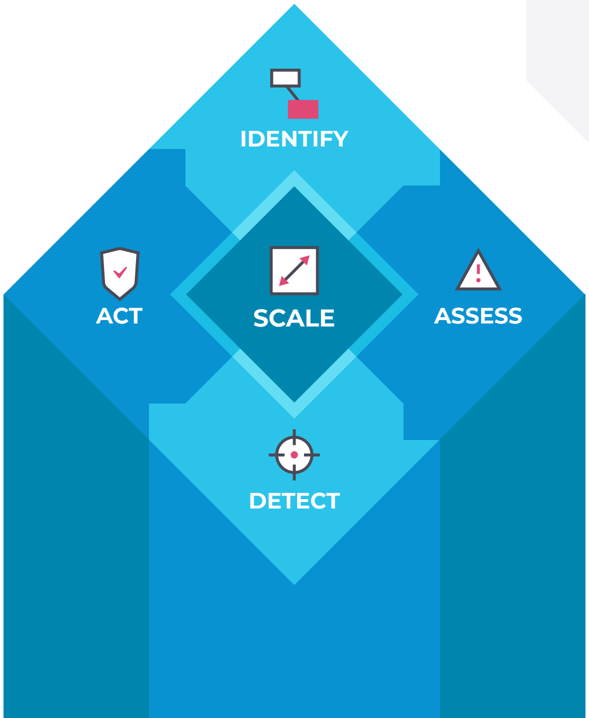
DATA SHEET

Guardian

Industrial Strength OT and IoT Security and Visibility

Nozomi Networks **Guardian**™ unlocks visibility across OT, IoT, and IT for accelerated security and digital transformation.

Guardian reduces OT risks for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world.



See

What's on your network and how it's behaving

Detect

Cyber threats, risks and anomalies for faster response

Unify

Security, visibility and monitoring across all your assets

Identify

Asset Discovery and Network Visualization

Automatically Track Your OT and IoT Assets

Up-to-Date Asset Inventory

Enhances cyber resiliency and saves time with automated asset inventory

Identifies all communicating devices

Provides extensive node information including name, type, serial number, firmware version and components

Presents risk information including security and reliability alerts, missing patches and vulnerabilities

ADD-ON

Smart Polling

Expands Guardian's built-in passive asset discovery with low-volume active polling, see: **nozominetworks.com/smart-polling**

SUBSCRIPTION

Asset Intelligence

Accelerates the asset learning process and keeps asset profiles and behavior data up-to-date, see: **nozominetworks.com/asset-intelligence**

Immediately Visualize Your Networks

Reduced Risk Through Network Visualization

Provides instant awareness of your OT/IoT network and its activity patterns

Presents key data such as traffic throughput, TCP connections, and protocols

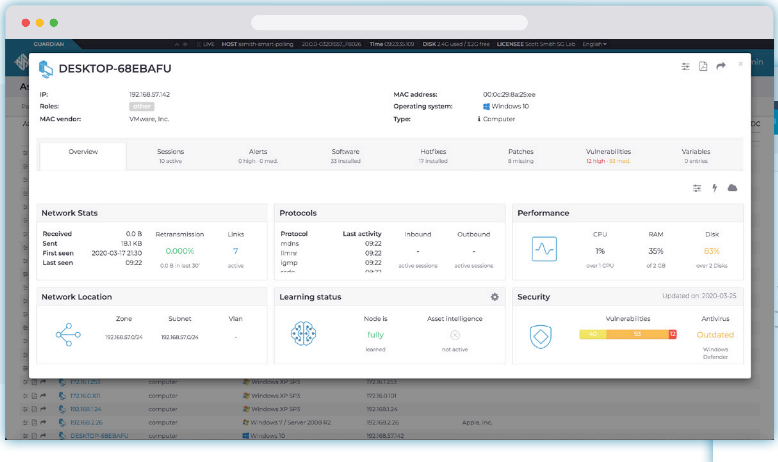
Improves your understanding of 'normal' operations

Intuitive Dashboards and Reports

Explore macro views as well as detailed information on endpoints and connections

Filter by subnets, type, role, zone and topologies

Group assets visually, in lists and detailed single asset views



GUARDIAN | LIVE **HOST** ssmith-smart-polling 20.0.0-03201557_F8026 **Time** 09:23:35.109 **DISK** 2.4G used / 3.2G free **LICENSEE** Scott Smith SG Lab English

DESKTOP-68EBAFU

IP:	192.168.57.142	MAC address:	00:0c:29:8a:25:ee
Roles:	other	Operating system:	Windows 10
MAC vendor:	VMware, Inc.	Type:	Computer

Overview	Sessions	Alerts	Software	Hotfixes	Patches	Vulnerabilities	Variables
	10 active	0 high · 0 med.	33 installed	17 installed	8 missing	12 high · 93 med.	0 entries

Network Stats

Received 0.0 B
Sent 18.1 KB
First seen 2020-03-17 21:30
Last seen 09:22
Retransmission 0.000% 0.0 B in last 30'
Links 7 active

Protocols

Protocol	Last activity
mdns	09:22
llmnr	09:22
igmp	09:22

Inbound - active sessions
Outbound - active sessions

Performance

CPU 1% over 1 CPU
RAM 35% of 2 GB
Disk 83% over 2 Disks

Network Location

Zone	Subnet	Vlan
192.168.57.0/24	192.168.57.0/24	-

Learning status

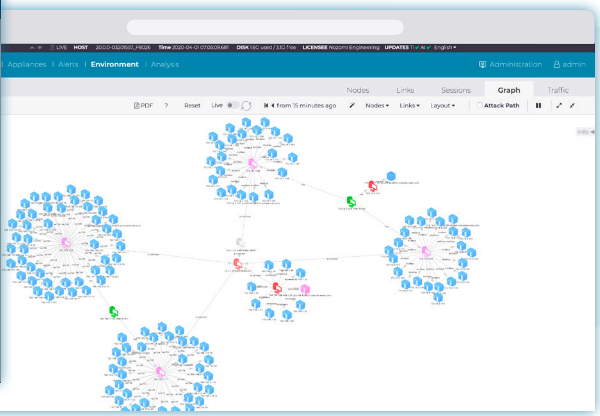
Node is fully learned
Asset intelligence not active

Security — Updated on: 2020-03-25

Vulnerabilities 40 93 12
Antivirus Outdated Windows Defender

172.16.1.253	computer	Windows XP SP3	172.16.1.253
172.16.0.101	computer	Windows XP SP3	172.16.0.101
192.168.1.24	computer	Windows XP SP3	192.168.1.24
192.168.2.26	computer	Windows 7 / Server 2008 R2	192.168.2.26	Apple, Inc.
DESKTOP-68EBAFU	computer	Windows 10	192.168.57.142

Single **Asset View** with extensive information.



LIVE **HOST** 20.0.0-03201557_F8026 **Time** 2020-04-01 07:05:09.681 **DISK** 1.6G used / 3.1G free **LICENSEE** Nozomi Engineering **UPDATES** TI ✓ AI ✓ English

Portion of interactive **Network** Visualization **Graph**.

Assess

Vulnerability Assessment and Risk Monitoring

Rapidly Identify Your Vulnerability Risks

Automated Vulnerability Assessment

Identifies which vendors' devices are vulnerable

Utilizes the U.S. government's National Vulnerability Database (NVD) for standardized naming, description and scoring

Efficient Prioritization and Remediation

Speeds response with vulnerability dashboards, drilldowns and reports

Answers questions like:

- "Are my ABC devices running vulnerable firmware?"
- "Are assets from Vendor X vulnerable?"

Continuously Monitor Your Network and Automation Systems

Comprehensive Cybersecurity and Reliability Monitoring

Monitors assets from all vendors and network communications

Displays summarized data related to alerts, incidents, vulnerabilities, compliance, etc.

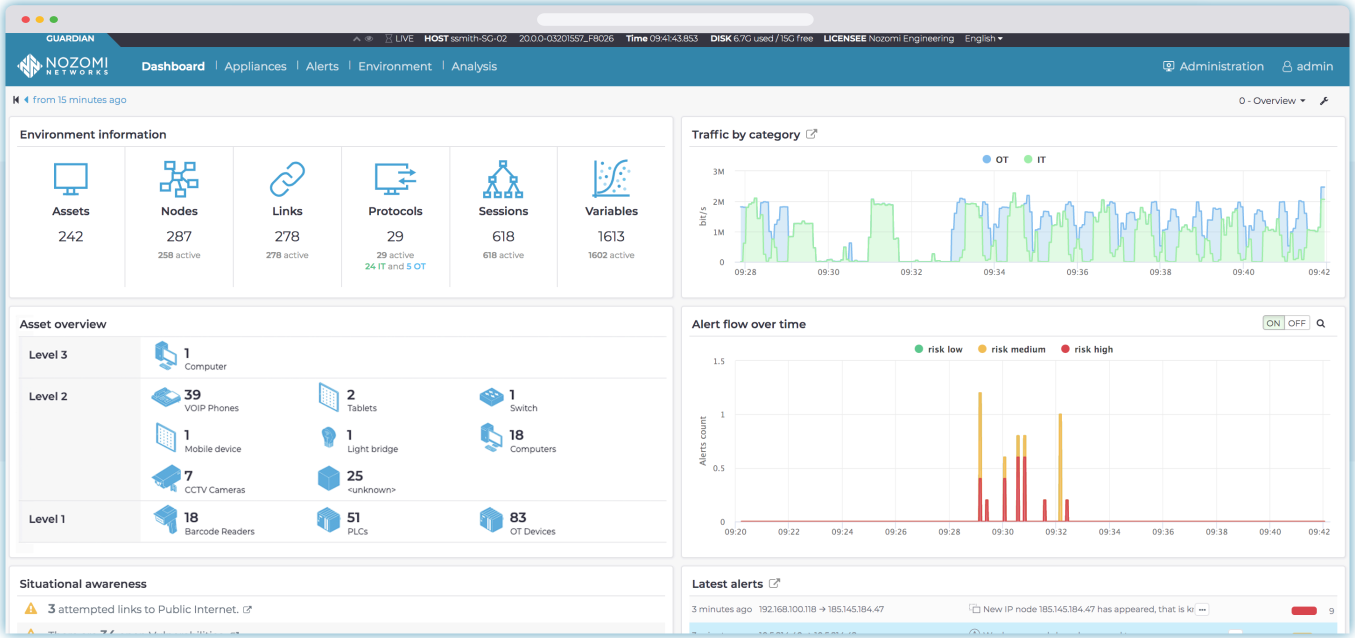
Highlights indicators of reliability issues, such as unusual process values

Easy Access to OT Data

Summarizes OT and IoT risk information for customizable date and time ranges

Supports drilldown on visual indicators for more detailed information

Queries any aspect of your network or control system performance, reducing data collection and spreadsheet work



Environment information

Assets	Nodes	Links	Protocols	Sessions	Variables
242	287	278	29	618	1613
	258 active	278 active	29 active 24 IT and 5 OT	618 active	1602 active

Asset overview

Level 3	1 Computer		
Level 2	39 VOIP Phones	2 Tablets	1 Switch
	1 Mobile device	1 Light bridge	18 Computers
	7 CCTV Cameras	25 <unknown>	
Level 1	18 Barcode Readers	51 PLCs	83 OT Devices

Situational awareness

3 attempted links to Public Internet.

Latest alerts

3 minutes ago 192.168.100.118 → 185.145.184.47 New IP node 185.145.184.47 has appeared, that is kı ... 9

Portion of customizable **Guardian Dashboard**.

Detect

Advanced Anomaly and Threat Detection

Quickly Detect and Disrupt Threats and Anomalous Behavior

Up-to-the-Minute Threat Detection

Identifies cybersecurity and process reliability threats

Detects early stage and late stage advanced threats and cyber risks

Blocks attacks when integrated with compatible firewalls and endpoint security products

Superior OT and IoT Threat Detection

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

Provides detailed threat information as Yara rules, packet rules, STIX indicators, threat definitions, a threat knowledgebase and vulnerability signatures

Effectively Monitor Mixed Environments

SUBSCRIPTION

Threat Intelligence

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

Delivers ongoing OT, IoT and IT threat and vulnerability intelligence

SUBSCRIPTION

Asset Intelligence

Powers breakthrough anomaly detection for OT and IoT that filters out alerts for benign behavior, accelerating incident response

Delivers ongoing OT and IoT asset profile and behavior data

Breakthrough Anomaly Detection for OT and IoT

Rapid Identification of Assets

▼

Ensures Precise Asset Inventory

Accurate Anomaly Alerts

▼

Accelerates Incident Response

Asset Intelligence for Dynamic Networks

▼

Sustains Accurate Inventory & Detection

Act

Time-saving Dashboards and Forensic Tools

Significantly Improve OT and IoT Risk Management

Dashboards and Reports Highlight Risks

Focuses attention on key concerns by summarizing risks and threats

Answers vital questions like:

- "What IoT assets do we have?"
- "What are they doing?"
- "What risks do they pose to my organization?"

Detailed Alerts Provide Key Information

Generates detailed, accurate alerts

Identifies security and reliability risks

Groups alerts into incidents, providing security and operations staff with a simple, clear, consolidated view of what's happening on their network

Greatly Reduce Troubleshooting and Forensic Efforts

Accelerated Incident Response

Combines Guardian's breakthrough anomaly detection for OT and IoT with the **Asset Intelligence**™ service for focused, actionable alerts

Understands normal behavior for devices with frequent behavior changes, eliminating alerts for benign anomalies

Improves response time and productivity with precise alerts that are easy to prioritize

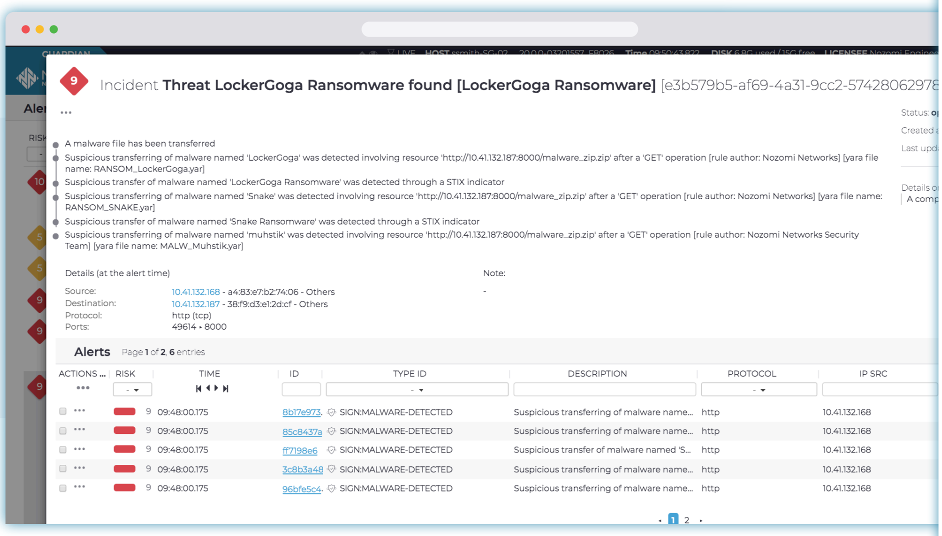
Fast Forensic Analysis

Focuses effort with Smart Incidents™ that:

- Correlate and consolidate alerts
- Provide operational and security context
- Supply automatic packet captures

Decodes incidents with Time Machine™ before and after system snapshots

Provides answers fast with a powerful ad hoc query tool



9 Incident **Threat LockerGoga Ransomware found [LockerGoga Ransomware]** [e3b579b5-af69-4a31-9cc2-57428062978

- A malware file has been transferred
- Suspicious transferring of malware named 'LockerGoga' was detected involving resource 'http://10.41.132.187:8000/malware_zip.zip' after a 'GET' operation [rule author: Nozomi Networks] [yara file name: RANSOM_LockerGoga.yar]
- Suspicious transfer of malware named 'LockerGoga Ransomware' was detected through a STIX indicator
- Suspicious transferring of malware named 'Snake' was detected involving resource 'http://10.41.132.187:8000/malware_zip.zip' after a 'GET' operation [rule author: Nozomi Networks] [yara file name: RANSOM_SNAKE.yar]
- Suspicious transfer of malware named 'Snake Ransomware' was detected through a STIX indicator
- Suspicious transferring of malware named 'muhstik' was detected involving resource 'http://10.41.132.187:8000/malware_zip.zip' after a 'GET' operation [rule author: Nozomi Networks Security Team] [yara file name: MALW_Muhstik.yar]

Details (at the alert time)

Source: 10.41.132.168 - a4:83:e7:b2:74:06 - Others
Destination: 10.41.132.187 - 38:f9:d3:e1:2d:cf - Others
Protocol: http (tcp)
Ports: 49614 ▸ 8000

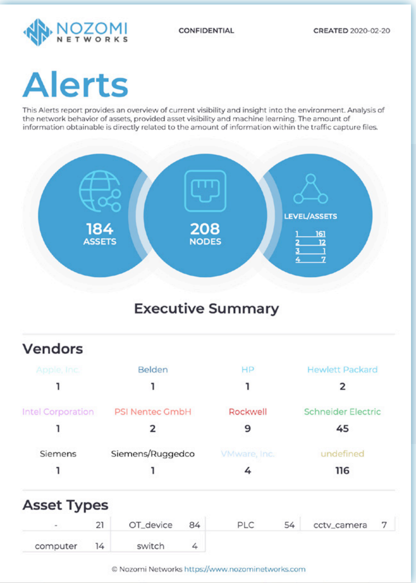
Note: -

Alerts Page **1** of **2**, **6** entries

ACTIONS ...	RISK	TIME	ID	TYPE ID	DESCRIPTION	PROTOCOL	IP SRC
□ •••	9	09:48:00.175	8b17e973.	SIGN:MALWARE-DETECTED	Suspicious transferring of malware name...	http	10.41.132.168
□ •••	9	09:48:00.175	85c8437a	SIGN:MALWARE-DETECTED	Suspicious transferring of malware name...	http	10.41.132.168
□ •••	9	09:48:00.175	ff7198e6	SIGN:MALWARE-DETECTED	Suspicious transfer of malware named 'S...	http	10.41.132.168
□ •••	9	09:48:00.175	3c8b3a48	SIGN:MALWARE-DETECTED	Suspicious transferring of malware name...	http	10.41.132.168
□ •••	9	09:48:00.175	96bfe5c4.	SIGN:MALWARE-DETECTED	Suspicious transferring of malware name...	http	10.41.132.168

‹ 1 2 ›

Smart Incident showing related alerts and security context.



NOZOMI NETWORKS CONFIDENTIAL CREATED 2020-02-20

Alerts

This Alerts report provides an overview of current visibility and insight into the environment. Analysis of the network behavior of assets, provided asset visibility and machine learning. The amount of information obtainable is directly related to the amount of information within the traffic capture files.

184 ASSETS

208 NODES

LEVEL/ASSETS

1	161
2	12
3	1
4	7

Executive Summary

Vendors

Apple, Inc.	Belden	HP	Hewlett Packard
1	1	1	2
Intel Corporation	PSI Nentec GmbH	Rockwell	Schneider Electric
1	2	9	45
Siemens	Siemens/Ruggedco	VMware, Inc.	undefined
1	1	4	116

Asset Types

-	21	OT_device	84	PLC	54	cctv_camera	7
computer	14	switch	4				

© Nozomi Networks https://www.nozominetworks.com

Report summarizing alerts for a site.

Scale

Unified Security for Thousands of Distributed Sites

Readily Scale with Optimal Performance

Exceptional Local & Global Performance

Processes data for up to 500,000 assets in real-time

Generates network visualizations, dashboards and reports quickly

Speeds up threat detection and response with local processing of threat and asset intelligence

Deploys quickly at multiple sites

Consolidated Monitoring of All Facilities

Aggregates data from multiple sites when used with the **Central Management Console**™

Enables centralized security risk management for all sites

Provides visibility into all OT/ IoT environments

Easily Integrate with SOC/IT Environments

Integrated Security Infrastructure

Streamlines security processes across IT/OT

Makes it easy to harmonize security data for cohesive response

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

nozominetworks.com/integrations

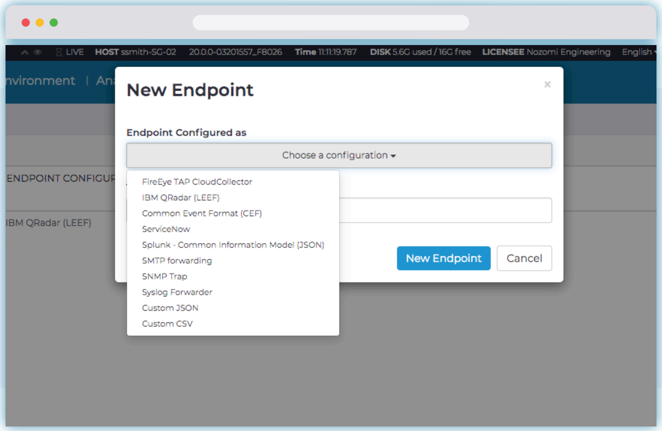
Broad Protocol Support

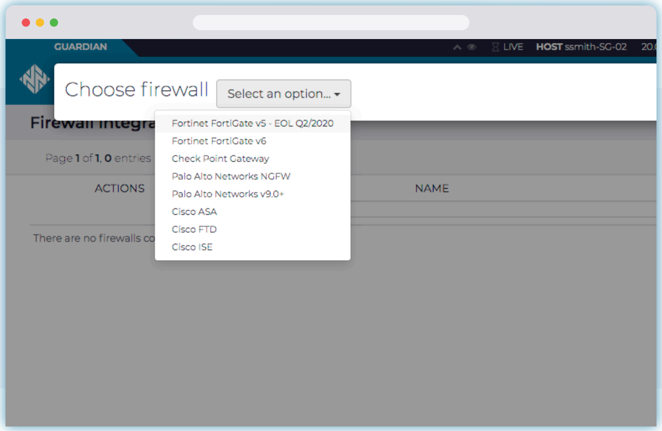
Supports hundreds of OT, IoT and IT protocols

Utilizes Nozomi Networks' deep expertise in OT protocols for accurate analysis

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

nozominetworks.com/techspecs





Built-in integrations make it easy to streamline security processes.

Enhance Guardian for Expanded Visibility and Threat Detection

SUBSCRIPTION

Threat Intelligence

Reduces risks by shrinking the mean-time-to-detection (MTTD), minimizing impacts

Delivers ongoing OT and IoT threat and vulnerability intelligence for rapid risk detection

Consists of rules, signatures and vulnerability updates created and curated by Nozomi Networks Labs, a team of expert security researchers

Complete details available at:
nozominetworks.com/threat-intelligence

SUBSCRIPTION

Asset Intelligence

Reduces risks by eliminating anomaly alert overload and focusing your attention on critical incidents, decreasing the mean-time-to-respond (MTTR)

Delivers ongoing OT and IoT asset intelligence for rapid asset identification and precise anomaly detection

Updates Guardian's anomaly detection technology with device profiles and behavior data based on analysis of millions of devices in use at sites around the world

Complete details available at:
nozominetworks.com/asset-intelligence

GUARDIAN ADD-ON

Smart Polling

Adds low-volume active polling to Guardian’s passive asset discovery

Identifies non-communicating assets and rogue devices

Delivers accurate vulnerability assessment for fast and efficient response

Complete details available at:
nozominetworks.com/smart-polling

GUARDIAN ADD-ON

Remote Collectors

Supplement Guardian data via low-resource appliances for distant and distributed locations

Collect data and send it to Guardian for further analysis

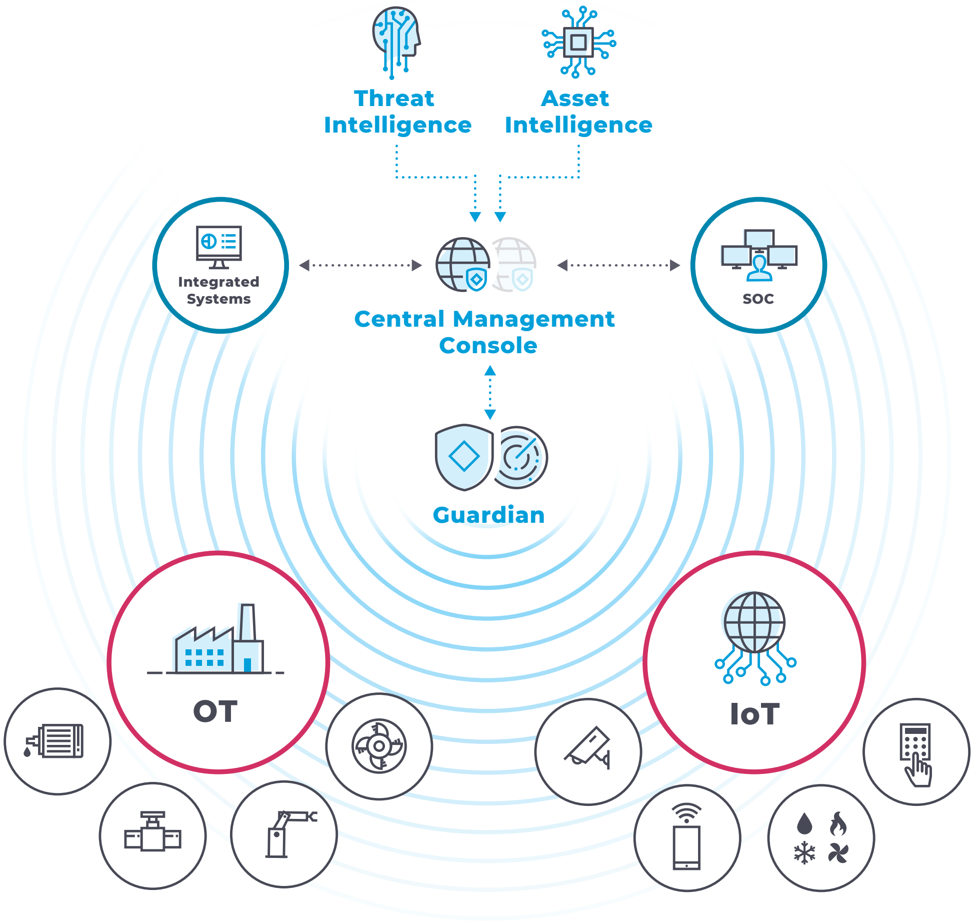
Reduce deployment costs for wilderness, off-shore or desert locations

Complete details available at:
nozominetworks.com/techspecs

Flexible Deployment and Licensing

Industrial Strength OT and IoT Security and Visibility

You can deploy the Nozomi Networks solution in a wide variety of mixed environments for rapid asset discovery, network visualization and accelerated security.



Multiple Licensing Options

Nozomi Networks offers a range of licensing options to fit your organization's preferences, including:

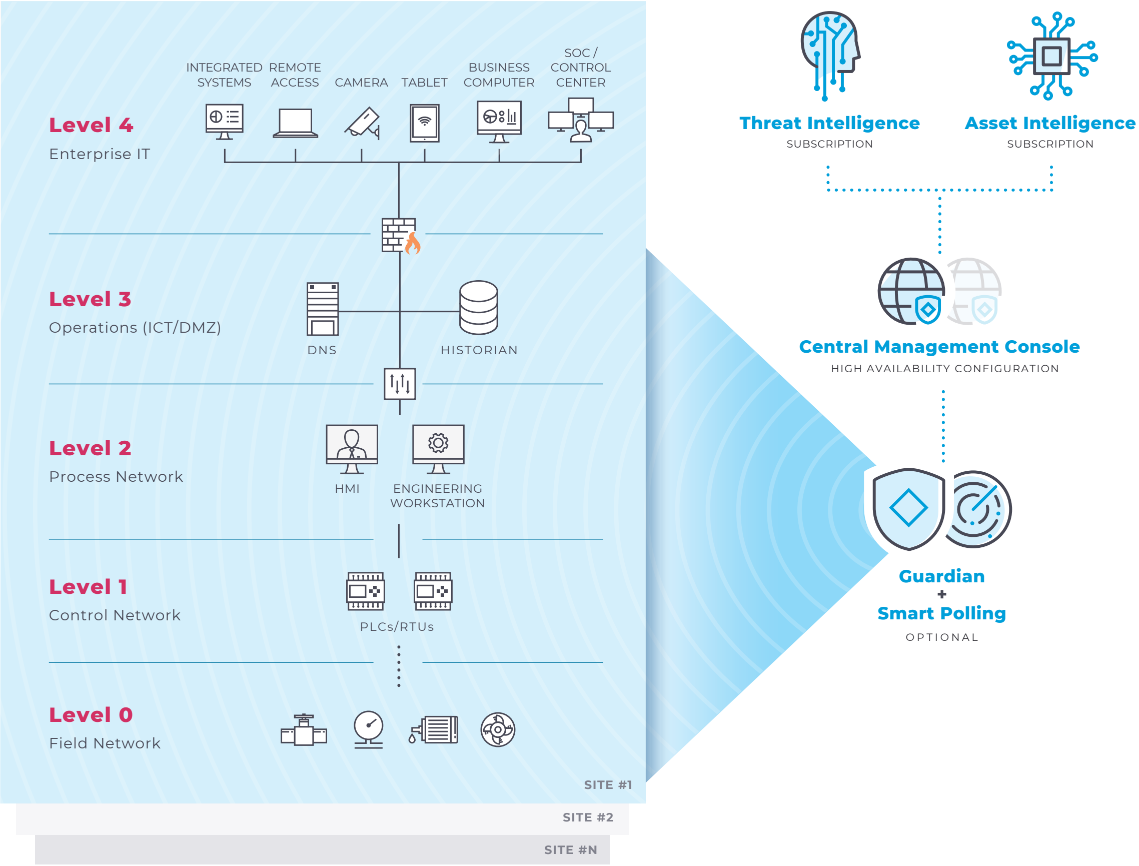
- **Subscription licenses**
- **Enterprise license agreements (ELAs)**
- **Perpetual licenses**

Please contact your Nozomi Networks Sales Director for more information.

Sample Deployment Architecture

Purdue Model Example

You can tailor the Nozomi Networks solution to meet your needs by utilizing its flexible architecture, extensive range of appliances, and integrations with other systems.



World Class Partners

Nozomi Networks partners deeply with the IT/OT services and technology companies you trust. These include:

- **Strategic alliances** with enterprise IT and managed security providers
- **Technology integrations** with leading IT/OT solutions
- **SI/VAR relationships** with 250+ prominent organizations around the world

Visit **nozominetworks.com/partners** for more information.

Guardian Appliances

for the Large Enterprise

NSG-HS Series

Rack-mounted appliances for real-time OT/IoT visibility, cybersecurity and monitoring

- **300,000 - 500,000 Nodes**
- **6 Gbps Max. Throughput**

NSG-H Series

Rack-mounted appliances for real-time OT/IoT visibility, cybersecurity and monitoring

- **100,000 - 200,000 Nodes**
- **3 Gbps Max. Throughput**

	NSG-HS 3500	NSG-HS 3000	NSG-H 2500	NSG-H 2000
Max. Protected Nodes	500,000	300,000	200,000	100,000
Max. Virtual RTUs*	3,000,000	1,800,000	1,200,000	600,000
Max. Throughput	6 Gbps		3 Gbps	
Max. Remote Collectors**	50		50	
Monitoring Ports	Modular up to 16+1		Modular up to 8+1	
Expansion Slots	4 slots available: 4x1000BaseT | 4xSFP | 4xSFP+		2 slots available: 4x1000BaseT | 4xSFP | 4xSFP+	
Storage	512 Gb		512 Gb	
Form Factor	1 rack unit		1 rack unit	
Max. Power Consumption	750 W		750 W	
Power Supply Type	100-240V AC - 50/60Hz		100-240V AC - 50/60Hz	
Temperature Range	0 / +40° C		0 / +40° C	
HxWxL (mm/in)	44 x 438 x 600 1.73 x 17.24 x 23.60		44 x 438 x 600 1.73 x 17.24 x 23.60	
Weight	18 Kg		17 Kg	

* Virtual RTUs can either be subRTUs or smart meters reachable through direct or serial communication. ** See Remote Collector tech specs for more details. For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Guardian Appliances

for the Mid-Enterprise

NSG-M Series

Rack-mounted appliances for real-time OT/IoT visibility, cybersecurity and monitoring

- **10,000 - 40,000 Nodes**
- **1 Gbps Max. Throughput**

NSG-L Series

Rack-mounted appliances for real-time OT/IoT visibility, cybersecurity and monitoring

- **1,000 - 5,000 Nodes**
- **250 - 500 Mbps Max. Throughput**

	NSG-M 1000	NSG-M 750	NSG-L 250	NSG-L 100
Max. Protected Nodes	40,000	10,000	5,000	1,000
Max. Throughput	1 Gbps		500 Mbps	250 Mbps
Max. Remote Collectors*	50		20	
Monitoring Ports	7x1000BASE-T + 4xSFP		5x1000BASE-T	
Expansion Slots	1 slot available: 4x1000Base-T | 4xSFP | 4xSFP$^+$		1 slot available: 4x1000Base-T | 4xSFP	
Storage	256 Gb		64 Gb	
Form Factor	1 rack unit		1 rack unit	
Max. Power Consumption	360W		250W	
Power Supply Type	100-240V AC - 50/60 Hz		100-240V AC - 50/60 Hz	
Temperature Range	0 / +45° C		0 / +45° C	
HxWxL (mm/in)	44 x 429 x 438 1.73 x 16.89 x 17.24		44 x 438 x 300 1.7 x 17.2 x 11.8	
Weight	14 Kg		8 Kg	

* See Remote Collector tech specs for more details. | For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Guardian Appliances

for Specialized Requirements

NSG-R Series

Ruggedized appliances for real-time OT/IoT visibility, cybersecurity and monitoring

- **500 - 1,000 Nodes**
- **100 - 250 Mbps Max. Throughput**

Portable

Portable appliance for real-time OT/IoT visibility, cybersecurity and monitoring

- **2,500 Nodes**
- **200 Mbps Max. Throughput**

	NSG-R 150	NSG-R 50	P550
Max. Protected Nodes	1,000	500	2,500
Max. Throughput	250 Mbps	100 Mbps	200 Mbps
Max. Remote Collectors*	20	10	Not available
Monitoring Ports	7x1000BASE-T	4x1000BASE-T	5x1000BASE-T
Expansion Slots	Not available		Not available
Storage	64 Gb		256 Gb
Form Factor	2 rack unit	DIN mountable	Desktop with wall mount kit
Max. Power Consumption	250W	60W	38W
Power Supply Type	100-240V AC 100-240V DC	100-240V AC 12-36V DC	90-240V AC 12-30V DC
Temperature Range	-40 / +70° C	-40 / +75° C	0 / +60° C
HxWxL (mm/in)	88 x 440 x 301 3.46 x 17.32 x 11.86	80 x 130 x 146 3.15 x 5.11 x 5.74	70 x 180 x 240 2.75 x 7.08 x 9.44
Weight	6 Kg	3 Kg	2.5 Kg

* See Remote Collector tech specs for more details. | For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Guardian Appliances

for Remote Sites

Remote Collector

Low-resource appliances that collect asset and network data in remote locations and send it to Guardian for further analysis

- **Up to 15 Mbps Throughput**

	NRC-5
Max. Throughput	Up to 15 Mbps
Remote Collector Support	Not available
Monitoring Ports	2x1000Base-T, 1xSFP
Expansion Slots	Not available
Storage	8 Gb
Form Factor	DIN mountable
Max. Power Consumption	12W
Power Supply Type	12-36V DC
Temperature Range	-40 / +70° C
Heat Generation	55.44 BTU/hr
HxWxL (mm/in)	41.5 x 170 x 138 / 2.71 x 6.67 x 5.00
Weight	1.2 Kg
Compliance	RoHS
Certifications	CE, FCC, UL
	Virtual Remote Collector
Max. Throughput	15 Mbps
Deployment Options	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+

For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Guardian Appliances

for Virtual Environments and Containers

Virtual Series

Virtual appliances for real-time OT/IoT visibility, cybersecurity and monitoring

- **1,000 - 40,000 Nodes**
- **1 Gbps Max. Throughput**

	V1000	V750	V250	V100
Max. Protected Nodes	40,000	10,000	5,000	1,000
Max. Throughput*	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Scenarios	Enterprise	Large	Medium	Small
Deployment Options	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+			
Max. Remote Collectors**	50	50	20	20

* Performance is dependent upon hardware configuration and resource allocation. ** See Remote Collector tech specs for details.

Container Edition

Embedded container appliance for switches, routers and other security infrastructure. Fast, flexible deployment option that leverage your existing devices.

- **Available for Guardian with the Smart Polling add-on module only.**

	Container
Embedded Offerings	Cisco Catalyst **|** Siemens RUGGEDCOM
Add-ons	Smart Polling module: *included* **|** Threat Intelligence and Asset Intelligence subscriptions: *can be added*
Remote Collector Support	Not available

For complete and current tech specs, visit: **nozominetworks.com/techspecs**, or contact us.

Multiple Deployment and Support Options

Here are several options for deployment and support assistance:

- **Nozomi Networks Global Strategic Alliance Partners**
- **Nozomi Networks SI/VARs**
- **Nozomi Networks Professional Services**
- **Nozomi Networks Global Customer Support**

Products and Services

PRODUCT

Guardian

Guardian provides industrial strength OT and IoT security and visibility. It combines asset discovery, network visualization, vulnerability assessment, risk monitoring and threat detection in a single solution. Guardian accelerates security and simplifies IT/OT convergence.

SUBSCRIPTION

Threat Intelligence

The Threat Intelligence service delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of the dynamic threat landscape and reduce your mean-time-to-detection (MTTD).

GUARDIAN ADD-ON

Smart Polling

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

PRODUCT

Central Management Console

The Central Management Console (CMC) consolidates OT and IoT risk monitoring and visibility across many distributed sites, at the edge or in the cloud. It integrates with IT security infrastructure for streamlined workflows and faster response to threats and anomalies.

SUBSCRIPTION

Asset Intelligence

The Asset Intelligence service delivers ongoing OT and IoT asset intelligence for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-response (MTTR).

GUARDIAN ADD-ON

Remote Collectors

Remote Collectors capture data in remote, distributed locations and send it to Guardian for analysis, improving visibility while reducing deployment costs.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

nozominetworks.com