Avanan's Secret Sauce

Background

This is a story we've heard from quite a few of our customers: When they asked their previous email security vendor why an attack was missed, they would get a canned response. "We cannot tell you, it's our 'secret sauce'". So, we decided to share some of our 'Secret Sauce', to help you understand how we catch what others miss.

When a vendor tells you it's their secret sauce, there's probably not much behind it

The Key: Protecting From the Inside

Avanan's patented, artificially intelligent (AI) software is embedded within your cloud email provider - Office 365 or Gmail, behind the default security, whether that's EOP or if you upgraded to ATP or use another security solution. This positioning allows our AI engine to add security and to be trained specifically on the attacks missed by default security.

1. **Adding a layer of security vs replacing it.** Email security solutions that are deployed as gateways in front of cloud email (SEGs) require you to practically disable the built in security layer. We have demonstrated in prior blogs how attacks that would have been blocked by the default Office 365 security, end up getting through to your inbox if you put Proofpoint in front of it. That's because Microsoft was disabled and Proofpoint missed the attack (Can 1+1=0?). With Avanan, we add another layer—the default security scans first and then Avanan scans the things it might have missed. Layered security is the best practice because two independent layers are exponentially harder to bypass. In addition, our weekly reports will provide a unified experience with all phishing detected and by which layer.

2. **Trained specifically on what previous layers missed.** In Machine Learning, the training set you select is the single most important component to what the AI would identify. Avanan's unique deployment and visibility gives Avanan a significant advantage over SEG: our AI is specifically trained on real attacks that were missed by the default layer. By focusing the AI on such attacks it becomes extremely efficient at catching the attacks that the first layer missed.

3. **Indicators of Attack to detect malicious intent.** As you might have seen from our attack briefs, Avanan is one of few vendors that consistently uncovers the hacking methods used by hackers to bypass Office 365 and Gmail built-in security. We know this because of how we deploy - after the default layer. By reverse engineering the reason the attack was missed by the default layer, we have consistently uncovered new sophisticated obfuscation methods that hackers use. For Avanan, we don't just make sure we are not vulnerable to these attacks—we use these methods as indicators of attack to determine and flag those emails or links. With several hundred live vulnerabilities in Office 365 and Gmail security that are being used by hackers, Avanan is capable of

flagging and blocking some of the most sophisticated hackers. SEGs are blind to a large number of attack indicators because they have no idea what would or wouldn't pass Office 365. With an SEG, you have to change your MX record, so hackers know what you use for email security. That means they can focus on attacks that bypass your SEG vendor.

This is why Avanan is a real 1+1=3: an additional layer designed specifically to catch the attacks that the first layer misses.

Additional Advantages In Avanan's Deployment Method

The above explained how we provide superior catch rates and detect the attacks others miss. There are several additional advantages to this approach:

1. **Ease of deployment.** Avanan does not require you to change the MX record or to apply any manual configurations to Office 365 or Gmail. All you have to do is approve our application with a global admin (in O365 or Gmail) and you are done. This one-time process literally takes one minute.

2. **Avanan has more context for accurate anti-phishing and BEC protection:** Through the API, Avanan knows a wealth of information that is not available in the legacy SEG model. For example:
    a. End-user titles: We know the CFO, CEO, COO is—and these are the people most likely to be impersonated in a BEC attack.
    b. Historical correspondence: We analyze who communicates with who, at what frequency, and with what email subjects and content.
    c. Login history for specific users

    This rich context allows Avanan's AI to build a social graph for better detection and low false-positive rates of phishing attacks. It also allows Avanan to establish each end-users' behavioral baselines to flag suspicious activities by compromised accounts or insider threats.

3. **All email protection, not just inbound:** Unlike Secure Email Gateways, Avanan is able to protect against phishing and other attacks from internal emails, utilizing a specialized AI model for scanning internal traffic, with relevant

indicators for internally-originated attacks. This is in addition to securing inbound and outbound emails.

4. **Protection for the entire suite, not just email:** Business doesn't just happen in email and so full-suite security needs to extend to all platforms where work is done. Our security solution extends to the collaboration suite, identifying potentially compromised accounts to protect OneDrive, SharePoint and Teams in Office 365, to Google Drive in G-Suite, and beyond the main collaboration suites to Slack, Box and Dropbox. All SaaS apps get unified security scanning, similar policy language and centralized workflows.

Inline via API

Avanan's patent is in the ability to deploy an API solution that is fully inline - the email never reaches the end-user until Avanan clears it. This unique capability is what allows Avanan to enjoy all the above, while also able to completely replace the SEG as your email solution. Unlike the other API solution, Avanan is not a supplement, Avanan is the new email security alternative for the legacy SEG architecture.