Cloud-Based Web Security Provides a Tailwind for This Airline's Digital Transformation

Headed for the cloud, the enterprise turned to Forcepoint to help safeguard open innovation and collaboration among employees—and reduced security operational costs by 80%.

As an airline that prides itself on efficient operations, this enterprise knows what it takes to move fast, be efficient, and provide consistent service. So it's no surprise that it's joining scores of other companies in the pursuit of digital transformation to keep business flying as smoothly in the office as it does in the sky. But moving data and processes off-network also sparks new security challenges.

CUSTOMER PROFILE:
Operating since the early 20th century, this South American airline flies to destinations across the globe with an annual revenue of over $2 billion.

INDUSTRY:
Airline

HQ COUNTRY:
Panama

PRODUCT:
Forcepoint Web Security Cloud

The highly distributed nature of the airline industry is pushing C-level executives to drive digital transformation at every level to benefit from advanced technologies. This airline is no different; still relatively early in its cloud journey, it recently moved to Office 365 and is evaluating the benefits of infrastructure-as-a-service. The company's security team knew that to safeguard its move to the cloud, it needed a security solution to strongly safeguard off-network activity while keeping business moving at cruising speed.

"As they move their operations to the cloud, they're looking for their security solutions to move there as well," Forcepoint Sales Engineer Ramon Castillo explained.

Securing an open web environment for everyone, everywhere

New digital technologies offer the promise of greater efficiencies in the workplace, reduced infrastructure spend, better communication and collaboration across teams and with external partners, and so much more. But, while providing distinct advantages, strategic digital transformation can also open the door to new types of cyber vulnerabilities—making many IT teams nervous about the move. When data and processes are located in the cloud, users are exposed to more points of entry for malware and other web-based risks.

This was one of the airline's main security concerns: "Because their web browsing is so open, there's more room for user error. They are innocently creating this vulnerability based on that free flow of access, but if they lock it down, then they can't do their jobs," said Castillo. Internal users need a free and fluid environment to exchange information, bolster creativity, and support collaboration through the cloud. And that need doesn't stop at the network perimeter—distributed and mobile users need secure, efficient access even off the network.

"They are innocently creating this vulnerability based on that free flow of access, but if they lock it down, then they can't do their jobs."

RAMON CASTILLO, FORCEPOINT SALES ENGINEER

Challenges

Digital transformation efforts are moving data and processes to the cloud, widening the attack surface and creating more entry points for malware.

Distributed and mobile teams need safe, efficient access to cloud data and processes.

Open web browsing policy is necessary for staff to do their jobs but leaves more room for user error.

Approach

Deploy Forcepoint Web Security in the cloud to safeguard and scale with the company's digital transformation.

Integrate data loss prevention and cloud security capabilities for further data protection.

An 80% cost reduction in 90 days

With Forcepoint's license mobility across deployment architectures, customers gain the freedom and flexibility to scale their business—whenever they're ready. So, when it was time for the airline to move from hybrid to full-cloud deployment, the organization knew it could trust Forcepoint to get it where it needed to go with minimal disruption to its security program.

In just three months, Forcepoint was able to migrate the enterprise's hybrid deployment to a full cloud web security solution. Moving to a competitor would have required it to rebuild existing policies or pay more money—not to mention the lengthy process of vetting and deploying a new vendor. And that wasn't the only way the enterprise saved money. The security team was able to reduce operational expenditures by 80-90% by eliminating the cost associated with physical, on-premises appliances.

The freedom to connect, without the vulnerabilities

Addressing the security team's concerns about new vulnerabilities created through open web access, Forcepoint Web Security Cloud reduces risk of malware without locking down web or cloud application use or disrupting users' productivity—even when those partners and employees are off the network. "We were able to expand security policies to roaming users in transparent mode as if they were at the office," said the airline's Chief Security Officer.

Going direct-to-cloud also improved roaming and distributed users' experience by removing latency, eliminating the need to backhaul traffic to the enterprise's main location.

"The customer was pleased that they were able to start on-premises, then move to the cloud without switching security services or paying more. We can adapt our solutions to whatever architecture our customers need," said Castillo.

Over the years, Forcepoint's partnership with the airline has only strengthened. The organizations hold regular tunings to ensure continued alignment between IT security and strategic business priorities. As it continues to modernize its IT and broader business operations, Forcepoint will be there to scale with it, providing the flexibility needed to protect the data and processes that drive the company forward.

"We can adapt our solutions to whatever architecture our customers need."

RAMON CASTILLO, FORCEPOINT SALES ENGINEER

Results

3 months to migrate from hybrid to cloud deployment, keeping all policies intact.

80-90% reduction in security operational expenditures through eliminating on-premises appliances.

Consistent security policies applied to roaming users

Reduced latency for roaming and distributed users.