Illumio + NVIDIA: Zero Trust for OT Environments

Visualize and enable Zero Trust policy for critical OT environments through integration with the NVIDIA BlueField Platform

A breakthrough partnership

Operational technology (OT) environments have long been difficult to secure. Legacy systems, limited visibility, and a patchwork of devices that can't run security or policy agents make protecting them a struggle.

To address this challenge, Illumio and NVIDIA have joined forces to deliver microsegmentation to critical OT environments — without forcing changes to OT devices.

By integrating the Illumio breach containment platform with NVIDIA® BlueField® data processing units (DPUs), organizations can now gain visibility into and enforce segmentation policies around OT systems. This joint solution helps security teams:

- Stop lateral movement
- Reduce the risk of downtime
- Build cyber resilience directly into OT environments

Illumio provides real-time telemetry and policy management; NVIDIA BlueField enforces policy at the network edge. Together, the solutions provide unified Zero Trust security across IT and OT domains.

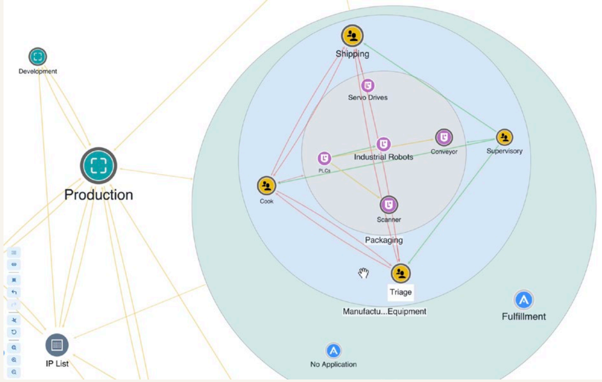
Stopping lateral movement

Attackers rarely stop at the initial breach. They move laterally — often exploiting two key weaknesses:

- **Human behavior** is unpredictable and can't be patched. Even well-trained users may click a malicious link or open a compromised file.
- **Open ports** between systems — including those leading to OT devices — offer attackers ready-made pathways to spread deeper into the network.

Once inside, they exploit misconfigurations and exposed services to move between IT and OT environments undetected.

Key Benefits



Deliver Zero Trust to OT devices

Illumio delivers real-time visibility and segmentation into OT environments, which has not been possible before.

Seamless visibility

Illumio enables the flexible labeling of OT devices to deliver full visibility to and from all OT devices.

Enforcement with NVIDIA BlueField

Protect OT environments using NVIDIA BlueField DPUs as edge enforcement points.

Enforcing OT security at the edge

Many OT devices can't support security agents — making them invisible to traditional security tools. NVIDIA BlueField DPUs solve this by offloading and isolating networking and security tasks from the host CPU, running them on dedicated Arm cores within the DPU.

This allows the BlueField platform to act as a proxy enforcement point for OT systems — no changes to the OT devices required.

By deploying BlueField on hosts connected to OT devices, organizations can bring those systems into the Illumio Platform. Illumio receives OT telemetry from inventory tools such as Armis and Claroty, populates metadata, and brings the devices into view for policy definition and enforcement. That means security teams can see all traffic to and from the OT devices and enforce Zero Trust policies for them.

Illumio blocks lateral movement by permitting only authorized traffic between systems. So breaches can't spread from a compromised OT or IT device to the rest of the environment. With an assume-breach mindset, Illumio focuses on containment — enabling organizations to detect, isolate, and limit the attack surface in real time.

Using Illumio's label-based policy model, segmentation rules can be defined for each OT resource. Those policies are pushed directly to the BlueField DPU, which enforces least-privilege access between OT and IT systems.

This integration brings scalable, agentless enforcement to OT environments across industries, from manufacturing to telecom to healthcare.

Illumio Insights

OT environments can generate mountains of telemetry. But buried in all that data are the few critical indicators that matter. Illumio Insights helps security teams find the needles in the haystack: the vulnerabilities, misconfigurations, and indicators of compromise that could lead to disaster.

By analyzing workload and network telemetry in real time, Insights surfaces both current and emerging risks. Teams can instantly quarantine compromised systems to stop threats from moving laterally.

Illumio Segmentation

Illumio is built on the assumption that breaches are inevitable. Rather than chasing perfect prevention, it focuses on fast, effective containment. Key capabilities of Illumio Segmentation include:

- **Application dependency mapping**: Visualize real-time traffic flows in context using an AI-powered security graph.
- **Context-based segmentation**: Use metadata such as role, application, environment, or location to organize workloads. Define scalable segmentation policies based on business logic, not IP addresses.
- **Least-privilege access control**: Limit communication between workloads to only what's necessary. Block protocols such as SSH and RDP by default, except from designated admin systems.

For critical OT assets, Illumio enables ringfencing. It allows trusted internal communication while locking down all external access attempts. The result is a dynamic protect surface around every system — across both IT and OT.

With NVIDIA, Illumio visualizes and protects all OT devices, quickly discovering threats at any scale, preventing a small breach of an OT device from escalating into a disaster.

Ready to contain the breach?

Start your free trial today.

Illumio.com/try-Illumio

About Illumio

Illumio, the most comprehensive Zero Trust solution for ransomware and breach containment, protects organizations from cyber disasters and enables operational resilience without complexity. By visualizing traffic flows and automatically setting segmentation policies, the Illumio Zero Trust Segmentation Platform reduces unnecessary lateral movement across the multi-cloud and hybrid infrastructure, protecting critical resources and preventing the spread of cyberattacks.