PRODUCT BRIEF

Illumio Core

Segmentation for on-premises and cloud data center workloads

The risk of a breach is accelerating

Assume breach is imperative

No one wants to be the next headline in the news. Stop breaches and ransomware from spreading across your cloud and data center workloads with Illumio Core.

Organizations are under constant pressure to keep business performance at optimum levels while managing a rapid pace of digitalization that increases IT complexity.

Workloads are everywhere. There is no longer a “traditional perimeter,” and organizations lack visibility into broadening attack surfaces, leaving them more vulnerable to targeted ransomware attacks.

A breach can be far more catastrophic, spreading before there is even an opportunity to identify or react to it.

To avoid becoming the next breach headline, many organizations are adopting Zero Trust security — focusing on strategies to reduce attack surfaces and mitigate exposure to rising threats.

Illumio Core delivers Zero Trust Segmentation (ZTS) across cloud and data center workloads to stop the spread of breaches inside your environments.

It provides real-time visibility into the connectivity between workloads across the hybrid attack surface, generates optimal segmentation policies based on observed traffic flows, and programs the policy quickly at the host level.

Illumio Core can uniquely segment at large scale without impacting network performance, allowing you to see rapid ROI.

Key benefits to stop the spread of breaches

See any workload

Traffic is visible across all workloads such as containers, IT/OT and virtual machines — within a single console.

Segment at any scale

Contain the spread of breaches by preventing lateral movement — regardless of architecture, size or complexity of your business.

Protect in minutes

An intuitive user interface provides a guided experience to track progress on ransomware resilience and easily deploy policy in minutes.

Realize a future without high-profile breaches

Zero Trust Segmentation is a critical control for preventing lateral movement.

It follows three core principles: assume breach, all entities are untrusted by default, and least-privilege access is enforced. By applying these principles, you contain and minimize the impact of breaches and ransomware.

Illumio Core ZTS has proven to be an effective way to stop ransomware from spreading — and critical to realizing a future without high-profile breaches.

Based on emulated attacks conducted by Bishop Fox, proactive Zero Trust Segmentation stopped a ransomware attack in 10 minutes, containing it at the first compromised host. By comparison, with detection-only capabilities, an advanced attacker could breach all hosts in 2.5 hours.

Critical capabilities

Eliminate traffic blind spots

Illumio Core provides unprecedented visibility into traffic across your cloud and on-premises data center workloads.

With a built-in application dependency map, you can visualize and organize workload traffic in an easy-to-understand way, making it easier for cross-functional teams to collaborate on segmentation policy design.

Gain an understanding of your level of risk by overlaying data from vulnerability scanning tools with the application dependency map to see where applications have unknown connections and are vulnerable. Use those key insights to prioritize and inform policy decisions.

> “Illumio Core enables us to roll out firewall changes much faster than before. Previously, it would be days or weeks. Now it’s minutes or hours.”
>
> **Nick Venn**
> **Global Collaboration and Cyber Infrastructure Manager**
> **QBE**

Protect at scale

Illumio Core is built to scale. Deploy across environments from hundreds to hundreds of thousands of workloads.

When emerging threats are identified, Illumio is built to respond. Proactively protect your organization by assessing the impact of new policies, then updating the applicable rules. These updates are immediately deployed to all impacted workloads.

Measurable risk reduction

User-friendly dashboards demonstrate measurable risk reduction with an auto-calculated protection score. With visibility into current ransomware risk, organizations can be proactive and take quick action.

Illumio Core suggests policies based on observed workload and protocol communications. With a few simple deny rules, you can quickly block the most common ransomware paths, realizing fast ROI and improving cyber resilience.

Effortless policy design

Easy-to-write policies allow you to safely and effectively build and operationalize your Zero Trust architecture.

Illumio Core’s allow-list approach does not require attention to rule ordering, making policy writing simpler to use and understand. Because traffic is denied by default, the Zero Trust Segmentation policies can be inherited by new workloads in your environment.

About Illumio

illumio

Illumio, the Zero Trust Segmentation Company, stops breaches 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.