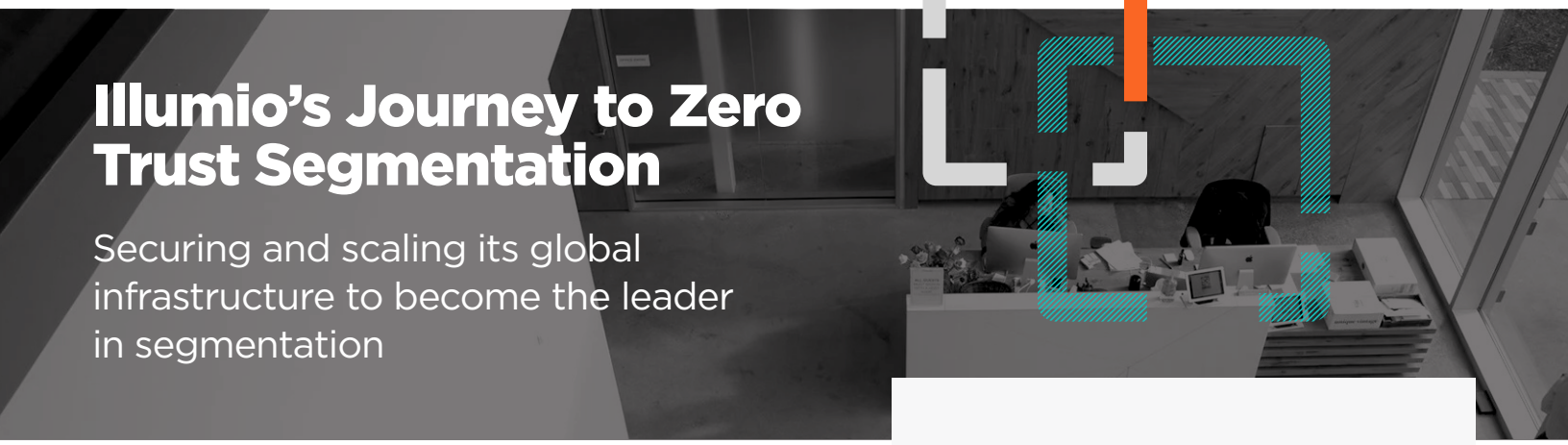
illumio

CUSTOMER STORY

Illumio's Journey to Zero Trust Segmentation

Securing and scaling its global infrastructure to become the leader in segmentation



Industry: Cloud, Network, and Endpoint Security

Challenge: Ensuring robust security, cyber and operational resilience, and regulatory compliance for an innovative, rapidly growing global cloud and network security company

Solution: Illumio Core, Illumio CloudSecure, Illumio Endpoint

Use cases: Asset Mapping & Visibility, Ransomware Containment, Critical Asset Protection, Cloud Workload Migration, Vulnerability Risk Reduction, Environmental Separation, Incident Response & Recovery

Location: Global

Business Goals

As the leader in Zero Trust Segmentation, Illumio is both an innovator and an implementer. Since 2010, Illumio's infrastructure, IT, and security teams have evolved and scaled along with its Zero Trust Segmentation platform — first by segmenting its crown jewels and critical assets, then its entire data center, endpoints, and cloud workloads.

Illumio is committed to realizing a world without high-profile breaches while helping its customers on their Zero Trust journey. At the same time, Illumio must meet stringent security requirements and manage a growing remote workforce and ever-increasing infrastructure.

Stephan Joe, Vice President of Information Technology at Illumio, and James Nelson, Vice President of Information Security at Illumio, and their teams who manage IT and security operations, know firsthand that Illumio needs visibility across its entire environment to identify and mitigate potential threats proactively. Joe and Nelson also know achieving cyber resilience requires Zero Trust with controls that limit risks and stop lateral movement.

Technology Challenges

As with any fast-growing company, Illumio must navigate a dynamic threat environment — whether it's ransomware or other cyber threats. Illumio doesn't just rely on perimeter-based security across its complex hybrid environment. Traditional perimeter-based defenses are insufficient against today's threats, which can bypass external defenses and exploit internal vulnerabilities.

As Illumio's remote workforce has grown, granular insights are essential to monitor and control remote traffic from anywhere in the world. And, without a single source of visibility across Illumio's complex hybrid environment, ensuring regulatory compliance, breach containment, and remediation of security incidents would be slowed — increasing the risk and impacts of a potential breach.

Relying on a single platform to see and control traffic helps meet the requirements of Illumio's growing hybrid infrastructure. "Usually, if there are rogue connections, they can be hard to identify," Joe said. "With Illumio, we can see what is connecting to our devices. Instead of piles of log files, we have a visual representation of where our traffic flows."

How Illumio Helped

Illumio's IT and security departments are very experienced in implementing Zero Trust throughout its complex environment. However, they don't have to hire senior network administrators; instead, teams focus on customers and innovation.

"With Illumio, you don't have to have resources with legacy firewall knowledge," Joe explained. "Our team has generalists versus senior-level infrastructure folks. Illumio requires some training, but it doesn't require certifications or years of experience to get us to a point where we are secure."

The Illumio team has widely deployed Illumio Core across its data center and managed workloads in the public cloud, establishing Zero Trust Segmentation policies that proactively restrict lateral movement and only allow traffic through authorized pathways. With Illumio Core, Illumio's team is confident that the organization's network paths are protected and that the SaaS clusters offered to customers are fully segmented and enforced at scale.

> We talk a lot about visibility into bad actors or internal threats, and how important it is to detect when something bad has happened. But it can be equally important to show that unauthorized access did not occur.
>
> James Nelson
> Vice President of Information Security
> **Illumio**

With the shift to hybrid work, Illumio Endpoint is indispensable for the Illumio team, restoring visibility that can be reduced by remote work. "With Illumio Endpoint, the time to value is super-fast. You can deploy the agents and get visibility right away," said Nelson.

Illumio's real-time application dependency map visualizes the connections between the on-premise servers and AWS and Azure clouds, revealing how Illumio's applications are communicating. The Illumio team can understand what needs protection and can take immediate action on blocking or authorizing workflows. This level of visibility, in addition to Illumio Core and Endpoint, enables precise policy enforcement.

The Illumio Platform with its Zero Trust controls is invaluable to the team. Combined with Illumio's SOAR integrations, the team can ingest logs using their standardized tooling and receive real-time alerts to security incidents. This enables quick containment action against any emerging threats.

"We talk a lot about visibility into bad actors or internal threats, and how important it is to detect when something bad has happened. But it can be equally important to show that unauthorized access did not occur," said Nelson.

Results & Benefits

- **Robust security:** Zero Trust Segmentation significantly reduced the internal and external threat surfaces.
- **Flexible controls:** With granular control of network activity, Illumio's IT team securely migrated to a new data center in just one week.
- **Compliance:** Illumio's controls simplified achieving and demonstrating compliance with regulations.
- **Incident response:** Incident management is now more efficient, enabling rapid containment of potential threats and minimizing disruptions to operations.
- **Deployed on AWS:** Illumio's SaaS offering is built on AWS, leveraging multiple services such as EC2, S3, EKS, and RDS — simplifying the customer implementation experience and improving performance.

About 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.