Illumio + ServiceNow Shift Zero

Contain what autonomous security finds at machine speed and under full governance.

AI gives attackers machine-speed tools, and AI agents inside the enterprise often carry more access than anyone has reviewed.

ServiceNow's Shift Zero operating model answers with governed, autonomous security that moves from remediation to prevention at machine speed. Illumio limits how far a threat can move once it's inside, so every breach Shift Zero detects stays small, contained, and governed.

Why Illumio + Shift Zero

Shift Zero gives you a live view of every asset, identity, and AI agent, along with the approvals that keep autonomous action safe. Illumio sees every connection between them and controls which ones are allowed.

Under Shift Zero, closing off one step on an attack path is enough to stop an exploit. Illumio does that by blocking risky connections before an attack and containing breaches in seconds after one lands, so attackers and rogue agents have no easy path to your critical assets.

With Illumio and Shift Zero working together, teams can:

- **Find and close attack paths.** Illumio Insights flags the paths that lead to your most critical systems, and Illumio Segmentation blocks the connections no workload needs.
- **Contain breaches the moment they're flagged.** When Shift Zero detects an incident, Illumio quarantines the affected system without taking the business offline.
- **Protect IT, OT, and IoT with one policy model.** Shift Zero shares device context with Illumio, so OT and IoT devices get the same containment as your data center and cloud.
- **Prove control to auditors and the board.** Shift Zero logs who approved each policy change or quarantine and when.

Key benefits

See the attack paths that matter

Illumio Insights maps how workloads connect across hybrid IT, cloud, OT, and IoT. Teams can see what puts critical systems at risk.

Contain threats at AI speed

Illumio Segmentation quarantines breached resources at machine speed, so a breached workload or rogue AI agent can't spread.

Keep every action governed

Shift Zero carries each containment request through approved workflows, with status and proof your teams can trust.

Act with full business context

Shift Zero adds asset and business context to Illumio maps, so you protect your most critical systems first.

How it works

Shift Zero runs in four stages: sense, decide, act, and govern. Illumio adds a map of every connection and the controls to stop a threat from spreading at each stage.

- **Sense.** Illumio Insights watches live workload traffic and flags lateral movement risk. Shift Zero adds real-time intelligence on every asset across IT, OT, and IoT, including its owner and business impact.

- **Decide.** Shift Zero scores each risk by exposure and business impact. Illumio shows which connections a threat could use, so teams know which paths to close and which systems to contain.
- **Act.** Illumio Segmentation applies policy, ring-fencing, or quarantine to cut off the paths a threat would use to spread.
- **Govern.** Shift Zero logs every policy change and quarantine with a full audit trail, so every team can see the approvals, status, and proof.

Containment in action

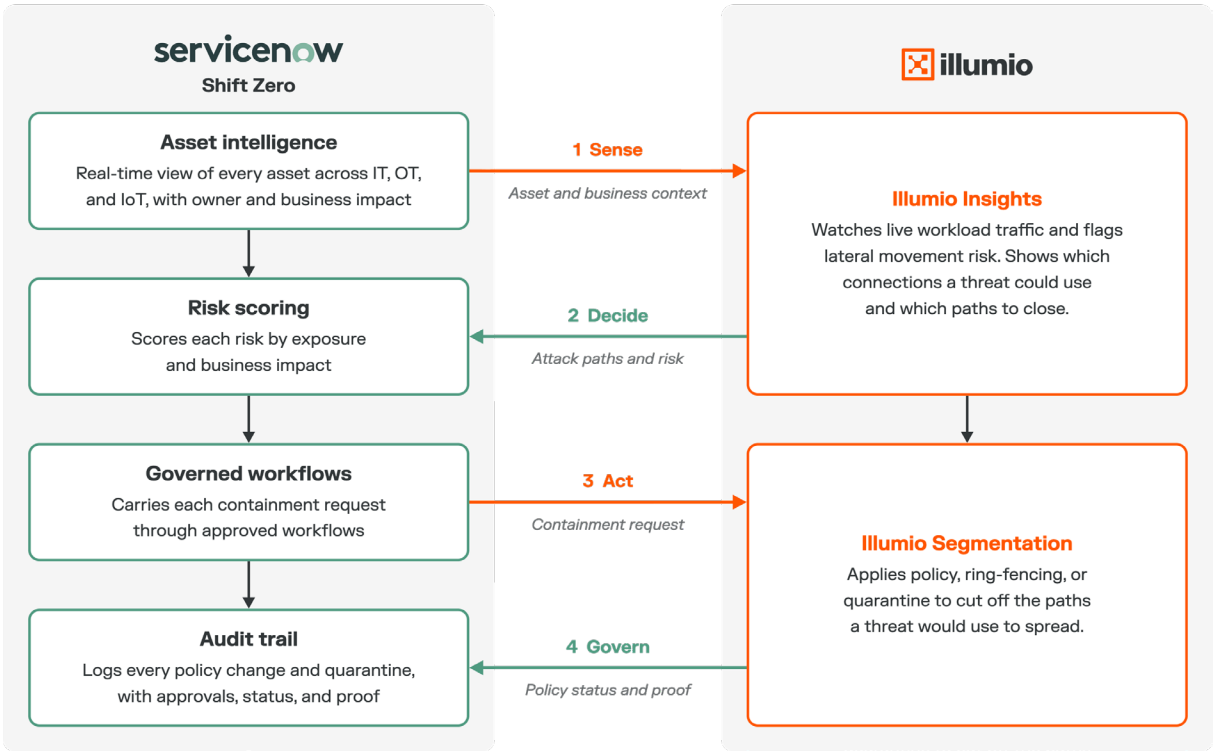
AI agents often run on service accounts with broad access, so a compromised or misconfigured agent can reach sensitive data fast.

When an agent starts reaching for systems it has never touched, such as a database of customer payment records, Illumio and Shift Zero respond in four steps:

1. Illumio Insights spots the new connections and flags them as lateral movement risk.
2. Shift Zero confirms the database supports a revenue-critical service and maps what the agent's identity can reach, so the alert jumps to the top of the queue.
3. Illumio Segmentation ringfences the database and quarantines the agent's host in seconds, and the rest of the business keeps running.
4. Shift Zero logs the approval, the action, and the outcome, so the security team can show exactly what happened and why.

Get started today

Contact your Illumio or ServiceNow account team to learn more.



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.