Sky High Security: How a Major Airline Secured Its Cloud Better

|  |
| --- |
| **Fly High Airway**Fly High Airway is a major domestic and international airline. **Requirements**As a major airline, Fly High needed better efficiency with their email catch rate than what they were getting with Proofpoint. Additionally, they were looking for protection for their Microsoft Teams account, which they rely upon heavily, for internal communications. They also wanted a solution that was cloud-native and connected via API.  **Cloud Suite**Office 365**Previous Email Security Solution**Proofpoint |

Background

Sebastian Thompson† is the CISO for Fly High Airway, a major domestic and international carrier.

As an airline, Fly High has stringent security requirements. Airlines are heavily regulated and are party to numerous treaties and protocols that govern cybersecurity. That applies to cyberattacks against the aircraft itself, as well as email security. An industry with tons of data and personal information is often on the receiving end of thousands of phishing attacks.

Thompson had used Proofpoint in their environment for a number of years, and was underwhelmed with its performance. In particular,  he was not happy with how many phishing emails were getting through on a regular basis. “It was just too much,” he says.

In fact, according to Avanan research, Proofpoint misses over 20 malicious emails per 100,000 emails.



Beyond that, Thompson was very interested in Microsoft Teams protection. Both before and during the pandemic, the airline relies heavily on Teams for communication. It’s used in-flight, by customer service and other internal teams. Proofpoint only offers limited protection related to data loss, and those protections are still relatively new. “We know Teams is a place where attacks are going to increase, and we need to be able to protect our users proactively,” Thompson says.

With their subscription to Proofpoint coming up for renewal, Thompson needed a new solution to stop email threats before they hit the inbox, and protect Teams and other collaboration apps.

He had a few requirements: It had to be cloud-based and connect via API. Two, it needed to have a clean user interface. Three, and perhaps most important, the solution needed to do a better job of stopping phishing attacks, both in email and Microsoft Teams.

“Too Many Issues”

When Thompson had Proofpoint installed, it caused him tons of trouble, far too many emails were coming through to end-users. His SOC was overwhelmed with all the end-user requests. Between restoring from quarantine and remediating false positives, Thompson’s team was stretched thin and overworked, leaving them with limited time to focus on other, critical tasks.

Like all SEGs, Proofpoint was built for the on-prem era. As such, they were not built to handle cloud email and collaboration apps.

As an SEG, Proofpoint blocks inbound and outbound emails. By their very nature, sitting outside the email server, they are blind to emails within the organization. 

That leaves them vulnerable to many potential malicious emails. SEGs, because of their architecture, can’t utilize AI to the fullest. AI is only as good as the training set it’s trained on. SEGs have a less focused training set, seeing only a single email at a single point in time. If trained on shoddy data, the output is going to be worse. That’s why SEG’s rules and signature-based solutions are not equipped to prevent advanced threats. For example, of today’s advanced phishing threats, 51% require AI/ML to identify and stop.

Further, as heavy users of Teams, Thompson needed complete protection. It wasn’t enough to just have data loss protection, as Proofpoint provides. Instead, Thompson needed a solution that had the ability to scan every file and message for malware, to proactively protect against phishing messages, and able to do time-of-click analysis on URLs.

“Overall, there were just too many issues,” he says, referring in particular to frustrated end-users, and burnt-out SOC employees. “We needed a change.”

Fly High needed a new solution. As he began his search, Thompson came across the glowing ratings for Avanan on Gartner and G2. Avanan has more five-star ratings than Proofpoint and Mimecast combined.

The next step was to do a POC.

“Our SOC’s Workload Has Drastically Dropped”

During the POC, Thompson was instantly impressed.

Avanan connects in seconds via API, which Thompson appreciated. Unlike other API solutions, Avanan’s patent blocks emails before reaching the inbox. Other API-based solutions take an average of three minutes and three seconds before removing a malicious email from the inbox, allowing time for users to click on the email. In an incredibly fast-paced environment, that sort of risk was unacceptable.

Thompson liked how Avanan drastically reduced phishing emails reaching the inbox and thus getting to end-users. Avannan users see a 99.2% reduction in phishing emails getting to the inbox.

Third, Avanan represented significant cost savings over Proofpoint.

Another thing that impressed Thompson was Avanan’s Teams protections. Avanan is one of a few security vendors that offer Teams protections. Proofpoint only offers DLP. Avanan adds malware protection, DLP, URL protection, compliance tools, and more.

Beyond that, Avanan controls access to confidential data, quarantines malicious content and informs users of security events. Avanan also offers a detailed dashboard that updates administrators on security issues with usage in Teams. Avanan logs the total number of users, files, shares, links, logins, channels and threat detections.

“Our SOC’s workload has dramatically dropped,” he says.

Finally, ease of use is incredibly important to Thompson, and he found it with Avanan. In the Avanan dashboard, it’s easy to quarantine messages and easy to find them. Everything operates in a single-pane-of-glass and configurations are super simple.

“I’m saving time, money and energy,” he says. “It’s huge.”

“It’s a Game-Changer”

As the CISO for a major airline, Sebastian Thompson needs reliable email security, one that catches all of the attacks coming its way. After years of using Proofpoint, Thompson decided it was time for a change. Not only was it costly, but it did not stop all the malicious emails.

Additionally, Proofpoint’s protection for Microsoft Teams was lacking. As power-users, Fly High Airlines needed industrial-strength security.

The answer to his questions came with Avanan. “It’s been a game-changer,” Thompson says.

†Company and individual names have been changed, but are available as a reference customer.