illumio

PRODUCT BRIEF

Illumio Segmentation for Cloud

Breach containment for public cloud applications and workloads

Architectural overview

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

Illumio Segmentation for Cloud turns your cloud from a single, flat environment into a resilient one, where breaches are contained the moment they happen.

With Segmentation for Cloud, you get a real-time map of application and workload connections across your entire hybrid environment. Showing detailed information in plain language, you gain insights into how cloud resources are communicating. See vulnerabilities, prioritize response, and minimize the fallout from inevitable breaches.

Create and manage label-based segmentation policies using AWS security groups (SGs) and Azure network security groups (NSGs). These ensure that only allowed traffic can move within and between cloud workloads.

Segmentation for Cloud helps your team work more efficiently and supports shift-left security during development.

Cloud resilience at scale

Map your environment

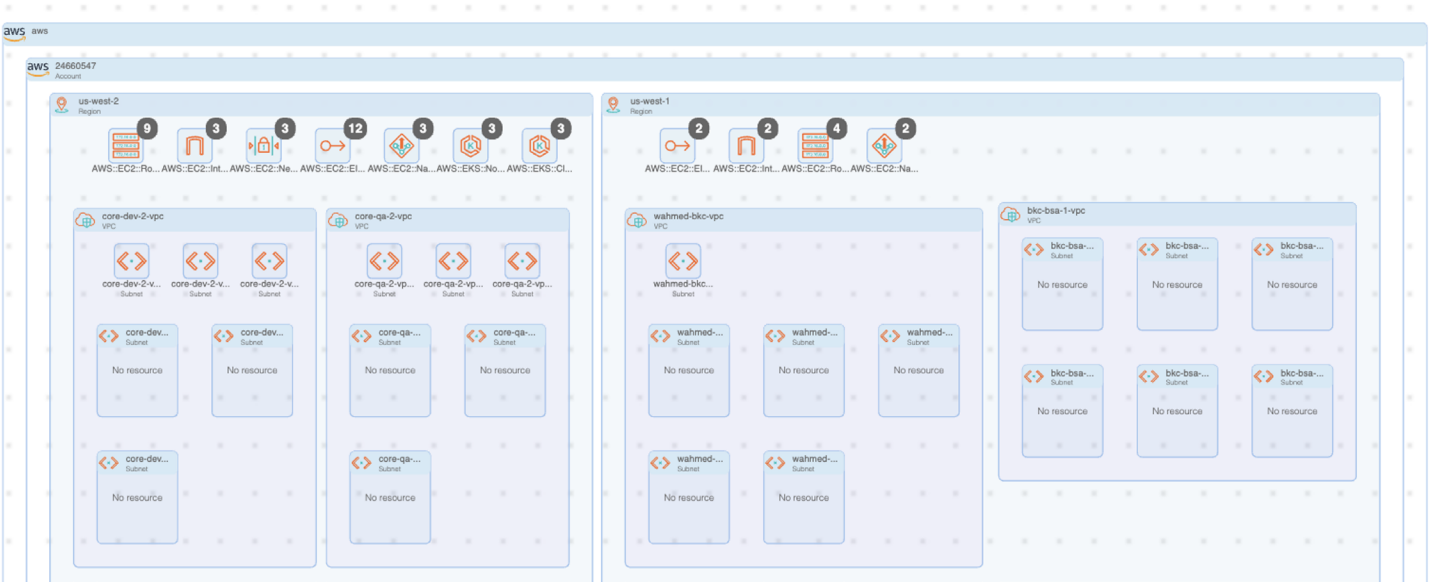
Gather contextual insights with an interactive map of application deployments, resources, traffic flows, and metadata.

Proactively segment workloads

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

Contain attacks

Adapt segmentation policies 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

Build segmentation policies at scale with native cloud controls like AWS SGs and Azure NSGs.

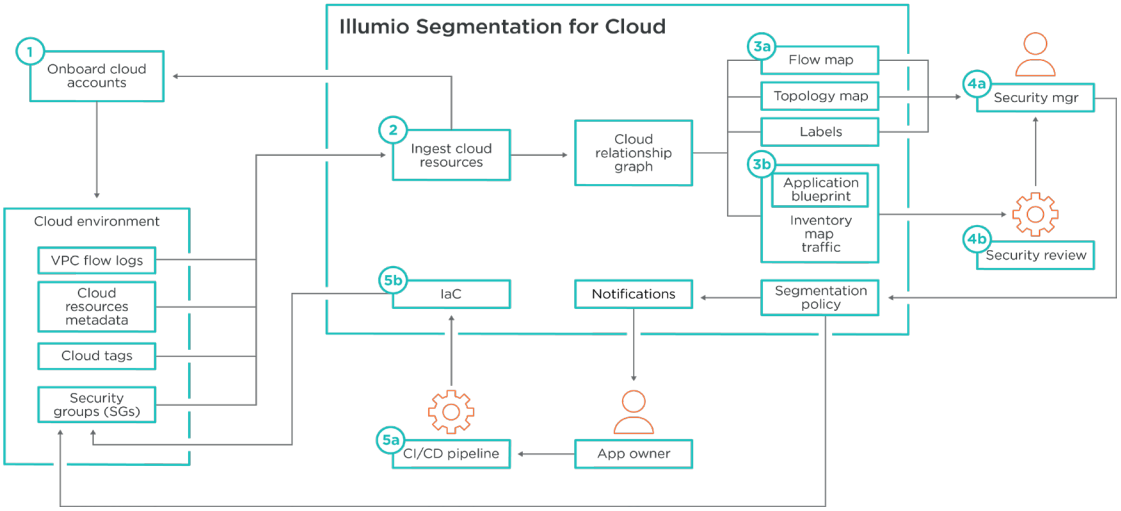
Analyze real-time communication patterns to automatically adapt policies as interactions change based on context such as tags, traffic, and logs.

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.

Support shift-left security efforts to guarantee application security at the earliest stages in the development lifecycle.

Illumio Segmentation for Cloud workflow



1: Bring AWS, Azure, GCP, OCI account information into Illumio

2: Ingest cloud resources

3a: Build visual maps for infrastructure and traffic data

3b: Create and view application blueprint

4a/b: Review application definition and policies

5a: Update CI/CD pipeline

5b: Use DevOps CI/CD process to apply policies

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.