# Avanan Cloud Security
# for Office 365

## THREATS

### PHISHING
Avanan uses advanced AI and machine-learning models trained on attacks that get past Office 365, analyzing over 300 indicators per message. Deploys between the inbox and native security to secure inbound, outbound and internal email from the most sophisticated attacks that evade Microsoft.

### ZERO-DAY MALWARE & RANSOMWARE
Multiple real time malware, sandboxing, and A.I. active-content analysis tools work in parallel to identify and stop ransomware and malicious content.

### ACCOUNT TAKEOVER / INSIDER THREAT
Avanan analyzes every user event across multiple SaaS, comparing historical behavior, anomalous activity, and profiles of real-world breaches to identify attacks in real time.

## DATA SECURITY

### DATA LEAK PROTECTION
Identify confidential data using industry-leading tools. Enforce regulatory compliance (PCI, HIPAA, SOX, etc.) across all your SaaS with cloud-aware, context-sensitive, policy work flows.

### POLICY-BASED ENCRYPTION
Automate the encryption of sensitive files — whether shared internally, via email, or public share — without deploying new infrastructure, using the protocols you already know and trust.

## GOVERNANCE

### SHADOW IT
Identify risky cloud services your employees are using in the office or at home that have been connected to your approved SaaS accounts, without redirecting traffic or using a proxy.
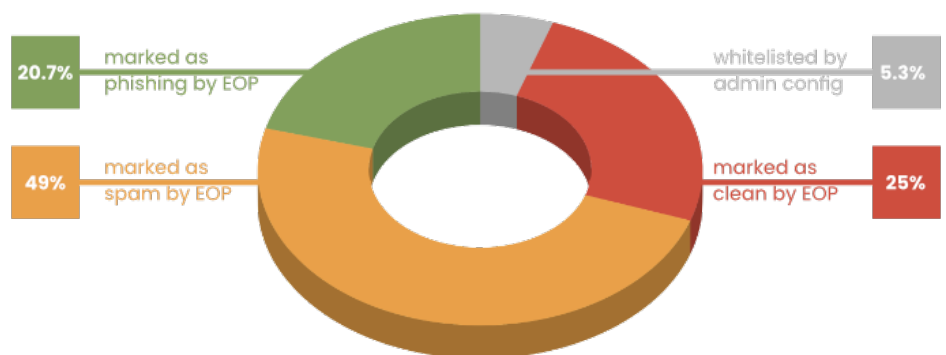
### SIEM INTEGRATION
Avanan correlates user and file events from all SaaS, combining them with real-time reports of the security stack, so you can monitor the cloud with your existing SIEM.

*If you're using Office 365, should seriously consider Avanan's email security. Don't wait until you're under attack. The included Microsoft email security is not sufficient. You need something like Avanan.*

*— IT Administrator, Information Services*



20.7% marked as phishing by EOP

whitelisted by admin config 5.3%

49% marked as spam by EOP

marked as clean by EOP 25%

30.3% of phishing emails sent to organizations using Office 365 EOP were delivered to the inbox.

Avanan offers complete, defense-in-depth security for Office 365, whether you use SharePoint, OneDrive, Teams, or the full collaboration environment.

Scan every inbound, outbound and internal email. Prevent phishing, malware and ransomware from spreading within your organization or to your customers and partners.

Check every file and message for malicious content using the most advanced sandboxing and active-content analysis in the industry. Quarantine threats before your users download them.

Identify confidential information and apply context-aware policies that confine the data to a particular organization or work group. Your users can leverage the full power of Office 365 collaboration, while automated work flows enforce regulatory compliance, ensuring PCI, HIPAA, PII, or other protected content does not leak.

Avanan is the best way to ensure seamless security. Deploy instantly with the only one-click, cloud-enabled platform, with no need for a proxy, appliance or endpoint agent.

# AVANAN
# Protect Office 365 from **the inside**

Catch the sophisticated attacks that default and advanced security tools miss, while adding an invisible layer of security for cloud-based collaboration suites.

A multi-layer, artificially intelligent solution, Avanan deploys in minutes and scales across enterprise architectures to prevent the attacks that bypass conventional security solutions.

## Full-Suite Protection

Manage data leakage, malware, and account takeover via a single threat intelligence interface. Robust protections extend to file-sharing and chat.

## Patented technology built specifically for the cloud

Avanan connects to your environment via API and scans for threats after your existing security — but before the inbox. It is laser-focused on advanced attacks like ransomware and BEC, while also filtering out spam and greymail.

Secure Email Gateway    Default Security    AVANAN
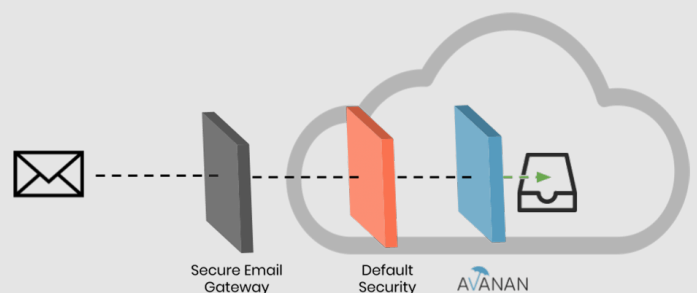
*"Avanan was so quick to deploy; we just checked the boxes of the security stack we wanted to incorporate, and almost immediately, we observed the phishing attacks and malware it was catching."*

Jim Nonn, CIO, Egan Company