

Major Insurer Shrinks Hybrid Attack Surface by 99% With Illumio

Multinational insurer eliminates thousands of vulnerabilities and improves security for high-value applications with Zero Trust Segmentation

Business Goals

One of the largest general insurers in the market undoubtedly understands the importance of managing risk. The company offers business and personal insurance services to nearly 9 million customers.

Managing its own cyber risk is critical to its aim to make the world a safer place.

Insurance firms are ripe for cyberattacks, with a wealth of policyholder data and personally identifiable information (PII) at stake. Accordingly, the company's infrastructure and cloud services team has a definitive goal: stay out of high-profile breach news.

The insurer has a 160-year brand reputation to uphold, and 9 million reasons to invest in security capabilities that reduce cyber risk and enhance resilience to attacks.

Technology Challenge

While integral to its impressive growth, the company's mergers and acquisitions have expanded the insurer's hybrid attack surface. Despite due diligence processes, risk is inherent to M&A activity.

"In scanning our environments, we discovered the critical need to remediate unpatchable vulnerabilities from acquired systems — and at large," explains an Executive Manager of Infrastructure and Cloud Services for the firm. "Tighter security controls were vital to better protect our high-value applications and assets."



Industry: Insurance

Challenge: Mitigate risk from vulnerabilities and protect high-value business applications

Solution: [Illumio Core](#)

Use cases: High-value asset protection

Benefits:

- 99% reduction in exploitable vulnerabilities and attack paths
- Better understanding of connectivity and risk via real-time visibility
- Confidence that granular security controls will not break critical production applications



"Since implementing Illumio, we've taken 5,000 exploitable vulnerabilities down to 9 across seven high-value applications and hundreds of workloads. It has proven to be invaluable to our risk mitigation strategy."

Executive Manager of Infrastructure and Cloud Services
Large Insurance Company

The team sought microsegmentation to protect the application workloads underpinning the business and to limit exposure to vulnerabilities.

They had specific requirements for a safe, seamless approach that would not break applications or threaten uptime. That's where Illumio came in.

How Illumio Helped

The insurer turned to Illumio Core, which ticked all the boxes for "safe and seamless" in its proof of concept. Illumio's Zero Trust Segmentation has proven value in spades since deployment.

By tightly controlling traffic to business-critical applications, the insurer eliminated thousands of vulnerabilities and reduced its exploitable attack surface by 99 percent.

“

From the beginning, there was a sense that the Illumio team would do whatever it takes to support our team. Time and again, they've proven exceptional in their responsiveness, expertise, and partnership.”

Manager of Security Services
Large Insurance Company

“Since implementing Illumio, we've taken 5,000 exploitable vulnerabilities down to 9 across seven high-value applications and hundreds of workloads,” the executive manager says. “Illumio has proven to be invaluable to our risk mitigation strategy.”

Illumio's real-time traffic map serves as a constant source of security, helping the infrastructure and cloud services team understand connections between applications and visualize the impact of policies before applying them.

“Zero Trust Segmentation with Illumio Core is a simple process,” explains the executive manager. “From an operational perspective, our number one goal is to never break production, which we achieved with Illumio. Our cyber operations governance board is extremely pleased.”

Results & Benefits

With segmentation controls as a foil against vulnerabilities and attackers, the company has gained assurance that the business's high-value assets are protected.

The team also sees Illumio Core as complementary to other tools, particularly its endpoint detection and response (EDR) from CrowdStrike.

“Zero Trust Segmentation and EDR give us a powerful two-pronged approach for defending against attacks,” says a security services manager. “We know Illumio will proactively prevent a breach from spreading, and EDR can then do its job of detecting it and responding.”

The team is strategizing on how they will leverage more Zero Trust Segmentation capabilities in the future and know they can always count on Illumio's partnership.

“From the beginning, there was a sense that the Illumio team would do whatever it takes to support our team,” he says. “Time and again, they've proven exceptional in their responsiveness, expertise, and partnership.”

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.