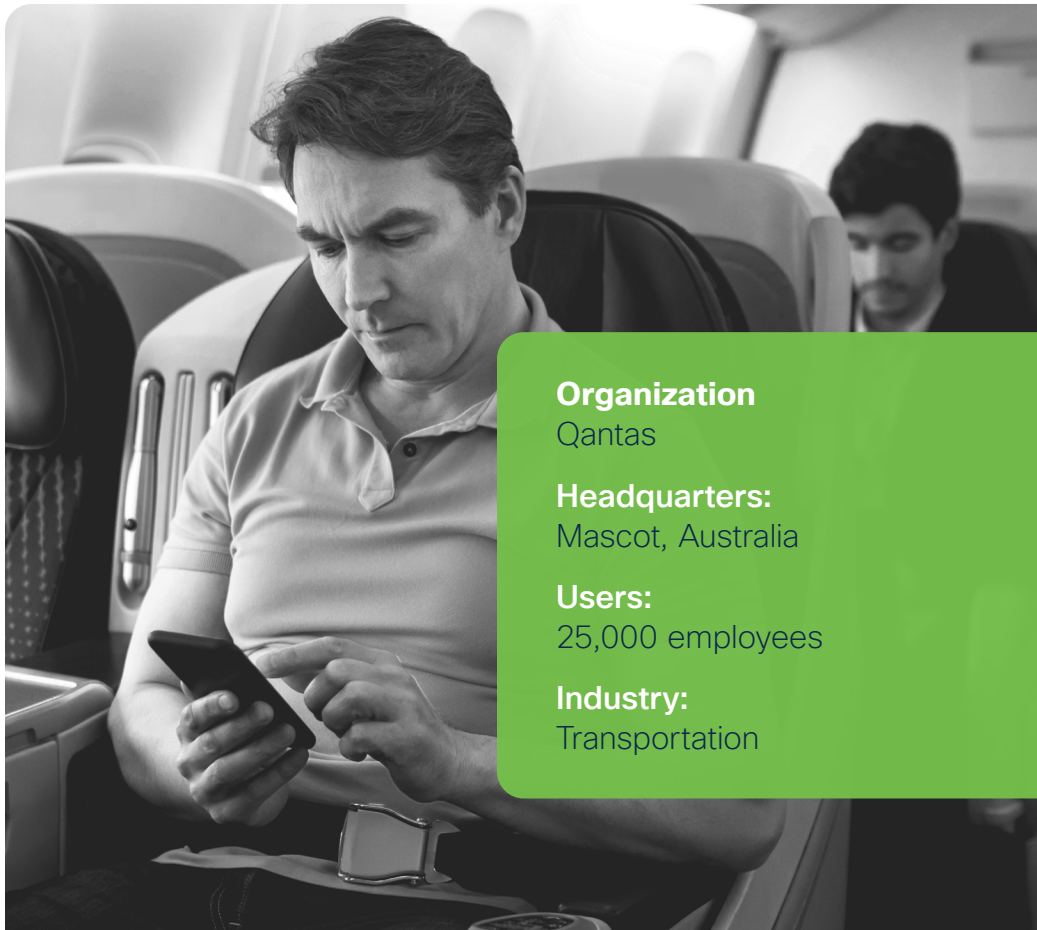
CISCO
SECURE

Case Study
Cisco Public

How a Leading International Airline Embarks on Its SASE Journey

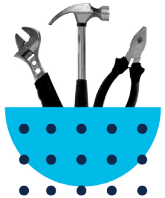


Organization
Qantas

Headquarters:
Mascot, Australia

Users:
25,000 employees

Industry:
Transportation



Objective

As one of the world's safest airlines, cybersecurity is as critical as safe skies. Australia's largest domestic and international airline, Qantas, needed to secure all employees, devices, and apps – anywhere. The airline wanted a holistic security solution that would not only protect remote workers, but also support its secure access service edge (SASE) initiative.

Challenge

- Lack of off network protection for remote users
- Controlling access and enforcing security protections for all users
- Replacement of its legacy secure web gateway (Cisco Cloud Web Security /CWS) which had become end of life

Solution

Cisco Umbrella

Cisco Secure Firewall

Cisco SD-WAN

Impact

- Secured remote workers, as well as visitors using guest Wi-Fi at Qantas locations
- Gained ability to protect users' web activity regardless of location, with full proxy for all traffic
- Moved security controls and traffic inspection to the edge and laid a foundation for its future SD-WAN transformation

Challenge

Rethinking IT and security during challenging times

Founded a century ago, Qantas soared from its beginnings as a small airline to today's commanding position as Australia's domestic and international carrier. Along the way, Qantas became known as one of the world's safest airlines.

"Safety is our number one goal for the whole airline, whether that's from the perspective of airplanes or cyberspace," explains John Gately, service delivery lead at Qantas. "Security is key to the brand, and cybersecurity breaches can really hurt the brand's reputation."

One of the drivers behind the company's success is its foundational flexibility that helps Qantas to rapidly take advantage of new opportunities. Qantas' booming freight business is a good example.

During the pandemic lockdowns, the company added new freight routes to serve its customers' changing needs. And despite being in an industry made particularly vulnerable by the pandemic, Qantas has been able to drive significant IT and security enhancements to its architecture.

This kind of agility depends on both flexibility and technology. "We always want to find new technologies and new ways to serve the customer," says Adam Kinsella, product owner for network, network security, and voice at Qantas. "As a premium airline, there's always that focus on delivering the best customer service — and not just the time on the plane, but the entire experience."

> "Safety is our number one goal for the whole airline, whether that's from the perspective of airplanes or cyberspace."
>
> John Gately, Service Delivery Lead, Qantas

QANTAS

Solution

Ensuring consistent levels of security for remote workers

When Qantas' existing secure web gateway (SWG), Cisco Cloud Web Security approached its end-of-life, they began a search for a new proxy solution.

"We evaluated another SWG provider, however, we chose Cisco Umbrella because it gave us all the functionality we wanted as well as additional features we could turn on in the future," Kinsella says. "Umbrella was also attractive because we could leverage the integrations with Cisco SD-WAN, among other Cisco products, and maximize our investment."

Qantas uses Umbrella to protect both its DNS and web traffic, as Cisco Umbrella combines multiple security functions in a single cloud service. Prior to Umbrella's deployment, Qantas didn't have off-network protection, which is especially important in a remote environment where employees are connecting to apps and data through their own wireless networks. "Off-network protection is a key factor for us, and Umbrella protects our people both on and off the Qantas network," Gately says.

In addition, Qantas has built IPsec tunnels to the SWG to protect guests using guest Wi-Fi. The company is also in the process of replacing its legacy on-premise SWG from a different vendor with Umbrella at Jetstar, Qantas' low-fare airline.

Since Qantas has a lean security team, they leveraged key partnerships and the Umbrella customer success team to drive faster implementation. They worked closely with Telstra, FirstWave, Fujitsu, and the Umbrella customer success team to ensure a successful deployment. "Each of our partners played an important part, and the Umbrella customer success team helped us with design and deployment best practices, troubleshooting, and faster implementation. Without that team, we wouldn't have been successful," Gately says.

"We're also replacing our ASA firewalls with Cisco next-generation firewalls. As we expand the ecosystem and get a single view into the environment, we'll see more value," Kinsella says.

> "Each of our partners played an important part, and the Umbrella customer success team helped us with design and deployment best practices, troubleshooting, and faster implementation. Without that team, we wouldn't have been successful."
>
> John Gately, Service Delivery Lead, Qantas

Results

The next steps in Qantas' SASE journey

Qantas now has complete visibility into internet activity across all users, locations, and devices, along with the ability to control access and enforce security protections anywhere. "Since we can see which apps employees are trying to use, we allow the ones that they should be able to access and block the ones that they shouldn't," Gately says.

In addition, Qantas is now enforcing consistent levels of security for employees whether they're connecting to apps and data at the office, at home, or on the go. "Threats and exploits can't get through, and Umbrella gives us confidence because we know that our users are protected when they're surfing the internet on or off the network," Kinsella says.

Umbrella not only helps Qantas meet its objective to secure users anywhere but also supports the company's vision of implementing a secure access service edge (SASE) approach. As the next step in Qantas' IT and security evolution, the company plans to deploy Cisco SD-WAN, powered by Viptela. This will enable Qantas to secure remote location direct-to-internet access (local breakouts) and gain the performance, efficiency, security efficacy benefits of moving security controls and traffic inspection to the edge. "Our plan is to use the SWG integration with Viptela and connect the tunnel directly to Umbrella from the SD-WAN edge devices. With the SWG integration, Qantas will be able to extend Umbrella's protections across the SD-WAN fabric.

"Umbrella gives us the foundation that will allow us to take advantage of other products, like SD-WAN, when we start to move to the technology refresh in the network space," Kinsella concludes. "Our goal is to think about how to join some of our strategies together and take advantage of our investments."

> "Threats and exploits can't get through, and Umbrella gives us confidence because we know that our users are protected when they're surfing the internet on or off the network."
>
> Adam Kinsella, Product Owner for Network, Network Security, Qantas