ARMIS®

SOLUTION BRIEF

Ensure the cyber-physical integrity of building management systems.

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

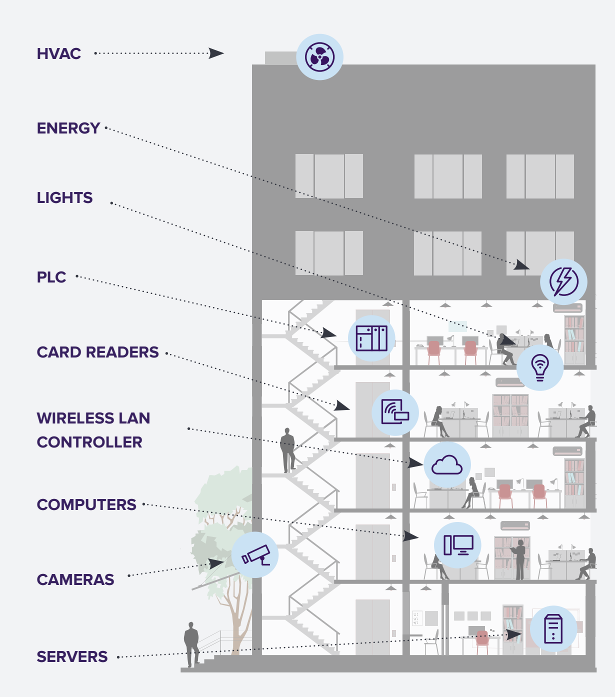


Figure 1: In addition to servers and computers, attackers are increasingly focused on unprotected critical systems in buildings.

Key Capabilities

- ➤ **Seamless identification and tracking of managed and unmanaged BMS devices, including:**
  - HVAC and mechanical controllers
  - SCADA servers
  - PLCs
- ➤ **Passive, real-time continuous risk and vulnerability assessment.**
- ➤ **Automatic or manual threat-response enforcement.**
- ➤ **Ability to report on key BMS protocols such as BACnet.**

Key Benefits

- ➤ **Provides 100% visibility into BMS devices.**
- ➤ **Streamlines identification and management of security risks.**
- ➤ **Enables operators to manage BMSs with confidence.**

The Solution

The cloud-based Armis platform enables you to easily discover, oversee, and secure 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 knowledgebase, you can instantly detect and mitigate unusual behavior. And 100+ integrations with your existing security, IT, and asset tools simplify administration.

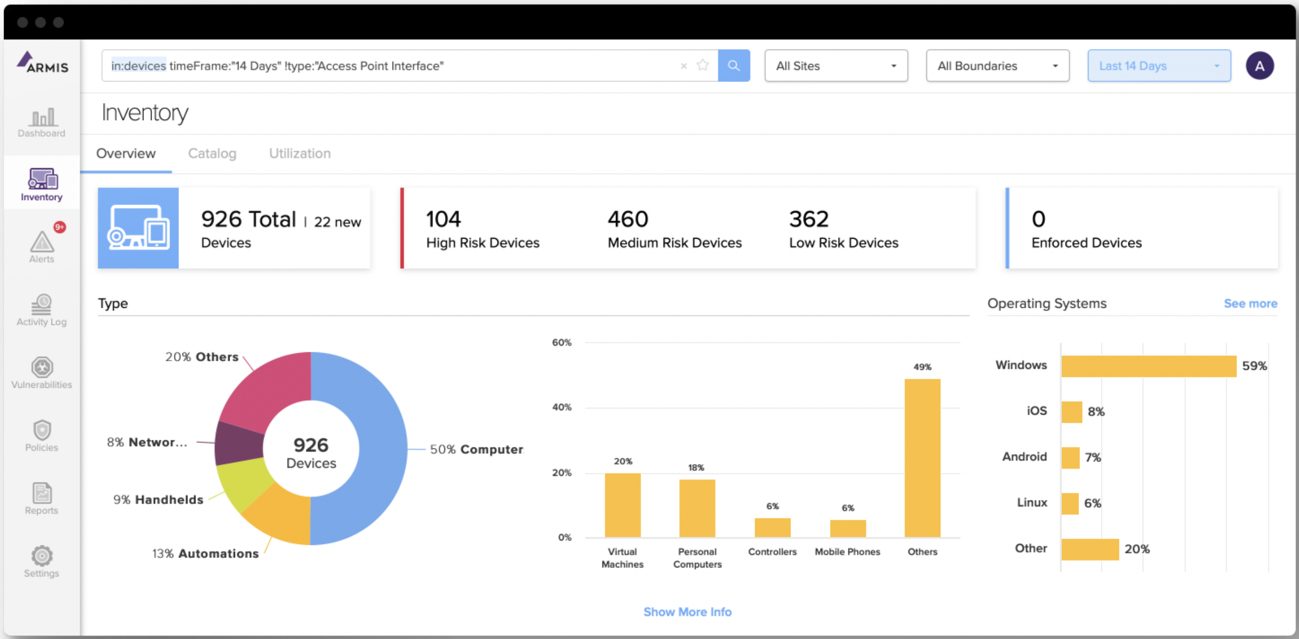
Gain complete visibility into BMS devices

Whether connected assets are located onsite or in distributed locations, the Armis platform's agentless approach makes it easy to inventory and quickly understand all of them. Get 100 percent visibility 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

Why Armis?

- **Comprehensive**
  Discover and classify all devices on your networks.
- **Agentless**
  Nothing to install, no configuration or device disruption.
- **Passive**
  No device scanning or network impacts.
- **Frictionless**
  Installs in minutes using existing infrastructure.



in:devices timeFrame:"14 Days" !type:"Access Point Interface"

All Sites | All Boundaries | Last 14 Days

Inventory

Overview | Catalog | Utilization

926 Total | 22 new Devices

104 High Risk Devices

460 Medium Risk Devices

362 Low Risk Devices

0 Enforced Devices

Figure 2: 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.

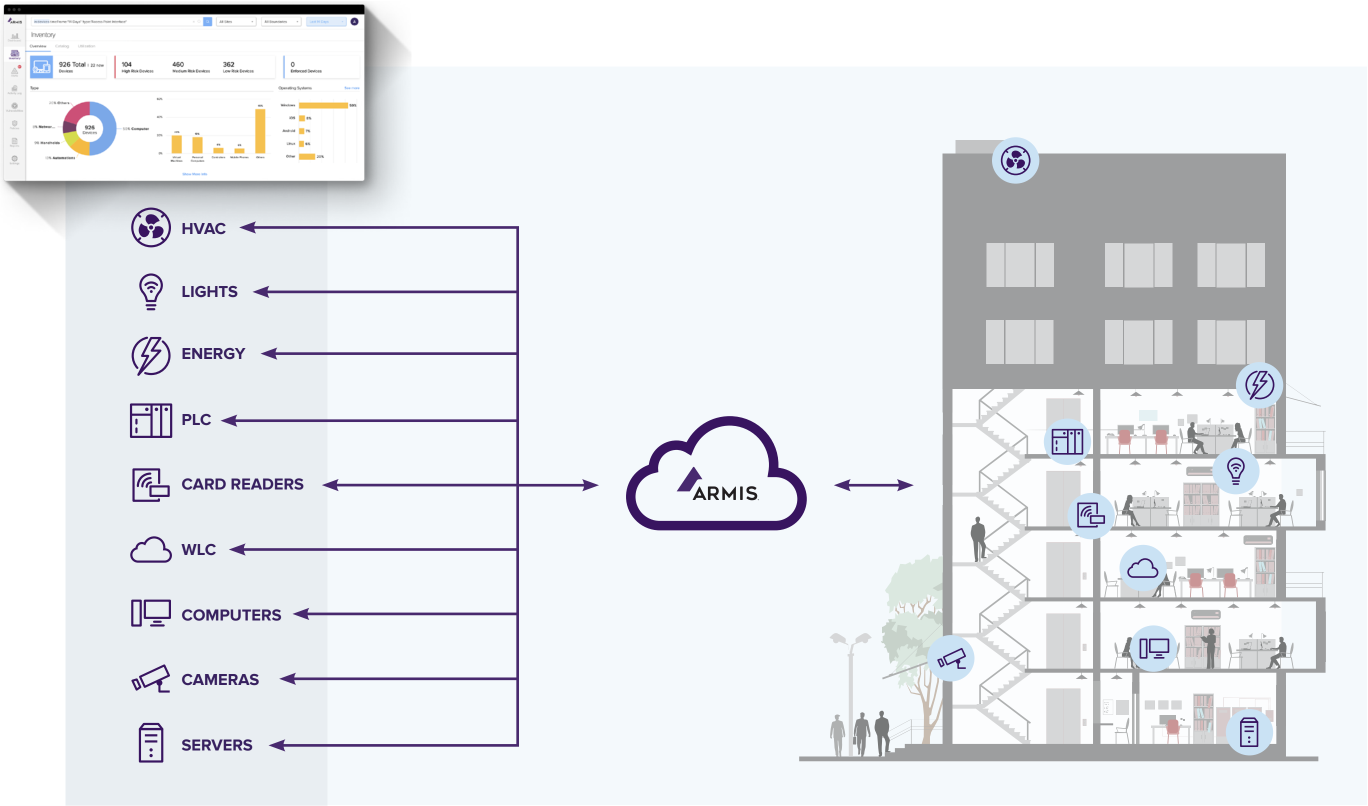


Figure 3: The Armis platform provides a central management console for every cyber asset and building across the enterprise,

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 "known-good" 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.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

1.888.452.4011 | armis.com

20210923-1

ARMIS.