illumio

SOLUTION BRIEF

Secure Cloud Workload Migration With Illumio

Illumio ensures consistent segmentation as workloads migrate from the data center to the cloud

New cloud services, new security mindset

Rapid digital transformation has forced many organizations to quickly adopt public cloud platforms and cloud-native services. But in the rush to migrate to the cloud, cloud security is often put off or left behind completely. This leaves critical data and resources exposed to new cloud-based cyberthreats.

And as organizations accelerate to adopt more cloud services, their ability to truly understand network interactions, access, and security becomes more complex. Without consistent visibility, cloud consumers not only have little insight into how their services are communicating but also which of them are relevant — and without this understanding, securing services becomes a nearly impossible task.

> "Illumio enables us to rapidly migrate virtual machines from data centers into our cloud environment while maintaining security controls based on least privilege."
>
> **– Mike Laak**
> Senior Infrastructure Engineer
> West Bend Mutual Insurance

Don't assume the cloud is secure by default

With cloud vendors offering built-in security tools, it's easy to assume that securing your cloud workloads falls under the vendor's responsibility.

But this isn't accurate: Vendors make a best-effort to secure the underlying cloud fabric, but the responsibility for securing workloads lies in the hands of the customer. The cloud vendor will not secure your workloads for you.

This is complicated by the fact that one vendor's security won't necessarily integrate with another vendor's security, and security tools in the data center aren't integrated with any cloud vendors by default.

As workloads are migrated to the cloud, the result is often a siloed security architecture – and silos are a roadblock when creating a scalable Zero Trust security solution.

The cloud requires breach containment

Breaches are inevitable – even in the cloud. And while prevention and detection tools are still necessary, they will never be perfect.

Illumio Zero Trust Segmentation (ZTS) fills this gap by providing breach containment in the cloud. Illumio offers real-time visibility to see and secure network exposure, automates security policy at the workload regardless of the underlying environment, and applies orchestrated, consistent security across your hybrid and multi-cloud environments.

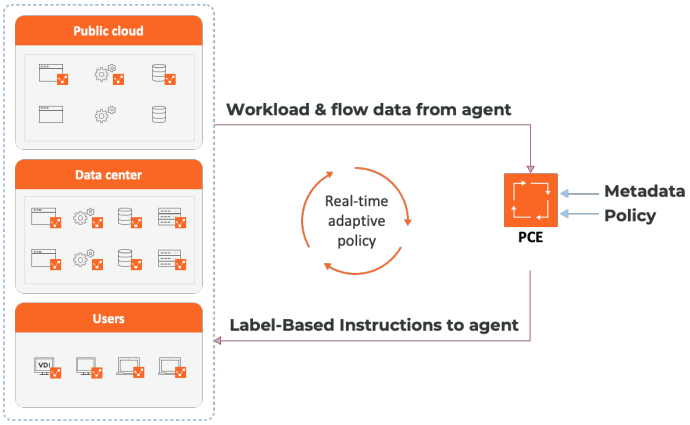
Breaches will happen – but Illumio ZTS will stop them from spreading, no matter if they enter the data center, AWS, or Azure. Illumio ensure the first resource that's breached is the only one, allowing operations to continue despite a breach.

Illumio Core for the cloud

Illumio Core enables trust boundaries directly at every workload at any scale using the Illumio VEN, a software agent deployed in the management plane of a workload.

The agent-managed workload can be deployed in either a cloud or data center environment. The VEN agent collects application telemetry which Illumio uses to visualize traffic, and the VEN receives instructions from Illumio to define policy directly on the workload.

The VEN agent on cloud workloads enables Illumio to be decoupled from each cloud vendor's unique security solutions, ensuring consistent, secure cloud migration.



Decoupling workload security from the underlying cloud environment ensures a consistent security architecture across multiple clouds and data centers, creating a single security model across all hosting environments. This frees up cloud security tools to address network-centric challenges, such as enforcing policies on traffic between VPCs in AWS using transit gateways. These are very different security challenges than those facing workload security.

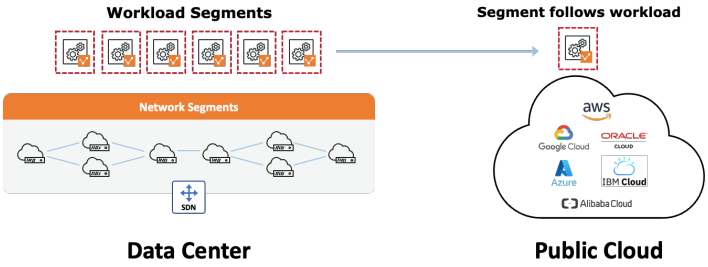
Illumio enables cloud and workload security challenges to be addressed without dependencies on the other.

Hybrid cloud security

Segmentation solutions exist for both the data center and cloud, but they're usually specific to each environment. This becomes an issue if a workload migrates from a data center to a cloud environment.

The data center segmentation solution will usually be left behind, and the cloud segment will need to be applied to that migrated workload. Typically, this isn't an automated workflow.

Illumio provides workload segmentation directly at the workload. This ensures segmentation policies follow the workload when it migrates from the data center to the cloud without depending on manually disconnecting from one and reconnecting to the other:



Illumio ZTS follows workloads wherever they migrate, enabling a single management plane for all segmentation across all hosting environments.

Learn more

Visit: illumio.com/solutions/cloud-workload-migration

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.