Abnormal

Email Security Architectures from Exchange to Microsoft 365

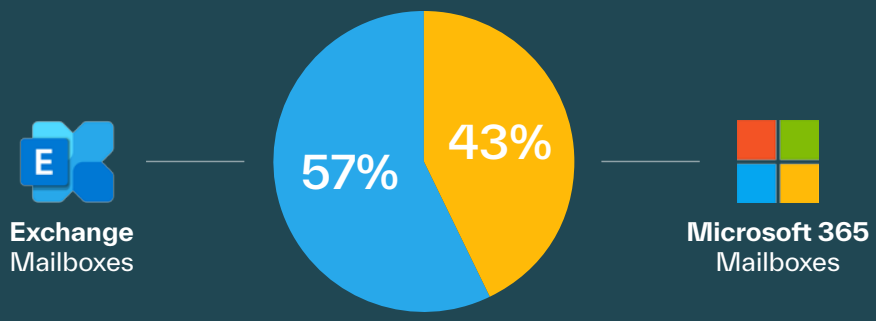
/ Comparing Coverage of Modern Threats to Cost Efficiency

Table of Contents

Introduction

With the early market adoption of on-premise mail servers like Microsoft Exchange, organizations also implemented security measures to protect against the wide array of email threats. Secure email gateway (SEG) deployments came in the form of either a server residing in the corporate network or as mail gateway cloud-based deployments through software-as-a-service (SaaS) vendors.

With the growing popularity of using cloud computing to manage corporate infrastructure and run applications, many organizations have moved their email hosting environment to the cloud. To meet this demand, Microsoft introduced Office 365, now named Microsoft 365. Subsequently, many corporate customers migrated from on-premise to cloud-based mail hosting. In fact, M365 cloud mailboxes now represent 57% of worldwide Exchange mailboxes while on-premise Exchange has fallen to 43%—a decrease of nearly 10% over the past year.*



The corporate migration from Exchange to M365 has also created a range of permutations for how to approach email security, which have expanded due to the threat protection capabilities embedded in the offering with native Exchange Online Protection (EOP) or, in advanced packages with Microsoft Defender for Office 365 (MDO). In addition to these protection options, companies can add integrated API-based security controls or a SEG solution, and some choose to use all three.

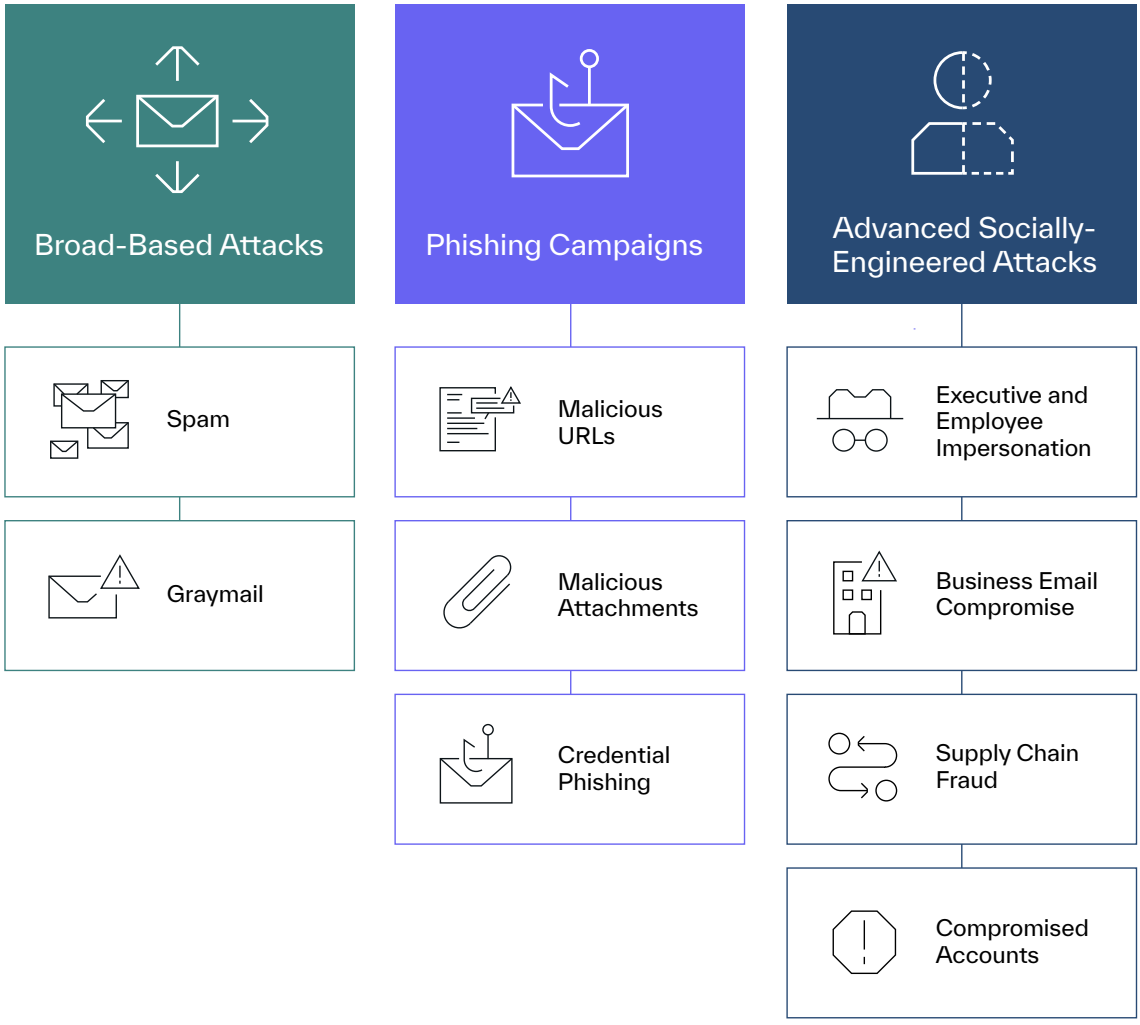
Of course, not all email security approaches deliver the same levels of threat protection and cost effectiveness. This paper maps the general progression that many organizations have taken through their architecture journey with a focus on the resulting coverage against the spectrum of attacks and security budget effectiveness of each. You'll see why organizations are shifting from the secure email gateway to integrated cloud email security solutions alongside the move to the cloud office.

*The Radicatti Group. Microsoft Office 365, Exchange Server and Outlook Market Analysis, 2021-2025. Published 2021.

The Spectrum of Attacks

While there are varied approaches to email security architectures, they all have the same goal: to provide complete coverage against the broad range of email-based threats.

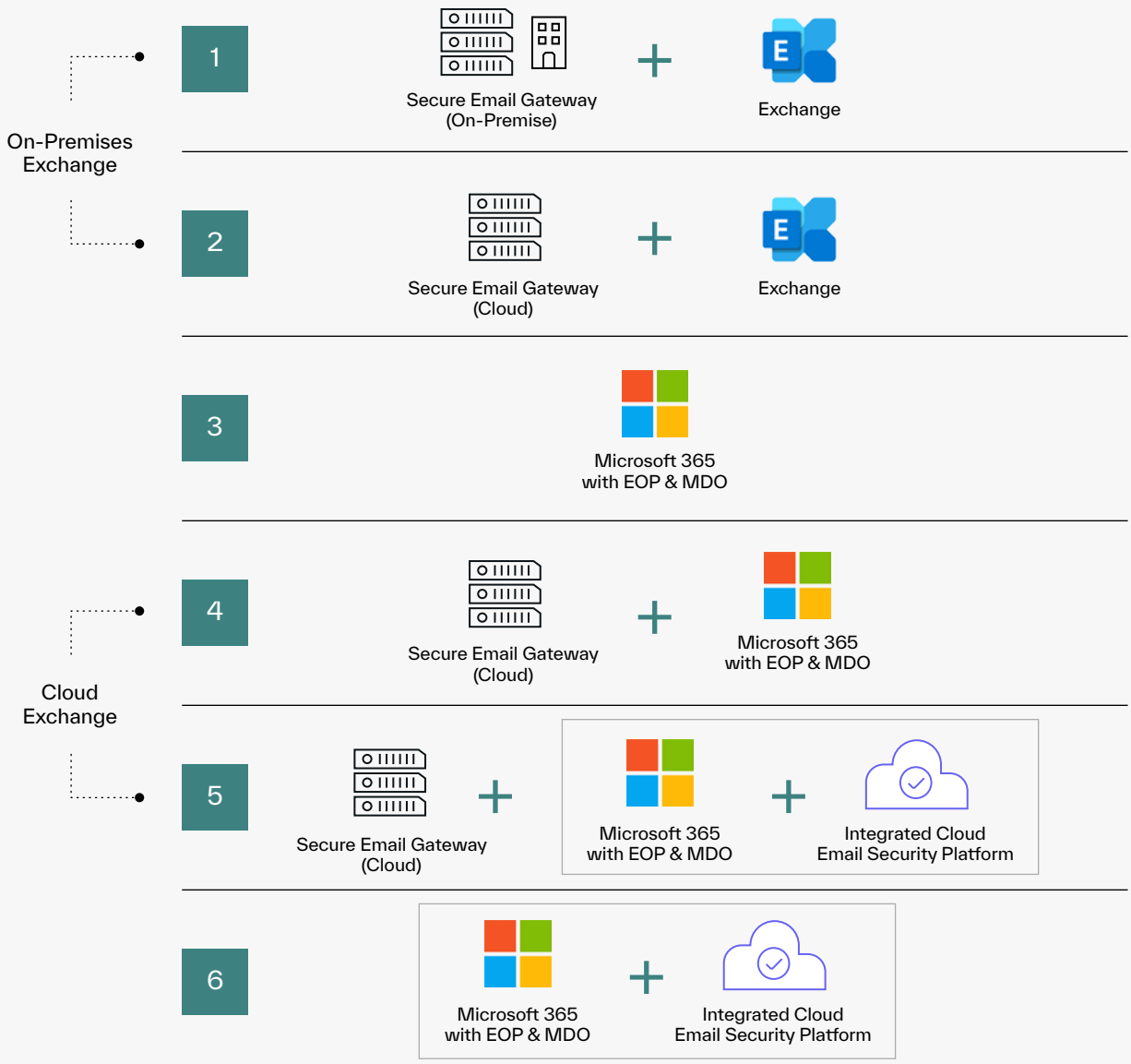
Before looking at the architectures, it's important to understand the threats they're meant to protect against.



Abnormal

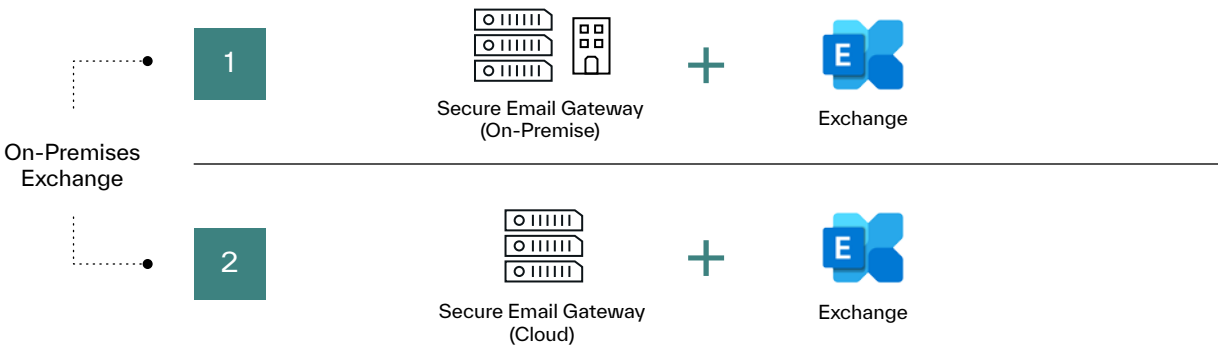
Architecture Approaches

The strategy each organization takes for their email security is based on how they are managing mail hosting—either on-premises or in the cloud. From there, the security architecture takes one of the following six approaches.



On Premises Exchange: Security Architectures #1 & #2

Hosted or Cloud-Based Secure Email Gateway



The secure email gateway provides protection against broad-based attacks but misses the low-volume, targeted attacks that are the most dangerous.

For those companies that have elected to manage an on-premises Microsoft Exchange Server, email security consistently takes the flavor of either an on-premises or cloud-based secure email gateway. SEG solutions sit in line with the mail flow and act as an SMTP relay, which also gives them essential connection-based protection features to analyze the authenticity of the message before it is fully received and unpacked.

Cloud and on-premises SEG solutions both provide the same protection capabilities. The main difference is the capital or operating expenditure the company incurs depending on how they decide to manage the SEG infrastructure, either onsite or offloaded in the cloud. Onsite management and maintenance is carried in the company's capital expenditures while cloud-based SEG services are reflected in operating expenditures.

One important consideration with the cloud option is that vendors have used the word "cloud" to represent different approaches. Some vendors have a solution that is a cloud-hosted model where each customer is running on a dedicated tenant. Comparatively, other SEG vendors have true cloud systems that support multi-tenancy.

In either approach, when organizations choose to manage an on-premises Exchange server with a security email gateway, they experience a mix of advantages and challenges, including:

PROS

+ Companies have complete control over mail flow and protection measures.
+ The organization maintains control of the Exchange data.

CONS

- For on-premises secure email gateways, organizations incur management and maintenance overhead including hardware, uptime, and upgrades.
- Security teams must manage another mail hop. If the SEG goes down, the company's inbound and outbound mail flow will be interrupted.

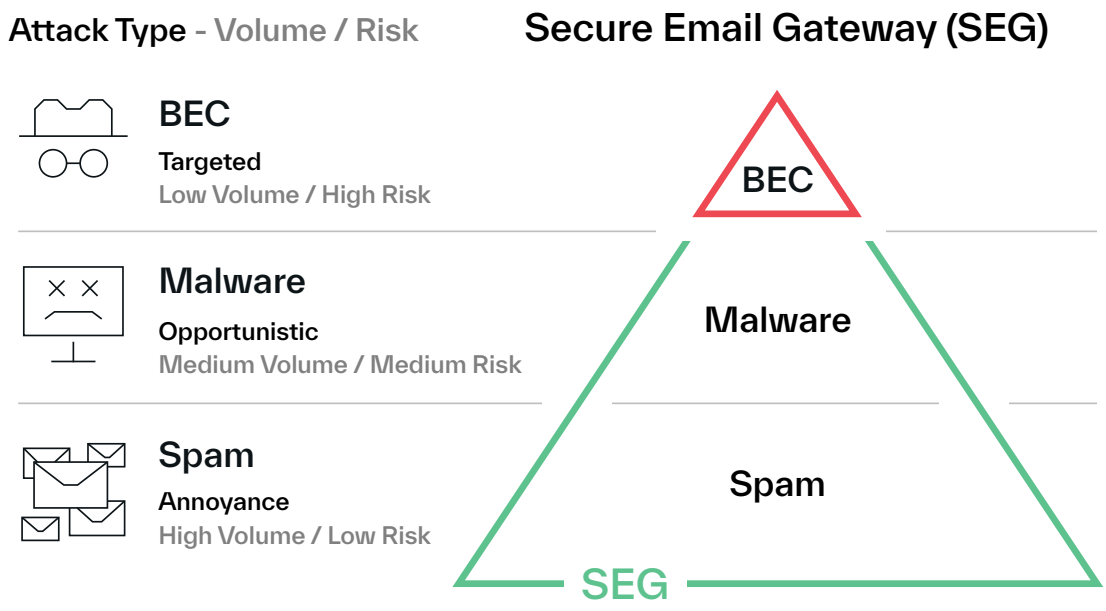


Figure 1: This architecture leaves business email compromise attacks unprotected.

Abnormal

Microsoft 365: Security Architecture #3

Native EOP and MDO Security Layers within Microsoft 365

3

Microsoft 365
with EOP & MDO

While this approach saves the cost of the secure email gateway, it opens organizations to socially-engineered attacks.

The group of companies using M365 largely represents the mass migration of Microsoft customers who have moved from on-premises Exchange to the cloud. And a big migration it has been, with more than a million companies worldwide using the platform.

One of the value-add business justifications behind the decision to move to M365 is cost efficiency. Microsoft 365 performs all the functions of a SEG, like connection-filtering, anti-spam, anti-virus, and other security features with its integrated Exchange Online Protection (EOP) and Microsoft Defender for Office 365 (MDO), without the need for additional infrastructure.

These email security features within Microsoft introduced an architecture evolution where many companies pursued technology consolidations and dropped their SEG solution as part of their M365 adoption. Notably, Microsoft has made solid investments to further enhance EOP and MDO in the last two years, which focus on increased effectiveness.

No doubt M365 with embedded threat capabilities provides an array of advantages. Yet, companies continue to experience email security challenges as well:

PROS

+ Companies gain capital and operating expenditure benefits.
+ M365 licenses provide financially-basked SLAs.
+ EOP and MDO protection capabilities enable companies to consolidate security investments by dropping the secure email gateway.

CONS

- Organizations experience incomplete coverage of the attack spectrum. While campaign-based threats like those that contain malicious attachments or links are well covered, this architecture does not safeguard against targeted, social engineering attacks.

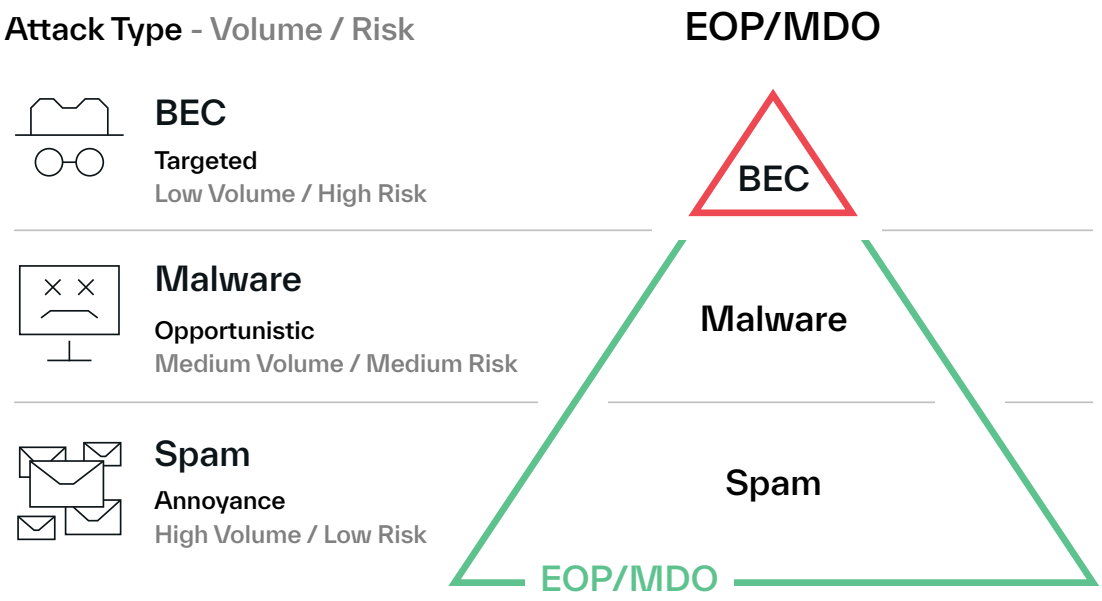


Figure 2: This approach leaves socially engineered attacks unprotected.

Microsoft 365: Security Architecture #4

Native EOP and MDO Protections + Secure Email Gateway

4

Secure Email Gateway (Cloud)

+

Microsoft 365 with EOP & MDO

While the end goal is best protection coverage, this approach introduces cost inefficiency with companies, paying twice for overlapping features across technologies.

Companies who use M365 with its embedded threat protection along with a secure email gateway solution arrived at this architecture by one of two paths:

1. They maintained their SEG solution as part of the company's migration to Microsoft 365

2. They originally dropped their SEG solution as part of the M365 migration and then added the SEG back in when they started receiving attacks.

One of the primary reasons organizations pursue this architecture is to gain broader coverage against the array of email attacks. While this effort is partially successful, the interesting result is that adding a SEG renders M365's connection protection capabilities inoperable and also duplicates some protection capabilities provided by EOP and MDO.

As noted, Microsoft has invested in ATP and MDO innovations recently, so many organizations with this security architecture are now re-evaluating to determine if they can successfully pursue consolidation and forgo renewing their SEG license.

Ultimately, companies experience a range of pros and cons with this architecture:

PROS

+ Adding a SEG provides better defense against spam and campaign attacks, such as malware and phishing campaigns.
+ Companies benefit from the best-of-breed capabilities present in the secure email gateway, such as sandbox analysis and reporting.

CONS

- Organizations miss coverage against the socially engineered attacks that are most damaging.
- Companies expend significantly higher security budgets than the other architecture approaches for incremental improvement in threat coverage.
- Security teams incur the complex challenge of managing multiple solutions. Investigating a false positive or false negative can require the security analyst to investigate in multiple systems to successfully diagnose.

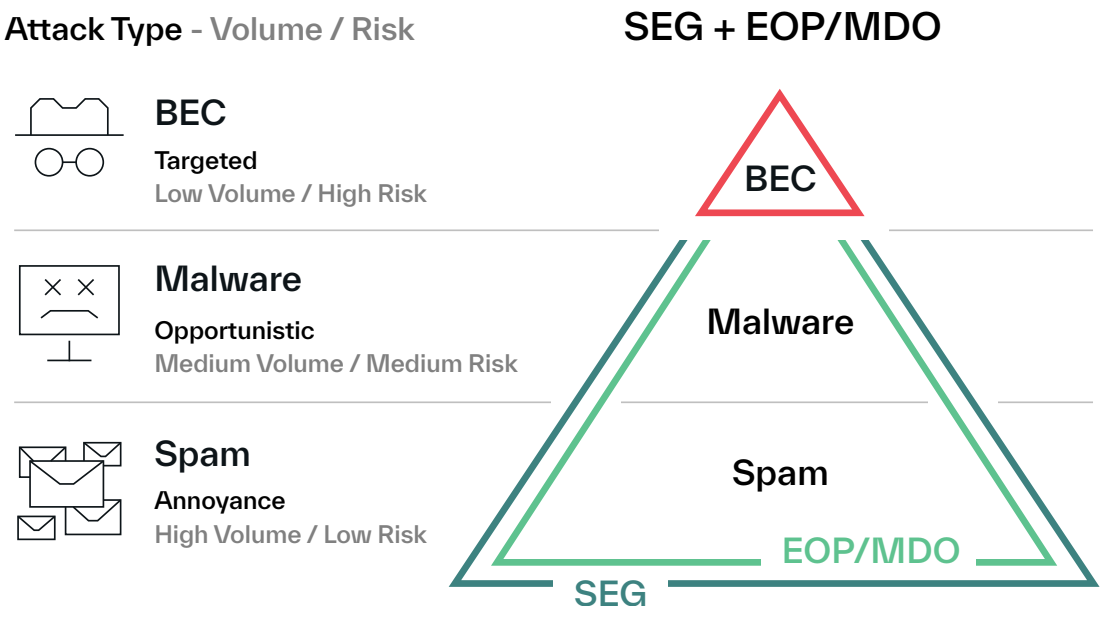


Figure 3: Business email compromise and other advanced attacks remain unprotected.

Microsoft 365: Security Architecture #5

Native EOP and MDO Protections + Secure Email Gateway + Integrated Cloud Email Security Platform

A multi-layer, multi-technique email security architecture delivers comprehensive email threat protection but organizations experience challenges related to cost and complexity.

To combat the complexity of socially engineered email threats, organizations often include API-based email protection that uses data science techniques to fill the gaps in coverage against advanced email threats. Microsoft allows these solutions to "snap in" via API to work seamlessly within the M365 architecture.

It is important to understand that these solutions, often called integrated cloud email security (ICES) platforms, are comprised of two essential elements:

1. An API-based architecture

2. Protection techniques based on data science

Why is a data science model essential? In order to gain the broadest threat protection coverage, companies should choose a solution that applies a different protection method than the intelligence-based approach available in Microsoft. Doing so protects against the threats that an intelligence-based approach misses.

This augments the existing EOP and MDO detection techniques, so organizations can gain greater effectiveness against business email compromise (BEC) and other socially engineered attacks.

Undoubtedly, this multi-layer, multi-technique email security architecture delivers comprehensive email threat protection. Nevertheless, organizations experience challenges related to cost and complexity due to working with multiple providers.

PROS

+ The API-based integrated cloud email security solution addresses gaps in the advanced threat defense capabilities provided by the secure email gateway, delivering an architecture that provides comprehensive coverage across the broad spectrum of attacks.

CONS

- The approach of employing M365 alongside a secure email gateway and integrated cloud email security platform creates significant budget inefficiencies. Organizations find themselves paying for duplicate threat coverage capabilities between M365 and the SEG.
- In the event that the organization adopts an ICES solution that uses similar detection techniques to M365 instead of a data science-based approach, they don't experience the increase in efficacy.
- Security teams incur even greater complexity in managing multiple solutions as analysts must navigate three solutions to manage incident response.

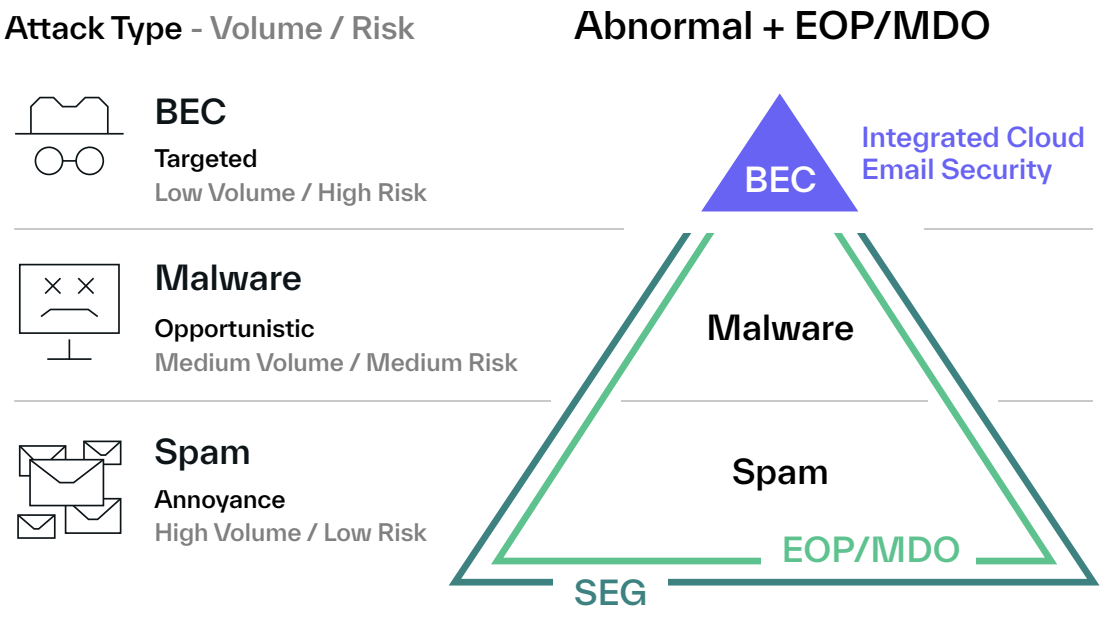


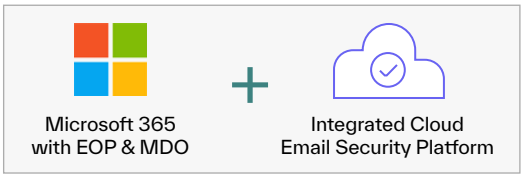
Figure 4: This architecture delivers threat protection against the broad spectrum of attacks.

Abnormal

Microsoft 365: Security Architecture #6

Native EOP and MDO Protections + Integrated Cloud Email Security Platform

6



Integrated cloud email security solutions strategically augment EOP and MDO features, creating greater budget synergies in the company's security technology investments.

This email security architecture is the newest in the evolutionary cycle. Companies using M365 mail hosting with EOP and MDO security features, plus an integrated cloud email security solution came to this decision by:

1. Pursuing an API approach to apply a different detection technique (data science) that augments Microsoft's EOP and MDO capabilities as the highest impact approach to catch all attacks.

2. Initiating technology and cost consolidation by dropping the company's incumbent secure email gateway after determining that SEG layer value was minimal.

This security approach integrates directly with M365 and provides an in-depth technological focus to specifically shore up the threat coverage gaps by applying a different protection technique that doesn't duplicate existing EOP or MDO features.

As a result, companies experience win-win benefits across the spectrum of threat coverage, technology management, and cost efficiencies:

PROS

+ Integrated cloud email security solutions with API architectures and data science-based approaches address the gaps in advanced threat detection capabilities provided by the incumbent SEG solution, delivering an architecture that provides comprehensive coverage across the broad spectrum of attack types.
+ API integrations with M365 strategically augment EOP and MDO features, creating greater budget synergies in the company's security technology investments.
+ Technology management and threat investigations are simplified with an API-integrated solution that works seamlessly within the M365 architecture.

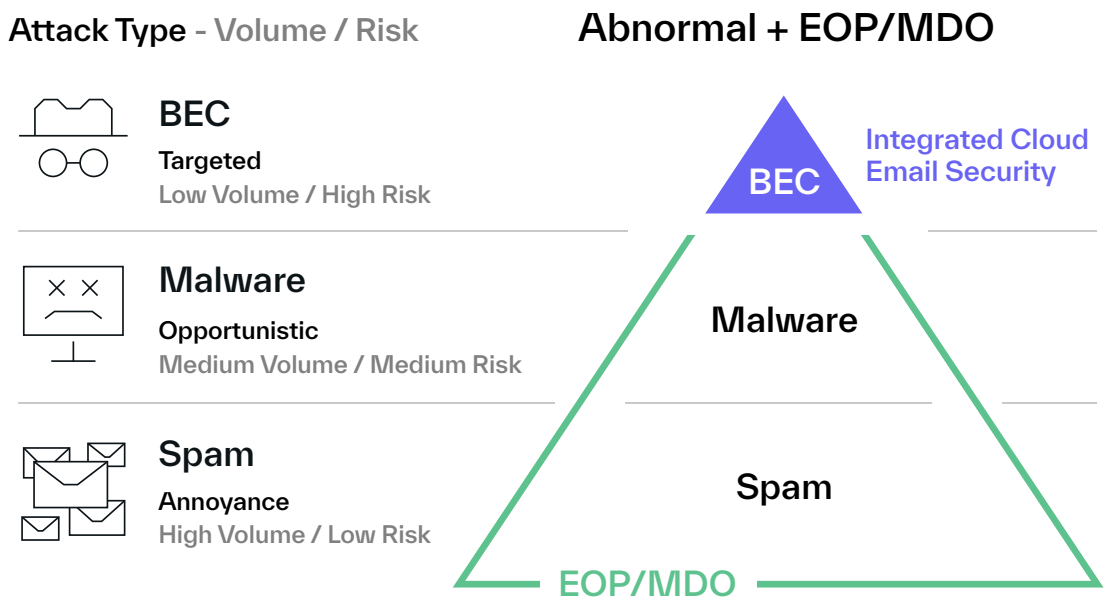


Figure 5: This architecture protects against the broad spectrum of attacks and maximizes cost efficiency.

Conclusion

The approaches to email security have evolved with the industry move to the cloud, and will continue to evolve as attacks become more targeted. Companies that manage an on-premises mail server have a proven approach of safeguarding against email attacks by using either a cloud or on-premises secure email gateway.

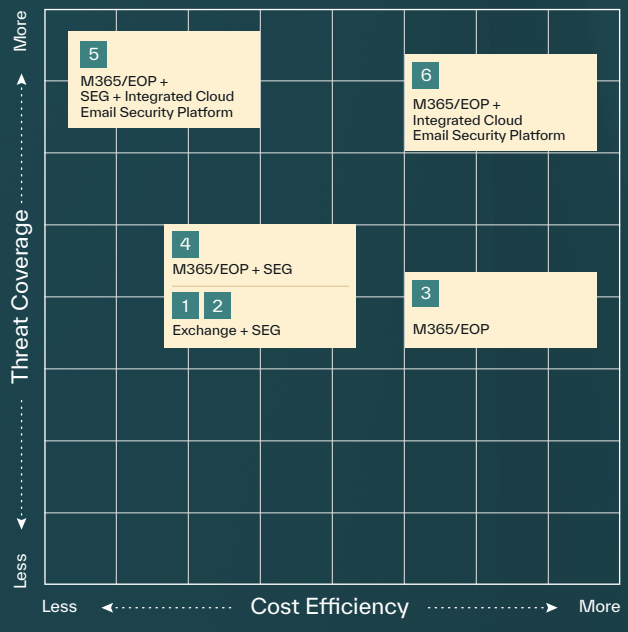
However, for organizations using Microsoft 365, there are several architecture options that deliver different results against the goal of broad threat coverage and optimized cost effectiveness. When security practitioners consider the M365 email security options, the question at the heart of the decision is: **can we realistically drop our SEG when it has a long legacy as a standard security control?**

The answer is yes. The cybersecurity market never stands still and it is always evolving, but the new category of integrated cloud email security solutions provide a way to protect organizations against all threats, while eliminating the duplicity in the secure email gateway. A security practice like the SEG should not endure if innovations have rendered it unnecessary.

The last two years have seen Microsoft make significant threat coverage gains with Exchange Online Protection and Defender for Office 365. When combined with a solution that has an API architecture and data science-based solution to detecting threats, organizations can close the coverage gap against socially engineered attacks, while maximizing cost effectiveness.

Microsoft 365 customers that never dropped their SEG or boomeranged back to an SEG solution should consider initiating a new evaluation cycle that reviews the threat protection and cost effectiveness of M365 with an integrated cloud email security solution against their current email security architecture.

To see how Abnormal can help you determine what is getting past your current infrastructure, request a Risk Assessment.



Abnormal

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 stopping BEC?

Request a Demo:

abnormalsecurity.com →

Follow us on Twitter:

@abnormalsec