NOZOMI NETWORKS

WHITE PAPER

Advancing ICS Visibility and Cyber Security with the Nozomi Networks Solution

July 2019

Table of Contents

Introduction

A Simple Way to Secure Industrial Networks and Improve Resilience

The Nozomi Networks solution improves reliability for industrial control systems. It does this by providing superior network and asset visibility and by rapidly identifying cyber security and process risks. It significantly reduces industrial control system (ICS) monitoring and threat response efforts and results in improved availability and cyber resiliency.

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:

> [A] growing trend is the use of cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning.
>
> **World Economic Forum, The Global Risks Report 2018**[1]

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

> Monitored in real-time for process and security anomalies to enhance visibility and improve asset control.
>
> **SANS Institute, Securing Industrial Control Systems — 2017**[2]

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

1 Improving Network and Operational Visibility for ICS

I. How ICS Security Differs from IT Security

Providing visibility and security to industrial networks is not simply a matter of implementing IT tools and practices. Unique ICS 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.

Cyber security 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.

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

Industrial Protocols

ICS 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.

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

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 tracks all types of assets & networks.

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

II. Overview of the Nozomi Networks Solution

Nozomi Networks provides the ideal ICS cyber security and visibility solution because it is designed with a thorough understanding of industrial networks and processes. With one solution, industrial asset owners gain advanced cyber security, improved operational reliability and easy IT/OT integration.

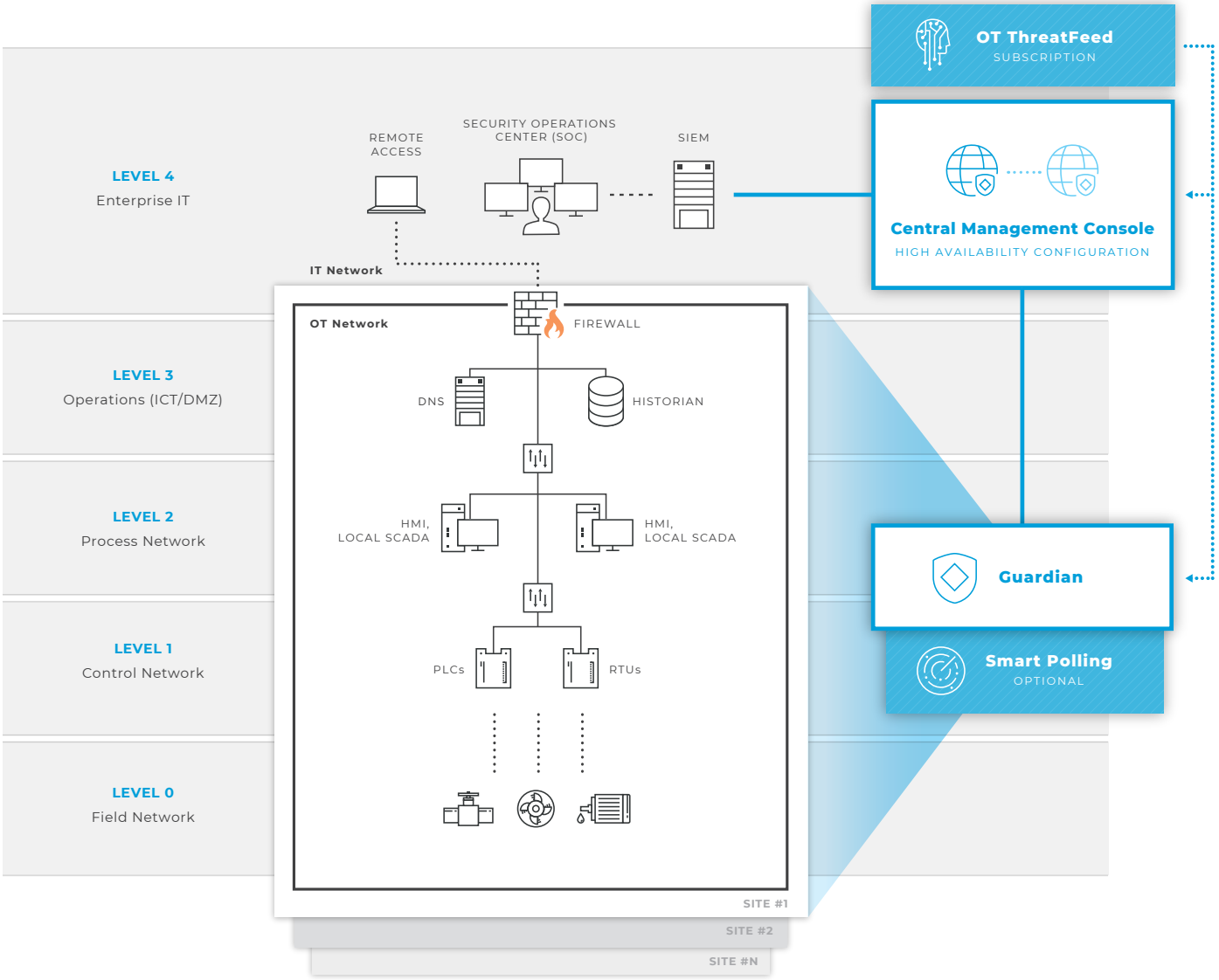


Figure 1 - Sample Deployment Architecture

Shown above is a general example of how the Nozomi Networks solution can be deployed.

A wide variety of appliances, a flexible architecture, and integrations with other systems allow us to provide a solution tailored to meet the needs of your organization.

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

Nozomi Networks Products and Services

Guardian™ provides complete visibility and cyber security for ICS environments by combining asset discovery, vulnerability assessment, threat detection, and anomaly detection in a single, unified solution.

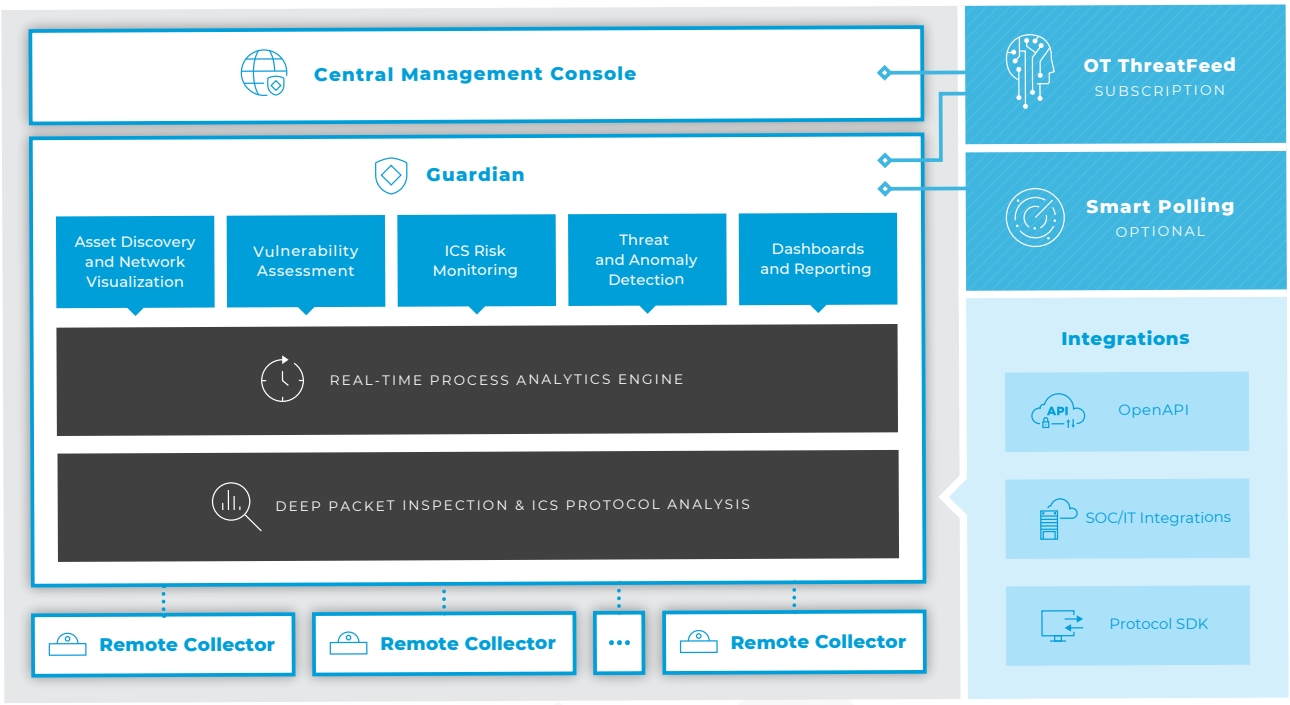
Central Management Console™ **(CMC)** enables centralized security visibility and management for multi-tier, distributed OT deployments across the world.

Smart Polling™, an add-on module to Guardian, uses low volume, active technologies to provide complete asset inventory, exact vulnerability assessment and advanced ICS security monitoring.

Nozomi Networks Labs reduces cyber risk for industrial and critical infrastructure organizations through research and collaborative contributions to the ICS security community.

The Labs team also produces threat and vulnerability updates for OT ThreatFeed.

Nozomi Networks Solution Architecture



The award winning Nozomi Networks solution improves cyber resiliency and reliability via a modular, extensible and scalable architecture.

III. Network Visualization Improves Situational Awareness and Speeds Troubleshooting

For far too long, industrial operators and cyber security staff have faced the impossible task of attempting to manage and monitor a system that was not thoroughly documented or easy to visualize.

As soon as the Nozomi Networks solution starts analyzing the network traffic of an ICS, 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 ICS 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.

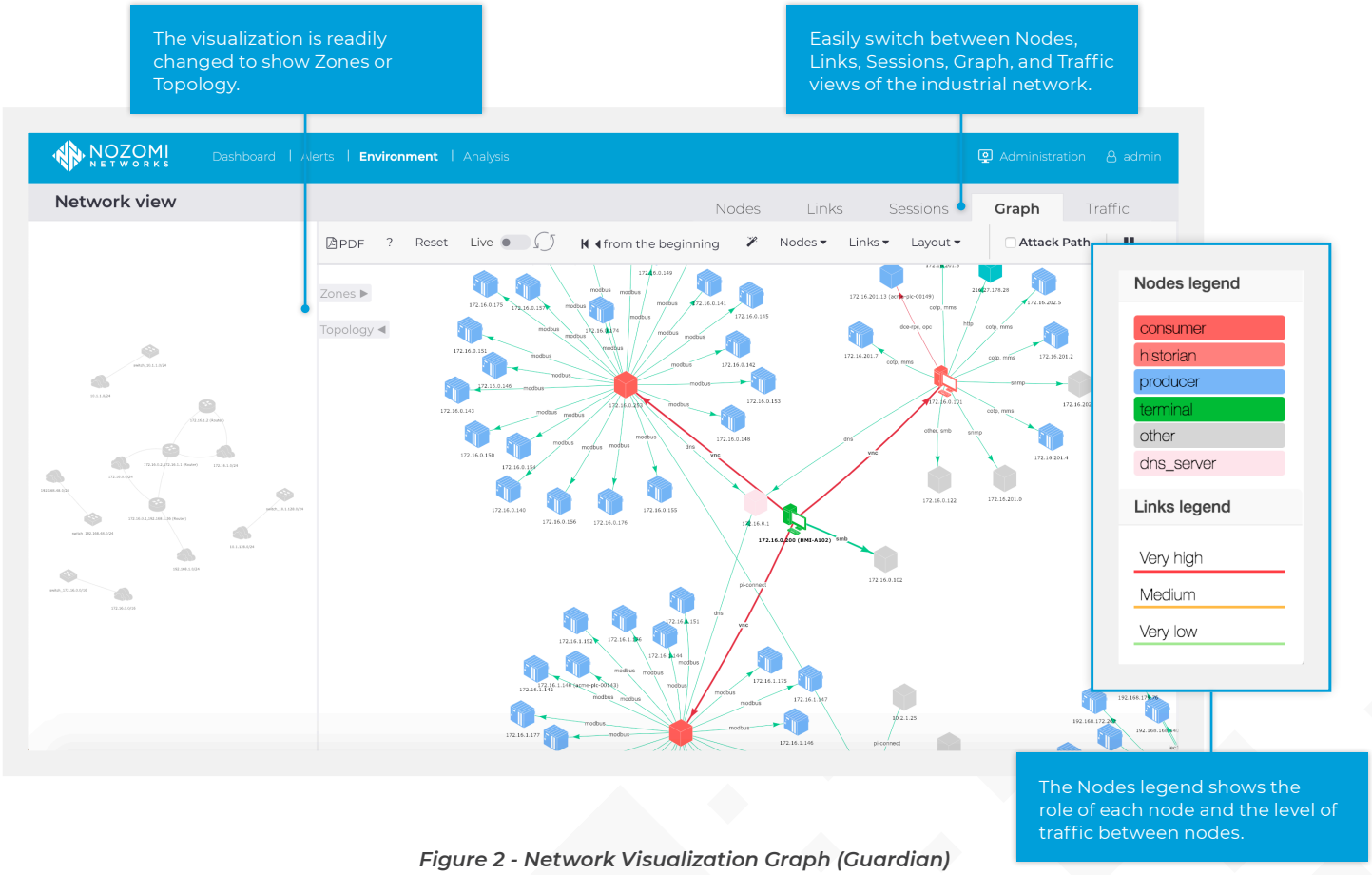


Figure 2 - Network Visualization Graph (Guardian)

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 control network (Only a portion is shown in the screen shot; in actual use, the operator can zoom in and out to see the desired level of detail.)
- The ability to navigate and filter by different subnets and network segments.
- The ability to drilldown on any endpoint or connection to see detailed attributes.

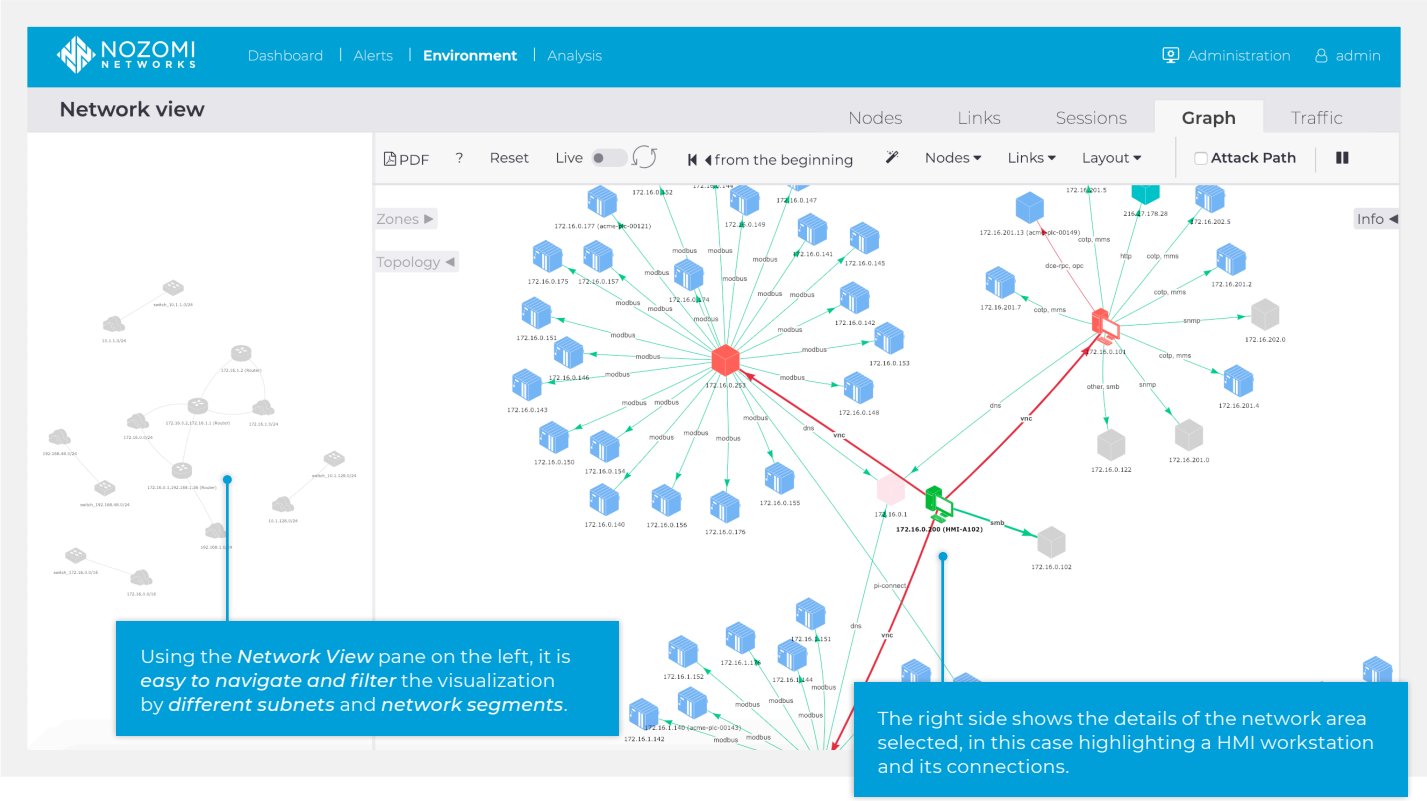


Figure 3 - Network Visualization: Topology (Guardian)

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 cyber security and reliability risk.

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 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, when 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

enel

"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
Multinational energy company

IV. Superior Asset Inventory Enhances Cyber Security and Saves Time

Developing and maintaining a centralized OT system inventory is a very difficult and time-consuming project. Guardian dramatically 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 of 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

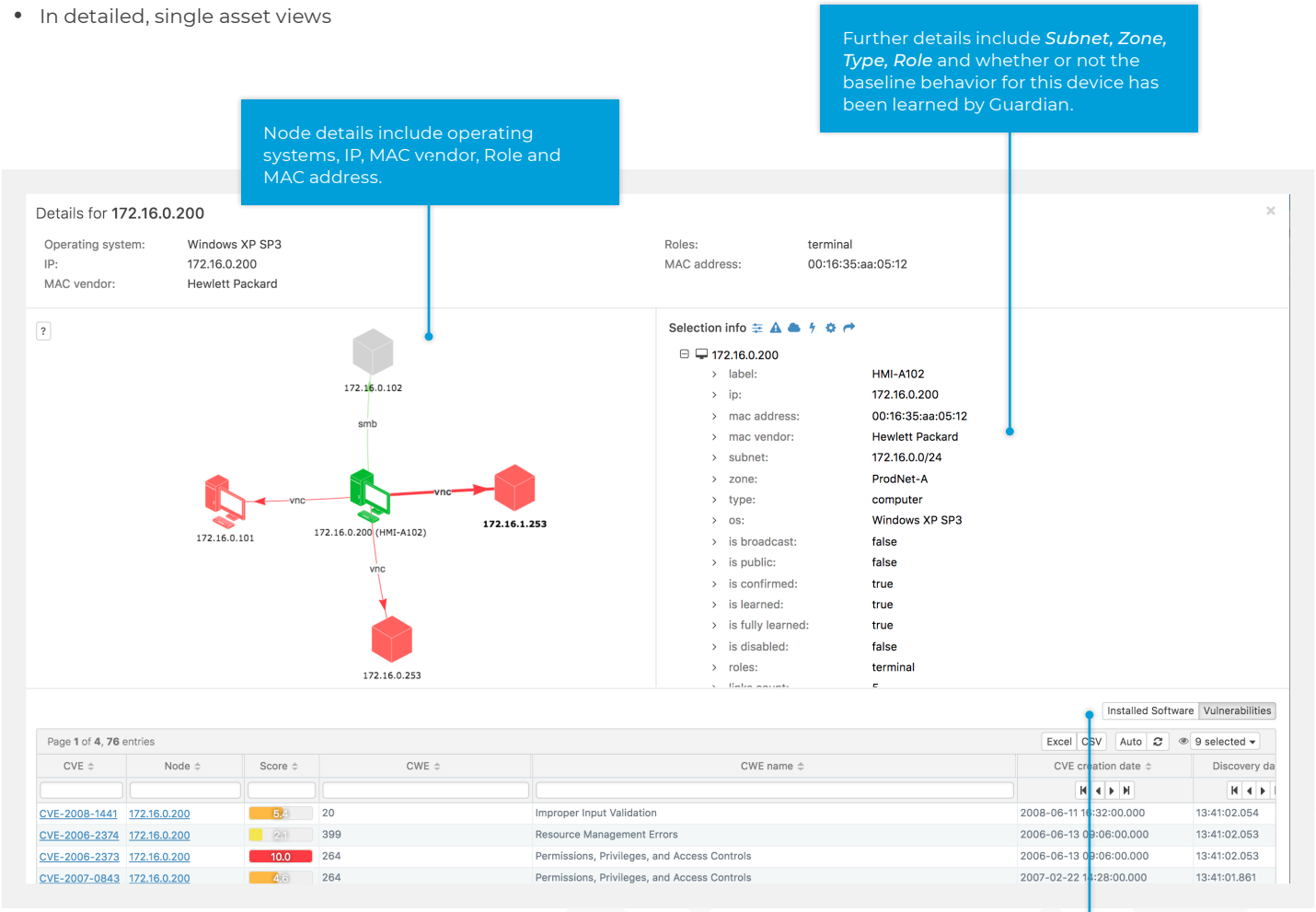


Figure 4 - Network Node Detail Screen (Guardian)
The amount of information shown for each node is extensive and includes vulnerabilities and installed software.

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 cyber security 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 cyber security and risk information provided by a solution.

In comparison with other passive ICS 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.

V. 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 ICS. 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.

VI. Deep Protocol Support Recognizes Improper Communications

When learning an ICS, Guardian analyzes communications utilizing its extensive understanding of dozens of ICS 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 Inspection2 (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.

VII. Vulnerability Assessment Helps Manage Risk Exposure

Another challenging aspect of ICS security and process reliability is knowing which devices are vulnerable and require updates or special protection. For example, engineering and cyber security 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 OT ThreatFeed. 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 resiliency.

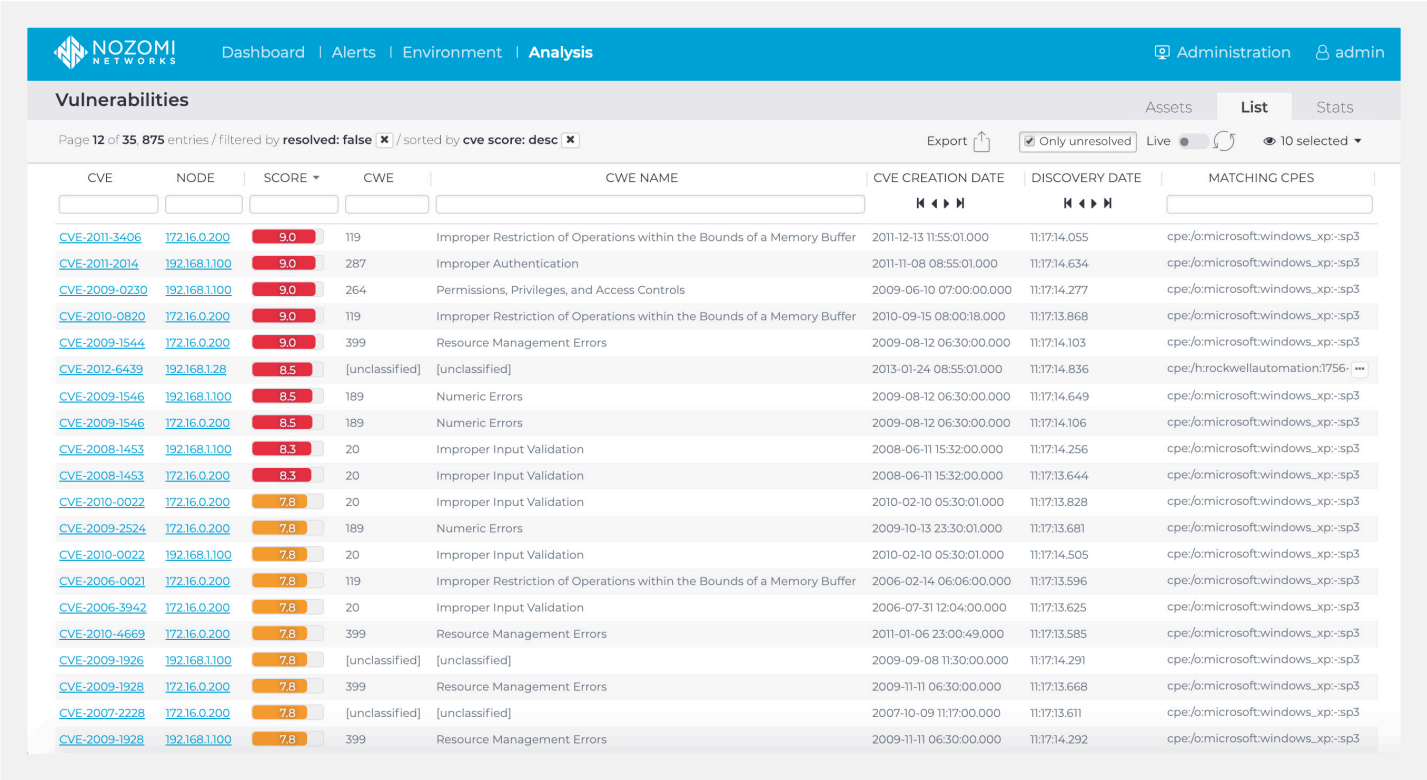


Figure 5 - List of Vulnerabilities by Severity Level (Guardian)
Shown above are the vulnerabilities present on a facility's industrial assets.

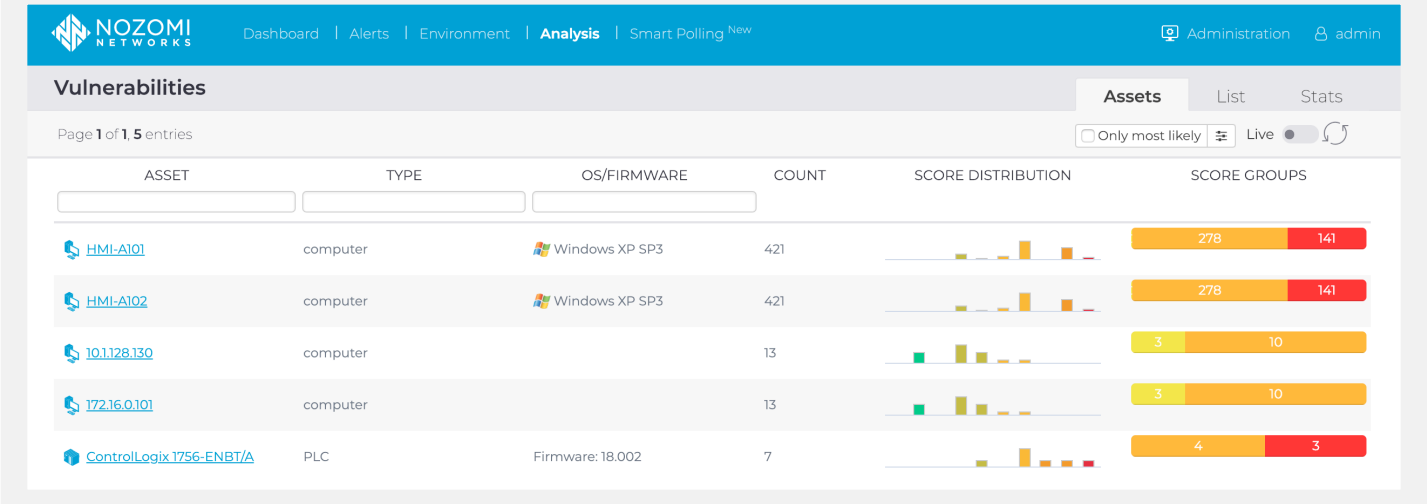


Figure 6 - List of Assets with Confirmed Vulnerabilities (Guardian with Smart Polling)

VIII. 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.

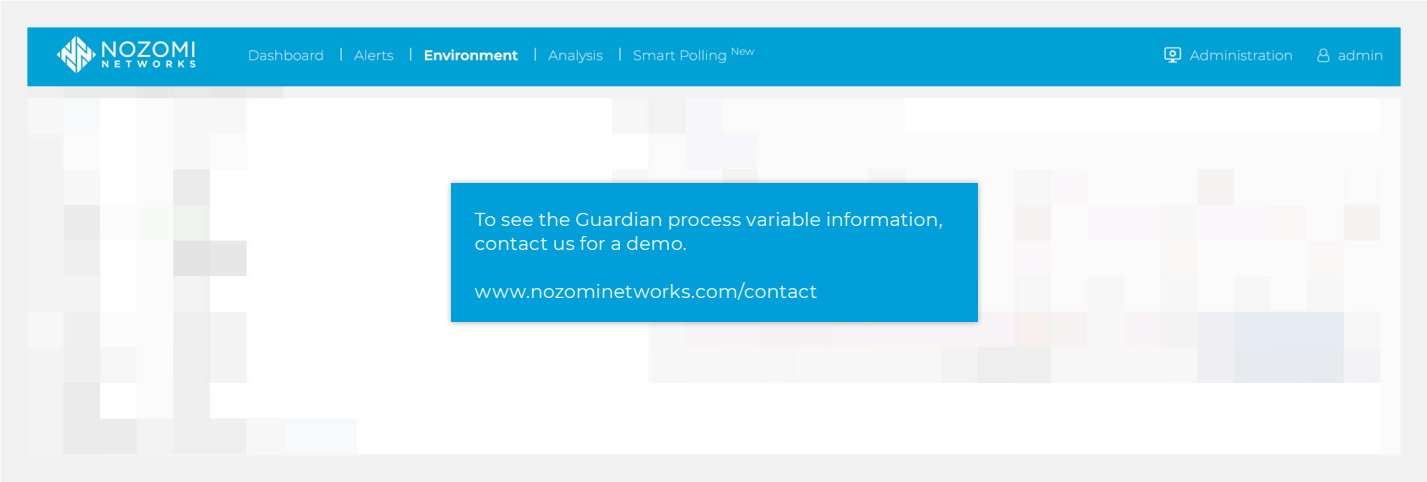


Figure 7 - Process Variable Detail Screen

Guardian's Process Views and Alerts

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

Alerts for example, 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).

IX. 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 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 cyber security 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.

X. Dashboards and Queries Enhance Risk Management and Staff Productivity

Dashboards Summarize OT Risks

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 ICS 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.

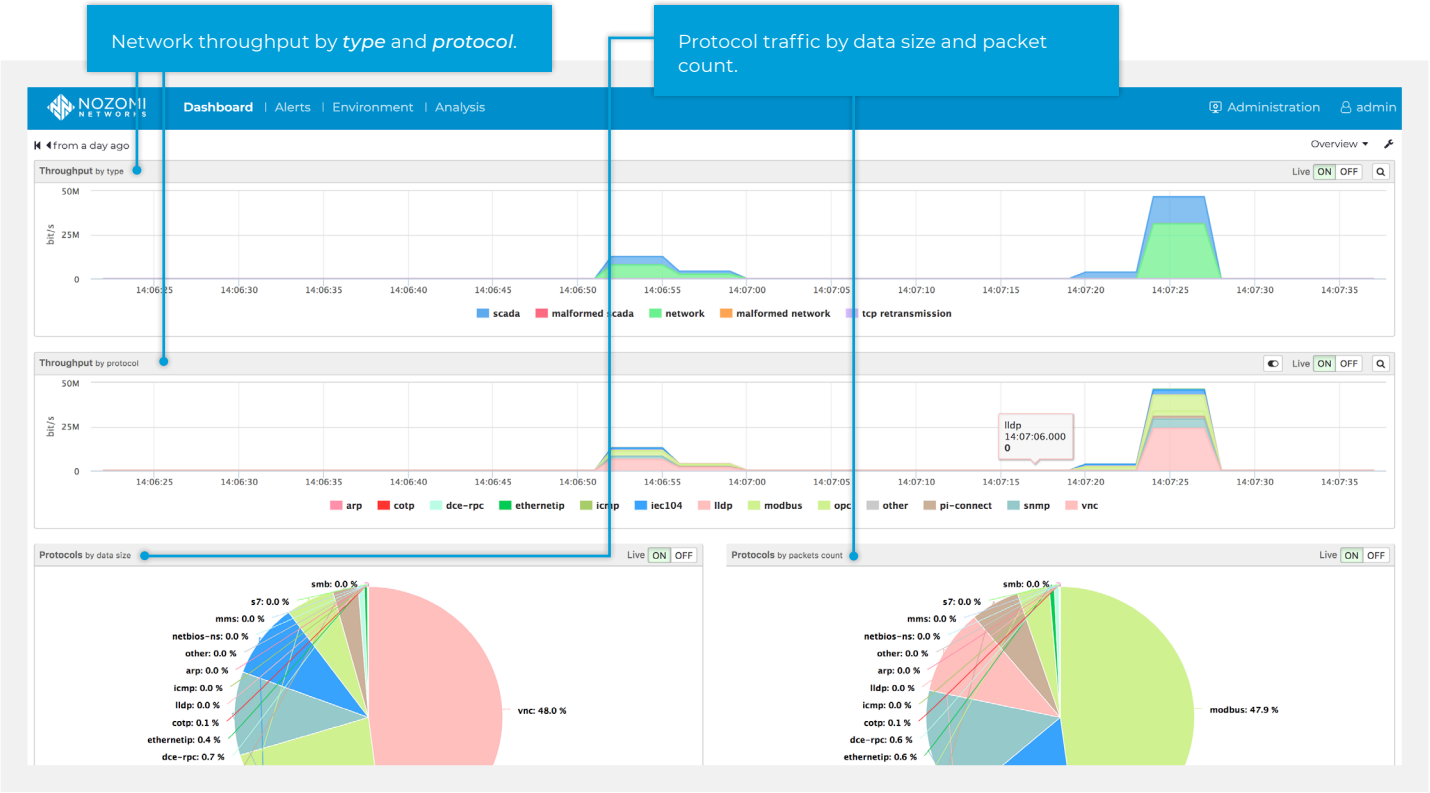


Figure 9 – Dashboard Showing Real-time Network Throughput (Guardian)

The high amount of VNC traffic might be normal or alarming, depending on the industrial network.

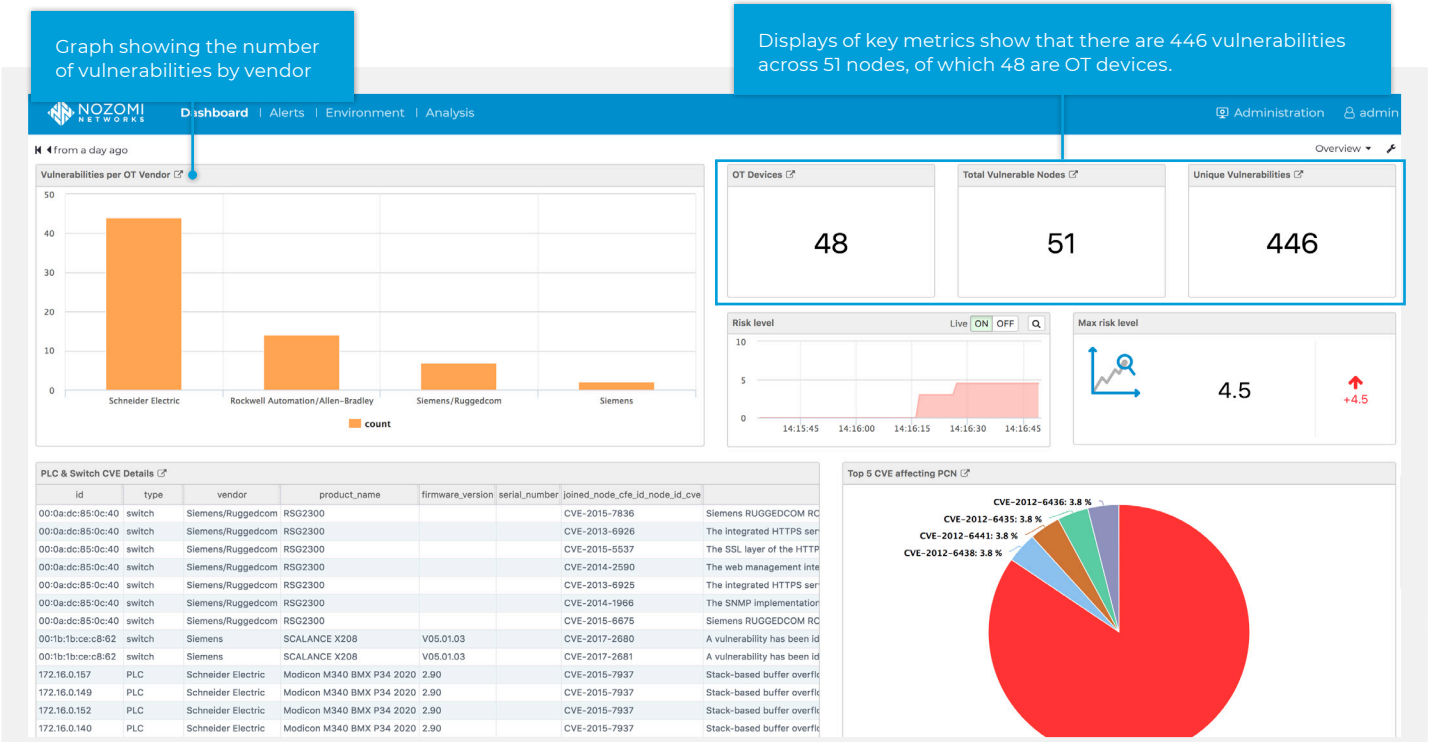


Figure 10 - Dashboard Showing Key Vulnerabilities Metrics (Guardian)

Using this data, vulnerability work can be prioritized, maximizing cyber resiliency enhancements per work hour of effort.

Queries Answer Real-time ICS 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 ICS performance.

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

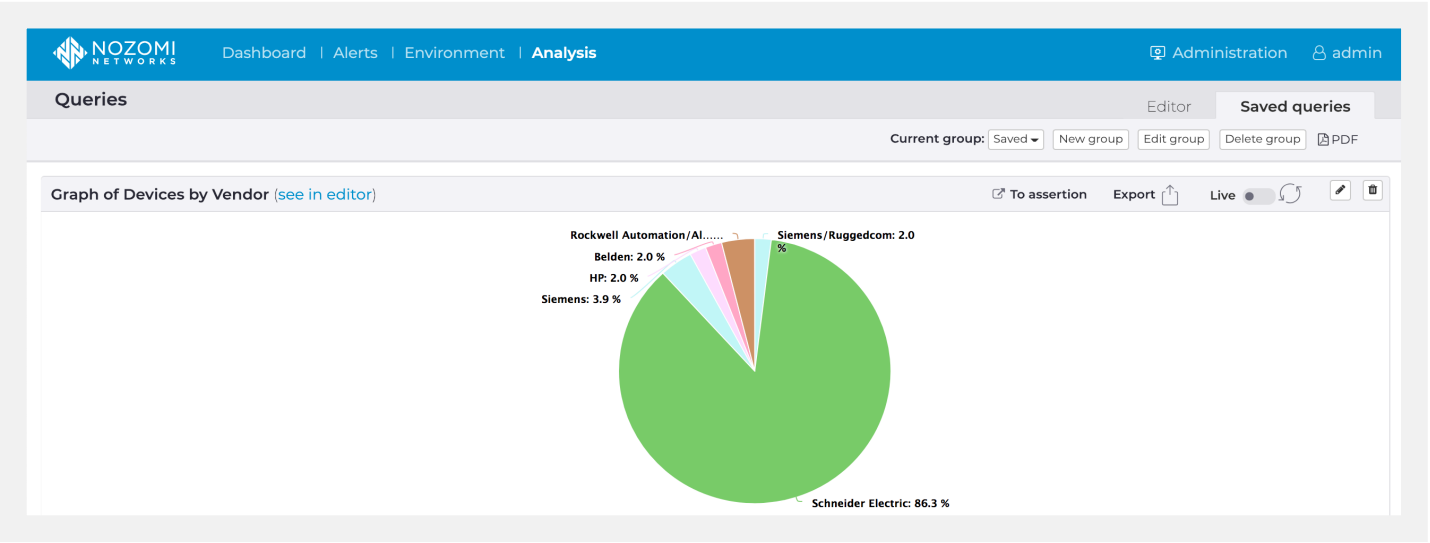


Figure 11 – Query Result Showing a Graph of Device Vendors
This widget can be included in dashboards, reports and API queries.

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.

Nozomi Networks Customer Efficiently Checks for IOCs

"I've also added IOCs [indicators of compromise] 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

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.

2 Detecting ICS 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 OT ThreatFeed. 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.

I. Hybrid Threat Detection for Best-in-Class ICS Cyber 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 ICS virtual image of an industrial installation, which serves as a logical and comprehensive model of its physical processes and network deployment. Then it uses:

- advanced industrial network behavioral analytics
- artificial intelligence (AI) techniques, and
- continuous real-time assessment

to rapidly identify anomalies and correlate them with process data readings.

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 cyber security context. Guardian correlates STIX indicators with other information to assess and alert on threats.

OT ThreatFeed

Guardian includes a limited set of rules out-of-the-box that help detect some commonly known threats. By adding the OT ThreatFeed subscription, you'll receive a more comprehensive ruleset that is updated on a regular basis, providing the latest threat information.

OT ThreatFeed makes it easy to stay on top of current ICS threats and vulnerabilities without the cost and complexity of maintaining multiple tools. If, after an update, threats or vulnerabilities are identified, alerts are immediately generated.

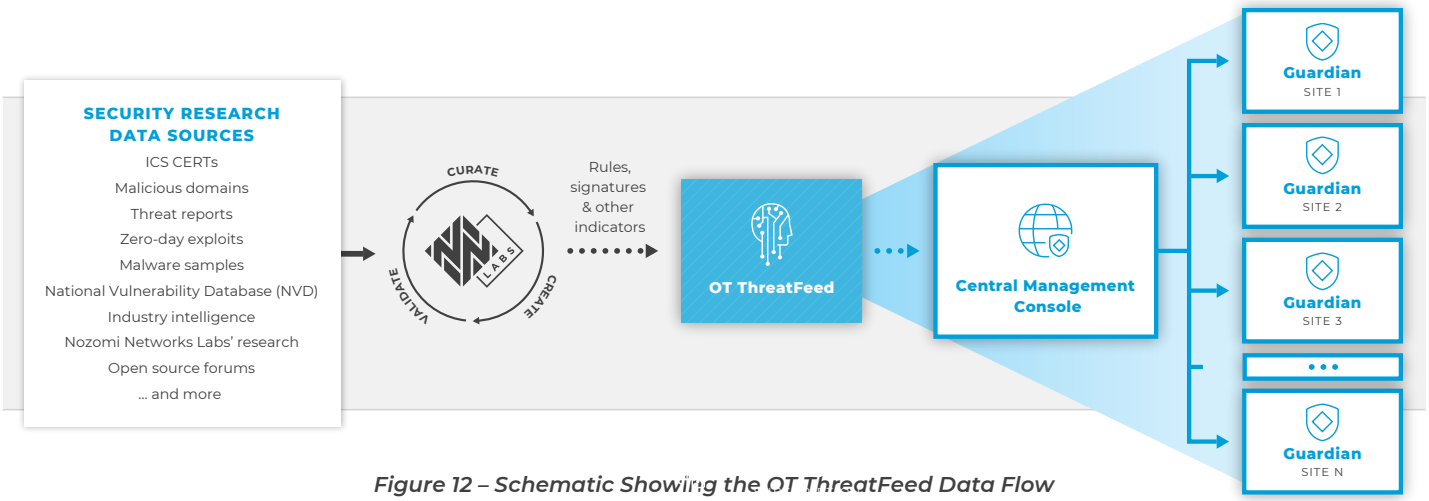


Figure 12 – Schematic Showing the OT ThreatFeed Data Flow

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 3.

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 ICS malware, as shown below.

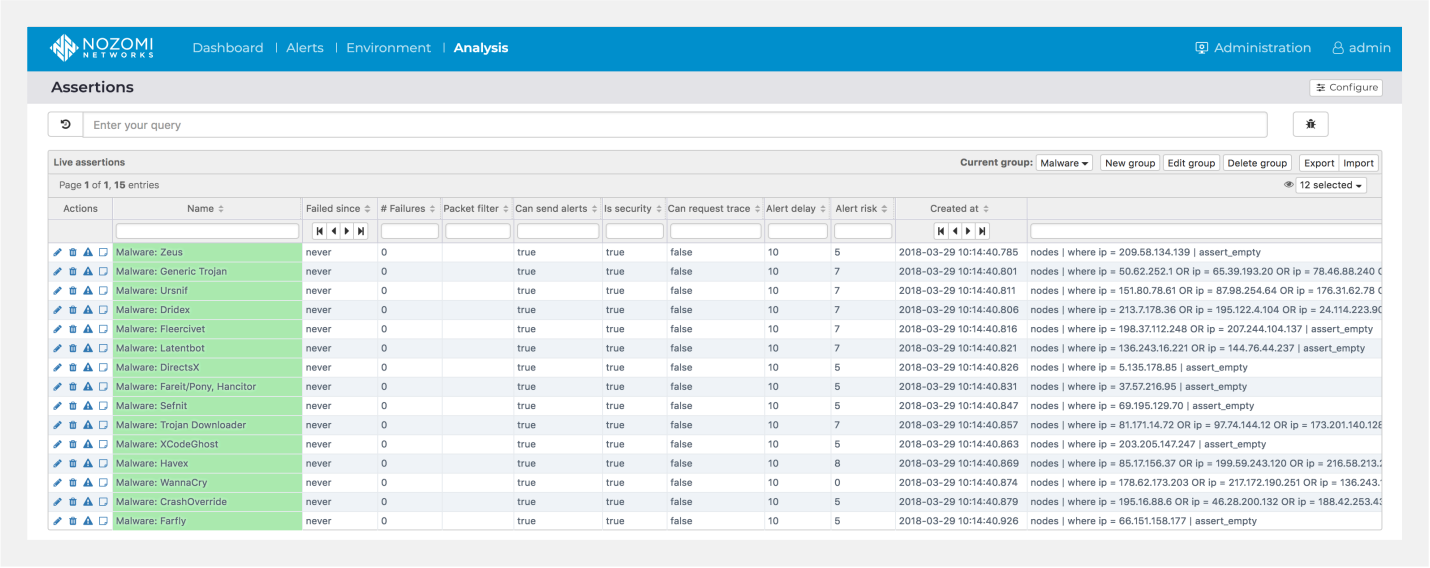


Figure 13 - List of Assertions that Check for Malware Communications with External Servers
If such communication occurs it indicates a compromise and requires an immediate response. In such a case the assertion automatically triggers an urgent alert.

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.

II. OT Risk Management for Proactive Security and Reliability

Identifying Network Risks for Ongoing Improvements to Cyber Resiliency

The Nozomi Networks solution proactively identifies risks that threaten the cyber security and reliability of industrial networks. Identifying these risks and scoring them helps operators act to improve cyber resiliency 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 cyber security 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.

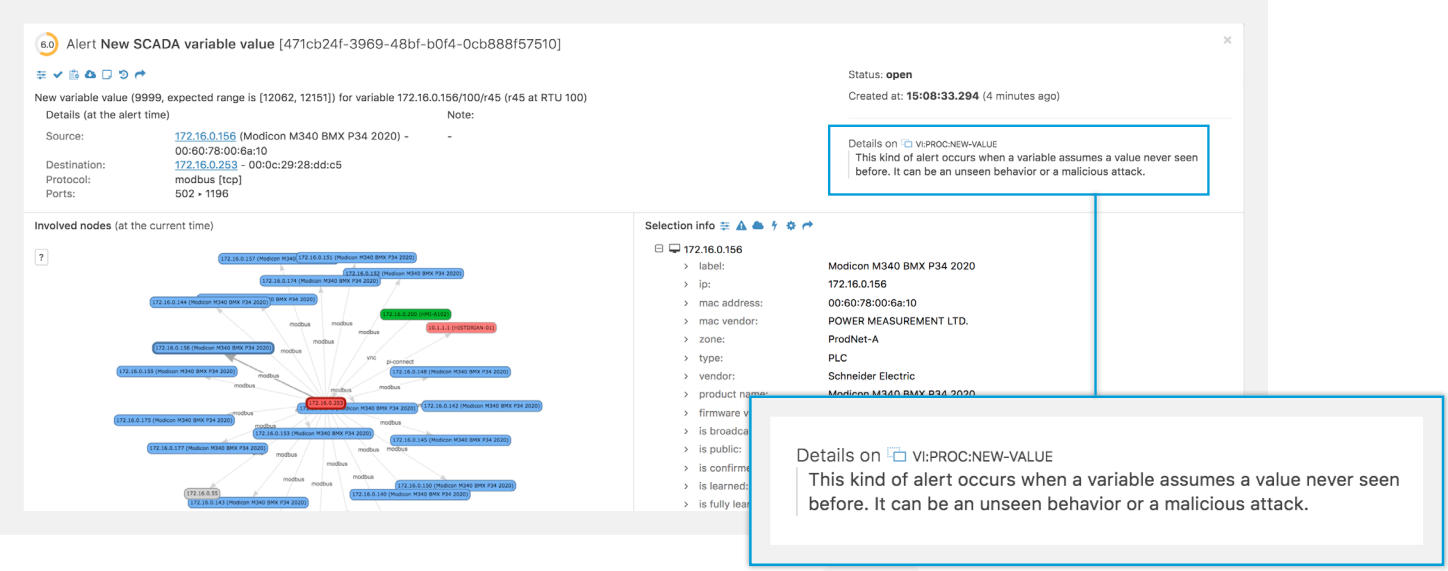


Figure 14 – Alert for a New SCADA Variable Value

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.

Guardian *automatically captures PCAPs* related to the alert and they can be downloaded.

Further clicking on the variable link, takes you to a *Process View* that includes a *graph of the variable's behavior over time*.

Figure 15 – Analyzing a Process Anomaly by Investigating Related Details

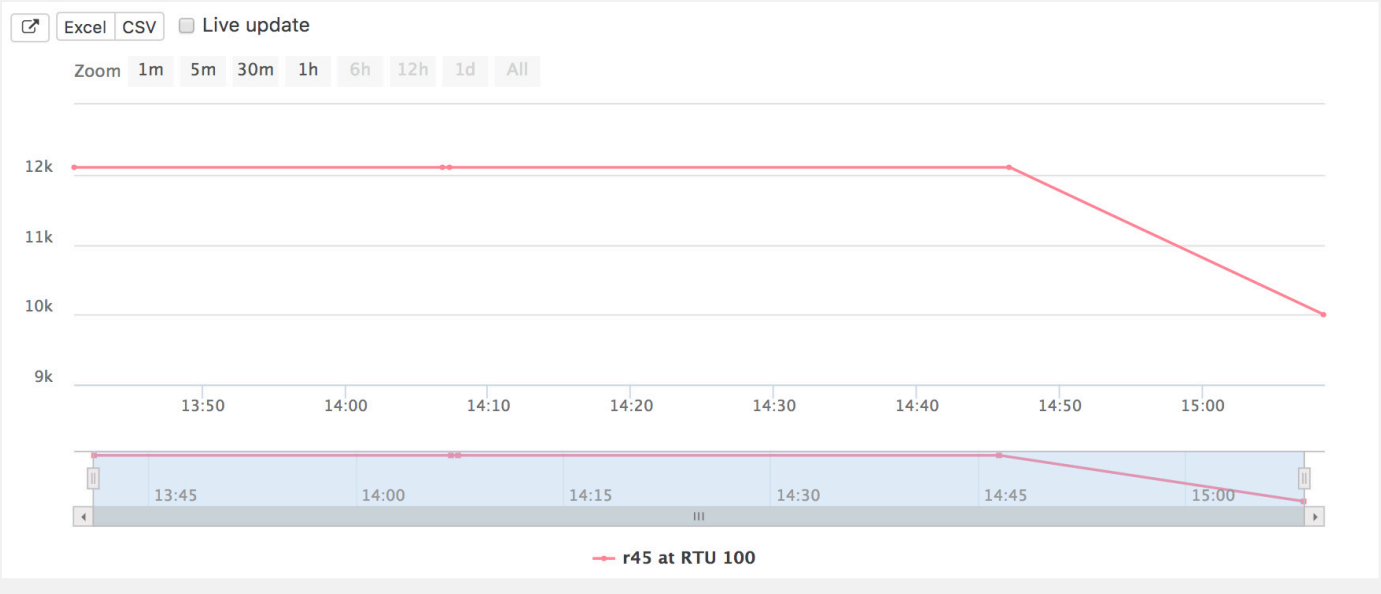


Figure 16 – Process Variable Graph

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 3.

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

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.

III. 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.

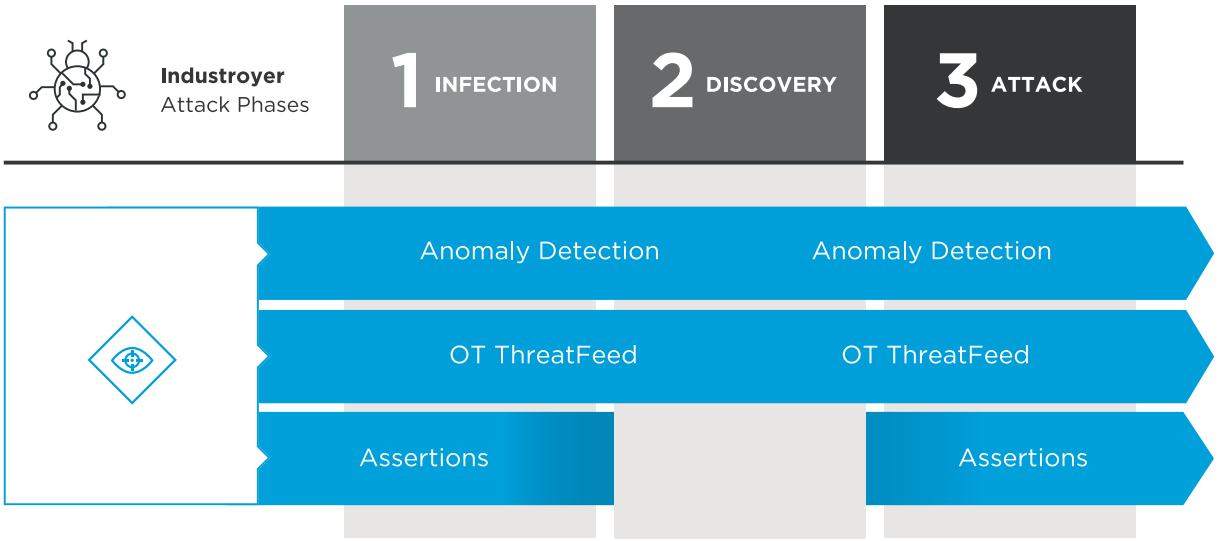


Figure 17 - Industroyer Attack Phases

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, OT ThreatFeed 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 included in OT ThreatFeed.

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).

> *"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**

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

IV. 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)

V. 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**.

3 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.

I. 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 ICS 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' (x's for further anonymization)."*

Alerts are grouped into a dozen types of context-aware incidents using a powerful correlation engine. The result is that operators or cyber security 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[3], 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.

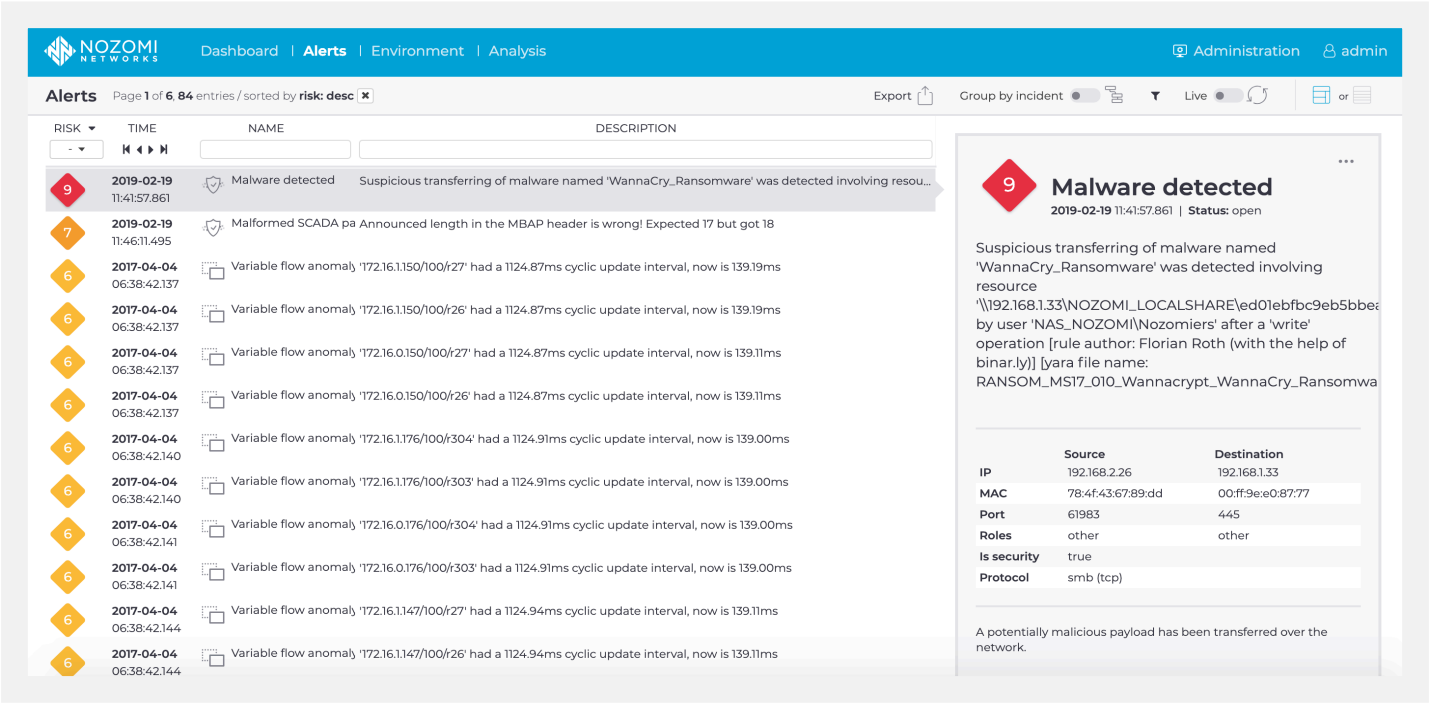


Figure 18 - The Guardian Incident / Alert View

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

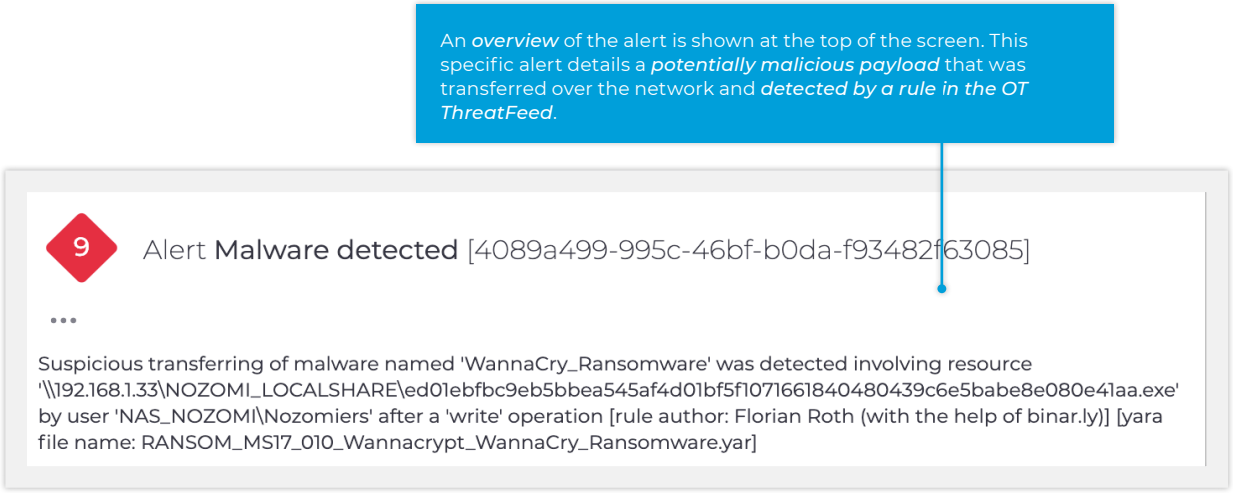


Figure 19 – Drilling Down on the Critical Incident shows Individual Alerts and Key Details that Enable Rapid Response

II. 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 ICS 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.

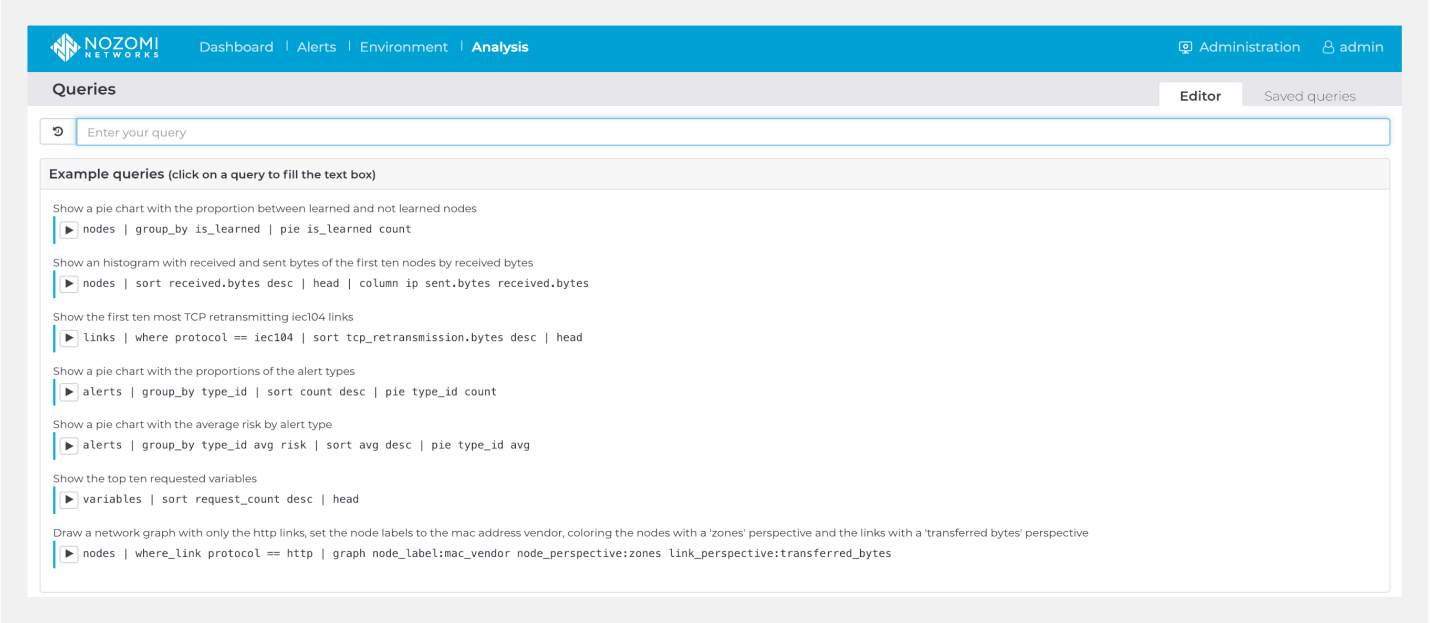


Figure 20 - The Nozomi Networks Query Tool Provides Answers to Real-time Network and Risk Questions

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)*.

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.

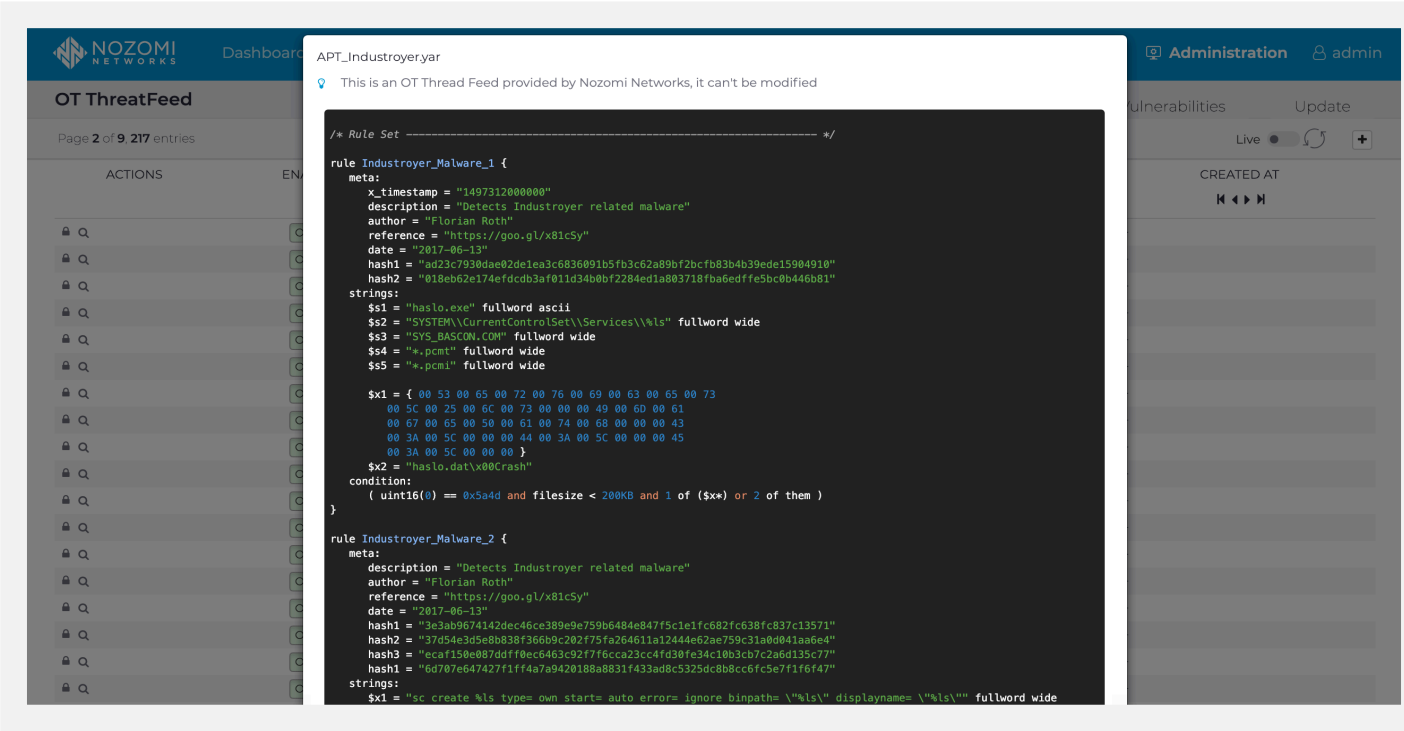


Figure 21 - Using a New Yara rule for the Industroyer Malware

4 Enabling Enterprise OT Risk Monitoring

I. High Performance and Scalability for Large Distributed Installations

Many critical infrastructure and industrial organizations span multiple sites across a large geographical area. Effective ICS cyber 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 appliances. It readily scales to monitor hundreds of industrial facilities and thousands of assets with optimal performance. Custom, hierarchical aggregations are used to amalgamate cyber security 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.

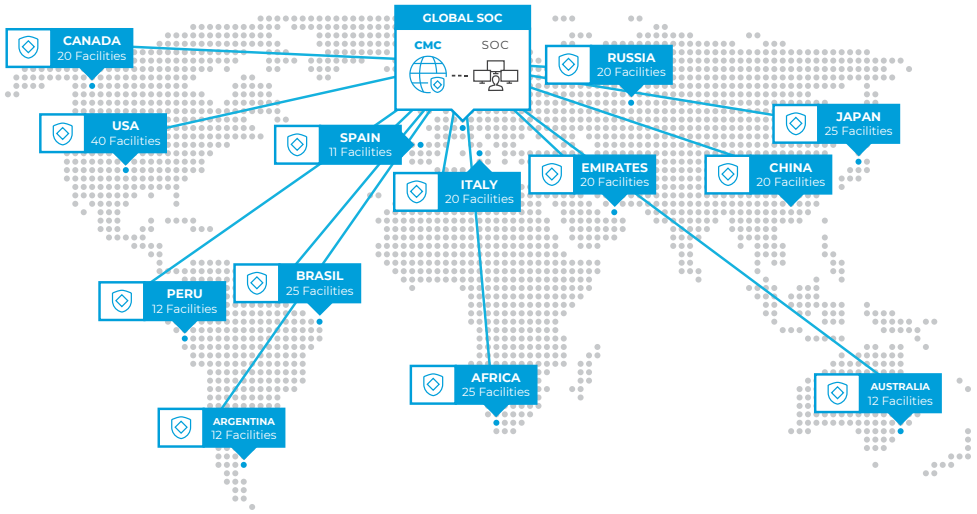


Figure 22 - Sample Deployment Map

II. Designed for Industry Skill Levels and Best Practices

In any large industrial organization there are many job functions that include responsibility for cyber security 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 cyber security 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.

Example of Segregation of Duties Implemented with Guardian

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 (i.e. South Area)	Like the role described above, but for a limited part of the system infrastructure.
Industrial System Operator (i.e. 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 (i.e. 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

	North Substations			South Substations		CMC
Permissions	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

III. Fast, Flexible Deployment for Immediate ROI

Typical deployment times for ICS 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 six physical appliances which vary by form factor, monitoring ports and maximum throughput. This includes a ruggedized, DIN-rail mounted appliance, multiple rack-mounted appliances, and a portable appliance. This product line is also available in four virtual appliances, and Guardian with Smart Polling is available as a container appliance.

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

The CMC is a virtual appliance 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**.

IV. 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 or ICS 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/ICS 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 a Real-time ICS Visibility and Cyber Security Solution

Digitization and connectivity has greatly increased cyber risk for critical infrastructure and manufacturing organizations. And, while cyberattacks dominate the news, there is reason to be optimistic.

New technology, such as the Nozomi Networks solution is easy and safe to deploy, dramatically improves OT cyber security and integrates seamlessly with IT infrastructure.

When choosing a cyber security solution and vendor for your organization, make sure they have the advantages shown here:

- **Accurate OT Operational Visibility**
- **Advanced ICS Threat Detection**
- **Proven, Large-Scale Global Installations**
- **Swift Deployment Across Many Sites**
- **Easy IT/OT Integration**
- **Global Partner Ecosystem**
- **Passion for Customer Success**

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**

Additional Resources

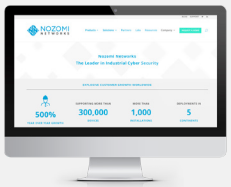
SOLUTION BRIEF

Nozomi Networks

DOWNLOAD

WEBPAGE

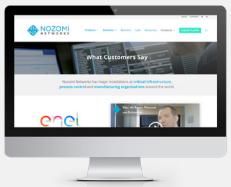
Company Overview



VISIT

WEBPAGE

What Customers Say



VISIT

WEBPAGE

Analysts and Awards

VISIT

References

1. **"Global Risk Report 2018"**, World Economic Forum, 2018
https://www.weforum.org/reports/the-global-risks-report-2018

2. 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.

3. **"Securing Industrial Control Systems – 2017"**, SANS Institute, June 2017
http://www.nozominetworks.com/downloads/US/SANS-Securing-ICS-2017-Report-from-Nozomi-Networks.pdf

4. **"Nozomi Networks Takes the Lead in ICS Cyber Security"**, Nozomi Networks, 2018
https://www.nozominetworks.com/company/infographic/

About Nozomi Networks

Nozomi Networks is accelerating the pace of digital transformation by pioneering innovation for industrial cyber security and operational control. Leading the industry, we make it possible to tackle escalating cyber risks to operational networks. In a single solution, Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest critical infrastructure, energy, manufacturing, mining, transportation and other industrial sites around the world.

NOZOMI NETWORKS

www.nozominetworks.com
@nozominetworks

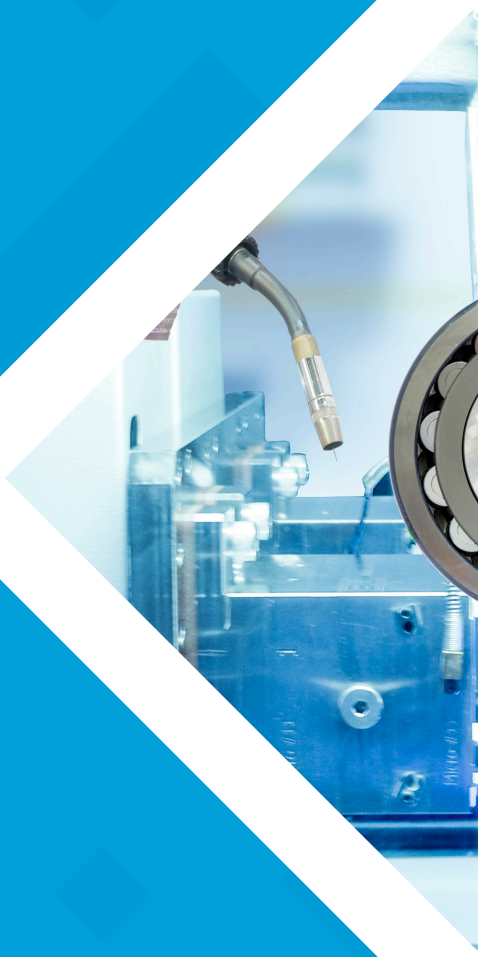
NN-SOL-WP-8.5x11-005

For detailed information about our products, visit

www.nozominetworks.com

#thosewhoknowpicknozomi

NOZOMI NETWORKS



#thosewhoknowpicknozomi

NN-SOL-WP-8.5x11-004