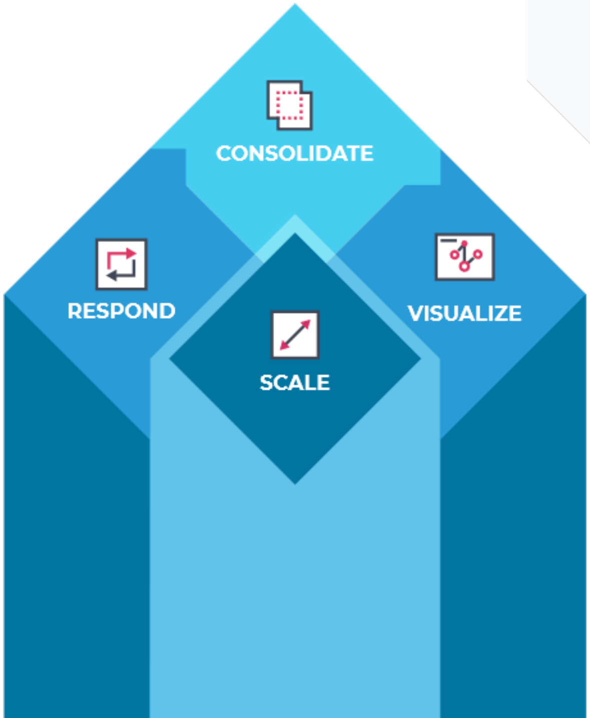
DATA SHEET

Central Management Console

Centralized OT and IoT Security and Visibility for Distributed Sites

Nozomi Networks **Central Management Console**™ (CMC) appliances deliver centralized edge or public cloud-based monitoring of Guardian sensors–no matter how distributed your business is.

Whether you're consolidating visibility and risk management at the edge or in the cloud, the CMC is fast and simple to deploy.



See

All OT and IoT assets and behavior on your networks for unmatched awareness

Detect

Cyber threats, vulnerabilities, risks and anomalies for faster response

Unify

Security, visibility and monitoring across all your assets for improved resilience

Consolidate

Unified OT, IoT and IT Security

Centrally Monitor Your Distributed Sites

Single Console Access from the Public Cloud or at the Edge

Delivers aggregated summaries with drilldown to detailed information by site

Answers questions fast with powerful queries about any and all OT/IoT data

Deploys in the cloud (AWS or Azure), or at the edge, for anytime, anywhere access

Enterprise OT/IoT Risk Monitoring

Maps your **Guardian™** sensors and shows risk level by site

Delivers fast insight into key metrics, alerts, incidents, vulnerabilities and more

Manages Nozomi Networks sensors and services

Easily Streamline SOC/IT Workflows

Unified Security Monitoring

Integrates quickly with asset, ticketing & identity management systems, and SIEMs

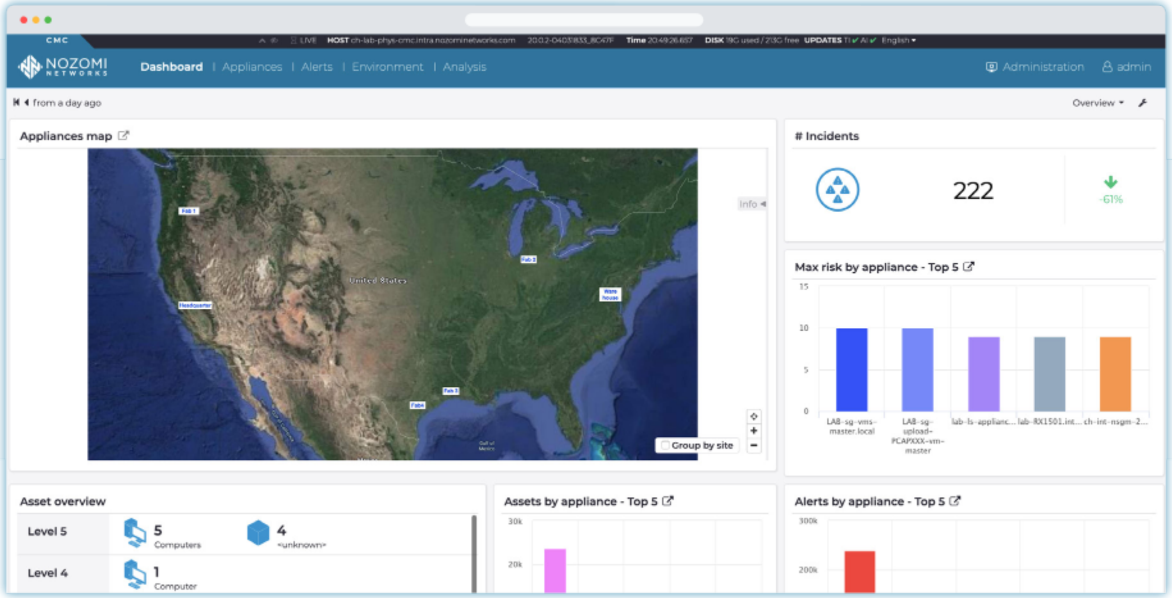
Streamlines security processes across IT/OT and harmonizes security data

nozominetworks.com/integrations

Enterprise-level Best Practices

Leverages enterprise single sign-on (SSO) credentials for fast access to OT and IoT information

Provides deep role-based access control (RBAC) "least privilege" permission options for maximum security



The **CMC** showing a geographic map of your Guardian sensors.

Visualize

Enterprise-wide Visibility

Instantly See Your Networks

Real-time Network Visualization

Delivers instant awareness of OT/IoT networks and their activity patterns

Captures key data such as traffic throughput, TCP connections, protocols used between zones and more

Accelerates incident response and troubleshooting efforts

Flexible Navigation and Filtering

Shows macro views of multiple sites, individual sites and detailed information on nodes and connections

Filters by subnet, type, role, zone and topology

Groups assets visually, in lists and detailed single asset views

Quickly Know Your Assets and Their Risks

Summarized Asset Information

Aggregates asset inventories that are automatically generated by Guardian at each site

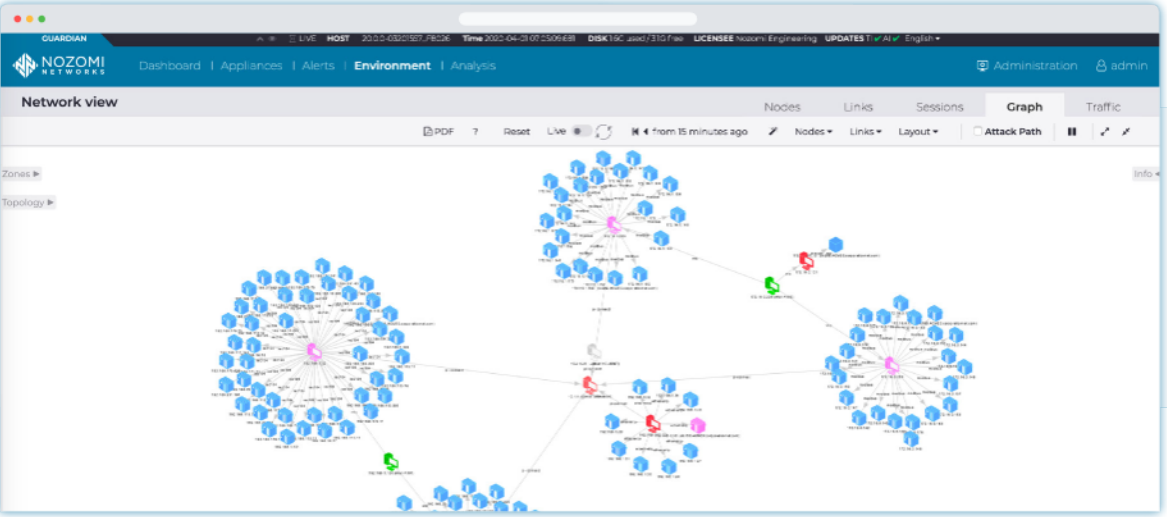
Provides key information such as:

- OT asset inventory
- IoT asset inventory
- Vulnerabilities by asset type, vendor or location

Drilldown to Individual Assets

Enables access to local Guardian sensors and individual asset details, such as:

- Operating system
- MAC vendor
- MAC address
- Installed software
- Vulnerabilities
- Captured URLs/files
- IP
- Subnet
- Zone
- Role
- Alerts



Portion of interactive **Network Visualization Graph**.

Respond

Time-saving Threat Summaries and Forensic Tools

Rapidly Respond to OT and IoT Risks

Detect and Disrupt Emerging Threats

Aggregates cybersecurity and process reliability threats

Reports attacks in process, reducing the mean-time-to-detection (MTTD)

Consolidates vulnerability assessment across sites

Unified OT and IoT Threat Detection

Combines behavior-based anomaly detection with signature-based threat detection for complete coverage

Integrates quickly with ticketing systems and SIEMs for streamlined security processes

Optimize Troubleshooting and Forensic Efforts

Powerful Tools for Fast Analysis

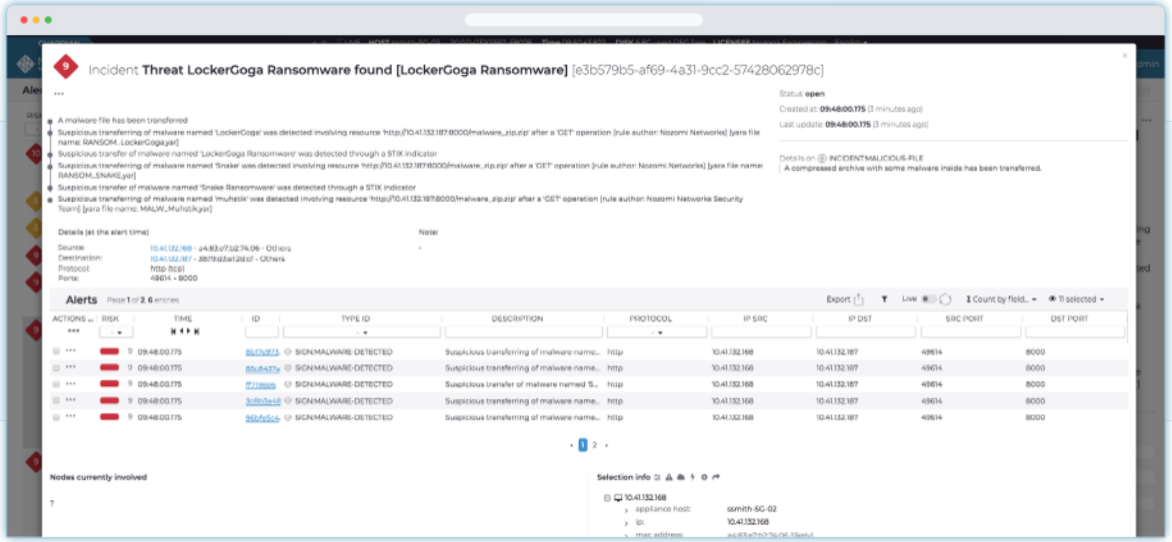
Decodes incidents with Time Machine™ before and after system snapshots

Provides fast answers with a powerful ad hoc query tool

Smart Incidents Speed Forensicss

Decreases response time with Smart Incidents™ that:

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



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

Status: **open**
Created at: **09:48:00.175** (3 minutes ago)
Last update: **09:48:00.175** (3 minutes ago)

Details on INCIDENT:MALICIOUS-FILE
A compressed archive with some malware inside has been transferred.

- 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:e7:02:74:06 - Others
Destination: 10.41.132.187 - a8:7f:dd:a1:20: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	IP DST	SRC PORT	DST PORT
···	9	09:48:00.175	8b17c973	SIGN:MALWARE-DETECTED	Suspicious transferring of malware name...	http	10.41.132.168	10.41.132.187	49614	8000
···	9	09:48:00.175	85c8437e	SIGN:MALWARE-DETECTED	Suspicious transferring of malware name...	http	10.41.132.168	10.41.132.187	49614	8000
···	9	09:48:00.175	ff71e6e6	SIGN:MALWARE-DETECTED	Suspicious transfer of malware named 'S...	http	10.41.132.168	10.41.132.187	49614	8000
···	9	09:48:00.175	3c8b3a48	SIGN:MALWARE-DETECTED	Suspicious transferring of malware name...	http	10.41.132.168	10.41.132.187	49614	8000
···	9	09:48:00.175	96bfe5c4	SIGN:MALWARE-DETECTED	Suspicious transferring of malware name...	http	10.41.132.168	10.41.132.187	49614	8000

Nodes currently involved

?

Selection info

10.41.132.168
appliance host: ssmith-SG-02
ip: 10.41.132.168
mac address:

Smart Incident showing related alerts and security context.

Scale

Unified Security for Thousands of Distributed Sites

Attain High Performance for Multinational Deployments

Centralized Monitoring of OT Risks

Consolidates information for thousands of sites and assets

Quickly scales for enterprise-wide deployment with optimum performance

Adapts to all sites, with multiple appliance models and flexible deployment options

High Availability, High Security

Ensures continuous OT and IoT monitoring with high availability and multitenant CMC configurations

Connects with field sensors using encrypted, bandwidth-optimized data transfers

Realize Rapid Time to Value

Swift Deployment

Installs as a proven, plug-and-play, ISO 9001: 2015 certified product

Deploys in the cloud on AWS or Azure, and at the edge on virtual and physical appliances

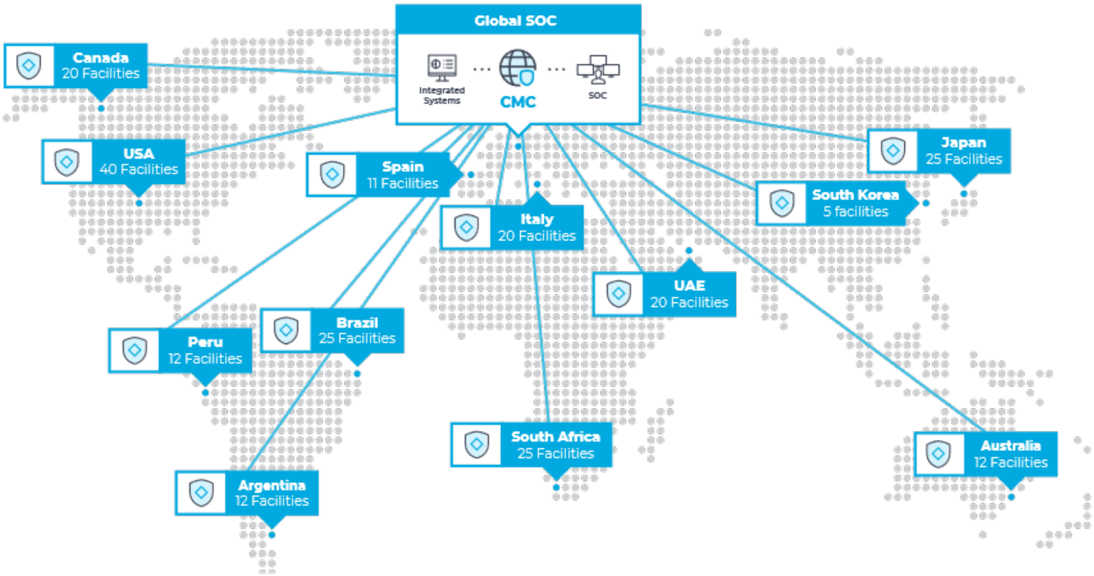
Rolls out to numerous sites within weeks

Immediately Valuable

Improves visibility, cybersecurity and reliability

Integrates with existing tools and workflows for fast adoption and high productivity

Accelerates IT/OT collaboration



Sample deployment map for centrally monitoring and securing many facilities.