Abnormal

Augmenting Your Microsoft 365 EOP and MDO Email Security Infrastructure

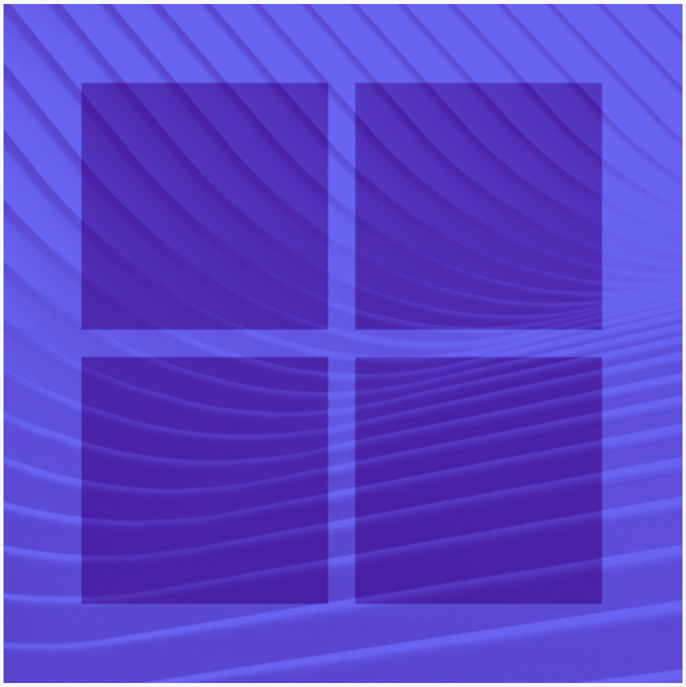


Table of Contents

Introduction

In today's cloud-first approach to managing corporate infrastructure and running applications, more than 56% of global organizations use Microsoft for email. Whether using Microsoft 365 (M365) or Office 365 (O365), this shift to the cloud has supported an agile and fluid way of doing business for more than 250,000,000 monthly users.

The move to the cloud has 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), organizations are able to use O365/M365 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 Microsoft 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.

As companies look to improve their approach and minimize their email security risks, it's important to start by identifying email security capabilities currently in place with Microsoft. The best email protection solution should supplement the existing investments, and not duplicate them or render them ineffective. Simply adopting another SEG solution 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 Microsoft 365 model. The ideal architecture will take a cloud API approach that preserves the benefits the organization has gained by adopting cloud-based email.

This paper reviews the capabilities Microsoft offers for organizations that have adopted Exchange Online Protection or Microsoft Defender for Office 365 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 M365.

$26B

Business Email Compromise

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 M365 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 Microsoft Office 365 Enterprise plans or Microsoft 365 business packages that include email hosting services, such as M365 Business Basic, M365 Business Standard, M365 Business Premium, E1, E3, and E5.

Microsoft describes EOP as a solution that protects organizations against spam and malware, and safeguards the organization from messaging-policy violations. The investment in EOP with M365 or O365 email hosting provides the following email security capabilities:

Connection Filtering	Checks the sender's reputation and applies IP safelists and IP blocklists.
Anti-Malware	• Inspects the message for malware using multiple anti-malware engines. • Inspects payload in message body and attachments.
Content Filtering	• Checks content for terminology or properties common to spam and applies malicious URL blocklists. • Provides anti-phishing protection for known spammers.
Mail Routing and Connectors	• Provides conditional mail routing. • Opportunistic or forced TLS is available with connectors.
Service Level Agreements (SLA)	Includes four financially-backed SLAs, including protection from 100% of known viruses and more than 99% of spam.

For more information about Exchange Online Protection, see the Microsoft EOP page.

Microsoft Defender for Office 365

Microsoft Defender for Office 365 (MDO), formerly known as Advanced Threat Protection or ATP, is available as an addo-on purchase and is included as part of the E5 or Defender for Office 365 (Plan 2) package. MDO expands on the email security capabilities provided in EOP to support additional protection capabilities, plus automated response and attack simulation to build user awareness.

Microsoft describes MDO as a solution that protects organizations against advanced threats to email and collaboration tools, including phishing, business email compromise, and malware attacks. Defender for Office 365 also provides investigation, hunting, and remediation capabilities to help security teams efficiently identify, prioritize, investigate, and respond to threats.

With MDO layered on top of the M365 email hosting environment, organizations gain the following:

Safe Attachments	Checks to see if email attachments are malicious and if so, takes action to protect the organization.
Safe Links	Provides time-of-click verification of web addresses (URLs) in email messages and Office documents.
MDO for SharePoint, OneDrive, and 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 based on the configured policies.

For more information about Defender for Office 365, see the Microsoft Defender page.

Augmenting M365: Stopping Advanced Email Attacks

To address the need for advanced email protection that will prevent the most dangerous and costly attacks, companies can achieve greater security budget efficiencies by selecting a solution that augments the email security capabilities already available with Microsoft EOP and MDO. The goal is to select a solution that does not duplicate these capabilities or render them ineffective, but instead augments them to provide greater protection.

API vs. SMTP Architecture

To achieve that objective, organizations will be best served by an API-based solution that integrates with M365, rather than re-adopting an SMTP security gateway. A secure email gateway sits in front of Exchange Online Protection, making the 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 native EOP capabilities.

Feature Duplication

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

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 MDO investments.

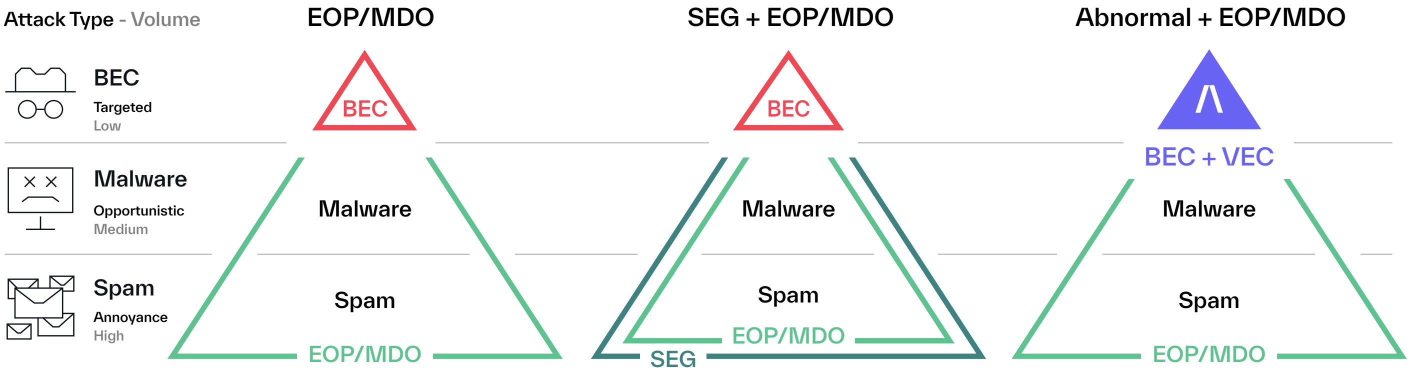


Figure 1. Organizations add secure email gateways to their M365 investments, resulting in incrementally better protection against spam and malware, but leaving targeted attacks largely unaddressed. Prioritizing a solution that stops these low volume but highly targeted socially-engineered attacks and takes advantage of native Microsoft capabilities 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 develops a deep understanding of the people in your organization and their behaviors. Abnormal analyzes and normalizes data across thousands of dimensions to assemble a single, consolidated profile of every person. The platform also observes communication patterns to understand informal organizational hierarchy and relationships between internal and external contacts.

Cloud-Native API Architecture

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

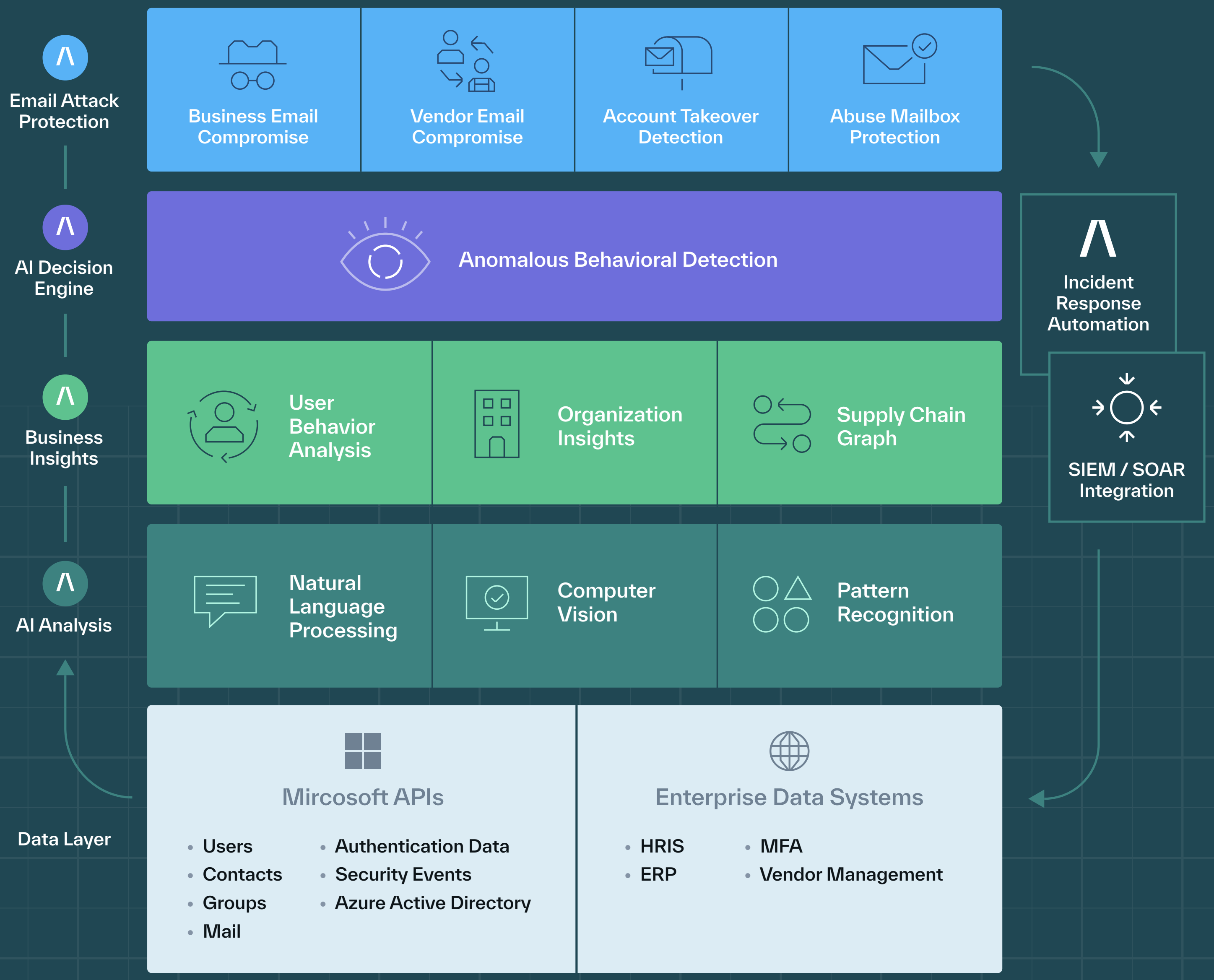
Business Insights

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 third parties.

Anomalous Behavior Detection Engine

Abnormal detects anomalies by comparing individual and sequences of events against behavioral norms to determine the 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 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.

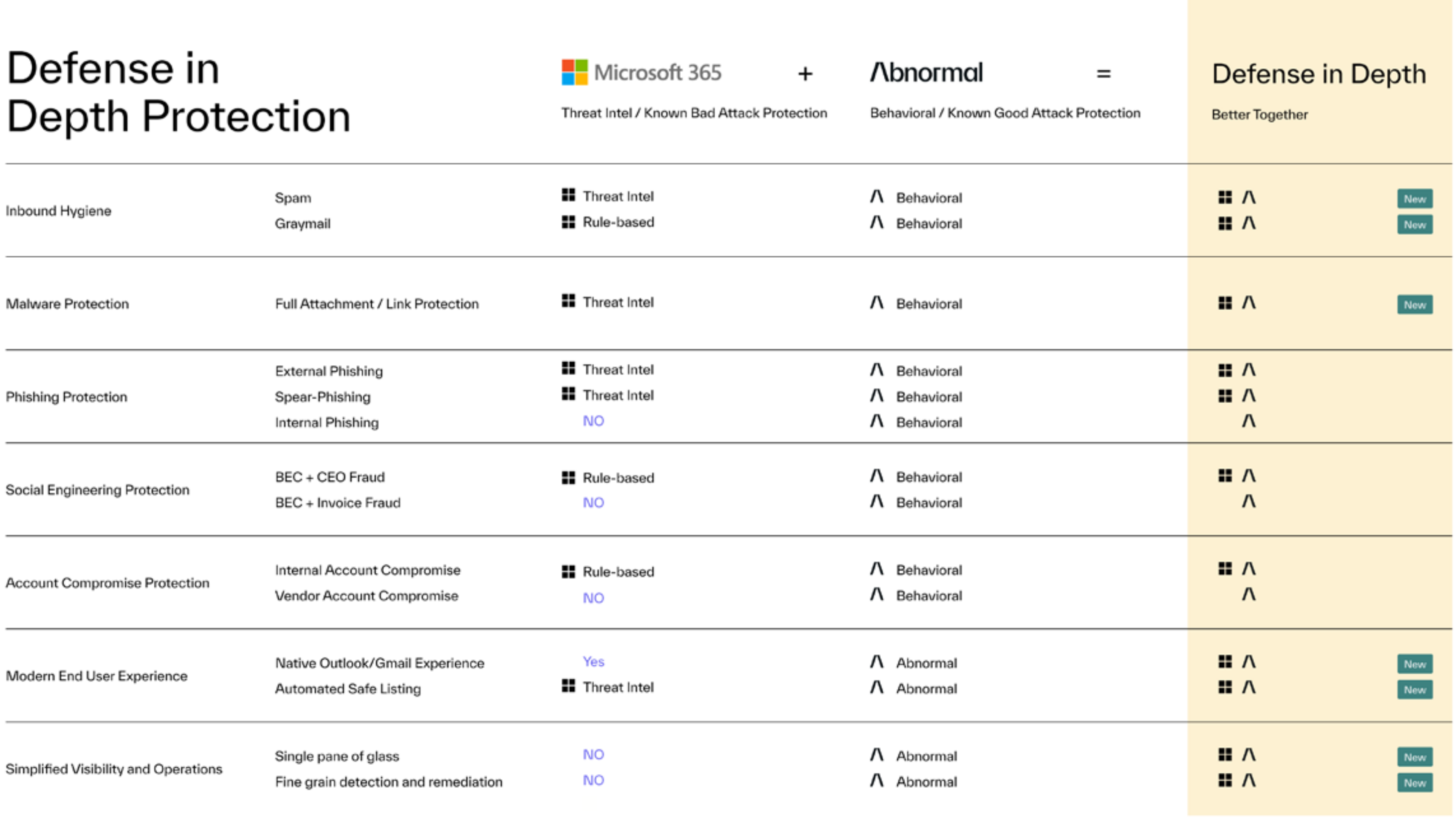


Maximize Security Coverage and ROI

Organizations have migrated their infrastructure to M365 to maximize operational efficiencies present in the cloud. When organizations feel the need to improve their email security capabilities, the return to an SEG may incrementally improve the threat coverage, but it also negatively and heavily impacts the cost efficiency due to feature duplication.

As a result, organizations continue to suffer from a gap in coverage against email threats and thus add a third solution into their email security stack, providing comprehensive coverage against the whole spectrum of email attacks. Abnormal can bridge this gap, providing extra coverage against the most dangerous threats, with or without a secure email gateway layer.

The optimal approach for comprehensive threat coverage is a solution that focuses on augmenting the native capabilities of Microsoft rather than replacing them.



Defense in Depth Protection		Microsoft 365 + Threat Intel / Known Bad Attack Protection	Abnormal = Behavioral / Known Good Attack Protection	Defense in Depth Better Together	
Inbound Hygiene	Spam Graymail	▦ Threat Intel ▦ Rule-based	Λ Behavioral Λ Behavioral	▦ Λ ▦ Λ	New New
Malware Protection	Full Attachment / Link Protection	▦ Threat Intel	Λ Behavioral	▦ Λ	New
Phishing Protection	External Phishing Spear-Phishing Internal Phishing	▦ Threat Intel ▦ Threat Intel NO	Λ Behavioral Λ Behavioral Λ Behavioral	▦ Λ ▦ Λ Λ	
Social Engineering Protection	BEC + CEO Fraud BEC + Invoice Fraud	▦ Rule-based NO	Λ Behavioral Λ Behavioral	▦ Λ Λ	
Account Compromise Protection	Internal Account Compromise Vendor Account Compromise	▦ Rule-based NO	Λ Behavioral Λ Behavioral	▦ Λ Λ	
Modern End User Experience	Native Outlook/Gmail Experience Automated Safe Listing	Yes ▦ Threat Intel	Λ Abnormal Λ Abnormal	▦ Λ ▦ Λ	New New
Simplified Visibility and Operations	Single pane of glass Fine grain detection and remediation	NO NO	Λ Abnormal Λ Abnormal	▦ Λ ▦ Λ	New New

Conclusion

As organizations pursue a new paradigm for protection against advanced email threats, they should look for one that provides the greatest efficiencies with their M365 architecture and existing EOP and/or MDO investments. To do so, 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 M365 and applys a unique data science-based approach, Abnormal Security provides comprehensive email protection, detection, and response.

Abnormal

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially-engineered and never-seen-before email attacks that evade traditional secure email gateways. Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, ransomware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com

Interested in Augmenting Your Microsoft Environment?

Request a Demo:

abnormalsecurity.com →

Follow us on Twitter:

@abnormalsec