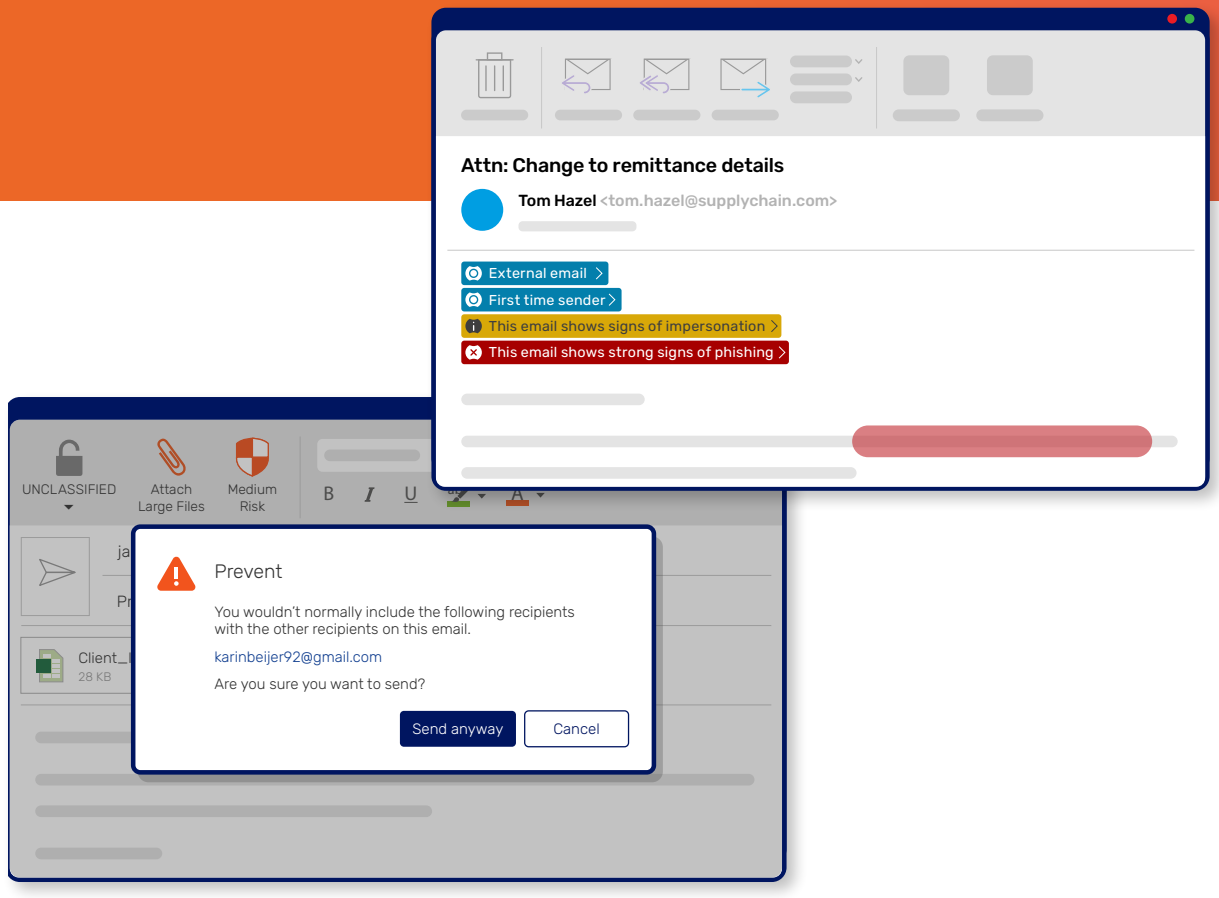
KNOWBE4 PRODUCT GUIDE

Enhance Microsoft 365 with KnowBe4 Cloud Email Security



KnowBe4

Contents

Introduction

The email security market has undergone a monumental shift in recent years, with the rapid migration to Microsoft 365 (M365) and adoption of the platform's native email security, and subsequent diminishing reliance on secure email gateways (SEGs) for inbound and outbound threat prevention.

While many organizations are realizing a total duplication in features and functionality between M365 native security and SEGs, others will continue to rely on their SEGs to meet a small number of very specialist security and operational requirements, such as complex routing rules, content-based rules and archiving. What all can agree on, however, is that the evolving threat landscape and continued anomalies in human behavior mean that, despite their current infrastructures, every organization remains vulnerable to advanced phishing attacks, data loss, and data exfiltration.

As a result, a new category of technology has emerged to complement and enhance the security offered by M365. Integrated cloud email security (ICES) products, such as KnowBe4, are designed to provide core capabilities that Microsoft does not offer and to enhance protection as part of a multi-layered, defense-in-depth strategy. In addition to its ICES benefits for inbound threat detection, KnowBe4 also uses intelligent technology to prevent outbound data loss and exfiltration caused by human error and risky and malicious behavior, beyond the native security provided in M365.

Improving Phishing Detection with ICES

Gartner coined the term 'integrated cloud email security' or 'ICES' in their 2021 Market Guide for Email Security.[1] The guide introduces ICES products as a new technology category and positions them as the best defense against the advanced phishing threats that evade traditional email security controls, such as those used by M365 and SEGs.

ICES products are cloud-based and detect anomalies in inbound emails by combining APIs with advanced AI techniques, including natural language understanding (NLU), natural language processing (NLP) and image recognition. Using inline analysis and/or API access to the cloud email provider, these products have much faster deployment and time to value and can analyze email content without needing to change the mail exchange (MX) record. ICES products also detect obfuscation techniques, behavioral anomalies through heuristic detection, and compromised internal accounts. Taking it one step further, ICES products can also augment security awareness training (SAT) programs through real-time risk alerts that form teachable moments.

1 Industry analyst Forrester refers to this category of technology as 'cloud-native, API-enabled email security' (CAPES). In this guide we'll use ICES for consistency.

In their report, Gartner reflected on the future of ICES products, suggesting that they would eventually render SEGs redundant:

"Initially, these solutions are deployed as a supplement to existing gateway solutions, but increasingly the combination of the cloud email providers' native capabilities and an ICES is replacing the traditional SEG."

Get More from Your M365 Deployment with KnowBe4 Cloud Email Security

KnowBe4 Cloud Email Security is designed to provide additional layers of security within M365 to defend organizations against the advanced inbound and outbound threats that get through the platform's native controls and SEGs. In addition, KnowBe4 enables organizations to maximize the benefits of M365 and deliver extra functionality.

This guide explains the ways KnowBe4 Cloud Email Security enhances M365 and the benefits this can bring for your organization.

Anti-Phishing Defenses

Microsoft offers different anti-phishing capability depending on the license your organization has. This security is focused on detecting 'known bad' (previously identified payloads for which libraries of definitions exist) and end-user training.

All environments have Exchange Online Protection (EOP), providing traditional antivirus engines to identify known-bad malicious payloads and leveraging techniques to check URLs in inbound emails against reputation lists. By default, EOP will send suspicious emails (and spam) to end users' Junk folders, with only emails that it classifies as "High Confidence Phishing" quarantined. By procuring enhanced licenses, organizations are given access to link rewriting for URLs identified as malicious to block users from visiting phishing websites; malware detonation within their sandbox environment; the ability to retrospectively purge phishing emails from users' mailboxes once they are identified as malicious; user phish reporting; and phishing simulation training.

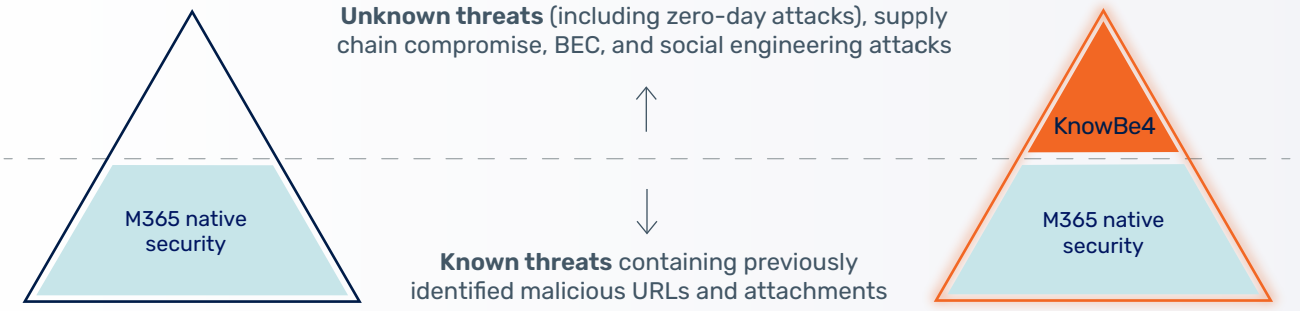
Stopping More Phishing Threats in M365 with KnowBe4 Defend

The native inbound email security in M365 is effective at addressing phishing threats containing a known payload.

Cybercriminals, however, continue to evolve their attacks to bypass this detection. This leaves organizations exposed to zero-day attacks, plus emerging attacks to cover the time lag while Microsoft's definitions libraries become available. Additionally, organizations can be exposed to "payloadless" attacks that leverage social engineering and written content within the message body, including those originating from compromised accounts on trusted external domains.

KnowBe4 Defend provides an additional layer of security to detect the threats that get through M365 native controls, with particular focus on identifying threats that traditional definitions lists cannot cater for, including zero-day events, supply chain compromise and business email compromise (BEC), spear phishing, impersonation, and CEO fraud. As Defend integrates directly with Exchange Online, rather than sitting in front of it like a SEG, messages analyzed by Defend have already been filtered by EOP, classified as legitimate emails, and delivered to the inbox. As a result, Defend delivers a valuable layer of security by detecting and neutralizing the phishing threats missed by Microsoft.

Augmenting Anti-phishing Defenses in M365 with KnowBe4



Organizations benefit from M365's effective detection of known phishing threats, which utilizes definitions libraries to determine whether a payload is malicious or not. With KnowBe4 Defend, organizations increase their detection capabilities to cover zero-day attacks ('unknown' threats) and advanced social engineering attacks, including BEC and attacks originating from compromised trusted domains.

Intelligent Phishing Detection with KnowBe4 Defend

KnowBe4 platform data shows that on average, organizations have experienced a 51% increase year-over-year in phishing attacks that evade Microsoft's signature-based detection. KnowBe4 Defend uses AI to detect and neutralize these advanced phishing attacks, and real-time teachable moments to improve employee awareness. All Defend's detection techniques are used to build a holistic understanding of an inbound email, providing more granular and reliable threat detection compared to products that implement their techniques in isolation of one another.

Linguistic and contextual analysis

Using natural language processing (NLP) and natural language understanding (NLU), Defend detects the linguistic indicators of phishing emails, including attention-grabbing subject lines, credibility statements, requests, pressure tactics and emotive language, and consequences of inaction. This enables the product to identify social engineering attacks, including those that don't contain a malicious payload but rely on the recipient to perform an action, such as BEC attacks, impersonation and CEO fraud, spear phishing, and invoice and payment fraud. Additionally, this linguistic analysis enables the product to detect the anomalies present in phishing emails sent from compromised trusted domains.

One-to-many detection

Defend proactively detects attackers' underlying techniques so it can stop the most sophisticated zero-day phishing attacks, as well as emerging threats before definition libraries are available for them.

Zero trust approach for all inbound emails

Defend implements a zero-trust approach to all inbound emails, which are analyzed pre-delivery to ensure malicious content is sanitized before it enters a user's mailbox. The product doesn't apply social graph or trust-based analysis until the technology understands the context and content of the email, enabling Defend to detect advanced threats including supply chain compromise (attacks sent from compromised trusted domains) and spoof attacks.

AI-powered phishing defense

Deployed together, Defend and KnowBe4 PhishER combine AI, machine learning, and human intelligence to provide the most advanced phishing detection. Defend analyzes emails and adds color-coded banners to deliver real-time teachable moments. Users can also report emails via the Phish Alert Button (PAB). PhishER Plus provides triage, threat hunting, and response, with PhishFlip converting real-world phishing attempts into training simulations to enhance both security and user learning.

Defend also minimizes admin friction by remediating both exact and similar threats from user inboxes, while also enabling easy threat triaging with a detailed threat table and clear workflow statuses.

How KnowBe4 Defend Proactively Protects Users from All Phishing Threats

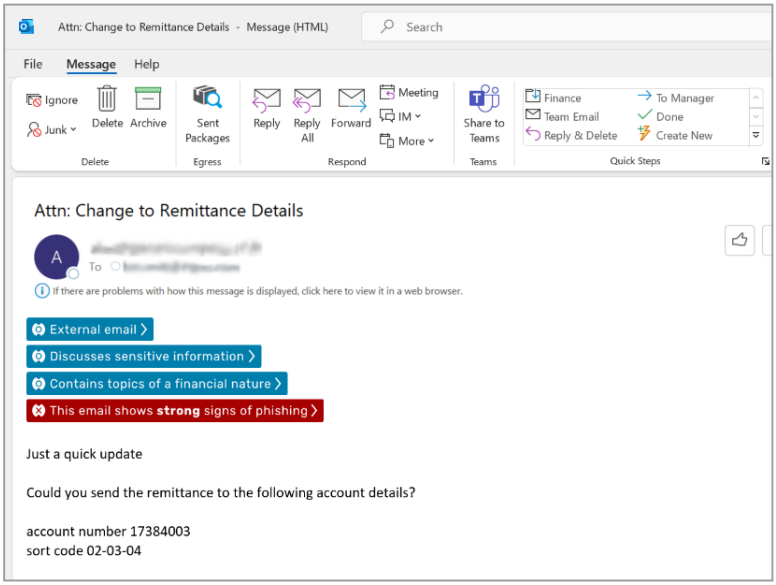
Anti-phishing guidelines consistently call out people as an unreliable mechanism for detection and reporting. People can't be expected to detect every phishing email, particularly advanced threats such as BEC. At the same time, removing any exposure to cyber threats works against SAT programs, making people even more unreliable. Additionally, non-cyber experts are unable to consistently differentiate between phishing and spam emails, which can poison some AI models.

By sanitizing emails within the inbox, Defend bridges the gap between neutralizing threats and improving employee education and awareness, while the user-based reporting built into the software has no negative impact on the technology's detection capabilities.

Dynamic banners that deliver real-time teachable moments

Defend adds banners to every external email but unlike generic warnings that stay the same, the banners vary based on the threat level detected within each email. Using a heat-based warning system, Defend shows amber and red banners depending on the severity of the threat detected, with concise explanations of risk. Users can also click on the banners to visit a webpage that explains how each email has been analyzed by Defend, with a clear explanation of the risks detected.

These visually rich and dynamic banners provide real-time teachable moments at the point of risk, transforming threats into training opportunities and are proven to tangibly reduce risk in customer environments.



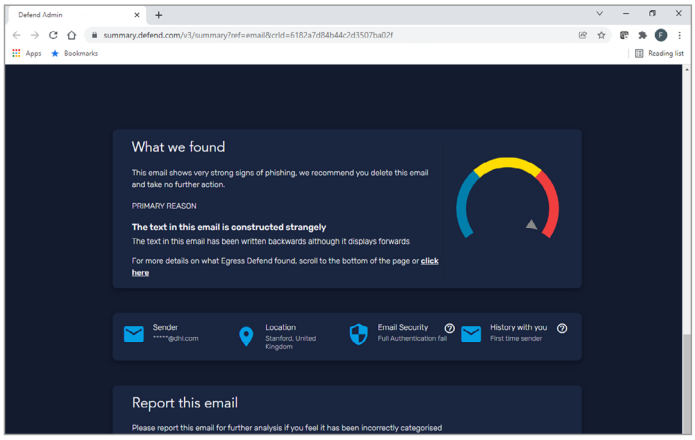
Neutralized phishing email with KnowBe4 Defend banners clearly and concisely explaining the threat.

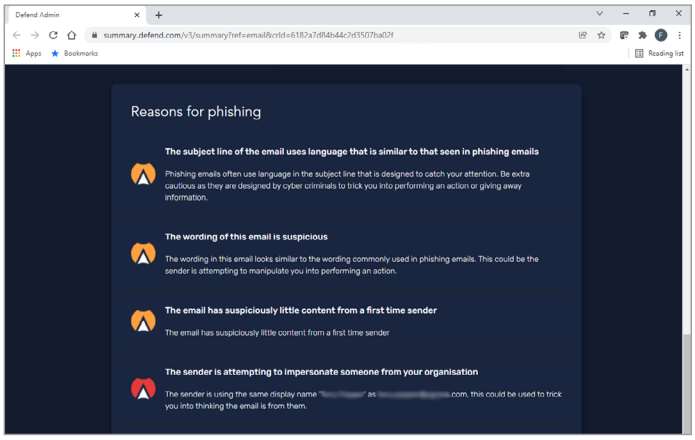
Link rewriting

Defend neutralizes all payloads, including malicious URLs. Every link contained within an inbound email is automatically rewritten and analyzed when it is clicked. Safe URLs take users directly to the legitimate website, while users are directed to an information page if they click on a phishing link despite the warning banners. This page provides a clear explanation of why the link is considered malicious and users can be blocked from visiting the phishing website itself.

Defend's detection capabilities for malicious URLs are focused on identifying anomalous redirects, brand and identity impersonation, and common link-based threats like credential harvesting. These techniques do not rely on existing definitions of "known bad" URLs, enabling Defend to augment Microsoft's SafeLink's capabilities by detecting zero-day and emerging threats, as well as URLs that are weaponized with post-delivery redirects to phishing websites.

KnowBe4 information pages block users from visiting phishing websites, while providing clear and detailed explanations of the risk.





User phish reporting

Defend empowers users to provide feedback on emails they believe have been miscategorized. The most common application for this is when Defend detects a low level of risk from an inbound email and the user detects no risk. For example, an email sent from a new external contact, which triggers a first-time sender banner in Defend.

Unlike other products, however, Defend is not reliant on this feedback to identify zero-day and emerging attacks. Additionally, this feedback is not used to inform Defend's AI detection models, meaning they are preserved from misinformation, for example spam reported as phishing, which can reduce detection capabilities in other products.

Customer Value Delivered by **KnowBe4 Defend** in M365

24,012 total number of inbound threats

(8,802 advanced threats missed by M365, and 15,210 threats detected by MS365 and sent to junk)

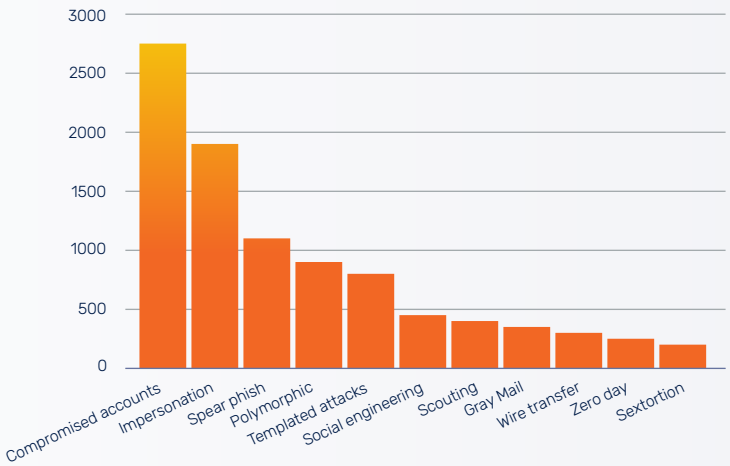
71% reduction in user interactions with phishing emails

2,789 compromised accounts

1,852 impersonation attacks

Data taken from 15,000 employees over a 30-day period.

Types of phish



Summary: Enhancing M365 Anti-Phishing Capabilities with KnowBe4 Defend

M365's native anti-phishing controls enable organizations to detect phishing emails that contain payloads (phishing links and malware attachments) that are identified in their definition lists, with some link rewriting, and end-user reporting and training capabilities, depending on their M365 licenses.

Defend enhances these controls by using intelligent technology to detect zero-day and emerging attacks that aren't available on Microsoft's definition list, and 'payloadless' attacks that leverage social engineering, including those sent from compromised trusted domains. Additionally, Defend delivers real-time teachable moments to improve employee education and awareness.

Summary of a Defense-in-depth Approach Combining M365 and KnowBe4

Augmenting M365 native security with KnowBe4 Defend enables organizations to stop more phishing attacks using Microsoft's protection for known bad attacks and KnowBe4's AI-driven and behavioral-based security for zero-day, emerging, and social engineering attacks.

		Microsoft 365 Threat intel Known bad attack protection	KnowBe4 Behavioral AI-driven Deception-driven Linguistical
Inbound hygiene	General phishing	Threat intelligence Rule-based	Linguistical
Malware protection	Full attachment/link protection	Threat intelligence	Behavioral Anti-deception
Phishing protection	External phishing Spear phishing	Threat intelligence Threat intelligence	Behavioral AI-driven Deception-driven Linguistical
Social engineering protection	BEC and impersonation fraud BEC and invoice fraud	Rule-based NO	Behavioral Behavioral
Account compromise protection	Vendor account compromise	NO	Behavioral Linguistical
Modern end user experience	Works on any device Automated safe listing	YES Threat intelligence	YES Behavioral
Simplified visibility and operations	Single pane of glass Fine grain detection and remediation	NO NO	YES YES

Outbound Email Defense

Outbound email threats are behavior-based and caused by both human error and deliberate actions.

Incidents caused by human error are completely unintentional and most commonly the result of:

- Misdirected emails, where one or more incorrect recipients are added to an email, often due to Outlook autocomplete
- Misdirected files, where one or more incorrect attachments are added to an email or attachments contain hidden sensitive data (like in a spreadsheet)
- Replying to spear phishing emails
- Failure to use the Bcc function
- Breach of internal information barriers
- Failure to protect confidential data to an appropriate level
- Replying to newly created or insecure domains

Data exfiltration, meanwhile, falls into two broad categories: well-intentioned but risky actions and malicious behavior. Well-intentioned but risky actions happen when employees knowingly break security policy while completing their work. Examples include sending company data to personal email addresses so they can work from personal devices or print at home, or not protecting sensitive data when shared externally due to complexity for sender and recipient.

People who exfiltrate data maliciously are also aware that their actions violate security policies, however their behaviors are motivated purely by personal advantage or gain – whether that's getting ahead at a new job by taking data with them, receiving financial payments for insider trading, receiving compensation from competitors, or the satisfaction of harming the company.

Microsoft's Azure Information Protection (AIP) provides static, rules-based data loss prevention (DLP) that can be used to detect some human error and deliberate data exfiltration events across the organization. This detection is based on Microsoft's out-of-the-box gateway policies that can be augmented by administrators' own rules. These policies integrate with Microsoft's classification system and work well for standardized data loss incidents, for example preventing certain classifications or types of data from being shared externally. The specific functionality provided depends on the license type an organization holds. Basic features come standard for E3 users and above, while AIP Premium P1, has more features centered on classifying documents that can then enforce DLP policies when shared via email. In addition, Microsoft provides 'Outlook Message Encryption (OME) for organizations with E3 licenses and above. OME provides basic levels of protection without end user features for tracking and revoking messages.

Stopping More Outbound Email Threats with KnowBe4 Prevent and KnowBe4 Protect

The simple ethos of KnowBe4's outbound email security is to protect an organization's most sensitive assets by ensuring only the right data is sent to the right person and with the appropriate level of security.

KnowBe4 Prevent and KnowBe4 Protect layer security on top of the standard Microsoft policies and tools, enabling organizations to address the most prevalent advanced outbound email threats caused by human error and intentional data exfiltration.

Using machine learning, deep neural networks, and other advanced techniques, KnowBe4 detects incidents that are driven by an individual's behavior at the specific time that they happen in a way that cannot be detected by static technology alone, primarily due to the unpredictable nature of this threat and scale involved to implement rules department or organization-wide.

When KnowBe4 detects that an accidental data breach is about to happen, it delivers prompts directly to the user within their mailbox (in the compose email panel), so mistakes can be corrected in real time. Additionally, email encryption can be automated without relying on end-user input, and specific risky actions can be blocked entirely.

AI-enabled Email Data Loss Prevention and Email Encryption with KnowBe4

KnowBe4's products leverage intelligent technology that makes them more scalable and flexible than static Cloud Email Security modules, meaning organizations can prevent more security incidents.

Machine learning that dynamically prevents data loss and data exfiltration

KnowBe4 Prevent uses machine leaning models to understand each individual user's behavior when using email, including the recipients and groups of recipients they contact, the regularity with which they email them, and the types of content shared.

The algorithms used include:

- **Supervised and unsupervised machine learning:** KnowBe4's machine learning is supervised by our policy engine and organizational rules set by administrators to meet a broader set of outbound email security use cases than unsupervised machine learning can alone. As well as enhanced detection and tailoring based on organizational inputs, this supervision also mitigates the chance that Prevent will learn wrong behaviors when incorrectly informed by users.

  Our self-learning technology is layered onto this and is informed by context and user behavior to provide real-time detection of the accidental and intentional behaviors that lead to data breaches.

- **Bayesian inference models:** Once deployed, Prevent is continuously learning and updating each users' behavior model to improve detection capabilities. User information is ingested as it becomes available and Bayesian inference is used to continuously update the statistical probability that a user is acting as expected.

- **Social graph database:** This technology is used to analyze each user's relationships, establishing their strength and how they interact, and enabling identification of new or atypical email recipients.

- **Gaussian mixture models:** As part of understanding whether a user is behaving as expected, Gaussian mixture models analyze their typical access patterns to highlight when they are working at unusual times or locations, which might indicate greater potential for error or intentionally malicious activity.
- **Levenshtein Distance model:** This is a metric used to measure the similarity or difference between two strings. Prevent uses this model to analyze words, email aliases and names that are similar but not identical to detect instances of mistyped email addresses, or potential phishing attempts.

Working in real time as an email is composed, these machine learning models determine whether the correct content is being sent to the correct recipient(s). When an anomaly is discovered, Prevent will prompt users to correct mistakes and can block intentionally risky or malicious actions.

Domain analysis

Prevent analyzes the domain(s) of every recipient as they are added to an email. As well as determining whether it's appropriate to share the content included in the email body and attachments, domain analysis can also be used to increase email security and reduce several additional risks.

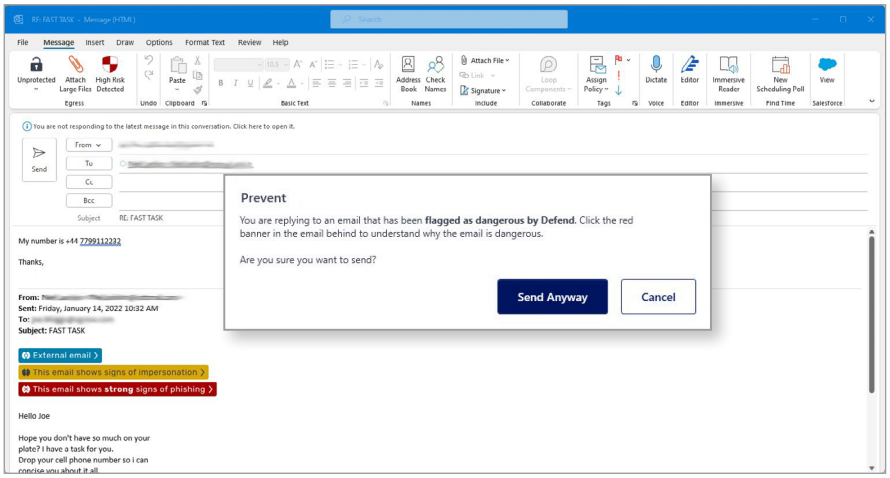
This analysis includes:

- Domain age – highlighting newly created domains
- Block-listed domains
- TLS hygiene/status

Stopping responses to phishing emails, including impersonation attacks

When a user replies to an email they have received, Prevent conducts its advanced domain analysis. Domain age and block-listing can be used to detect responses to phishing attacks, including scenarios where a spoofed email address has been used and masked from the end user or was difficult for them to detect.

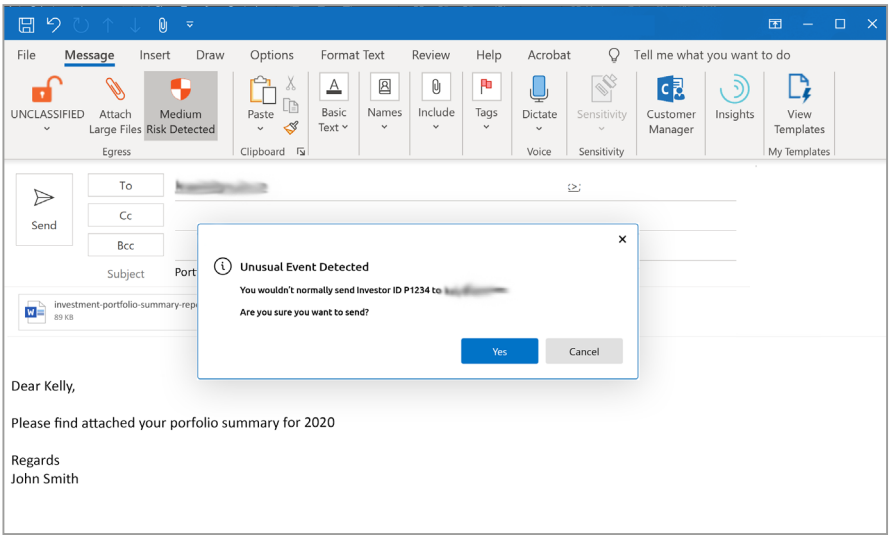
Dynamic KnowBe4 Prevent prompt alerts user to reply to a phishing email.



Content analysis

Prevent analyzes the content contained in the email body (including earlier messages within email threads) and any attachments. Leveraging its machine-learning models, Prevent compares the content with the recipients and the senders' previous behavior patterns to detect misdirected emails and files, as well as data exfiltration.

KnowBe4 Prevent uses intelligent technology to analyze email recipient(s) and content to prompt users when they inadvertently include incorrect email address(es) or attach incorrect file(s).



Monitoring employee departures

As Prevent is continuously analyzing each user's behavior, it can alert administrators to unusual behavioral patterns that have been detected (while also blocking risky actions and those that violate security policy). This includes detecting key indicators that an employee is about to resign from their position, for example sending certain data to their personal email address to be used in a new job.

Once a user has formally resigned, they can be placed on a "watch list" until their contract ends, with greater policy controls to stop user departure exfiltration.

Automating email encryption

Prevent performs content inspection for sensitive data in the message body and attachments for every email. Customizable policies scan the subject line, message body, and attachments for sensitive data, such as social security numbers, financial details, or other specified keywords and expressions. Prevent can also detect Microsoft AIP metadata and apply policy based on these identifiers.

KnowBe4 uses this data to perform a risk assessment of the message and the recipient(s) it is being sent to and will prompt the user if it identifies sensitive content or a potential security problem. Users can be notified to encrypt emails where the risk is high or encryption can be automated using KnowBe4 Protect, with the message body and attachments seamlessly encrypted with 256-bit AES encryption to keep all data secure and accessible to the intended recipients only.

Transport Layer Security (TLS)

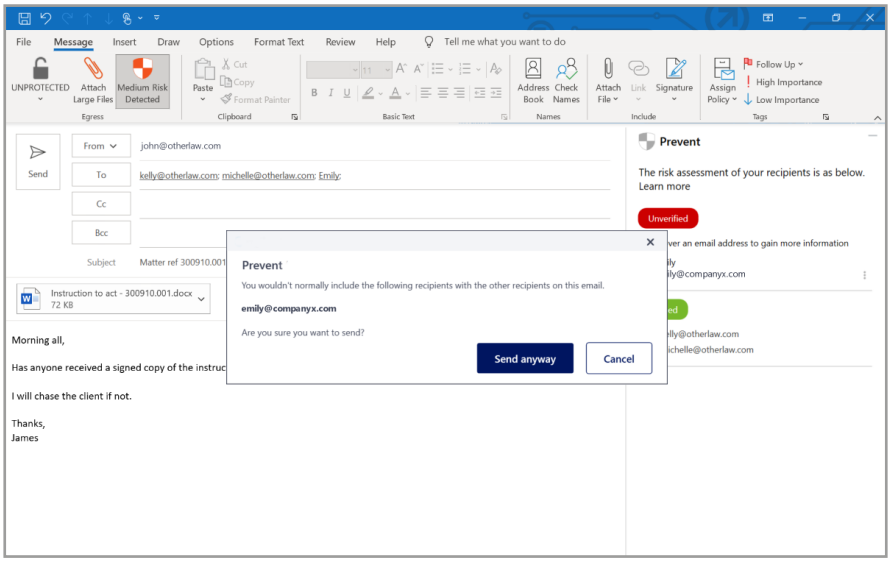
Where sender organizations have configured for opportunistic TLS to fail open, senders are not notified that the message will be sent unprotected if TLS is not correctly configured by the recipient organization(s).

When analyzing recipient domains, Prevent determines whether the correct configuration is in place to allow emails to be sent via TLS. Where it is not in place Prevent can notify the sender that their email will be sent unprotected and prompt them to use email encryption (such as Protect) to secure sensitive content. Additionally, where risk to sensitive data is high, Prevent can notify the user to apply more protection even when TLS is available or can automate encryption via Protect.

Dynamic prompts within the mailbox for real-time tangible risk reduction

Prevent delivers real-time notifications to users at the point when risk occurs. These prompts differ significantly to static DLP products, which are formulaic in format and frequency – for example, notifying the sender every time they send an email to an external domain or asking them to approve every recipient and attachment before an email is sent. These static products lead to click fatigue, where the sender no longer reads or checks the prompts.

Instead, Prevent only prompts users when a risk is detected, drawing attention to it in real time in the email ribbon and via an expandable side panel. Prevent's prompts are also customizable and will change based on the warning being given. As a result, Prevent provides value to the user at the point of risk, without overloading them with unhelpful or irrelevant checks. As part of KnowBe4's philosophy of real-time teachable moments, Prevent transforms threats into training opportunities and tangibly reduces risk.



KnowBe4 Prevent alerts users to risk through a combination of the Prevent Shield within the Outlook ribbon, expandable side panel, and dynamic pop-up alerts.

Preserving rules for the transmission of classified data and information barriers

One of the biggest advantages of M365 E3 and E5 licences is the additional security capabilities available. KnowBe4 can integrate with these capabilities, like AIP, to deliver targeted use cases such as advanced DLP, information barrier protection, or specific rules aligned to the transmission of classified data.

As part of the KnowBe4 Outlook Add-in and combined with KnowBe4's gateway infrastructure, Prevent enforces information barriers and ethical walls within an organization based on the system

administrators' customizable parameters. Using space between Graph and API to access metadata, as well as other data sources within the organization, KnowBe4 can dynamically manage and synchronize keywords, terms, and policies to preserve information barriers on email.

Certified email encryption with enhanced rights management controls

Protect provides certified AES 246-bit encryption to protect sensitive files and content shared by email. Through integration with Prevent, encryption can be automated based on organizational policies and real-time risk to confidential data as it is shared by email.

Encryption can also be applied by the user. A user-friendly Outlook add-in makes it easy to encrypt email content by selecting the appropriate option. This menu and related encryption policies are fully customizable by an organization.

Revoking access to sent emails and additional access controls

As Protect provides message-level encryption, both users and administrators can revoke access to encrypted emails after they have been sent to prevent unauthorized access to sensitive data.

Additionally, each encryption label applies varying levels of permissions and control, including read-only access, disabled attachment downloads, and restricted forwarding. The different options also assign their own recipient authentication.

Authentication

KnowBe4 offers multiple authentication measures to reduce recipient friction. Trusted recipients enjoy seamless authentication without needing to log into the KnowBe4 web portal. However, portal-based access, multi-factor authentication, SSO via OpenID, and access using a shared secret remain options for when the risk to sensitive data is higher.

Customer Value Delivered by **KnowBe4 Prevent** in M365

566 total number of incidents detected

(of which 11% previously identified, and 89% previously unidentified)

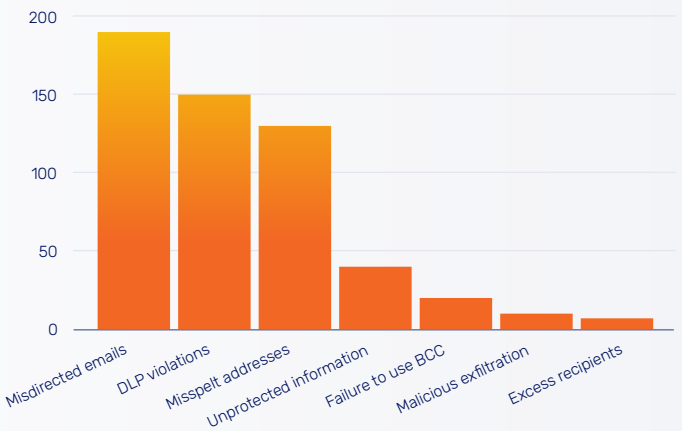
233 accidental data breaches prevented

223 instances of human error

203 instances of data exfiltration

Data taken from a legal firm with 3,000 employees over a 60-day period.

Types of outbound threats



Summary: Enhancing M365 DLP and Encryption Capabilities with Prevent and Protect

M365's native DLP controls enable organizations to prevent some human error and data exfiltration security use cases using static rules and email encryption.

Prevent and Protect enhance these controls by using intelligent technology to detect the abnormal behavior that leads to data loss and data exfiltration to dynamically prevent risks and automate protection for sensitive content. In addition to ensuring the right content is sent to the right recipient with appropriate protection, Prevent delivers real-time teachable moments that improve employee education and engagement.

Summary of a Protection-in-depth Approach Combining M365 and KnowBe4

		Microsoft 365	KnowBe4
		Static Rules	Static rules ML AI-based detection
Email data loss prevention	Advanced DLP detection for sensitive content	Gateway-based, standard libraries	Client-based, custom libraries
Information barriers	Prevent cross-boundary communication for sensitive or restricted content	Azure AIP provides classification markings	Static rules synchronized with OU/group membership
Misdirected email protection	Prevent emails being sent to the wrong person	Not supported	ML AI-based detection
Mis-attached file protection	Prevent mis-attached files/data being sent to the wrong person	Not supported	ML AI-based detection
Data exfiltration detection	Prevent and alert on data exfiltration events	Not supported	ML AI-based detection
Enforced email security	Automatically apply appropriate message security	Azure AIP feeds into classification status	TLS Message-level encryption applied based on classification and destination
Track sensitive content	Automatically classify encrypted content and track delivery	Azure AIP	KnowBe4 Classification feeds into message-level encryption
Revoke or expire encrypted emails	Stay in control of encrypted content at all times	Office Add-in	Message-level encryption
Realtime Domain Analysis	Perform domain hygiene analysis for email addresses	Basic domain verification only	Authenticity, reputational analysis including lookalike/ anomaly detection

Conclusion: Combining KnowBe4 and Microsoft Email Security to Stop More Inbound and Outbound Threats

Combining KnowBe4 and Microsoft is an effective defense-in-depth email security strategy. KnowBe4 has purpose-built its Cloud Email Security modules to be highly complementary to M365, using technologies not provided by Microsoft or SEGs to provide enhanced security and to support an increased number of use cases.

When customer organizations layer KnowBe4's advanced technology into their M365 environment, they benefit from intelligent threat detection and prevention capabilities to stop more inbound and outbound threats, without a costly and cumbersome duplication of features.

By enhancing M365 with KnowBe4 Cloud Email Security, organizations are proven to detect the advanced phishing attacks (including BEC, impersonation attacks and CEO fraud, invoice and payment fraud, etc.) that are engineered to circumvent Microsoft's detection capabilities. At the same time, organizations enhance their outbound security and controls with KnowBe4's machine learning-based DLP and certified email encryption to stop security incidents caused by human error and data exfiltration, as well as ensure confidential data has the correct level of protection applied.

Integrated seamlessly into M365, KnowBe4 Cloud Email Security is fast to deploy and provides immediate value. With KnowBe4 deployed directly into Microsoft Outlook for Windows and Mac, Outlook Web Access (OWA) and all mobile platforms, users require minimal or no training and no changes to working practice. Users also benefit from real-time teachable moments, delivered through banners and prompts directly in the inbox, tangibly reducing risk and augmenting SAT programs.

The improvements to email security delivered by combining KnowBe4 and Microsoft enables organizations to increase their resilience in today's evolving threat landscape, operate with greater efficiency, and protect themselves from the reputational damage, financial impacts, and customer churn associated with breaches of email security.

Learn more about KnowBe4's innovation in the ICES space and how it can help you protect your organization.

Learn more

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 empowers your workforce to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps you strengthen your security culture and manage human risk. KnowBe4 offers a comprehensive AI-driven "best-of-suite" platform for human risk management (HRM), creating an adaptive defense layer that fortifies user behavior against the latest cybersecurity threats.

The HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time security coaching, crowdsourced anti-phishing, AI Defense Agents and more. As the only global security platform of its kind, KnowBe4 transforms your largest attack surface—your workforce—into your biggest asset, actively protecting your organization against cybersecurity threats.

For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

01F01K04