Abnormal Security

White Paper

Closing the Email Security Gap in Your Modern O365 Email Infrastructure

Contents

Introduction

In today's cloud-first approach to managing corporate infrastructure and running applications, more than 56% of organizations globally now use Microsoft Office 365 (O365).[i] This has supported an agile and fluid way of doing business.

The move to O365 also allowed companies to streamline their email security investments. Rather than licensing an on-premises Microsoft Exchange server and a separate secure email gateway (SEG), companies were able to move to the cloud with O365 and the included email security provided by Exchange Online Protection (EOP). Overall, this approach has provided companies with a good email security posture.

But, as it does, the email threat landscape has continued to evolve, and when it comes to managing email security as part of their O365 investment, organizations are now experiencing greater challenges ensuring targeted email attacks, phishing, business email compromise (BEC), and other email risks don't reach users' inboxes. In fact, the FBI reports that BEC has cost enterprises a staggering amount of money, reaching $26 billion over a three-year period.[ii]

The best email protection solution should supplement the existing investments, and not duplicate them or render them ineffective.

As companies look to improve their approach to shore up their email security risks with their O365, it's important to start by identifying current email security capabilities the company has in place based on their O365 investment. The best email protection solution should supplement the existing investments, and not duplicate them or render them ineffective. Simply adopting another SEG solution again means companies are "double paying" for the same capabilities and are not achieving security budget efficiencies.

Furthermore, companies should consider an architectural approach for email protection that best complements the cloud-native O365 model. The ideal architecture will take a cloud API approach that preserves the benefits the company has gained by adopting cloud-based email.

This paper reviews the capabilities Microsoft offers for firms who have adopted Exchange Online Protection or Advanced Threat Protection and narrows down the required, supplementary email protection capabilities, as well as investigates the merits of an API-based architecture that provides seamless cloud integration with O365.

[io] PTG. Microsoft Office is Being Adopted at an Enormous Rate. April 2019.
[ii] TechTarget. FBI says $26B lost to business email compromise over last 3 years. September 2019.

Microsoft Exchange Online Protection

Even with the expanding communication mediums available to companies today, email remains the bedrock of corporate communication. Cybercriminals know this, and they have spent years creating a multitude of email attack methods. In turn, the security industry has built a strong foundation of email security capabilities that are thorough and comprehensive.

Microsoft incorporated a worthy library of these capabilities in their O365 business offerings, which enabled companies to move away from their perimeter secure email gateway (SEG) when they adopted O365.

Microsoft Exchange Online Protection

Companies pay for Exchange Online Protection (EOP) as part of the O365 business packages that include email hosting services, such as O365 Business Essentials, O365 Business Premium, E1, E3, and E5. Microsoft describes EOP as a solution that protects organizations against spam, malware, and safeguards the organization from messaging-policy violations.

The investment in EOP with O365 email hosting provides the following email security capabilities:

Connection filtering	Checks the sender's reputation and applies IP Allow and IP Block lists.
Anti-malware	Inspects the message for malware using multiple anti-malware engines and inspects payload in message body and attachments.
Content filtering	Content is checked for terminology or properties common to spam and applies malicious URL block lists. Anti-phishing protection with 750,000 domains of known spammers.
Mail routing and connectors	Conditional mail routing. Opportunistic or forced TLS is available with connectors.
SLAs	5 financially backed SLAs, including protection from 100% of known viruses and 99% of spam.

For more information about EOP, visit Microsoft EOP features.

Microsoft Exchange Online Protection

O365 Advanced Threat Protection

O365 Advanced Threat Protection (ATP) is available as an add-on purchase and is included as part of the E5 business package. ATP expands on the email security capabilities provided in EOP to support additional protection capabilities, plus automated response, and attack simulations to build user awareness. Microsoft describes ATP as a solution that protects organizations from sophisticated threats, such as phishing and zero-day malware, and enables companies to automatically investigate and remediate attacks.

With ATP layered on top of the company's O365 email hosting investment, they gain the following:

Safe attachments	Performs dynamic malware analysis to protect the organization from malicious attachments.
Safe links	Provides time-of-click verification of web addresses (URLs) in email messages and Office documents.
ATP for SharePoint, OneDrive, and Microsoft Teams	Identifies and blocks malicious files in Microsoft Teams sites and document libraries.
Advanced anti-phishing protection	Applies machine learning models and advanced impersonation-detection algorithms to avert phishing attacks.

For more information on ATP, visit Office 365 Advanced Threat Protection.

Even with the expanding communication mediums available to companies today, email remains the bedrock of corporate communication.

Supplementing O365: Ideal Approach to Close the Gap Against Advanced Email Attacks

To address the advanced email protection needs, companies will achieve greater security budget efficiencies by selecting a solution that augments the email security capabilities they already have in their EOP and/or ATP investments. Again, the goal here is to select a solution that does not duplicate these capabilities or render them ineffective.

API vs. SMTP architecture

To achieve that objective, companies will be better served by an API-based solution that integrates with O365 rather than re-adopting an SMTP security gateway. A secure email gateway sitting in front of EOP, makes EOP connection filtering and detection capabilities ineffective. In fact, many SEG vendors will often recommend disabling features of EOP in order to ensure functional compatibility.

In contrast, an API architecture enables EOP to continue functioning exactly as it was designed. The API-integration will purely provide an additional layer of protection to address the continued risk of advanced email attacks, without diminishing or impeding EOP's capabilities.

Feature duplication

In addition to the architectural approach, the other equally important consideration is maximizing the security budget efficiencies by ensuring that the steps taken to address the email protection requirements limit duplicating capabilities that are already provided in EOP and ATP.

The chart below provides a helpful inventory review of general email protection categories to identify if or where an API or SEG solution will duplicate a company's existing EOP and ATP investments.

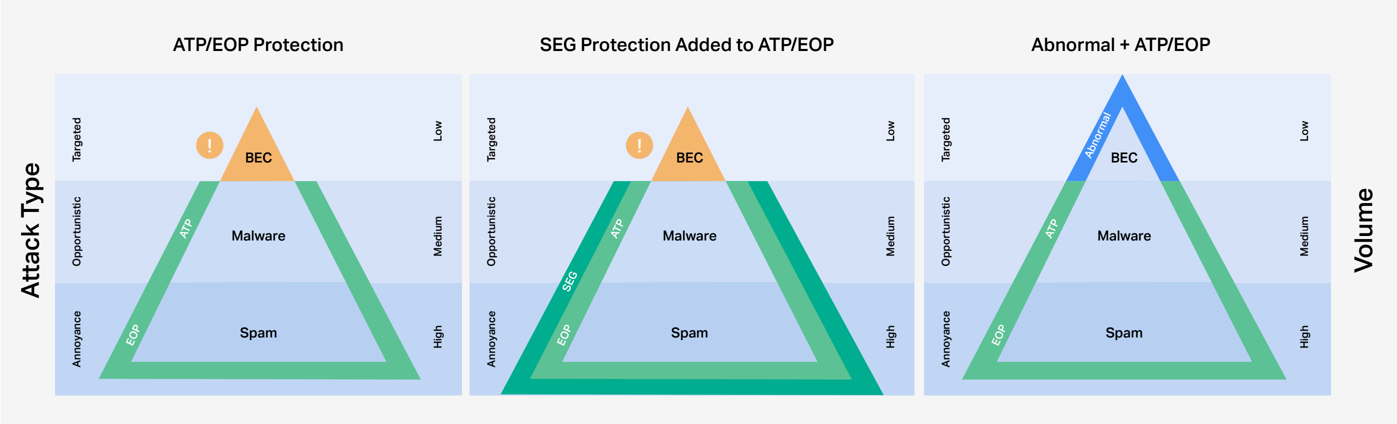


Figure 1: Organizations add SEG's to their O365 investments that include EOP & ATP, resulting in incrementally better protection against spam and malware, but leaves targeted attacks such as BEC largely unaddressed. While low in volume, left unabated, these targeted attacks represent a tremendous financial risk to the organization. Prioritizing a solution to address the targeted attacks provides the highest impact and potential ROI.

Ideal API Effectiveness Approach: Data Science

When companies evaluate API-based email protection solutions, effectiveness is, of course, an essential requirement.

Given EOP and ATP apply modern threat intelligence approaches, companies should “shore up” EOP and ATP with an email security solution that uses a different approach, like data science, rather than simply using a variation of the same threat intelligence technique.

Different threats require specialized detection techniques. The greatest email compromise threats impacting organizations today are socially engineered threats that are sneaking by reputation systems (e.g., Microsoft: Connection Filtering) and do not contain malicious payloads (e.g., Microsoft: Anti-Malware and ATP). Simply adding better versions of reputation and malware scanning engines won’t address the root cause of the problem.

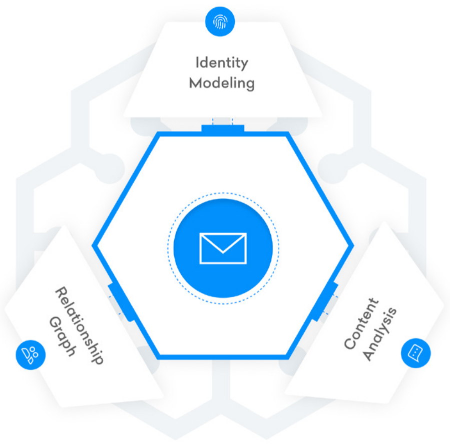
A data science approach, looking beyond data within the email, adds context to the analysis of email communications. Understanding why two people are communicating is as important as what they are communicating. A textbook example of a BEC attack uses standard business language, targeted at individuals with relevant topics. Detection of these attacks requires an approach to understand the differences between legitimate business communications and malicious ones. Most importantly, a data-science approach perfectly augments the threat intelligence approaches that EOP and ATP take.

The email protection solution’s detection capabilities are foundational to adopting one with the greatest effectiveness. To that point, companies should conduct a proof of concept that deeply reviews how the vendor is performing email threat detection to validate the effectiveness.

Given EOP and ATP apply modern threat intelligence approaches, companies should “shore up” EOP and ATP with an email security solution that uses a different approach, like data science, rather than simply using a variation of the same threat intelligence technique.

Abnormal Security: Effective Data Science in Action

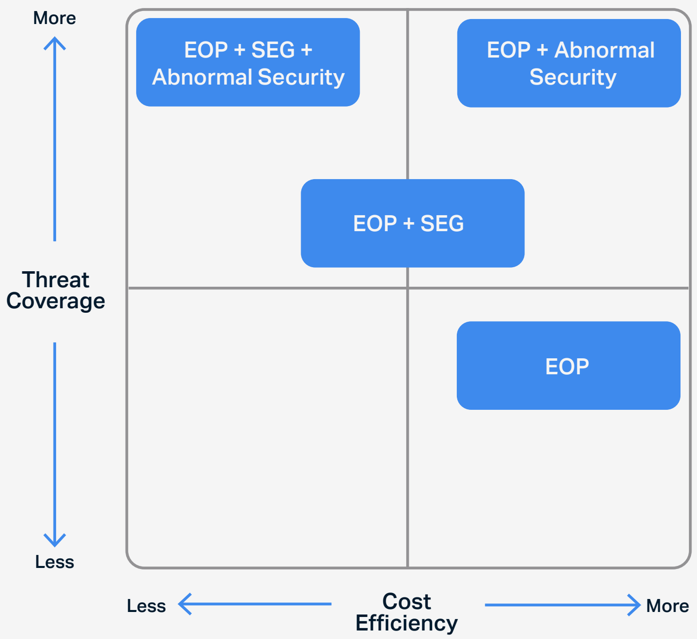
Abnormal Security applies Abnormal Behavior Technology (ABX), which takes a unique data science-based approach. Using an API that directly integrates with O365, ABX looks beyond email data and redefines the scope of behavioral analysis. ABX analyzes dozens of data sources specific to each organization to arrive at high-confidence decisions to block BEC and other targeted email attacks.



The roots of ABX derive from experience within the advertising technology space, where data scientists honed their craft analyzing user behaviors. With data beyond just email available via platform APIs from Microsoft Office 365 and Google G Suite, organization specific inputs can be leveraged to understand baseline behaviors of users and organizations, both internal and external. ABX can then identify abnormal behaviors indicative of attacks.

ABX analyzes the rich data from dozens of data sources to profile communications across three distinct perspectives: identity modeling, relationship graph, and content analysis. For further about the Abnormal Security data science approach, read the ABX: Abnormal Behavior Technology whitepaper.

Maximize Security Coverage and ROI



Organizations have migrated their infrastructure to O365 to maximize operational efficiencies. When organizations feel the need to improve their email security capabilities, the return to an SEG may incrementally improve the threat coverage, but negatively, and heavily, impacts the cost efficiency due to the feature duplication discussed earlier.

Many organizations continue to suffer from a gap in coverage against email threats and add a third solution into their email security stack, providing comprehensive coverage against the whole spectrum of email attacks.

The optimal approach for comprehensive threat coverage with the highest cost efficiencies lies with solutions that focus on augmenting the native capabilities of Microsoft, not replacing them.

Conclusion

As organizations pursue a new paradigm for protection against advanced email threats that provides the greatest efficiencies with their O365 architecture and existing EOP and/or ATP investments, they should turn to a solution with an API-based architecture that uses data science to maximize security coverage and return on investment.

Abnormal Security delivers on that promise with the next generation of email security. Using a simplified, cloud-native architecture that seamlessly integrates with O365 and applying a unique data science-based approach, Abnormal Security provides comprehensive email protection, detection, and response.

About Abnormal Security

The Abnormal Security cloud email security platform protects enterprises from targeted email attacks. Powered by Abnormal Behavior Technology (ABX), the platform combines the Abnormal Identity Model, the Abnormal Relationship Graph and Abnormal Content Analysis to stop attacks that lead to account takeover, financial damage and organizational mistrust. Though one-click, API-based Office 365 and G Suite integration, Abnormal Security sets up in minutes, requires no configuration and does not impact email flow. Backed by Greylock Partners, Abnormal Security is based in San Francisco, CA. Please visit www.abnormalsecurity.com and follow the company at @AbnormalSec.