FORCEPOINT
POWERED BY Raytheon

Case Study

Global Airline

"We needed to hedge against the business risk of users and business lines taking up cloud apps faster than IT could discover, monitor and protect them. We needed a solution that automated the process and put us back in control – Forcepoint CASB was the best solution to meet these goals."

— Director of Information Security, Global Airline

INDUSTRY
Transportation

PRODUCT TYPE
Forcepoint CASB

SECURITY ISSUE
Empowering a Mobile Workforce for SaaS Apps while Reducing Risk

OVERVIEW

Since its founding, this global airline (choosing to remain anonymous) has led the industry in flight technology innovation and customer satisfaction, providing an upscale flying experience at attractive fares. The company employs over 2,800 staff in more than two dozen locations across North and South America.

The airline's technology leadership extends beyond their ground breaking in-flight service systems to flexible and cloud-deployed IT infrastructure and apps for employee communication and collaboration, operations and finance.

CHALLENGE

The company is a model organization for detailing the challenges of leveraging cloud apps and services to run a highly distributed and complex business. The company's staff is spread across more than 24 airport locations and its employees often depend on public networks for access to critical tools to perform their jobs and collaborate with colleagues.

Under these circumstances, users were frequently adopting unauthorized applications that could help them complete a given task for their job. Given the requirement for anywhere, anytime access, cloud apps are a natural choice for this airline's needs. While users embraced IT-sanctioned applications, several workgroups, including finance and sales, had also adopted unauthorized apps that created an additional blind spot for the IT staff.

In both scenarios, ubiquitous access and a fast, smooth user experience were required. However, the company's IT staff realized that this was not possible with VPN-based approaches that are often difficult to configure, unreliable and slow.

The major challenges for IT staff were how to gain visibility and control over a growing list of sanctioned cloud apps for employees to use, and also the ability to log and manage cloud services, such as file sharing, that users adopt on their own. In addition, the company was concerned about the "larger attack surface" that the long list of "front door" login screens presented to cyber criminals attempting to use stolen credentials to hijack accounts and steal sensitive data. For these reasons, IT staff decided to bring both the authentication and the post-authentication activity monitoring back in house for all apps in the cloud.

The airline realized it needed to adopt a fundamentally new approach for assessing cloud app risks, gaining insight into cloud app usage and protecting cloud apps from account-centric threats. Since security is an afterthought for some cloud providers, the company required detailed visibility into cloud app activity and intelligent analytics across all the cloud apps in use. Like most organizations, their existing on-premises security infrastructure was not designed to mitigate risks surrounding cloud apps.

SOLUTION

The evaluation criteria included testing any proposed solution with key applications (among the over twenty cloud apps and services used by their employees). In addition, IT security required a reporting solution that would allow actionable resolution to identified issues. They also required built-in multi-factor authentication, along with consistent policies for access across all apps, since every cloud provider had different approaches to authentication and access. Finally, the solution had to offer seamless deployment with the company's existing single sign-on provider, SecureAuth.

The IT staff's search for a comprehensive cloud app visibility and control solution led them to select Forcepoint CASB (Cloud Access Security Broker). The top selling points for them were Forcepoint's early market advantage and full range of integrated capabilities that addressed all their evaluation criteria. The company did not consider any other vendors since no other products had the capabilities they required.

Initially, the IT staff deployed Forcepoint CASB in an offline sniffer mode to monitor authentication requests against their single sign-on infrastructure. This allowed them to see if any attacks targeting their cloud accounts were in progress.

RESULTS

Forcepoint enabled this global airline company's IT security staff to quickly address new business initiatives and secure existing cloud apps and services. Forcepoint provided them the following unique advantages:

- Consistent, detailed and clear visibility into all cloud app activity without any disruption to user experience, operations and customizations
- Privileged user activity monitoring and separation of access control policies from cloud app administrators
- Simplified deployment in the cloud that immediately leveraged existing single sign-on deployment
- Dashboards and reports covering who accesses which cloud apps with drill down to specific data and objects accessed
- Global enforcement of access controls for any endpoint type from any location; no need to use slow and hard-to-configure VPN access
- On-premises, centralized control of multi-factor authentication to enforce out-of-band authentication based on a range of flexible policies
- Real-time alerts to IT staff on risky behavior, anomalous activity and account takeover threats

The airline needed to hedge against the business risks associated with a distributed workforce accessing cloud apps over public networks from a range of endpoint devices, including personal smart phones and tablets. Given the dozens of cloud apps in use, they wanted a comprehensive solution that addressed all their criteria and provided comprehensive SaaS discovery and real-time cloud app protection. In addition, the solution needed to be deployed without impacting the user experience or IT operations. The only solution to meet and exceed their demanding requirements was Forcepoint CASB.

LOOKING FORWARD

The company plans to leverage the Forcepoint CASB connectors to directly feed all their cloud activity to their existing SIEM deployment. This will enable correlation of cloud data with event data from other sources across the enterprise into a centralized repository for analysis while maintaining the Forcepoint dashboard for visibility into their cloud environment.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[CASESTUDY_CASB_GLOBALAIRLINE_EN] 300099.041217