Solution Comparison

Office 365 Advanced Threat Protection

VS

Avanan

AVANAN

The Cloud Security Platform

NOVEMBER 2017

Avanan

The Avanan Cloud Security Platform protects the full Office 365 environment including Outlook.com, One Drive, Teams, Azure and the Office Apps in a way that is seamless to the user and combines policy controls into a single pane of glass.

Partnering with the industry's top security vendors, Avanan offers cloud-native versions of the most advanced technology to protect against malware, phishing, ransomware, data leakage, insider threats and more.

Microsoft Advanced Threat Protection

Office 365 provides a spam and phishing filter for every Outlook.com account, including a signature-based malware scanner. For companies that need more than the default layers of security, Microsoft offers its Advanced Threat Protection (ATP) for an additional $24 per user per year.

How Advanced Threat Protection Compares to Avanan

The most significant difference between Microsoft's ATP and Avanan's Cloud Security Platform is the scope of coverage. While ATP was built as an add-on feature for Outlook, Avanan was designed to be a comprehensive integrated security platform to orchestrate policy across multiple cloud applications. It protects more. It protects better.

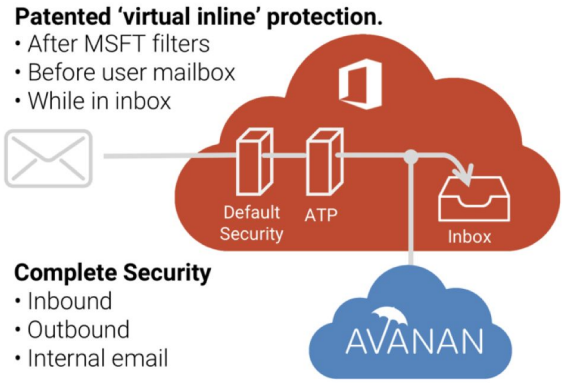
SaaS Protections	Office 365 Default	Advanced Threat Protection	AVANAN
Email Protection	Inbound	Inbound	Inbound, Outbound, Internal
SaaS Protection	Email Only	Office 365	Any SaaS/IaaS
Account Takeover Protection			✓

Avanan Protects All Email

Microsoft's security tools assume that the threat lies outside your domain, only scanning inbound email. Avanan monitors inbound, outbound and internal email to detect the insider threat before it spreads.

Avanan Protects All of Office 365 in One Window

Microsoft's default security is limited to email. For a long time, ATP had the same limitation, but in a recent announcement, Microsoft has revealed its plan to eventually extend ATP to SharePoint Online, OneDrive for Business and Teams because the threats extend beyond email. Unfortunately, its administration will separately embedded within each application, requiring individual configuration and management. Avanan has always offered its protection across all of Office 365 as a single pane of glass for policy and reporting



Avanan Offers Account-Takeover Protection

Microsoft offers very little protection after the breach. Because Avanan is so tightly integrated with the full Office 365 Suite, it can correlate login information, policy edits, file activity, data shares or other anomalous behavior across the entire suite, or even across multiple SaaS, identifying the insider threat and blocking malicious behavior before it happens.

Advanced Phishing Protection

Avanan's Phishing Protection goes far beyond the metrics used by most security tools, analyzing over 200 unique factors to identify a malicious message.

Phishing Protections	Office 365 Default	Advanced Threat Protection	AVANAN
Spam	✓	✓	✓
Domain Spoofing		✓	✓
Brand Impersonation			✓
User Impersonation			✓
Business Email Compromise			✓

Domain Spoofing is a Minimum

The simplest attacks attempt to spoof your domain but you have access to this protection only when you upgrade to Advanced Threat Protection.

Brand Impersonation

Beyond spoofing your domain, attackers will attempt to spoof the domain of trusted brands like FedEx or Amazon. Avanan identifies email that might spoof the domain, images, the language or just the look and feel of the most likely spoofed companies on the internet.

User Impersonation

With its complete API integration, Avanan gets to know your employees by name and role, making it possible to identify messages that are attempting impersonate a real person.

Business Email Compromise

Using the multi-factor spoof detection data, advanced contextual analysis can identify messages that might exploit human nature to reveal confidential information or worse. Tight integration with the inbox makes it possible to interact with the user to second-guess suspicious conversations.

Multi-layer Malware Detection

Avanan has partnered with over 60 of the industry's most advanced security vendors to cloudify and containerize their most advanced detection tools. Each and every message is scanned in parallel so that additional security does not add additional latency.

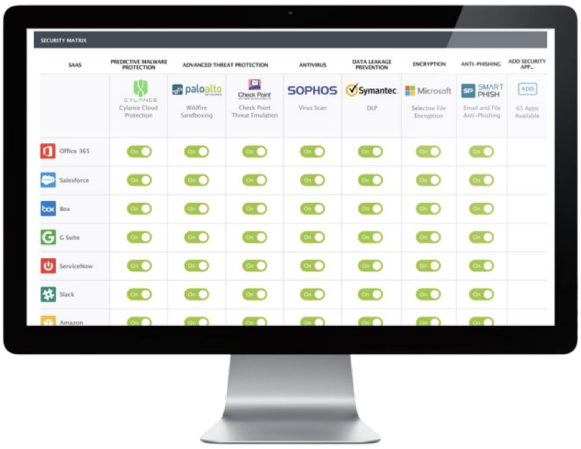
Malware Protections	Office 365 Default	Advanced Threat Protection	AVANAN
Antivirus Signatures	✓	✓	✓
Sandboxing		✓	✓
Active Content Analysis			✓
File Sanitization			✓

Antivirus Signatures

Signature-based antivirus is still a quick and easy way to screen the most common attacks. Avanan works alongside Microsoft's default security to block what is misses. Because many AV solutions subscribe to the same real-time databases that Microsoft uses internally, Avanan seeks out vendors that offer results above and beyond those lists.

Malware Sandboxing

Emulation analysis has become the de facto minimum standard for security as zero-day malware bots can generate millions of unique versions to bypass signature-based tools. For Office 365 users, this requires an upgrade to ATP. On the Avanan platform, users are protected with advanced technology from companies like FireEye, Check Point, Palo Alto and Lastline.



Active Content Analysis

The next generation of malware detection eliminates the delay that often prevents customers from deploying sandboxing tools. Vendors like Cylance and Solebit use machine learning and other algorithmic science to provide an instant evaluation.

Avanan uses all three categories of malware analysis in parallel, analyzing the results with a machine-learning supervisor that incorporates the threat score from each tool. This provides a detection rate that no single vendor can offer.

URL Protection

Most phishing attacks incorporate a link to a malicious web page, file or form, often hidden behind legitimate sites or redirects from trusted domains. They are the most difficult to identify because the malicious content is remote and under the control of the attackers.

URL Protections	Office 365 Default	Advanced Threat Protection	AVANAN
Domain Reputation Filter	✓	✓	✓
Malicious File Analysis		✓	✓
Page Emulation Analysis			✓
Brand Spoof Analysis			✓
Active Form Analysis			✓

Domain Reputation

By default, Microsoft analyzes the root of the URL to determine if the domain is blacklisted. With Advanced Threat Protection, Microsoft will follow the link, through redirects and other misdirections to determine if the target page is on a blacklisted site or leads to a file download. Avanan also actively follows redirected links and supplements the domain analysis with a variety of other blacklist databases.

Malicious File Analysis

If the link leads to a file download, Advanced Threat Protection will analyze it using its own AV and sandboxing tools. Similarly, Avanan analyzes each file with its suite of malware tools—AV, sandboxing, and advanced AI—to test a link before it reaches the inbox.

Page Emulation Analysis

Advanced Threat Protection does no analysis beyond domain reputation and file analysis. Avanan, however, will analyze the pathway and resulting pages to look for phishing design and behavior.

Brand Spoof Analysis

In the same way Avanan identifies an email that pretends to be from a trusted brand, page emulation looks for logos and language that might fool a user into believing they are on a trusted site. A site that looks like eBay but isn't eBay.com is suspicious.

Active Form Analysis

If the resulting page includes a form, Avanan will identify look-alike content and malicious code. If a page looks like a Microsoft login but the form posts to an unrelated site, it could fool a user into entering their credentials. Avanan prevents the link from even reaching the inbox.

Keeping Up with The Ever-Changing Threat

The number and variety of phishing attacks grow every year. No single company can hope to keep up, especially when the attackers can create methods to specifically bypass a particular technology.

As phishing attacks become increasingly sophisticated, Avanan actively seeks out new technology from both large and niche vendors to keep up with the changing threat. Our goal is to bring the full force of the entire security industry to build the most complete, most effective defense-in-depth security stack for email; for Office 365; for the cloud.