Total Visibility, Absolute Control.

See Every Asset, Stop Every Threat: How to Secure Your Critical Operations.

The Partnership

The alliance between Armis and Illumio integrates best-in-class asset intelligence with leading Zero Trust Segmentation to deliver a unified security architecture.

This partnership bridges the critical gap between visibility and enforcement by combining **Armis Centrix™** and its ability to see and analyze every asset—managed, unmanaged, IT, OT, and IoT—with Illumio's ability to apply granular access controls.

Together, they enable organizations to visualize their entire attack surface and immediately apply breach containment policies, effectively turning deep asset context into active protection across the enterprise.

Why IT Matters

Digital convergence has dissolved traditional air gaps, allowing ransomware and cyber threats to move laterally between IT and OT environments with ease.

With connected assets expected to reach 50 billion, organizations face massive visibility blind spots because standard tools often fail to detect unmanaged and industrial devices. Implementing Zero Trust security is essential to stop these threats, but organizations cannot segment what they cannot see or understand.

This partnership eliminates those blind spots, providing the foundational visibility and context required to build safe, effective segmentation policies that prevent minor compromises from escalating into "cyber disasters".

Together Armis and Illumio are on a mission to protect our client's most critical assets, including:

Unified Asset Visibility:

Armis Centrix™ delivers real-time, comprehensive discovery of all assets—including IT, OT, IoMT, and cloud workloads—presented in a single, unified view to eliminate shadow IT and blind spots.

Context-Driven Policy Building:

Armis Centrix™ provides deep intelligence on asset behavior, risk scores, and communication flows, enabling Illumio to build accurate Zero Trust policies that align with operational requirements without disrupting business.

Secure Digital Transformation:

Organizations can safely integrate new technologies and connect industrial environments by enforcing policies that maintain compliance and uptime while securing airgapped, converged and hybrid IT/OT environments.

Proactive Lateral Movement Protection:

Users can identify and microsegment offending assets (such as critical infrastructure or patient databases), ensuring that only verified assets and associated communications are allowed and preventing the spread of malware.

Automated Threat Response

The integration allows for dynamic response; when Armis Centrix™ detects a threat or abnormal behavior, it can trigger Illumio to automatically apply strict segmentation controls to isolate the compromised asset immediately.

By combining Armis's "map" of risks and dependencies with Illumio's "enforcement" engine, the joint solution empowers organizations to move from reactive detection to full situational awareness and proactive containment. Armis Centrix™ understands every asset and its risk, while Illumio executes the necessary Zero Trust segmentation, ensuring breaches are contained before they impact critical operations.

ARMIS®

Customer Value

How do Armis and Illumio specifically prevent ransomware from spreading?

Extreme Visibility With Context

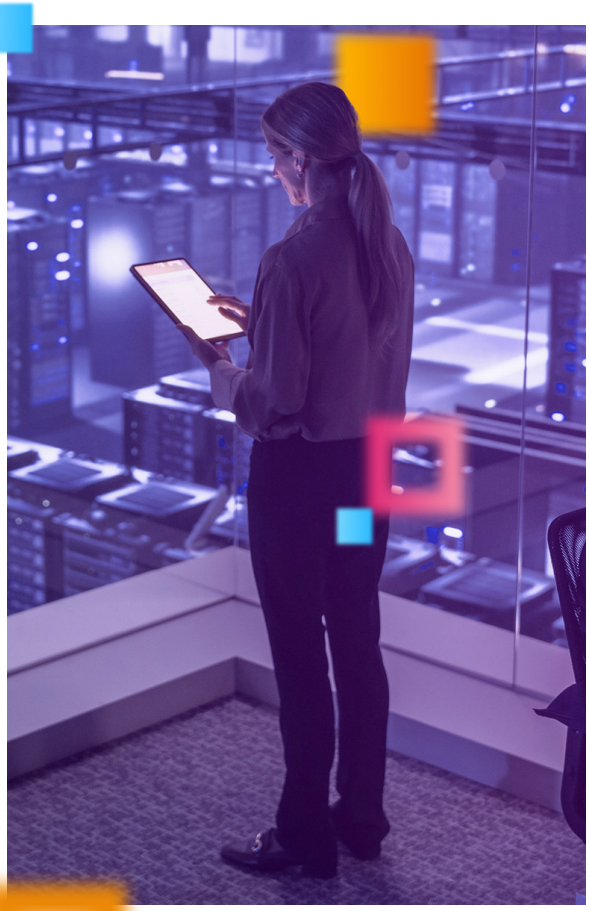
Accelerated Segmentation

Prioritized Mitigation

- **Accelerated Zero Trust Implementation:** Removes visibility barriers, allowing teams to deploy micro-segmentation faster and with confidence that they will not break critical processes.
- **Minimized Blast Radius:** Stops ransomware and breaches from spreading across the hybrid attack surface, protecting core business operations from downtime.
- **Operational Resilience:** Ensures continuity for critical infrastructure and healthcare environments by securing unmanaged and legacy devices that cannot take traditional agents.
- **Streamlined Compliance:** Helps organizations meet strict regulatory standards (e.g., NIST, NIS2) by enforcing access controls and proving segmentation efficacy.
- **Reduced Manual Effort:** Automates the discovery of communication pathways and the application of containment policies, reducing the burden on security operations.

Armis and Illumio deliver total visibility, unprecedented security, absolute control for your converged enterprise.

By combining cyber exposure management and security with automated Zero Trust enforcement, you can proactively stop ransomware and contain breaches without disrupting critical business operations.



Get the big picture on today's security challenges—and how Armis helps solve them.

Explore Armis Centrix™ Today

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