NOZOMI NETWORKS

The Leading Solution for OT & IoT Security and Visibility

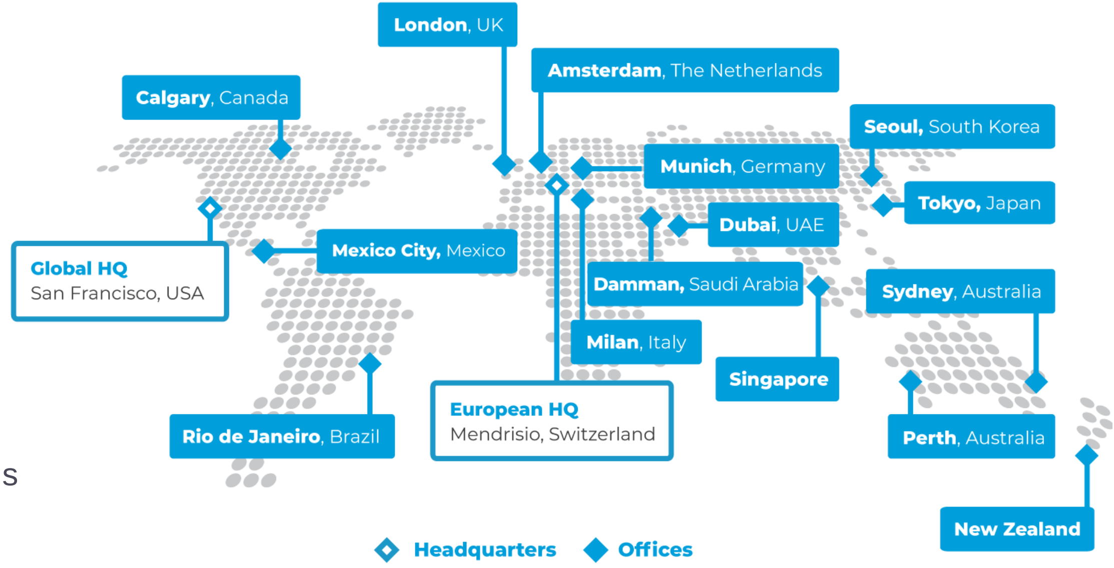
Global Leadership Footprint

Global Customer Base
7.6K+ Installations

82M+ Devices Monitored
Across Converged OT/IoT

Scalable Deployments
Across **6 Continents**

Global Expertise
Worldwide Network of Partners
and **1,500+** Certified Professionals



Nozomi Networks Vertical Focus

OT / IIoT Market Leader

IoT / IT Evolution

- Power / Electric
- Oil & Gas
- Mining
- Water

- Manufacturing
- Pharmaceutical
- Chemical
- Rail / Metro

- Smart Buildings
- Data Center
- Stadium / Venue
- Government / Defense

- Airports
- Food / Retail
- Hospitals
- Finance

- Agriculture
- University / Campus
- Logistics
- Smart City

2013

2023

How do OT/IoT cyber physical systems defend against emerging attacks and keep processes running?

An Explosion of Connected Devices

- 5G
- Digital transformation
- Process automation

37b

Industrial IoT connections by 2025

- Juniper Research

NOZOMI NETWORKS

More Data =
More Opportunity

- Lower cost of operations
- Cloud-scale deployments
- Automation
- Business agility
- Process optimization
- AI-driven insights and analysis

NOZOMI NETWORKS

More Connectivity = More Risk

- More vulnerable access points
- Increased attack surface
- Understaffed security teams
- Legacy infrastructure
- Siloed organizations
- Disparate security technologies
- Financial exposure

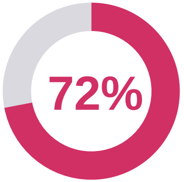
NOZOMI NETWORKS

The Digitization Imperative

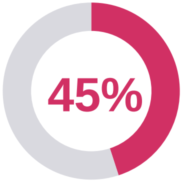
Discrete manufacturers are embracing digital transformation to ensure every investment supports underlying business objectives.

Forces to contend with:

- Cyber threats
- Digitizing legacy equipment
- Cyber-physical systems
- Supply chain disruptions
- Workforce: shortages, skill gaps, remote
- Expanding into IoT
- IT/OT convergence and integration



72%
Manufacturing companies have a digital transformation roadmap in place*



45%
Manufacturing executives expect efficiencies from IoT investments**

*Source; The Aptean 2022 Manufacturing Forecast

**Source: Deloitte 2022 Manufacturing Industry Outlook

© 2022 Nozomi Networks Inc. | All rights reserved. | www.nozominetworks.com

Attacks on organizations in critical infrastructure sectors have increased dramatically, from less than 10 in 2013 to almost 400 in 2020 — a 3,900% change.

> The traditional network-centric, point solution security tools originally deployed in critical infrastructure operations are no longer adequate to account for the speed and complexity of the emerging threat environment.
>
> **– Gartner November 10, 2021**

© 2022 Nozomi Networks Inc. | All rights reserved.

Attackers used a **fish tank thermometer** to hack a casino network and pull the high-roller database across the network, out of the thermostat and into the cloud, compromising personal and financial data.

Many IoT devices are stripped-down sensors without security features but still have **open access to IT networks** and applications.

Hackers gained access to over **150,000 of Verkada video surveillance cameras**, including those in Tesla factories and warehouses, Cloudflare offices, Equinox gyms, hospitals, jails, schools, police stations, and Verkada's own offices.

The hack was meant to show how commonplace the company's security cameras are and **how easily they're able to be hacked**.

NOZOMI NETWORKS

Example - Discrete Manufacturers

Maintain and improve operational resilience while undergoing digital transformation.

IT

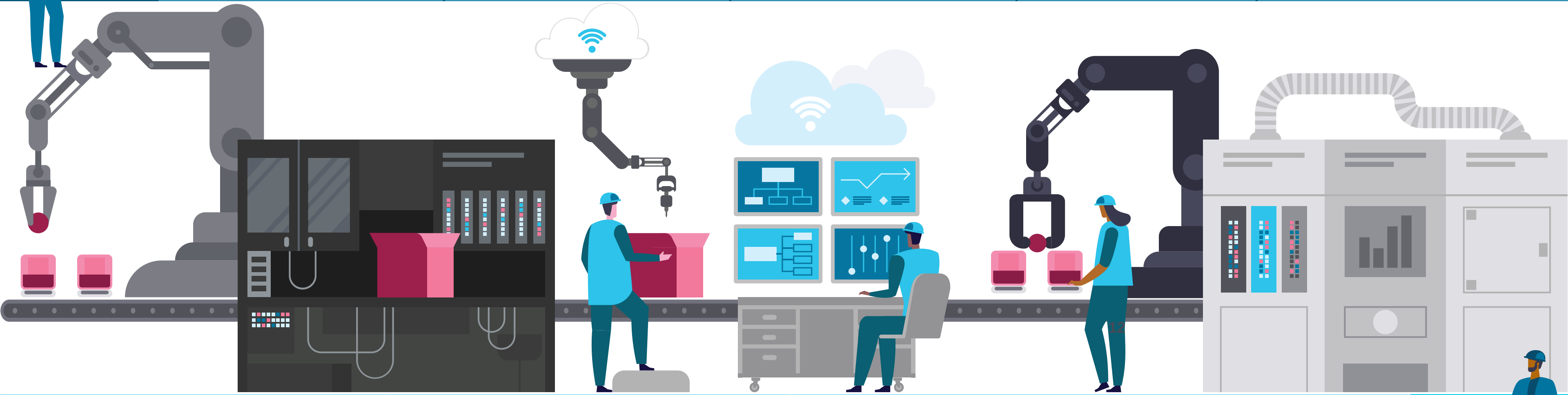
Need to secure operational environments, which include a high diversity of OT, IoT and IT assets.

Can't protect what you can't see – low visibility into OT and automation systems and their cybersecurity gaps.

Need a common platform for monitoring operational systems that consolidates information from all facilities.

Need a platform that integrates with IT tools and workflows.

Need actionable insights to prioritize vulnerabilities and threats, expediting response and reducing manpower needs.



Need a "no process risk" solution that provides comprehensive visibility and monitoring for all systems and assets, no matter the vendor.

Need a system that helps maximize production uptime, quality and volume. Insight into risks, such as failing equipment and unusual variable values, is ideal.

Need to see not just production systems, but maintenance systems too (CCTV, HVAC, etc.).

Need a system that makes it faster to troubleshoot issues through easy access to network information.

OT

Challenges Facing Smart Buildings

Keep your buildings running, minimize your financial exposure, and improve your OT and IoT cybersecurity with an easy-to-deploy and resource-efficient solution.

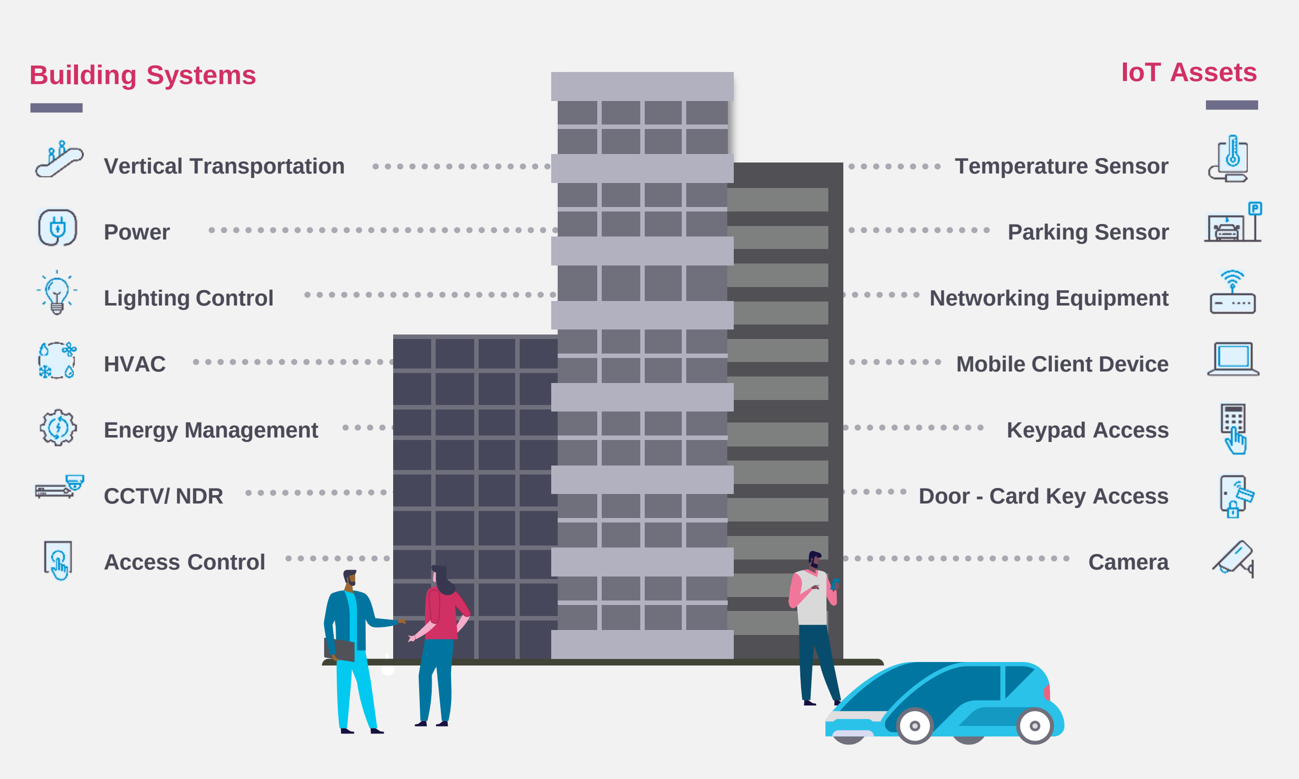
Facilities

Need advance warning of failing equipment or network stability issues in order to act before problems impact occupants

Need faster and more resource-efficient troubleshooting of IoT/OT incidents with insightful forensic tools

Need to keep track of diverse building automatio n systems and many maintenance contractors

Need remote monitoring of IoT/OT systems across distributed building locations



Building Systems

- Vertical Transportation
- Power
- Lighting Control
- HVAC
- Energy Management
- CCTV/ NDR
- Access Control

IoT Assets

- Temperature Sensor
- Parking Sensor
- Networking Equipment
- Mobile Client Device
- Keypad Access
- Door - Card Key Access
- Camera

IT

Need comprehensive visibili ty of all IoT and OT assets and networks, including their risk exposure

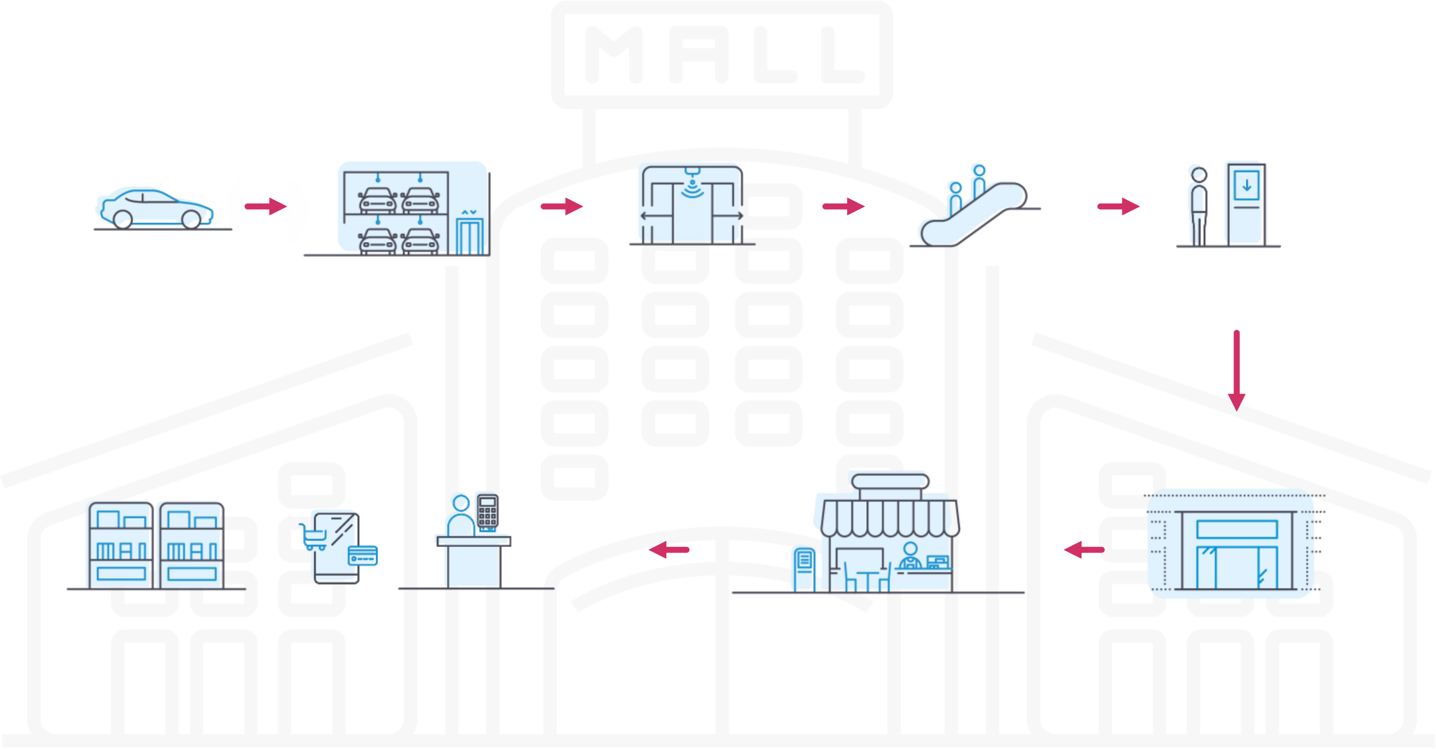
Need clear identification and prioritization of the threats and risks that threaten security the most

Need consolidated information from siloed building networks and sites via one monitoring tool

Need to reduce security risk in a constantly changing threat landscape that includes targeted attacks

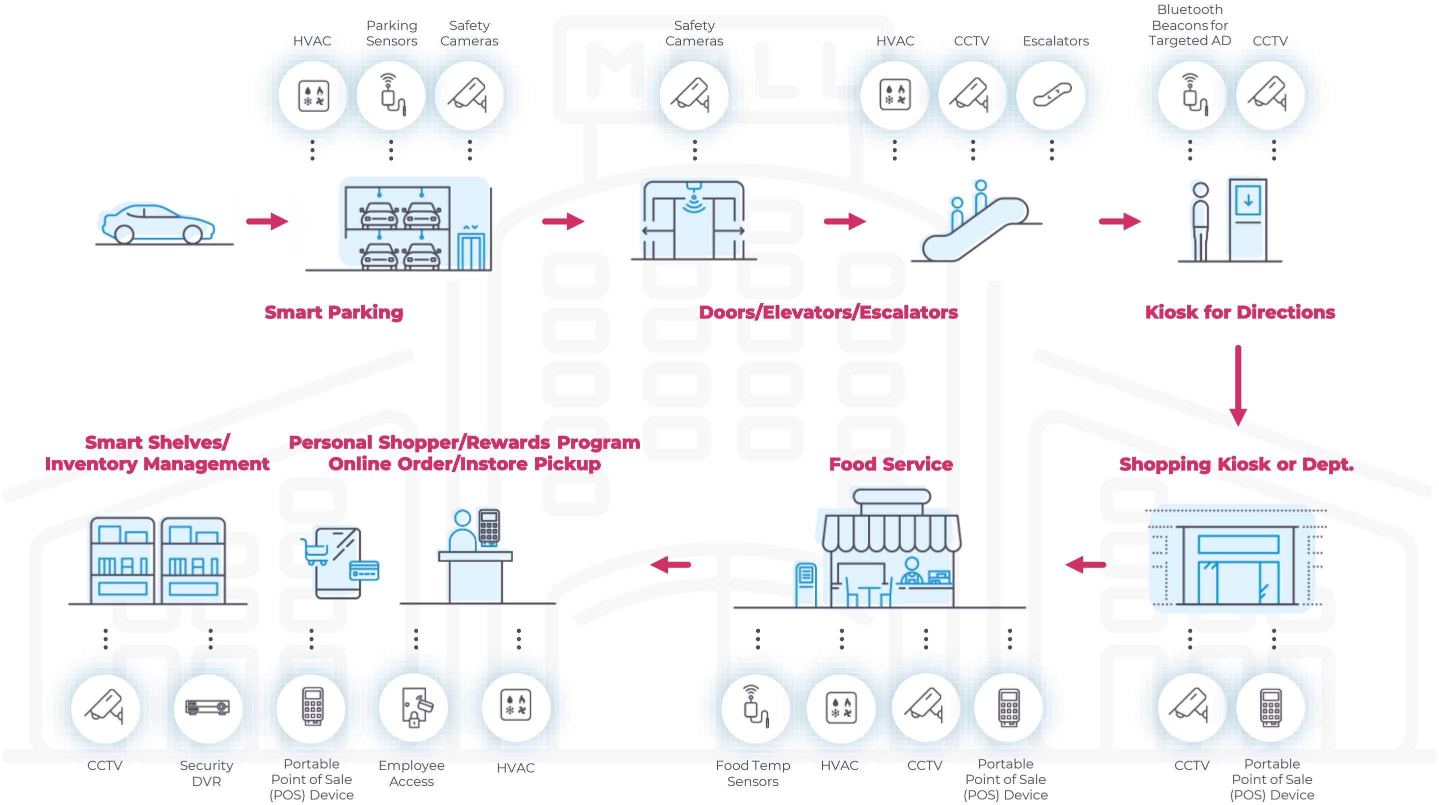
© 2022 Nozomi Networks Inc. | All rights reserved. | www.nozominetworks.com

IoT in Daily Life: The Connected Retail Experience



© 2022 Nozomi Networks Inc. | All rights reserved. | www.nozominetworks.com

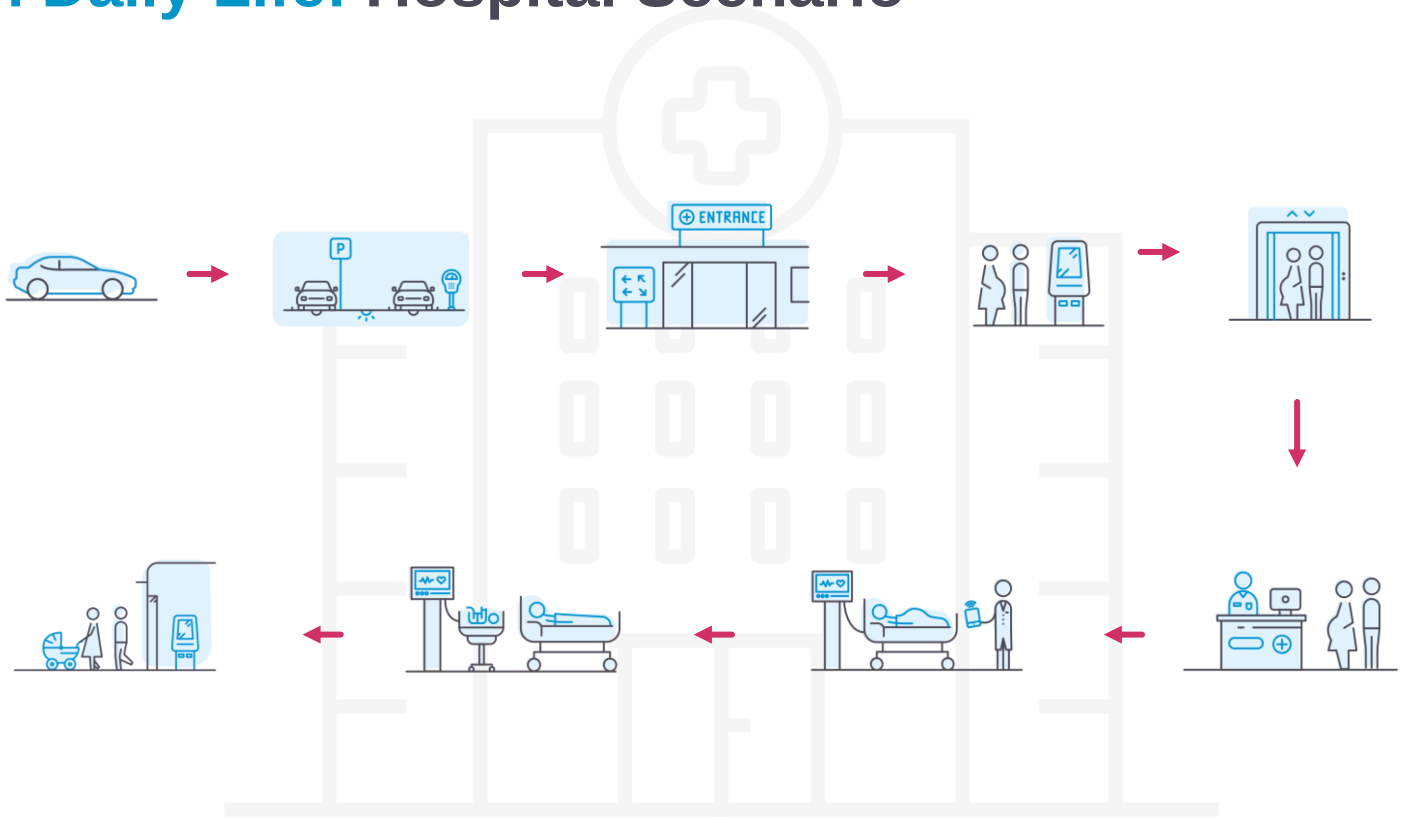
IoT in Daily Life: Connected Retail showing Systems


HVAC
Parking Sensors
Safety Cameras
Safety Cameras
HVAC
CCTV
Escalators
Bluetooth Beacons for Targeted AD
CCTV
Smart Parking
Doors/Elevators/Escalators
Kiosk for Directions
Smart Shelves/ Inventory Management
Personal Shopper/Rewards Program Online Order/Instore Pickup
Food Service
Shopping Kiosk or Dept.
CCTV
Security DVR
Portable Point of Sale (POS) Device
Employee Access
HVAC
Food Temp Sensors
HVAC
CCTV
Portable Point of Sale (POS) Device
CCTV
Portable Point of Sale (POS) Device

NOZOMI NETWORKS

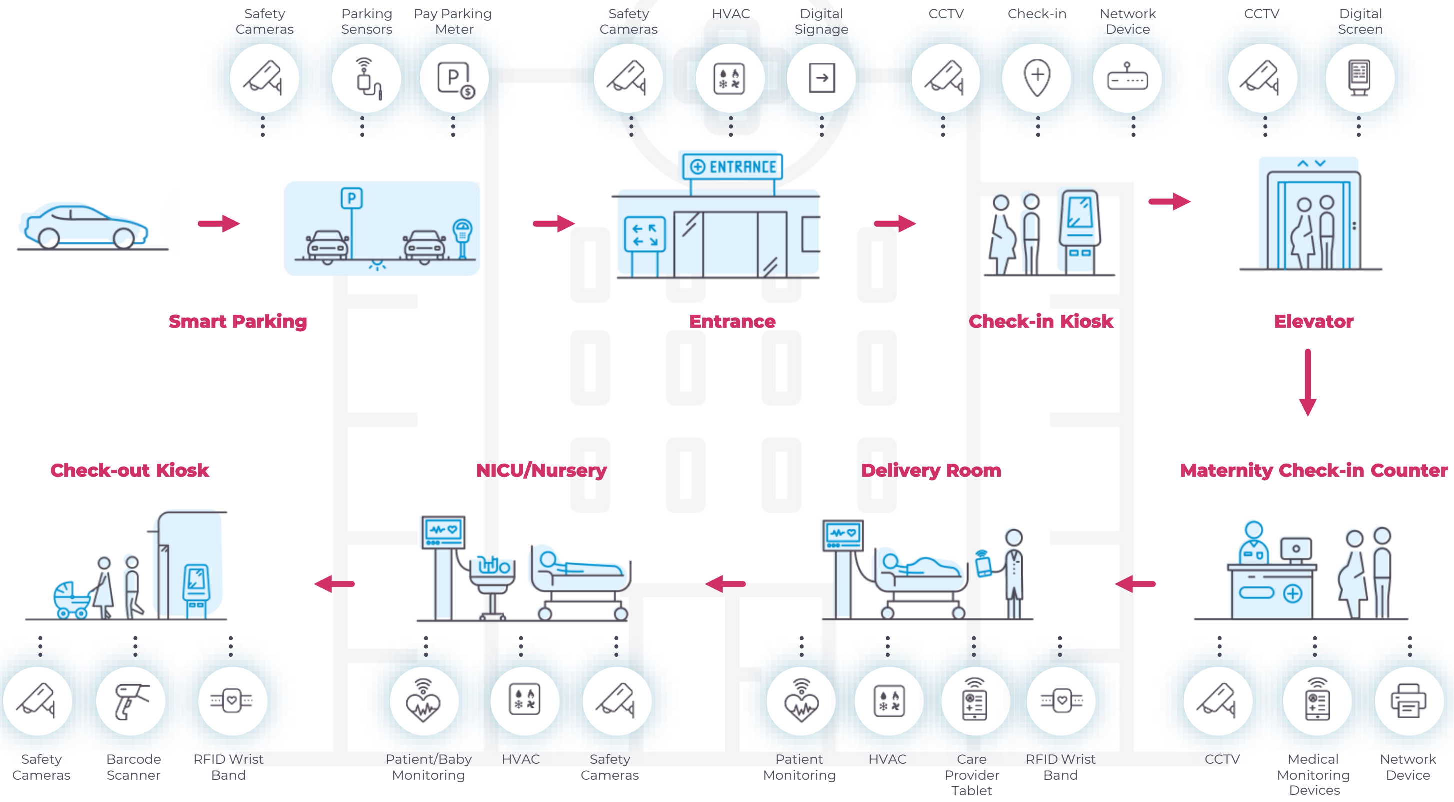
© 2022 Nozomi Networks Inc. | All rights reserved. | www.nozominetworks.com

IoT in Daily Life: Hospital Scenario



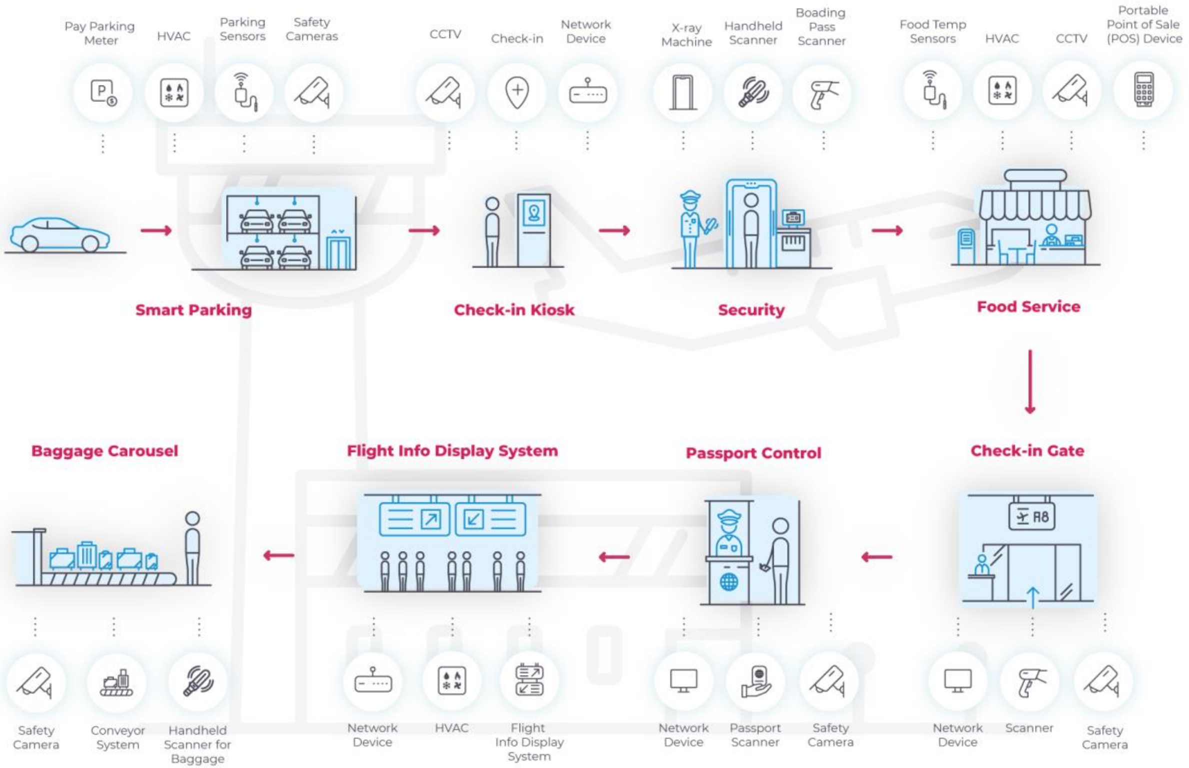
© 2022 Nozomi Networks Inc. | All rights reserved. | www.nozominetworks.com

IoT in Daily Life: Hospital Scenario with Systems



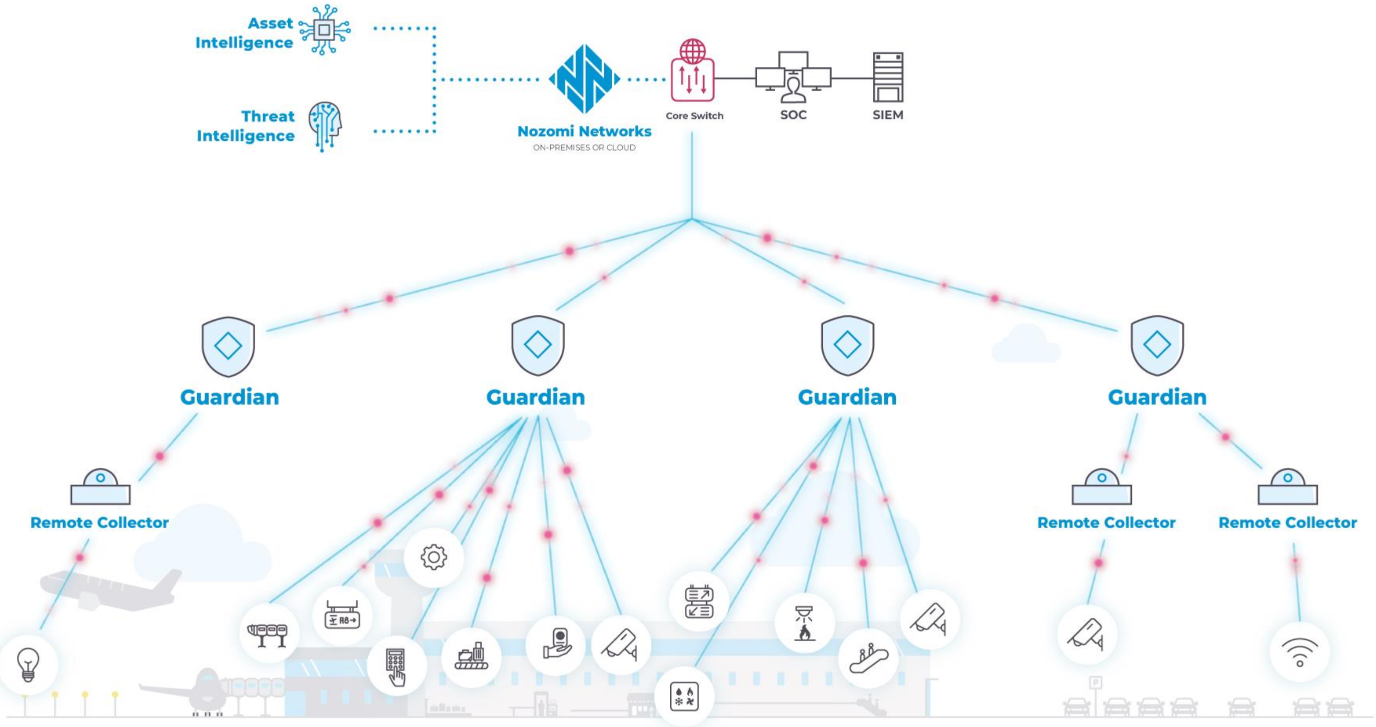
© 2022 Nozomi Networks Inc. | All rights reserved. | www.nozominetworks.com

IoT in Daily Life: Airport Scenario with Systems



NOZOMI NETWORKS

Sample Scalability Architecture: Airport



Nozomi Networks – From OT to Smart Cities

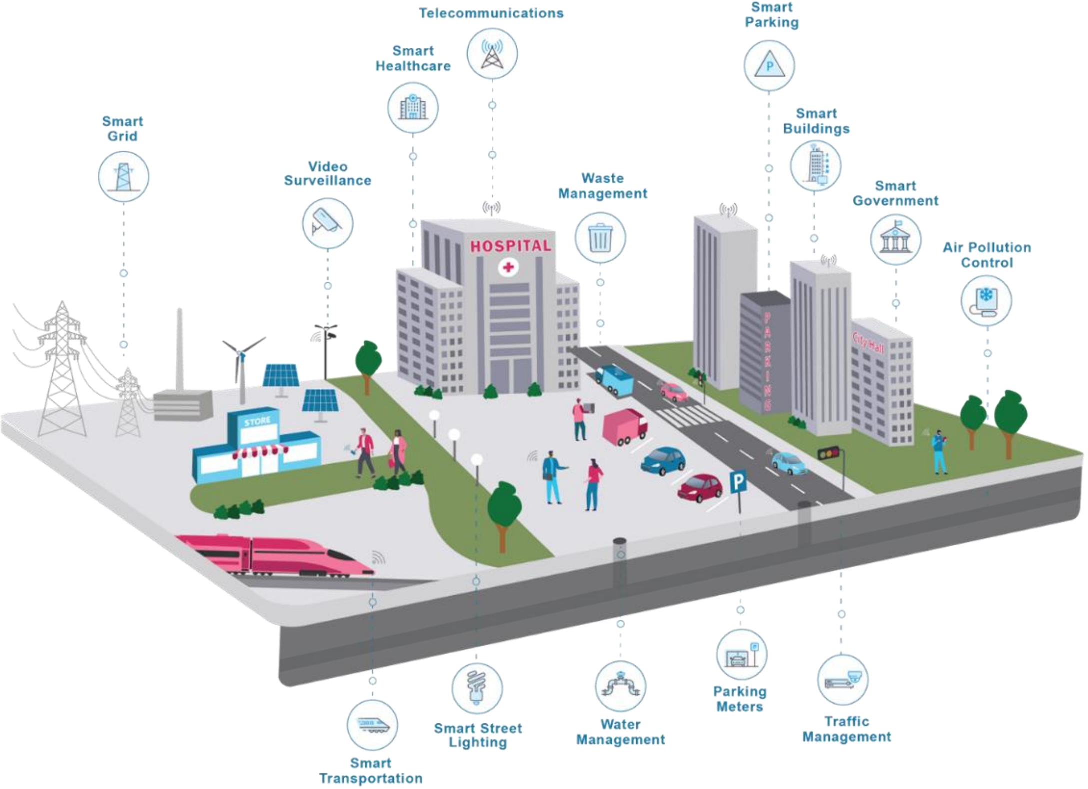
Nozomi Networks covers all smart city systems, from smarts grids, metering and transportation to video surveillance and more.

Tracking known vulnerabilities across all assets and devices, and correctly determining patch priorities

Lack of forensic tools to diagnose breaches and identify anomalies

Lack of centralized data aggregation and correlation across services and applications

Need for non-disruptive approach to Zero Trust compliance



Achieving comprehensive visibility of all IoT and OT assets and networks, including their risk exposure

Need of clear identification and prioritization of the threats and risks that threaten security the most

Lack of consolidated information from siloed city networks and sites via one monitoring tool

Pressure to reduce security risk in a constantly changing threat landscape that includes targeted attacks

© 2022 Nozomi Networks Inc. | All rights reserved. | www.nozominetworks.com

Nozomi Networks Key Differentiators

See

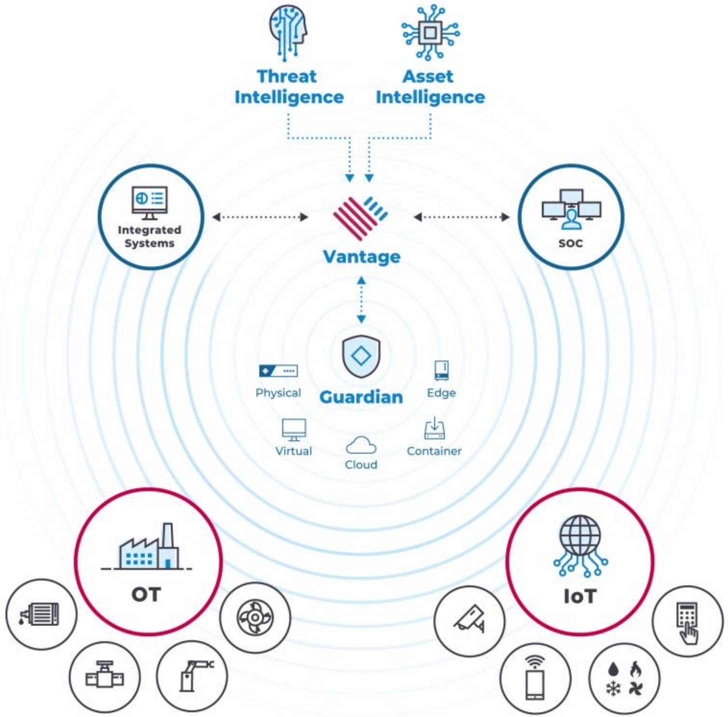
All assets and behaviors on your OT/IoT networks for comprehensive awareness

Detect

Cyber threats, vulnerabilities, risks and anomalies for faster response

Unify

Security, visibility and monitoring across all your assets for improved operational resilience



© 2022 Nozomi Networks Inc. | All rights reserved. | www.nozominetworks.com

Nozomi Networks Solution Portfolio

Core Solutions

Vantage

Guardian

Central Management Console

Extended Functionality

Smart Polling

Asset Intelligence

Threat Intelligence

Remote Collectors

Service Offerings

Certified Engineer Training

Professional Services

Customer Support

100% Customer Retention

Gartner peerinsights™

★★★★★

“The Guardian appliance Is powerful, their team is skilled, they solved our problem.”

Senior Program Manager

Manufacturing Industry

★★★★★

“Innovative, easy to implement and even easier to maintain.”

Systems Specialist

Services Industry

★★★★★

“Once you try Nozomi and its rich feature set you cannot imagine operating without it!”

Security Analyst

Manufacturing Industry

★★★★★

“We wanted the most advanced technology available.”

Manager, Cyber Security

Oil & Gas Industry

NOZOMI NETWORKS

Summary

- Automation and Convergence are driving change in traditional OT networking and security
- Traditional security approaches don’t provide the insight and intelligence required for OT and IoT processes
- Only Nozomi Networks has full insight, accuracy and intelligence across OT, IoT and IT networks to optimize processes

NOZOMI NETWORKS

Will Stefan Roth
will.roth@nozominetworks.com

Thank You!

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

nozominetworks.com