Abnormal SECURITY

Augmenting Your Microsoft Office 365 EOP and ATP Email Security Infrastructure

Abnormal SECURITY

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). 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.[1]

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.

Abnormal SECURITY

WHITE PAPER

Microsoft email protection capabilities

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 applies IP Allow and IP Block lists
Anti-malware	• Inspects the message for malware using multiple anti-malware engines • 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 email protection capabilities cont.

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	Checks to see if email attachments are malicious, and then takes action to protect the organization
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 team sites and document libraries
Advanced anti-phishing protection	Applies machine learning models and advanced impersonation-detection algorithms to avert phishing attacks

For more information about EOP, visit Office 365 Advanced Threat Protection.

Augmenting O365: stopping 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. The goal 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.

Augmenting O365: stopping advanced email attacks cont.

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.

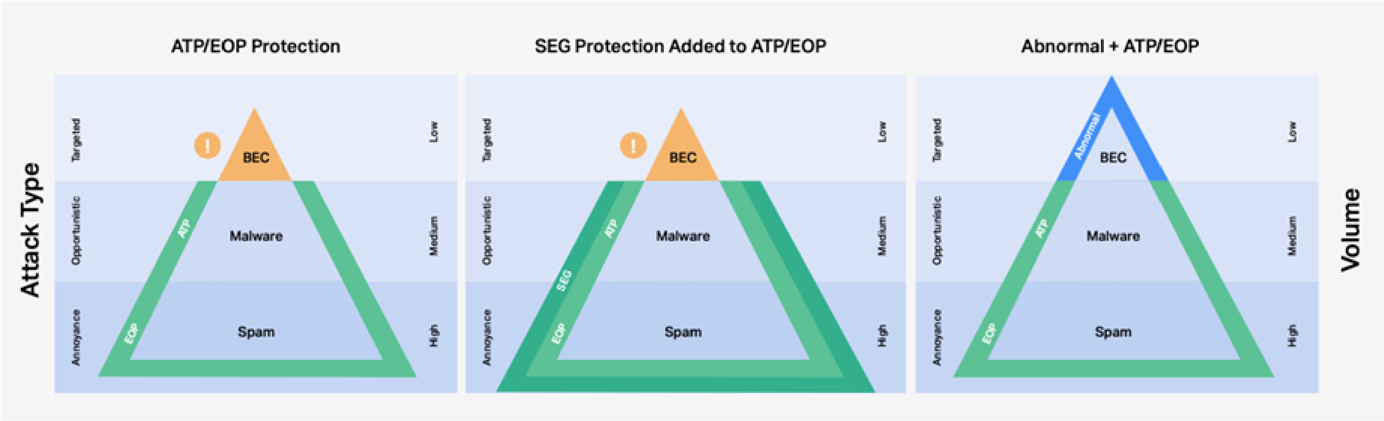


Figure 1: Organizations add SEG's to their O365 investments that include EOP & ATP, resulting in incrementally better protection against spam and malware, but leaves targeted attacks such as BEC largely unaddressed. While low in volume, left unabated, these targeted attacks represent a tremendous financial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

Abnormal Security: effective data science in action

By leveraging advanced AI and Natural Language Processing (NLP) techniques, Abnormal Security develops a deep understanding of the people in your organization and their behaviors. By analyzing and normalizing data across thousands of dimensions, Abnormal assembles a single, consolidated profile of every person, and understands the informal organizational hierarchy by observing communication patterns.

Abnormal Security uses three distinct ways to understand, analyze and protect organizations:

Cloud-Native API Architecture

Unlike email gateways, Abnormal integrates into Microsoft 365 APIs and deploys in seconds without disrupting mail flow. It leverages both email and non-email data (identity, calendar, contacts, collaboration tools, event logs, in addition to ERP, HRIS systems and more) and seamlessly integrates into your existing SIEM, SOAR, detection tools, and ticketing systems.

Business Insights

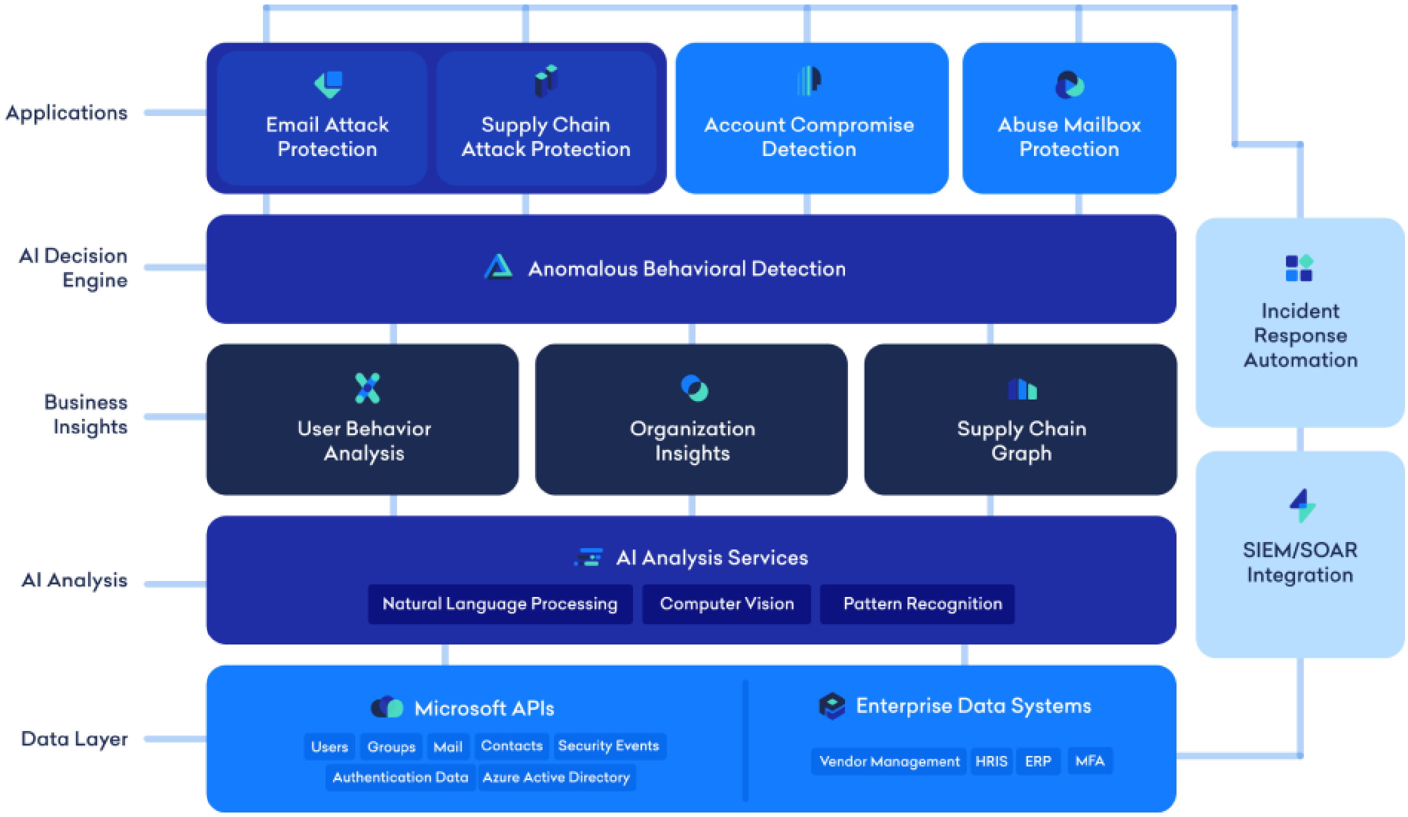
In creating a unified profile of each person, Abnormal maps the internal and cross-functional relationships and captures tribal knowledge of organizational processes. This extensive mapping has allowed Abnormal to create a global, federated supply chain graph of hundreds of thousands of business entities for real-time risk assessment of 3rd-parties.

Abnormal Security: effective data science in action cont.

Anomalous Behavior Detection Engine

Abnormal detects anomalies by comparing individual and sequences of events against behavioral norms to determine level of risk from threats that cannot be addressed by traditional gateways. Specifically, it stops socially engineered attacks from compromised accounts and includes explainable AI to ensure the results of the decision engine can be understood and trusted by your SecOps team.

With Abnormal, security teams protect employees from phishing attacks without the need for policy configurations, or manual review processes, giving your organization the most sophisticated and advanced email security solution on the market.



WHITE PAPER

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 is a solution that focus on augmenting the native capabilities of Microsoft, not replacing them.

Product	Capability	Secure Email Gateway	Office 365 EOP & ATP	Office 365 EOP & ATP + Abnormal
Unsolicited Mail	Spam	●	◑	●
	Graymail	◕	◑	●
Targeted Attack Protection	Malware/Sandboxing	●	◑	●
	Phishing/URL Analysis	◕	◑	●
	BEC/Payload-less/Fraud	◔	○	●
	Internal Phishing/Attacks	○	◔	●
Account Protection	Employee Account Compromise	○	◔	●
	Vendor Account Compromise	○	○	●
	Vendor Risk Assessment	○	○	●
SOC Platform	Post Delivery Remediation	◑	○	●
Multi-Channel	Microsoft Teams Protection	○	◔	●

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.

Learn More

For more information about Abnormal Security, visit: **www.abnormalsecurity.com**

About Abnormal Security

Abnormal Security is a next-generation email security company that protects enterprises from advanced targeted attacks including business email compromise. Abnormal Security's cloud-native architecture integrates directly into cloud office APIs and requires no configuration. Its innovative AI provides enterprises with an inside-out understanding of its people, organizational processes and the extended supply chain to stop targeted email attacks and detect compromised accounts. Backed by Greylock Partners, Abnormal Security is based in San Francisco, CA. More information is available at: www.abnormalsecurity.com.

Abnormal Security Corporation
797 Bryant Street
San Francisco, California 94107

www.abnormalsecurity.com