Abnormal

# CISO Guide to Replacing Your SEG

## Protect More and Spend Less with a Modern Solution

MKT340_Aug_2023

# Introduction

The last few decades have seen a massive transformation in the way we think about email security. From the days of server-hosted email to the present age of cloud-based email, the security landscape has dramatically changed.

**400%**

year-over-year increase in advanced phishing attacks.

*CyberTalk*

**$9.44M**

average cost of a breach in the United States.

*IBM Cost of a Data Breach Report*

**$2.7M**

lost due to business email compromise attacks in 2022.

*FBI Internet Crime Report*

**55%**

increase in the number of BEC attacks in 2023.

*Abnormal Security*

The first email security solutions relied on attack signatures to detect viruses. However, variants were quickly developed by bad actors to sidestep detection. Enterprise teams soon discovered that staying ahead of the evolving attack landscape would require more expansive security tools.

The second generation of email security was characterized by proactive attempts to combat viruses and malicious links that arrived in a recipient's inbox, and was marked by the introduction of the secure email gateway—the SEG. When this technology first launched, gateways were very effective at securing email from common email threats, especially those with payloads.

Unfortunately, threat actors have become even more sophisticated since the advent of the SEG. Modern cybercriminals utilize advanced attack methods that rely on social engineering techniques to complete their scams. These business email compromise (BEC) attacks often impersonate high-profile executives, vendors, and partners to convince the target to wire money or send confidential information.

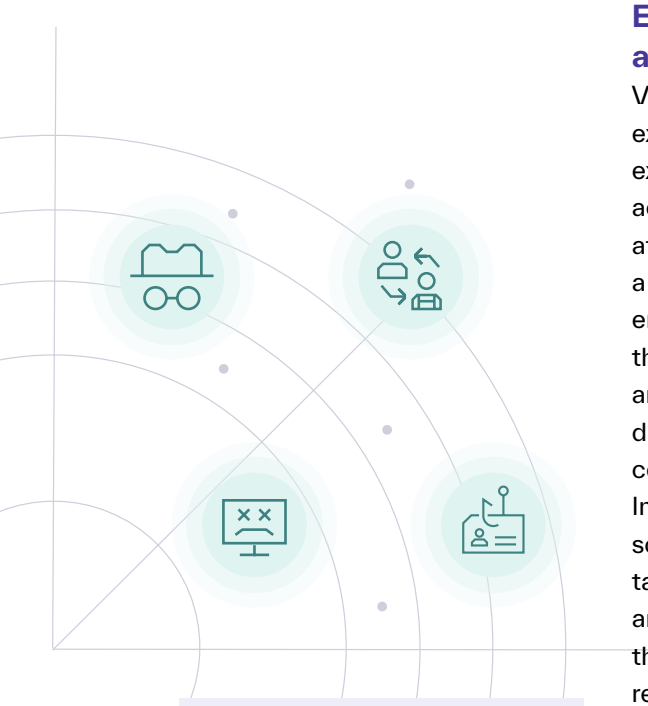
Since 2013, BEC alone has resulted in more than $51 billion in exposed losses globally, with $2.7 billion in actual losses in 2022 alone. And that says nothing of the modern credential phishing, malware, and lateral spear phishing attacks that have grown in sophistication as well.

The attacks are successful because traditional email security tools lack the sophistication to combat these modern threats. Once they arrive in inboxes, employees can open and respond to them, putting your organization at risk of financial and reputational damage.

So what can be done? It's time to move into a new era of email security—one that uses behavioral AI and natural language processing to understand your organization and then block anomalous activity—even when traditional indicators of compromise are not present. By replacing your secure email gateway with a modern email security solution, you can protect against more attacks, spend less time and money on email security, and secure your organization against future shifts in the cyber threat landscape.

# Types of Modern Attacks Bypassing the SEG

While SEGs are great at leveraging threat intelligence, they are ineffective against the advanced threats created by modern email threat actors. Here are just a few types of attacks bypassing SEGs today.



It's worth noting that these are only a few types of email threats seen today, and are only a subset of the attacks that bypass the SEG. Attackers are becoming increasingly savvy, in large part due to the widespread adoption of generative AI, and constantly changing tactics to stay ahead of threat intelligence.

## Executive Impersonation and BEC

Various kinds of BEC attacks exist, but they all depend on exploiting trusted relationships to achieve their objectives. In these attacks, threat actors impersonate a CEO, CFO, or other high-ranking employee to make a request of the target—often to purchase and send gift cards, update their direct deposit information, or send confidential information via email. In contrast to standard email scams, these attacks are highly targeted and require research and personalization to convince the victim to complete the requested action. But because they are typically text-based, sent from a known domain, and have no malicious links or attachments, they bypass traditional detection tools.

## Malware and Payloadless Malware

While traditional malware is often stopped by the SEG, attackers have again learned how to bypass security tools. Payloadless malware is on the rise, where an attacker will send an email, often a fake payment receipt, and then request follow-up via phone. From there, they can convince the recipient to download malware to the device to reverse payment. Because it lacks any payload—no .exe files or Google Drive links to be found—traditional tools have a hard time detecting these messages.

## Vendor Impersonation and VEC

Vendor email compromise or VEC is a more malicious subset of BEC, where attackers impersonate vendors to request payment of invoices or an update to banking account information. VEC attacks are highly successful because conversations with vendors are inherently financially-focused and threat actors know how to exploit these trusted communications with customers. Making matters worse, cybercriminals are becoming increasingly resourceful in invading vendor email accounts and using legitimate invoicing information to trick their targets.

## Credential Phishing

Phishing is the most common advanced email threat faced by organizations, accounting for two-thirds of all advanced attacks. These emails appear to come from trusted brands or people and lure victims into providing login credentials to various accounts—giving the attacker access to email accounts, banking accounts, social media accounts, and more. Secure email gateways can stop simple phishing attacks that contain obviously malicious links or attachments, but more sophisticated phishing messages with hidden redirects or multi-step processes often sail through.

# Impact of Modern Attacks Bypassing the SEG

**$51 billion**
in exposed losses due to business email compromise.

*FBI IC3*

**74%**
of data breaches include the human element.

*Verizon DBIR*

**300K+**
total reported phishing incidents in 2022.

*FBI IC3*

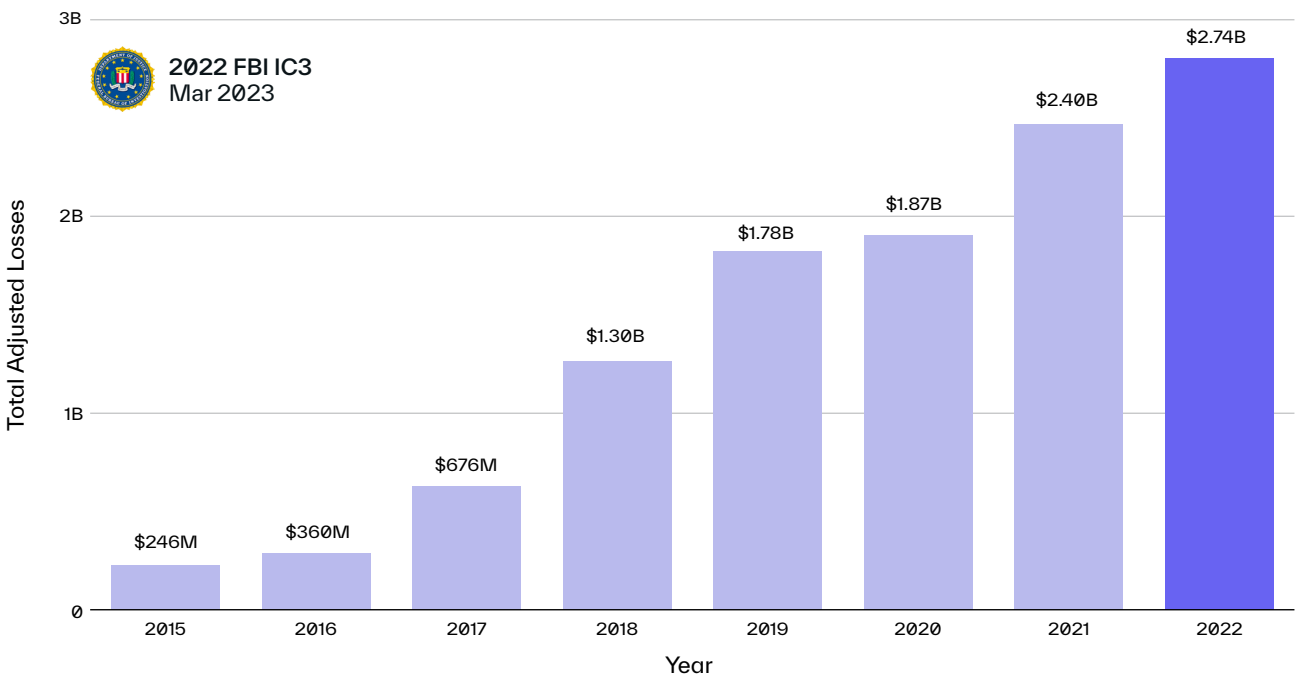
Modern email attacks have had a significant impact on the safety and security of online communication. Without advanced email security, attackers continue to wreak havoc on organizations across the globe—costing billions in losses annually.

The FBI Internet Crime Complaint Center (IC3) recently released an updated Public Service Announcement, identifying nearly $51 billion in exposed losses due to business email compromise since the attack type was first identified in 2013. The frequency of BEC attacks has doubled over the past year—making up nearly 60% of all social engineering incidents, according to Verizon's 2023 Data Breach Investigations Report.

According to Abnormal data, BEC attacks—known for their reliance on text-only emails and social engineering tactics—grew in volume by 55% in 2023. This is an increase from 1.63 attacks per 1,000 mailboxes in the latter half of 2022 to 2.52 attacks over the first half of this year. And only two years ago, there was fewer than one BEC attack per 1,000 mailboxes, showcasing how quickly this threat has grown.

And while security awareness training can prevent some of these losses, malicious attackers continually adapt their tactics in order to remain one step ahead of advancements in tech and education. Unfortunately, their efforts are often successful.

**Losses from BEC Attacks Continue to Grow**



# Why SEGs Are Ineffective at Stopping Modern Attacks

Secure email gateways were designed to defend against basic attacks that rely on known indicators of compromise—attacks that are high in volume but low in impact. When you have a mountain of email traffic coming in and out of your organization, a SEG can be effective at filtering known threats out of the email tenant at scale.

However, they were never designed to stop highly-targeted, socially-engineered attacks that are sent from known domains without indicators of compromise. They simply do not have the detection capabilities needed to do so, and they also fail to detect emerging threats that go beyond email into adjacent applications or channels.

## The Gaps in Your Secure Email Gateway

With an in-depth knowledge of how SEGs work, threat actors have evolved their tactics—leveraging positive signals in their emails, such as recognized domain names and legitimate accounts. They've simultaneously removed negative signals like malicious links and attachments in order to bypass the tools put in place to thwart them.

Some examples of leveraging positive signals include:

- Sending a message from a legitimate email account that the attacker has compromised. This is mostly commonly seen with VEC attacks.
- Sending a message via legitimate sending infrastructure that passes authentication checks like SPF, DKIM, and DMARC.
- Leveraging multiple stages for phishing or malware payload delivery.
- Seeking engagement outside of email, such as over the phone or a service like WhatsApp for payloadless malware delivery.

By removing negative signals, and threat actors can evade traditional threat detection techniques that rely on intelligence and heuristics based on those signatures.

> Put more simply, they are **outsmarting the threat intelligence systems put in place to block them**—using new techniques to deliver their email attacks.

Starting small, requesting payment via PayPal, Apple Pay, or Zelle

# Real-World Examples of Attacks That Bypassed the SEG

Having a better understanding of the types of attacks that bypass the traditional SEG is helpful, but seeing real-world examples showcases the full threat. Let's take a closer look at the specific ways these attacks work.

## A Traditional BEC Attack that Bypassed the SEG

This first example depicts a BEC threat originating from a compromised Gmail account seeking a relatively small payment via PayPal, Apple Pay, or Zelle.

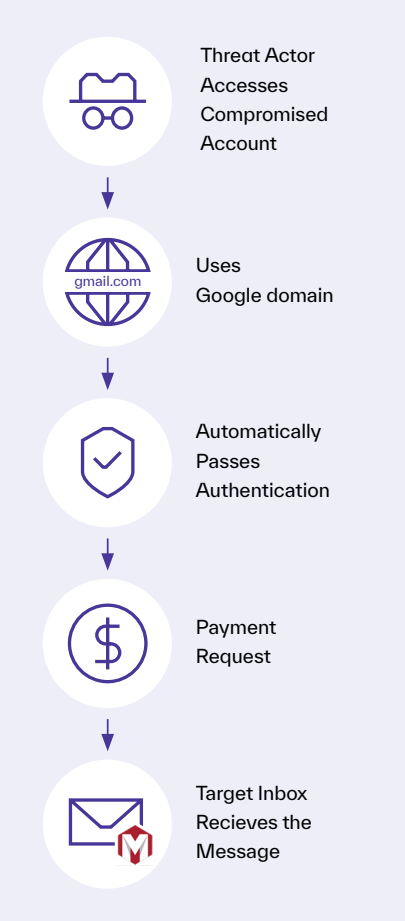
**BEC Threat from a Compromised Gmail Account**

**Subject:** Paypal favor
**From:** [redacted] <[redacted]@gmail.com>
**To:** [redacted] <[redacted]>
**Date:** September 27, 2022 at 8:03 AM

**Hi Kerry,**
**How are you? Can I ask a favor? Do you use PayPal or Apple Pay? I needed to pay a client for $520 but PayPal closed my two accounts. Try to see if you can lend it to me. I only use Zelle and check. I appreciate it.**

**Regards,**

**[redacted]**
**Attorney at Law**
**McKinney & Co**




This email bypasses the SEG because it is sent from a Google domain, which automatically passes SPF, DKIM, and DMARC authentication.

**Sender Identity Analysis**

**Sender ID**

Sender Display Name

Sender Email Address

@gmail.com UNKNOWN IDENTITY

Sender Domain

**gmail.com**

Sender Authentication

SPF: PASS

DKIM: PASS

DMARC: UNKNOWN

The recipient of the message engaged and was ultimately prompted to pay the criminal, who uses the the name of the law firm in the PayPal account to add legitimacy:

**On Wed, Sep 28, 2022, 8:42 PM, , @gmail.com wrote:**

**@ mckinney**
**Please send the screenshot upon payment. I will send you the receipt by email after receiving it.**

**Best regards,**

## An Invoice Fraud Attack that Bypassed the SEG

In this next example, the threat actor is impersonating a vendor in an attempt to redirect ACH payments to an external fraudulent account. They try to trick the user by stating that their organization is undergoing a system change and the banking information needs to be updated.

The attacker has cc'd an email address that uses a look-alike domain to ensure that they can track the conversation and even continue it in the event they can no longer control the compromised account:

"please update your banking information"

**An Invoice Fraud Attack**

**Subject:** ACH Vendor Enrollment
**From:** < lisa@companyname.com>
**To:** [redacted] <[redacted]>
**CC:** Vendor Maintenance <vendor@lookalikecompany.com>
**Date:** February 6, 2023 at 3:28 PM

**Hi,**

**I emailed Vendor Maintenance awhile back and have yet to hear back from them.**

**We are undergoing a system change, our account information for invoices has been updated due to our (Q1) bank financial reconciliation, and we cannot receive or transmit money until the review is complete.**

**To prevent credit loss, we permit all future payments to be sent to our primary bank account which is attached.**

**Please confirm the change as quickly as possible, and if you need additional information, please reply to this email as soon as possible.**

**Thank you,**
**Lisa** [redacted]

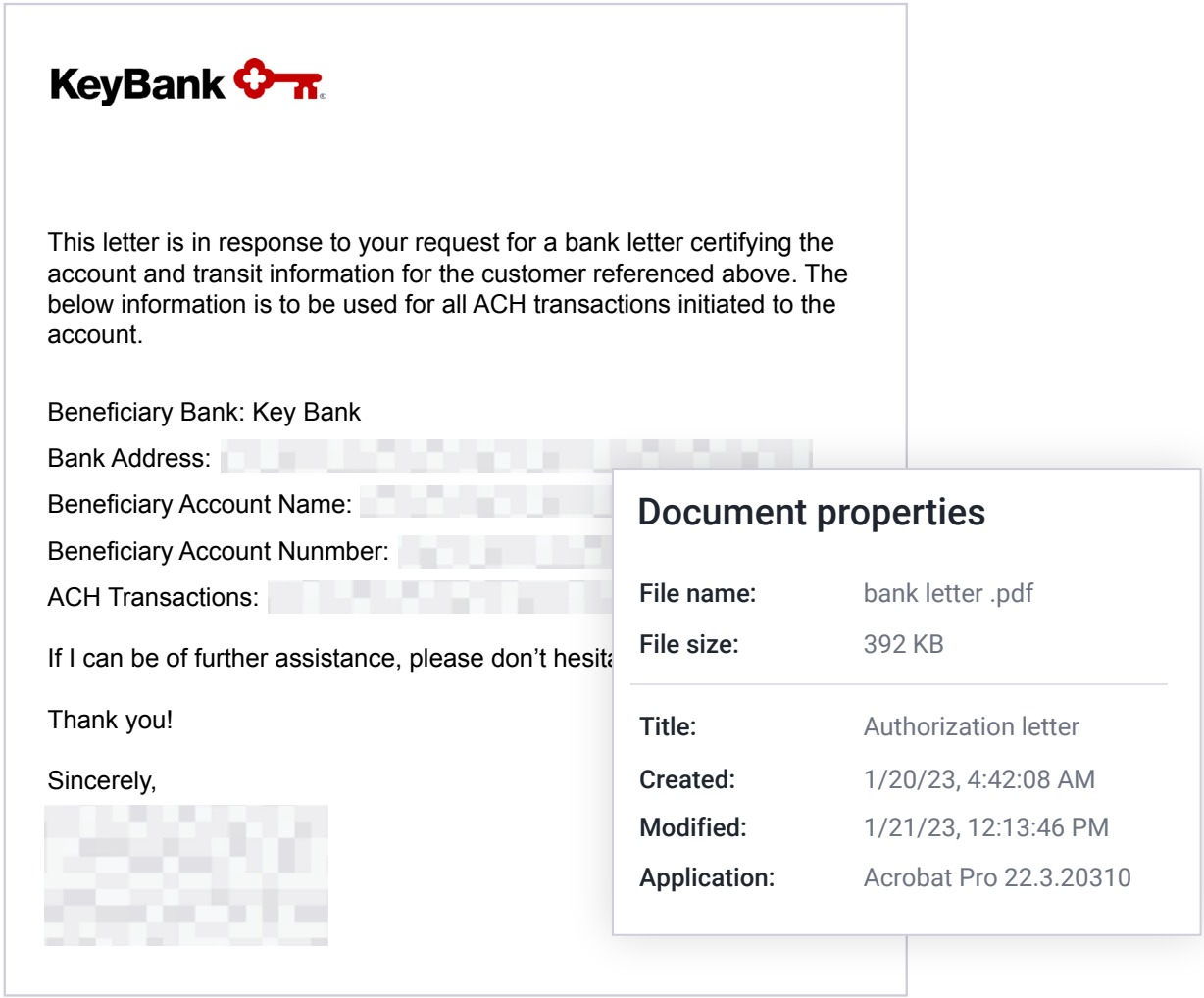
**Attachments:** bank letter .pdf

This email bypasses traditional checks by the SEG because it was sent from a compromised account, so it automatically passes SFP, DKIM, and DMARC authentication. However, analysis of the cc'd look-alike domain shows that it was registered for one year on the same day this message was sent.

| Registrar: | Registered On: | Expires On: | Updated On: |
|---|---|---|---|
| Wild West Domains, LLC | 2023-02-06 | 2024-02-06 | 2023-02-06 |

The attached  is a flat file with no malicious code, making it difficult for secure email gateways to determine its nefarious intent. However, further investigation shows that it is a letter impersonating KeyBank that includes details on the new banking information.

**An Invoice Fraud Attack**

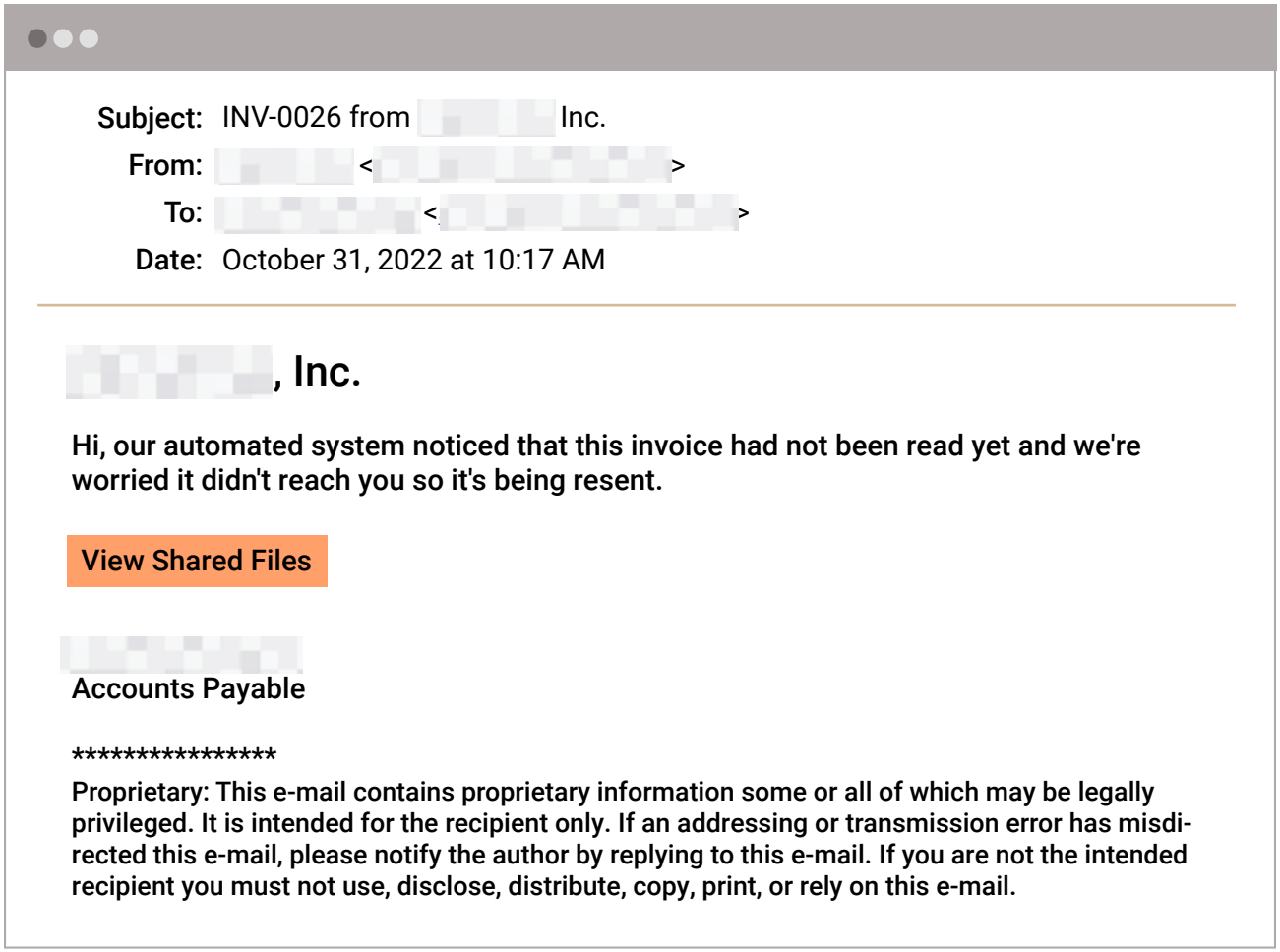


## An OAuth App Phishing Attack that Bypassed the SEG

This next real-world example features an OAuth app phishing attack in which the threat actors first compromise a legitimate email account. They then send emails from it that encourage the target to click on the link, using an unpaid invoice as a pretext and including legal information at the bottom to add to the legitimacy.

If the target were to click the button to view shared files, it would prompt the user to download an application to view. Upon doing so, the victim would install a malicious application that would equip the attackers with API permissions that allow them to carry out additional nefarious activities.

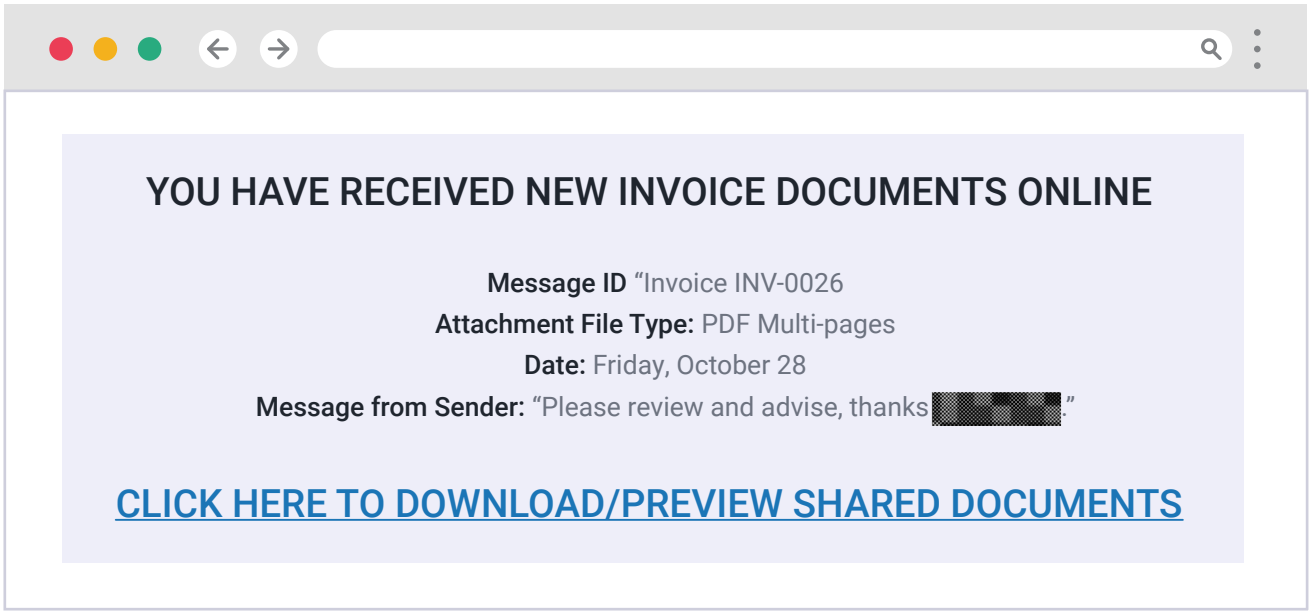
**An OAuth App Phishing Attack**




The email bypasses traditional checks by the SEG because it is sent from Outlook servers and thus passes SPF, DKIM, and DMARC authentication for the sending domain.

When the recipient receives the message from what they presume is a trusted vendor, they click on the "View Shared Files" button to view the invoice, which sends them to a real Canva page. Because a link to Canva—a popular document templating app—is not inherently malicious, neither the SEG nor the employee is likely to catch that it contains a second link. That second link is the malicious one, hiding behind the first (safe) link to avoid SEG detection.

**An OAuth App Phishing Attack**




Clicking the "CLICK HERE TO DOWNLOAD/PREVIEW SHARED DOCUMENTS" button then takes the victim to another URL, which will automatically redirect twice, then ask them to log into their Microsoft account, and allow an OAuth application to install the app. Upon installation, that application would have the ability to read and write email, read and write calendar, edit mailbox settings, access user directories, and more.

# Impact of Today's Macroeconomic Conditions on the Email Security Budget

So while it now may be obvious that the SEG can no longer prevent advanced threats from reaching inboxes, it's not quite so easy to change tools—especially given the current macroeconomic conditions. Budget reductions ranging in severity from technology spending cutbacks to throngs of employee layoffs have sent waves of uncertainty throughout the workforce.

And while cybersecurity spending is often shielded from significant budget cuts as the exposure to risk poses a greater cost than the technology itself, it is not immune to cutbacks. Adding another tool to the list, especially one that is duplicative of a platform that already exists, is often not an option.

So how do you provide your employees with better email security, without increasing your budget? In recent months, security teams have been tasked with assessing the overall value of each tool in their security toolbelt. When doing so, many have realized that there is no longer value in the SEG—especially given recent advancements Microsoft has made in its own native security functionality.

As a result, they're **removing the SEG** and using the money typically spent there for a more effective solution. Implementing new technologies allows organizations to create more efficient processes overall, which could mean more productivity from fewer employees, or reallocating talent from previously manual processes to projects yielding higher ROI. Of course, especially with budget concerns, security platforms should be evaluated with increased scrutiny to ensure that they integrate seamlessly and are both cost and time efficient.

Taking the time and effort to replace the SEG is not a decision that should be taken lightly, but by doing so, organizations can stop more attacks, save time, reduce spend, and increase efficiency for the entire security team.

"We had two SEGs inline and both were still missing stuff that needed additional analysis. They kept missing attacks like those asking for updated W-2 information and ones with lookalike domains asking for payment on fake invoices. After replacing our SEG, **we reduced our email security cost by 40%.** Abnormal really helped my team streamline the investigation process."

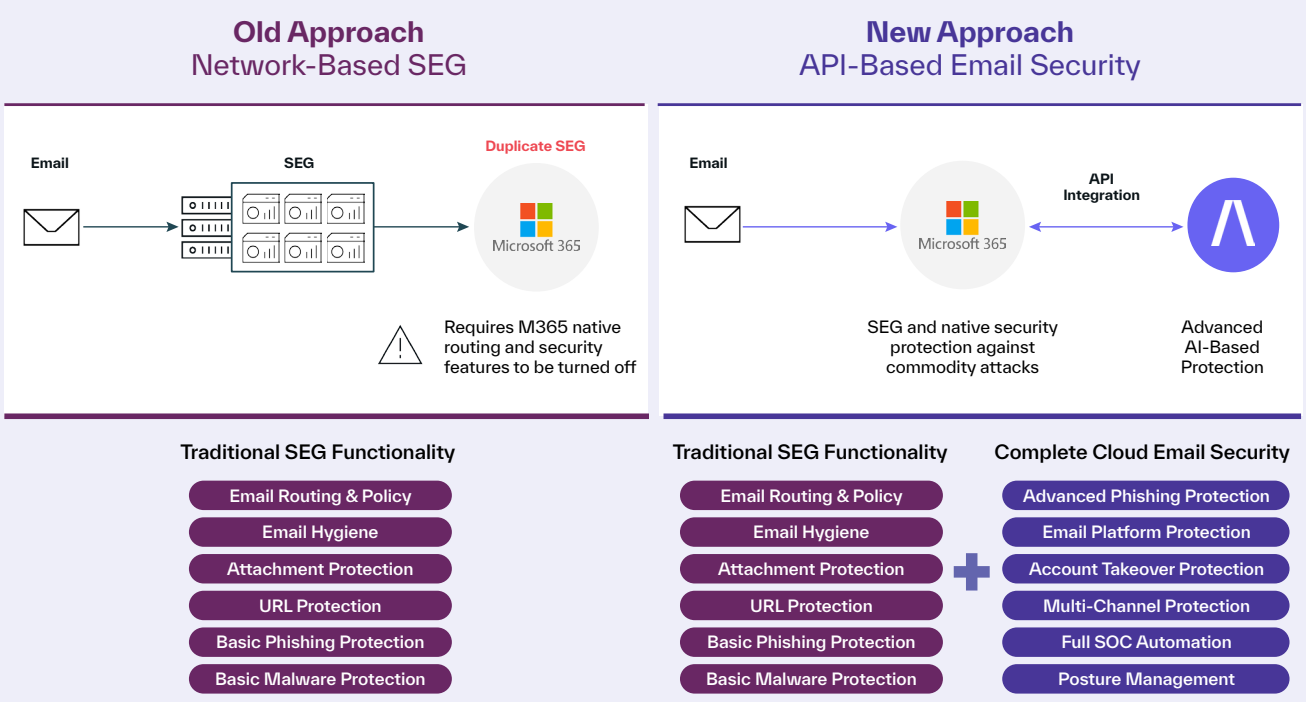
— Ben Fields, CISO, Florida Crystals Corporation

Watch Webinar →

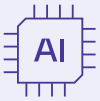
# Replacing Your SEG with a Modern Solution

While the secure email gateway may have been the most efficient solution in the past, it certainly does not stack up against modern threats. To protect the cloud email environment from highly sophisticated email attacks, organizations need the right cloud email security platform alongside the native functionality provided by Microsoft or Google.

**Abnormal and Microsoft Solution and How it Compares to the SEG Approach**



To truly secure cloud email from the full spectrum of threats, the next-generation platform should include the following elements:




## Behavorial AI Approach

The solution should use a fundamentally different approach that leverages behavioral data science and AI to profile and baseline good behavior and detect anomalies. It should use identity modeling, behavioral and relationship graphs, and deep content analysis to identify and stop emails that show anomalous behavior.

## Organizational and Supply Chain Insights

The solution must understand both formal and informal organizational hierarchy and map internal and cross-organizational relationships to identify atypical communication patterns and behavior. It should include a focus on vendor relationships to protect against business email compromise, account takeovers, and other types of fraud throughout the supply chain.

## API Architecture and Integrations

A solution that connects to Microsoft 365 and Google Workspace via an API and in doing so, provides access to the signals and data needed to detect suspicious activity. This includes unusual geolocations, dangerous IP addresses, changes in mail filter rules, unusual device logins, and more. More advanced solutions can also connect to other applications—such as Slack, Okta, Zoom, and CrowdStrike—to understand identity and detect multi-channel attacks.

## Automatic Remediation

The solution should also leverage AI to automate the review and remediation of malicious emails, compromised accounts, and user-reported emails. By removing the manual triage and response process, SOC teams can save time and resources which are better spent on other areas of the business.

With these capabilities, the solution can use thousands of signals to detect anomalous behavior so that the full spectrum of modern attacks will be stopped before they reach the inbox.

# Steps to Replace Your SEG

Replacing the SEG may seem like a daunting task, but it doesn't have to be. In fact, modern solutions make the migration process seamless for your security team, accomplishing the transition in a few easy steps.

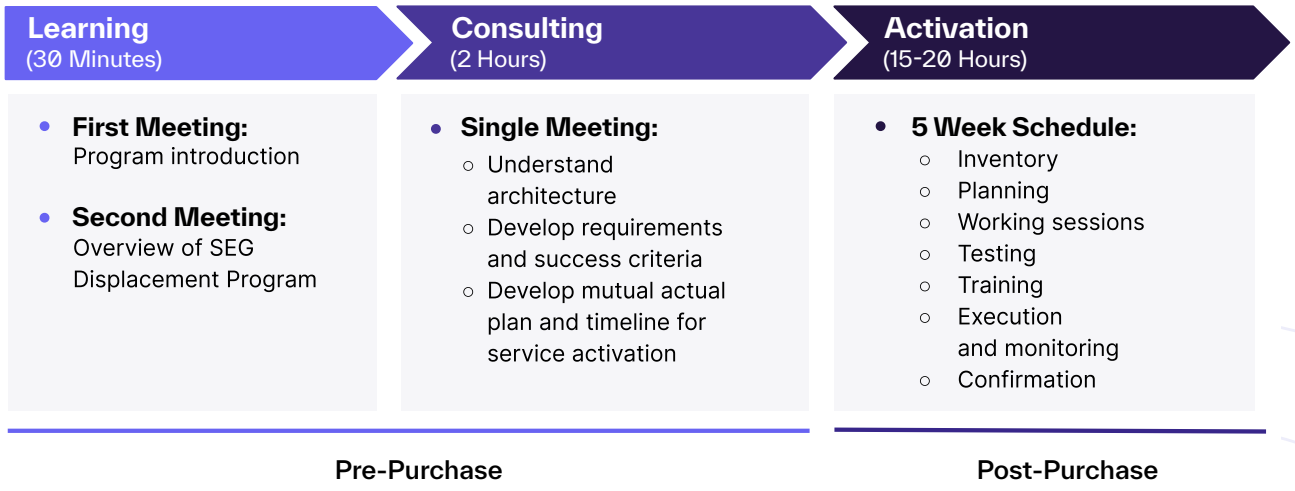
After an initial meeting, a specialist will sit down with you to better understand the architecture of your current security stack and help develop a mutual actual plan and timeline for your activation. In total, it should take about **20 hours across five weeks** to fully replace the secure email gateway.

Replace your secure email gateway in only

**20 hours**

across five weeks.

**Easy Steps to Replace Your SEG**



## Pre-Deployment: Learning and Consultation

During these meetings, your security team will determine the requirements and success criteria and develop a schedule for migration. This should take about 2-3 hours for your team.

## Post-Deployment: Activation and Migration

After purchase of your modern solution, it's time to replace the gateway! Over the course of five weeks, you'll work through the stages of migration from inventory and planning to execution and confirmation with the support of your cloud email security provider. With the right provider, you should receive individualized support throughout the migration process, along with detailed documentation to support the onboarding journey.

## Post-Deployment: Life After the Secure Email Gateway

After migrating to a new solution and removing your secure email gateway, you'll experience a range of benefits.

| Protect More | Spend Less | Secure the Future |
| --- | --- | --- |
| Detect and stop attacks with instantaneous remediation—no tuning required. | Remove your duplicate software and enjoy automated triage across a single dashboard. | Protect your organization against emerging threats with a flexible and adaptable architecture. |

"If you're using a traditional SEG, tweaking dials, checking buckets, and manually remediating things, Abnormal provides modern email security built to work with today's cloud platforms on a budget."

— Peter Mueller, Systems Programmer, Saskatoon Public Schools

Read Case Study →

# Conclusion

There is little denying that secure email gateways were once useful preventative tools to stop attacks targeting organizations. However, while SEGs have proven to be effective in protecting email recipients from known threats, they are not immune to the sophisticated techniques used by present-day threat actors.

Modern threats require a modern security solution that allows organizations to stop advanced email attacks, reduce their spend, consolidate their tools, and prevent emerging threats from reaching their employees. It's only by stopping the most advanced attacks from reaching inboxes that we can truly ensure that organizations will stay protected—now and in the future.

# Abnormal

Abnormal Security provides the leading behavioral AI-based email security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails and messages in milliseconds—all while providing visibility into configuration drifts across your environment.

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, with additional protection available for Slack, Teams, and Zoom.

More information is available at abnormalsecurity.com

## Interested in Seeing How to Replace Your SEG?

Request a Demo →

See Your ROI →