Illumio + NVIDIA: Bringing Zero Trust to the Edge of OT

Stop lateral movement with hardware-accelerated segmentation

Operational technology (OT) is notoriously hard to secure. Legacy systems, flat networks, and performance-sensitive applications leave little room for legacy network controls. This creates blind spots where attackers can move unseen.

Illumio and NVIDIA have partnered to close that gap. By integrating Illumio Network Enforcement Nodes (NENs) with NVIDIA BlueField Data Processing Units (DPUs), organizations can enforce Zero Trust security policies closer to devices for more granular and effective OT security.

This hardware-enhanced approach offloads segmentation and enforcement to the DPU. Security teams get deep visibility and real-time control without slowing down OT applications. The results:

- Attacks are contained faster.
- Workloads are more strongly isolated.
- Lateral movement is contained.

With Illumio and NVIDIA BlueField, organizations gain a new, purpose-built layer of defense for today's most complex IT/OT environments.

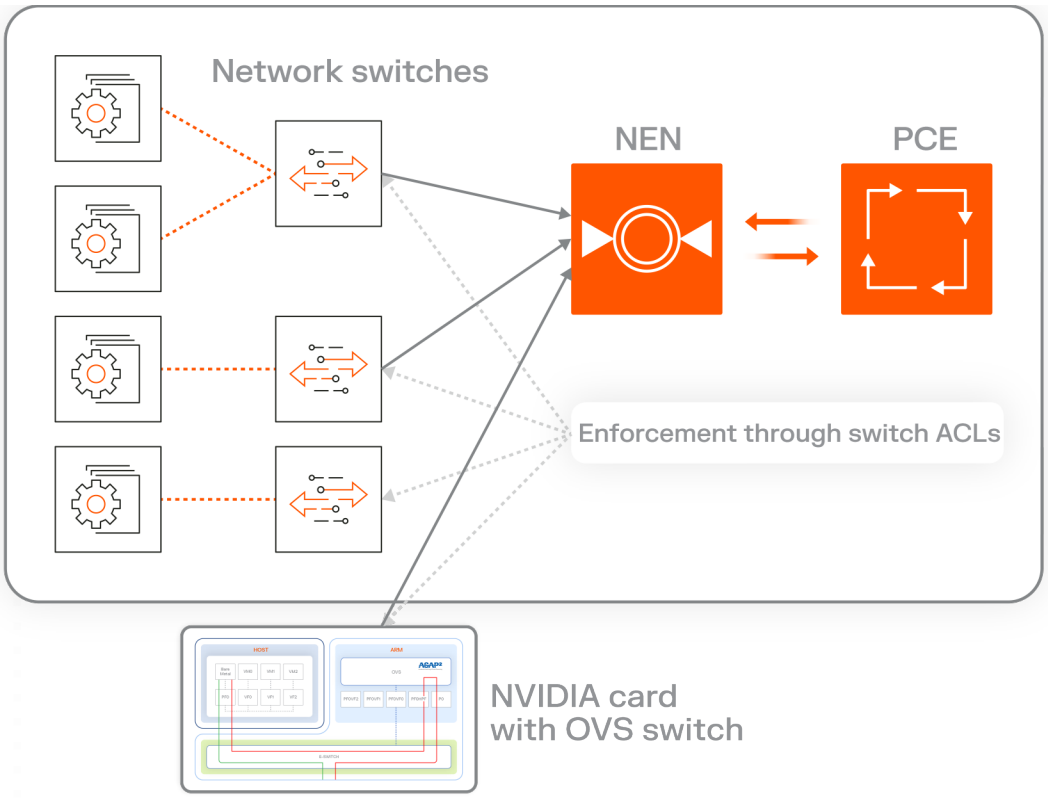
Architectural overview

The joint architecture blends hardware acceleration with policy-driven segmentation. Together, Illumio and NVIDIA deliver a practical design that embeds Zero Trust enforcement into the fabric of OT systems.

NVIDIA BlueField DPUs

Modernizing OT security doesn't have to mean expensive hardware upgrades. NVIDIA BlueField DPUs drop directly into existing systems. You can replace or augment standard network interface cards (NICs) with BlueField-enabled SmartNICs, which fit into standard PCIe slots.

This approach lets you strengthen security at the hardware level without overhauling your IT/OT environment. You keep the systems you've already built — and gain the security you need.



Illumio Network Enforcement Node (NEN)

Illumio Network Enforcement Nodes (NENs) integrate with NVIDIA BlueField DPUs, making each DPU a policy enforcement point. The two work together to:

1. **Define policies.** Security teams define workload-specific rules in the Illumio Policy Compute Engine (PCE).
2. **Distribute rules.** Policy rules are instantly sent to NEN instances running on BlueField DPUs.
3. **Generate ACLs.** Each NEN translates the rules into precise access control lists (ACLs) for your network switches
4. **Enforce policy.** ACLs are loaded to Open vSwitch (OVS) on the NVIDIA DPU. This enables dynamic, policy-driven segmentation.

Policies are enforced in OT environments

Instead of relying on upstream firewalls or external controls, this architecture enforces policies for each group of OT devices.

When traffic reaches a BlueField DPU running an Illumio NEN, the DPU:

1. **Inspects traffic.** The DPU receives and inspects network traffic.
2. **Applies policy.** The NVIDIA Open vSwitch (OVS) on the DPU applies the Illumio-generated Access Control Lists (ACLs).
3. **Accelerates enforcement.** The DPU offloads processing tasks. This lets OVS enforce policies efficiently without hurting performance.
4. **Centralizes logic management**. OVS manages enforcement logic across the environment for consistency and control.

This design delivers both speed and precision. Policies enforced at the OT level are the same as those applied to the rest of the environment.

Technical capabilities

The joint Illumio and NVIDIA BlueField architecture strengthens security without adding complexity, so you can:

- Deploy faster
- Enforce policies more uniformly
- Minimize disruption to your environment

In short, your team gains value quickly while maintaining performance and reliability.

Simplified access to critical intelligence

Illumio NENs combine network intelligence into a single stream to the PCE. By consolidating data from different switches, teams gain faster analysis, clearer decisions, and consistent policy enforcement.

Lightweight deployment

NENs have a small footprint, so they deploy quickly and are easy to manage. Teams can accelerate time-to-value and start capturing intelligence right away with little overhead.

Non-intrusive

Deploying NENs doesn't require costly or time-consuming changes to your IT architecture. That means you can keep your established workflows and infrastructure investments in place while instantly getting better visibility and control.

Future-ready footing

By combining Illumio policy-driven segmentation with NVIDIA BlueField hardware acceleration, you can finally bring Zero Trust security to the edge of OT environments. This joint architecture delivers deep visibility, fast enforcement, and real-time containment. Best of all, it doesn't slow down the business. It's a future-ready footing for securing the most critical parts of modern OT.

See how Illumio and NVIDIA can help secure your critical OT systems.

Visit: www.illumio.com/partners-tap/nvidia

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.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.