Augmenting Your Microsoft 365 Email Security Infrastructure

SEPTEMBER 2025

Abnormal

Table of Contents

In the Microsoft 365 Era Email Security Has Entered a New Phase

$55B

lost in exposed losses to business email compromise since 2013.

88%

likelihood of being targeted by a BEC attack each week.

Only 1.46%

of employees report advanced text-based email attacks.

70%

of all Abnormal customers no longer use a secure email gateway.

In today's cloud-first approach to managing corporate infrastructure and running applications, more than a million organizations use Microsoft 365 for email, including more than 80% of the Fortune 500. The shift from on-premises to cloud-based email has resulted in increased employee productivity and a more agile way of doing business for more than 321 million monthly active users.

The move to the cloud has also allowed organizations to rethink their email security investments. With the on-premises email servers of the past, a secure email gateway (SEG) was nearly always required to prevent an onslaught of spam and opportunistic malware. However, the wide adoption of Microsoft 365 has enabled organizations to use the native security provided by Exchange Online Protection and the optional Microsoft Defender for Office 365 add-on—either standalone or in addition to a third-party secure email gateway.

Overall, this approach has provided companies with adequate email security posture. But as the email threat landscape continues to evolve, more sophisticated attacks are now reaching end users. Despite advances in security tools and an increase in end-user awareness, business email compromise and other socially-engineered attacks are still seeing success with $2.8 billion in exposed BEC losses in 2024 alone.

The Need for AI-Native Protection

So how can security leaders better protect their organizations without spending more money? SOC teams can start by identifying the native email security capabilities in Microsoft 365 and assessing where legacy tools overlap.

To strengthen protection and streamline budgets, additional email security solutions should complement Microsoft's native features rather than duplicate or disable them. This paper examines Microsoft's current capabilities and explores the value of supplemental approaches to email security.

Email Protection Capabilities in Microsoft 365

Despite the rise of collaboration platforms, email remains a critical channel for enterprise communication—and the most frequently exploited entry point for cyberattacks. Threat actors continue to perfect their tactics with the help of AI, exploiting the trusted nature of email to bypass legacy defenses.

In response, Microsoft has embedded a broad set of email protection capabilities into its Microsoft 365 platform, enabling organizations to reduce reliance on traditional secure email gateways (SEGs). Whether adopted from the outset or added over time, these native tools now form the baseline of many organizations' email security stacks.

Microsoft Exchange Online Protection

Exchange Online Protection (EOP) is included in all Microsoft 365 Enterprise plans. For smaller organizations, it is included in all Microsoft 365 Business packages that include an Exchange Online mailbox.

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 email hosting provides the following email security capabilities:

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

Category	Description of Features
Protection	Includes anti-malware, anti-phishing, anti-spoofing, and inbound/outbound anti-spam policies, as well as connection filtering, block/allow lists, and edge blocking.
Quarantine and Submission	Includes capabilities like admin and user submissions, admin and user quarantine, and add-ins for reporting messages or phishing.
Mail Flow	Includes features such as transport rules, accepted domains, connectors, and skip listing.
Monitoring	Includes features such as message tracing, email and security reports, and audit logging.
Service Level Agreements (SLA)	Includes multiple financially-backed SLAs, including protection from 100% of known viruses and 99% or greater filtering efficiency against spam.

Microsoft Defender for Office 365

Microsoft Defender for Office 365 (MDO) is available as an add-on purchase in one of two plans (Plan 1 and Plan 2), or as part of the E5 license.

While EOP protects against high-volume known attacks, MDO P1 adds additional capability to protect email and collaboration tools against zero-day malware, phishing, and business email compromise. MDO P2 extends even further to add investigation and response capabilities alongside simulation and training.

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

Category	Description of Features
Prevention and Detection	Includes features such as Safe Links and Safe Attachments, protection for workloads, time-of-click protection, advanced anti-phishing, and user and domain impersonation protection.
Investigation	Includes features such as SIEM integration API for detections, real-time detections tool, and URL tracing. Additional features available in P2 include threat explorer and trackers and campaign views.
Response	Includes automated investigation and response from threat explorer and compromised users, as well as a SIEM integration API for automated investigations.

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

Augmenting Microsoft 365 to Stop Advanced Email Attacks

To address the need for advanced email protection that will prevent the most dangerous and costly attacks, companies can achieve greater budget and operational 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.

Choosing the Right 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.

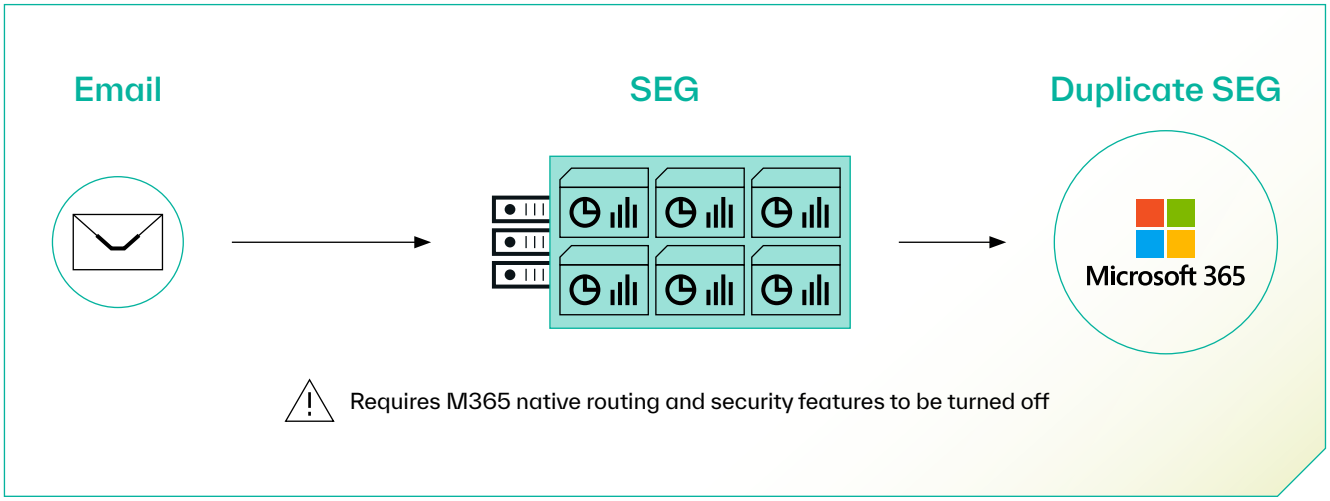


Figure 1. *Organizations can add secure email gateways to their M365 investments to protect their environments, but the architecture requires that they disable Microsoft functionality.*

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

Figure 2. Organizations can instead add cloud-native API solutions to their M365 investments, which allows Microsoft to function as it was intended.

Avoiding Feature Duplication

In addition to the architectural approach, the other equally important consideration in maximizing 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.

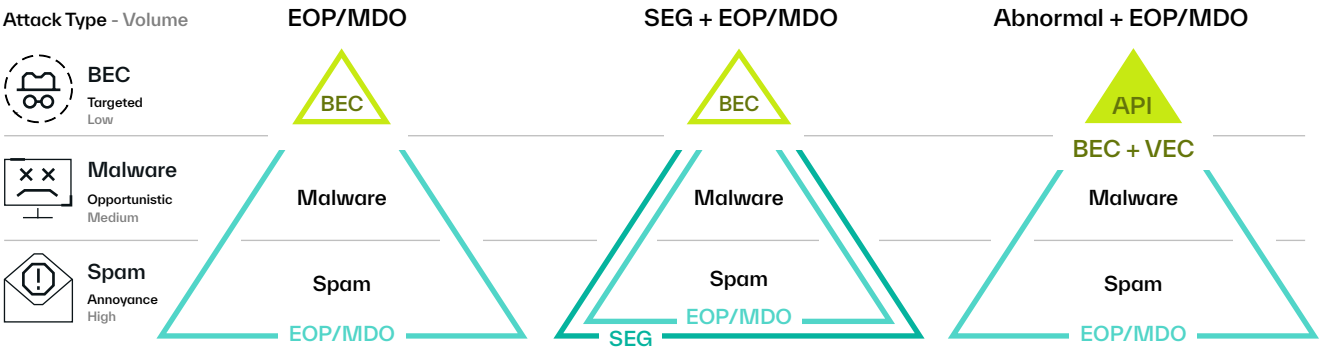


Figure 3. Organizations add secure email gateways to their M365 investments, resulting in incrementally better protection against spam and malware, but leaving targeted attacks largely unaddressed. Prioritizing a solution that stops these low volume but highly targeted socially-engineered attacks and takes advantage of native Microsoft capabilities for spam and malware provides the highest impact and potential ROI.

Maximizing Coverage and ROI

To increase feature coverage, organizations have historically added a third solution into their email security stack to provide comprehensive coverage against the whole spectrum of email attacks. In theory, this works and does ultimately protect the organization and employees from both basic and sophisticated attacks.

However, the right solution can work alongside Microsoft to provide the needed extra coverage—even without the secure email gateway. When combined with Abnormal, the native protection in Microsoft 365 provides superior protection against all threats while eliminating the financial and operational burdens associated with the SEG.

Considering an SEG Replacement?

Take a **short self-assessment** to see whether your current architecture still serves your needs.

> I didn't see the value that a SEG would provide on top of [our enterprise email] and Abnormal. We haven't noticed any loss by not having a SEG; we just noticed gain. So I basically redeployed the budget I used to spend on the SEG to Abnormal.

Read the Forrester TEI Report ›

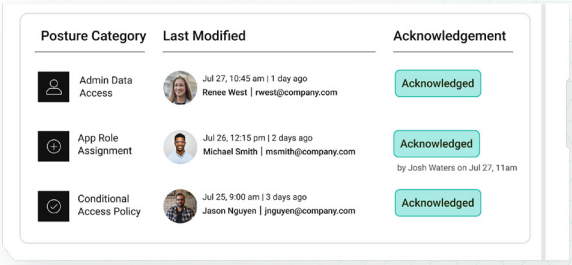
Defense-In-Depth Protection

		Microsoft 365 + Abnormal = Defense-In-Depth		
		Threat Intel / Known Bad Attack Protection	Behavioral / Known Good Attack Protection	Better Together
Inbound Hygiene	Spam	Threat Intel	Behavioral	✓ ✓
	Graymail	Rule-Based	Behavioral	✓ ✓
Malware Protection	Full Attachment / Link Protection	Threat Intel	Behavioral	✓ ✓
Phishing Protection	External Phishing	Threat Intel	Behavioral	✓ ✓
	Spear-Phishing	Threat Intel	Behavioral	✓ ✓
	Internal Phishing	Rule-Based	Behavioral	✓ ✓
Social Engineering Protection	BEC + CEO Fraud	Rule-Based	Behavioral	✓ ✓
	BEC + Invoice Fraud	NO	Behavioral	✓
Account Compromise Protection	Internal Account Compromise	Rule-Based	Behavioral	✓ ✓
	Vendor Account Compromise	NO	Behavioral	✓
Modern End User Experience	Native Outlook Experience	Yes	Abnormal	✓ ✓
	Automated Safe Listing	Threat Intel	Abnormal	✓ ✓
Simplified Visibility and Operations	Fine-Grained Detection and Remediation	NO	Abnormal	✓

Abnormal Behavioral AI in Action

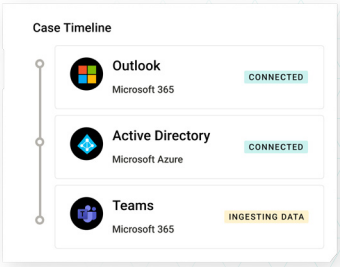
Improves Email Security Posture

Abnormal improves the risk posture of cloud email environments by helping security teams understand and take action on configuration gaps–without manual efforts, spreadsheets, or PowerShell scripts.



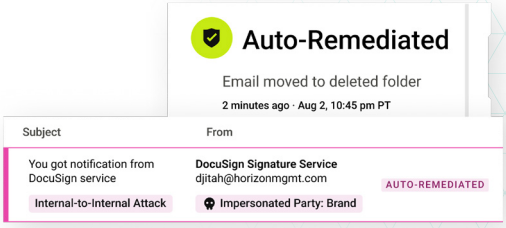
Simplifies Email Security Architecture

Abnormal simplifies email and security architecture, eliminating the complexity of secure email gateways. Our modern, cloud-native solution integrates via API and deploys in minutes. No policies, transport rules, or change of MX records are required.



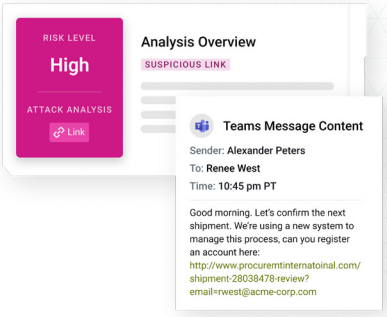
Automates SOC Operations

Abnormal fully automates email triage, remediation, and reporting, bringing together all auto-detected and user-reported threats into a single interface. Analysts can use search and respond functionality to rapidly contain missed attacks or misdirected emails.



Protects Your Microsoft Teams Messages and Accounts

Abnormal monitors communication across group chats, teams, channels and direct messages to identify suspicious URLs and compromised accounts. It also dynamically monitors global admins and alerts security teams of changes that may indicate a threat.



Conclusion

As organizations re-evaluate their security strategies in the face of rising threat sophistication and budget constraints, they need solutions that work seamlessly with Microsoft 365—not around it. The most effective approach builds on existing investments in Exchange Online Protection and Defender, while filling the critical gaps those native tools weren't designed to cover.

Abnormal delivers on that model with a cloud-native, API-integrated platform purpose-built for behavioral detection at scale. By understanding human behavior and organizational context, Abnormal stops socially-engineered attacks that evade traditional tools—without duplicating protection, disrupting mail flow, or requiring manual policy tuning. This architecture not only strengthens security posture but also drives significant return on investment by reducing operational overhead and tooling costs.

Together, Abnormal and Microsoft provide comprehensive coverage across the email threat spectrum, eliminating the need for a secure email gateway entirely. In fact, 70% of Abnormal customers have retired their SEG as part of this shift. In a landscape shaped by AI-driven attacks and shrinking budgets, Abnormal offers a simple, intelligent path to greater protection, lower total cost of ownership, and long-term efficiency.

About Abnormal AI

Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by more than 3,200 organizations, including over 25% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI.

Interested in Augmenting Your Microsoft Security?

Request a Demo ›

See Your ROI ›