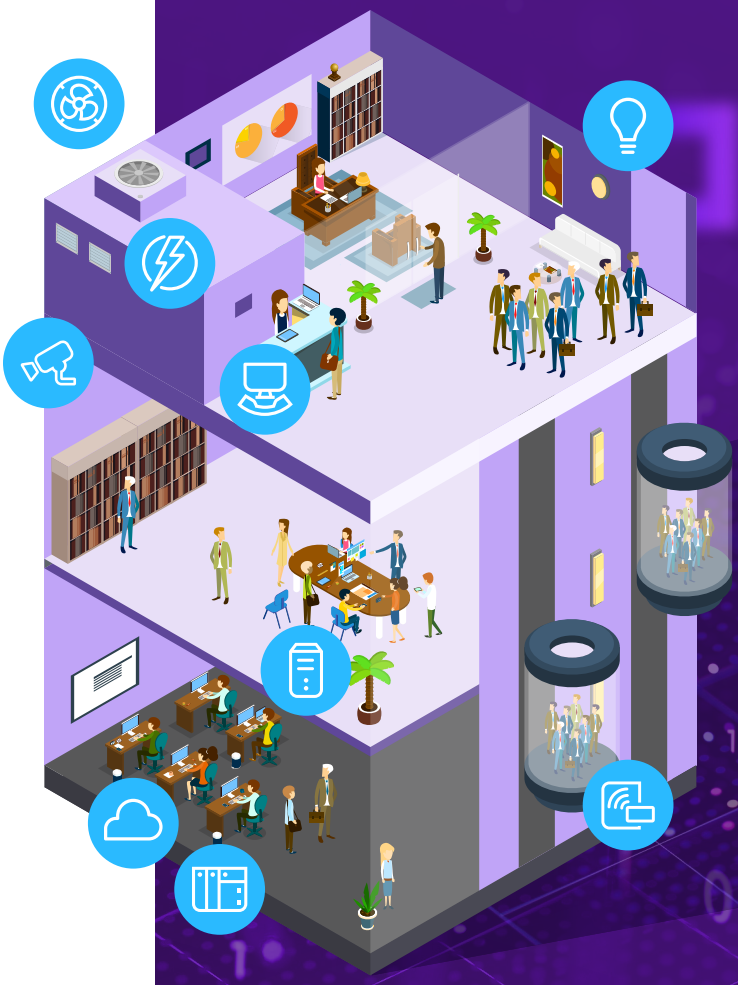
PARTNER BRIEF

The New Age of Building Management

Unifying Cyber Exposure Management, Operations, and Governance Across BMS Programs

© Copyright Armis 2025

The Challenge: We've Connected Everything, But Can't Control It



Modern smart buildings have evolved into complex ecosystems of interconnected assets that underpin the daily operation of diverse environments from skyrise office buildings and warehouses to data centers and critical infrastructure. These assets span IT, OT, and IoT systems, encompassing everything from HVAC, lighting, and elevators to sensors, meters, and access controls. While the integration of these systems has delivered unprecedented efficiency and insight, it has also introduced extraordinary complexity and risk. The challenge is compounded by the coexistence of legacy and modern, often unmanaged devices, making it difficult to maintain accurate inventories or fully assess cyber exposure and risk. In leased facilities or third party environments like datacenters, this complexity deepens, as landlords and tenants pursue different priorities: owners seek to protect physical infrastructure, while tenants focus on securing their digital estate and intellectual property. This, in turn, creates silos, gaps in visibility, and barriers to effective collaboration.

Organizations today face fragmented and incomplete asset inventories, devices running outdated firmware or with unverified configurations, forgotten or unsanctioned connections and fragmented telemetry and maintenance data. Onboarding and governance processes are often inconsistent across sites, creating silos that prevent cohesive oversight. The result is limited control over the estate and delayed action, meaning stakeholders can't govern systems properly because they can't secure complex systems they don't understand.

© Copyright Armis 2025

The Solution: Armis + KODE Labs + IntelliBuild

Armis, KODE Labs, and IntelliBuild have come together to unify cybersecurity, operational intelligence, and governance across the entire building management lifecycle.

Armis + KODE Labs: Real-Time Contextual Asset Intelligence

At the core of this collaboration is Armis Centrix™, the cyber exposure management platform. Armis continuously discovers, identifies, deduplicates and classifies every connected asset, their exposure risk and their pathways in real time without causing downtime.

Armis provides

- Manufacturer, Model, Firmware/OS version,Serial/MAC/IP, Device type and category
- Vulnerabilities (CVEs), Risk scoring, Exposure level, Compliance relevance
- Anomalous behavior flags, Protocols used, Communication patterns
- Ports and services, Connection history (internal + external), Location (VLAN/site)
- Business function/role, Utilization patterns, Connected systems/dependencies, Lifecycle status (EoL/EoS)
- Patch/update level, Support status, Asset tags/ownership
- Device behavior baselines- tracking an asset database of 6.5+ billion
- Network communication mapping, attack path analysis, and dynamic risk scoring
- Vulnerability management, deduplication and ownership
- Security posture, CVE exposure, and patch recommendations that create a proactive security posture with early warning capabilities.

© Copyright Armis 2025

KODE Labs

KODE delivers an end-to-end smart-building operating system that transforms fragmented environments into intelligent, high-performing portfolios. It starts by aligning with your vision: identifying the smart-building outcomes that matter most to you and defining a tailored roadmap across areas like Smart Commissioning, Energy Management, Team Experience, and portfolio-level insights. From there, KODE conducts a precise gap analysis to map your desired use cases against your current infrastructure, ensuring immediate actionability and clarity on where enhancements will deliver the greatest impact.

KODE integrates seamlessly across your entire building technology stack. This includes traditional BMS platforms like Tridium Niagara, Honeywell, Distech Controls, and Siemens Fire Systems, as well as modern IoT devices and enterprise ERP systems. As each connection comes online, KODE OS automatically validates data quality in real time, ensuring every sensor, system, and data stream is accurate and reliable.

By unifying BMS, IoT, and ERP data into a single operational layer, KODE enables true end-to-end building optimization. Digital Commissioning verifies equipment performance from day one. Fault Detection and Diagnostics (FDD) continuously monitors system health and identifies inefficiencies. Energy Optimization algorithms intelligently fine-tune energy usage as building conditions evolve. This connected ecosystem powers the full lifecycle of smart building and workplace management, from installation to ongoing energy and operations optimization.

By integrating verified Armis intelligence directly into KODE OS, you gain a validated, trusted digital profile for every asset. This combines accurate cybersecurity context with operational telemetry, fault trends, and performance data. This fusion closes the gap between system inventory, security posture, and real-time building behavior, providing unprecedented visibility and control.

IntelliBuild

IntelliBuild helps you operationalize intelligence by embedding governance, standards, and validation workflows throughout your entire building-management lifecycle, whether you are working with new construction or modernizing legacy environments. With the Quick-Deployment Playbook, Digital Commissioning, and Data Validation Services, IntelliBuild ensures that every one of your sites operates from a secure, consistent, and intelligent baseline.

IntelliBuild empowers you to navigate every stage of the smart-building journey with clarity and confidence. It guides you through new construction by helping you understand emerging technologies, modern design principles, and the operational impacts of creating intelligent spaces, while also preparing you for the cultural and strategic shifts required to adopt next-generation building environments.

For your existing structures, IntelliBuild provides the frameworks and best practices to seamlessly integrate with other tools/your existing stack, enabling you to execute retrofits and upgrades that enhance performance, efficiency, and resilience. It also supports you in managing the complexities of both ground-up projects and modernization efforts (greenfield or brownfield sites), offering strategies that elevate the intelligence of your entire portfolio through energy-efficient improvements and advanced IoT integrations. Beyond the technology itself, IntelliBuild strengthens operations by helping you optimize processes, align resources, and maximize the organizational impact of your smart-building initiatives, resulting in sustained performance improvements.

© Copyright Armis 2025

A Security Stack that Serves Multiple Personas

Stakeholder	Insight	Action
Facilities	Live performance and risk data	Predict and prevent downtime
IT / Cybersecurity	Full device visibility and posture	Enforce patching and segmentation policies
Owners / Operators	Portfolio-level insight	Benchmark risk, performance, and compliance
Project Teams	Construction-phase validation	Commission securely and accurately

The Power of This Collaboration in Greenfield Sites

The real promise of this partnership is realized in new construction or greenfield projects. For the first time, developers and owners can deliver buildings that are digitally accurate, secure, and operationally ready from day one.

In greenfield deployments:

> **Armis Centrix™** automatically discovers and fingerprints every device and pathway as it connects to the network, establishing the “source of truth” for all assets, their firmware, and their expected behaviors.

> **KODE Labs** validates telemetry and performance data in real time, ensuring each device behaves within approved design parameters before handover.

> **IntelliBuild** expertly deploys Armis Centrix™ and KODE Labs to enforce commissioning standards, while verifying configuration, governance, and cybersecurity readiness at every phase.

© Copyright Armis 2025

This creates a verified, digital-first foundation for the building's management:

- Complete and accurate asset inventory from day one
- Verified firmware and security posture baked into commissioning
- Reduced handover time and rework costs
- A future-proofed digital twin, continuously monitored for deviations

This is the new age of building management where cyber-resilience, performance, and governance are built in, not bolted on.

Business Outcomes: Bridging IT, OT, IoT and Operations

Reduced Operational Stress and Increased Empowerment

Operations teams experience significantly less pressure as visibility, validation, and governance are automated across the asset lifecycle. With Armis providing trusted device intelligence, KODE Labs consolidating performance and fault data, and IntelliBuild enforcing governance, operators gain the confidence to make informed decisions backed by verified insights. They can clearly communicate the true scope, dependencies, and risks of system issues to system owners and their respective responsibilities, aligning expectations and resource needs. This transparency removes fear around downtime and accountability, ensuring service-level agreements (SLAs) are met without guesswork. The result is a shift from reactive firefighting to proactive, empowered operations - where teams can focus on performance, not damage control.

Data-Driven Capital Planning and Investment Decisions

By unifying cybersecurity, operational, and lifecycle intelligence, the joint solution transforms how organizations plan and justify capital expenditures. Armis provides real-time visibility into device health, firmware status, and risk exposure; KODE Labs adds performance trends and analytics; and IntelliBuild links this intelligence directly to governance reporting and asset lifecycle data. Together, these insights allow owners and asset managers to prioritize replacements and upgrades based on verified condition, risk, and impact, not just age or failure history. This ensures capital investments target the assets that matter most, preventing unnecessary spend while reducing unplanned downtime. The outcome is smarter, defensible CAPEX forecasting that aligns technical needs with financial strategy.

© Copyright Armis 2025

Unified View

A single, shared data model aligns IT, OT, IoT, and operations. Everyone sees the same verified truth, from cyber posture to performance metrics.

Contextual Risk in Building Systems

Armis links device vulnerabilities directly to the building systems they support — translating abstract cyber risks into tangible operational impacts. If a BAS controller, field device, or sensor is compromised, teams can immediately see which HVAC zones, lighting sequences, or access systems are affected, what downstream dependencies exist, and the precise operational risk posed to comfort, safety, and uptime.

Empowered Building Operators

Operators gain full operational and cybersecurity context for every issue. When an air handler fault or network anomaly appears, they can explain exactly what's wrong, how it affects building performance, and what resources or downtime windows are needed to resolve it. This clarity enables proactive planning and credible communication with IT and ownership.

Automated Validation of Building Assets

No more blind device swaps or unchecked contractor fixes. Each time a controller, thermostat, or sensor is replaced or updated, the system automatically validates that the new asset meets configuration, performance, and security baselines. This ensures every action taken actually improves the building's reliability and cyber posture. It also keeps your contractors accountable.

Trust and Adoption Across Operations Teams

By continuously verifying vendor work, firmware compliance, and network dependencies, operators are supported rather than scrutinized. Instead of feeling exposed when Armis identifies risks, teams see a shared system of record that helps them demonstrate diligence, not deficiency, fostering confidence and collaboration.

Shared Accountability Across Stakeholders

Service-level agreements (SLAs), key performance indicators (KPIs), and compliance metrics are now grounded in verified, real-time data - not manual entries. Building owners, system owners, and facilities personnel share a single version of truth, ensuring transparency in both performance and risk, and aligning everyone toward measurable building outcomes.

© Copyright Armis 2025

BMS Use Cases and Measurable Impact

Use Case	Challenge	Outcome
HVAC Optimization	Drifted sensors, overrides, schedule misalignment	Energy savings; reduced downtime
OT Network Expansion	Untracked or unapproved devices	Complete visibility; zero-trust enforcement
Live Commissioning	Manual, error-prone asset capture	Much faster commissioning; no data gaps
Proactive Maintenance	Outdated CMMS data	Predictive CAPEX & OPEX planning; reduced unplanned downtime
Portfolio Governance	Inconsistent compliance tracking	Unified dashboards; continuous NIST/ISO alignment

Quantified Business Value

Metric	Measurable Outcomes
Visibility	Complete device and attack pathway discovery across IT/OT/IoT
Efficiency	Faster commissioning
Operational Cost	Lower maintenance and energy costs
Risk Reduction	Fewer untracked or vulnerable devices
Data Integrity	CMMS and telemetry accuracy

© Copyright Armis 2025

Building the Future of Secure, Intelligent Operations

The integration of Armis, KODE Labs, and IntelliBuild marks a pivotal shift in how smart buildings are managed, secured, and optimized. Together, these platforms unify the digital and physical layers of building management, transforming fragmented data into trusted intelligence that drives real action. From design and commissioning through daily operations, this partnership delivers continuous visibility, verified performance, and embedded governance. Operators gain confidence, system owners gain context, and building owners gain assurance that their assets are protected, efficient, and future-ready. This is more than a technical integration; it is the foundation for the next generation of building lifecycle management: secure by design, intelligent by default, and governed by data.

Explore Armis Centrix™ and learn how we help you see, secure, and manage every asset.

Book a Personalized Demo

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

armis.com

© Copyright Armis 2025