illumio

PARTNER BRIEF

Illumio + Armis: Securing Converged IT/OT Environments

Stop OT threats from turning into downtime with visibility and control across IT, OT, and IIoT environments.

OT is evolving. So are the risks.

The shift to Industry 4.0, smart grids, and new systems like EV charging networks is transforming how operational technology (OT) works.

Today's environments are more connected and efficient than ever. But they're also more vulnerable. As legacy equipment merges with gateways and modern controls, the attack surface grows.

Cyber resilience can no longer be assumed. It has to be built in.

Why OT security is so complex

Securing OT isn't as straightforward as security IT. Many OT environments still rely on decades-old machines that were never designed with cybersecurity in mind.

You're often working with a patchwork of industrial control systems (ICS), legacy hardware, and purpose-built devices — many of which can't be easily patched, accessed, or even seen.

That lack of visibility means if an attacker gets in, it's hard to know where they went or stop them before damage is done.

Zero Trust isn't optional for OT environments

Zero Trust isn't just for IT anymore. In OT environments, it's essential.

By default, Zero Trust assumes no device should talk to another unless it has to — and only when it's safe. That's exactly the mindset you need to contain attacks and limit their fallout when every second counts.

Key benefits

Visibility

Discover assets in real time and continuously map all connections in your IT and OT environments.

Context

Understand how assets interact. Ensure your security policies support your business, not block it.

Control

Easily enforce segmentation to contain threats fast and keep operations running.

Transformation

Adopt new tech with confidence and accelerate innovation without increasing risk.

Visibility is key to OT security

Visibility is the foundation of Zero Trust, but it's not always easy to achieve in OT environments. Many systems are closed off from traditional IT security tools. That's why you need a solution that's purpose-built to deliver granular visibility and breach containment across IT, OT, and IIoT environments.

Illumio + Armis: how it works

Together, Illumio and Armis deliver a real-time, unified map of all assets and communications across OT, IT, IIoT, cloud, and applications. You can quickly understand your risk and proactively prepare for breaches.

- Armis automatically discovers every connected asset, shows how they're talking to each other, and adds rich context about their role and risk to your business.
- Illumio ingests this intelligence, using tags and telemtry from Armis to label workloads and track traffic in and out of your OT fabric. Everything is visualized in a single, intuitive map.
- With this information, Illumio can automatically enforce policies, isolate high-risk assets, deny or allow specific communication, and stop lateral movement before it spreads.

Why OT security is so complex

Go beyond visibility into your OT environments. The integration layers vulnerability data from trusted scanners to flag the most at-risk assets. Teams can prioritize what to fix based on both risk level and operational impact.

You don't have to guess. You know exactly where to focus remediation efforts for the biggest payoff.

Zero Trust for OT made simple

With Illumio and Armis, you can build Zero Trust security across your OT environment with just a few clicks:

- **Build segmentation** policies straight from the map.
- **Contain threats** before they disrupt operations.
- **Compartmentalize systems** to stop threats from spreading.
- **Protect IT, OT, and IIoT systems** with the same level of confidence.

Resilience starts with visibility and control

When a breach happens — and eventually, one will — you need to detect it fast and stop it even faster.

The Illumio and Armis integration gives you the context, control, and confidence to do just that. Together, we help you protect uptime, reduce risk, and keep your most critical systems running, no matter what.

Learn more about the Illumio + Armis integration

illumio.com/partners-tap/armis

About Illumio

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments – stopping the spread of attacks before they become disasters.

About Armis

Armis, the cyber exposure management and 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.