INTEGRATION BRIEF

Illumio + Armis: Zero Trust for Converged Networks

The leader in microsegmentation and the leader in Unified Asset Intelligence deliver Zero Trust across IT, OT and IoT Networks.

Securing the Converged IT/OT Environment

Convergence has enabled new business models and generated significant improvements in operational efficiency for many industries, including manufacturing, energy and healthcare. However, hyperconnectivity has also exposed these environments to cyber risk that attackers are actively exploiting. If IT/OT convergence is not implemented with effective security controls in place, connected assets can allow the spread of ransomware and other threats across these environments.

The implementation of a Zero Trust security model can help contain threats and block cyberattacks across these environments, as the main concept behind Zero Trust is that devices should not be trusted by default and should not be allowed to communicate with each other unless required. Microsegmentation offers an efficient way to implement the foundations for Zero Trust security.

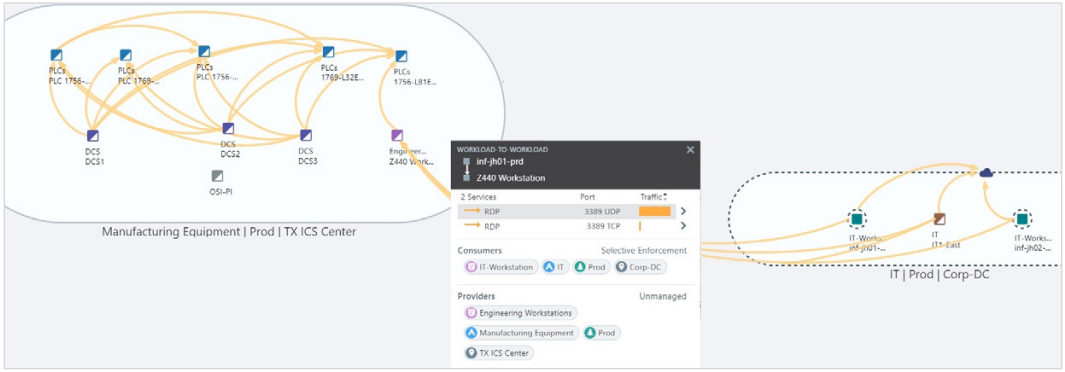
However, before implementing these controls, organizations must understand what assets are connected to these networks, what their business context is and how they communicate with each other. A lack of visibility across the converged IT/OT environment makes it difficult to understand the connectivity between devices and potential threats. This makes putting the appropriate policies in place nearly impossible.

Full Visibility & Zero Trust Segmentation

The integration between Illumio's microsegmentation solution and Armis's Unified Asset Intelligence Platform provides unprecedented protection across converged IT/OT environments, covering all connected assets.

With Illumio and Armis, you can:

- Discover, categorize, and map all IT, OT, IoT, and cloud communications in a single view, regardless of location: on premises, in the cloud, in data centers, on the plant floor, at retail stores, or at remote bank branches.
- Understand the business context of the assets and the risk they may introduce to the business.
- Identify and ring-fence high-value systems to protect them from the spread of breaches. Zero Trust Segmentation means only verified communications will be allowed, preventing the movement of any malware.
- Build an automated incident response system to apply extra restrictions should an attack be detected.



Complete Visibility of IT + OT + IoT Assets and Network Flows

Visibility and Control Across the Converged IT/OT Environment

Visibility
See the connections across your IT and OT environments to map where security policies are required.

Context
Understand the context of the different connected assets and their operations to make informed decisions.

Control
Put in the policies to prevent attacks from becoming business disasters by deploying Zero Trust Segmentation.

Transformation
Accelerate business growth and innovation by securing the digital transformation and adoption of new connected technologies.

Unified Asset Intelligence: The Key to Effective Zero Trust Implementations

By integrating Armis with Illumio, it is now possible to see all connected assets across converged networks and understand their context and the flow of communications between operational technology (OT) systems, information technology (IT) systems, industrial IoT (IIOT), cloud workloads, applications, and services — all in a single, interactive map.

Armis Unified Asset Intelligence Platform discovers all connected assets, maps out the communications and relationships between them, and adds contextual intelligence to help you understand their business context and the risk they may introduce to the business.

Illumio uses compute workload metadata and flow information to map communications between workloads. Using your existing naming structure, simple labels are applied to each workload to display the entire infrastructure. These IT systems could be traditional Linux and Windows systems, AIX, IBM Z Series, containers, and cloud platforms.

The combined contextual data of Illumio-labeled systems and Armis asset intelligence is imported into the Illumio application dependency map and displayed in a single view. Vulnerabilities, imported from industry-leading scanners, that indicate points of higher risk within the infrastructure can be identified and prioritized, with appropriate remediation measures put in place.

For example, you can implement Zero Trust Segmentation with only a few simple clicks on the map to protect IT and OT assets. All the devices and systems within a function can be compartmentalized to isolate them from potential threats in other areas of the infrastructure.

Illumio's mapping and Zero Trust Segmentation capabilities powered by Armis contextual asset intelligence gives organizations the comprehensive visibility and control needed to reduce risk and increase cyber resilience.

When a breach occurs, the Illumio and Armis integrated solution can help you quickly identify and contain its spread, avoiding a major shutdown of critical systems.

Illumio + Armis: Complete Visibility, Intelligence, and Enforcement

It is now possible to see, analyze, and apply microsegmentation across your network of IT, OT, and IoT systems within a single, interactive dashboard.

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

About Illumio

As the pioneer of Zero Trust Segmentation, Illumio prevents breaches from becoming cyber disasters. Gain real-time visibility and segmentation control to see your risks, isolate attacks and secure your data across hybrid clouds, data centers and endpoint devices.

About Armis

The Armis Asset Intelligence Platform automatically collects and analyzes data through hundreds of integrations to provide complete and continuous visibility into your asset security posture.