

Enforcing Security Policy Across OT and IT with Illumio

Connections, not flaw counts, decide where OT policy goes first

In an OT network, the riskiest system may be the one with the fewest flaws. Take an engineering workstation with only a few known vulnerabilities. It connects to many systems, so an attacker who takes it over can use it to reach them. Now take an OT device full of vulnerabilities that talks only to one secure PLC. An attacker who takes that over has almost nowhere to go.

Operational technology (OT) covers a lot of ground. It includes industrial control systems (ICS), distributed control systems (DCS), supervisory control and data acquisition (SCADA), medical IoT, building management systems (BMS), and more. Each comes with its own regulations and operating constraints. They all share one rule, though: security can't stop production.

That's why OT security calls for a risk-based approach. It protects the most critical systems first and doesn't waste resources on low-risk ones. Illumio makes that practical. It maps how systems connect, shows where exposure is highest, and enforces policy at whatever point each environment allows, without interrupting production.

Start with visibility and context

Illumio partners with vendors such as ServiceNow and Claroty to identify assets and add context about each one. Illumio then maps in real time how those systems communicate and uses AI to flag potential risk. With that context, policy can target the assets that matter most.

Three key questions:

- 1 What are the critical parts of the system you're protecting?
- 2 How are things connected?
- 3 What are the threats?

Policy can work at many layers to build defense in depth. Exposure should decide where it goes first. As the workstation example shows, a system's connections can matter more than its flaw count. The most connected systems go to the top of the list.

Pair the Illumio map with a partner's vulnerability data, and you can see each system's exposure and where policy will help most. Some systems are high-value targets and should always be secured. These include engineering workstations, energy management systems (EMS), historians, and OPC servers.

Regulators increasingly recommend host-based firewalls as the preferred way to enforce policy. Illumio makes host-based enforcement simple, whether systems run on Windows or Linux, in containers, or in the cloud.

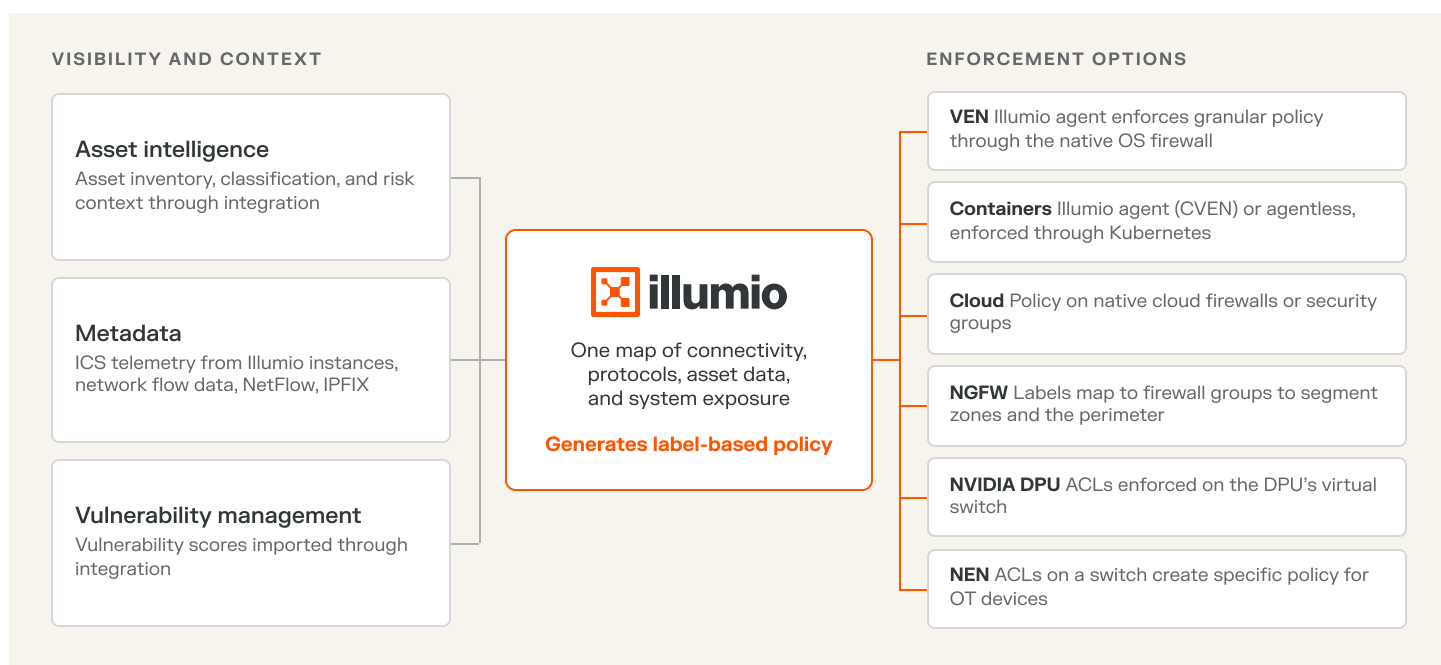
Address the core challenges

Security policy in an OT environment has four main priorities:

- 1 Mitigate exposure:** Secure vulnerable and overconnected systems.
- 2 Standardize policy:** Make sure systems use secure protocols consistently.
- 3 Harden the IT/OT boundary:** At remote sites, this line can blur.
- 4 Build and test an isolation plan:** Decide ahead of time what gets cut off during an attack.

Choose an enforcement point

In OT, the goal is secure connectivity. Illumio uses one label-based policy model to tackle all four priorities. You enforce it in whichever way fits each environment's regulatory and operating needs.



Why it matters for OT

- **The line keeps running.** Planned, tested containment takes seconds. It needs no maintenance window and doesn't halt production.
- **One policy model, many enforcement points.** The same labels and policy apply on hosts, in Kubernetes, in the cloud, and on network switches.
- **Proof for the frameworks that matter.** Policy and containment evidence map to NERC CIP, NIS2, IEC 62443, and NIST SP 800-82. You can show your security posture on demand.

Remember that engineering workstation with only a few flaws? With Illumio, you can see every system it talks to, limit it to the connections it needs, and contain it fast if an attacker gets in. The rest of the plant keeps running.

Enforcement options at a glance

Path	How it enforces	Where it fits
VEN (Illumio agent)	Applies policy through the system's host firewall without disrupting operations.	Engineering workstations, EMS, manufacturing execution systems (MES), OPC servers, historians
Containers (agent and agentless)	Applies policy through Kubernetes.	MES, OPC servers
Cloud	Applies policy to cloud firewalls or security groups.	MES, EMS, digital twins
NEN (network enforcement)	Translates policy into ACLs on supported switches. Nothing is installed on the device.	Connections from OT devices to controllers, medical technology, and anywhere other options aren't available
NGFW (existing firewalls)	Enforces segmentation policy through firewall instances, including those between IoT/OT zones and across IT infrastructure.	Available today: Microsoft Azure Firewall, Check Point. Planned: Fortinet, Palo Alto Networks, AWS Network Firewall.
NVIDIA BlueField DPU	Loads NEN-generated ACLs onto the DPU's virtual switch (OVS) to enforce at the switch interface. Flow data from the OVS feeds the same Illumio map.	Systems that can't run a VEN

Learn more

See how Illumio secures OT and IT with one policy model. Visit:

illumio.com/solutions/use-cases/it-ot-convergence

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 and Customer Favorite in The Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.

Copyright © 2026 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.