



SOLUTION BRIEF

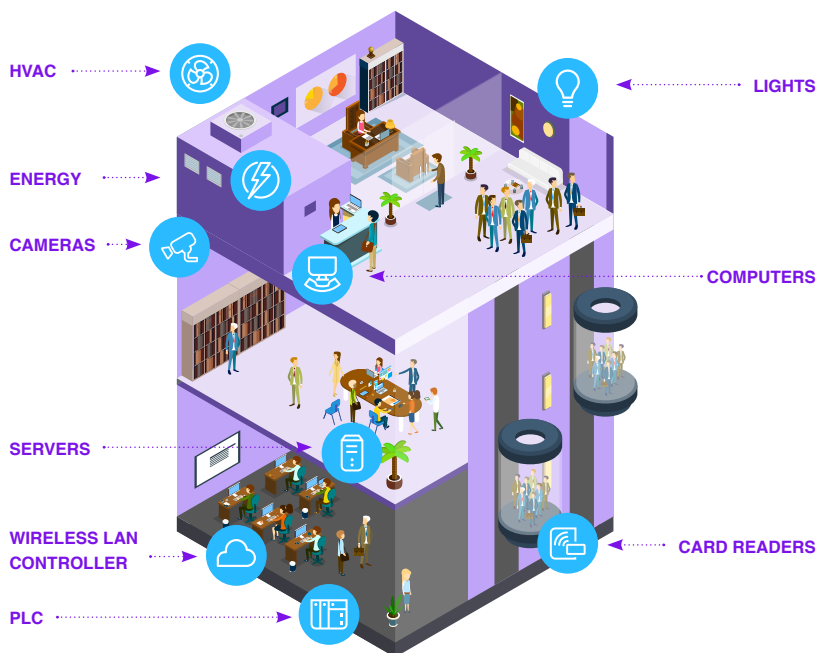
Ensure the Cyber Physical Integrity of Building Management Systems

Armis enables you to easily see, protect and manage wired and wireless assets on your networks, including BMS controllers and devices.

The Challenge

When it comes to improving operational efficiencies, reducing energy consumption, and extending the life of critical, costly equipment, building management systems (BMSs) are indispensable. But attacks on unprotected critical systems can also pose risks to everything from peoples' safety and comfort to production runs.

- Most BMSs lack built-in security controls and can't host security agents;
- Software patches are often difficult or impossible;
- New smart devices create new attack vectors;
- Ransomware targeting physical infrastructure is on the rise, given all the security blind spots attackers can exploit in a BMS.



In addition to servers and computers, attackers are increasingly focused on unprotected critical systems in buildings.

Key Capabilities

Seamless identification and tracking of managed and unmanaged BMS devices, including HVAC and mechanical controllers, SCADA servers, and PLCs.

Complete, real-time continuous risk and vulnerability assessment.

Automatic or manual threat-response enforcement.

Ability to report on key BMS protocols such as BACnet.

The Solution

The Armis Centrix™ Platform enables you to see, protect and manage every wired and wireless asset on your networks, including BMS controllers and devices. Through continuous, real-time security that relies on contextual intelligence from the industry's most comprehensive AI-powered asset intelligence engine, you can instantly detect and mitigate unusual behavior. In addition, hundreds of integrations with your existing security, IT and asset tools simplify administration.

Gain complete Lifecycle Management over your BMS Devices and Cyber Physical Environment

Whether connected assets are located onsite or in distributed locations, the Armis Centrix™ platform's holistic approach makes it easy to inventory and quickly understand all of them. Get complete situational awareness of BMS assets, including thermostats, sensors, elevator controllers, and fire and safety systems. And keep a close eye on every other connected asset, including smart devices like TVs, IP cameras, and printers with comprehensive asset details.

- Device manufacturer, model, firmware version, and serial number
- Location/site, username, IP address, MAC address
- Operating system (OS) and installed applications
- Known vulnerabilities associated with each OS/application
- Changes in device state and state anomalies
- Activities and connections made over time
- Device risk scores based on static and dynamic analysis

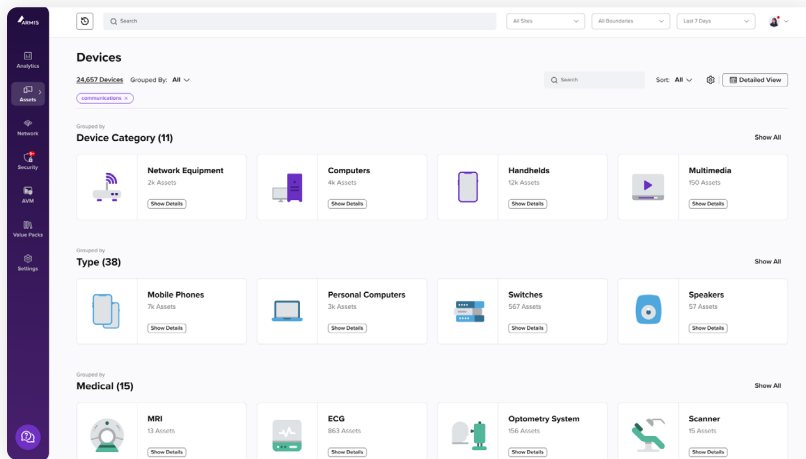
Key Benefits

Provides complete asset visibility of all BMS devices.

Streamlines identification and management of security risks.

Enables operators to manage entire BMS security lifecycle.

Improves cyber and operational resilience for BMS environments.



Inventory screen example of a typical office building. The Armis platform gives you a high-level view of every asset type, along with the ability to quickly and easily drill down into the specifics of every device that is sharing data on your networks, including HVAC and mechanical controllers, lighting systems, PLCs, security cameras, and more.

Why Armis?

Comprehensive

Discovers and classifies all devices in your environment, on or off your network.

Agentless

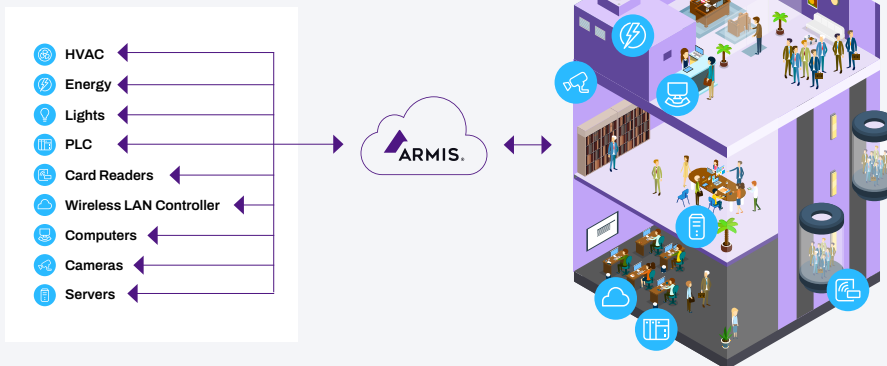
Nothing to install on devices, no configuration, no device disruption.

Tailored visibility of your environment

A holistic approach to asset discovery including network traffic analysis, deep packet inspection and non-disruptive active discovery

Cloud Native

Installs in minutes using the infrastructure you already have.



i The Armis platform provides a central management console for every cyber asset and building across the enterprise.

Identify and manage security risks

The Armis platform performs continuous, non-invasive monitoring of every wired and wireless device in your environment. The platform:

- Protects your business from disruption by relying on the world's largest crowd-sourced, device knowledgebase to detect threats with a high degree of accuracy.
- Monitors devices communicating in the airspace via peer-to-peer protocols, which are invisible to traditional security products.
- Enables you to automatically disconnect or quarantine devices operating outside of "knowngood" baselines.

Manage BMSs with confidence

The Armis platform gives operators the additional capabilities they need to optimize BMS operations.

- Complete network visibility with automatic discovery of every BMS asset.
- Continuous network monitoring and detection of anomalous, suspicious, or malicious behavior, and unauthorized actions.
- Real-time detection of device misconfigurations, unscheduled changes, and device malfunction.

**Keep your building systems secure and your people safe.
Protect your BMSs with the Armis platform.**



Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo

