PARTNER BRIEF

Illumio + Armis: Cyber Exposure Management & Security Delivers Zero Trust Across Converged Environments

Digital convergence has revolutionized industries such as manufacturing, energy, and healthcare by enabling new business models and driving operational efficiency. However, hyperconnectivity has also introduced significant cyber risks, with attackers increasingly exploiting these interconnected environments. Without robust security controls, IT/OT convergence can facilitate the lateral movement of ransomware and other threats across networks.

Implementing a Zero Trust security model is essential to containing threats and blocking cyberattacks in these environments. Microsegmentation serves as a cornerstone for implementing Zero Trust security by restricting unauthorized communications, access and activities. However, before effective policies can be enforced, organizations must achieve comprehensive visibility into all connected assets, their accessibility, business context, and communication pathways. Without this foundational insight, implementing proper security policies becomes nearly impossible.

Full Visibility & Zero Trust Segmentation

The integration between Illumio's Zero Trust Segmentation solution and Armis Centrix™ Cyber Exposure Management Platform delivers unprecedented protection for converged IT/OT environments, ensuring security across all connected assets.

With Illumio and Armis, you can:

- **Discover, classify, and map all IT, OT, IoT assets** in a unified view, spanning on-premises, cloud, data centers, industrial facilities, retail locations, and remote branches.
- **Gain deep situational awareness and risk context** for all assets, ensuring security measures align with operational requirements and business resilience.
- **Identify and proactively isolate high-value assets** to prevent the lateral spread of cyber threats and unacceptable risk. Zero Trust segmentation ensures only verified communications and activities are allowed, minimizing attack vectors that can be exploited.
- **Automate response actions** by dynamically applying segmentation controls when malicious activity is detected in order to arrest the threat and contain the risk.

Securing the Converged IT/OT Environment

The integration between Illumio's Zero Trust Segmentation solution and Armis Centrix™ Cyber Exposure Management Platform delivers unprecedented protection for converged IT/OT environments, ensuring security across all connected assets.

1 Visibility

- Achieve real-time asset discovery and continuously map all connections within IT and OT environments.
- Identify all pathways that attackers could exploit to gain access to critical systems.

2 Context

- Understand how assets interact within the network, ensuring security policies align with business functions.
- Deduplicate, contextualize, prioritize, assign, and mitigate vulnerabilities based on real-world risk exposure and potential impact.

3 Control

- Enforce Zero Trust Segmentation policies to isolate and contain threats before they disrupt operations.
- Dynamically restrict access and apply granular controls in response to emerging threats.

4 Transformation

- Accelerate digital transformation securely by integrating new technologies while minimizing cyber risk.
- Ensure compliance with regulatory and cybersecurity standards by enforcing strict access controls.

Unified Asset Intelligence: The Foundation of Zero Trust Security

The Armis and Illumio integration enables organizations to achieve complete visibility, security and control across converged IT and OT networks. Armis Centrix™ continuously discovers and classifies all connected assets, mapping communication flows between operational technology (OT), information technology (IT), industrial IoT (IIoT), cloud workloads, applications, and services—all presented within a single, interactive dashboard.

Capabilities include:

- **Automated asset discovery and continuous monitoring,** ensuring complete visibility with deep situational awareness into the attack surface.
- **Context-driven security insights,** allowing organizations to prioritize and address the risks that matter, effectively.
- **Seamless integration with Illumio,** enhancing segmentation policies with real-time asset intelligence and risk assessments.

Illumio applies Zero Trust Segmentation across IT workloads, including Linux, Windows, AIX, IBM Z Series, containers, and cloud environments. By incorporating Armis's contextual asset intelligence, security teams gain a comprehensive view of network dependencies and can enforce segmentation policies with a few simple clicks.

When an issue is identified, the Armis and Illumio joint solution rapidly identifies the affected assets, applies containment measures, and prevents lateral movement, minimizing operational disruption and protecting critical systems.

Illumio + Armis: Unifying Visibility, Intelligence, and Enforcement

With Illumio and Armis, organizations can see, secure and manage Zero Trust Segmentation across IT, OT, and IoT environments from a single, interactive platform. This powerful integration delivers:

- Complete asset visibility and risk-based prioritization
- Real-time threat containment and Zero Trust policy enforcement
- Seamless security orchestration for IT and OT convergence

Visit: https://www.illumio.com/partners-tap/armis or www.armis.com/illumio

illumio

Illumio, the Zero Trust Segmentation Company, stops breaches and ransomware from spreading across the hybrid attack surface.

The Illumio ZTS Platform visualises all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organisations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.

ARMIS

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

Free Trial