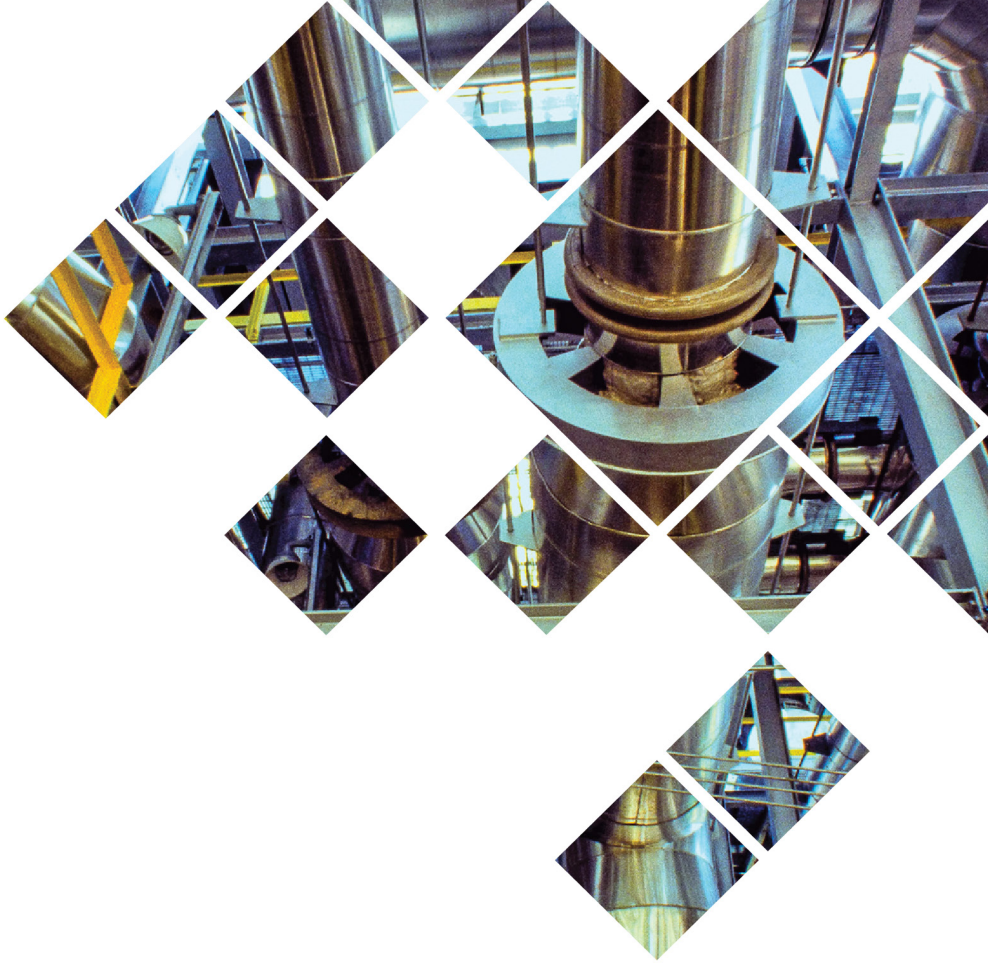
NOZOMI NETWORKS

IKARUS security software



COMPLIANCE MAPPING GUIDE

How the Nozomi Networks Solution Supports the NIS Directive & Regulations

Table of Contents

1. Introduction

The Network and Information Systems Regulations (NIS Regulations), developed under the European Union (EU) **NIS Directive**, place legal obligations on providers to protect critical services by improving cybersecurity.

The regulations are applicable across all EU member states, and cover all operations within scope regardless of the country of ownership. International organisations must ensure that facilities and operations in the jurisdiction of NIS are compliant with the NIS Directive.

Compliance is mandatory, and failure to do so could result in significant fines. Each member state must legislate penalties for non-compliance. In the UK this amount can reach up to £17 million or 4% of global turnover (similar to GDPR penalties).

The regulation came into effect in May 2018. It aims to ensure that operators of essential services (OES) are equipped to deal with increasing cyber threats. Unlike a compliance-based approach with a prescriptive ruleset for organisations to follow, the NIS Directive outlines a set of principles that can be used consistently in decision making to help achieve and maintain a high level of network and information system security.

There has been much debate around the effectiveness of these approaches. This guide does not discuss which approach is better. Rather, it focuses on how the Nozomi Networks solution maps against NIS objectives, and helps organisations drive effective OT and IoT cybersecurity policy. Adopting a measurable, target-driven cybersecurity posture should ultimately result in an organisation having demonstrable 'indicators of good practice' and fulfil the objectives of the NIS Directive.

2. NIS Directive / NIS Regulations Scope

NIS Regulations designed for OES in all EU member states, with the following sectors explicitly included in their scope:

- Energy
- Transportation
- Health
- Water
- Digital Infrastructure

While the NIS Directive may enforce compliance within the sectors outlined above, any organisation may choose to align itself with the NIS principles in order to measure and improve its cybersecurity posture within a recognized framework.

3. NIS Directive Compliance

Given that NIS is a principle-based approach, how does an organisation demonstrate 'compliance' with the NIS Directive?

Ultimately, NIS drives an organisation to take a risk-based approach to cybersecurity. As such, an organisation needs to have an effective risk management process, a defined governance structure and assigned roles and responsibilities relating to cyber resiliency.

To help businesses become cyber-aware organisations that adapt to an ever-changing threat landscape, an assessment framework has been developed that specifies indicators of good practice. In addition, references to industry standards have been provided for each objective defined in the NIS Directive.

3.1. Cyber Assessment Framework (CAF)

The Cyber Assessment Framework offers a systematic method for assessing the extent to which OES are achieving the outcomes specified by the NIS principles. It can be used by competent authorities when assessing OES, or by OES themselves as a self-assessment tool.

The CAF provides 'indicators of good practice' which if aligned with, demonstrate that an organisation has an effective cybersecurity management system and is positioned to drive cybersecurity controls using a risk-based approach that is relevant to the business.

3.2. Industry Standards

In addition to indicators of good practice, organisations can demonstrate compliance within the intent of the NIS Directive by implementing controls that are aligned with industry standards. In the UK, the National Cybersecurity Center (NCSC) has published references to relevant industry standards for each of the key principles.

4. How the Nozomi Networks Solution Supports the NIS Directive

Effective cybersecurity – and NIS compliance – revolves around three core principles: people, process and technology. Focus only on one, and gaps in the organisation's cybersecurity posture will likely remain.

Adopting a trusted security framework such as the NIS Directive, and using the advanced operational visibility, monitoring and risk identification capabilities of the Nozomi Networks solution will help organisations embed security into their processes and improve their cyber resiliency.

The Nozomi Networks solution supports all three pillars of effective cybersecurity. For example, its industrial cybersecurity and visibility functionality provides real-time network intelligence, monitoring and AI-powered threat detection. This enables a proactive approach to risk reduction. It also provides real-time alerts to threats and anomalies within an industrial control network.

The solution includes a flexible and intuitive interface for reporting and operational oversight. This allows an organisation to develop a level of cybersecurity maturity that aligns with and demonstrates compliance with the NIS Directive.

The Nozomi Networks unified solution delivers information that enables an intelligent and targeted approach to cybersecurity within OT and IoT environments. The result is fast track risk reduction for an organisation's most critical assets.

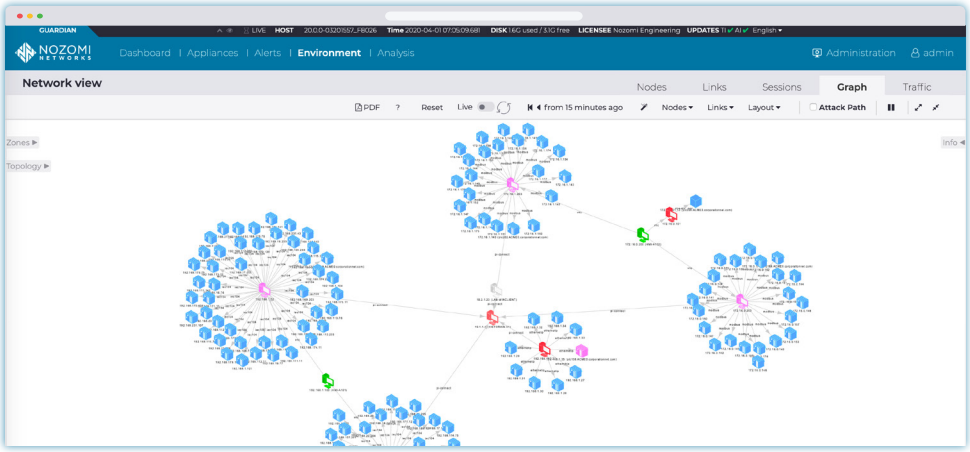
5. Nozomi Networks Mapping to NIS Directive Objectives

Objective	Principles	Summary	Nozomi Networks Support
A. Managing Security Risk	**A1. Governance**	The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.	PARTIAL
	A2. Risk Management	The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services.	COMPLETE
	A3. Asset Management	Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood.	COMPLETE
	A4. Supply Chain	The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers.	PARTIAL
B. Protecting Against Cyberattacks	**B1. Service Protection Policies and Processes**	The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services.	COMPLETE
	B2. Identity and Access Control	The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services.	PARTIAL
	B3. Data Security	Data stored or transmitted electronically is protected from actions such as unauthorized access, modification, or deletion that may cause disruption to essential services.	COMPLETE
	B4. System Security	Network and information systems and technology critical for the delivery of essential services are protected from cyberattacks. An organisational understanding of risk to essential services informs the use of robust and reliable protective security measures.	COMPLETE
	B5. Resilient Networks and Systems	The organisation builds resilience against cyberattacks and system failure into the design, implementation, operation and management of systems that support the delivery of essential services.	COMPLETE
	B6. Staff Awareness and Training	Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the delivery of essential services..	PARTIAL

Objective	Principles	Summary	Nozomi Networks Support
C. Detecting Cybersecurity Events	C1. Security Monitoring	The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and track the ongoing effectiveness of protective security measures.	COMPLETE
	C2. Proactive Security Event Discovery	The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services, even when the activity evades standard signature-based security prevent/detect solutions, or when it is not possible to use signature-based detection, for some reason.	COMPLETE
D. Minimizing the Impact of Cybersecurity Incidents	D1. Response and Recovery Planning	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	COMPLETE
	D2. Lesson Learnt	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	COMPLETE

5.1. NIS Directive Objective A: Managing Security Risk

The Nozomi Networks **Guardian** provides maximum visibility and risk strategy preparedness. Industrial control systems are often insufficiently managed from a security perspective. They may be missing or have inaccurate asset inventories, and lack detailed network architecture diagrams and data flow diagrams. This missing data means that organisations do not have the required information to be able to drive effective governance or risk management. As a result, organisations are faced with the insurmountable task of generating and managing this information.



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

Guardian creates a network diagram that includes precise and detailed asset information. This data is obtained passively and automatically when the appliance is connected to a span or mirror port on the industrial network. This allows an organisation to quickly assess exposure to new and existing vulnerabilities, manage resiliency through critical spares management, and perform audit capabilities. A detailed data flow map is also generated which helps an organisation understand its conformance with internal and industry standards. For example, the IEC 62443 requirements for device communications between levels of the Purdue model.

With the detail provided by Guardian, an organisation can begin to understand and identify:

- Assets that are critical to the operation of essential services
- Security deficiencies

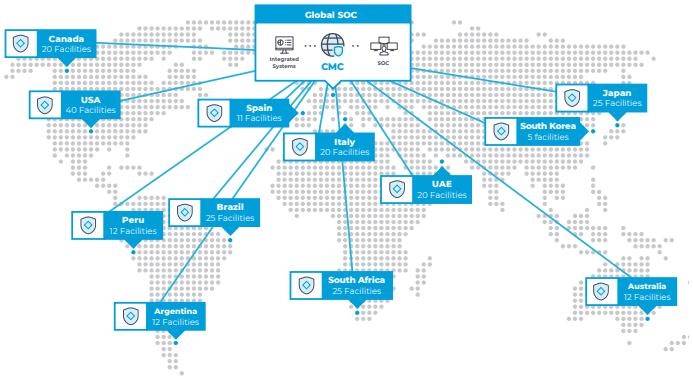
Cyber threats to critical assets become apparent and risk decisions become informed. Mitigations then deliver demonstrable risk reductions that can be clearly communicated to key stakeholders and auditors.

5.2. NIS Directive Objective B: Protecting Against Cyberattacks

With Guardian, implementation of policies and procedures can be verified, producing metrics that demonstrate risk reduction, such as reduction of critical vulnerabilities, reduction in number of unsupported operating systems, etc. By providing detailed and accurate information in real time, Guardian learns the normal operation of the network and process. Once the learning process has been completed, the system switches into protection mode which alerts users to changes in process and network behaviour. Network traffic flow can also be enforced with integration into next generation firewalls, creating a virtualized approach to network segmentation.

Guardian and the Nozomi Networks Central Management Console (CMC) monitor communication paths between network assets, allowing for real-time intelligence to support an access management strategy.

Guardian devices can be aggregated using the CMC, allowing asset monitoring across geo-distributed, multi-department deployments.



The **Nozomi Networks Central Management Console** provides consolidated access to data from all Guardian deploymentsin the field or on the plant floor.

By combining AI and behaviour-based analytics with a rule-based threat detection mechanism, Guardian detects exploitation of vulnerabilities. This provides protection for known vulnerabilities in an environment where routine patching may not be possible. These same mechanisms also provide protection against known threats and malware as well as zero day threats.

This approach to network security means that should conventional protection mechanisms fail, attempted breaches would be detected, minimizing any impact from attacks that would otherwise remain undetected.

The network mapping and visualization capabilities of Guardian support good network design – for example leveraging information on how traffic flows in an existing network. Virtual segmentation can be used to develop an appropriate segmentation strategy that is both achievable and maintainable. This approach to virtual segmentation can enforce traffic flow, or provide alerts against policy breaches, providing an additional level of security in line with a defence-in-depth approach to security.

Network mapping also supports NIS regulations with respect to data storage and system dependency mapping. With this information, an organisation can better understand the impact of corruption or loss of availability of this data, enabling a focused and risk-based approach to the protection of critical services. Incident response processes can also be better informed and enabled to rapidly restore essential services following disruption.

Guardian provides a level of monitoring at the network and process layer that has not previously been attainable. An unapparelled level of process integrity can be achieved, thanks to real-time alerts to any changes in process data, communication links or assets. With industry leading integrations with traditional IT security tools, security teams can leverage the power of the Nozomi Networks solution within their existing toolsets.

5.3. NIS Directive Objective C: Detecting Cybersecurity Events

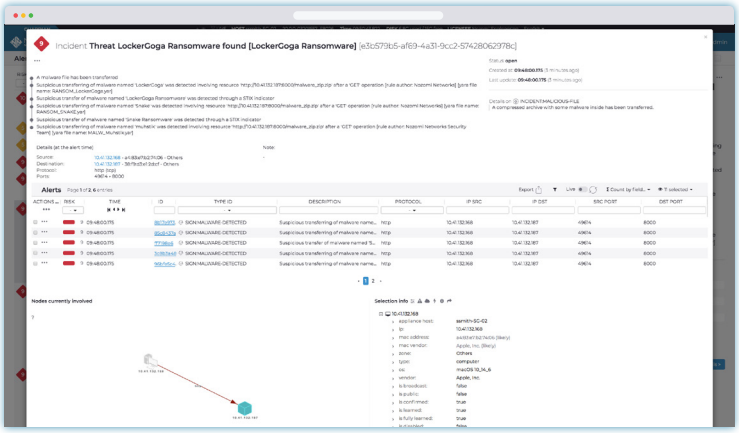
Based on comprehensive AI behaviour-based analytics and signature-based detection engines, Guardian reliably detects security incidents, policy breaches and process anomalies that could affect the delivery of essential services. Covering the entire industrial control network environment, Guardian learns and understands normal network and process behaviour. Changes from known state results in alerts, allowing users to detect known “indicators of compromise” (IoCs) and zero-day threats.

The Nozomi Networks solution is built with full control of its entire technology stack, including the firmware and operating system on the physical appliance, in addition to the software solution itself. The system is hardened and subject to regular in-depth security checking. Nozomi Networks manages system patching through product updates where required. This means that the total cost of ownership is minimized while still delivering a highly secure platform.

The solution also provides industry-leading alert capabilities with regards to incident management. Security alerts can be prioritized, resolved and flagged allowing incident responders to focus efforts on genuine security issues.

Nozomi Networks Threat Intelligence service delivers up-to-date threat intelligence to Guardian, making it easy to detect threats and identify vulnerabilities in OT and IoT environments. Threat Intelligence is produced and curated by the Nozomi Networks Labs team of expert security researchers. Nozomi Networks also supports the addition of custom signatures provided by industry sources working closely on threats specific to a particular sector.

Nozomi Networks Asset Intelligence service continuously updates Guardian with rich OT and IoT device profile and behavioural data. It enables Guardian appliances to precisely classify assets, which accelerates the the learning process, and provide detailed alerts that pinpoint significant security and operational anomalies.



Smart Incident showing related alerts and security context.

5.4. NIS Directive Objective D: Minimizing the Impact of Cybersecurity Incidents

The Nozomi Networks solution provides detailed information across all aspects of an industrial network, supporting enhanced incident response capabilities. Detailed information on network traffic flow and dependencies helps with incident response planning, covering multiple attack scenarios.

AI and behaviour-based analytics provide detailed and accurate security event alerting with event correlation and root cause identification. Security event information is available in the Nozomi Networks solution. In addition, packet traces can also be downloaded from the appliance and made available to security and forensics teams for in-depth packet level analysis.

Guardian also ingests data in the form of network packet captures (PCAPs). The solution can be used to simulate an attack, as a training tool, and to help organisations exercise their incident response procedures. The latter is a requirement of NIS, as well as all current security standards processes.

Detailed event correlation and attack vector analysis enabled by the Guardian appliance can be fed back into the incident response and security protection policies. This helps ensure that lessons are learned from security incidents, and leads to a more robust cybersecurity posture going forward.

6. Conclusion

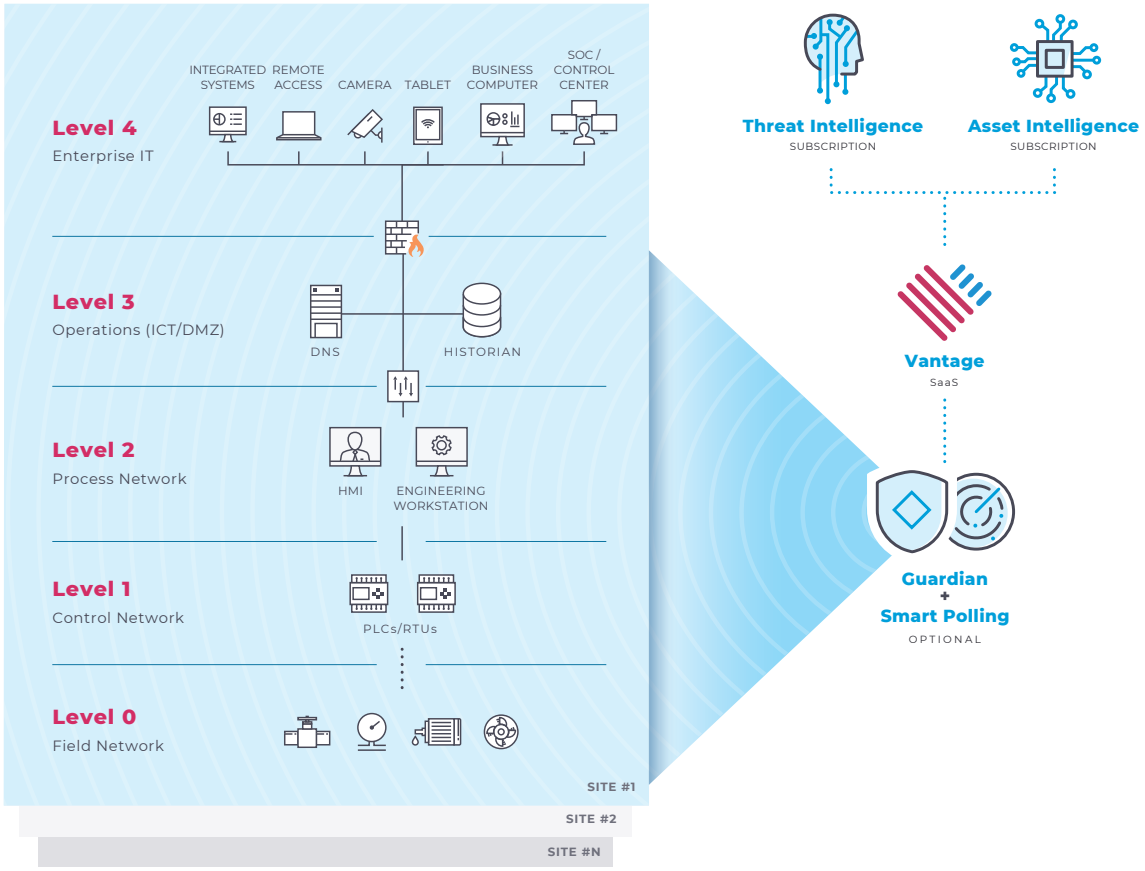
The key to effective network monitoring lies in using information to inform an accurate risk view.

The Nozomi Networks solution provides detailed asset identification and network discovery that helps an organisation achieve deep visibility into the status of its OT and IoT networks. Armed with information, an organisation can identify risks and threats active in its environments. Insight also allows it to implement an effective and targeted mitigation program that maximizes the use of limited human resources, while making informed risk decisions that are both efficient and effective.

Nozomi Networks industry-leading integrations with standard IT security platforms and intuitive user interface deliver value to engineers, IT and security teams alike. By providing contextualized alerts, organisations can rapidly respond to threats in their ICS environments. With customisable dashboards and reporting, organisations can deliver target driven risk reduction across the global business.

Nozomi Networks Guardian is a fundamental tool that helps organisations achieve compliance with the NIS Directive and NIS Regulations.

Sample Deployment Architecture



Products and Services

SAAS

Vantage accelerates security response with unmatched threat detection and visibility across your OT, IoT and IT networks. Its scalable SaaS platform enables you to protect any number of assets, anywhere. You can respond faster and more effectively to cyber threats, ensuring operational resilience.

Requires Guardian sensors.

EDGE OR PUBLIC CLOUD

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

SUBSCRIPTION

The **Threat Intelligence** service delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of emerging threats and new vulnerabilities, and reduce your mean-time-to-detect (MTTD).

GUARDIAN ADD-ON

Remote Collectors are low-resource sensors that capture data from your distributed locations and send it to Guardian for analysis. They improve visibility while reducing deployment costs.

EDGE OR PUBLIC CLOUD

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

SUBSCRIPTION

The **Asset Intelligence** service delivers regular profile updates for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-respond (MTTR).

GUARDIAN ADD-ON

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

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NIS-C-8.5x11-006

nozominetworks.com