PLATFORM BRIEF

Nozomi Vantage

The OT/IoT Cyber Resilience Platform

Get the context, control and confidence to protect your most critical environments.

The Challenge

Securing Converged OT, IoT and IT Environments

OT, IoT and IT systems are increasingly interconnected, creating complex environments that are harder to secure and easier for attackers to exploit. As convergence expands the attack surface, organizations also face growing pressure to demonstrate resilience, safety and compliance across digital and physical operations. In these high-stakes environments, cyber incidents can affect far more than data — they can disrupt operations, create safety risks, drive revenue loss and trigger regulatory consequences if not contained quickly..

To reduce cyber risk and protect operations, security and OT teams need to:

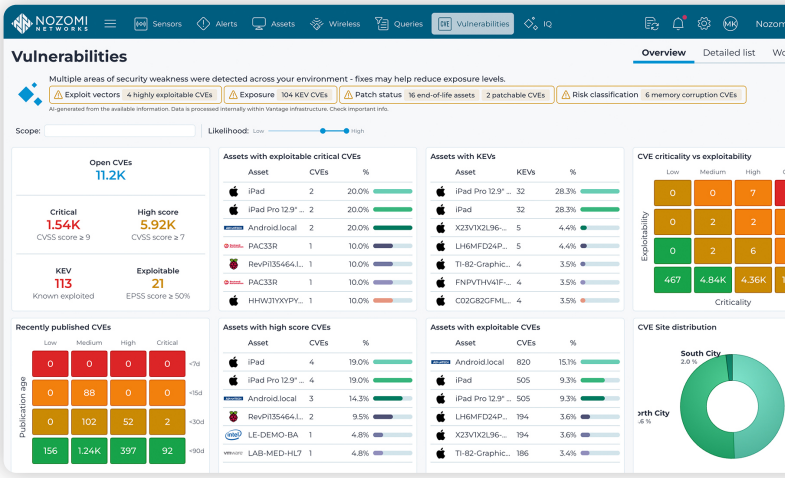
- **Eliminate blind spots** across IT, OT and IoT environments with unified visibility and monitoring.
- **Secure legacy OT systems and IoT devices** that were never designed to withstand modern threats
- **Build and operationalize incident response capabilities** for cyber-physical environments.
- **Improve security outcomes with limited resources** through automation and operational efficiency.

The Solution

Nozomi Vantage: A Unified Platform for Cyber-physical Resilience

Nozomi Vantage is a cloud-based OT/IoT cyber resilience platform that unifies visibility, vulnerability management, threat intelligence, detection, response and risk management. It helps security and operations teams identify risk earlier, respond faster and reduce the likelihood of operational disruption.

With Nozomi Vantage, teams can gain context, take control and build confidence in their cyber resilience across converged cyber-physical environments.



Three Ways Nozomi Vantage Strengthens Cyber-physical Resilience

Gain Context with Real-time Asset Visibility and Exposure Management

Unified OT and IoT visibility:
Continuously discover and map every connected asset — from sensor to software — across wired and wireless networks. Gain a real-time view of assets, communications, vulnerabilities and behavioral anomalies to eliminate blind spots.

Proactive Exposure Management:
Identify vulnerabilities in legacy and networked devices that were never designed for security. Integrated vulnerability management and anomaly detection help reduce risk before attackers can exploit weaknesses.

Take Control with OT/IoT-specific Detection and Response

Purpose-built threat intelligence and monitoring:
Leverage OT- and IoT-specific threat intelligence, curated by Nozomi Networks Labs, to identify early indicators of compromise in sensitive and unpatchable environments.

Coordinated detection and response
Enable IT and OT teams to act in lockstep with high-fidelity detections, response playbooks and workflows across the cyber-physical environment. Non-intrusive monitoring and prioritized remediation guidance help teams contain threats before they affect operations or safety.

Build Confidence with Measurable Risk and Resilience

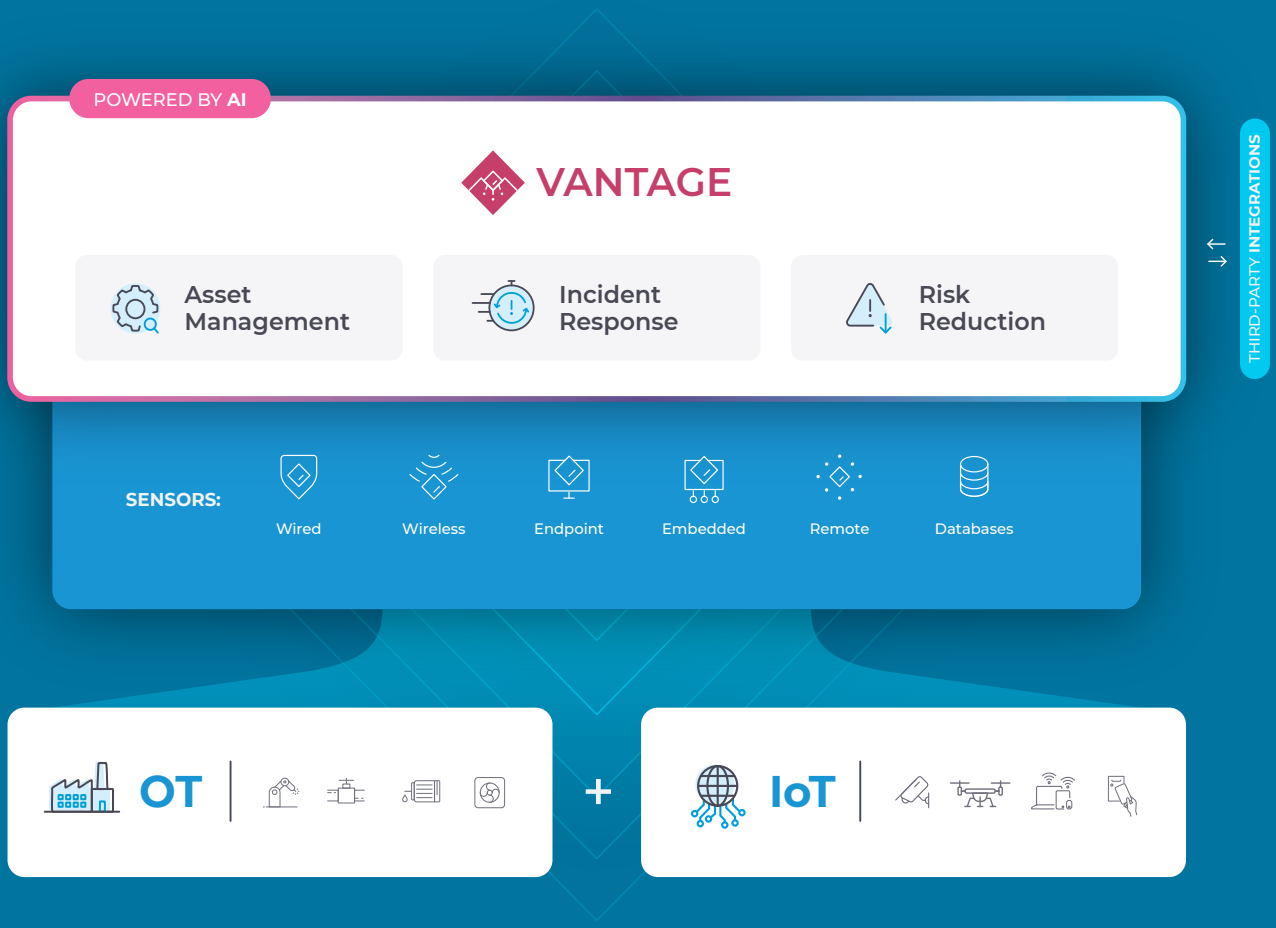
Quantified cyber risk reduction:
Measure risk with multi-factor scoring at the asset, zone, site and enterprise levels. Standards-informed metrics provide a consistent framework to track and improve cyber resilience over time.

Actionable risk management
Use customizable risk scoring and prioritized guidance aligned to operational realities, so security and operations teams can focus on the most critical risks first.

Demonstrated resilience and compliance
Use executive dashboards, benchmarks and audit-ready reports to communicate risk posture, show progress over time and support compliance efforts. This helps leaders demonstrate resilience to internal and external stakeholders.

A Complete Platform for OT/IoT Cyber Resilience

Gain context, control and confidence to withstand cyber threats — without disrupting the physical world.



PLATFORM COMPONENTS

VANTAGE Only cloud-scale, cyber-resilient architecture for OT/IoT security

Asset Management

Guardian - Deep OT/IoT network visibility and threat detection in a single sensor

Guardian Air - Full-spectrum wireless monitoring for industrial environments

Arc - Endpoint-level visibility and threat detection from any industrial host

Arc Embedded - First security sensor that runs inside industrial controllers

Integrations with third-party asset databases

Asset Intelligence - AI-driven asset enrichment to build complete and accurate a sset profiles

Incident Response

Proactive response with integrations to network, endpoint and SOC tools

IR playbooks to give SOC teams OT/IoT context

OT/IoT specific **threat and anomaly detection**

Threat Intelligence - Actionable OT/IoT threat and vulnerability intelligence to stay ahead of attackers

Risk Quantification

Multifactor custom **risk scoring**

Benchmarks and **dashboard**

Board-ready **metrics**

Powered by AI

Vantage IQ - Your OT/IoT-smart AI assistant capable of uncovering insights, writing rules, assessing compliance and generating board-ready metrics

Key Features

Complete Asset Context

Passive and active monitoring across **wired, wireless, endpoint and embedded sensors** for comprehensive data collection

Vulnerability management and AI-driven anomaly detection to reduce exposure continuously

OT/IoT-specific Security Controls

OT/IoT threat intelligence enriched with Nozomi Networks Labs research

Rich threat detection, response and forensics capabilities for operational environments

Comprehensive integrations and playbooks enabling streamlined response workflows across teams

Risk Management & Compliance

Multi-factor risk scoring at asset, zone, site and enterprise levels

Customizable scores enabling organizations to align risk models with their operational realities

Prioritized recommendations helping security and operations teams focus on the highest-impact risks.

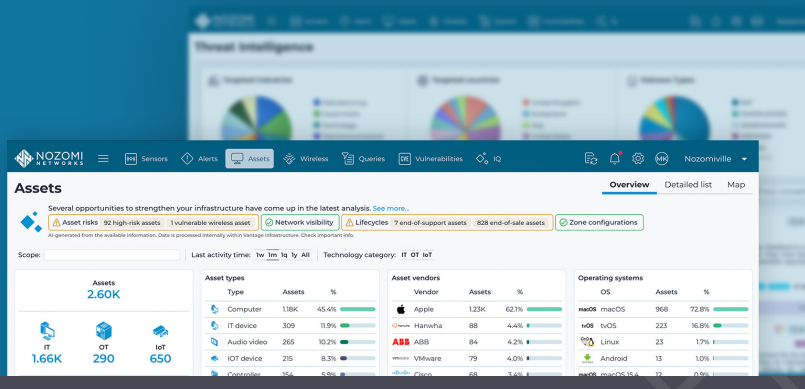
Platform

Only hybrid & resilient architecture that scales with your business

Purpose-built AI transforms OT/IoT telemetry into actionable intelligence

See Nozomi Vantage in action

Request a Demo | nozominetworks.com/demo



© 2026 Nozomi Networks, Inc. | All Rights Reserved.