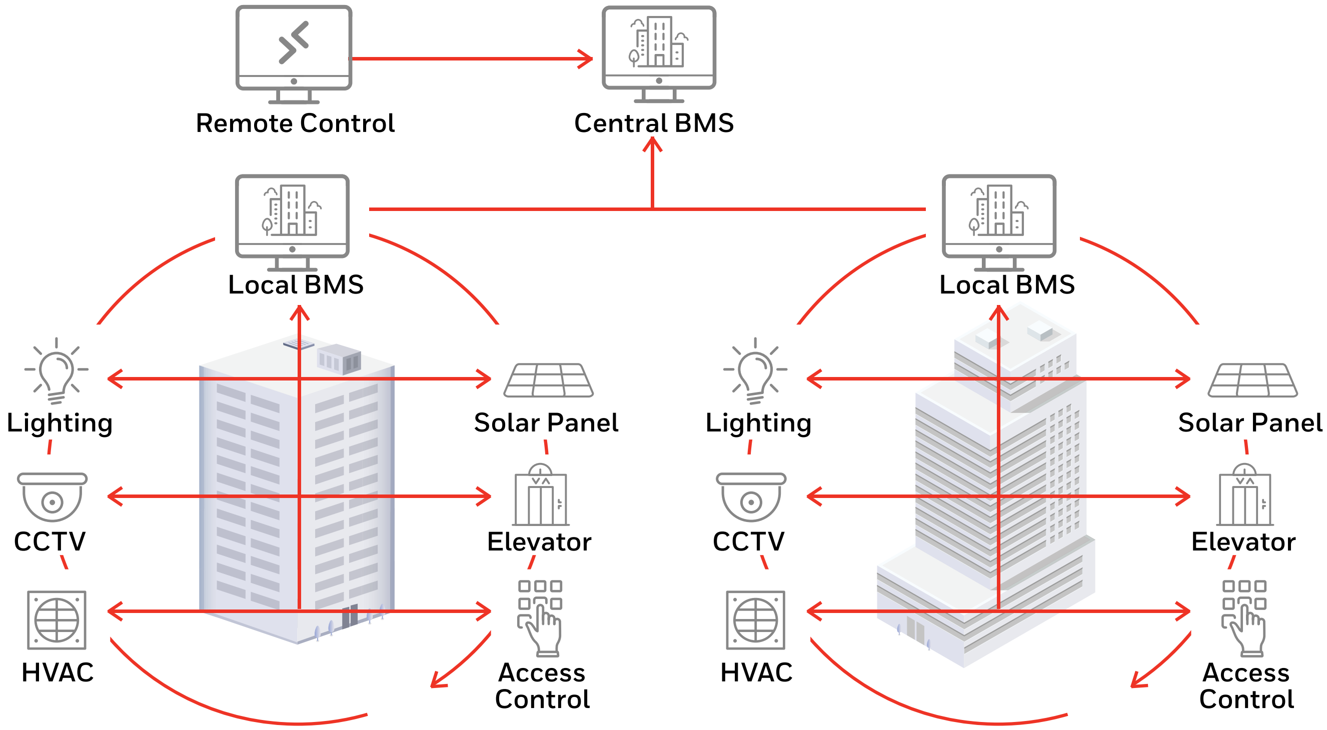
SECURITY FOR BUILDING MANAGEMENT SYSTEMS

Honeywell

THE RISE OF SMART BUILDING TECHNOLOGY

Building management systems (BMS), or "smart building technology" is expanding to an increasingly wide range of applications. A single smart building can include dozens of different smart devices, such as lighting, asset control, HVAC (heating, ventilation, and air-conditioning) systems, fire protection, elevators, sanitation, parking sensors and more.

The motivation for the increased use of advanced BMS technology is clear. Smart building technology increases comfort, efficiency, sustainability, and safety. However, ensuring the proper functioning of these technologies while keeping the attack surface as small as possible is a challenge. To solve this challenge, there is a need for cutting-edge technology and a deep understanding of how these platforms are used and how to better secure them.



The different systems used in a smart building

INCREASED CONNECTIVITY

> In order to achieve the business benefits from building management systems, increased connectivity is required

BETWEEN BUILDING MANAGEMENT SYSTEMS AND THE IT NETWORK

The BMS systems are part of other organizational systems residing in the IT network and are potentially also exposed to the internet, enabling remote management and operations.

AMONG SYSTEMS

Separate BMS systems can be interconnected to increase overall operational efficiency. For example:

- Fire alarm and security systems can trigger changes in elevator or door behaviors
- Motion alerts can trigger actions in HVACs, lighting, sound, and elevator management systems

WITHIN ONE BUILDING MANAGEMENT SYSTEM

Deployed devices, such as smoke sensors, HVAC systems, CCTV cameras (and others), need to connect to their control servers for reporting and for command and control purposes.

AMONG BUILDINGS OR WITH SMART CITY SYSTEMS

In advanced BMS scenarios, one building can benefit from connectivity with neighboring buildings, or with a city-wide infrastructure, such as a smart grid.

INCREASED SECURITY RISKS

An increasing number of interconnected smart devices means exposure to many more attack vectors, making it almost impossible to fully isolate these devices. With hundreds or thousands of devices in one building, the potential attack surface grows significantly.

The criticality of these systems makes them a lucrative target for both targeted and non-targeted attacks. Even comfort-oriented systems, such as HVAC, or motion detection systems, can cause significant damage when crippled by a cyber attack. Whereas a brief air conditioning malfunction can cause some discomfort in an office building, even a minor temperature change in hospitals, medical labs, data centers and other environmentally sensitive sites can cause significant damage.

Coordinating attacks or failures that bridge between the cyber and physical worlds can have a devastating outcome. For example, simultaneous failures or lack of visibility in fire safety systems or access control may result in fatalities.

Various Attack Scenarios on BMS Networks Include:

MALWARE AND RANSOMWARE ATTACKS

Malwares can cripple operational systems. Ransomware can take control of critical systems, such as in the case of the hotel in Austria, where hotel residents were locked inside their bedrooms.

PROPAGATING BETWEEN NETWORKS

Smart IoT devices, with no security controls, can be hacked, granting access to the main IT systems of the entire organization. The BMS network can serve as a back door to an adjacent network, providing unauthorized access to an organization's critical IT, IoT or BACnet assets.

BUILDING SERVICE DISRUPTION

Accidental actions or deliberate denial of service (DoS) attacks on BMS systems can cause significant damages and can introduce life-threatening conditions, as well as disrupting critical systems.

INTERNAL ATTACK VECTORS

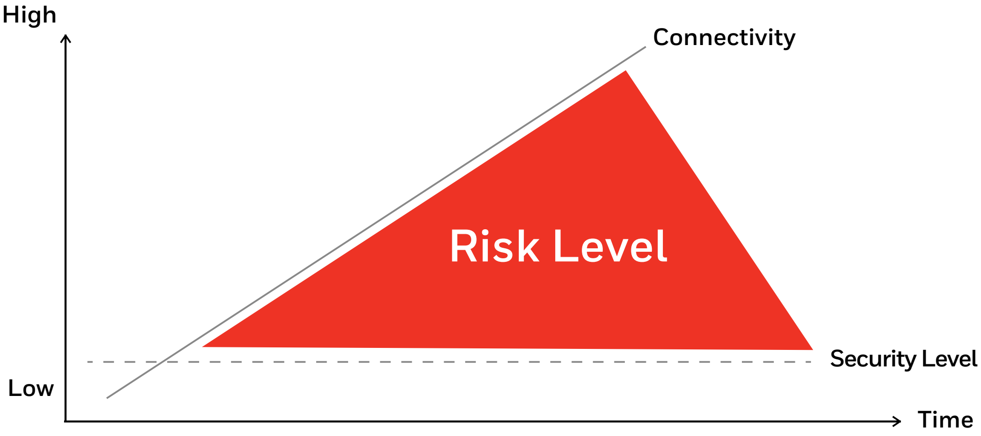
Unwitting visitors and technicians, disgruntled employees, or accidental actions and infections can initiate attacks from inside a poorly secured BMS network.

MULTI-DIMENSIONAL TERROR ATTACKS

A combination of attacks on the physical and cyber layers – in one or more systems, and in one or more buildings can cause significant damage and even loss of life.

Today's building management systems typically lack cybersecurity protection such as encryption, authentication or access control.

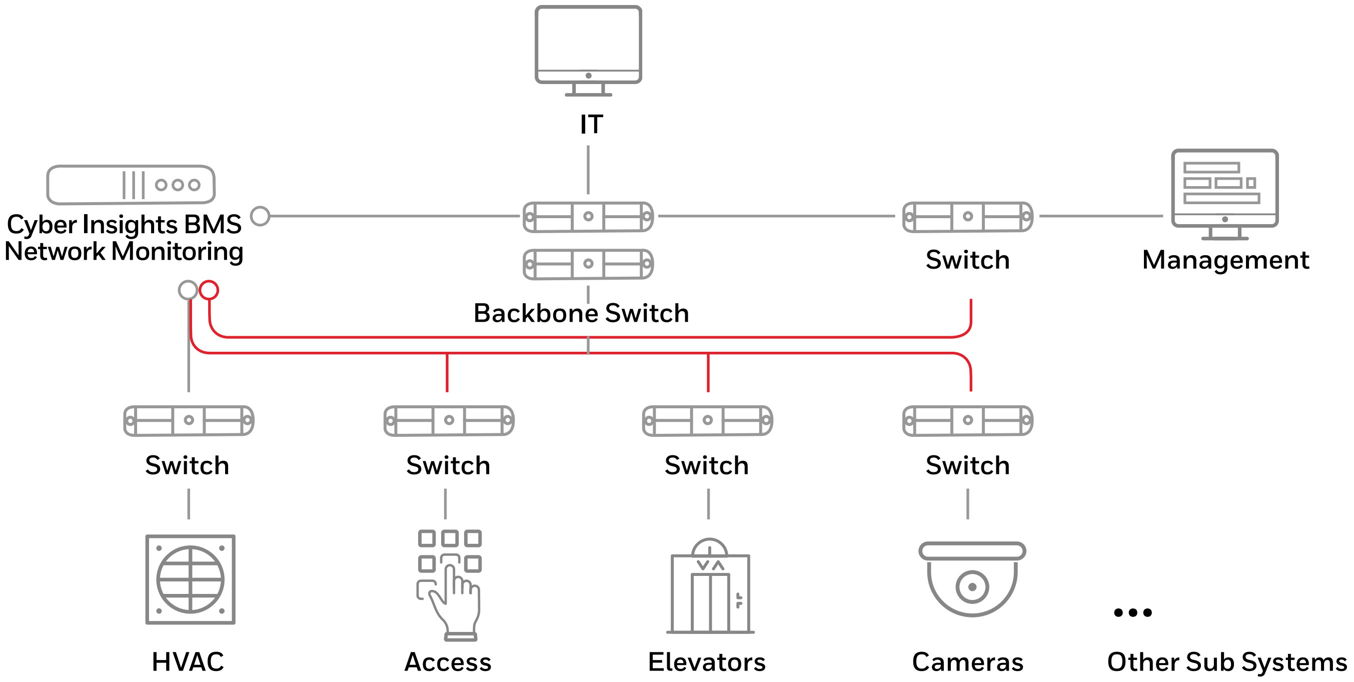
While connectivity levels increase, and BMS security controls do not keep up, the risk to BMS infrastructure significantly increases, making severe incidents only a matter of time.



SECURITY FOR BUILDING MANAGEMENT SYSTEMS

In order to address the security challenges of building management systems, it is essential to have security controls in place that can discover all the assets on the BMS network. Allowing real-time detection of rogue devices and detecting any activities that can jeopardize the operational continuity of the building and sites is critical.

Honeywell Forge Cybersecurity+ for Buildings | Cyber Insights is a passive detection and response platform designed for the unique challenges of IoT and BMS networks. By monitoring and analyzing the network traffic and network behavior, as well as by analyzing proprietary BMS protocols such as BACnet and LonWorks, the solution is capable of rapidly identifying and monitoring every asset in the network, and providing visibility across the entire network. This allows users to identify weaknesses in their network topology, indicators of an attack in real time, operational issues and many other security-related aspects.



THE BENEFITS OF BMS NETWORK MONITORING WITH HONEYWELL FORGE CYBERSECURITY+ FOR BUILDINGS | CYBER INSIGHTS

Honeywell Forge Cybersecurity+ for Buildings | Cyber Insights is designed to map the BMS network, help enhance its security protections and improve its operational availability. The solution begins by automatically discovering all of the assets and their roles in the network, and then provides visibility into their behavior. It is then designed to provide day-to-day protection by identifying malicious and non-malicious activities as well as network and service failures.

Automated Asset Inventory is designed to automate your entire asset inventory and to provide detailed information on all the devices connected to the BMS network, including devices behind BACnet gateways. It is also designed to automatically generate asset inventory without needing any prior knowledge or user configurations. It can also provide insights on important changes such as new device connections, device failures and on any changes that are done to the devices.

Detect Anomalies in the BMS Processes Designed to increase your safety by detecting malfunctions in BMS equipment, it's capable of detecting abnormal communication patterns, unauthorized commands and down to out-of-range values in critical components that endanger the building infrastructure. Examples include:

- Interfering or shutting down security cameras
- Manipulating access control systems
- Damaging heating or cooling systems and/or sensor reporting in temperature critical rooms
- Manipulating fire extinguishers and alarm systems
- Disrupting housekeeping services such as lightning and HVAC
- Additional threats in BMS environments

BENEFITS

- Discovery and inventory management of all devices throughout the building
- Enhancing security for critical systems such as HVAC, elevators, surveillance & access control
- Full deep packet inspection support for proprietary protocols such as BACNet and LonWorks
- Non-intrusive monitoring with little to no impact on the performance of the smart devices
- Adaptive dynamic baseline for learning of normative behavior and automatic detection of anomalies
- Future-proof with the ability to adapt immediately to new BMS configurations and devices
- Easy administration and operation for both OT staff and IT staff
- Seamless integration of BMS OT security into existing security controls

HELP PREVENT MALWARE AND RANSOMWARE INCIDENTS

Honeywell Forge Cybersecurity+ for Buildings | Cyber Insights is designed to detect anomalous network behavior and detects malware before it spreads. This helps security teams to quickly remediate cybersecurity incidents with early detection and automated response, while keeping the operational status of the building systems intact.

HELP PREVENT THE BMS NETWORK FROM BECOMING AN ATTACK VECTOR INTO THE IT NETWORK

Honeywell Forge Cybersecurity+ for Buildings | Cyber Insights is designed to quickly detect and prevent attempts of utilizing the BMS network to penetrate the larger organizational IT network. It can also monitor the different network segments for efficiency.

HELP PREVENT ATTACKING THE OT NETWORK FROM THE IT NETWORK

Honeywell Forge Cybersecurity+ for Buildings | Cyber Insights is designed to detect any policy violations or firewall bypassing, which causes intrusions to the BMS network and systems.

For more information

buildings.honeywell.com

Honeywell Building Technologies
715 Peachtree St NE
Atlanta, Georgia 30308
www.honeywell.com

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell