

Securing the Manufacturing Industry with Illumio

How Illumio gives manufacturers real-time IT and OT visibility, contains breaches, and keeps operations running.

Modern manufacturing runs on connection. Industry 4.0 tied operational technology (OT) to IT systems, cloud platforms, and remote support teams.

The efficiency gains are real. But each of those links can also create a security gap. When ransomware finds one, the production line stops and losses pile up by the hour. This is why manufacturing sits near the top of every attacker's target list.

The scale of the damage comes down to one thing: how far an attack can spread laterally once it's inside.

Key challenges facing manufacturing

The pressures on a plant floor are specific, and they compound. Six of them show up in nearly every manufacturing environment.

Converged IT and OT environments. Control systems that once ran on closed networks now connect to business apps, cloud services, and remote maintenance links. Every connection opens another path between IT and OT.

Legacy equipment and long asset lifecycles. Programmable logic controllers (PLCs), human-machine interfaces (HMIs), historians, and supervisory control and data acquisition (SCADA) systems stay in service for decades. Most can't be patched or replaced without stopping production.

Ransomware and lateral movement. Downtime costs money by the hour, and once attackers are inside, perimeter defenses do nothing to stop them moving toward production systems.

Lack of visibility. Old network diagrams and partial asset lists leave teams guessing at which systems talk to each other. Guesswork makes risk impossible to judge.



Illumio provides unparalleled and practical traffic transparency. This allows us to manage all traffic and to discover misconfigurations and malicious activity rapidly.”

Thomas Vavra

Communication Infrastructure Manager
Mondi Group

Operational downtime. OT can't absorb outages the way IT can, so security has to hold while the lines keep running.

Regulatory and standards compliance. Meeting IEC 62443 and national agency guidance gets harder across large sites spread over many countries.

How Illumio secures manufacturers

The Illumio approach to manufacturing security rests on Zero Trust principles: see everything, connect only what the business needs, and be prepared to contain the breach. Illumio answers manufacturing pressures with six main capabilities that cut risk and maintain operations.

See every connection in real time across IT and OT

Illumio maps how devices, apps, workloads, controllers, and business systems actually talk to each other in real time. Rather than trusting a diagram drawn years ago, you can see live traffic flows and the real dependencies behind them. That map is the basis for sound risk decisions and better planning.

Paired with tools such as Armis and Claroty, Illumio extends that view to unmanaged, legacy, and niche OT devices that standard tools tend to miss.

Find and rank risk

Once your traffic is visible, Illumio flags high-risk pathways, needless access, and systems that carry real exposure. Flow data combined with business context allows you to fix what matters most, rather than working down a long list of technical flaws.

Reduce risk exposure

Many breaches work because systems leave ports and services open that nobody uses. Illumio shrinks the attack surface by finding weak links, cutting needless access, walling off obsolete devices, and limiting inbound traffic. This is particularly valuable for legacy OT systems that can't be patched or upgraded.

Enforce secure connectivity with microsegmentation

Microsegmentation sits at the core of the Illumio approach. Instead of letting a whole trust zone talk freely, Illumio grants secure connectivity, so each system reaches only the

services and devices it needs. A PLC can talk to its control system, and the rest is blocked by default.

This lines up with the segmentation rules in IEC 62443 and leaves attackers far less room to spread through the environment.

Contain the breach

Illumio takes the view that breaches are inevitable but disasters are optional. When an attacker lands on a workstation, engineering system, or vendor connection, microsegmentation policy limits where they can go next. That shrinks the blast radius of an attack and keeps one incident from spreading across the plant.

Respond and isolate threats faster

With Illumio, you can build and test isolation plans well before an incident happens. During a breach, you can restrict traffic, ringfence key assets, and contain the threat without shutting down the whole system. Production keeps moving while your team responds to the breach.

Modernizing manufacturing security without the risk

Manufacturers face a tough mix: IT and OT growing together, ageing systems, ransomware, thin visibility, and almost no room for downtime. Illumio meets those pressures with a Zero Trust approach built on real-time visibility and breach containment, so an attack that gets in has nowhere to go. Every new connection that a plant adds shrinks your window to act. Plants that put containment in place before the breach are the ones that keep running.

Learn how Illumio keeps manufacturers running.

illumio.com/solutions/manufacturing

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.

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.