Armorblox

WHITE PAPER

Augmenting Native Office 365 Email Security to Stop Targeted Email Attacks

Contents

Executive Summary

Email continues to be the lifeblood of business communications, but it's also undergoing a paradigm shift. This shift has two clear drivers: a shift to the cloud, and a commoditization of certain email security features. Microsoft sits at the intersection of these email trends. Of the 81% of businesses that have made the shift to cloud services, over half are Office 365 users1. The groundswell of momentum heralded by cloud-based Office 365 offerings has improved organizational agility and simplified the management of corporate applications.

Microsoft has included a wide spread of email security features within their Office 365 suite, enabling customers to move away from on-premise Secure Email Gateways (SEGs). Exchange Online Protection (EOP) and Advanced Threat Protection (ATP) together offer good protection against spam, known and unknown malware, and mass phishing campaigns. However, there are entire categories of email compromise that evade O365 detection, manipulate language and intent, and lull victims into a false sense of security that the email they're replying to is legitimate. These Business Email Compromise (BEC) attacks have cost businesses $26 billion over the past three years according to the FBI2.

Organizations should complement native O365 email security with third-party controls that take a different approach to threat detection. Since BEC attacks can't be detected by heavy-handed 'all or nothing' signals, third-party email security controls should provide a breadth and depth of signal analysis that cuts across user identity, user behavior, and email language.

Furthermore, to future-proof their email security investments, companies should embrace solutions that are driven by models that learn and get better with time. These models should strike a balance between global datasets that train across organizations and local datasets that capture the context of specific organizations and their employees.

IT and security teams are lean both by necessity and by design. Hence, organizations should implement supplementary email security solutions that complement the native functionalities of O365 email security. To minimize deployment complexity and maintenance, companies should look for API-first deployment models rather than traversing down the well-trodden path of SMTP-based gateways.

This paper will summarize current Office 365 email security offerings and focus on the required capabilities that third-party email security controls should have to effectively complement - and not duplicate - these native security features.

[1] Microsoft Office 365 is Being Adopted and Used at an Enormous Rate: https://blog.goptg.com/microsoft-office-365-statistics

[2] Business Email Compromise: The $26 Billion Scam: https://www.ic3.gov/media/2019/190910.aspx

The New Face of Email Attacks

Email attacks were prevalent ten years ago and will probably still be rearing their heads ten years from now. What's worth noting is the evolution of email attacks beyond mass phishing campaigns and spam. While these types of 'click-and-run' attacks still exist, attackers don't spend too much time crafting them and they're effectively blocked by existing security controls.

Cybercriminals have moved towards email attacks that evade metadata-based detection, don't have binary 'good or bad' payloads, and are finely crafted to push all the right psychological buttons of their intended victims. These attacks - broadly classified under the Business Email Compromise (BEC) umbrella - have dripped and dripped over the years to create a billion dollar ocean. The 2019 IC3 Report from the Federal Bureau of Investigation found that over $26 billion has been lost in BEC attacks over the past three years.

$26 BILLION

The 2019 IC3 Report from the Federal Bureau of Investigation found that over $26 billion has been lost in BEC attacks over the past three years.

BEC attacks usually share these characteristics:

Laser targeted

BEC attacks eschew the scattergun approach of mass phishing attempts and are the result of extensive groundwork and research conducted by the attacker. The perpetrator is aware of the victim's name, job title, reporting manager, and sometimes even what days they'll be out of office.

Rules and metadata are not enough

Since BEC attacks are more sniper than sledgehammer in their technique, metadata and binary rules are not enough to flag these emails. These protection techniques either lead to a flood of false positives or let finely crafted BEC attacks escape their grasp.

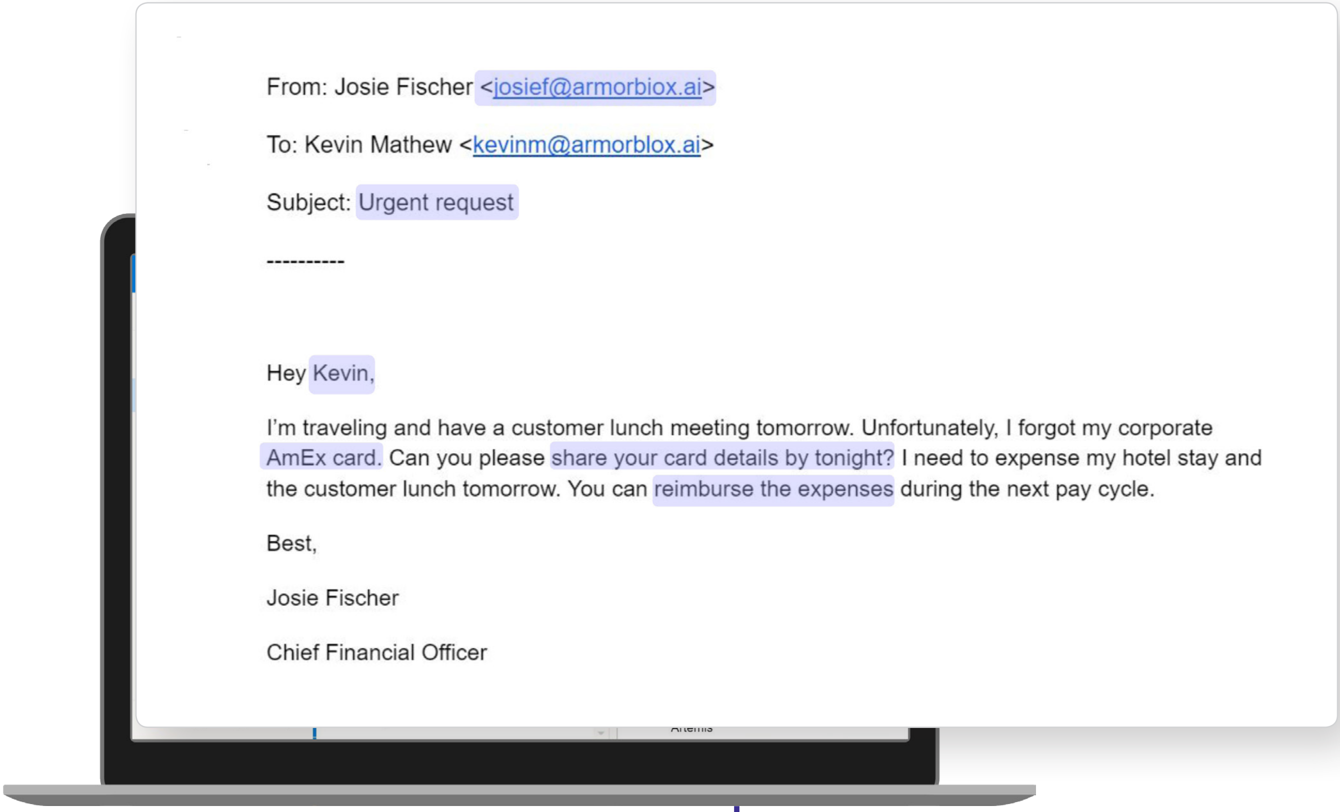
No malicious payloads

BEC attacks rarely include URLs or attachments that contain malicious payloads, especially in the first email. Payloads may sometimes be introduced at the end of email chains, after the attacker has gained the victim's trust. It's more likely for the 'payload' to be within the email content itself i.e. requests that are framed like they're coming from a legitimate person that the victim knows.

Socially engineered

BEC attacks prey on human nature as much as (if not more than) security controls. Leaning on age-old psychological tricks like urgency, authority, persuasion, and fear, the language in these emails make the victims 'want' to take action without thinking too much about it.

Today’s Email Attacks Get Past Traditional Defenses



From: Josie Fischer <josief@armorbiox.ai>

To: Kevin Mathew <kevinm@armorblox.ai>

Subject: Urgent request

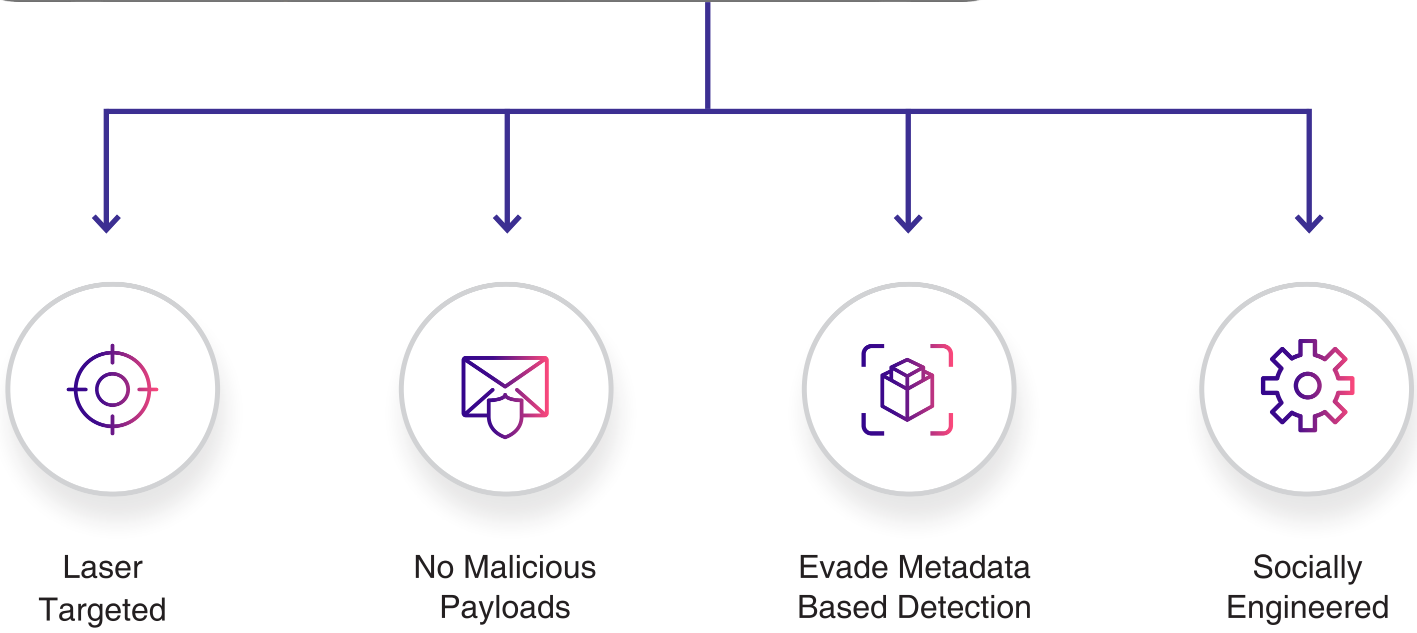
Hey Kevin,

I’m traveling and have a customer lunch meeting tomorrow. Unfortunately, I forgot my corporate AmEx card. Can you please share your card details by tonight? I need to expense my hotel stay and the customer lunch tomorrow. You can reimburse the expenses during the next pay cycle.

Best,

Josie Fischer

Chief Financial Officer



Office 365 Email Security Capabilities

As email goes through a paradigm shift, Microsoft Office 365 has unquestionably turned into the vendor of choice for business email needs. This paradigm shift is marked by two major trends: a shift to the cloud, and the commoditization of certain email security capabilities.

Microsoft has acknowledged both aforementioned trends by including a good spread of email security features within their Office 365 suite, enabling customers to move away from on-premise Secure Email Gateways (SEGs) as they transition to cloud-based Office 365.

Exchange Online Protection (EOP)

Microsoft describes Exchange Online Protection (EOP) as a cloud-based email filtering service that helps protect organizations against spam, malware, and messaging-policy violations. Organizations pay for EOP as part of both the E3 and E5 O365 licenses.

EOP security capabilities include:

Anti-spam protection	Blocks spam by using URL and domain lists, content filtering, and connection filtering.
Anti-malware protection	Multiple anti-malware engines along with customizable malware filtering rules.
Mail routing and flow rules	Route and filter emails by domain, region, keywords, subject line, and other parameters.
Reporting and logging	Audit logs, web-based reports, and message tracing provide visibility into email activity.
SLAs and support	A spam effectiveness SLA of >99% and a virus detection/blocking SLA of 100%

A full list of EOP capabilities is available here.

Advanced Threat Protection (ATP)

Microsoft describes Advanced Threat Protection (ATP) as an add-on security offering that safeguards organizations against malicious threats posed by email messages, links (URLs), and collaboration tools. Organizations pay for ATP as part of the E5 O365 license, with two ATP plans available to choose from.

ATP security capabilities include:

Safe attachments and links	Protects against zero-day malware with dynamic analysis. Provides time-of-click verification for all URLs.
SharePoint, OneDrive, and Teams support	Identifies and blocks malicious files on team sites and document libraries for cross-platform protection.
ATP anti-phishing protection	Applies machine learning models for advanced phishing protection.
Threat investigation and response	Uses threat intelligence and real-time reports for threat identification and analysis.
Attack simulation	Runs realistic attack scenarios to identify organizational vulnerabilities.

A full list of ATP capabilities is available here.

Studying these capabilities highlights both strengths and gaps in the O365 email security suite. While EOP/ATP provide effective protection against spam, known/unknown malware, and conventional phishing attacks, there are entire categories of email attacks left unaddressed by these offerings.

Strengths	Gaps
Spam ✓	✗ Business Email Compromise
Known/Unknown malware ✓	✗ Advanced impersonation attacks
Phishing campaigns ✓	✗ Payroll/invoice fraud
Cross-platform Microsoft support ✓	✗ Socially engineered email attacks

How Contextual Understanding Helps

Native Office 365 email security (EOP) does a good job protecting against spam, known malware, and mass phishing campaigns. ATP leverages threat intelligence and machine learning models to detect advanced phishing attempts, stop zero-day malware, and provide attack simulations to improve end user education. But there are entire categories of email compromise that evade O365 detection, manipulate language and intent, and lull victims into a false sense of security that the email they're replying to is legitimate.

There's only so far that eye tests and phishing awareness can take us. Organizations should complement native O365 email security with third-party controls that take a different approach to threat detection. Such an email security suite results in a more holistic approach, a better spread of techniques, and a more efficient allocation of the security budget.

Since BEC attacks can't be detected by heavy-handed 'all or nothing' signals, third-party email security controls should provide a breadth and depth of signal analysis that cuts across user identity, user behavior, and email language.

Identity

Email security controls need to exhaustively analyze who users are in order to prevent impersonation and spoofing attempts. What's the user's name, role, and hierarchical status within the organization? What devices, browsers, and email clients do they normally use?

Behavior

Identity is a critical part of email analysis, but these signals can turn noisy if used in isolation. It's also important to analyze what users do, create a behavior baseline, and study any anomalies from this baseline to accurately detect problems such as account takeovers and insider threats. What's the extent of interaction that a user has with internal and external recipients? What time of the day do they normally send most of their emails? What location and IP address do they usually login from?

> Organizations should complement native O365 email security with third-party controls that take a different approach to threat detection. Such an email security suite results in a more holistic approach, a better spread of techniques, and a more efficient allocation of the security budget.

Language

If cybercriminals are able to mask their identity and/or behavior, understanding the language in the email and the intent behind the email can be analysis signals that stop a pernicious attack. What's a user's normal writing style and are they noticeably deviating from it? Does the email have a tone of inordinate authority or urgency?

Analyzing a confluence of signals across identity, behavior, and language can enable third-party security controls to detect attacks that EOP/ATP or SEGs might let through. And with recent advancements in Natural Language Understanding (NLU) and machine comprehension, technology today is capable of making this breadth and depth of analysis a reality.

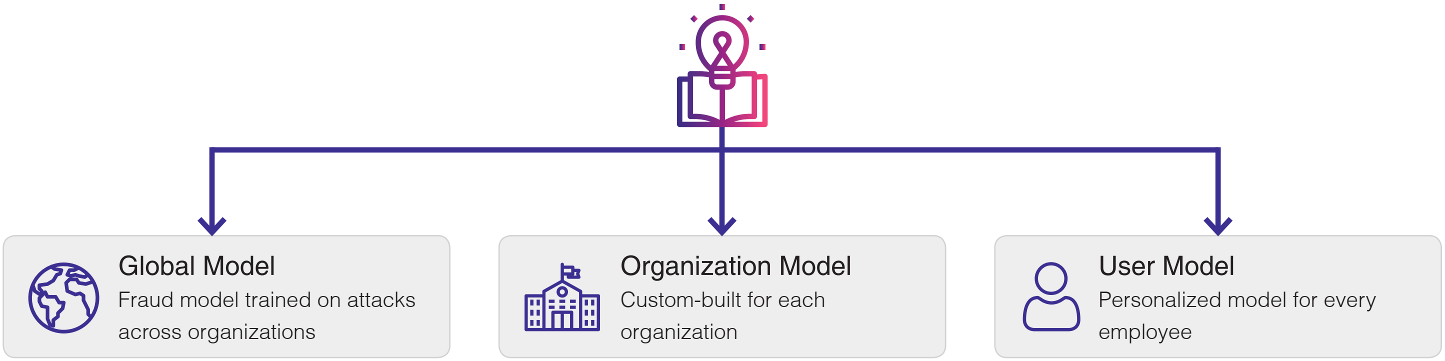
Look for Learning-Focused Systems

As long as email remains a critical vehicle for communication, attackers will try and evolve their techniques to bypass existing security measures. Ripping and replacing the entire email security stack every few years is not a cogent way to run security operations. Organizations should invest in email security solutions based on technologies and machine learning models that get better with time.

Organizations should invest in email security solutions based on technologies and machine learning models that get better with time.

It's understandable if reading 'machine learning' engenders some skepticism, given the prevalent overuse and misuse of the term among security vendors. Here are some learning-focused capabilities within email security solutions that effectively complement EOP/ATP protection features:

- Learning across organizations: Solutions that leverage anonymized signals across organizations as training data for their ML and fraud prediction models can offer broad and forward-looking email threat protection. Some BEC attacks start with one industry and replicate successful techniques across other industries. A model that learns across organizations minimizes this attacker advantage.
- Learning within organizations: If learning across organizations offers breadth, building custom self-learning models for each organization offers depth. Models that account for the volume and nature of external/internal email interactions, frequency of communication across departments, legitimate third-party vendor context, and other enterprise-specific signals can provide high-fidelity and relevant email threat detection.
- User-focused learning: The most focused and possibly deepest level of learning comes from studying individual user identity, behavior, and language signals. A user's writing style, the topics they discuss, their common login locations, and the people they frequently communicate with are signals that can provide vital context during an email account compromise or targeted attack.
- Learning from manual actions: The goal of machine learning systems should never be to replace human insight in security. Rather, ML models should channel human insight where it's needed most and preclude security teams from manual, repetitive response whenever possible. To this end, every manual action that security teams take (for example, marking an email threat as a false positive) should turn into valuable data that recalibrates ML models and minimizes similar manual actions in the future.



Global Model
Fraud model trained on attacks across organizations

Organization Model
Custom-built for each organization

User Model
Personalized model for every employee

API-First Deployment

As organizations move their email to the cloud with Office 365, it's advisable to rethink the preferred deployment of third-party email security controls as well. Specifically, organizations should look for API-first deployment models rather than traversing down the well-trodden path of SMTP-based gateways.

Organizations should look for API-first deployment models rather than traversing down the well-trodden path of SMTP-based gateways.

Deploying SEGs often requires modification of MX records and rerouting emails through either on-premise or hosted servers, increasing complexity and negatively affecting email availability on occasion. Ensuring ongoing compatibility also diverts resources from IT and security teams that already tend to be lean by necessity and design.

A SEG sitting in front of EOP/ATP not only duplicates security capabilities, but it also reduces the effectiveness of some EOP connection filtering and detection features. Some SEG vendors actually recommend disabling EOP features to realize full value from their solutions.

An API-based email security solution will sit on top of (rather than in front of) EOP/ATP, providing additional controls and detection capabilities that address attacks only once they get past native Microsoft defenses. This deployment model enables organizations to extract full value out of their existing O365 investments rather than tweaking and duplicating efforts.

How Armorblox Complements Office 365

Armorblox augments native Office 365 email security capabilities to provide the widest non-overlapping breadth of attack protection. By leveraging unique detection techniques, a cloud-native deployment model, and comprehensive interconnectivity with Microsoft APIs, Armorblox provides organizations with the most efficient allocation of their email security budget.

Broad Spectrum of Detection Techniques

Armorblox utilizes a broad spectrum of both classical and cutting-edge detection techniques to analyze thousands of signals across user identity, user behavior, and email language. Rather than replicating the features of native O365 email security, like threat intelligence and malware detonation, Armorblox detection techniques enable a more holistic spread of protection against varied email attacks.

> By leveraging unique detection techniques, a cloud-native deployment model, and comprehensive interconnectivity with Microsoft APIs, Armorblox provides organizations with the most efficient allocation of their email security budget.

- Statistical techniques: Clustering and anomaly detection help identify behaviors outside established norms (eg. unusual or anonymous IP address logins outside of home and work locations).
- Traditional machine learning: Multi-modal classifiers categorize emails into specific buckets (eg. differentiating between a marketing email, a payroll-related email, and an email with an invoice).
- Deep learning: Recurrent neural networks and LSTM learn from training data to predict fraudulent and suspicious emails.
- Natural language understanding: Entity recognition, sentiment/tone analysis, coreference resolution, and semantic role labeling enable context-aware attack detection.

API-First Architecture

Armorblox connects with Office 365 over APIs instead of adopting SMTP-driven deployment like SEGs. An API-based approach accelerates and simplifies deployment without any modification of MX records or rerouting of emails.

Getting Better With Time

Many Office 365 email security capabilities are dependent on lists of threat sources and vectors (eg. anti-phishing protection from EOP that includes 750,000 domains of known spammers). While these lists will be continuously updated, they won’t be enough to stop attacks that leverage the context of a particular organization or its employees.

Armorblox ML models learn across three tiers, enriching detections with both global attacks and organization-specific context. A global model is trained on attacks detected across organizations, an organization-specific model is custom-built for every Armorblox customer, and a user-specific model identifies patterns and anomalies for each individual user.

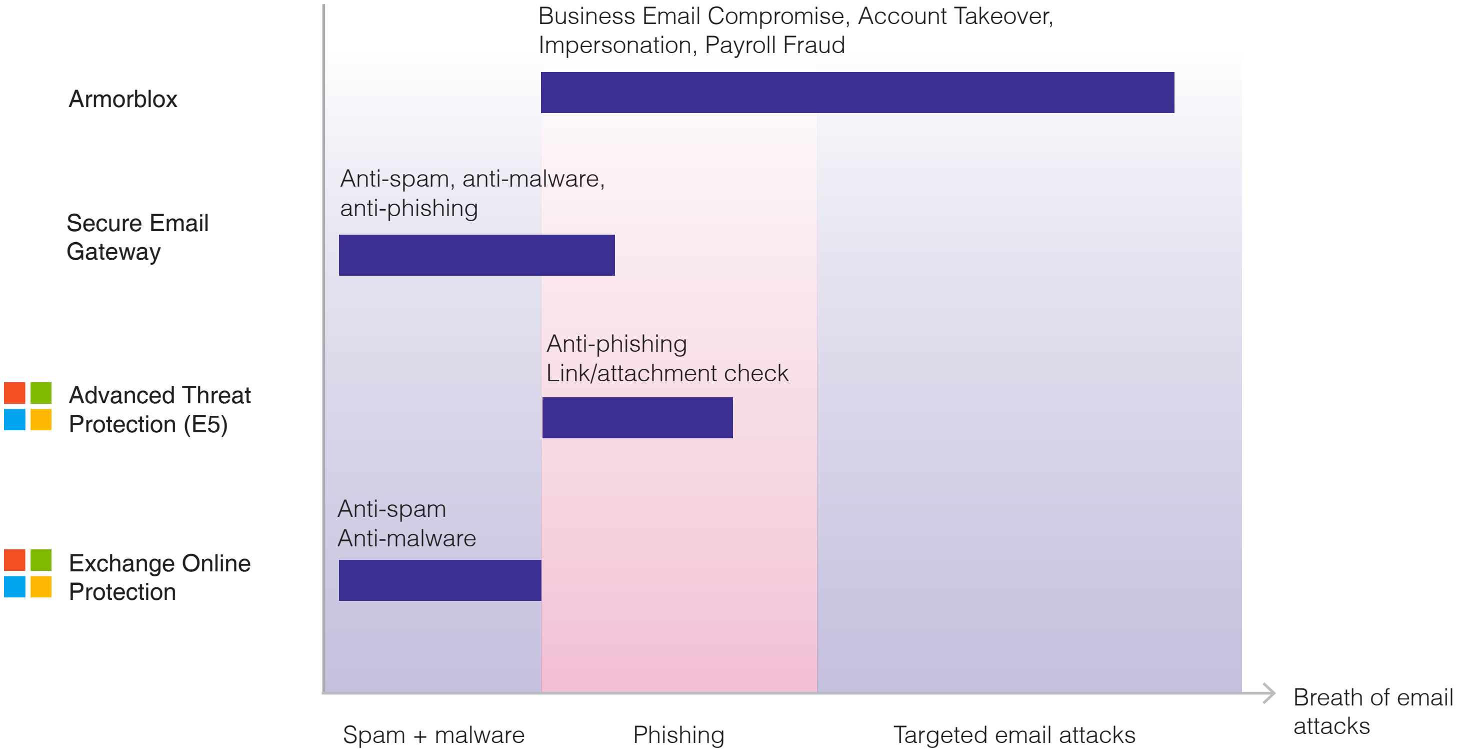


Fig: Armorblox complements native Office 365 security to offer the widest non-overlapping breadth of email attack protection

Armorblox

Armorblox is a cloud-native and content-aware email security platform that protects against targeted attacks such as business email compromise, account takeover, and executive impersonation. Organizations use Armorblox to deploy pre-configured policies that block suspicious emails, automate abuse mailbox remediation, and prevent outbound data loss.

☎ (408) 475 - 8713

armorblox.com

19200 Stevens Creek Blvd. Suite 100 Cupertino, CA 95014