illumio

TECHNICAL BRIEF

Illumio CloudSecure

Segmentation for public cloud applications and workloads

Architectural overview

Illumio CloudSecure protects your public cloud with the right segmentation policies, minimizing the impact of breaches and ransomware attacks that can result in theft, halted operations, and loss of trust.

Illumio CloudSecure delivers a real-time map of application and workload connections across the entire hybrid attack surface combined with detailed information in plain language about these resources.

This information provides insights into how cloud resources are communicating to help teams see vulnerabilities, prioritize response, and minimize the impact of inevitable breaches.

Teams can create and manage label-based segmentation policies with the ability to implement label-based policy using AWS Security Groups (SGs) and Azure NSGs. This ensures the right Zero Trust Segmentation policies get implemented to allow only authorized traffic within and between workloads in the cloud.

Illumio CloudSecure can increase your team's efficiency and aid in efforts to shift-left security during development.

Innovation at a glance

Visualize cloud workload connectivity

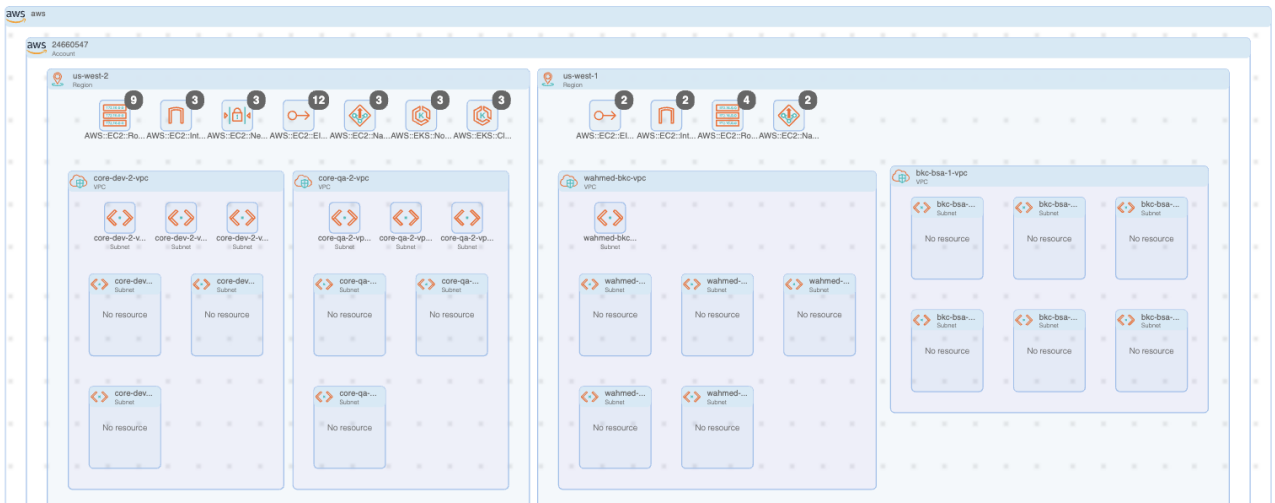
Gather insights with an interactive map of application deployments, resources, traffic flows, and metadata.

Apply proactive segmentation controls

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

Contain cloud attacks

Adapt segmentation policies in dynamic, constantly changing environments.



Technical capabilities

See and understand the entire attack surface

- See traffic flows using context-based labels and metadata (labels and tags) to visualize cloud, endpoints, and on-premises data center workload and application traffic flows in one view. Use these insights to build Zero Trust policies across public cloud environments, including physical and virtual servers, containers, and serverless clouds.
- Illumio CloudSecure uses existing native tools to collect object meta-data and real-time app, data, and workload traffic telemetry in AWS and Microsoft Azure to build a map of application behavior. Use this information to prioritize and implement the right policies to secure your applications.

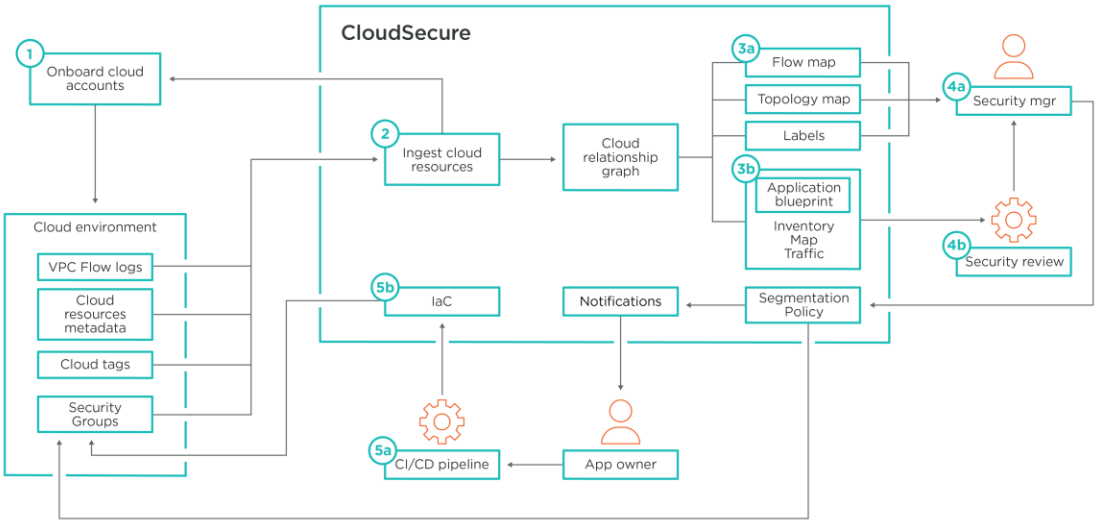
Contain breaches and ransomware in the cloud

- Implement segmentation policies at scale with native cloud controls like AWS Security Groups (AWS SGs) and Azure Network Security Groups (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 Illumio's map, quickly diagnose issues to manage and maintain controls, preserving consistent security across diverse cloud services.
- Support shift-left efforts to guarantee application security at the earliest stages in the development lifecycle.

Illumio CloudSecure Workflow



1: Bring AWS and/or Azure 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, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.