NOZOMI NETWORKS

EBOOK

Solving Cybersecurity for Building Management Systems

Smart Buildings:
Mitigating Cyber Risks and Costs

Smart building owners are adding IoT systems and sensors to their often-aging building management systems as they look for ways to cut operational costs and reduce energy consumption.

However, connected IoT devices increase the cyberattack surface – at a time when smart buildings are an alluring target for bad actors. They offer numerous opportunities for breaches due to the high variety of systems deployed, their lack of inherent security and a low focus on managing their cyber risks. Exposed systems include many that are not covered by IT, such as HVAC, elevator, IoT, lighting and parking.

How do you navigate this exposure and maintain continuity of vital operations while keeping occupants safe and comfortable? To ensure cyber and operational resilience, you need visibility and cybersecurity for all your IoT devices and building management systems—using a solution and vendor with deep smart building expertise.

The Challenge: Reducing Cyber Risk and Maintaining Operational Resilience

Smart buildings contain a multitude of systems, such as power, access control, CCTV, energy management, HVAC and lighting control. Adding IoT sensors into the mix makes buildings more vulnerable to cyber threats and disruptions. Since building cybersecurity often doesn't have an owner, companies need a solution that reduces cyber risk and improves operational resilience – efficiently and at scale.

Smart buildings face three major security challenges:

- **Lack of visibility**
- **Increased cyber risk**
- **Limited cybersecurity resources**

> There is an area of cybersecurity that IT companies and departments have been unable to tame—the vulnerability, fragmentation and inconsistency from building systems and contractors.
>
> ***Intelligent Buildings***

Lack of Visibility

Increased Cyber Risk

Limited Cybersecurity Resources

Protecting smart buildings from cyber threats is challenging due to significant **blind spots** and **security gaps** across OT and IoT systems.

Cyber risk grows as you add more IoT and OT devices to your infrastructure. But you can't protect what you can't see. IT specialists and facility managers need full visibility of all devices and systems, from all vendors, for better cybersecurity. Visibility makes it possible to accurately detect vulnerabilities and anomalies, so you can mitigate cyber risks and minimize disruptions.

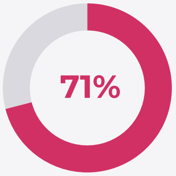
As attacks on smart buildings become more frequent, threat vectors enter through building OT and IoT devices, such as building access, cameras, elevators, HVAC and lighting. Due to their high variety, it is challenging to get a holistic view of all systems and a prioritized assessment of their risks.

Facility managers and their IT counterparts need an automated, consolidated view of all their assets, networks and systems to adequately assess risk and take efficient action to maintain operational resilience.

Lack of Visibility

Increased Cyber Risk

Limited Cybersecurity Resources



of facility managers consider OT cybersecurity either **a “concern” or a “worry.”***

**Source: Honeywell, "Protecting Operational Technology in Facilities from Cyber Threats,“ 2021

Cyberattacks are on the rise, intensified by geopolitical tensions around the world. An attack on a building threatens not just the safety and comfort of the occupants but also the brand reputation and the financial standing of the building owners and managers.

Yet, securing smart buildings is not as straightforward as one might expect. IT cybersecurity solutions are not suited to covering IoT and OT devices and the various vendors that manage building management systems often have limited cybersecurity expertise and focus.

Increasing cyberattack sophistication makes identifying and prioritizing vulnerabilities critical for both existing and new devices. IT departments need comprehensive monitoring and continuously updated risk information, at scale, to properly secure smart buildings.

Lack of Visibility

Fragmented Systems

Limited Cybersecurity Resources

The cybersecurity of building management systems often suffers from lack of a clear owner and inadequate resourcing.

Cybersecurity programs run by IT departments usually don't cover risks coming from building automation OT and IoT systems.

Facility managers also have a limited focus on cybersecurity risk and don't prioritize looking for a solution. They are motivated by the need to keep facilities running and building occupants comfortable and safe.

A lack of shared monitoring tools makes it hard for IT departments and facilities managers to detect cyber risk and mitigate effectively.

When it comes to securing smart buildings, the limited cross-silo alignment, along with a lack of resources and expertise, presents a significant obstacle.

Legacy systems were not built to withstand **today's sophisticated cyber threats.**

The Opportunity:
Anticipate, Diagnose, Respond

Smart buildings have a large attack surface and are increasingly the target of sophisticated threat actors. Diverse systems and networks in multiple facilities require unified monitoring. Companies need solutions that scale easily to contain costs and keep up with their pace of innovation.

The only way to increase situational awareness and fix issues that could jeopardize the safety of building occupants is with accurate and deep IT, OT and IoT visibility and security.

To stay ahead of cyber threats and ensure operational resilience, you need to:

Anticipate

security vulnerabilities and maintenance requirements to optimize operational processes

Diagnose

emerging security threats and process issues with AI-based analytics to reduce business risk

Respond

to the highest priorities with actionable insights and guided remediation efforts for maximum efficiency

Anticipate

Diagnose

Respond

Comprehensive, Real-Time Visibility and Early Warning of Cyber Threats and Equipment Malfunction

Anticipating issues starts with visibility. Do you really know what devices are on your network and how many there are? Which ones are actively communicating? How to take action before a cyberattack inflicts damages?

To spot and troubleshoot cyber incidents or networking issues that threaten reliability, you need real-time visibility into your assets, connections, communications, as well as early warning of risk.

By automating building management inventory, you eliminate blind spots and reveal assets that might have been previously missed. You save time and money by using a solution that builds always up-to-date inventory vs. relying on snapshots of data.

What's needed is a vendor that gives you a full picture of your OT, IoT and IT ecosystem and alerts you of security vulnerabilities and maintenance requirements so you can always be one step ahead of any disruption.

"Good Product to Detect Anomalies and Give Visibility

This product is giving me more visibility to my OT environment. Really good and easy to manage. Support is good as well, fast and effective. The interface to administrate the device, it is very easy and gives a lot of information."

~ Customer review

Anticipate

Diagnose

Respond

Advanced Threat and Anomaly Detection

The evolving sophistication of cyber threat actors is raising the bar for facility managers and IT specialists tasked with securing smart buildings.

How accurate is your security analysis? Are you considering operational data from all your systems and subsystems when assessing risk?

Resource efficiency is key when collecting and analyzing information coming from all your facilities' complex building management and IoT environments.

Smart buildings need continuously updated risk information that gives you confidence in the state of your security and the resilience of your operations.

And, to analyze potentially problematic network changes over time, or execute fast incident response, strong, forensic timeline analysis and query tools are needed.

> **"It gives a great security to our network.**
> *Nozomi is a great network analyzer. It secures our network from any threat. It shows any vulnerable devices real time. There are no any false alarms. Key reasons for purchase: cost management, improve business process agility, improve business process outcomes."*
>
> ***~ Customer review***

Anticipate

Diagnose

Respond

Time-Saving Playbooks

As important as it is, situational awareness is not enough. You need to know how to treat the alerts that signal cyber risk or anomalous behavior.

A system that summarizes and prioritizes risks, with actionable intelligence and playbooks for remediation, helps you efficiently and systematically make your facilities more secure.

You need step-by-step instructions for each type of problem you are trying to solve and threat intelligence to prioritize risk reduction. With the right information and tools, you can focus your efforts and reduce your mean-time-to-respond (MTTR).

> **“A CISO Must Have For OT Environment**
> *Nozomi Networks is the leader in this field. It’s not just a security technology it’s simple a eye wide open into the darkness world of the Operation technology. For me as Security Manager it’s really a must have!!"*
>
> ***~ Customer review***

Taking Action

Building managers and IT specialists who understand these challenges and recognize that the right solution can help mitigate risk will be the ones that come out ahead.

Here are three strategies you can act on now:

Consolidate monitoring

Expand your cybersecurity strategy

Scale up

Learn more about our products

Guardian™

What is it? Sensors that analyze and visualize data from intelligent building networks.

Learn More

CMC™

What is it? Appliances that aggregate data from Guardian sensors for single console, on-premises monitoring.

Learn More

Vantage™

What is it? SaaS that scales security monitoring and visibility for multiple connected facilities and complex building management environments.

Learn More

Effective across all IoT and operational systems in a smart building, including lighting, elevators, CCTV, emergency, fire systems, HVAC, public address and safety.

Consolidate Monitoring

Expand Your Cybersecurity Strategy

Scale Up

Attackers know how to exploit IT/OT defense gaps. Large quantities of building IoT and connected building management systems across multiple facilities lead to cyber risk in difficult to detect places. To reduce risk, it's essential to consolidate the monitoring of OT and IoT assets into a single view.

Smart buildings need a solution that provides comprehensive visibility and monitoring for diverse systems and assets.

IT needs to be able to see all assets and networks and quickly detect illegitimate uses and activities. A solution that consolidates information from all systems and subsystems, prioritizes vulnerabilities and threats, and expedites response with actionable intelligence is ideal.

Improving Smart Building Security

Read our Building Management Systems solution infographic to see how Nozomi Networks delivers smart cybersecurity for smart buildings

Download

IoT devices open the door to cyber breaches due to their lack of security features and connection to external systems. Smart buildings may use IT cybersecurity tools, but if existing and newly added IoT and OT devices are not adequately covered, they are exposed to cyber risk.

Third-party vendors rarely patch or update IoT devices and OT devices are hard to patch for operational reasons, leaving building operations at risk.

To limit exposure to cyber threats and the ensuing financial liability, smart building operators need an inclusive cybersecurity strategy that covers not just traditional IT systems, but the expanding IoT and OT infrastructure.

With a comprehensive cybersecurity approach, you can safely enjoy the full benefits of digital transformation, including energy savings. And the right IoT/OT solution helps future-proof your buildings with continuous threat intelligence to counter tomorrow’s malware and scalability to handle new technology and properties.

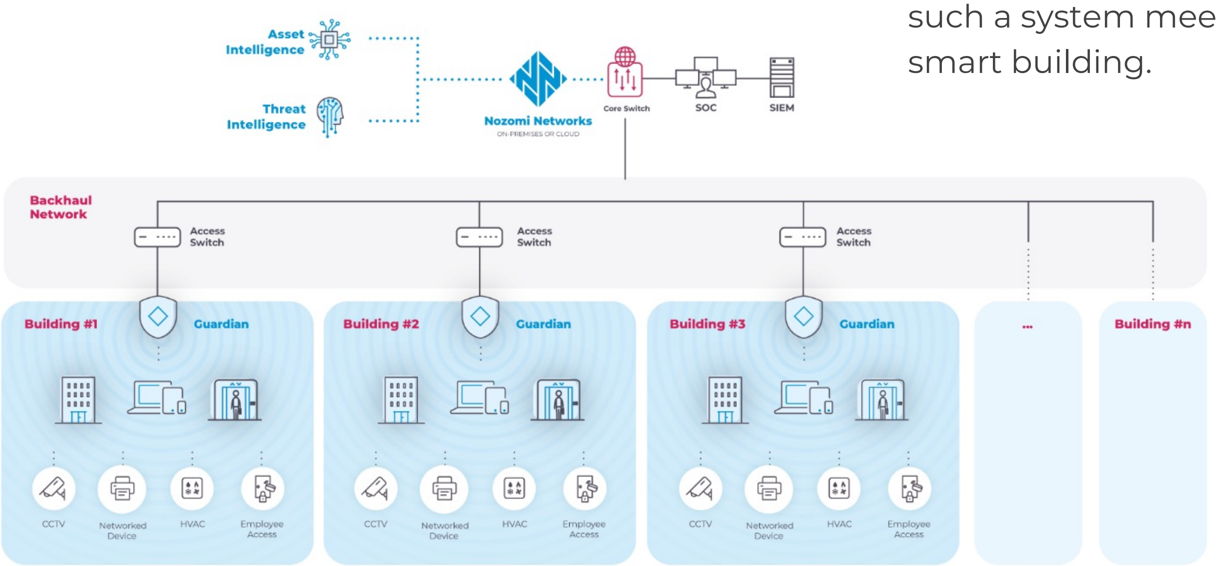
Consolidate Monitoring

Expand Your Cybersecurity Strategy

Scale Up

Dispersed buildings and quickly evolving IoT systems require monitoring at scale. It's critical to implement a solution that can protect any number of OT, IoT, IT, edge and cloud assets.

You need an easy-to-deploy and resource-efficient system that scales elegantly. A SaaS-powered application provides a single pane of glass view of aggregated and prioritized risks across all facilities. It scales quickly and reduces complexity and cost. Paired with a wide range of onsite sensors, such a system meets the needs of any smart building.



What Could **Success Look Like for You?**

Case Studies:

Top 5 Mall Owner

Top 5 Hotel Owner

Top 5
Mall Owner

The
Challenge:

A top 5 global mall owner wanted to:

Gain visibility into an environment with a high number of IoT and OT devices and systems managed by multiple vendors

The
Result:

By deploying the Nozomi Networks solution, the company can:

Achieve visibility into core building management systems, including those controlled by 3rd-party vendors

Reduce time to visibility by automating inventory of all assets, including IoT devices

Consolidate monitoring

Top 5
Hotel Owner

The
Challenge:

A top 5 global hotel owner wanted to:

Minimize cyber risk

Protect the brand from the negative consequences of a cyberattack

The
Result:

By deploying the Nozomi Networks solution, the company can:

Determine if any IoT, OT or IT devices are exposed to cyber threats

Get a clear understanding of cyber risks

Use actionable insights to implement mitigations and speed up response times

Customer Reviews Gartner Peer Insights

Gartner peerinsights™

★★★★★

ROLE: SR. CYBERSECURITY ANALYST
INDUSTRY: OTHER
COMPANY SIZE: <500M -1B USD

With Nozomi We Have An In-Depth View of the OT Network and Extremely Qualified Professionals

Its adoption has allowed us to have a broader visibility of the industrial network in a more in-depth way, giving us bases to improve in several aspects. Aspects that go beyond the analysis and anomalies that are the main focus, but also help us to understand the legacy networks.

★★★★★

ROLE: INFRASTRUCTURE AND OPERATIONS
INDUSTRY: HEALTHCARE
COMPANY SIZE: 30B + USD

Nozomi Provides and Excellent Solution to Monitor OT Networks

Working with Nozomi has been an excellent partnership. Their tool provides the visibility we need to secure our OT environments. … Easy to deploy.

★★★★★

ROLE: CORPORATE CYBERSECURITY MANAGER
INDUSTRY: HEALTHCARE
COMPANY SIZE: 250m – 500m USD

A CISO Must Have for OT Environment

Nozomi Networks is the leader in this field. It's not just a security technology it's simple a eye wide open into the darkness world of the Operation technology. For me as Security Manager it's really a must have!!

More Reviews from Nozomi Networks Customers

Next Steps

Find out how Nozomi Networks can help you improve cyber resilience, visibility and security for your smart buildings:

Building Automation Webpage

Request a Demo

Want to **Learn More?**

About Nozomi Networks and Smart Buildings

Nozomi Networks is your partner in security and visibility for smart buildings and building automation systems. Our scalable and flexible solution closes OT and IoT blind spots and security gaps by providing exceptional visibility and monitoring of assets and networks. This results in accurate detection of cyber threats, risks and anomalies as well as improved enterprise risk mitigation and operational resilience.

Additional Resources:

Improving Smart Building Security

Solution Infographic

SOLUTION BRIEF

Full Spectrum Visibility and Threat Detection for IoT Networks

Full Spectrum Visibility and Threat Detection for IoT Networks

Securing Building Management Systems from Cybersecurity Threats

Blog: Securing BMS from Cybersecurity Threats

Securing OT & IoT in Building Management Systems

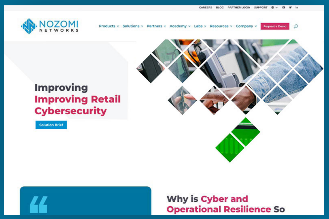
Why is Cyber and Operational Resilience So

Securing OT & IoT in BMS

Improving Internet of Medical Things (IoMT) Cybersecurity

Why is Cyber and Operational Resilience So

Improving IoMT Cybersecurity


Improving Improving Retail Cybersecurity

Why is Cyber and Operational Resilience So

Improving Retail Cybersecurity

NOZOMI
NETWORKS

Thank You!

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