

Abnormal

WHITE PAPER

7 Lessons Learned From Replacing 800+ SEGs



Table of Contents

Evolving Past the
Secure Email Gateway

04

Lessons Learned From
Replacing 800+ SEGs

05

▪ 01

The Great SEG Migration Has Begun

05

▪ 02

SEG Rules Are Ineffective at Combating
Modern Email Threats

06

▪ 03

Account Takeovers Are Increasing

08

▪ 04

Native Cloud Email Security
Has Come a Long Way

09

▪ 05

SEG Replacement Is Quick and Easy

10

▪ 06

Life After the SEG Is Pretty Great

11

▪ 07

You Can Try It With No Risk

12

Conclusion

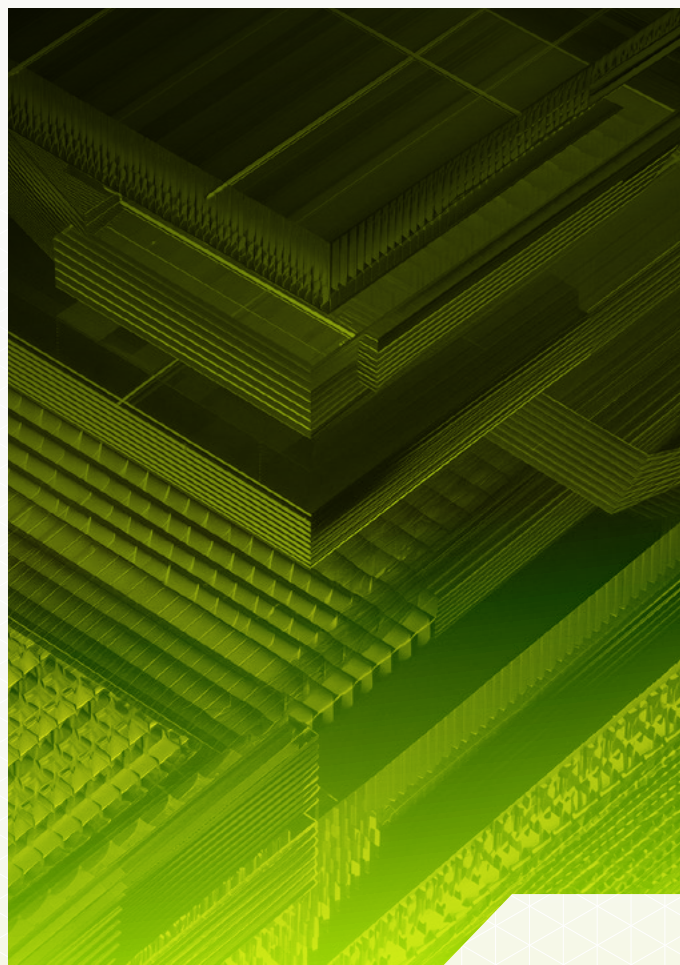
13



Executive Summary

Secure email gateways have long been a cornerstone of email security, providing a vital layer of defense against spam, malware, and other malicious email. But as threats have grown more sophisticated, and organizations have shifted to cloud-based platforms like Microsoft 365 and Google Workspace, SEGs built on static rules and signature-based detection have struggled to keep up.

Abnormal has been on the frontlines of this migration, helping organizations remove their secure email gateway and replace it with a modern, API-native solution, so they get better protection with a lighter lift. To help others make the same move, this paper collects seven of the most impactful lessons learned from replacing more than 800 SEGs with Abnormal's AI-native email security platform: where traditional SEGs fall short, real-world attacks now being caught, what organizations that made the switch have to say, and the results you can expect.



What surprised me was the volume of advanced attacks that the SEG was missing, like compromised internal email conversations between our HR teams and our CFO.”

Jonny Concannon, Group Information Security Manager, Boohoo





Evolving Past the Secure Email Gateway

\$3.05B

In reported BEC losses in 2025, across ~24,800 cases

FBI IC3 2025 Report

>1,200

Attacks per 1,000 mailboxes bypass SEGs each month, on average

Internal Abnormal AI Data, 2026

\$300M+

In attempted theft through vendor email compromise over 12 months

Abnormal AI, 2025

SEGs were designed to serve as the first line of defense against email-based threats, and in their infancy, they proved invaluable at filtering spam, malware, and other common attacks. Their signature-based detection and pattern-matching provided real security in an earlier, simpler threat landscape.

But today's cybercriminals have gotten better at exploiting exactly the gaps that architecture leaves open. Social engineering, polymorphic malware, and zero-day exploits are now standard tools for bypassing traditional SEG detection, and generative AI has made those tactics faster and easier to scale.

As organizations recognize these limitations, many are turning to AI and machine learning-powered solutions that analyze traffic patterns, user behavior, and content in real time, rather than relying on static rules built from yesterday's attacks.



LESSON
01

The Great SEG Migration Has Begun

SEGs were originally built to catch high-volume, low-impact attacks with known indicators of compromise, and they did that well. But that same design leaves organizations exposed to sophisticated attacks that don't carry those indicators at all.

Security teams that stick with a SEG for cost reasons often end up spending more overall: multiple dashboards, complex rules and policies, and manual processes that eat into time the SOC could spend on higher-value work. Many organizations are also paying twice, running a SEG alongside the native security their cloud email provider already includes.

SEGs are also poorly suited to future threats. Their architecture doesn't extend to multi-channel attacks on adjacent surfaces like collaboration apps, so organizations chasing that coverage end up needing new point solutions anyway. The combination of stronger native cloud platform security and an integrated, API-based email security layer is increasingly replacing the SEG outright, and for most organizations, that shift is no longer theoretical.



~75% of Abnormal customers run with no third-party secure email gateway at all."

Internal Abnormal AI Data, 2026



LESSON 02 SEG Rules Are Ineffective at Combating Modern Email Threats

Organizations commonly lean on custom rules and policies within their SEG to prevent attacks, but those measures are often inadequate against sophisticated tactics. SEGs rely on static rule sets and signature-based detection, built from historical attack patterns and known indicators of compromise, which makes them inherently reactive rather than proactive.

Here's a real advanced attack that bypassed the SEG at an Abnormal customer, walked through step by step.

Successful Authentication

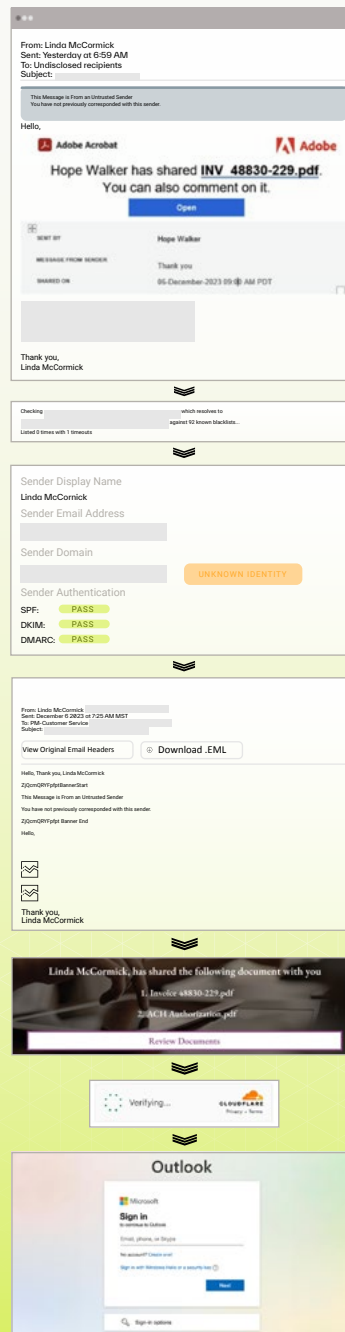
The attacker's initial message appeared to be a link to an invoice PDF shared from an external Adobe Acrobat account. The email passed SPF, DKIM, and DMARC authentication, and because the sender address also carried no negative reputation, it cleared the SEG's checks entirely and reached the inbox.

Images Used as Text

The message body was shared as an image, with the only real text being the greeting and sign-off. The SEG's own caution banner was added to the message, but the email still reached the inbox. Using an image in place of text can reduce the effectiveness of text-based scanning, while still looking entirely legitimate to the recipient.

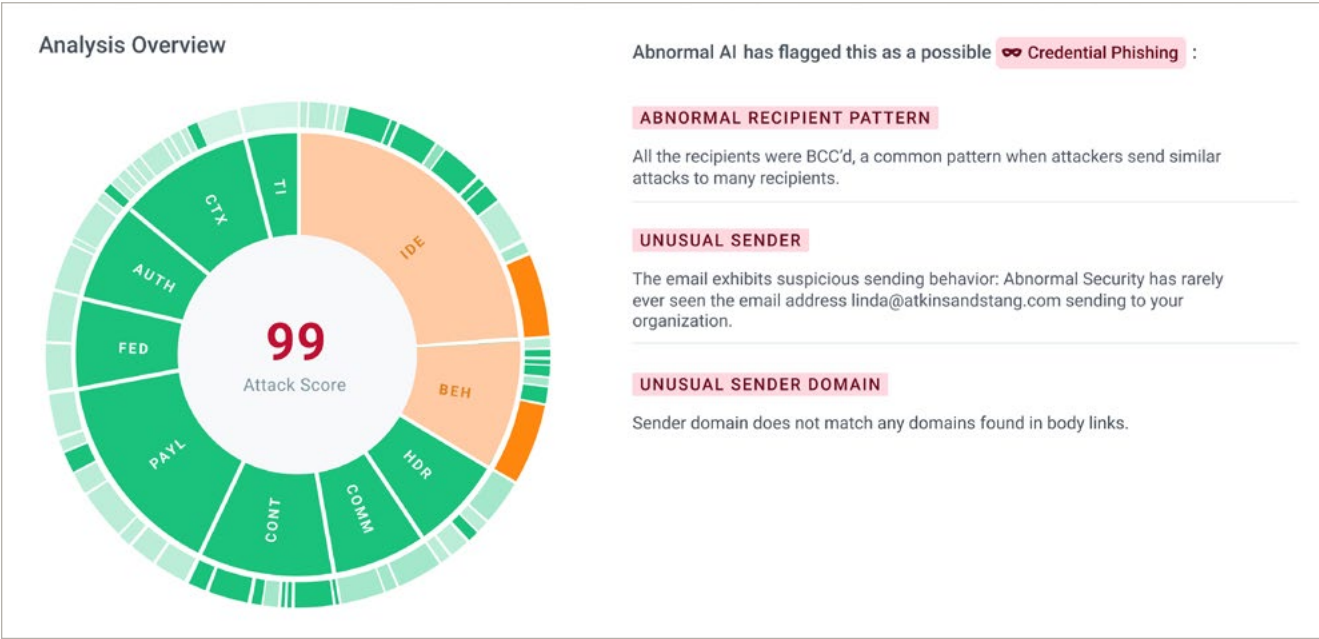
Redirect to Credential Phishing Page

Clicking the image redirected to an abused Google Sites page, which then led through a series of redirects to what appeared to be a Microsoft login page, preceded by a Cloudflare verification step, adding a veneer of legitimacy. In reality, it was a credential phishing page designed to harvest the recipient's Microsoft 365 login.



Using AI to Detect the Attack

Abnormal's AI flagged this as likely credential phishing by combining an abnormal recipient pattern (the message was BCC'd to many recipients, a common mass-attack pattern), an unusual sender the organization had essentially never seen, and a sender domain that didn't match the domains in the message body. Identity, behavior, content, and payload analysis combined to produce a high-confidence malicious verdict before the message ever reached an inbox.



Identity Analysis Rare sender name outgoing email patterns ⓘ Detected Rare sender name incoming email patterns ⓘ Detected Email content domain frequency ⓘ Detected Impersonating strategy ⓘ UNKNOWN SENDER Attacked party ⓘ EMPLOYEE Impersonated party ⓘ UNKNOWN PARTNER INDIVIDUAL	
Behavior Analysis Recipient message-read verification ⓘ Detected Uncommon sender ⓘ Detected Uncommon sender email domain ⓘ Detected WHOIS registered domain age scan ⓘ 8794	
Content Analysis Attachment detected in email ⓘ Detected Email body link count ⓘ 1 Email registered domain count ⓘ 1 Number of attachments in email ⓘ 2 Number of images in content ⓘ {'1': 2.0} Attack goal ⓘ CREDENTIAL THEFT Attack vector ⓘ LINK	
Payload Analysis Suspicious hosting-site domains ⓘ Detected	
Authentic Verification Uncommon authentication FQDN ⓘ Detected	
Business Context Analysis Voicemail language patterns ⓘ Detected Email conversation ⓘ Detected	



LESSON 03 Account Takeovers Are Increasing

When credential phishing bypasses a SEG, it can lead directly to account takeover. A single successful phish can hand an attacker access to an email account, everything inside it, and every connected application. Because email is core to business operations, the fallout from a compromised account ranges from financial loss to reputational damage.

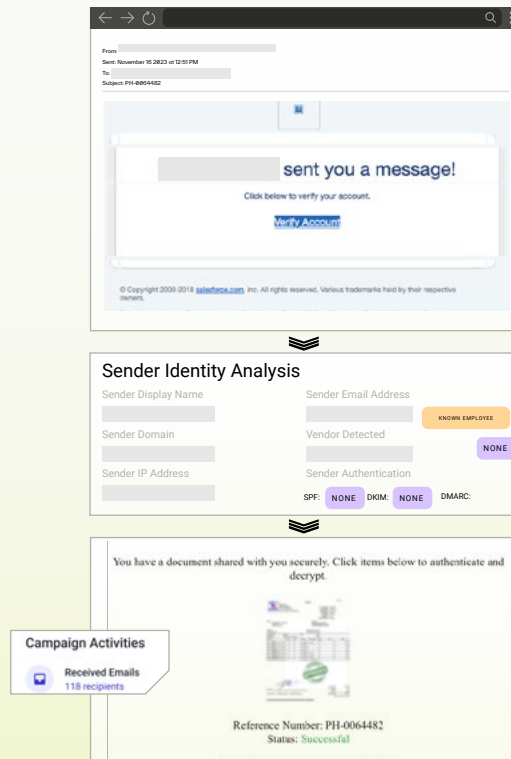
Here's a real account takeover that slipped past a SEG, detected by Abnormal during a read-only proof of value.

A Message From a Compromised Account

The platform detected a message sent from an already-compromised internal account, meaning it was never scanned by the SEG at all and landed directly in the recipient's inbox. The message looked like something a coworker might legitimately send, but its "Verify Account" link led to a legitimate content platform being abused to host a second link, which led to the actual credential phishing site.

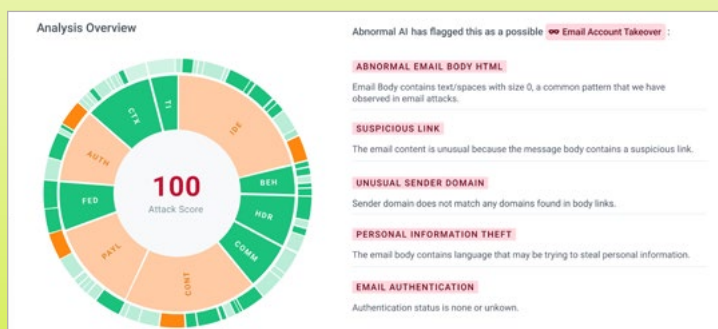
Redirect to a Second Credential Phishing Page

The email went to 118 recipients internally, sharply raising the odds that at least one person would enter their credentials.



Using AI to Detect the Attack

Abnormal flagged this as a likely account takeover after detecting an abnormal email body structure, a suspicious link, and a sender domain that didn't match the links in the message body. Further analysis confirmed the originating account itself was compromised, evidenced by a risky sign-in event and an unusual internal email burst to 118 recipients, a classic lateral phishing pattern. A traditional SEG would not have flagged this message at all, since it never passed through the SEG in the first place. Because attackers can always find a way into an account, whether by purchasing credentials or brute-forcing a password, account takeover can never be prevented with certainty. That's exactly why detecting suspicious behavior and auto-remediating compromised accounts before damage occurs matters as much as blocking the initial phish.



Risky sign-in	Based on historical attack patterns, Abnormal has determined this sign-in to be risky.
Internal Email Burst	An unusually large number of internal emails were sent from this account, which could be a lateral phishing campaign.
Email campaign detected	Email campaign was observed for larry.antonelli@meemic.com



LESSON 04 Native Cloud Email Security Has Come a Long Way

Network-based SEGs scan traffic inline at the network perimeter, an architecture that predates the cloud email platforms most organizations now run, and one that comes with real maintenance overhead and delivery latency.

API-based email security represents a different approach entirely. Instead of intercepting traffic, it integrates directly with the cloud email platform itself (Microsoft 365 or Google Workspace) via API, gaining deeper visibility into both traffic and user behavior. That architecture enables real-time detection, easier scaling, simpler deployment, and the ability to analyze inbound and outbound traffic alike.

The native security built into cloud email platforms has also improved dramatically. As of July 1, 2026, Microsoft 365 E3 and Office 365 E3 include Microsoft Defender for Office 365 Plan 1, adding Safe Links, Safe Attachments, anti-phishing protection, and real-time detections to the capabilities many enterprises already license. This expanded native coverage further reduces the need for a separate SEG to provide foundational email security. With Microsoft handling a wide array of known threats at scale and Abnormal adding behavioral AI for sophisticated attacks like business email compromise, vendor fraud, and account takeover, organizations can replace overlapping gateway controls with complementary layers of protection. The table below shows how capabilities once handled by a SEG are now covered by Microsoft and Abnormal, with one narrow exception: SPF flattening and DMARC enforcement, which most organizations solve with a lightweight specialist tool alongside their email security stack.

SEG Capability	Before	After
Inbound/outbound routing	Handled by the SEG	Completed via Microsoft E3
Edge/reputation checks, file type & AV/malware blocking	Handled by the SEG	Completed via Microsoft E3
Anti-spam and anti-bulk	Handled by the SEG	Microsoft E3 + Abnormal Email Productivity
Custom rules, message annotation	Handled by the SEG	Completed via Microsoft E3
SPF/DKIM/DMARC authentication, DKIM signing	Handled by the SEG	Completed via Microsoft E3
SPF flattening, DMARC enforcement	Handled by the SEG	Completed via a third-party tool (e.g. Valimail)
Post-delivery threat remediation	Based on intel/signature updates	Microsoft E3 + Abnormal Inbound Email Security
Email DLP and encryption	Handled by the SEG	Completed via Microsoft E3



LESSON 05 SEG Replacement Is Quick and Easy

Replacing a SEG can sound daunting, but it doesn't have to be. Abnormal provides a no-cost migration service for organizations moving off platforms like Proofpoint, Mimecast, or Cisco, designed to eliminate redundant license costs and streamline the switch to Microsoft MX records, with hands-on support from Abnormal's SEG Deployment team throughout.

The program itself is designed to minimize customer effort: more than 80% of SEG migrations require just 5 to 10 hours of configuration work, guided by Abnormal's Solutions Architecture and Professional Services teams from kickoff to go-live.

Abnormal's Solutions Architecture and Professional Services teams bring more than 100 years of combined experience to SEG migrations, with more than 800 displacements completed to date.



LESSON 06 Life After the SEG Is Pretty Great

Organizations that move off a legacy SEG typically trade cumbersome maintenance, rigid architecture, and limited visibility for proactive detection, simpler integration, and management tools that don't require a rules engineering background. Here's what that's looked like for two Abnormal customers.

PEGASYSTEMS

Pegasystems' incumbent SEG was missing hundreds of VIP impersonation emails and nearly 250,000 spam and graymail messages a month, and the security team was spending roughly 60 hours a week on manual investigation and remediation. After adding Abnormal alongside its existing Microsoft 365 investment, Pegasystems eliminated 100% of its SEG licensing costs and now saves more than 925 hours a month across email security and graymail management. In head-to-head testing against another API-based vendor, the alternative caught fewer threats and generated 75% more false positives than Abnormal.



Unlike moving from SEG to SEG, trying Abnormal was low-risk, and the functionality was the reward. We already owned the M365 products that Abnormal complements, and it costs much less than our SEG.”

Steve Tieland, Corporate Security Operations Director, Pegasystems

BOOHOO

Even with a traditional SEG in front of Microsoft 365, Boohoo's employees were still receiving credential phishing, invoice fraud, and impersonation attacks. Since replacing its SEG with Abnormal, Boohoo saves its security team roughly 40 hours a month on manual email tasks and has saved 463 employee hours on graymail and spam over 90 days, across more than 7,800 protected mailboxes.



When Abnormal found threats our SEG wasn't detecting, we had to make a change, and Abnormal tying into Microsoft via API was gold for us. Leveraging Microsoft and Abnormal moves us away from the traditional SEG, eliminates that cost, and improves our security.”

Jonny Concannon, Group Information Security Manager, Boohoo



LESSON 07 You Can Try It With No Risk

If the first six lessons weren't proof enough, Abnormal's proof-of-value process makes the gap visible. Across environments protected by a SEG, Abnormal detects more than 1,200 attacks per 1,000 mailboxes each month that bypass upstream gateways. With 99.999% efficacy and a median time to value of just 15 days, organizations can quickly see both what their existing defenses are missing and the impact of adding behavioral AI.

The process itself is built to carry no risk: integration takes about a minute for an IT admin via a read-only API connection, with no changes to MX records and no impact on existing email flow. From there, Abnormal builds a historical analysis of the threats already present and delivers a customized threat report detailing individual, departmental, and organization-wide risk.

99.999%

Efficacy

Internal Abnormal AI Data, 2026

15 days

Median time to value

Internal Abnormal AI Data, 2026



Conclusion



- ▶ SEGs have historically served as vital tools for preventing email attacks, but the threat landscape has increasingly evolved beyond the environment they were built to defend. SEGs still shield recipients from known threats effectively; they fall short against the sophisticated, human-targeted techniques modern attackers now use by default.

Organizations need a security approach that can thwart advanced email attacks, consolidate tooling, and intercept emerging threats before they reach an inbox, without adding cost or complexity. Organizations that have layered Abnormal's behavioral AI into their cloud email environment have done exactly that, benefitting from stronger defenses, lower risk, and fewer moving parts to manage.

A no-risk proof of value is the fastest way to see what's currently getting past your own defenses.

About Abnormal AI

Abnormal AI stops cybercrime with AI, protecting more than 4,500 organizations, including more than 25% of the Fortune 500. The Abnormal Behavioral Security Platform spans email, identity, and insider threat, and is built on proprietary specialized Behavioral AI models designed to detect the attacks that legacy, rules-based tools are not built to detect. Learn more at abnormal.ai.

Interested in Seeing How To Replace Your SEG?

[Request a Demo >](#)[Replace Your SEG >](#)