WHITE PAPER

7 Lessons Learned from Replacing 200+ SEGs

Abnormal

Executive Summary

Secure email gateways, or SEGs, have long been a cornerstone of email security, providing organizations with a vital layer of defense against spam, malware, and other malicious emails. However, as cyber threats have grown more sophisticated, SEGs have faced increasing challenges in effectively detecting and mitigating advanced attacks. The traditional approach of SEGs, relying primarily on signature-based detection and pattern matching, has proven insufficient in identifying the rapidly evolving tactics employed by modern threat actors.

Thanks to new technology like generative AI, the sophistication and volume of email threats have escalated in recent years—placing a significant burden on security teams tasked with managing SEGs. Additionally, the sheer number of emails processed by SEGs can overwhelm traditional systems, leading to performance issues and delays in detecting and responding to threats. These challenges, combined with the transition to cloud-based email platforms like Microsoft 365 and Google Workspace, have prompted organizations to re-evaluate their email security strategies.

Abnormal has been on the frontlines of this migration, helping organizations worldwide to remove their secure email gateways and replace it with a modern solution. In doing so, they can get better protection with a lighter lift—helping protect against more attacks while saving time on their email security initiatives.

To help others make this transition, we've put together seven of the most impactful lessons we've learned since replacing more than 200 SEGs with Abnormal's AI-native email security solution. These lessons explore the limitations of traditional SEGs in addressing modern email threats, highlight real-world attacks that are now being caught, provide insights from organizations that have made the migration, and showcase the results you can see with a similar approach.

Let's get started!

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.

Jonathan Concannon
Director of Cybersecurity Operations, BooHoo

Table of Contents

Evolving Past the Secure Email Gateway

54%

increase in BEC attacks between 2023 and 2024.

Abnormal Security H1 2025 Threat Report

$2.8B

in exposed losses due to BEC in 2024 alone.

FBI Internet Crime Complaint Center (IC3)

$4.88M

average cost of a data breach in the United States.

IBM Cost of a Data Breach Report

Introduced as a pivotal component of organizational cybersecurity infrastructure, SEGs were designed to serve as the first line of defense against a myriad of email-based threats. In their infancy, SEGs proved invaluable in filtering out spam, malware, and other common threats, effectively safeguarding users' inboxes and corporate networks. Their signature-based detection mechanisms and pattern-matching algorithms provided a semblance of security in an increasingly digital world.

However, as the cyber threat landscape evolved, so too did the tactics employed by malicious actors. Today's cybercriminals have become adept at exploiting vulnerabilities in SEG defenses, leveraging sophisticated techniques to evade detection and infiltrate email systems. Social engineering, polymorphic malware, and zero-day exploits are just a few examples of the advanced tactics utilized by threat actors to bypass SEGs undetected.

In 2024, the FBI Internet Crime Complaint Center (IC3) reported exposed losses of $2.8 billion due to business email compromise (BEC), which uses social engineering tactics to target human behavior. And this staggering sum does not account for the advanced credential phishing, malware, and lateral spear phishing attacks that have also evolved in sophistication.

In response to these evolving threats, organizations are increasingly recognizing the limitations of traditional SEGs and seeking alternative solutions to bolster their email security posture. By embracing advanced email security solutions powered by artificial intelligence (AI) and machine learning (ML), security leaders can enhance their ability to detect and mitigate sophisticated email-based threats in real-time. AI-powered solutions offer a proactive approach to threat detection, analyzing email traffic patterns, user behavior, and content to identify anomalies and potential security risks.

Lessons Learned From Replacing 200+ SEGs

The transition away from the secure email gateway underscores the growing recognition among organizations of the limitations inherent in traditional SEGs and the need for more advanced and adaptive email security solutions.

By migrating away from legacy SEGs, organizations can streamline operations, reduce complexity, and achieve greater visibility and control over their email security posture. Throughout this transformative journey, several key lessons have emerged.

LESSONS LEARNED FROM REPLACING 200+ SEGS \\ 01

The Great SEG Migration Has Begun

As previously noted, SEGs were originally designed to detect traditional high-volume, low-impact attacks with known indicators of compromise. And while they did this well, this approach leaves organizations vulnerable to increasingly sophisticated attacks that lack these indicators.

Security teams that have yet to migrate away from the SEG due to cost are actually finding themselves spending more overall. By relying solely on the SEG, they are forced to navigate through multiple dashboards and maintain complex rules and policies, leading to cumbersome and time-consuming processes. This manual approach also consumes valuable resources in the security operations center (SOC) that could be otherwise allocated to more crucial security tasks. Additionally, there is often redundancy in the email security stack, with both the SEG and the native security provided by the cloud email security provider, resulting in unnecessary costs.

> Increasingly, the combination of the cloud email providers' native capabilities and an integrated cloud email security solution is replacing the traditional SEG.
>
> *The Gartner Market Guide for Email Security, 2023*

70%

of Abnormal customers do not use an SEG.

Moreover, SEGs are not adaptable enough to effectively mitigate future threats. Their architecture limits their ability to detect and prevent emerging multi-channel attacks, including those carried out on adjacent channels like collaboration applications. For organizations seeking these capabilities, they will need to explore new point solutions that can address these evolving threats.

To address these challenges, more organizations are now investing in AI-powered security technology that is designed to support cloud-based email platforms and provides comprehensive protection from a wide range of threats. The great SEG migration is no longer an idea—it has already begun.

LESSONS LEARNED FROM REPLACING 200+ SEGS \\ 02

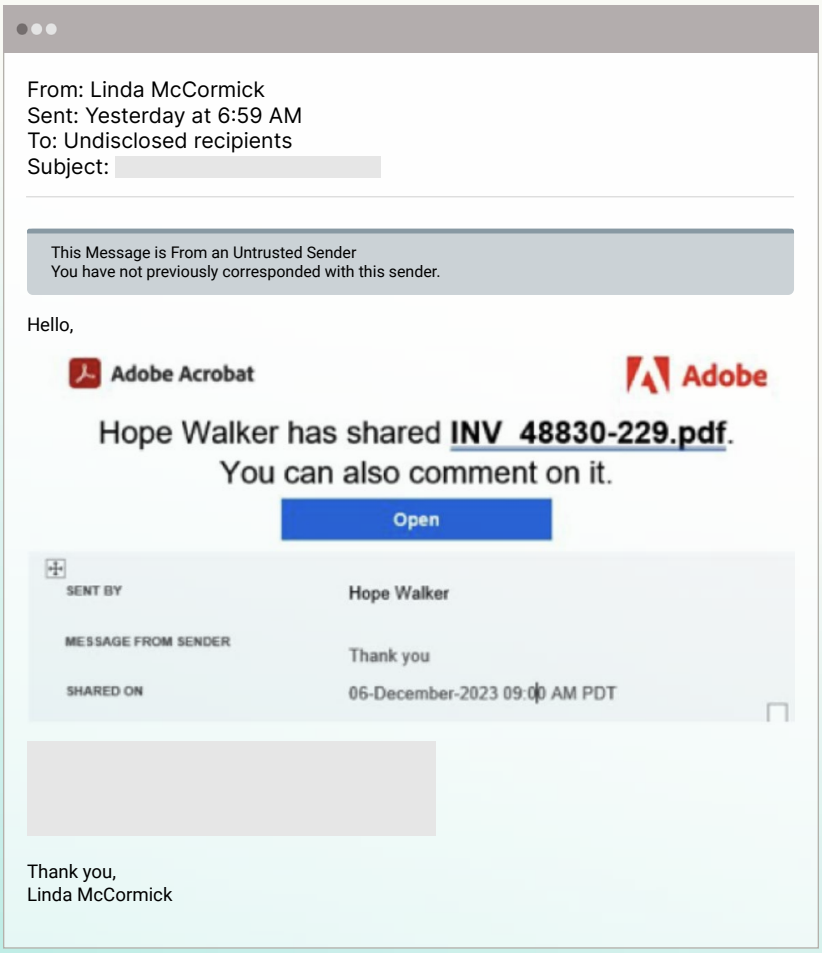
SEG Rules Are Ineffective at Combating Modern Email Threats

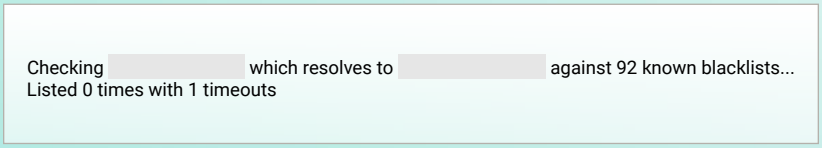
Organizations commonly rely on custom rules and policies within their SEGs to prevent attacks, but the reality is that these measures often prove inadequate in addressing the sophisticated tactics. The inherent limitations of SEGs stem from their reliance on static rule sets and signature-based detection mechanisms, which struggle to keep pace with the dynamic nature of cyber threats.

Many custom rules within SEGs are crafted based on historical attack patterns or known indicators of compromise, making them inherently reactive rather than proactive in nature. To illustrate this, let's take a look at an advanced attacks that bypassed the SEG employed by this Abnormal customer.

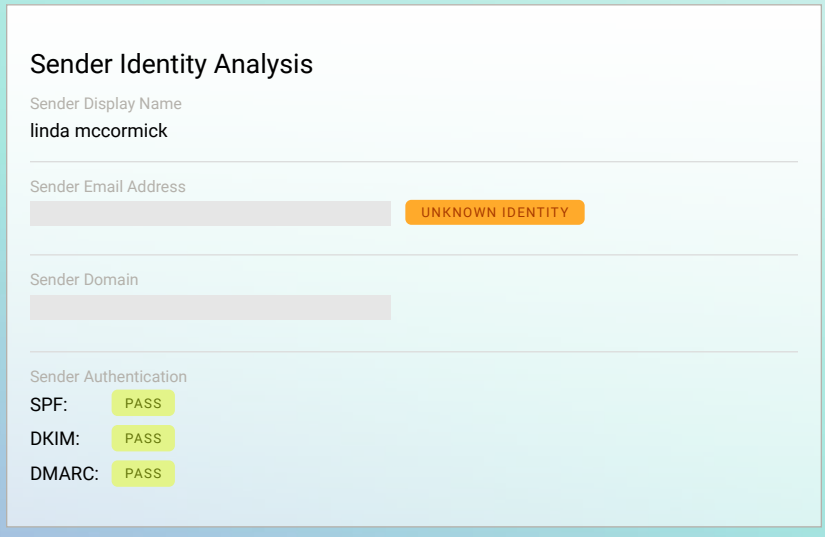
Successful Authentication

The attacker's initial message appears to be a link to an invoice PDF shared from an external Adobe Acrobat account.





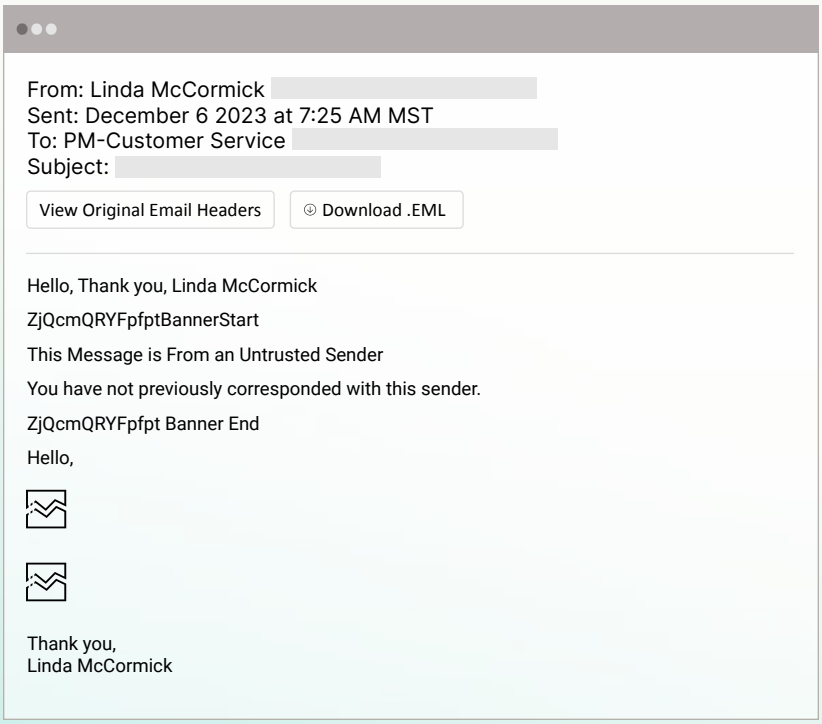
Since the sender email address does not have a poor reputation, the email bypasses initial defenses and is successfully authenticated across SPF, DKIM, and DMARC.



Images Used as Text

Additionally, the message body is shared as an image and the only actual text in the email is the greeting and sign-off, as shown here. The caution message was added in by the SEG, but as you can tell, it was not prevented from reaching the inbox.

This method of using images that include text removes the opportunity for a legacy SEG to detect the content but appears entirely legitimate to the end user.

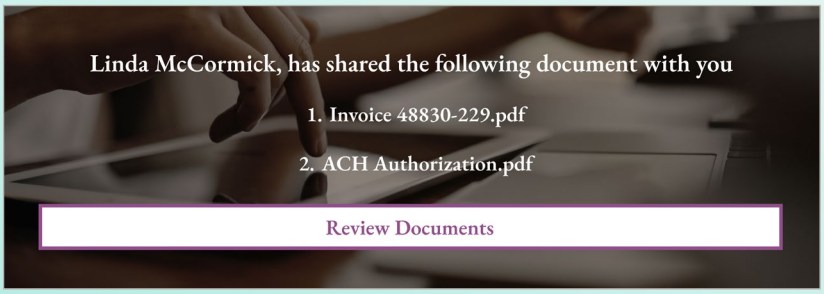


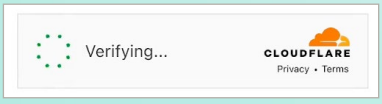
Redirect to Credential Phishing Page

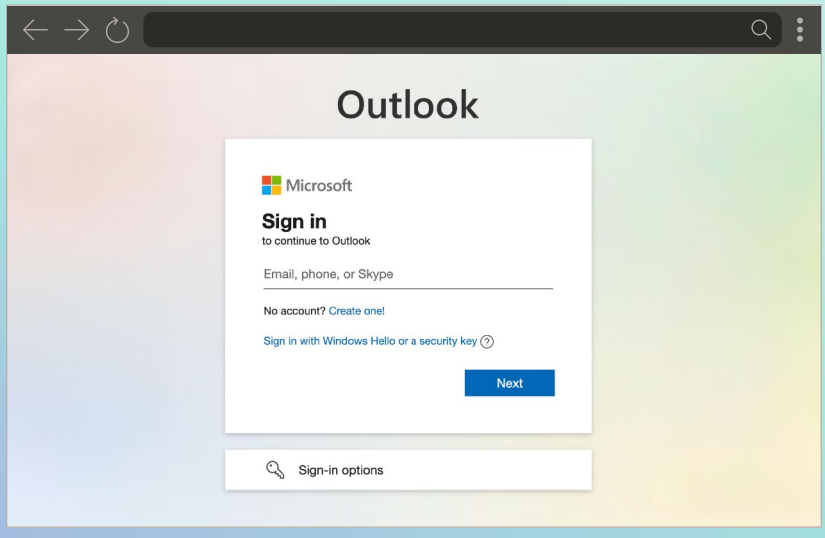
If the recipient of the email were to click on the image in the message body, they would be redirected to an abused Google Websites location.

Upon clicking the 'Review Documents' link on this secondary page, the recipient will be taken through a series of redirects to what appears to be Microsoft login page verified by Cloudflare.

From here, it appears to the target that they need to sign in to the Microsoft 365 account in order to gain access to the PDF invoice. In actuality, it's a credential phishing page which will compromise sensitive login information.

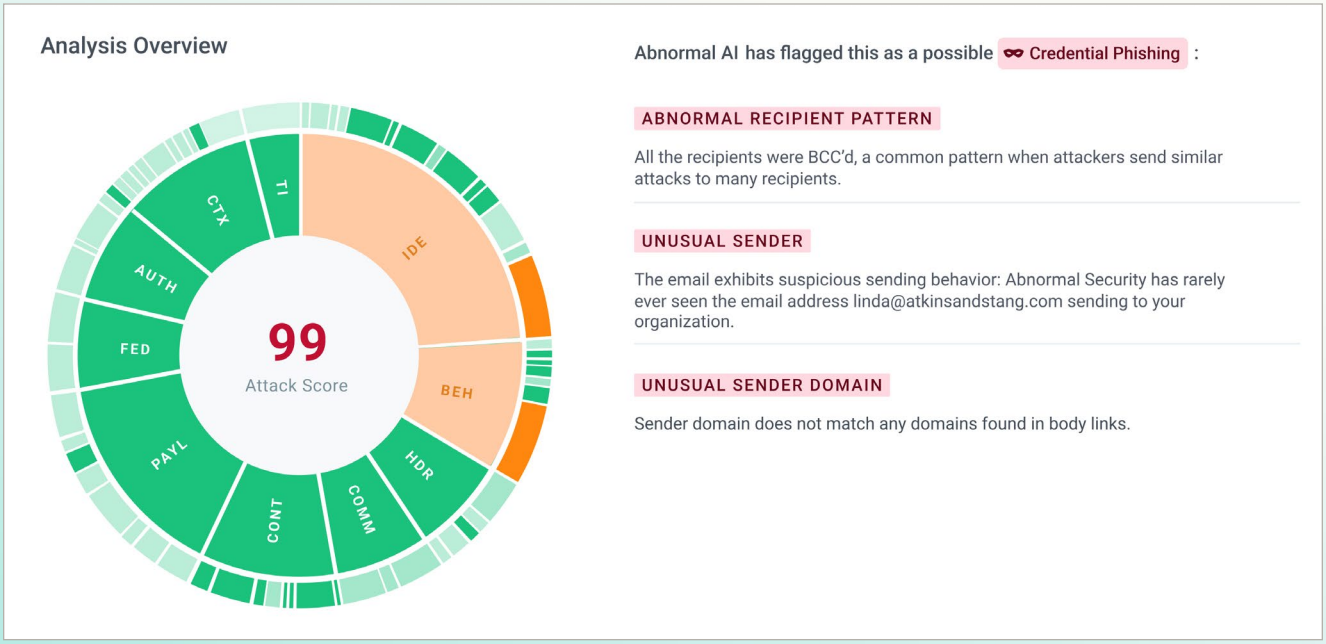






Using AI to Detect the Attack

While this attack would easily bypass the legacy SEG, Abnormal's AI-powered solution quickly flagged it as a possible credential phishing attack. Abnormal detected the malicious activity by analyzing various factors, including an abnormal recipient pattern an unusual sender and an unusual sender domain.



Additional identity, behavior, content, and payload analysis enables Abnormal to detect enough suspicious signals to classify this message as malicious and prevent it from reaching user inboxes.

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

Payload Analysis

Suspicious hosting-site domains	Detected

Authentic Verification

Uncommon authentication FQDN	Detected

Business Context Analysis

Voicemail language patterns	Detected
Email conversation	Detected

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

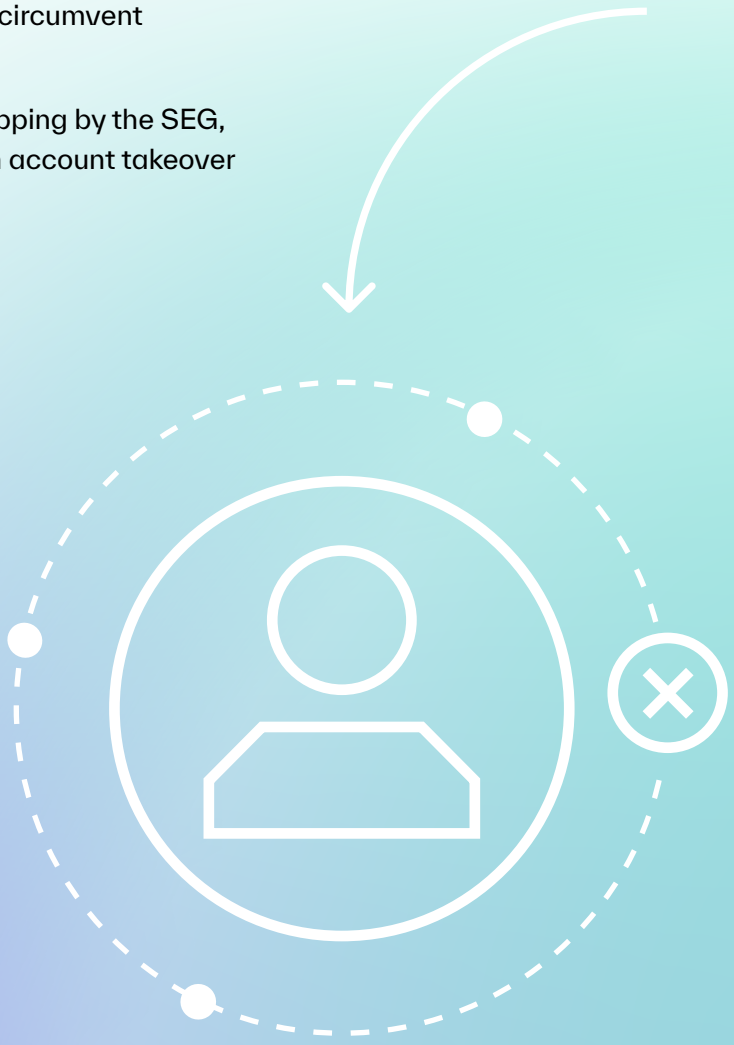
LESSONS LEARNED FROM REPLACING 200+ SEGS \\ 03

Account Takeovers Are Increasing

Because secure email gateways allow credential phishing attacks into inboxes, account takeovers are becoming more frequent. With a single successful credential phishing attack, threat actors can quickly gain access to an email account, all of the information inside it, and every connected application. Because email accounts are the core of business operations, the consequences of a successful compromised account can be severe, ranging from financial losses and identity theft to reputational damage for businesses.

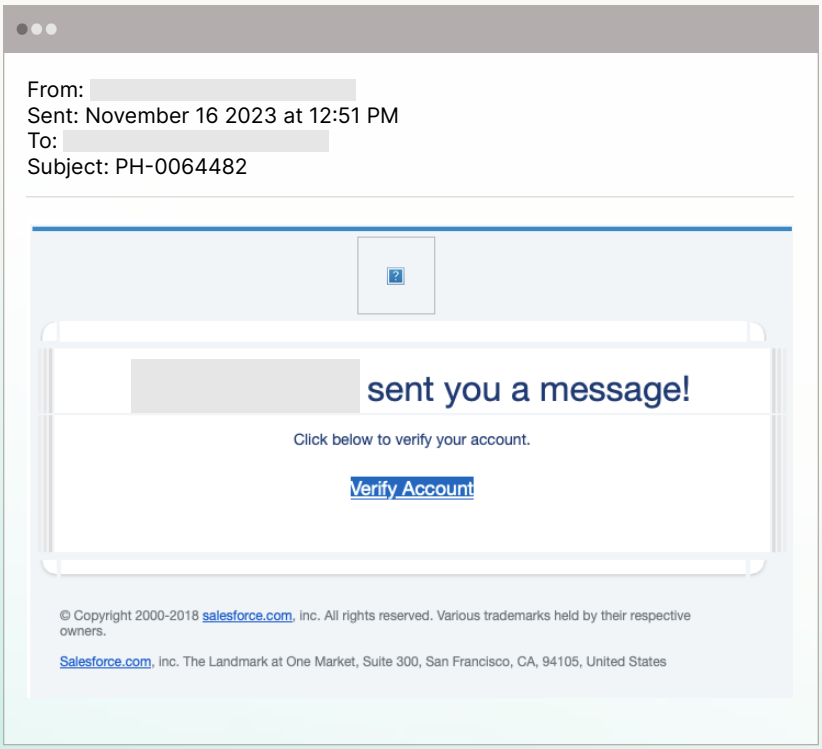
Legacy SEG solutions are ill-equipped to combat these increasingly sophisticated threats, as modern cybercriminals continually devise new methods to create inbound attacks that circumvent traditional defenses.

To illustrate exactly how these attacks are slipping by the SEG, let's take a look at a real-world example of an account takeover attack detected by Abnormal.



In this real-world example, Abnormal was implemented in read-only mode as part of a proof of value for a potential customer. While in read-only mode, the platform detected a message sent from an internal user, meaning it was never analyzed by the SEG and entered the recipient's inbox unimpeded.

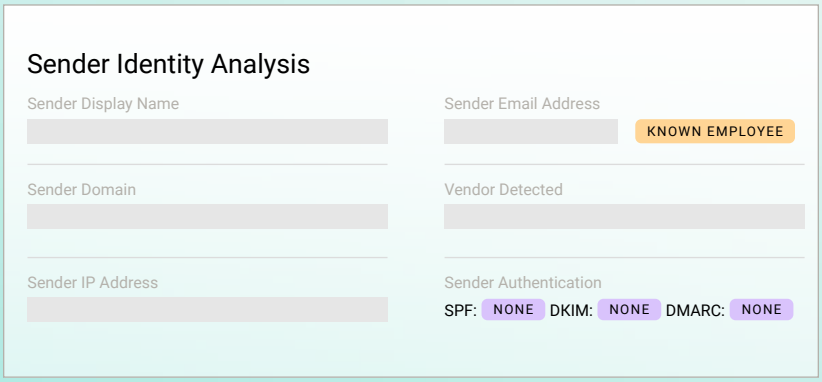
The message was sent from a compromised internal account to another user and looks like something the recipient may expect to receive from a coworker.

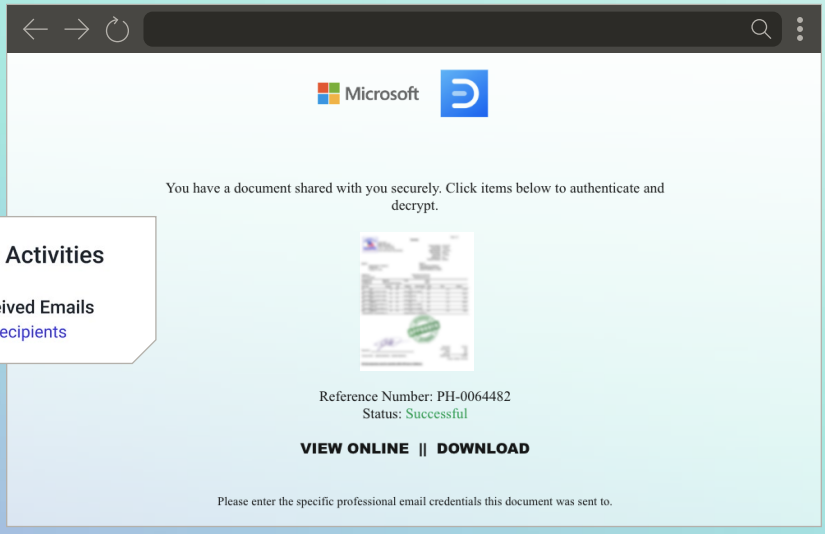


However, the 'Verify Account' link in the body of the message takes the recipient to a legitimate content platform that is being abused to host a second link.

That 'View Online' link will then lead to the actual credential phishing site, where the recipient is prompted to enter their login information, and their account will eventually be compromised by a bad actor.

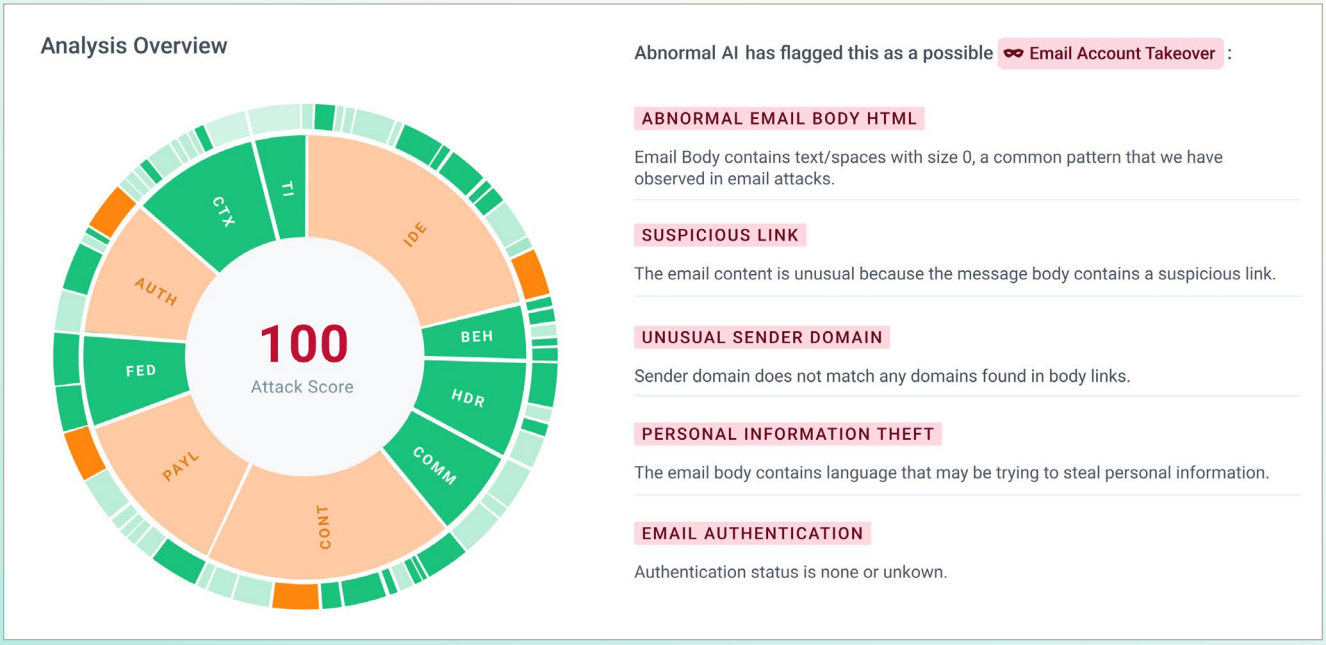
Unfortunately, this email was sent to 118 recipients within the organization—drastically increasing the likelihood that at least one person would enter their information.



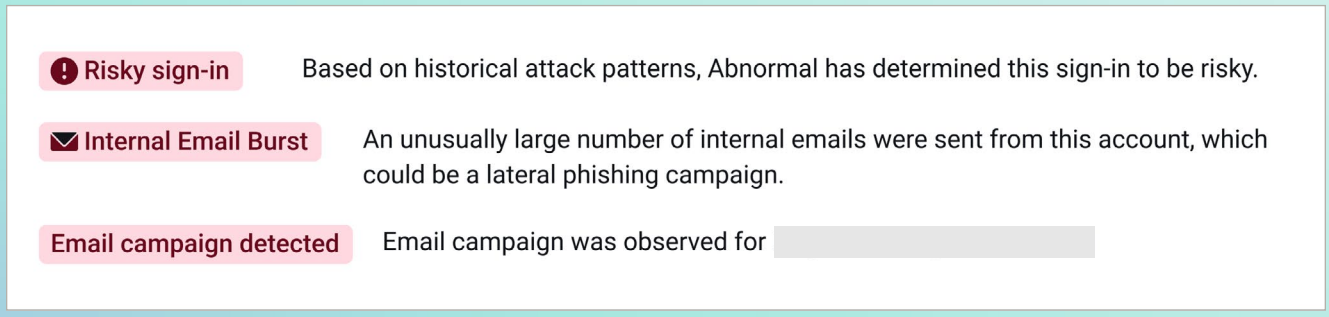


Using AI to Detect the Attack

Abnormal flagged the attack as a possible Email Account Takeover attack after detecting a number of suspicious factors, including an abnormal email body HTML, a suspicious link in the email body, and the fact that the sender domain does not match the links in the body of the email.



Further analysis shows that the originating account was compromised—as indicated by the risk sign-in and the internal email burst to the 118 recipients.



While Abnormal could quickly auto-remediate this attack, a traditional SEG would not have flagged the email as suspicious and would have allowed it to enter the user's inbox.

To stay ahead of these threats, businesses must invest in modern solutions with comprehensive protection and account takeover remediation capabilities. Because threat actors can always find ways into email accounts, like purchasing credentials or through brute force attacks, account takeovers can never be prevented entirely. This is why it's important to have a solution that can immediately detect suspicious behavior and auto-remediate accounts before damage can be done.

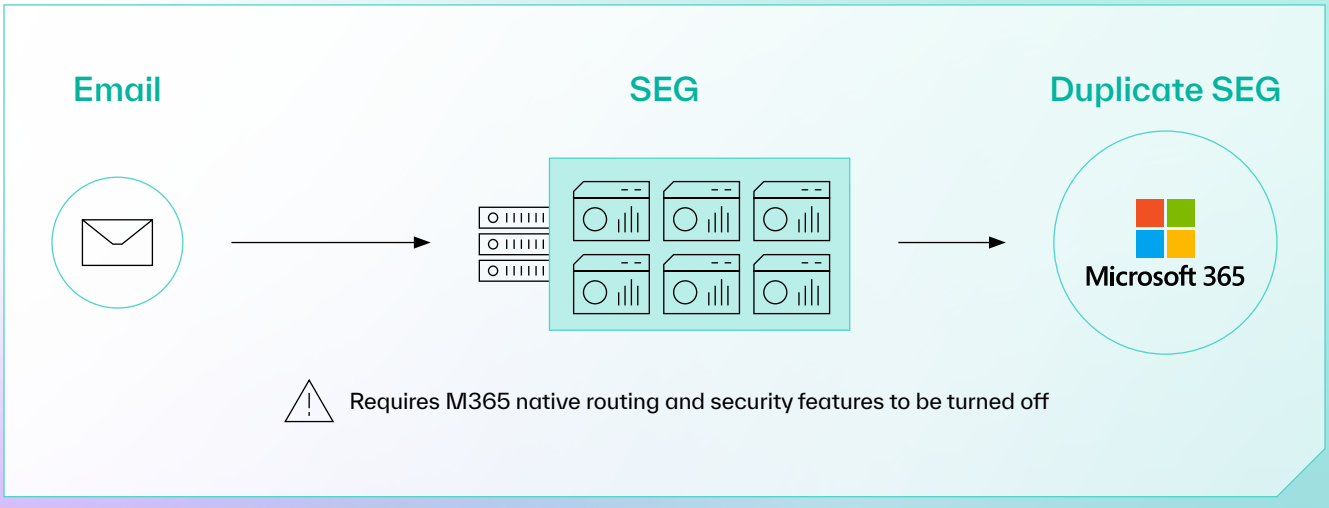
LESSONS LEARNED FROM REPLACING 200+ SEGS \\ 04

Native Cloud Email Security Has Come a Long Way

When SEGs were first developed, their architecture represented the sole approach for combating email threats. However, as businesses transitioned to cloud-based email solutions, alternative architectures emerged to offering deeper visibility and the ability to maximize investments in the cloud email platform. To better understand the evolution of email security, let's delve deeper into these advancements.

Old Approach: Network-Based SEG

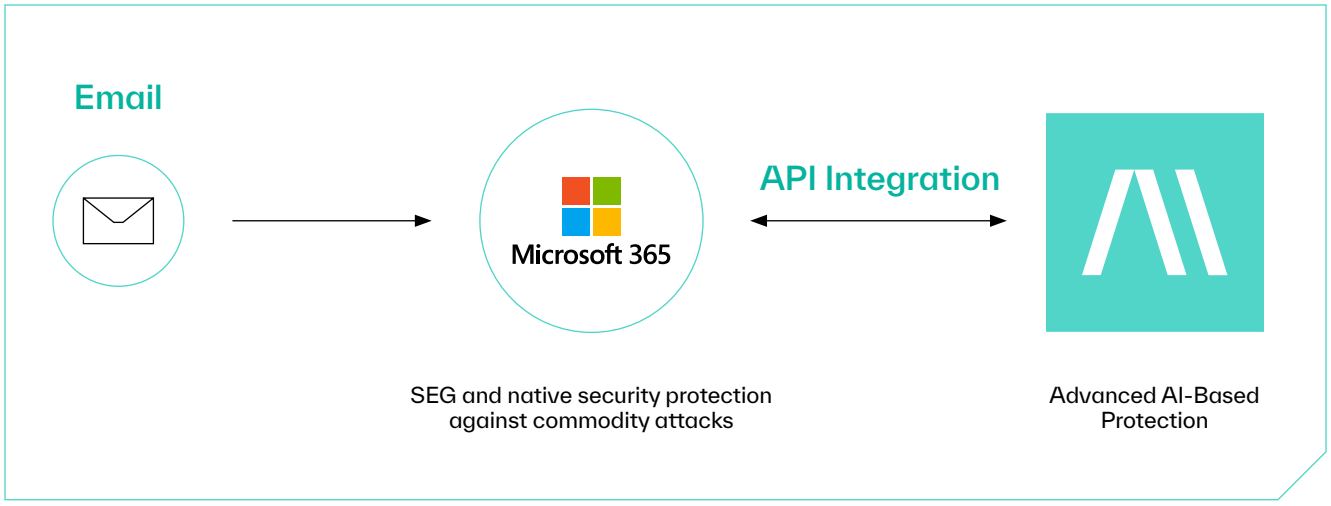
The old approach of network-based SEGs relied on intercepting and scanning email traffic as it passed through the network perimeter. These operated inline, meaning they were positioned between the email server and the external network, scrutinizing each email for signs of malicious content or suspicious activity.



While effective to a certain extent, this approach had limitations, particularly in terms of scalability and adaptability. Maintenance was often cumbersome, requiring constant updates and configuration adjustments to keep pace with evolving threats. Additionally, network-based SEGs could introduce latency into email delivery processes—impacting user experience.

New Approach: API-Based Email Security

In contrast, the new approach of API-based email security represents a paradigm shift in email threat detection and prevention. Instead of relying on network interception, API-based solutions integrate directly with cloud-based email platforms, such as Microsoft 365 or Google Workspace, via their API.



By tapping into the email platform's native capabilities, API-based security solutions gain deeper visibility into email traffic and user behaviors. This approach offers several advantages, including real-time threat detection, enhanced scalability, and reduced complexity in deployment and management. Moreover, API-based solutions can analyze both inbound and outbound email traffic, providing comprehensive protection.

Providing Defense-in-Depth With Native Solutions

The functionality available today in cloud email platforms has increased dramatically. We are no longer in a situation where the native platforms are unable to stop even basic attacks; they're actually pretty good at stopping the vast majority of attacks. For example, the following chart shows which functionalities of the traditional SEG can now be replaced (almost entirely) by Microsoft E3 comprehensive protection.

SEG Category		Before (SEG Core Capability)	After (SEG Replacement Program Completed)
Routing (MTA/Sendmail)	1. Inbound/Outbound Routing	Email routing and conditional routing	Completed via MSFT E3
	2. Address Rewriting	Email address rewriting	Completed via MSFT E3
Inbound Protection (Dynamic Reputation, TAP, PPS, POD)	3. Edge/Reputation Checks	Email address, domain, IP, URL, attachment	Completed via MSFT E3
	4. File Type Blocking	Any file type extension	Completed via MSFT E3
	5. Anti-Virus/Anti-Malware Checks	Multiple antivirus engines	Completed via MSFT E3
	6. Anti-Spam and Anti-Bulk	Spam and bulk mail protection	Completed via MSFT E3 + Abnormal EPR
Inbound Policy (Email Firewall)	8. Custom Rule Creation	Any policy type	Completed via MSFT E3
	9. Message Annotation	Email disclaimers and subject line tags	Completed via MSFT E3
Sender Authentication (Email Fraud Defense)	10. Email Authentication	SPF, DKIM, DMARC assessment for inbound messages	Completed via MSFT E3
	11. DKIM Signing	DKIM for outbound messages	Completed via MSFT E3
	12. Additional Authentication	SPF flattening/compression (>10 mailers), DMARC enforcement	Completed via Third Party (Valimail)
Remediation (TRAP)	13. Post-Delivery Threat Remediation	Based on intel/signature updates	Completed via MSFT E3 + Abnormal IES
Outbound Compliance (DLP)	14. Email DLP and Encryption	Complete policy-based encryption (HIPAA, PCI, PII, etc.)	Completed via MSFT E3

Abnormal then provides the necessary protection for the advanced threats discussed above. By leveraging Abnormal alongside Microsoft 365 licenses, businesses can now fortify their defenses against a wide array of email-based attacks. This approach ensures comprehensive protection against evolving email threats while optimizing the utility of existing technology investments.

Curious if you can replace your SEG?

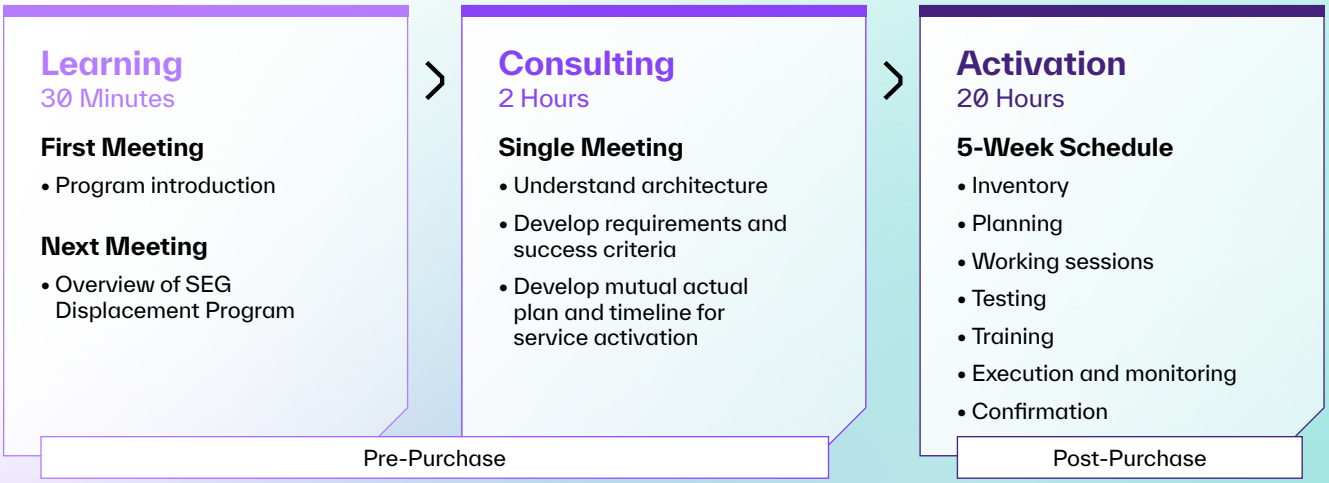
Try our interactive quiz and find out by answering a few quick questions.

SEG Replacement Is Quick and Easy

So now you've realized that it's likely time to replace your SEG. This 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.

For example, Abnormal provides a comprehensive, no-cost migration service tailored to assist customers in transitioning away from their existing SEG solutions. This initiative is particularly beneficial for those migrating from platforms such as Proofpoint, Mimecast, or Cisco. The primary objective of this program is to streamline operations and help customers eliminate redundant software license costs.

The migration process is designed to be end-to-end, culminating in the seamless switchover to Microsoft MX records. Throughout the entire migration journey, customers benefit from hands-on support delivered by the experienced Abnormal SEG Deployment team. Let's delve into the details of this program journey.



The program starts with an introductory phase, where customers familiarize themselves with the program's offerings and understand its potential benefits. Following this initial stage, the Abnormal team collaborates closely with the customer to gain insights into the existing email architecture. Through in-depth consultations, both parties develop a clear understanding of the environment's unique requirements and establish criteria for a successful migration. This phase culminates in the creation of a mutually agreed-upon action plan, laying the groundwork for the subsequent steps.

During the activation stage, migration begins, and the designated five-week schedule is set into motion. As part of this process, the Abnormal team conducts a thorough inventory analysis of the existing email infrastructure, identifying key components and potential areas for optimization. This ensures a seamless transition to the new Abnormal email security solution. Throughout this phase, continuous communication and progress updates are provided to the customer, maintaining transparency and alignment with predefined milestones.

This entire process has been completed more than 200 times. Abnormal takes the legwork out of it, so you can enjoy the benefits—without the pain.

Life After the SEG Is Pretty Great

By transitioning away from legacy SEGs, organizations experience a notable transformation in their security posture. Gone are the days of grappling with cumbersome maintenance, rigid architectures, and limited visibility into email threats. Instead, they experience proactive threat detection, seamless integration, and intuitive management tools that redefine the landscape of email security.

But you don't have to take our word for it. Here are just a few Abnormal customers who have seen the transformative impact of migrating off their SEG.

PEGASYSTEMS

Our systems operations and IT teams were blown away by how easy it was to connect Abnormal via API to try it out. In our head-to-head test with another solution, Abnormal detected twice the malicious emails and generated 75% fewer false positives than the other vendor.

Steve Tieland, Director, Corporate Security Operations, Pegasystems

Pegasystems, an American software company, recently displaced its SEG with Abnormal. Their incumbent SEG was missing hundreds of VIP impersonation emails and nearly 250,000 spam and graymail messages each month. Overall, they were spending too much time on reporting, investigating, remediating, and managing promotional emails.

The company decided to move away from their SEG and add Abnormal to their security stack, while leveraging their existing investment in Microsoft. The outcome has been remarkable. Overall, Pegasystems has eliminated $100K in license spend and saved more than 220+ security team hours every month. They have also saved 624 employee and 67 VIP hours with Abnormal's graymail filtering in only one month.

BOOHOO

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

Online fashion retailer Boohoo also migrated off of its legacy SEG with Abnormal. Since implementing a new AI-powered security solution, Boohoo has experienced zero missed attacks or false positives. Dozens of compromised vendor accounts have been identified, with real-time detection of hijacked email conversations before financial losses could occur. Additionally, the organization has reclaimed hundreds of hours per quarter, allowing the security team, employees, and executives to focus on their core business.

LESSONS LEARNED FROM REPLACING 200+ SEGS \\ 07

You Can Try It With No Risk

If the first six lessons weren't proof enough, the Abnormal POV process shows just how many attacks are currently bypassing your SEG. In fact, upon deployment in Fortune 1000 companies, we see an average of 36 BEC emails still sitting in inboxes, and that nearly 80% of organizations have at least one compromised account in their environment.

Here's how the process works:

Quick, three-click integration with no configuration needed.

Fast integration via API takes one minute for an IT admin. Works directly out of the box on day one.

Zero risk with no impact to your existing email infrastructure.

Read-only API integration performs analysis passively. No action is taken on emails and there are no changes to MX records.

Customized email threat report detailing your risk.

Historic analysis identifies and summarizes key issues, analytics, and trends across individuals, departments, and in total.

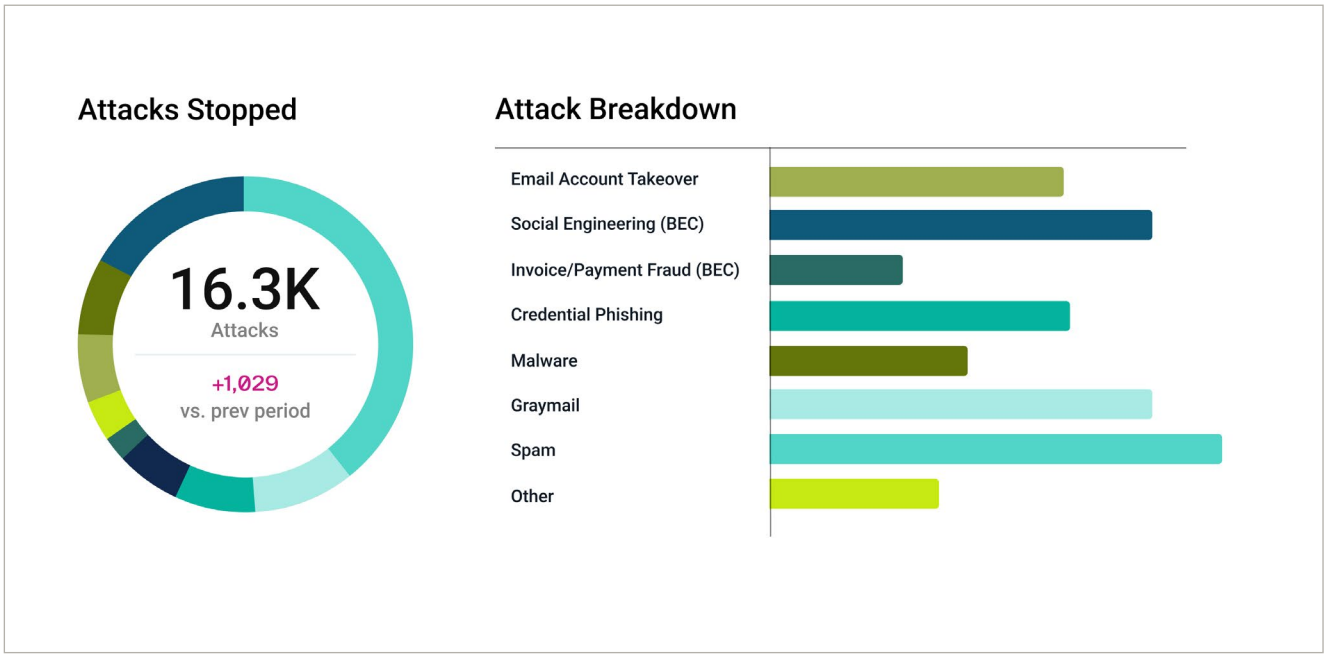
36 BEC attacks

stopped by Abnormal per month/customer (on average).

$36 million

The largest invoice fraud attack stopped requested $36 million from the organization.

Upon integration, Abnormal's solution operates in a read-only and passive manner, requiring just one minute to complete the process. The system then conducts a retrospective analysis to construct its models. Following this, a comprehensive analysis of any remaining undetected threats within the email environment is presented after the first week. Then, access to the console is provided, facilitating ongoing monitoring and management. After another week, real-time passive detections are reviewed.



Conclusion

So what are you waiting for? Though SEGs have historically served as vital tools in preventing email attacks, their efficacy is increasingly challenged by the evolving threat landscape. While SEGs excel in shielding email recipients from known threats, they fall short against the sophisticated techniques employed by modern threat actors. As cybercriminals continue to innovate, organizations require a modern security solution capable of thwarting advanced email attacks, optimizing expenditure, consolidating tools, and proactively intercepting emerging threats before they infiltrate employee inboxes.

By leveraging an AI-powered solution like Abnormal, organizations have made remarkable progress in bolstering their defenses, reducing risks, and ensuring seamless operations despite the dynamic nature of cyberattacks. This proactive security approach not only enables organizations to navigate the ever-changing threat landscape effectively but also instills confidence in their capacity to safeguard critical assets with resilience and adaptability.

Try it out today with no risk. You won't regret it!

About Abnormal AI

Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

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. Additional protection is available for Slack, Workday, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by more than 3,200 organizations, including over 20% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI.

Interested in Seeing How to Replace Your SEG?

Request a Demo ›

Replace Your SEG ›