NOZOMI NETWORKS

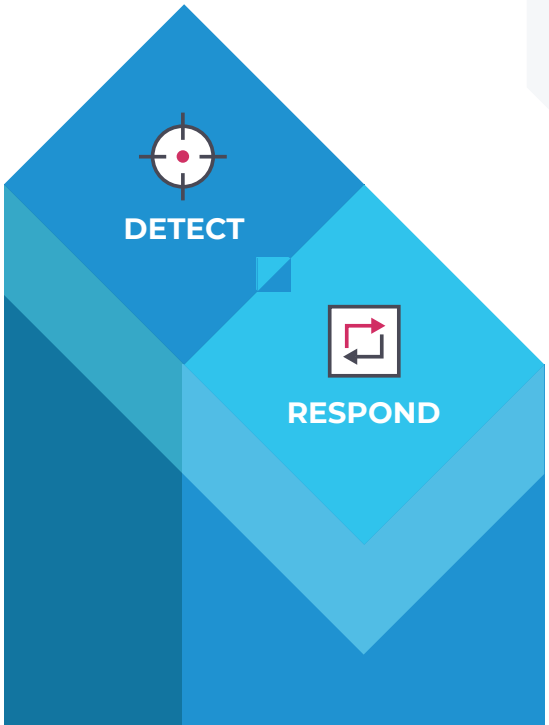
DATA SHEET

Threat Intelligence

Detect Emerging OT and IoT Threats and Vulnerabilities

Nozomi Networks **Threat Intelligence**™ continuously updates **Guardian**™ sensors with rich data and analysis so you can detect and respond to emerging threats faster.

Guardian correlates Threat Intelligence information with broader environmental behavior to deliver maximum security and operational insight.



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

Detect

Intelligence that Reduces the Mean-Time-to-Detect (MTTD)

Rapidly Detect Threats and Identify Vulnerabilities

Up-to-Date Threat Intelligence

Delivers continuously updated OT and IoT threat and vulnerability intelligence

Detects early stage and late stage advanced threats and cyber risks

Identifies assets at risk of attack with OT and IoT vulnerability assessment

Extensive Threat Indicators

Provides detailed threat information:

- Yara rules
- Packet rules
- STIX indicators
- Threat definitions
- Threat knowledgebase
- Vulnerability signatures

Significantly Strengthen Your Security Posture

OT and IoT Threat Insights

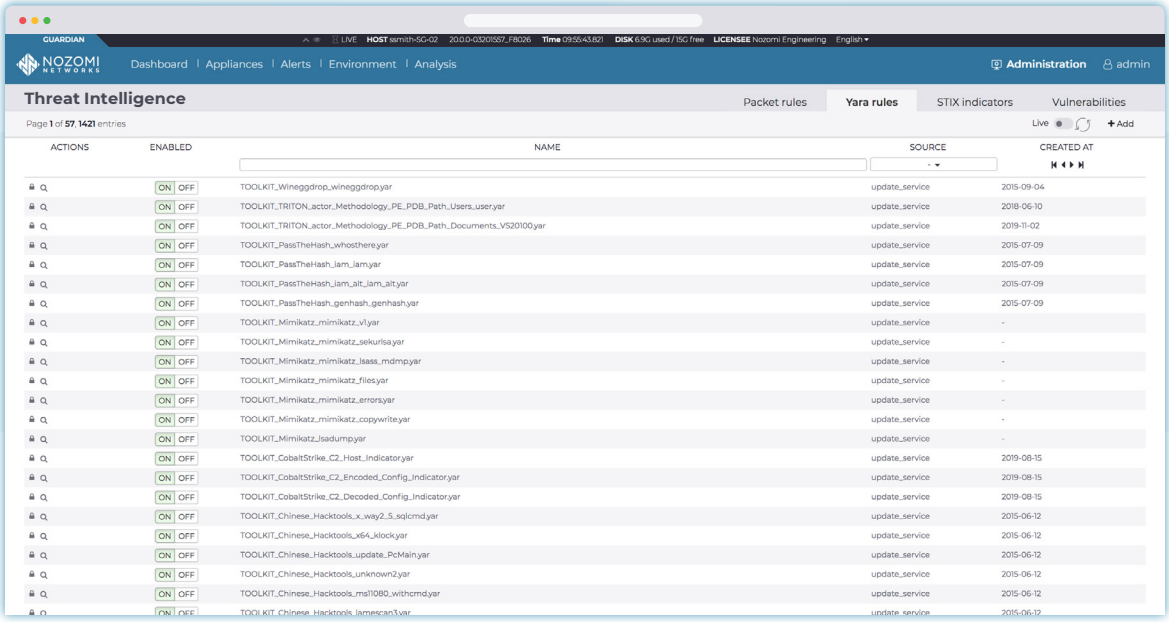
Provides an accurate assessment of your security posture through full network visibility with integrated threat intelligence

Provides the information you need to effectively manage OT and IoT risks

High Performance for Fast MTTD

Conducts analysis on Guardian sensors for accelerated threat detection

Delivers immediate, accurate alerts grouped into incidents for fast response



Threat Intelligence provides continuously updated and detailed threat information.

Respond

Detailed Alerts and Forensic Tools for Fast Response

Quickly Respond Using Detailed, Accurate Information

Accurate Threat Intelligence

Ensures valid threat insights based on the expertise of Nozomi Networks Labs, a team of specialized security researchers

Delivers accurate rules subjected to rigorous testing before release to minimize false positives

Detailed, Helpful Alerts

Provides detailed alerts that pinpoint what occurred

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

Swiftly Analyze Incidents and Simplify IT/OT Processes

Simplified IT/OT Security Processes

Reduces costs with a single, comprehensive OT and IoT threat detection and vulnerability assessment

Integrates with IT security infrastructure for streamlined security processes, see: **nozominetworks.com/integrations**

Harmonizes security data across enterprise tools for cohesive response

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

Continuous Threat Research reduces the time to detect active threats and vulnerabilities.

Products and Services

SAAS

Vantage accelerates digital transformation with unmatched security 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

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.

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 **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).

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

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

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.

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.

DS-TI-8.5x11-006

nozominetworks.com