Illumio Segmentation for Cloud

Integrated visibility and breach containment for hybrid, multi-cloud applications and workloads.

Architectural overview

Public cloud environments today are dynamic, complex, and — without the right controls — completely open to lateral movement risk.

Organizations operating in hybrid, multi-cloud environments today face a critical challenge: understanding how data center workloads connect to cloud workloads, how cloud workloads communicate with each other across different public clouds, and where real lateral-movement risk exists.

Illumio starts your journey to breach containment with lateral movement visibility and risk insights across your entire hybrid and multi-cloud environment.

Complete visibility and control across data centers and public clouds

Illumio gives you one consistent view of application communication and risk across your entire hybrid, multi-cloud environment. You get workload-level communication mapping and risk insights that cloud-native tools simply can't deliver across environments.

Before you change a single rule, Illumio shows you where risk actually lives and which controls matter most. See real traffic against intended policy. Identify over-permissive rules. Find unused or redundant access. Understand your true lateral movement exposure.

As you move workloads to the cloud, Illumio keeps security visibility intact. You get continuous visibility before, during, and after migration — with no new blind spots introduced by cloud adoption.

Cloud resilience at scale

Map your environment

Gather contextual insights with an interactive map of application deployments, resources, traffic flows, and metadata.

Gain risk and policy insights

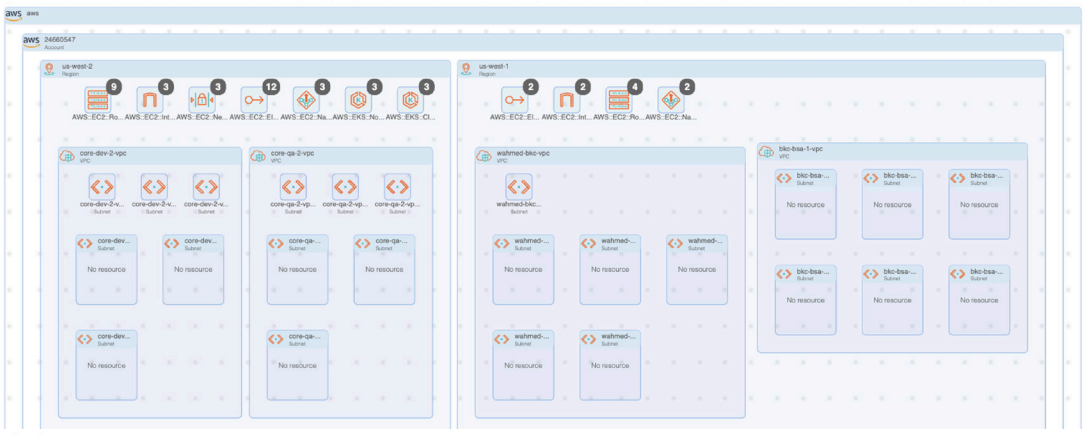
Visualize actual traffic versus intended policy. Identify lateral movement paths and exposure.

Proactively segment workloads

Create and deploy controls using labels and IP lists to build trusted communications between applications.

Orchestrate cloud rules

Create new rules that coexist with existing cloud native security groups. Improve rule management workflows in dynamic, constantly changing environments.



Technical capabilities

Understand the entire attack surface

Visualize traffic flows using context-based labels and metadata (labels and tags). See cloud, endpoints, and on-premises data center workload and application traffic flows in one view.

Act on these insights to build Zero Trust policies across public cloud environments, including physical and virtual servers, containers, and serverless clouds.

Illumio Segmentation for Cloud uses existing native tools to collect object metadata and real-time application, data, and workload traffic telemetry in AWS, Microsoft Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI). Use this information to build a map of application behavior.

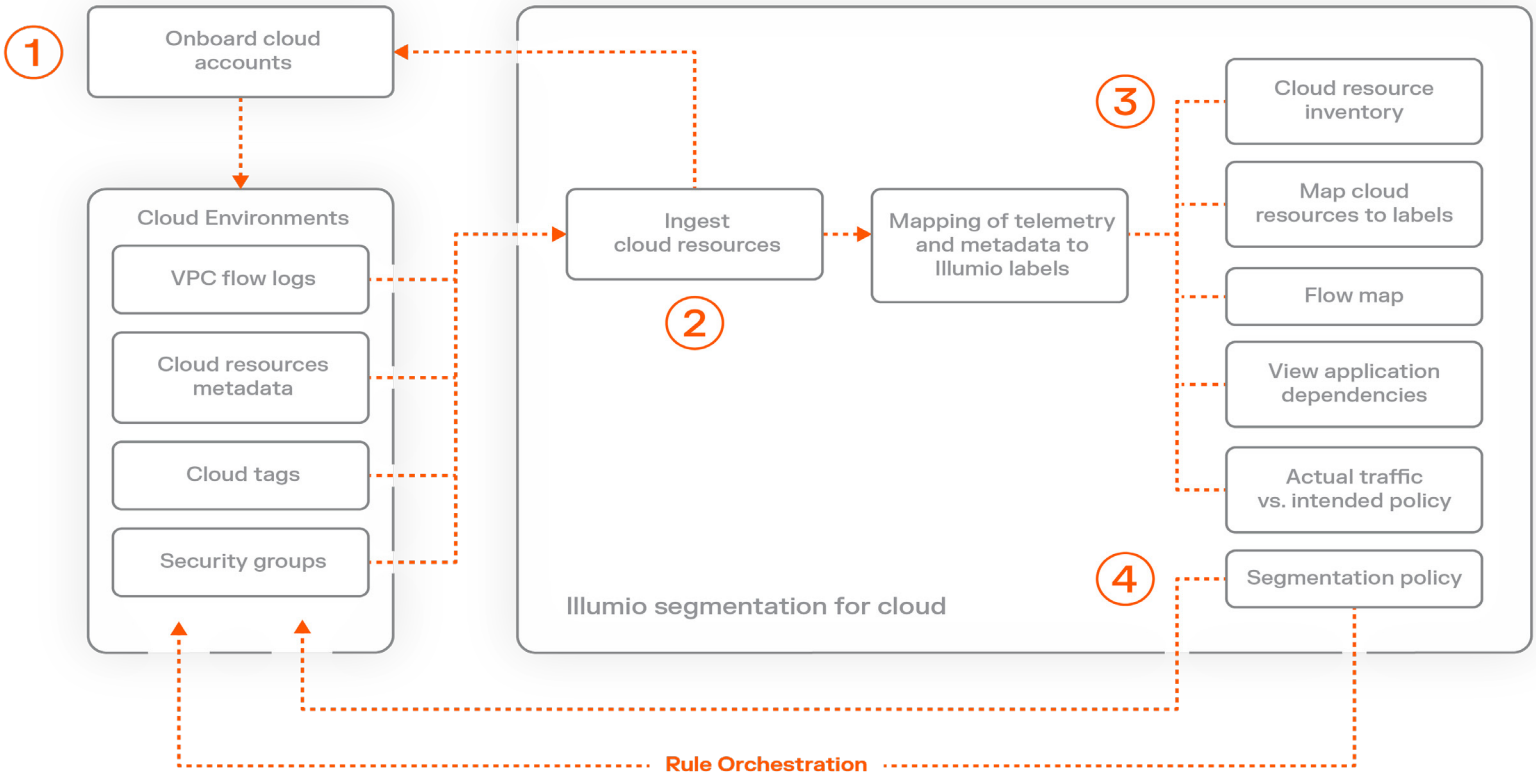
Contain breaches and ransomware

Adopt segmentation policies at scale that coexist with native cloud controls like AWS security groups (SGs) and Azure Network security groups (NSGs).

Analyze real-time communication patterns as interactions change based on context such as tags, traffic, and logs.

Make faster, better-informed decisions about cloud security

Using insights from the Illumio map, quickly diagnose issues to manage and maintain controls. Maintain consistent security across diverse cloud services.



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.