illumio

SOLUTION BRIEF

Environmental Separation With Illumio

Easily separate environments to stop breaches from spreading to critical assets

Traditional security methods aren't efficient in complex environments

When attackers can spread far and wide throughout a network, organizations can suffer significant damage. Trends like multi-cloud architectures, containerized applications, and serverless computing are the new standard, making proactive defense not just an option but a must-have.

The constraints of VLANs and traditional firewall-based segmentation are amplified by the requirements of today's hybrid networks. The complexity of ensuring separation between production and development environments, for instance, isn't just about using firewall rules — it's also about using context-aware segmentation that understands the nuances of application dependencies and data flows.

For security and network experts, the challenge is clear: How can you ensure that the principle of least privilege is adhered to within a constantly changing, multi-faceted environment?

Answering this question is imperative. According to Verizon's 2023 Data Breach Investigations Report, breaches in these kinds of complex environments are $1.44 million more expensive than those in simpler environments, totaling $5.28 million on average. And when events like mergers and acquisitions, compliance reviews, or cloud migrations are initiated, the risk of separating environments using traditional methods grows.

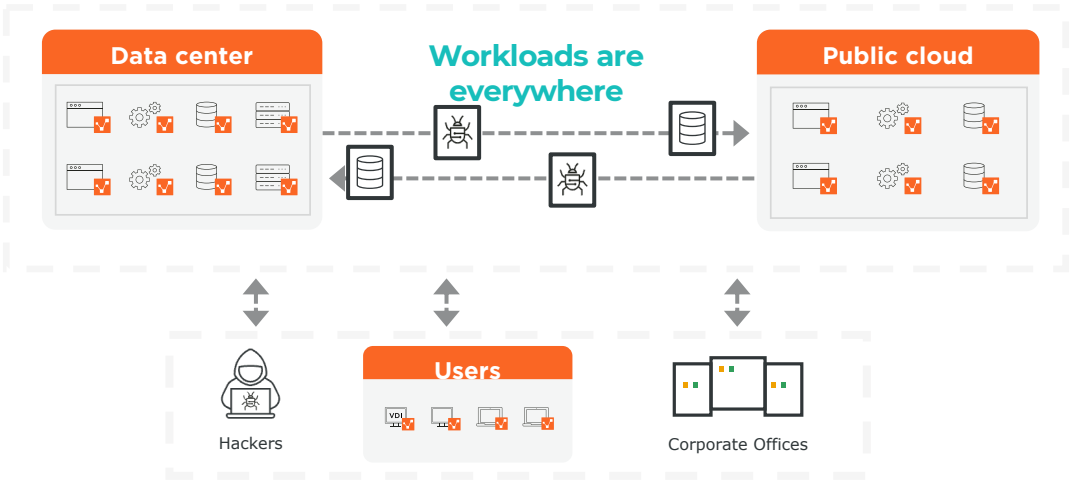
Precise environmental separation must go beyond drawing boundaries to include gaining visibility and building intelligent, adaptive, and context-aware barriers at scale.

> "Illumio gives us an invaluable holistic view of traffic across our data center and multi-cloud environments — with vastly more information than a collection of tools amounted to previously."
>
> **– Ryan Fried**
> Senior Security Engineer
> Brooks Running

Separate complex environments with Illumio

Illumio enables segmentation based on multidimensional labels enforced directly on the workload itself, providing control that isn't tied to the network. Illumio's application dependency map uses these labels to gather traffic flow data so that security teams can visualize all communication and traffic between workloads and devices.

Combining this visibility with firewall control allows environments to be separated based on characteristics such as location, application, role, compliance frameworks, and more. With a simple rule, development can't communicate with production assets, PCI data can't travel outside an application, and only allowed traffic can flow between different critical resources.



Seamless separation

Illumio is purpose-built to control traffic between diverse environments, ensuring that only approved traffic flows are allowed. Illumio combines visibility with control for seamless segmentation that doesn't impact the business.

Policies are dynamically applied to the native OS firewall on the workload itself. This ensures that as workloads are spun up, migrated, or decommissioned, the associated segmentation policies adjust automatically, eliminating stale configurations and maintaining an optimal security posture.

Smaller attack surface

Limiting the attack surface has never been more critical. Illumio helps prevent unauthorized traffic between environments, allowing seamless operations without exposing systems to the risk of lateral movement.

By thwarting accidental security gaps, Illumio meticulously controls communication between critical production systems and less secure development or test setups to seal potential breach points.

Ensure compliance

With Illumio, security teams can apply compliance labels on workloads with PCI or HIPAA requirements and enforce strict traffic limitations to and from these workloads no matter where they are or move to.

Use Illumio to ensure compliance during mergers and acquisitions by enabling granular introduction of a new environments so policies can be harmonized without the risk of data leakage.

Similarly, during divestments, Illumio can carve out distinct environments, guaranteeing data isolation and preventing the potential risk of sensitive information traversing between environments.

Learn more

Visit:
illumio.com/solutions/environmental-separation

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.