SOLUTION BRIEF

Full Spectrum Visibility and Threat Detection for IoT Networks

Deeper Insights for IoT Vulnerability Management, Cyber Threats, and Process Optimization

The Internet of Things (IoT), Internet of Medical Things (IoMT), and Operational Technology (OT) devices now make up more than 30% of the assets on enterprise networks. Despite this rapid proliferation, IoT devices pose immense cybersecurity risks as they are often stripped-down platforms with virtually no security features and are often accessible by external users via wireless networks.

In fact, many of these devices, which often ship with their own vulnerabilities, are rarely patched or updated. They are susceptible to a number of well-documented exploits by increasingly sophisticated and well-funded attackers. It is especially concerning when IoT devices are network-connected to the larger IT infrastructure, data center, and cloud networks without internal segmentation or access controls.

> "The product is providing the visibility into our environment we have never had before. I have enjoyed the partnership with Nozomi, they have listened to all of our use cases and assisted whenever possible."
>
> **Cybersecurity Architect, Industrial Manufacturing Company ›**

> "Nozomi's technology has passed a rigid vendor selection and weeks of proof of value. Its adoption allows us to increase the visibility of the industrial network with a double benefit. The cyber security side is able to detect deviations from normal behavior as well as identify the main attack vectors by integrating with the company SIEM."
>
> **CISO, Energy Production Company ›**

Fueled by automation and digital transformation, plus the widespread adoption of IoT technologies, security challenges are increasing rapidly. adoption of IoT technologies, connectivity and security requirements are also increasing rapidly. Traditional security approaches, however, are proving inadequate for many of these IoT environments, due to the unique requirements of a wide range of industries, processes and device protocols that must be analyzed and protected.

Smart manufacturing, smart buildings, smart cities, smart grids, smart healthcare — all these verticals leverage IoT platforms and IT integration to respond to market needs faster and to reduce costs. As defenders and engineers who need to keep systems running securely and safely, it's important to understand how IoT environments can be efficiently secured.

IoT Security Challenges

- Proliferation of devices as part of operational processes stretch ability of admin teams to manage assets efficiently, reduce risk, maintain visibility and increase attack surface.
- Stripped down, single function or low cost IoT devices typically lack defensive security features of full-featured operating systems.
- Many classes of IoT devices in industrial processes are rarely patched or updated to remove vulnerabilities.
- Wireless connectivity to IT networks and lack of network segmentation make IoT devices a common entry point for external attacks.
- Breaches of IoT devices that support the operational networks run an inordinate risk of disrupting business operations and materially impact revenue.

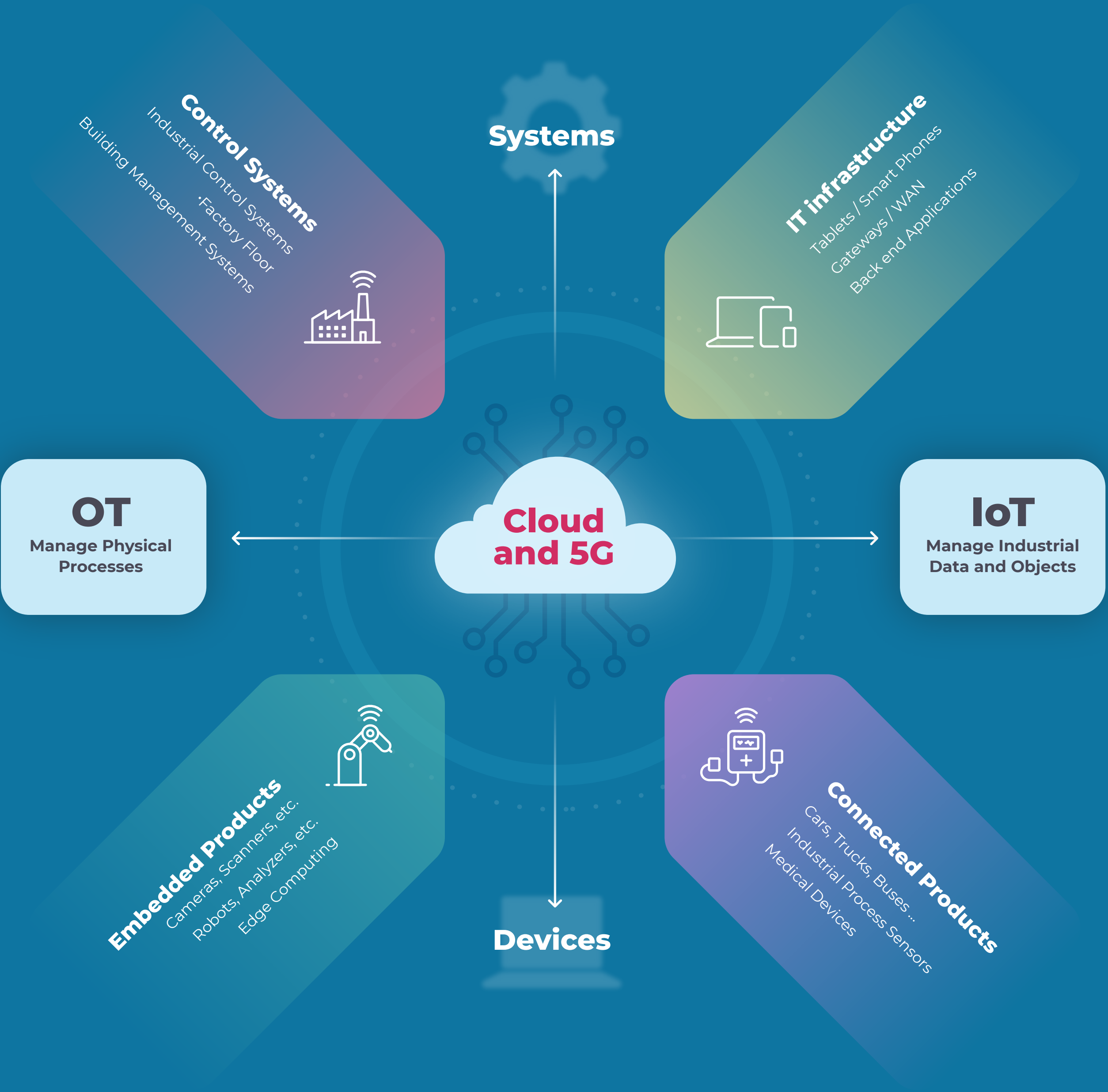
Nozomi Networks Benefit Highlights

Automate the analysis of IoT devices and network traffic to quickly identify potential threats and eliminate vulnerabilities.

Maintain visibility of all network assets, including known vulnerabilities, device types, and baseline behavior to manage security risks.

Leverage data and process knowledge to anticipate process issues, predict maintenance requirements and diagnose problems.

Unifying asset intelligence, threat detection and process visibility across divergent industrial and network environments.



Systems

Control Systems
Industrial Control Systems
·Factory Floor
Building Management Systems

IT infrastructure
Tablets / Smart Phones
Gateways / WAN
Back end Applications

OT
Manage Physical Processes

Cloud and 5G

IoT
Manage Industrial Data and Objects

Embedded Products
Cameras, Scanners, etc.
Robots, Analyzers, etc.
Edge Computing

Connected Products
Cars, Trucks, Buses ...
Industrial Process Sensors
Medical Devices

Devices

The Nozomi Networks Solution

Nozomi Networks delivers cybersecurity and analytics for IoT-based processes. With a zero-trust approach to network visibility and security for industrial digitization, we provide real-time integration of security and asset intelligence that is purpose-built for enabling reliable operations. The Nozomi Networks solution detects and secures the growing number of devices, the increasing amount of data, and the rapidly evolving number of network vulnerabilities and threats to critical infrastructure.

Nozomi Networks Guardian and Vantage platforms automate a full life cycle of IoT vulnerability management, threat detection, diagnosis, and remediation to ensure you are addressing risks in real-time. Our platforms provide the deepest insight into the widest range of IoT devices and processes to deliver actionable intelligence when and where you need it.

Nozomi Networks allows organizations to:

Anticipate

Detect potential issues in your IoT networks by analyzing device inventory and vulnerabilities, changes in process variables, or network traffic. Address issues before they can be exploited or disrupt operations.

Diagnose

Understand where threats may be coming from, or when maintenance may be required. Quickly identify root cause issues and where to direct remediation efforts.

Respond

Manage response with guided playbooks that coordinate and track specific remediation efforts based on the problem type. Get help in prioritizing risk reduction efforts using our asset intelligence and operational awareness.

MQTT

Understanding the MQTT Protocol and Gaining Operational Insights

MQTT is an OASIS standard messaging protocol for IoT. It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth. MQTT today is used in a wide variety of industries, such as automotive, manufacturing, telecommunications, oil and gas, etc.

MQTT is designed for scalability to millions of devices and collect data from sensors at a much higher rate and more frequently than traditional OT environments. The protocol uses a publisher to broker model rather than client/server handshake. Client applications subscribe to an MQTT broker to access the relevant data they need.

MQTT is one of many OT and IoT protocols that our solution provides deep insights for. In addition, Nozomi Networks can monitor process data and identify and correlate changes to provide insight to potential issues, predict maintenance or help optimize the process.

Products and Services

SAAS

Vantage

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

Guardian

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

Asset Intelligence

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

Threat Intelligence

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

Smart Polling adds discreet 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.

nozominetworks.com