illumio

CUSTOMER STORY

Cathay Pacific Gains First-Class Microsegmentation with Illumio Core

Protecting critical applications and coming in ahead of schedule

Industry: Airlines

Environment: 3000+ servers and ~600 applications, on-premises and multi-cloud including Azure and AWS.

Challenge: Tighten internal security controls and protect applications to uphold the criticality of their cybersecurity program initiatives

Solution: Illumio Core for precise protection of critical applications, enabling Zero Trust control against the spread of potential attacks

Benefits: Easy-to-deploy microsegmentation with quick time to value; reliability and confidence from testing; visibility for cross-team collaboration; millions in savings vs. ACI and NGFWs; and deployed on AWS

Customer Overview & Challenge

Their name has been on just about every "who's-who of airlines" list, ranking top 10 from aircraft safety to ticket sales. These accolades have been all but inevitable for Cathay Pacific as they've focused on delivering world-class airline operation. But when they were targeted by an attack, a new inevitability in today's cybersecurity landscape, the Hong Kong-based carrier redoubled their focus on their security program in short order.

"Zero Trust and least privilege came into the discussion right away. We knew we had to implement microsegmentation for the right level of protection for our most critical applications," explained YC Chan, Head of Infrastructure Engineering at Cathay.

If the end goal of microsegmentation is to prevent lateral movement and protect "crown jewel" applications, they had to know their network better than anyone else from the start. The team required visibility into application traffic across the entire network. But more than that, YC sought a solution that would help them achieve their visibility and segmentation goals in the most efficient way possible.

"We had discovery tools that provided some visibility and insights, but ultimately did not integrate visualization and policy workflow. In order to achieve our goals by the year-end deadline, we needed an interface that showed us application and workflow traffic and enabled us to act quickly and efficiently to block or allow flows."

Illumio Solution

YC and team turned to Illumio Core and quickly realized it was "the easiest way to do microsegmentation."

Illumio's real-time application dependency map visualized the connections between the on-premise servers and AWS and Azure clouds, revealing how Cathay Pacific's applications are communicating. The team can understand what needs protection and can take immediate action on blocking or authorizing workflows.

The ability to run policies in test mode before going into enforcement played an essential role in the success of their deployment. This empowered ongoing collaboration between infrastructure and security teams and application owners. The results? A reliable, thorough process for enforcement that helped them beat their most pressing deadline.

"We partner with application owners to review flows and help define policies. You couldn't ask them to read firewall rules, but Illumio's App Owner View map and plain language labels make it infinitely easier for them to

understand the flows and apply policy. We are confident that our applications are protected with the right level of segmentation – with no disruptions during enforcement."

Not only do YC and team continue to use Illumio to bolster their internal defenses, but it is also helping solve another challenge: PCI DSS compliance. Securing cardholder data is of paramount importance to Cathay. With Illumio Core's mapping and policy creation capabilities, they're able to meet many PCI compliance requirements. The team is also leveraging SecureConnect on over 1,000 workstations for instant workload-to-workload encryption of data in motion.

The alternative route for this compliance initiative was installing tens of data center firewalls to shore up their call center offices, amounting to an estimated $5M. With far less effort and spend, they're well on their way to PCI peace of mind.

Whenever we introduce new servers or applications, Illumio is part of the commissioning process. It's proven to be easy to deploy and implement and has helped us be more application centric.

YC Chan
Head of Infrastructure Engineering
Cathay Pacific

Results & Benefits

- **Fast time to value:** The team came in ahead of schedule, faster than anticipated, in segmenting their most critical and vulnerable applications.
- **Less risk, more uptime:** The ability to test the impact of new policies without any changes to the network gives them much-needed confidence that enforcement will never break applications.
- **Greater visibility, cross-functionally:** Using the real-time map to involve application owners in the segmentation process improves policy accuracy and ultimately increases Cathay's security posture.
- **Clear path to compliance:** Saving millions in potential firewall costs for PCI compliance, the team has Illumio Core's encryption, visibility, and segmentation capabilities at their disposal for compliance mandates.
- **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.