NOZOMI NETWORKS

SOLUTION BRIEF

Maritime Cybersecurity

In ports, undetected cyber incidents can cause disruption that can last for hours, days, or weeks, resulting in financial losses. On ships, an undetected or incorrectly diagnosed cyberattack can send the ship off course, putting crew and passengers at risk. As maritime companies become more connected and autonomous, their vulnerability to cyber threats is increasing, making cybersecurity a priority.

Maritime networks increasingly rely on connected industrial control systems (ICS) and satellite communications, using a blend of information technology (IT) and operational technology (OT) systems, which expand the threat landscape.

Protecting dispersed operation centers, fleets spread across the world and connected devices in ports, such as cranes, CCTV systems, and scanners can be challenging. Vulnerabilities are caused not just by increasing digitization, but also by a lack of cybersecurity awareness among crew, employees, and contractors. Meanwhile, traditional cybersecurity measures, such as IT firewalls, often fail to protect operational equipment from cyberattacks.

In response, there has been an increase in regulations, guidelines and mandates demanding more stringent protections from cyber threats.

To achieve cyber and operational resilience, port and shipping operators must protect themselves from current and emerging cyber threats with threat intelligence and timely alerts. Nozomi Networks is the leading solution in this space that helps you anticipate, diagnose and respond to cybersecurity risks.

$300M estimated losses in ransomware attack

Maersk, a Danish container shipping company, experienced a devastating ransomware attack involving the NotPetya virus in 2017.

For almost two days, the attack prevented port personnel from accessing operations data and moving cargo—and it took two weeks to restore normal business operations.

Although the shipping company is not believed to have been the intended target of the attack, it ultimately resulted in estimated losses of $300 million.

Anticipate Cybersecurity Risks Through Asset Discovery, Network Visualization and Workbooks

The Nozomi Networks platform anticipates cybersecurity risks within your shipping fleet or port operational equipment, helping you to understand what is on your network and anticipate where risks may arise.

Asset Discovery

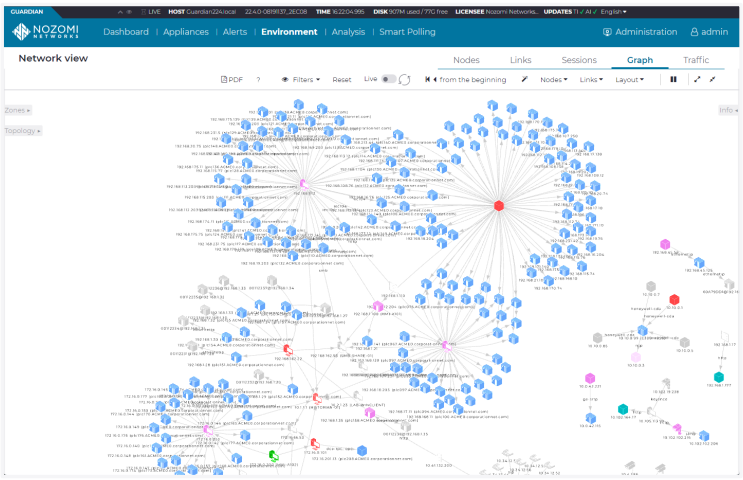
Identify risks and patch priorities with Nozomi Networks' extensive databases of known vulnerabilities from researchers and security bodies around the globe.

Keep your organizations up to date with the latest vulnerability research, current OS and firmware patch levels and recent breaches with our optional Asset Intelligence subscription service.

Network Visualization

Observe mirrored traffic to passively discover assets in OT and IT environments without disrupting critical processes, triggering alarms or generating additional traffic.

Get a complete view of communicating devices and traffic patterns with a visualization map that can alert you of traffic anomalies.



Workbooks

Prioritize remediation efforts with workbooks that highlight the most critical endpoint vulnerabilities.

Diagnose Threats and Anomalies and Provide Actionable Intelligence That Helps Keep Systems Reliable and Secure

Nozomi Networks' industry-leading AI engine delivers quick root-cause diagnosis and actionable intelligence to detect anomalies and remediate incidents fast.

Anomaly Detection

Compare network traffic and process trends over time to identify potential threats and keep systems running uninterrupted.

Eliminate false alerts and get deeper insights into trends based on learned behaviors over time.

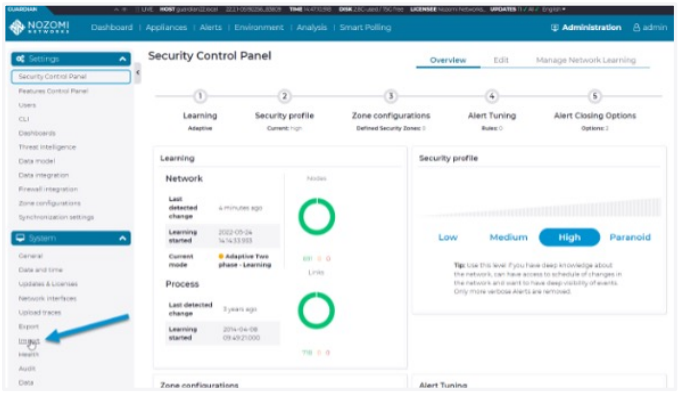
Go beyond surface-level anomaly detection to process variable trends and control system data to expand root cause analysis.

Threat Intelligence

Detect more threats to more devices with the industry's widest range of industrial device and protocol coverage.

Stay up-to-date with emerging malware and IoT and industrial process indicators of compromise.

Obtain additional protection for third-party security solutions, like firewalls and SOAR platforms, with Nozomi Networks' Threat Intelligence Feed.



Content Packs

Access prefabricated Nozomi Networks platform configurations for particular use cases, or threat and compliance initiatives.

Obtain insights to your specific environment with readily available Content Packs for common issues and emerging threats.

Get immediate free reports for challenges such as Industroyer2 and others.

Respond to Security Breaches or Process Control Issues with Minimum Cost and Disruption to Operations

When it's time to respond to a security breach or a process control issue, you need actionable intelligence to address the problem with the minimum cost and impact on your operations.

Time Machine

Replay network events around an incident to isolate the root cause and visualize the impact, minimizing cost and impact to operations.

Dashboards

Gain high-level and actionable view of events, systems, assets and security issues across all smart city systems.

Filter potentially enormous amounts of information while keeping it fully organized and accessible.

Quickly isolate vulnerabilities and incidents or identify and inventory assets with custom queries.

Use or build repeatable or common queries and report combinations for Content Packs available from Nozomi Networks and partners.

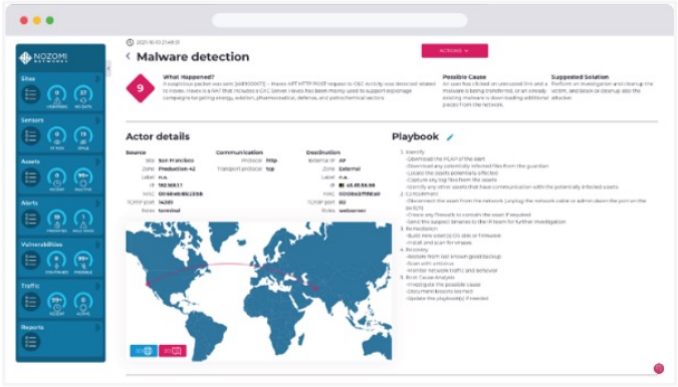
Playbooks

Coordinate a rapid response to an incident or outage using defined playbooks that provide remediation steps for any type of incident.

Import or design your own security playbooks in the Nozomi Networks system to define the process for remediation steps for any type of incident.

Customize playbooks to include specific admins or executives dependent on incident type or location.

Track playbook steps to coordinate incident response as a workflow and integrate with ticketing systems.



The Nozomi Networks Difference

Protocols to support radar systems, radio systems, GPS systems and management systems

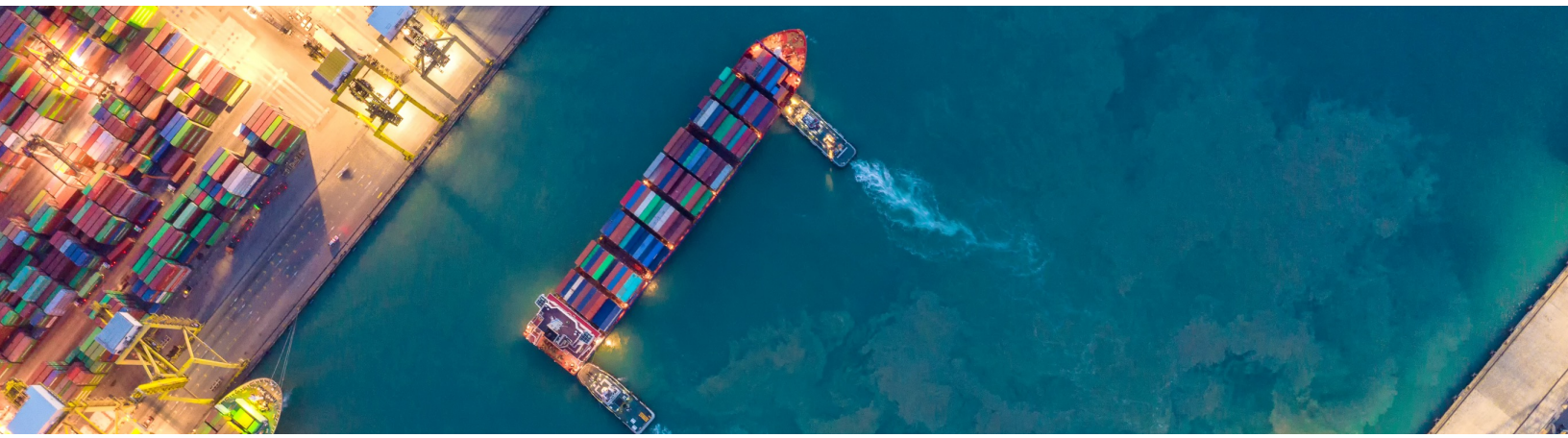
Guardian sensors are **easy to install** while the ships are in ports

Industry-leading, high-accuracy **detection of cyber threats** and **operation anomalies**

Centralized security visibility at scale for dispersed and diverse operation centers and fleets

Competitive pricing and **attractive subscription packages** for both cloud and on-premise solutions

Ruggedized sensors for real-time OT/IoT visibility, cybersecurity and monitoring, certified for use on ships and sturdy enough to use on cranes



NOZOMI NETWORKS

Cybersecurity and Analytics for All Your Connected Devices

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.

NN-SB-MARITIME-8.5x11-001

nozominetworks.com