Illumio + Armis from ServiceNow: Protect Critical Infrastructure

Secure converged IT and operational technology (OT) systems against disruption and downtime.

Ransomware that starts on one office laptop can end with a stalled production line or a hospital diverting ambulances. Attackers no longer stop at the IT network. They use it to reach the machines, medical devices, and control systems your business runs on. Together, Armis from ServiceNow and Illumio find every connected device, map how it communicates, and block the paths an attacker would use to reach operations.

Connected operations, connected risk

Factories, hospitals, utilities, and public services now connect operational technology to IT and cloud systems. The air gaps that once protected industrial equipment are gone. Ransomware can move laterally from system to system and cross freely between IT and OT.

Much of that equipment was built for uptime, with little thought for security. It runs around the clock and can only be changed in short maintenance windows. Frontier AI now helps attackers find and exploit weaknesses faster than teams can patch them.

When attackers move faster than patches, the job is to keep a breach small. That takes two things: knowing every device on your network and controlling what each one can reach. Armis from ServiceNow delivers the first. Illumio delivers the second.

40%

of connected assets are invisible to tools built for the IT perimeter.[1]

58%

of companies hit by ransomware had to shut down operations.[2]

From asset visibility to breach containment

Armis from ServiceNow discovers and classifies every connected asset, managed or unmanaged. That includes legacy controllers, Internet of Things (IoT) devices, and medical devices. For each one, Armis adds context on its role, behavior, and risk.

[1] ServiceNow, *Blueprint for Autonomous Security*, 2026.

[2] Ponemon Institute for Illumio, *The Global Cost of Ransomware Study*, 2025.



Illumio maps how those assets and your applications communicate. It shows where an attacker could move laterally, then helps you build segmentation policies that allow only the traffic operations need. That cuts exposure before an attack and contains a compromised device during one.

Armis from ServiceNow provides the asset context. Illumio provides the map and the policy enforcement.

How the joint solution works

Teams move from visibility to containment in seven steps:

1. **Discover.** Armis from ServiceNow identifies every connected device and its attributes.
2. **Map.** Illumio pairs that context with traffic data and maps IT, cloud, and OT flows in one view.
3. **Identify risk with context.** Device risk, vulnerability data, and asset criticality show what to fix first.
4. **Reduce exposure.** Teams close unused paths and risky services after Illumio tests each change on live traffic.
5. **Standardize policy.** Teams write rules in business terms, like site, zone, and device role, instead of IP addresses. The same rules then work across every site.
6. **Harden the IT/OT boundary.** Only approved communications cross between IT and OT, without re-engineering the network.
7. **Prepare to isolate.** If a device is flagged as high risk, a pre-approved containment policy limits its reach. The rest of the operation keeps running.

What this means for your business

Together, Armis from ServiceNow and Illumio help you:

Limit operational downtime

Isolate critical production systems from non-essential traffic so an intrusion in one area doesn't halt a line, a plant, or a hospital wing.

Protect the people who depend on you

Keep the power on, the water clean, patients cared for, and public services running by containing threats before they reach safety-critical systems.

Fix the riskiest gaps first

Use asset context and real traffic data to find the exposures that matter most. Then close them with policy tested against how operations actually run.

Where customers put it to work

Industry	Outcome
Manufacturing	Keep production lines running and limit vendors to the systems they maintain.
Healthcare	Separate medical devices from administrative networks so patient care continues.
Energy and utilities	Isolate operational zones across plants and substations to prevent cascading outages.
Government	Keep public infrastructure separate from general-purpose networks.

Connected to the ServiceNow workflows you already run

The joint solution fits the way your teams already work in ServiceNow:

- **Business context in.** Illumio uses data from the ServiceNow Configuration Management Database (CMDB) to keep workloads and labels current, so policy reflects how the business describes its own systems.
- **Accountable action out.** Illumio creates and tracks tickets in ServiceNow IT Service Management (ITSM), so containment actions are recorded in the system your teams use for change and incident management.

Support for key regulatory standards

Segmentation between zones, plus a record of which communications are allowed, supports programs aligned to NERC CIP, IEC 62443, and NIST SP 800-82. It also helps protect patient data under HIPAA.

See the joint solution in action

The next attack may still start on an office laptop. With Armis from ServiceNow and Illumio, it doesn't have to end on the plant floor or in the ER.

Ask your Illumio or ServiceNow representative for a demo, or learn more at:

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. 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.