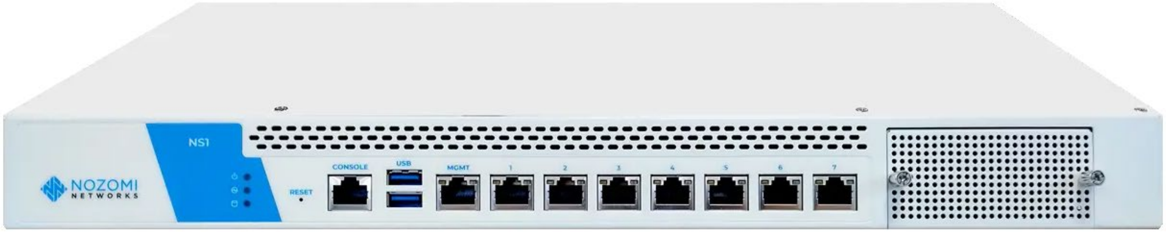
OT Security Sensor Guardian™ by Nozomi Networks

OT Security Sensor to monitor industrial networks in real time

The OT Security Sensor Guardian™ by Nozomi Networks is a comprehensive passive security solution for industrial networks that enables real-time monitoring, inventory and detection of cyber threats, vulnerabilities, and anomalies.



Integration and Basic Features

- ✓ Quick and easy to install without disruption.
- ✓ Seamless integration into existing security systems.
- ✓ Self-learning system to adapt to infrastructure changes.
- ✓ Threat detection including ransomware, malware, and DDoS attacks.
- ✓ Scalable for every company size and requirement.
- ✓ Supports Rugged Guardians for extreme conditions and the Nozomi Arc Endpoint Sensor for advanced asset monitoring.

www.IKARUSsecurity.com/industrial-cyber-security

Protocol support

Guardian supports a comprehensive range of OT/IoT and IT protocols, enhancing visibility and security monitoring across diverse industrial environments. This ensures the integrity and availability of critical processes while promoting full network transparency.

Regulatory Compliance

By implementing the Guardian sensor, companies can meet the core requirements of the NIS2 Directive—leading to enhanced security and improved regulatory compliance.

IKARUS OT Security Professional Services

Combining IKARUS OT Security Professional Services with Nozomi Networks technologies provides a strong foundation for establishing and expanding an effective OT/IoT security program. This approach helps minimize cyber risks, ensures compliance with regulatory standards, and strengthens operational resilience.

Typical Use Cases for Deploying Guardian Sensors

» **Asset Management and Risik Assessment**: Gain full visibility and classification of assets within the network, along with identification of vulnerabilities and threats.

» **Real-Time Detection**: Identify vulnerabilities, misconfigurations, threats, and attacks in real time to enable rapid response to security incidents.

» **Network Segmentation and Access Control**: Support the implementation of a secure network architecture by detecting and managing network flows and enforcing segmentation policies.

» **Compliance and Reporting**: Facilitate compliance with relevant security standards and regulations, including automated reporting and audit support.

Your Next Step Toward Industrial Security and Resilience:

Proof of Value (PoV)

The Proof of Value (PoV) allows companies to experience the effectiveness and tangible benefits of the OT security sensor within their own network environment. It serves as a critical step in the implementation process of security solutions—particularly in the field of Operational Technology (OT).

During the PoV phase, Guardian sensors and related services are deployed in a real-world setting to deliver practical insights into the company's current OT cybersecurity posture, existing risks, and operational resilience. The objective of this phase is to generate concrete, measurable outcomes that help decision-makers recognize the necessity and value of investing in advanced OT security measures.

The PoV provides a solid foundation for informed decision-making and supports the strategic planning of security initiatives. It fosters transparency around the performance and impact of the proposed solutions, illustrating how they contribute to strengthening the organization's cybersecurity posture.

Benefits of the PoV

- ✓ Automated Asset Discovery
- ✓ Visibility into Assets and Network Communication
- ✓ Real-Time Detection of Threats, Vulnerabilities, and Anomalies
- ✓ Interactive Network Visualization
- ✓ Monitoring of Operationally Relevant Process Variables

Get in Touch:

☎ +43 1 58995-500
✉ sales@ikarus.at

CERTIFIED NOZOMI PLATINUM PARTNER

CERTIFIED NOZOMI MSSP PARTNER

OT Security Add-Ons and Complementary Solutions

Asset Intelligence

Asset Intelligence is a key feature within Nozomi Networks' OT security solutions that enables organizations to gain a complete and continuous overview of all their OT and IoT devices. It delivers accurate insights into device types, manufacturers, behaviors, configurations, and the communication protocols in use.

By integrating Asset Intelligence into your security architecture, cyber threats and operational anomalies can be detected faster and more effectively. Through continuous correlation of network activity with an extensive database of device profiles and learned behavioral baselines, the system helps reduce false positives and ensures focus remains on truly security-relevant events.

Smart Polling

As an advanced add-on to the Guardian OT Security Sensor, Smart Polling enables deep and granular monitoring of network infrastructure. It enhances passive monitoring by introducing active queries that gather detailed information on operating systems, software, firmware versions, and device patch levels.

Smart Polling empowers security teams to accurately assess vulnerabilities and make informed prioritization decisions for patch management and other security measures. This feature is especially valuable in environments where full visibility and up-to-date asset information are critical to maintaining the security and integrity of the network.

Threat Intelligence

Nozomi Networks' Threat Intelligence delivers comprehensive, up-to-date information on the latest security threats and vulnerabilities that may affect industrial networks. The service includes the distribution of packet rules, YARA rules, and STIX indicators—based on in-depth analysis and real-time data.

With Threat Intelligence, security teams can take proactive action by detecting and understanding threats before they impact the network. Organizations can strengthen their defense strategies by leveraging detailed alerts and analysis, enabling fast identification and response to potential attacks.

Central Management Console (CMC)

The Central Management Console (CMC) by Nozomi Networks is a centralized platform for monitoring, managing, and analyzing network security data across multiple sites and entities. This powerful management solution provides security teams with comprehensive visibility into all OT, IoT, and IT assets within the enterprise network.

The CMC offers advanced capabilities for event and alarm management, along with seamless integration of threat intelligence. By centralizing security data and events, the CMC makes it easier to identify patterns and anomalies that span across different locations or devices—enabling more efficient and effective responses to security incidents.

IKARUS MSSP Vantage

IKARUS MSSP Vantage is an innovative solution specifically designed to scale, manage, and optimize the security of networks and industrial systems across large and complex enterprise environments.

The platform empowers organizations to centrally control their security and monitoring operations while gaining visibility into thousands of devices and systems across the globe. Leveraging advanced analytics and machine learning capabilities, Vantage provides proactive monitoring and threat detection that goes beyond traditional security approaches. This enables early identification and mitigation of complex cyber threats and ensures continuous improvement of security in dynamic and ever-evolving industrial environments.

Nozomi Arc

Arc is a specialized software component designed for enhanced data collection and analysis from endpoints and network devices that fall outside the direct monitoring scope of standard Guardian sensors. It enables detailed monitoring and evaluation of assets such as workstations, servers, and other critical endpoints within the industrial network.

By implementing Arc, security teams gain visibility into the activities and security posture of previously overlooked blind spots. This includes log file analysis, insider threat detection, and monitoring of connected USB devices. This deeper and broader visibility strengthens the overall security architecture and enhances the ability to detect and defend against threats that would otherwise go unnoticed.