illumio

PRODUCT BRIEF

Illumio CloudSecure

Segmentation for public cloud applications and workloads

Cloud security is unique

The volume and speed of applications and workloads moving to the cloud continues to grow — and so do their security challenges. In fact, 94 percent of IT security leaders say that connectivity between their cloud services and other environments increases the likelihood of a breach.

When it comes to fast-changing cloud environments, security teams are dealing with several challenges:

- **Despite prevention, breaches still elude detection:** If attackers bypass preventative measures and compromise sanctioned applications and systems, they can easily and quietly move through other approved channels.
- **Prioritizing breach containment in the cloud is more complex:** Constantly changing cloud environments in which applications spin up and down — and may only be used for a few hours — can escape security focus.
- **Lateral movement is easier in the cloud:** Hybrid and multi-cloud environments, decentralized application deployment, and workload proliferation can make it easier for attackers to move through the network.

Contain breaches in the cloud

Illumio CloudSecure extends Zero Trust Segmentation (ZTS) to your cloud applications and workloads.

Forrester research found that Illumio ZTS reduces the impact, or blast radius, of a breach by 66 percent. It helps prevent unauthorized movement within a cloud infrastructure without placing additional stress on SecOps teams, providing a 90 percent decrease in operational effort.

Key benefits to contain cloud attacks

Visualize cloud workload connectivity

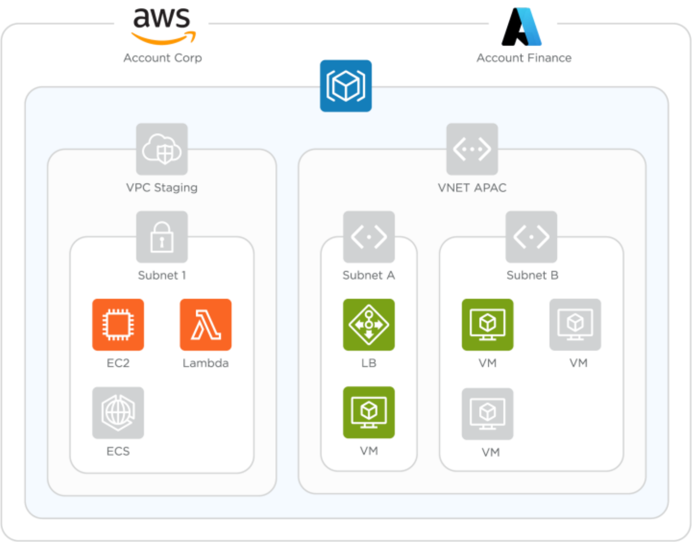
Gather insights using an interactive map of application deployments, resources, traffic flows, and metadata.

Proactively apply segmentation controls

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.



Critical capabilities

A unified view of the cloud

Illumio CloudSecure provides comprehensive mapping of traffic telemetry across multi-cloud environments into applications, data, and cloud workloads — all without an agent. Get a full understanding of application and workload connectivity along with context-based labels and object metadata.

This visualization allows security teams to uncover unnecessary connectivity that increase risk. It also categorizes test and production workloads, providing insight to create and edit the right policies and controls.

With Illumio CloudSecure, you can easily know if you're at risk of an attack or currently under attack at any moment.

Fast, better-informed decision-making

Illumio CloudSecure identifies unnecessary traffic between applications and workloads across multi-cloud environments. Detailed context-based label descriptions of objects guides teams as they create policies, based on applications' components and relationships. Teams can make faster, more informed decisions about what traffic to segment to proactively maintain a strong security posture or reactively isolate a breach.

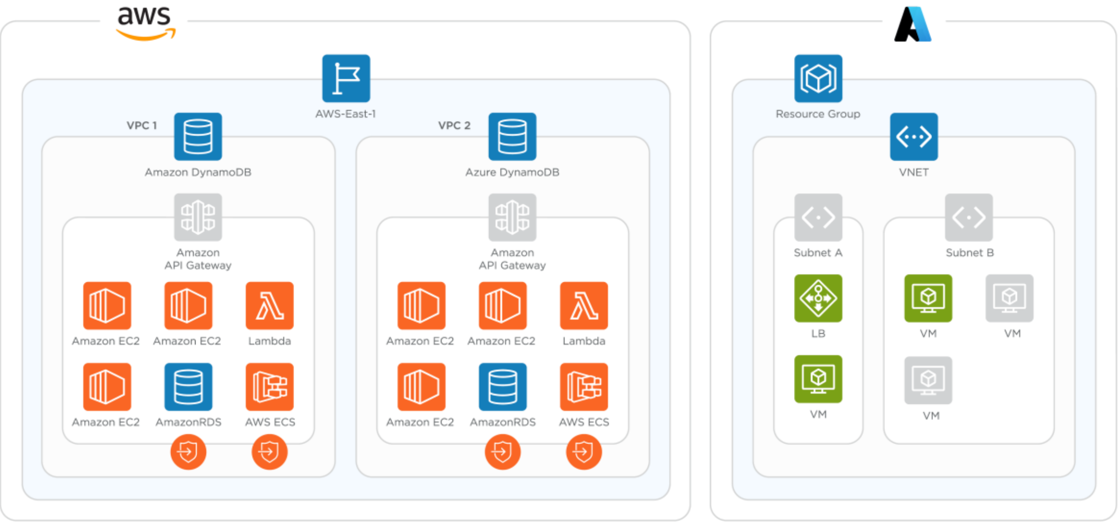
Contain the blast radius

When a breach happens, it must be stopped and contained as quickly as possible. With Illumio CloudSecure, you can implement Zero Trust Segmentation in cloud environments to proactively prepare for breaches or reactively contain them.

During a breach, quickly visualize connectivity between applications and workloads alongside detailed resource descriptions. Get insight into the connectivity between cloud applications and resources allowing attackers to move through the network. Adjust controls to stop lateral movement, contain the attack, protect applications, and limit the blast radius.

To proactively prepare for breaches, Illumio CloudSecure helps teams plan and optimize security rules to reduce the attack surface and secure programs using native controls.

Try Illumio CloudSecure free for 30 days
Start now at illumio.com/clousecure-free-trial



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.