AVANAN

Avanan – Industry Insights

API-Based Security: We Prevent. They Respond.

June 30, 2020

Highlights

- Avanan is the pioneer in API-based email security, having substantially more deployments than all other API-based vendors combined.
- The critical architectural difference between Avanan and other vendors is Avanan's ability to block ***before the inbox***. We are preventative, they are reactive.
- Avanan is the only API-based solution that is a true replacement for a Secure Email Gateway because it protects ***before*** the inbox.

Background

Avanan was the first vendor to adopt the API-based approach for email security. The technology solves multiple problems that still plague traditional Secure Email Gateway (SEG) vendors:

- Insider threats/compromised accounts: SEGs are blind to internal email.
- Retraction of threats after they have reached the inbox. More attacks use 'post-delivery arming' tactics.
- Post-attack forensics and remediation.

Avanan pioneered the technology five years ago and received a formal patent in 2018. Since that time, multiple vendors have joined the market.

Gartner recognized the API-based approach in its 2019 Market Guide for Email Security, designating 10 vendors as “Cloud Email Security Supplements” (CESS) that can solve the problem of “specific threats, often in the realm of hard-to-detect phishing, and can leverage full access to cloud-hosted inboxes via APIs for detection and remediation.”

Because of Gartner’s report, and the fact that incorporating APIs into the functionality makes sense, there is an influx of API-based solutions on the market. Compounding the confusion is the fact that legacy Secure Email Gateways (SEGs) solutions are starting to incorporate API language into their marketing, but their technology is clunky and only peripheral to their product with little integration.

Between all the marketing and Gartner recommendations, it's easy to be confused and miss the one fundamental difference that sets Avanan apart.

How Does Avanan Differ From Other API-Based vendors?

Only Avanan is a true replacement for a Secure Email Gateway because it is the ***only*** solution that blocks ***before*** the inbox. All the others are just 'supplements'.

In the Avanan policy manager, we have three modes.

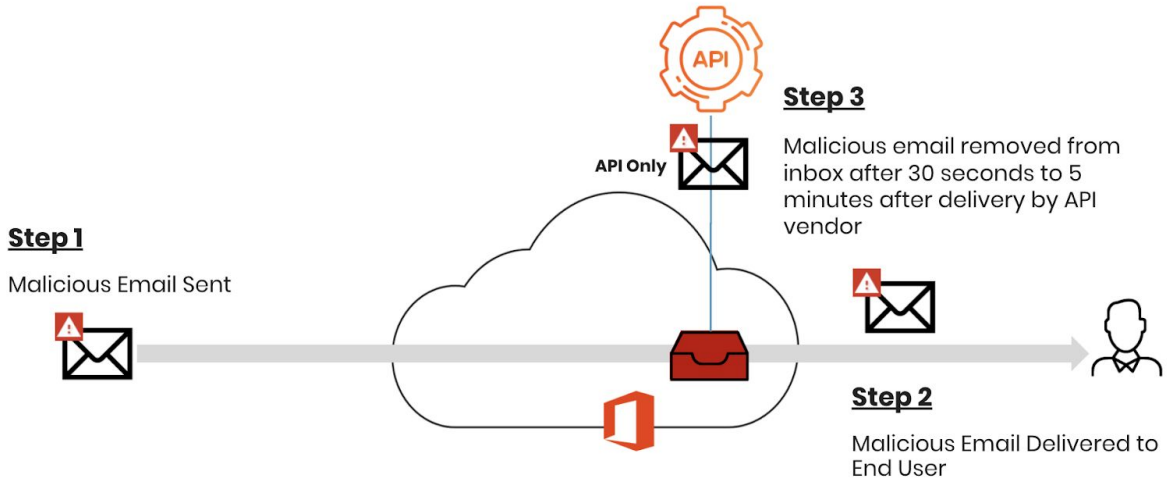
- Protect
- Detect and Prevent
- Monitor Only

Other API-based solutions are limited to "Detect and Prevent", retracting email after it has been delivered.

Avanan deploys before the inbox, able to hold a message until it has been scanned and determined to be safe.

Other API-Based Vendors Don't Protect, They React. Often, Too Late.

All API-based vendors, including Avanan, can retract a message if it is determined to be malicious after delivery, but this is dangerous if it is your ***only*** enforcement mechanism.



This is the difference between ***Protection*** and ***Response***.

Avanan offers **Protection:** preventing the malicious emails from reaching the end users.

Other vendors offer **Response:** removing the email after it has already been delivered, typically after 30 seconds or more. For new, zero-day threats or malware that requires additional analysis, the delay can be measured in minutes or require manual intervention which could take much, much longer.

This delay gives far too much time for a user to click on a malicious message. According to the Verizon Data Breach Investigation Report:

- In 93% of data breaches, compromise occurred in minutes or less
- The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds

CESS vendors emphasize their “low response time” and the "simplicity of an administrator to respond to threats." Any response time greater than zero is too long. A manual response is too late.

Worse, these response times grow even longer in large deployments.

Other API-Based Vendors Do Not Scale

The problem that other API-based vendors have not been able to solve is scalability. Their response time is directly correlated to the size of the environment. More users and greater email volume lead to more simultaneous API calls which lead to longer response delays resulting in a greater window of opportunity for users to click on a malicious email.

The response times promoted in sales and marketing literature reflect ideal conditions in small environments. During peak times of day, when users are busiest and most likely to be fooled by a phishing attack, response times grow longer. Five minutes, ten minutes. Even a few seconds is a security risk.

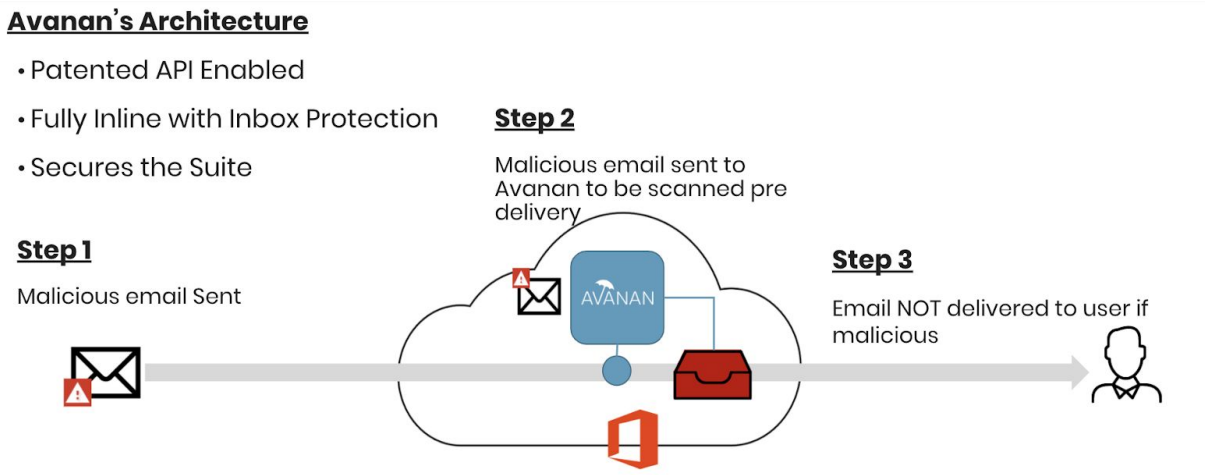
The problem of scalability has reduced other vendors in the Cloud Email Security Supplement market to small and medium businesses of just a few hundred users, limiting their funding and relegating them to a niche in the greater email security market.

Avanan is the only vendor that can offer CESS capabilities at scale.

Avanan: Integrated Cloud Email Security

Avanan's patented email security solution combines all the benefits of a Cloud Email Security Supplement with the true, ***pre-inbox*** security of a Secure Email Gateway (SEG).

The architectural difference is significant. It is a hybrid of API-based and pre-inbox technologies.



The Avanan infrastructure is API-enabled, with patented technologies that offer very unique advantages over both SEG and CESS vendors. Specifically Avanan's patent allows us to *prevent the delivery of* ***malicious emails before the inbox*** as well as deliver all the benefits of ***internal email protection and post-delivery enforcement.***

This architecture not only blocks malicious email before the inbox, it is able to do it at scale, protecting companies of all sizes, from 25 to 250,000 users or more.

Avanan offers all the capabilities of a **Secure Email Gateway**

- Pre-inbox protection, scanning and quarantining before the inbox,
- URL replacement for post-delivery link protection,
- Malware sandboxing, threat-feed filtering,
- Enterprise-grade security.

Avanan offers all the capabilities promoted by **Cloud Email Security Supplements**, but does so ***at scale.***

- Business Email and Email Account Compromise (BEC/EAC) Protection
- Internal email protection,
- Post delivery retraction of messages later deemed malicious,
- Post-attack forensics and response,
- Ease of installation.

Avanan also offers capabilities that ***neither*** category of vendor can provide:

- Outbound email protection for both malware and data leakage.
- Historical analysis of a year's worth of email to protect against BEC attacks
- Protection for the rest of the Microsoft or Google Suite including file sharing, Teams or Slack, Data Leak Prevention and more.

These are the reasons that Avanan was named as a Gartner's Peer Insights Customer Choice for email security.

Conclusion

Avanan pioneered the use of APIs to protect email and watched with keen interest as others have tried to follow.

The unique vantage point has allowed us to observe what works and what doesn't. It's clear that Pure API-based vendors are limited in the type of protection they can offer.

Only Avanan, with its patented, hybrid, integrated approach can prevent the delivery of malicious emails to the inbox, as well as secure the entire business suite.

Email security will continue to migrate to the cloud and will often be API-based, particularly as the world moves away from legacy Secure Email Gateways.

You need an API-based solution but you need one that works at scale. Look to the creators of the solution. Look to those that continue to innovate.