SaaS Giant Secures High-Value Assets at Scale with Illumio

Crisis turns to opportunity when segmentation is decoupled from the network, enabling improved DevOps

Customer Overview & Challenge

When your network is your business delivery model, there is no room for security failure.

A Fortune 300 SaaS pioneer faced a potential crisis when its decade-old homegrown network security model threatened to fail entirely during the move to a new data center. Ruleset explosion from hypergrowth caused switches programmed with Access Control Lists (ACLs) to run out of TCAM memory. The team caught the issue and identified that no new servers could be provisioned for six months – potentially grinding the business to a halt.

At the same time, DevOps was struggling to transform automation to run smoothly and consistently across environments and meet the need for speed in business performance.

Under board-level scrutiny, the team had to migrate a massive amount of automation with zero mistakes on a tight timeline. With a fully embedded network security model, there wasn't a path to quickly change, but they couldn't continue on the current trajectory. The cost of replacing every switch in five data centers would be over $50 million. More importantly, the operational burden of re-architecting the network under the given turnaround time was untenable at any cost.

Illumio Solution

With 50,000 workloads, the organization had to identify and resolve many special cases one by one. Automation was not consistent across all affected data centers because the organization was highly acquisitive, with multiple layers of automation for builds and maintenance. Any changes would be significantly complex.

Leveraging Illumio Core™ and its real-time application dependency map, the IT team worked with application owners to gain an understanding of communication flows and effectively apply policy. Modeling policy in test mode allowed teams to experiment without the threat of breaking systems or creating downtime, which was an unacceptable risk to the business.

Because Illumio Core uses native firewalls at the host layer and policy follows the workload, security could run consistently in any data center – without re-architecting the network.

Summary

Industry: Web-scale Software as a Service (SaaS)

Environment: 50,000 production workloads across 5 global data centers

Challenge: Mission-critical security without re-architecting the network

Solution: Illumio's host-based security policy ends firewall sprawl and simplifies deployment

Benefits: Save the business and transform IT delivery to future-proof its need for speed

illumio

Customer Benefits

Be a security superhero

Project leads saved the day, coming in significantly under budget and eventually scaling to 70,000 workloads across 5 data centers.

Avoid re-architecting the network

With host-based segmentation, security follows the workload wherever it runs without touching the network.

Give business the speed it needs

As an offshoot of the project, application teams cleaned up automation and owners were positioned to accept a full DevOps management model for their servers, transforming the service model and future-proofing their need for speed.

illumio

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.

Gartner
peerinsights™

See what customers have to say about Illumio.

Follow us on:

illumio