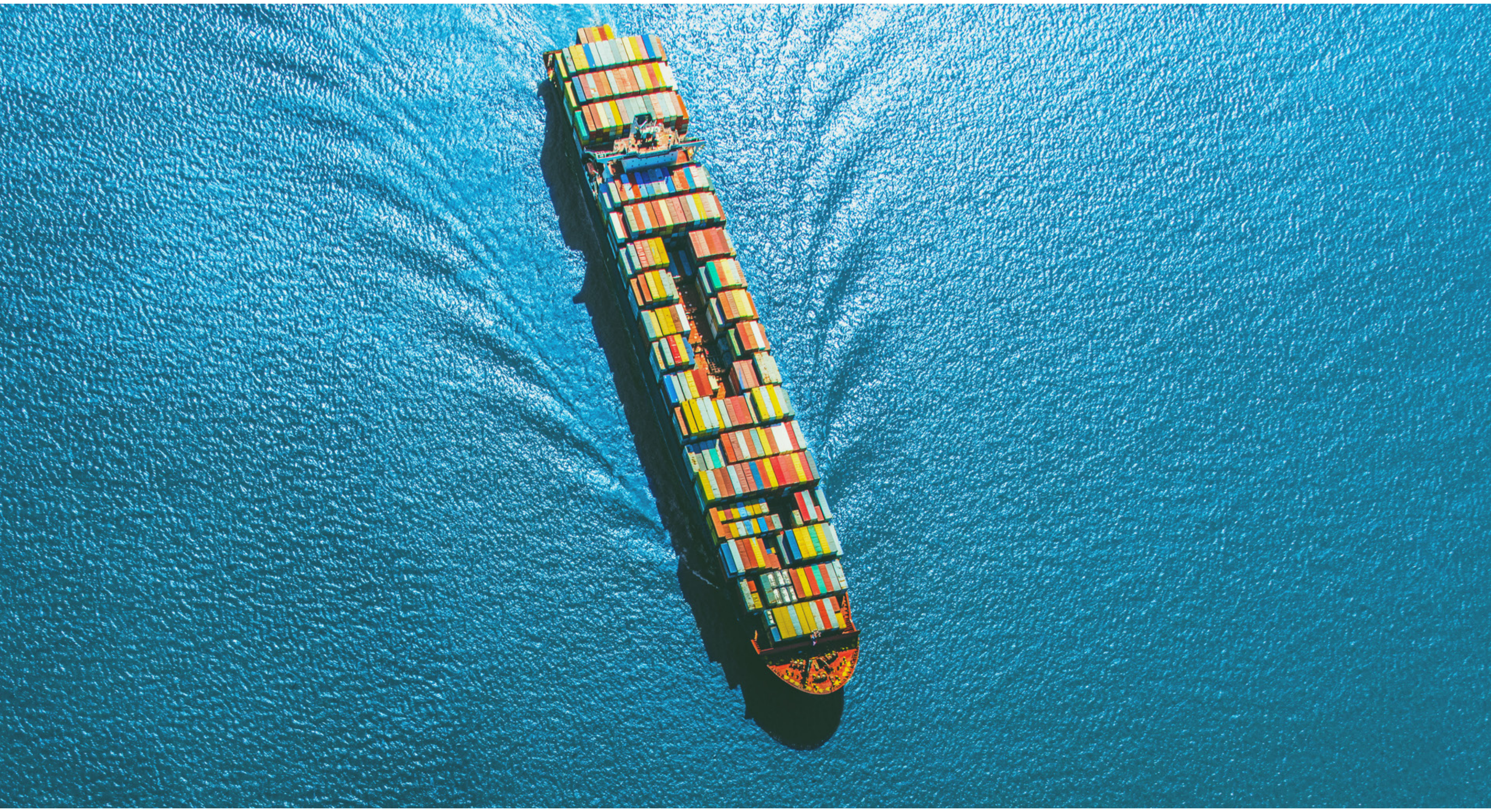
CASE STUDY



QBE Strengthens Zero Trust Posture with Illumio

Gaining micro-segmentation that reduces complexity and risk across a globally distributed infrastructure

Customer Overview & Challenge

With a 135-year history marked by a commitment to customers and innovation, QBE is one of the world's largest global insurers. As operations span Australia, Asia Pacific, Europe, and North America, the scope and scale of the company's compute estate continues to expand. The move to hybrid multi-cloud data centers and an increasingly complex application environment required QBE to think differently about how to protect the organization and its customers.

Further compounded by the rising threat of ransomware in the industry, a Zero Trust approach to security became front of mind for CISO Andrew Dell. "We have partners inside our network, service providers that are in the cloud, and other networks connected to us," he explained. "So, we need to think differently about controlling access to our data and our applications, how we reduce risk, and what technologies will help get us to a Zero Trust model."

A focus on Zero Trust meant re-evaluating the company's segmentation strategy. QBE relied on physical firewalls and virtual firewall appliances for segmentation, which proved to be "labor intensive and complex," according to Andrew. Firewall rulesets would become almost unmanageable for the team, potentially putting the very applications they were trying to protect at risk.

QBE needed micro-segmentation for more efficient, granular control over dynamic environments. Future-proofing the business with a solution that would empower the organization to "go faster, safely" was critical.

Illumio Solution

"We are always looking for simple solutions to complex problems," said Andrew. He found exactly that in Illumio Core: a software-based micro-segmentation solution that eliminates network segmentation headaches and provides the foundation for Zero Trust security – starting with visibility capabilities.

Illumio's real-time application dependency map showing traffic flows between workloads wherever they run delivered quick value. "The initial attraction was really the simplicity," recalled Andrew. "Having the ability to span the physical and the virtual and present insights in a highly resolved fashion is a game-changer. It enabled us to be more efficient with our resources and planning right away."

Equipped with the understanding needed to segment confidently, the team set out to tackle "crown jewel" applications first. According to Nick Venn, global collaboration and cyber infrastructure manager at QBE, "Since Illumio policies are independent of underlying infrastructure, we get greater and granular security and performance. And the best thing is the policy can now follow the workload, so we don't have to worry about recreating policies or re-architecting the network. That flexibility is absolutely essential."

These efficiencies translate into years saved for QBE. "For an organization of our size and scale and complexity, traditionally rolling out an equivalent solution was a multi-year proposition," said Andrew. "But with Illumio, we had production assets enforced and under control in months, fulfilling our need to move faster and further our Zero Trust posture."

Summary

Industry: Insurance

Environment: 10,000 workloads across globally distributed data centers and multi-cloud

Challenge: Segmentation across heterogeneous environments without the complexity of firewalls

Solution: Illumio Core for real-time visibility and micro-segmentation essential for Zero Trust security

Benefits: Fast time to Zero Trust; flexibility for the future; stronger internal alignment

The team also realizes time savings in previously labor-intensive tasks. “Illumio Core enables us to roll out firewall changes much faster than before,” added Nick. “Previously, it would be days or weeks. Now it’s minutes or hours.”

QBE relies on the product’s ease of management, which allows them to “focus on protecting the organization, rather than thinking about how we schedule downtime or get investment for new hardware,” said Andrew.

With micro-segmentation in place, QBE can stop the lateral movement of ransomware or attackers, minimize impact, and ultimately respond quicker and recover faster.

The ability to plug in other services has also been a “real force multiplier” over time, explains Nick. “The map grew legs when we overlaid vulnerability data from our scanner software,” he said. “This allows us to see what applications are connecting to vulnerable ports, then make a business decision and a cyber decision to determine what needs to be closed.”

Today, Illumio continues to help drive collaboration and the need to think differently. Security and application infrastructure teams are much more aligned since they can understand and address risks to applications like never before. As a result, Nick concluded, “cybersecurity has become part of the answer rather than being a problem.”

Customer Benefits

Fast time to Zero Trust

Default-deny policies that are decoupled from the network enable the team to enforce effective Zero Trust controls quickly – and with confidence, afforded by the ability to test policies before going into enforcement.

Future-proofed with flexibility

No longer limited by traditional constraints, QBE can count on scalable and flexible segmentation for consistent workload security as the organization continues to innovate and accelerate its multi-cloud strategy.

Improved operational efficiencies

By cutting the complexity of managing firewalls for segmentation, QBE has a more effective and efficient solution that gives the team more time to focus on protecting the organization and driving its digital agenda.

Stronger internal alignment

Real-time application insights help security and application teams understand application risks and vulnerabilities and make it easy to collaborate on policy decisions.

> For an organization of our size and scale and complexity, traditionally rolling out an equivalent solution was a multi-year proposition. But with Illumio, we had production assets enforced and under control in months, fulfilling our need to move faster and further our Zero Trust posture.
>
> **Andrew Dell, CISO**

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.