



knowbe4

Are You Ready to Replace Your SEG?

Email Security Guide

WWW.KNOWBE4.COM



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

00060825

Inside this Report

- **03** CISOs Are Replacing Their SEGs in the Modern Email Security Stack
- **04** Engineered to Evade: The Phishing Attacks Getting Through the SEG
- **06** A Question of Context: Static Data Loss Prevention Can't Stop Human Error and Data Exfiltration
- **08** Are You Ready to Replace Your SEG?
- **09** Stop Advanced Phishing Attacks and Data Loss in Microsoft 365

CISOs Are Replacing Their SEGs in the Modern Email Security Stack

The email threat landscape is evolving at a sprinting pace – and cybersecurity leaders say their traditional defenses can't keep up.

Two forces have aligned to cause cybersecurity leaders to question the value of their secure email gateways (SEGs).

The phishing threat landscape continues to evolve at an incredible rate, fueled by technological advances (such as AI); the adoption of cloud services and applications accessed through single sign-on credentials; and an ever-increasing crime-as-a-service ecosystem that retails advanced phishing attacks with money-back guarantees for ROI.

At the same time, Microsoft has invested heavily in its core Microsoft 365 platform, including its email security defenses. This has brought its email threat detection capabilities in line with those offered by SEGs for both inbound phishing emails and outbound data loss and exfiltration.

Our [Email Security Risk Report](#) found that cybersecurity leaders are frustrated with their SEG. The top inbound issue was that too many phishing emails end up in employees' inboxes and the top outbound concern that it isn't effective in stopping misdirected emails and files caused by human error.

These feelings are founded: despite deploying perimeter email security via Microsoft Exchange Online Protection and SEGs, 94% of organizations experienced inbound and outbound incidents.

Consequently, 87% of cybersecurity leaders are considering replacing their SEG with Microsoft 365 native controls and AI-driven integrated cloud email security (ICES) solutions – or have already done so.

In this modern email security stack, organizations leverage Microsoft 365 native security to prevent traditional threats and spam, and an ICES solution to stop the advanced inbound and outbound threats that get through Microsoft – meaning that in most organizations, the SEG's days are numbered, if not already ended.

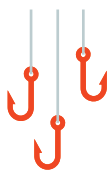
Engineered to Evade: The Phishing Attacks Getting Through the SEG

With more phishing emails bypassing SEG detection, organizations are left vulnerable to advanced attacks.

The widespread adoption of signature-based and reputation-based email defenses, whether through Microsoft's native controls or a SEG (or both), means that getting through these defenses is now a minimum requirement for every successful phishing campaign.

In the March 2025 edition of our [Phishing Threat Trends Report](#), our Threat Intelligence Analysts highlighted a 47% increase in the number of attacks getting through SEG detection. The majority of these emails passed authentication checks, including DMARC (a primary detection capability used by SEGs).

When analyzing the attacks getting through, we found:



58%

were sent from compromised accounts, enabling them to more easily bypass reputation-based detection.



Phishing hyperlinks

were the most frequent payload, as these websites can be created and recreated faster than they can be blocklisted.



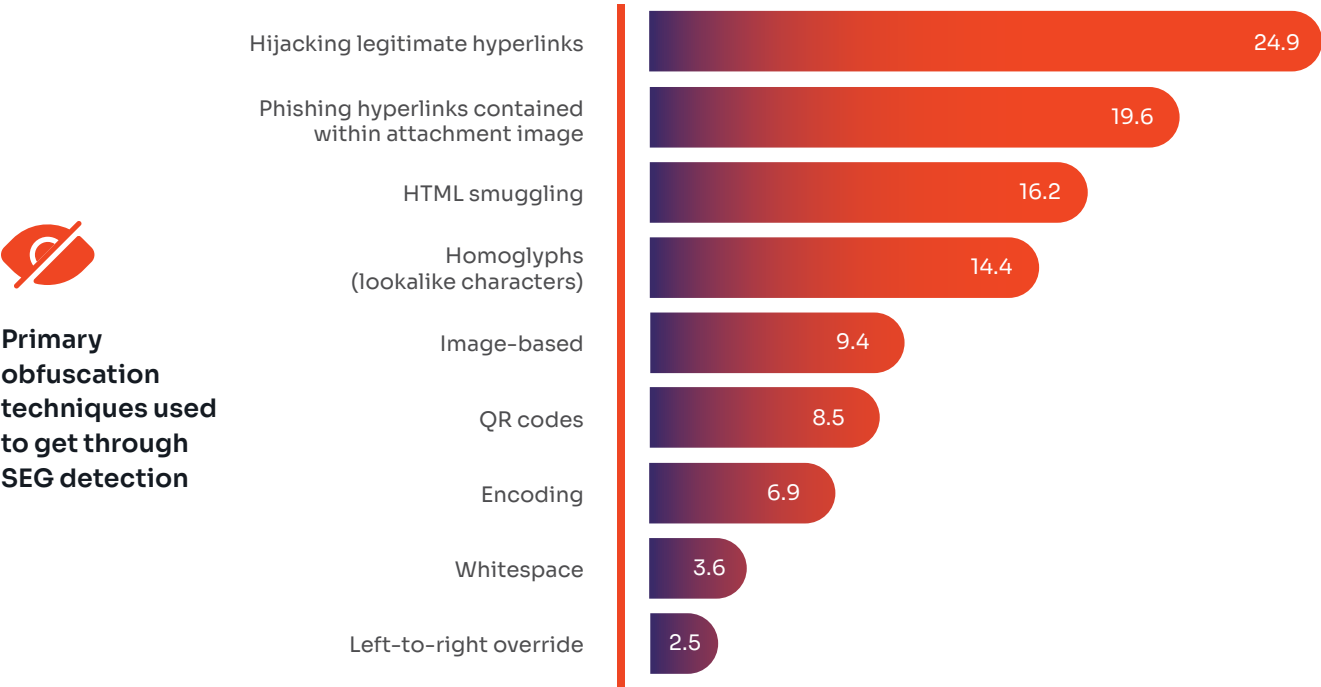
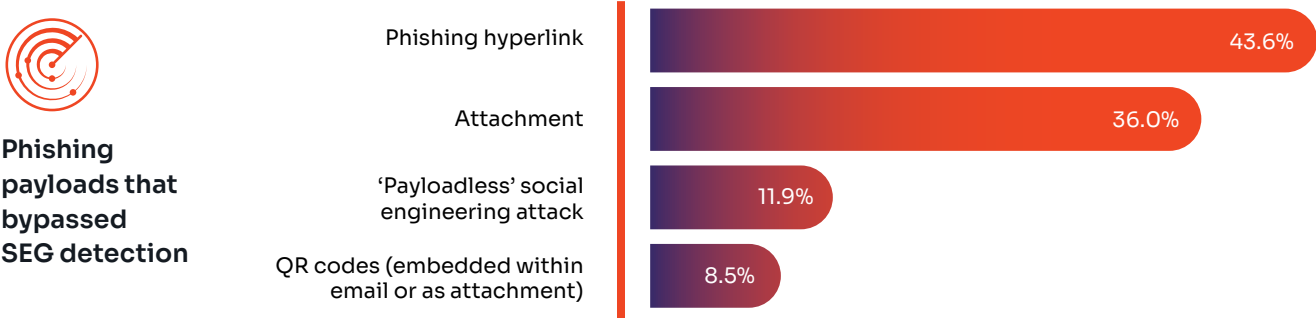
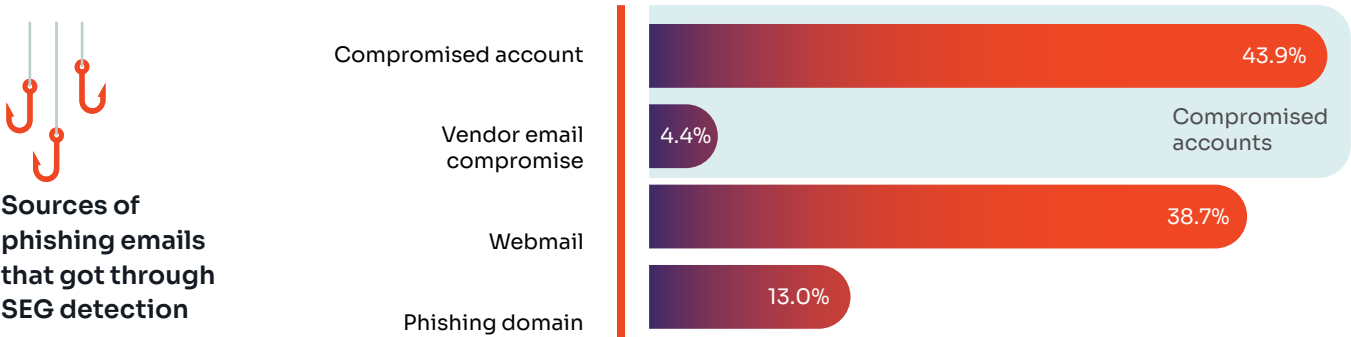
A 23% increase

in the use of technical obfuscation measures that enabled them to evade detection, such as hijacking legitimate hyperlinks (e.g to file sharing sites), HTML smuggling and quishing.

Once these threats find their way into the inbox, organizations are reliant on employee reporting or external threat intelligence to identify them. It then becomes a race against time to remove the email from any other mailboxes before an employee falls victim – a race that's unfortunately supported by a slow and manual search and delete process. This process is also ineffective for polymorphic phishing campaigns and heterogeneous attacks, with changes to phishing emails leaving security analysts at a loss for what to look for.

While the capability offered by SEGs and Microsoft is effective at blocking bulk known attacks, organizations urgently need enhanced detection to stop the advanced threats they are still vulnerable to, including zero-day and emerging attacks, phishing emails sent from legitimate but compromised accounts, and social engineering and technical attacks.

In numbers, how many phishing emails are getting through SEG

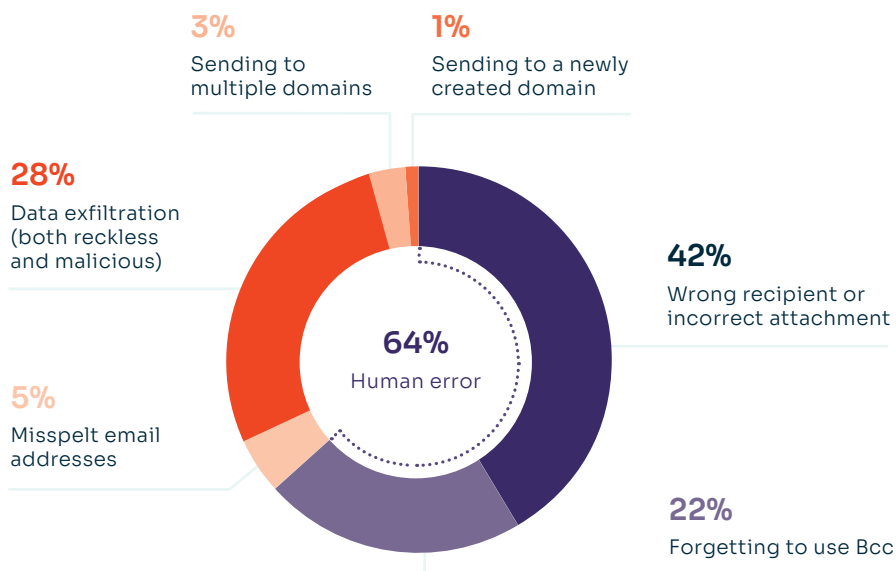


A Question of Context: Static Data Loss Prevention Can't Stop Human Error and Data Exfiltration

People are most likely to leak sensitive information via email and solely relying on a rules-based approach can't prevent the behaviors that lead to breaches.

There's a wide margin for human error when using email – from Microsoft Outlook autocomplete suggesting the wrong recipients or forgetting to use Bcc, to attaching the wrong file(s) or not removing hidden data. Similarly, people frequently “break the rules” by sending privileged information to a personal address to print or work on using a personal device. Finally, people also intentionally exfiltrate data for personal gain, such as client or project information to a new job.

Platform data from 1.7 million emails analyzed by KnowBe4 reveals human error is the most common DLP trigger



Despite using static DLP, 91% of organizations experienced outbound email security incidents.

Put simply: on its own, the static, rules-based email data loss prevention (DLP) offered by SEGs can't detect and prevent this broad range of outbound incidents that organizations are exposed to. It isn't intelligent enough to understand both the content and context of every email being sent to cater for every incident at scale across an organization. For example, it might be entirely appropriate for one employee to send emails to a webmail address but not for another, so rules would have to be deployed per individual, which is manual and time-consuming.

Despite using static email DLP, 91% of organizations surveyed for our Email Security Risk Report experienced outbound email security incidents and 94% of these suffered negative outcomes as a result including loss of revenue, operational impacts, regulatory penalties and customer and employee churn.

One-hundred percent of cybersecurity leaders relying on static email DLP expressed frustrations with it. The biggest issues were the need to alter rules because they were negatively impacting operational efficiency and, consequently, the high level of admin overhead required to maintain them.

Static email DLP works for "set and forget" blanket policies that are a catchall across all teams and departments, for example preventing all employees from sharing a specific type of information externally.

Organizations, however, also need to layer intelligent email DLP into their tech stack to enhance threat detection. By leveraging machine learning to deeply understand each employee's behavior, intelligent email DLP detects when they are about to make a mistake or intentionally exfiltrate data to proactively prevent incidents.

Organizations need to layer intelligent
email DLP into their tech stack to
enhance threat detection.

Are You Ready to Replace Your SEG?

In a small proportion of organizations, SEGs may continue to deliver value for non-security use cases. For almost all, however, the combination of Microsoft's native controls and ICES will simplify their tech stack to avoid duplication of features between Microsoft and the SEG and potentially offer budgetary savings, while also enabling them to detect and prevent a broader spectrum of both inbound and outbound threats.

Specifically, the evolution of advanced phishing threats and unpredictability of human behavior means all organizations must enhance their defenses beyond the traditional signature-based and reputation-based controls and static email DLP offered by Microsoft and SEGs.

To effectively manage human risk on email, organizations must deploy AI-driven email security that provides behavioral and context-based analysis of advanced threats, such as that offered by [KnowBe4 Cloud Email Security](#). This enhancement of the email security tech stack is now table stakes; without it, organizations will remain highly vulnerable to email security incidents and the negative fallout that follows.

SEG Solution Guide

Read our solution guide '[Can you replace your SEG?](#)' for key considerations when evaluating your email tech stack.

Download



Stop Advanced Phishing Attacks and Data Loss in Microsoft 365

People are organization's biggest risk – and they're most vulnerable when using email.

To empower organizations to manage human risk on email KnowBe4 takes a new approach to behavioral-based threat detection and response.

We've architected a single cloud-based intelligent platform that enhances Microsoft 365's native controls and SEGs to help eliminate advanced inbound and outbound threats from getting through.

The world's first cloud email security platform to use an adaptive security architecture, we automate threat detection and response for advanced phishing attacks, data loss, and data exfiltration.

Combining contextual machine learning and AI, we use zero-trust and pre-generative modeling to provide the highest efficacy of inbound threat detection, while leveraging social graph and pretrained deep neural networks to detect human error and data exfiltration. Our products are easy to deploy and provide immediate time to value. KnowBe4 also offers a powerful combination of contextual banners and prompts that provide in-the-moment education when people need it most.

[Request Demo](#)



[Learn More](#)





Free Phishing Security Test

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



Free Email Exposure Check

Find out which of your users emails are exposed before the bad guys do



Free Automated Security Awareness Program

Create a customized Security Awareness Program for your organization



Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain



Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click

About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps to strengthen security culture and manage human risk. KnowBe4 offers a comprehensive AI-driven “best-of-suite” platform for Human Risk Management, 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 coaching, crowdsourced anti-phishing, AI Defense Agents and more. As the only global security platform of its kind, KnowBe4 utilizes personalized and relevant cybersecurity protection content, tools and techniques to mobilize workforces to transform from the largest attack surface to an organization’s biggest asset. For more information, please visit www.KnowBe4.com.



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

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.