

The Illumio Breach Containment Platform

Detect, assess, and stop lateral movement across your hybrid environment with a single platform.

What happens after the breach matters most

Today's breaches are defined by what happens after attackers get in. Once they're past the perimeter, modern threats move laterally to compromise sensitive systems. This internal movement — not the initial entry — is what drives operational disruption and catastrophic damage.

Modern environments make this easier. Hybrid and multi-cloud architectures, virtual workloads, IT/OT convergence, and third-party access all increase internal connectivity. Each connection creates another path for attackers to move.

Many security teams lack clear visibility into this internal activity. They can't easily see traffic flows, system relationships, or where risk concentrates after a breach.

Without this insight, teams struggle to understand exposure across their environment.

At the same time, breach containment has become a business priority. Attackers move faster than teams can respond, and automation increases both speed and impact. Third-party access adds ongoing internal risk that perimeter defenses can't control.

Executives and regulators now expect proof of security effectiveness. Teams must show how controls reduce the blast radius, support compliance, and protect critical operations.

Yet, security teams are stretched thin and must respond quickly with minimal disruption.

Perimeter-based and detection-only tools fall short once attackers are inside. Organizations need breach containment: continuous visibility and the ability to act before, during, and after a breach.

The Illumio Platform

Illumio Insights

Get real-time visibility into internal traffic and lateral movement across hybrid and multi-cloud environments, helping teams understand how a breach is unfolding.

Illumio Segmentation

Enforce Zero Trust controls that stop lateral movement and contain breaches by limiting access across workloads, applications, and environments.

Contain breaches with Illumio

Illumio Insights and Illumio Segmentation form a single breach containment platform. Together, they help teams detect and stop lateral movement across hybrid multi-cloud environments.

Illumio Insights provides continuous visibility into internal traffic. See workload connections, dependencies, and abnormal behavior. Identify risk and prioritize action without assumptions or disconnected tools. Reduce the blast radius, respond faster, and report clear, board-ready metrics.

Illumio Segmentation turns insight into action. One-click, policy-based controls isolate compromised workloads without network changes or disruption.

Illumio capabilities and benefits

- **Fast, simple deployment.** Illumio deploys quickly without disrupting operations. It is OS- and infrastructure-agnostic and uses lightweight agents. There are no firewall rewrites, VLAN changes, or routing updates.
- **Asset inventory and topology views.** Teams can immediately see all assets across environments from a single interface. Illumio identifies assets using clear, natural-language labels that adapt to custom needs.
- **Real-time visibility.** Illumio automatically maps traffic flows and workload communications across hybrid cloud environments. Teams can clearly see lateral movement paths and risky connections, eliminating blind spots.
- **AI-powered, risk-based prioritization.** Illumio analyzes abnormal and malicious behavior and shows where lateral movement would have the greatest impact. It highlights high-risk assets and recommends where to apply containment first, helping teams focus effort where it matters most.
- **Least-privilege policies.** Zero Trust-based segmentation policies isolate critical assets from lateral movement. This reduces the blast radius in a clear, provable way without downtime or network changes.
- **Phased enforcement modes.** Teams can move from visibility-only mode to full enforcement over time. This allows teams to test and validate policies before turning them on.
- **Dynamic quarantine.** Suspicious or compromised workloads can be isolated instantly. One-click containment stops lateral movement without disrupting network operations.
- **Proof of value with reporting and metrics.** Visual reports show blocked paths and reduced exposure. These metrics help teams measure blast radius reduction and clearly show risk reduction to leadership.

- **Continuous monitoring and response.** AI continuously monitors network activity to detect lateral movement, malicious IPs, and data exfiltration attempts. Automated response helps stop threats before they spread.
- **Scalable hybrid and multi-cloud support.** The platform scales easily across hybrid multi-cloud environments, supporting growth without added complexity.

How Illumio delivers value

Map assets and gain visibility

Get continuous insight into internal traffic, risky connections, open ports, and abnormal behavior. Reduce unknown risk and improve breach readiness.

Protect critical assets

Identify and protect systems essential to business operations. Isolate incidents fast to reduce blast radius and limit disruption.

Prove audit and compliance readiness

Apply policy-based segmentation aligned to regulatory requirements with provable enforcement. Support audit readiness and clear reporting to leadership and regulators.

Secure cloud environments

Get visibility and segmentation for cloud applications across AWS, Microsoft Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI). Contain breaches and ransomware. Strengthen resilience across hybrid environments.

The only platform built for breach containment

illumio.com/illumio-platform

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.

