Why This Benefits Administration Company Finally Gave up on Mimecast

The Promise

Jonathan Chambers† heads the information technology group at TPA America, a national benefits administration company. When the company hosted their email within their own datacenter, he felt he knew and understood his security, so when the company decided to move to Office 365, he wanted something that was easy and low maintenance. He compared the range of vendors and because the IT staff was small, he wanted something "set-and-forget".

Based on the pitch they received, they decided to go with Mimecast. “We were sold on the idea that it is pretty seamless,” Chambers says. “Everything just works. You don’t worry about it, it’s all taken care of—a one-size-fits-all approach.“

After deployment and a period of transition and tuning, he was promised he could get back to business.

Unfortunately, the problems started as soon as it was configured to protect emails in real-time. Chambers saw a few issues.

TPA America†

TPA is a Third Party Trust Fund Administrator and IT Services organization with offices across the United States.

Requirements

The bulk of client communication has moved from phone to encrypted email so it has become business critical. While TPA maintains a large help desk team for its service and software clients, it has a limited staff for internal support and employee incidents. TPA needs an email security solution that requires minimal maintenance and does not disrupt daily operations.

Cloud Suite

Microsoft Office 365

Previous Email Security Solution

Mimecast

False Positives

The first problem to arise was the number of false positives. While most of the evaluation and comparison focused on catch rates, it had not occurred to him that false positives would be the greatest source of disruption to the business. Emails would just ‘disappear’ until a user would ask about it the next day or spend time looking through quarantine. Each item would lead to a helpdesk ticket or an urgent call from a department head.

The relationship with employees changed, causing both distrust of their email inbox and IT’s ability to manage it.

Confusing Interface

Adding to the challenge was the confusing interface. Despite assurances, switching to the new solution required a very steep learning curve.

“It didn’t make sense to us,” Chambers says. “From a layout standpoint, there’s two different types of grey lists, one spelled with an E, one spelled with an A. They both do their own things.”

It was difficult to find a message or understand why it was blocked. “It’s like, just show me! Show me where! Show me why!” And it just didn’t.”

Eventually, despite security best practices, he began putting entire domains on the Allow-List. While this opened the company up to attacks from spoofed addresses, it was the only way to reign in the number of help desk tickets

Lost Time

It was the lost time, both on the IT team and for company employees, that became an expensive burden.

Email-related tickets are often time-sensitive and because they can lead to a breach, potentially critical, forcing the helpdesk to grant each priority. “Just administering the product took an awful lot of time,” he says. “An awful lot of energy and an awful lot of focus that we just didn’t have.”

It became necessary to add staff to manage the system and “it was just a challenge to work through the UI for everything,” Chambers says. “And, in fact, it was hard to cross-train somebody. I mean, it was a very meticulous process to have to wrangle it all the time. And frankly, we as a department just did not have time to sit and babysit or hand-hold everything. It was an unsustainable model.”

At this point, the status quo was unacceptable. “We were just so soured on the issue,” he says. “It was just time to go. It was time to go.”

Chambers remembers, with a laugh, the decision came the moment when he was locked out of his Mimecast account. “The solution from Mimecast support was a document…that required signing in to view!”

> **It made sense to be able to monitor internal email as well.**

Missed Attacks

While he had already decided to find an alternative, Chambers only realized how bad things had gotten after starting the Avanan trial.

Deployed inside Office 365, effectively behind the Mimecast gateway, Avanan immediately began catching attacks that would have otherwise reached the inbox.

“All along, we would have things that came through that we were sure would be easily caught, but Mimecast would explain them away as configuration issues. Or they wouldn’t provide any details because the reasons were alway part of their ‘secret sauce’.”

This company needed something that not only kept their promises of blocking attacks—but also showed why that attack was blocked.

> **It was difficult to find a message or understand why it was blocked. “It’s like, just show me! Show me where! Show me why!” And it just didn’t.**

The Avanan Solution

Originally, Chambers was attracted to the fact that Avanan deploys inside Office 365. The API-integration seemed the modern solution when compared to the MTA gateway architecture reminiscent of his data-center days.

"It made sense to be able to monitor internal email as well," he says.

Intrigued because it was different, Chambers was pleased to find that it was better.

The IT team was immediately attracted to the UI of the Avanan portal and the speed at which they could identify and understand an event. Because of their experience with the flow of false positives from Mimecast, it took a couple of months for the helpdesk to trust the results, but the fact that the interface could "Just show me where! Just show me why!" so quickly, it saved time immediately.

"It just started off on the right foot," he says.

One of the most powerful, but hidden features of the Avanan platform is the machine learning system specifically designed to prevent false positives. Analyzing a year's worth of messages on the first day of deployment, the engine creates a reputation matrix for both internal users and trusted partners. Not only did this reduce IT workload, Chambers could finally remove partner domains from their Allow-list configuration. This is often the most common security hole that attackers use to reach the inbox.

Not only did the Avanan interface offer a near-zero adoption curve for the IT team, users were quick to switch to the new system. Phish reporting and quarantine release requests use the existing Office 365 infrastructure so there is only one quarantine to manage and no new tools to learn.

After years of struggling with a SEG that was far too complicated and ineffective, Chambers and his company has embraced the simplicity and reliability of Avanan.

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

About Avanan

Avanan is a cloud email security platform that pioneered and patented a new approach to prevent sophisticated attacks. It uses APIs to block phishing, malware, and data leakage in the line of communications traffic. This means Avanan catches threats missed by Microsoft while adding a transparent layer of security for the entire suite that also protects other collaboration tools like Slack. The solution has been recognized as the top-rated cloud email security solution by customers and can replace the need for multiple tools that surround email and file sharing.

See how Avanan can transform your security
avanan.com/demo