Reliability

The Nozomi Networks solution provides visibility not just to cybersecurity risks, but also to operational risks. To achieve this, it analyzes network traffic using a multi-dimensional approach that considers both network connections and the process state.

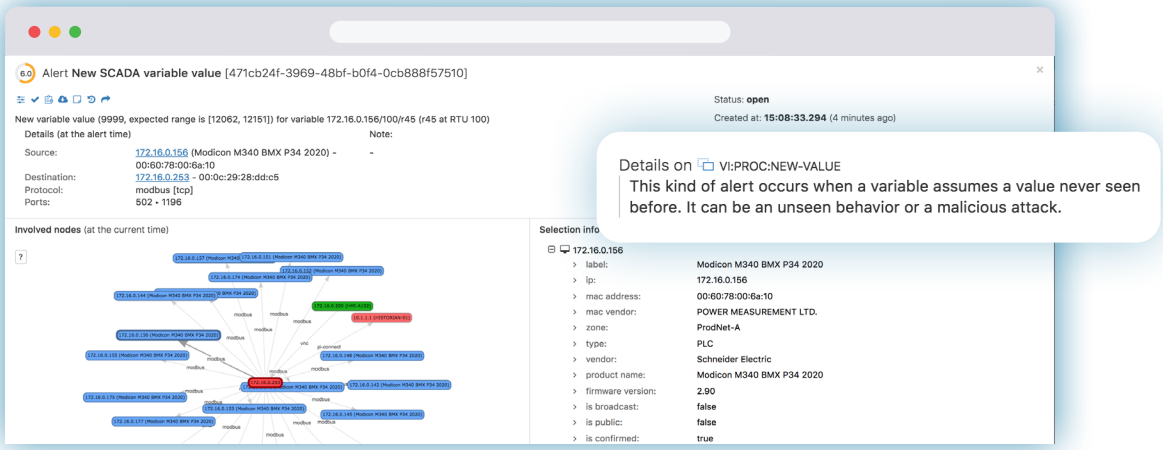


Figure 14 – Alert for a New SCADA Variable Value

There could be many reasons for the new variable value. The facility may have changed its process or it could, in the worst case, be the result of a stealthy cyberattack. There might also be a problem occurring in the process. Using Guardian, it's easy to investigate further. Simply clicking on the Navigate button brings up links to all of the nodes related to the alert.

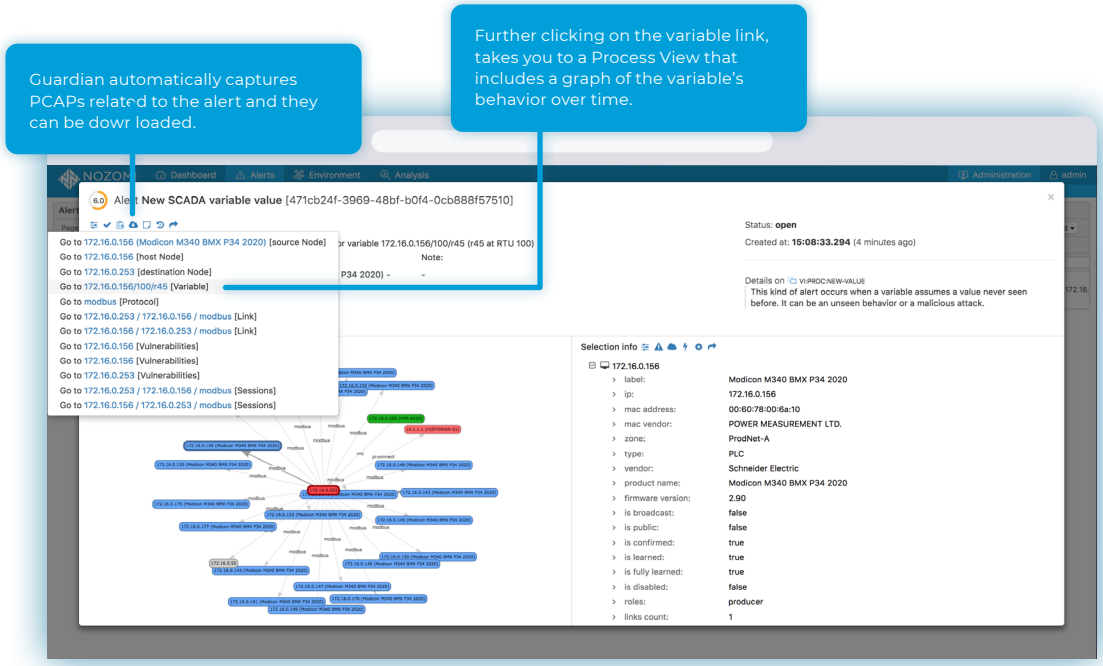


Figure 15 – Analyzing a Process Anomaly by Investigating Related Details



Figure 16 – Process Variable Graph

The graph shows a sudden change in the value of the variable, which should not occur in a stable process.

Operators will want to dig deeper, and Guardian helps with that, using forensic tools described in section 4.

Other ways that Guardian could contribute to better reliability are:

- Recognizing problematic links before there is a connection issue. For example, identifying that link retransmission rate is not very high (5.5%) but requires four connection attempts to complete a three-way handshake. This information can be used to take action before a connection issue occurs.
- Verifying maintenance work at remote sites, such as checking whether a firmware update of IEDs was completed or not. If not, the vendor can be contacted to address the situation before there is a problem. Similarly, Guardian can be used to ensure that Service Level Agreement work is done on time.
- Documenting complex device bugs. Often troubleshooting tools are cumbersome to set-up, logs from different vendors are hard to compare, or trace logs are not available. Guardian helps track down and document issues, facilitating proactive measures to improve reliability.

Nozomi Networks Customer Improves Operational Efficiency

The solution also helps reduce time spent on troubleshooting and forensic activities.

"Guardian allows us to drill down in protocols for new and existing equipment to efficiently diagnose issues. Consequently, we've improved our operational performance and in some cases can avoid costly truck rolls."

Kris Smith, Manager Operations Engineering, Vermont Electric Cooperative



3.3 Early Warning for Neutralizing Advanced Threats

Advanced threats that aim to disrupt industrial processes typically go through lengthy infection, reconnaissance and lateral movement phases before conducting their final attack. Guardian detects malware at each of these phases, and in the early stages, alerts practitioners with information that allows them to prevent the final attack from occurring.

An example is Industroyer (also known as CrashOverride or Win32/Industroyer), which was revealed in 2017. It is believed to have been responsible for shutting down electrical power to large parts of Kiev, Ukraine in December 2016.

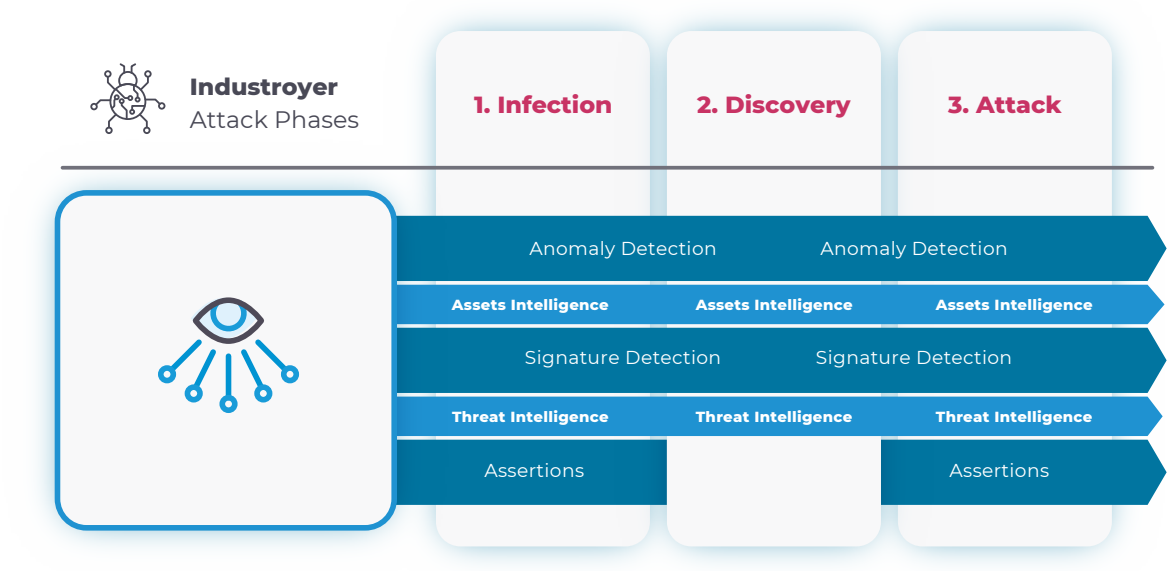


Figure 17 - Industroyer Attack Phases
The lower part of the diagram shows which hybrid threat detection technologies are effective against each phase.

Guardian detects Industroyer in all three attack phases. In Phase I, the Threat Intelligence service has specific Yara rules for Industroyer and immediately identifies the malware. In addition, Guardian's anomaly detection identifies that the malware is beaconing out to an external Command and Control server (C&C) through its connections to a new public IP address. Finally, assertions can be used to detect data and events in network traffic related to the presence of the malware at a particular site.

In Phase 2, the malware engages in a learning process to prepare an effective attack. In this phase Industroyer would also be identified by IOCs from Threat Intelligence.

If this was a never-seen-before attack, Guardian's anomaly detection would excel in identifying the threat. It identifies new commands in the host network and generates alerts that include the source of the commands. Even if the attacker uses regular industrial protocols to communicate,

its messages are different from the system's baseline behavior, allowing them to be identified.

In Phase 3, if an attack did occur, it would be quickly identified, and security or operations staff could implement new firewall rules, or take other actions, to stop further attack commands.

Alternatively, thanks to integration with security infrastructure, Guardian can automatically trigger the implementation of rules that block the attack upon detecting irregular commands. Examples of integrated infrastructure include firewalls, UTMs (Unified Threat Management solutions), and EDRs (Endpoint Detection and Response solutions).

Other incidents that Guardian detects, which can indicate the early stage of an attack, include:

- Nodes with a high number of connections within a short time interval
- Invalid IP addresses
- Anomalous packets
- Anomalous protocol behavior
- New values on producer – variables on a host have new values
- New variables request – producer has been asked for new variables from consumer due to suspect reconfiguration of the consumer
- Configuration downloads



FIREEYE™

Adversaries are increasingly targeting critical infrastructure around the world and operators are prioritizing cybersecurity for industrial control systems and other types of operational technology.

After extensive testing, we've partnered with Nozomi Networks because they provide the right solution customers need to detect these attacks at the earliest stages and minimize the impact before the safety and reliability of their critical operations is threatened.

Grady Summers, CTO, FireEye

3.4 Attack Detection for Rapid Mitigation

While cyberattacks with malicious intent dominate the headlines, many cyber incidents result from inadvertent actions.

Regardless of intent, Guardian identifies these indicators of attacks:

- Distributed Denial of Service (DDoS) attacks
- Logic changes
- Man-in-the-Middle (MITM) or scanning attacks
- Process variable values reach a critical state
- Set-point changes
- Firmware downloads
- Malware signatures detected
- PLC actions (Start, Stop, Monitor, Run, Reboot, Program, Test)

3.5 Blocking Attacks for Maximum Protection

The Nozomi Networks solution is integrated with firewalls from leading vendors for optional automated active response. If an anomaly or suspicious behavior is detected, an alarm is generated and sent to security operators and network administrators.

At the same time, Guardian is capable of automatically modifying the right policy in a firewall to block the suspicious traffic. For more information on this, send us a request at **nozominetworks.com/contact**.



4. Facilitating Rapid Threat Response

The Nozomi Networks solution includes incident and forensic tools that are designed to speed response times and maximize staff productivity. These tools are built on top of a foundation of effective and proprietary Dynamic Learning, which minimizes false alerts.

4.1 Detailed Alerts and Incidents Improve Risk Management

Once the learning phase for each network segment is closed, and the protection period starts, Guardian identifies deviations from baselines as well as the presence of known malware signatures. Depending on the irregularity or risk identified, more than 50 types of alerts can be generated.

Nozomi Networks alerts have been praised for their accurate and helpful detail. As an example, another passive OT and IoT monitoring solution might provide an alert that says:

> "TCP ports were scanned."

In comparison, the same alert from Guardian indicates:

> "xxxxx.xxxscada.local, Telvent OASYSDNA Host tried to discover services on target IPS: 101 connection attempts with 0 successful connections in less than 10 seconds, also target 10.xx.xx.xx'."

Alerts are grouped into a dozen types of context-aware incidents using a powerful correlation engine. The result is that operators or cybersecurity staff are provided with a simple, clear, consolidated view of what is happening in the industrial network.

For example, Figures 17 shows a list of alerts and incidents with a critical incident at the top of list. This incident indicates a new node has been found. As described in the SANS 2017 Report. those responsible for the security of industrial networks rate the risk of devices and "things" that cannot protect themselves being added to the network as their highest area of concern.

Figure 18 shows the detailed alerts related to the incident, and from these correlated results it is straight forward to understand what has happened. Likely a new laptop was connected, and it transferred the Dragonfly 2 malware onto the industrial network.

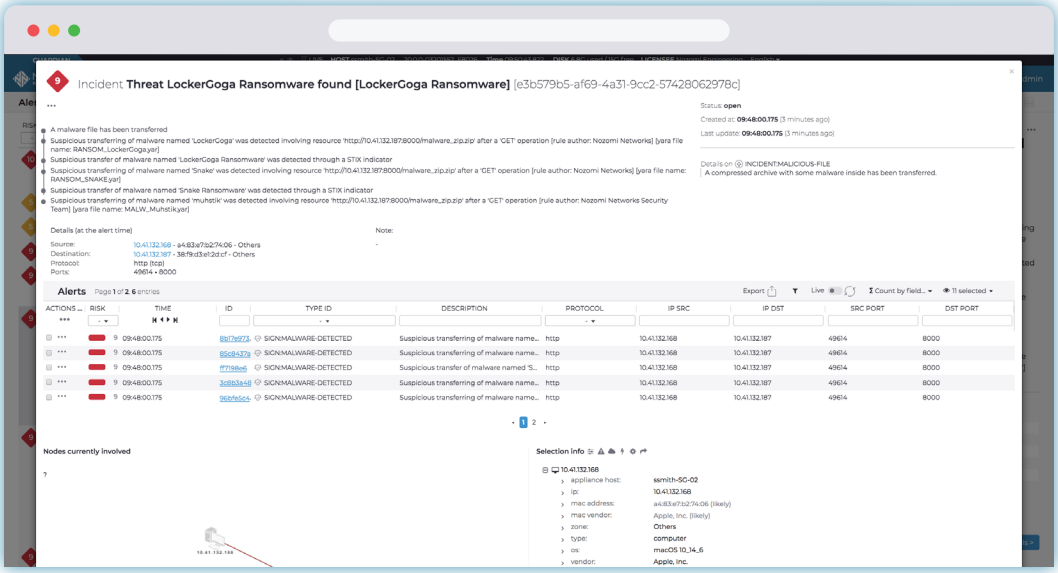


Figure 18 - The Guardian Incident / Alert View

The top alert has a risk score of 9 (high) to warn that malware has been detected on the network.



Figure 19 – Drilling Down on the Critical Incident shows Individual Alerts and Key Details that Enable Rapid Response

4.2 Forensic Tools Reduce Mean Time to Resolution and Improve Staff Productivity

When an operator sees that a critical incident is underway via an alert (or incident), they can bring up a detail screen for more information. They can then examine the PCAP related to the alert, download the PCAP, and also easily access a diff report for times before and after the alert by simply clicking on a button. Once changed parameters are identified, personnel can take immediate action to stop or mitigate an attack.

Diff reports are an aspect of Guardian's unique Time Machine capability. The Time Machine takes system snapshots at periodic time intervals, allowing it to be explored and investigated at many moments in time. The snapshots are dynamic, allowing operators to drill down and examine a rich information set. This invaluable forensic tool speeds up incident response.

Guardian further facilitates incident response with its powerful ad-hoc query tool that provides real-time responses to inquiries. The query tool can access the wide range of OT and IoT data generated by Guardian, such as alerts, assets, links, nodes, sessions, variables and zones. It can also use commands and functions to analyze the data.

Assertions can also play a role by regularly checking that IOCs do not exist and raising an alert if they are found (see Figure 13 page 18).

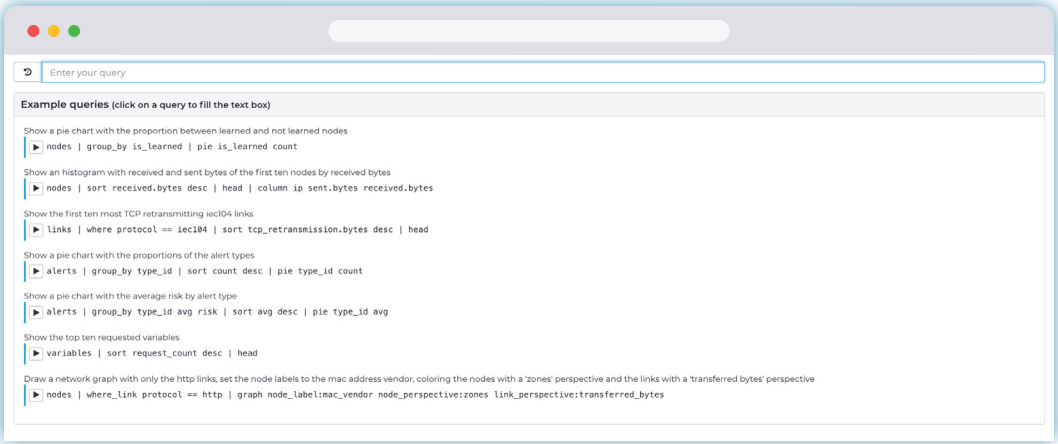


Figure 20 - The Nozomi Networks Query Tool Provides Answers to Real-time Network and Risk Questions

Finally, when a new malware is reported, and Yara rules for it are released, operators can use Guardian to see if their systems have been infected.

```
/* Rule Set ----------------------------------------------------------------- */

rule Industroyer_Malware_1 {
   meta:
      x_timestamp = "1497312000000"
      description = "Detects Industroyer related malware"
      author = "Florian Roth"
      reference = "https://goo.gl/x81cSy"
      date = "2017-06-13"
      hash1 = "ad23c7930dae02de1ea3c6836091b5fb3c62a89bf2bcfb83b4b39ede15904910"
      hash2 = "018eb62e174efdcdb3af011d34b0bf2284ed1a803718fba6edffe5bc0b446b81"
   strings:
      $s1 = "haslo.exe" fullword ascii
      $s2 = "SYSTEM\\CurrentControlSet\\Services\\%ls" fullword wide
      $s3 = "SYS_BASCON.COM" fullword wide
      $s4 = "*.pcmt" fullword wide
      $s5 = "*.pcmi" fullword wide

      $x1 = { 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 73
         00 5C 00 25 00 6C 00 73 00 00 00 49 00 6D 00 61
         00 67 00 65 00 50 00 61 00 74 00 68 00 00 00 43
         00 3A 00 5C 00 00 00 44 00 3A 00 5C 00 00 00 45
         00 3A 00 5C 00 00 00 }
      $x2 = "haslo.dat\x00Crash"
   condition:
      ( uint16(0) == 0x5a4d and filesize < 200KB and 1 of ($x*) or 2 of them )
}

rule Industroyer_Malware_2 {
   meta:
      description = "Detects Industroyer related malware"
      author = "Florian Roth"
      reference = "https://goo.gl/x81cSy"
      date = "2017-06-13"
      hash1 = "3e3ab9674142dec46ce389e9e759b6484e847f5c1e1fc682fc638fc837c13571"
      hash2 = "37d54e3d5e8b838f366b9c202f75fa264611a12444e62ae759c31a0d041aa6e4"
      hash3 = "ecaf150e087ddff0ec6463c92f7f6cca23cc4fd30fe34c10b3cb7c2a6d135c77"
      hash1 = "6d707e647427f1ff4a7a9420188a8831f433ad8c5325dc8b8cc6fc5e7f1f6f47"
   strings:
      $x1 = "sc create %ls type= own start= auto error= ignore binpath= \"%ls\" displayname= \"%ls\"" fullword wide
```

Figure 21 - Using a New Yara rule for the Industroyer Malware

5. Enabling Enterprise OT and IoT Risk Monitoring

5.1 High Performance and Scalability for Large Distributed Installations

Many critical infrastructure and industrial organizations span multiple sites across a large geographical area. Effective OT and IoT security monitoring for these situations requires enterprise-class capabilities.

The Nozomi Networks Central Management Console (CMC) provides consolidated and remote access to ICS data from field-deployed Guardian sensors. It readily scales to monitor hundreds of industrial facilities and thousands of assets with optimal performance. Custom, hierarchical aggregations are used to amalgamate cybersecurity and operational data to meet the needs of each organization.

Additionally, the CMC's multitenant and high availability capabilities are ideal for global customers with multiple business units. It is also the solution of choice for Managed Security Service Providers (MSSPs). (See a Sample Deployment Architecture in Figure 1 on page 3.)

The CMC provides broad ICS network visibility within a single tool with "at-a-glance" summaries. It consolidates threat and risk detection from distributed locations and enables real-time queries of any aspect of network or process status. Furthermore, it often eliminates the need for onsite data collection for compliance reporting.

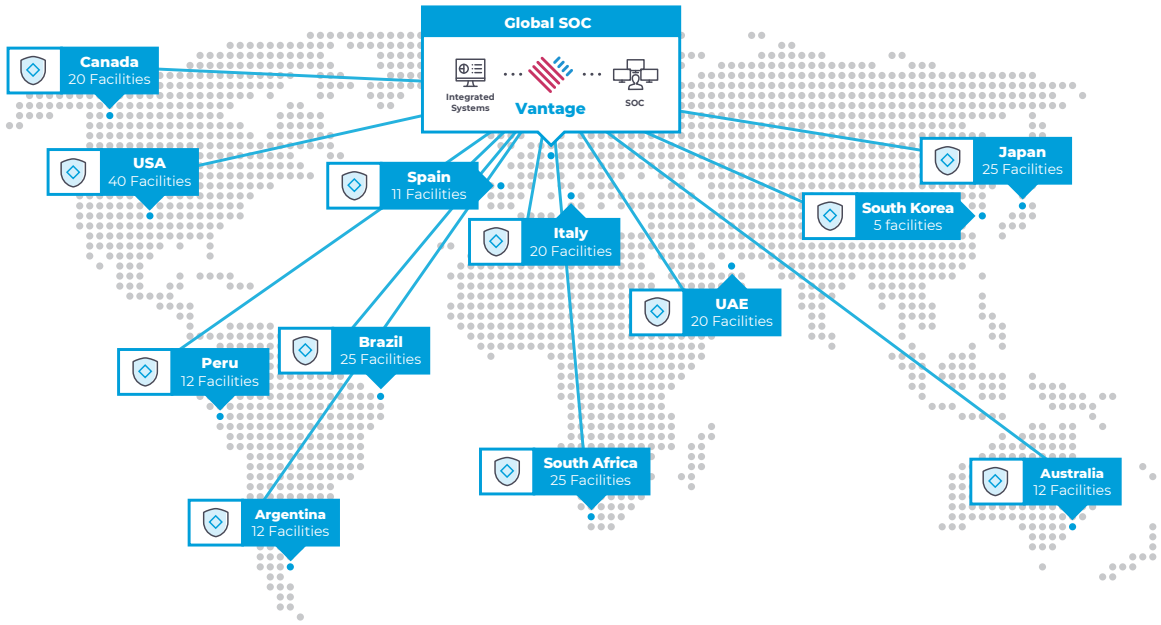


Figure 22 - Sample Deployment Map

5.2 Designed for Industry Skill Levels and Best Practices

In any large industrial organization there are many job functions that include responsibility for cybersecurity and availability. The Nozomi Networks solution is designed for ease-of-use, and has been shown to increase productivity for roles as diverse as onsite control engineers to SOC cybersecurity experts. It helps employees be more effective while leveraging their existing skill sets, rather than requiring them to acquire special analyst skills.

The Nozomi Networks solution also supports the security best practice of segregation of duties through the creation of granular permissions and restrictions. User roles can be defined to restrict functionality and network visibility, limiting insider risks. The tables below show an example of how this could be applied in a large electricity utility.

Group	Description
Super-Admin	This is a privileged account for performing system administrative tasks such as implementation, commissioning and emergency activities. It should not be used by production personnel for everyday duties.
Local-Admin (e.g. South Area)	Like the role described above, but for a limited part of the system infrastructure.
Industrial System Operator (e.g. South Area)	For personnel whose primary function is to operate and monitor the energy transmission and distribution process. This account is used to assess performance and efficiency, and to ensure safety.
Network Engineer (e.g. Site A)	This account is used by personnel who design and manage network devices. It includes communication within the industrial network and between different networks.
Cyber Security Analyst	Used by people who assess the cyber resilience of the environment and perform mitigations. They also monitor for cyberattacks and cyber incidents and perform incident investigations.
Auditor	For personnel whose primary function is to perform regular audits to evaluate the industrial environment and its compliance with internal and external standards.

Figure 23 - Example User Groups for a Large Electricity Utility

Permission	North Substations			South Substations		CMC
	Site A	Site B	Site C	Site D	Site E	
Query and Export	● ●	●	●	● ● ●	● ● ●	● ● ●
Trace Requests	● ●	●	●	● ●	● ●	●
Link Events	● ●	●	●	● ●	● ●	●
Captured URLs	● ●	●	●	● ●	● ●	●
Alerts	●	●	●	● ●	● ●	● ●
Traffic	● ●	●	●	● ●	● ●	●
Performance	●	●	●	● ●	● ●	●
Process View	●	●	●	● ● ●	● ● ●	●
Time Machine	●	●	●	● ●	● ●	● ●
Dashboard Configuration	●	●	●	● ● ●	● ● ●	●
System Configuration	●	●	●	● ●	● ●	●

Figure 24 - Example of Permissions by Site for a Large Electricity Utility

5.3 Fast, Flexible Deployment for Immediate ROI

Typical deployment times for OT and automation applications are measured in months and even years. The Nozomi Networks solution, by contrast, is implemented in days and delivers immediate value. Most customers rapidly discover assets and links they did not know exist and some, unfortunately, are immediately made aware of the presence of malware in their industrial networks.

Nozomi Networks products come in a wide range of formats to meet the needs of any organization. For example, Guardian is available in 10 physical sensors which vary by form factor, monitoring ports and maximum throughput. This includes two ruggedized sensors (one DIN-rail mount and one rack mount), multiple rack-mounted sensors, and a portable sensor. This product line is also available in four

virtual sensors, and Guardian with Smart Polling is available as a container sensor.

Smart Polling is also available as an embedded container application for switches, routers and other security infrastructure.

The CMC is available as a physical, virtual, or cloud appliance for Microsoft Azure and Amazon AWS cloud platforms that includes hierarchical and multitenant installation options.

All products are completely self-contained, full technology stack solutions that can be installed on any operating system. For complete deployment option details, visit **nozominetworks.com/techspecs**.

5.4 Easy IT/OT Integration for a Complete Solution

It is easy to integrate Guardian and the CMC with other applications that are part of security, IT, IoT and OT infrastructure. The products have built-in support for many asset management systems, firewalls, identify management systems, ticketing systems, SIEMs and more. They also exchange data with other IT/OT applications through an open API.

Additionally, the Protocol SDK (Software Development Kit) extends support for protocols beyond the dozens already supported.

What to Look for in an OT and IoT Security and Visibility Solution

Technology advancements, such as those found in the Nozomi Networks solution, can dramatically improve security and reliability.

When choosing a solution, look for the following characteristics:

- Comprehensive visibility of all assets in your network
- Advanced threat detection
- Accurate anomaly alerts
- Proven scalability
- Easy IT/OT integration
- Global partner ecosystem
- Exceptional customer engagement and support

See the Nozomi Networks Solution in Action

If you would like to see our solution in action, and experience how easy it is to work with Nozomi Networks, please contact us at **nozominetworks.com/contact**

Contact Us

Want to Know More?



DATA SHEET
Vantage

DOWNLOAD



DATA SHEET
Guardian

DOWNLOAD



DATA SHEET
Central Management Console

DOWNLOAD



DATA SHEET
Threat Intelligence

DOWNLOAD



DATA SHEET
Asset Intelligence

DOWNLOAD

6. References

1. **"Global Risks Report,"** World Economic Forum, 2020.
2. **"SANS 2019 State of OT/ICS Cybersecurity Survey,"** SANS Institute, June 11, 2019.
3. **"Securing Industrial Control Systems – 2017,"** SANS Institute, June 2017.

NOZOMI NETWORKS

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.

© 2022 Nozomi Networks, Inc.
All Rights Reserved.
NN-SOL-WP-8.5x11-006

nozominetworks.com