Nozomi Networks Platform

One platform for unified visibility and security of OT and IoT environments

Nozomi Networks' industrial cybersecurity solutions are designed to protect mission-critical environments across all industries and sectors, including today's OT and IoT physical devices and processes.
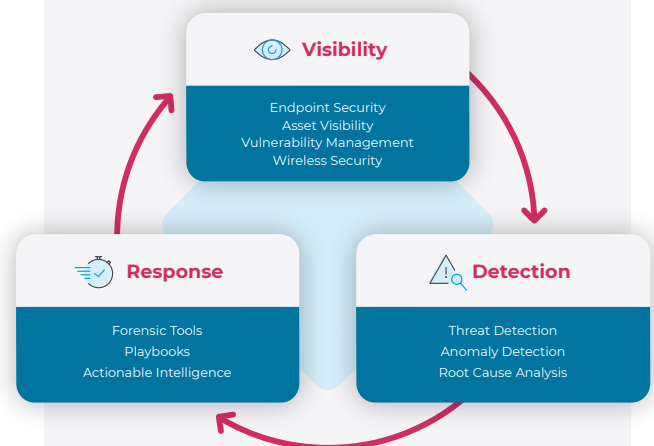
We uniquely combine network (wired and wireless) and endpoint visibility, threat detection and AI-powered analysis for faster, more effective response.

We deliver:

- Unified visibility and monitoring of network and endpoint assets in your OT and IoT environments

- Unmatched protocol coverage and comprehensive, accurate analysis of dozens of OT, IoT and IT protocols

- AI-driven insights and root cause analysis help to guide remediation efforts

- Proven in the largest and most complex customer environments around the world

- Seamless integration with SIEM and SOC systems for closing operational visibility and security gaps

- Rigorous forensic analysis for incident response and greater insights

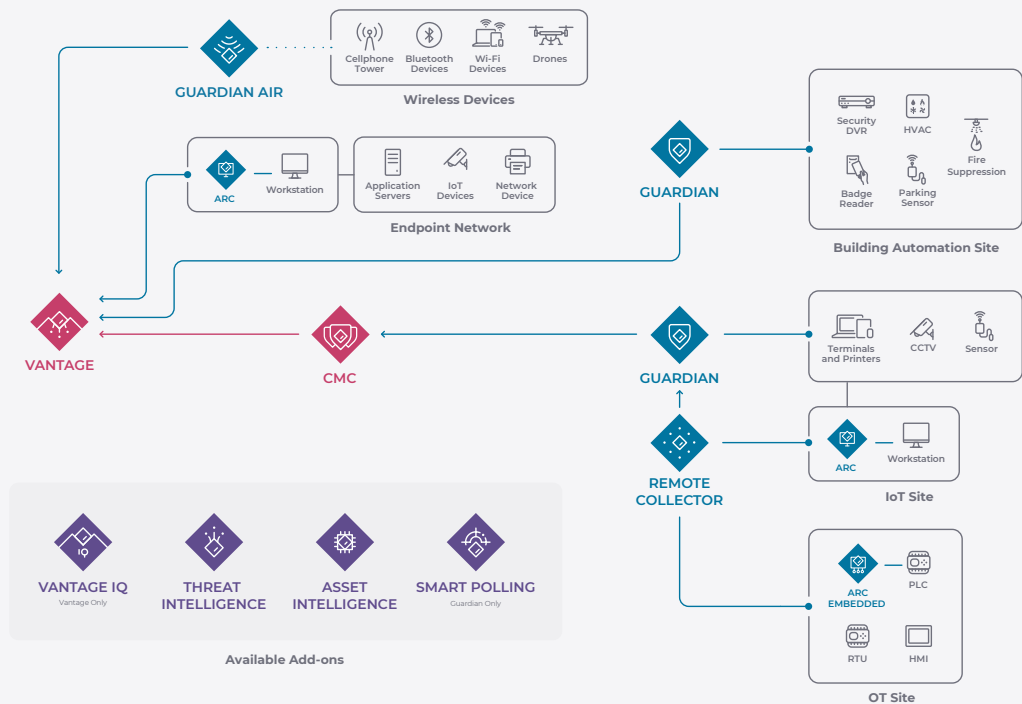- Global partner ecosystem for purchasing and service needs

The Nozomi Networks platform methodology revolves around the incident response lifecycle phases of Visibility, Detection, Response.

Our platform provides key features to support typical administrative, security and networking tasks for each of the phases as described below.

Visibility
Endpoint Security
Asset Visibility
Vulnerability Management
Wireless Security

Response
Forensic Tools
Playbooks
Actionable Intelligence

Detection
Threat Detection
Anomaly Detection
Root Cause Analysis

Build Your Solution

The Nozomi platform provides a wide range of components and form factors to flexibly deploy and scale on-premises and in the cloud in a wide range of industrial and corporate environments.

GUARDIAN AIR

Wireless Devices — Cellphone Tower, Bluetooth Devices, Wi-Fi Devices, Drones

Endpoint Network — ARC, Workstation, Application Servers, IoT Devices, Network Device

GUARDIAN

Building Automation Site — Security DVR, HVAC, Fire Suppression, Badge Reader, Parking Sensor

VANTAGE

CMC

GUARDIAN — Terminals and Printers, CCTV, Sensor

REMOTE COLLECTOR

IoT Site — ARC, Workstation

OT Site — ARC EMBEDDED, PLC, RTU, HMI

Available Add-ons

VANTAGE IQ — Vantage Only

THREAT INTELLIGENCE

ASSET INTELLIGENCE

SMART POLLING — Guardian Only

MANAGEMENT

VANTAGE

A SaaS solution for unified security monitoring and risk management. FIPS compliant.

CENTRAL MANAGEMENT CONSOLE

Centralized visibility and management of Guardian sensors in distributed sites.

NETWORK SENSORS

GUARDIAN

Industrial strength sensors for comprehensive visibility and network monitoring. ANSSI-certified and FIPS-compliant.

GUARDIAN AIR

Plug and play sensor for visibility and monitoring of wireless connected assets.

REMOTE COLLECTOR

Low-resource sensors for offshore, remote, and distributed locations.

ENDPOINT SENSORS

ARC

Enhanced data collection and asset visibility across endpoint attack surfaces.

ARC EMBEDDED

Delivers enhanced OT/IoT security and visibility with world's first security sensor embedded into the lowest levels of ICS networks.

ENHANCED CAPABILITIES

VANTAGE IQ

AI-based data analysis that helps security teams close security gaps and speed response.

SMART POLLING

Active polling to identify non-communicating assets and rogue devices.

THREAT INTELLIGENCE

Detect emerging OT and IoT threats and vulnerabilities. Available for third-party platforms.

ASSET INTELLIGENCE

Stay up-to-date with known information about assets and anomalies.

Want to learn more? Visit nozominetworks.com/products

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com