WHITE PAPER

The Unexpected Benefits of Replacing a Secure Email Gateway with Abnormal AI

Customers Highlight Simple Administration, AI-Enhanced Investigation, and the Joy of "It Just Works"

Abnormal

Highlights of Replacing a SEG With Abnormal

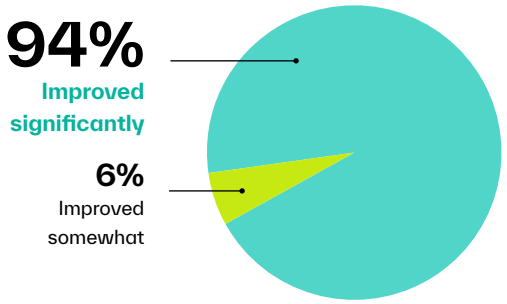
59%
FTEs to Administer and Manage Email Security Tools

91%
Cost to Investigate and Respond to User-Reported Emails

92%
Cost to Investigate False Positive Email Attack Alerts

100%
Time Employees Spend Reviewing Graymail Messages

Change in Email Security Efficacy



Executive Summary

Legacy secure email gateways (SEGs) can no longer keep pace with today's advanced threats. From business email compromise (BEC) and ransomware to payment fraud and account takeover, attacks are more sophisticated, frequent, and AI-powered than ever before, making traditional tools less effective and more resource-intensive to manage.

That's why many organizations are making the shift to a new model of email protection, one that fights malicious AI with AI-powered defense and stops advanced threats before they hit the inbox. Abnormal's technology exemplifies this modern approach, using behavioral AI to understand context and patterns associated with identities throughout your organization to better detect threats missed by legacy solutions.

But security professionals very reasonably ask if the benefits attributed to these platforms can be quantified. Are they large or small? In what specific areas do they produce operational cost savings and improved security? How soon are the benefits felt?

To better illustrate the value of this modern approach, Abnormal commissioned independent research from AimPoint Group. The research included a survey and interviews with a panel of cybersecurity managers from organizations that replaced their legacy third-party SEGs with the Abnormal platform. The findings highlight measurable improvements in operational efficiency and surprising cost savings, particularly in areas like incident response, platform management, and user-reported emails.

While the study focused on quantifiable operational outcomes, it also revealed broader benefits, including increased team productivity and confidence in stopping advanced threats. As the threat landscape continues to evolve, the research makes a compelling case for behavioral AI as the future of cloud email security.

Table of Contents

A New Paradigm for Email Security

Email security is a critical defense against the most serious cyber threats of our time, including credential phishing, ransomware, email account takeover, social engineering and business email compromise (BEC) attacks, invoice and payment fraud, and others.

Until recently, most organizations relied on secure email gateways (SEGs) to protect them against these menaces. But as email-based attacks have become more sophisticated and more frequent, SEGs have fallen farther behind, allowing an unacceptable number of malicious emails to reach employees. And there is little doubt that the increasing use of artificial intelligence by threat actors will result in even more sophisticated attacks in higher volumes, further exploiting weaknesses in SEG technology.

Beyond the increased risk of successful attacks reaching inboxes, other issues with SEGs include time-consuming administration and management, tedious work investigating and replying to phishing reports from users, and long times required to investigate and respond to email security incidents.

The Behavioral AI-Driven Email Security Platform

Solutions like Abnormal AI that utilize behavioral analytics and AI offer a new approach. Rather than relying on static rules or known indicators of compromise, they continuously analyze thousands of signals across identity, behavior, and communication patterns to detect anomalies that signal malicious intent. This shift from rule-based to behavior-based detection is key to stopping modern email attacks in real time. They also use AI to automate labor-intensive processes such as containing attacks, responding to phishing reports from users, and gathering context to investigate email security incidents.

While Abnormal is fully compatible with SEGs and can operate alongside them, in this report we surveyed and spoke exclusively with organizations that removed their SEG after deploying the platform.

Why? Because eliminating the SEG provides a clear view into the standalone efficacy of the Abnormal platform. These customers weren't just looking for an additional layer—they wanted to simplify their stack, reduce administrative overhead, and most importantly, improve their protection against the advanced, socially-engineered attacks that traditional tools often miss.

Unexpected Benefits

The success of behavioral email security platforms in real-world settings has led to rapid adoption as organizations deploy them to either replace or supplement SEGs. However, the value of this new model extends beyond blocking threats. By automating key tasks like phishing response, false positive reviews, and platform management, the Abnormal platform dramatically reduces operational overhead.

The magnitude of the changes is sizable, as shown by the tables in this document. But those numbers only tell part of the story. Behind each metric is a meaningful shift in how teams work, the stress they experience, and the value they're able to deliver. The following sections explore each of these benefits in more detail.

Simplified Security Tool Management

SEGs have developed a reputation for being relatively labor-intensive security tools in areas like configuration, administration, and management. Comments from interviews with the expert panel and survey data both bear out this assessment.

Panelists recalled that configuring SEGs involves a laborious process of creating safelists and blocklists, keyword lists, and complex policies, as well as configuring integrations with messaging, security, and network tools. They highlighted the fact that these types of tasks are ongoing as well—requiring constant additions and changes to lists, updating of policies, and new integrations. They also pointed to a continuing stream of exception requests that required modifying and extending policies, which often required a high level of expertise.

Data from the survey indicates that the average organization using a SEG devotes **1.4 staff members or full-time equivalents (FTEs) per 1,000 protected mailboxes** to administrative and management tasks.

In contrast, after replacing the SEG with Abnormal, the **FTEs devoted to these activities dropped to an average of .6 per 1,000 protected mailboxes, a reduction of 59%**.[1]

Panelists attributed the marked reduction in labor requirements primarily to the fact that the Abnormal platform replaces most lists and static policy rules with AI-driven behavioral analysis, which identifies and scores suspicious messages and attachments based on anomalous behaviors and continuous, detailed analysis of contextual factors.

Administration and Management of Email Security Tools

(All Figures are per 1,000 Protected Mailboxes)

WITH SEG	WITH ABNORMAL	SAVINGS	
1.4 FTEs	.6 FTEs	.8 FTEs	59%

> It's saved me personally hours every day and so much stress.
>
> **- SECURITY PRIVACY COMPLIANCE ANALYST,** GLOBAL TELECOMMUNICATIONS COMPANY

> It just works.
>
> **- SENIOR DIRECTOR OF INFORMATION SECURITY AND CISO,** FORTUNE 500 MANUFACTURER

1. The reductions tended to be somewhat less for small organizations and more for large ones. This probably reflects the fact that larger organizations have more diverse business units and locations, requiring more complex rules and more exceptions when using a SEG.

Accelerated Response to User-Reported Emails

Most email systems today allow email users to report what they suspect are phishing messages, often with a single click. This is an extremely powerful tool for fighting all the threats that attempt to entice employees to reveal confidential information or account credentials, download malware, visit compromised websites, or take other actions that undermine security.

However, as the panelists explained, very few people outside of email operations and security groups are aware of how much time most organizations spend on this task. For every user-reported email, security team members must:

- Investigate the email and contextual information to determine if it is or is not a genuine attack.
- Investigate the potential impact and determine if other email users received the same or similar emails, and if they have clicked on suspicious links or taken other potentially damaging actions.
- Compose a response to the employee reporter informing them of the outcome of their investigation and outlining the reasons for that verdict.
- Determine actions to contain it immediately and then tune email security tools to detect similar messages in the future.

Time Spent Responding to User Submissions with a SEG

According to survey data, when a SEG is the primary email security tool, the average organization receives 21.8 user-reported emails weekly for every 1,000 protected mailboxes and spends 15.3 minutes investigating and responding to each one. That works out to roughly 5.6 hours staff time per week for every 1,000 mailboxes within the organization.

To provide a rough idea of the cost in dollar terms, we assumed that the fully burdened cost of security team members doing the investigation and generating the responses was $65 an hour. At that rate, the cost to the average organization of these tasks is about $362 a week, or roughly $18,827 per year, for every 1,000 protected mailboxes.

Time Spent Responding to User Submissions with Abnormal AI

After implementing Abnormal and removing the SEG, the number of user-reported emails reaching security teams fell by 77%, from a weekly average of 21.8 to 5.1 per 1,000 protected mailboxes. The time spent investigating and responding to each reported email dropped from 15.3 minutes to 6.1 minutes, a reduction of 60%. When those two changes are factored together, they produce **a 91% overall reduction in time spent on user-reported emails**.

What might be the impact on cost to the organization? Using our assumption of $65 an hour for staff time, the cost for every 1,000 mailboxes for performing these tasks is reduced to $34 per week or $1,753 per year. That represents savings for every 1,000 mailboxes of **about $328 per week or $17,074 annually.**

What are the factors behind such dramatic savings? According to the panelists, an AI-driven behavior platform:

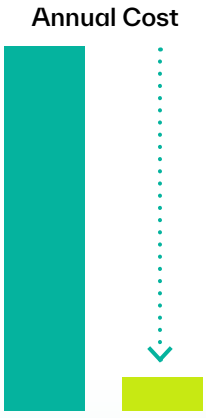
- Produces highly accurate verdicts on most reported emails, substantially reducing the number of messages that analysts need to investigate.
- Automates the collection and evaluation of contextual information, including other users receiving the same email and their actions, in case analyst investigations are required.
- Automatically generates clear, accurate responses to the employees who reported the emails.
- Automatically determines and initiates actions to contain the attack and improve detection in the future.

One panelist pointed out that the AI-generated responses to users increased the effectiveness of the organization's cyber awareness program, because they reinforced lessons about how to detect phishing emails.

Investigating and Responding to User-Reported Emails

(All Figures are per 1,000 Protected Mailboxes)

	SEG	ABNORMAL	REDUCTION	
Reported Emails Weekly	21.8	5.1	16.7	77%
Minutes to Investigate/Respond	15.3	6.1	9.2	60%
Hours Spent per Week	5.6	.5	5.1	91%
Cost per Week ($65/Hour)	$362	$34	$328	91%
Annual Cost	$18,827	$1,753	$17,074	91%



Reported Emails Weekly × Minutes to Investigate ÷ 60 = Hours Spent per Week × Cost per Week ($65/Hour) = Annual Cost

> I have confidence in what it's saying [about reported phishing emails]. If Abnormal says that it's fine, it's fine.
>
> - **SENIOR SYSTEMS ADMINISTRATOR,** LEADING MEDIA PRODUCTION COMPANY

Reduced False Positives with Smarter Detection

Security teams are inundated with alerts that flag emails as potential threats. While each alert demands attention, most turn out to be false positives. Despite this, analysts must still spend valuable time reviewing each message, gathering context, researching threat indicators like suspicious links, and determining whether others in the organization received the same email—and what actions, if any, were taken.

Our panelists described this work as not only time-consuming but also stressful. The stakes are high, and missing even one truly malicious email could have serious consequences. Yet the majority of this effort is spent chasing down harmless messages that were flagged unnecessarily.

False Positive Alerts With a SEG

According to survey data, when a SEG is the primary email security tool, in the average organization **41% of email security incident investigations are based on false positive alerts**. For many organizations the situation is much worse: 58% of respondents said that the number of false positives is in the "51-60% range" or "More than 60%." Further, organizations spend an average of **24.1 minutes investigating each false positive alert**.

When those factors are combined, we can calculate that for every 100 email attack alerts received and investigated, **16.6 hours is spent investigating the false positives**. If we assume that the average hourly cost of a staff member is $65, **the cost is $1,076 for each 100 alerts investigated**.

False Positive Alerts With Abnormal

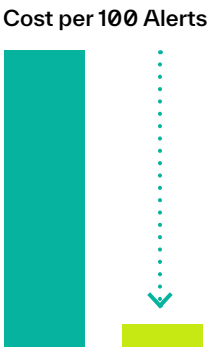
After implementing Abnormal and removing the SEG, the percentage of email attack alerts found to be false positives **fell dramatically, from an average of 41% of investigations to 8%**. In fact, for 78% of the organizations, false positives accounted for 10% or fewer of the total alerts.

Further, after implementing Abnormal and removing the SEG, the average minutes spent investigating each false positive alert **dropped from 24.1 minutes to 9.9 minutes—a reduction of 59%**. When combined with the 81% reduction in the percentage of alerts caused by false positives, **the average time spent investigating false positive email attack alerts fell 92%, producing an annual cost savings of $993 per 100 alerts**.

According to the panelists, the Abnormal platform filters out nearly all false positive alerts by using AI and behavioral analysis to accurately predict which emails are, and are not, malicious. They also note that for alerts that do get through, the platform collects and organizes contextual information that helps analysts conclude investigations much sooner. In addition, they point to features that accelerate containment and remediation, such as allowing them to pull back malicious emails that have been forwarded to other users.

Investigating False Positive Email Attack Alerts

	SEG	ABNORMAL	REDUCTION	
% of Email Alerts Based on False Positives	41%	8%	–	81%
Minutes to Investigate Each False Positive	24.1	9.9	14.2	59%
Hours Spent per 100 Alerts	16.6	1.3	15.3	92%
Cost per 100 Alerts ($65/Hour)	$1,076	$83	$993	92%



100 Alerts **x** Percent False Positives **x** Minutes to Investigate **÷** 60 **=** Hours Per 100 Alerts **x** $65 **=** Cost Per 100 Alerts

> [When we were using a SEG] we hardly had time or the right tools to investigate emails. Now we have that time and the assistance of Abnormal. We have a much more involved, accurate, all-encompassing email security system that we can manage.
>
> **- SENIOR DIRECTOR OF CORPORATE SECURITY OPERATIONS,** ENTERPRISE SOFTWARE COMPANY

Increased Productivity with Less Graymail

While most of this report focuses on how Abnormal reduces the burden on email and cybersecurity teams, it can also have a substantial impact on regular employee productivity by substantially reducing time spent sorting through graymail.

Graymail is often described as communications from legitimate sources that are unwanted by the recipient. It usually results from employees opting to receive updates, news, tips, and analysis from vendors and information providers, but finding that the information contained in them is low-value.

However, unlike spam and phishing messages, an email that is perceived as useless graymail by most people may be of interest or even very important to some. Simply blocking messages that appear to be graymail will harm those few potential recipients who do value the content and potentially cause complaints about intrusive email security. To avoid these conflicts, most organizations throw the burden of dealing with graymail on employees.

Hidden Cost of Graymail Without Abnormal

How costly is this hands-off approach to managing graymail? According to our survey data, without Abnormal **the average employee receives 18.2 graymail messages per day and spends an average of 13.9 seconds opening, assessing, and deleting each message**. That works out to 253 seconds, or just over 4 minutes, per employee per day.

While 253 seconds a day doesn't sound like much, across 1,000 protected mailboxes it adds up to 70.4 hours per day. If we assume that the fully-burdened cost of an average employee is $50 an hour and that employee works 200 days a year, then **the lost productivity time for 1,000 mailboxes is $3,518 per day, or $703,513 annually**.

Productivity Gains From Graymail Removal with Abnormal

According to the panelists, Abnormal almost eliminates employee time spent assessing and rejecting graymail messages. It accomplishes this by using AI to determine which emails will be unwanted for each individual, based on that person's observed behaviors and preferences. For example, if an employee regularly deletes messages with certain characteristics or moves them to a spam or promotions folder for later review, the platform can perform the same actions automatically on behalf of the employee.

Increased Productivity with Less Graymail

(All Figures are per 1,000 Employees)

	SEG	ABNORMAL	REDUCTION
Graymail Messages in Mailbox Daily	18.2	–	–
Seconds to Investigate Each Message	13.9	–	–
Hours per Day per 1,000 Employees	70.4	–	–
Cost per Day ($50/Hour)	$3,518	–	–
Annual Cost	$703,513	–	$703,513

Graymail Messages Daily **x** Seconds to Investigate **x** 1000 ÷ 3600 **=** Hours per Day per 1,000 Employees **x** $50 **x** 200 Days **=** Annual Cost

Over the last 30 days, Abnormal has saved our employees over 600 hours reviewing graymail. And 51 hours for VIPs. It's actually kind of ridiculous.

- SENIOR DIRECTOR OF INFORMATION SECURITY AND CISO, FORTUNE 500 MANUFACTURER

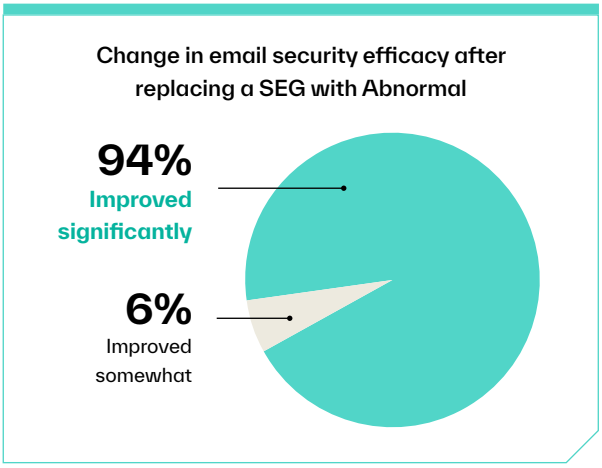
Reduced Costs Across Security Operations, Tools, and Teams

Replacing a SEG with an AI-powered email security platform clearly produces significant operational and productivity savings. But do those savings come at the expense of reduced security, higher costs in areas such as licenses and service fees, or long and expensive implementation projects? Survey data shows that, on the contrary, email security efficacy improved, direct costs decreased, and implementation was fast and simple.

Efficacy of Security Operations

In the survey, we asked respondents about the impact replacing a SEG and implementing the Abnormal Behavior Platform had on security efficacy.

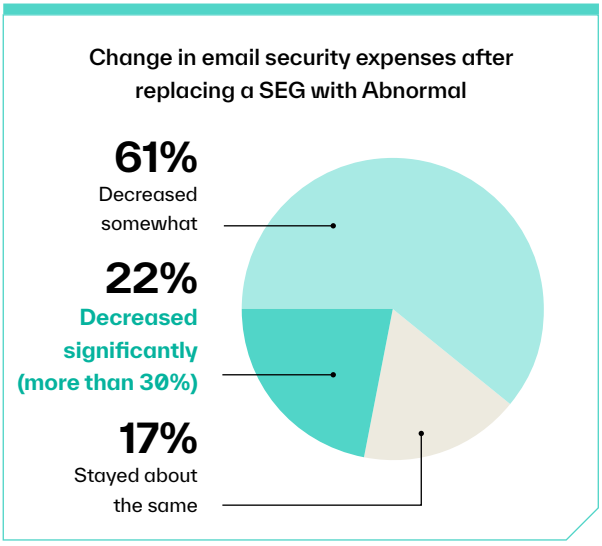
Six percent of the respondents indicated that security efficacy improved somewhat, and a whopping **94% stated that security efficacy improved significantly**. No respondents indicated that their organization's security efficacy stayed the same or weakened.



Security Tool Expenses

We asked the survey respondents about the impact of replacing a SEG and implementing the Abnormal Behavior Platform on expenses for email security.

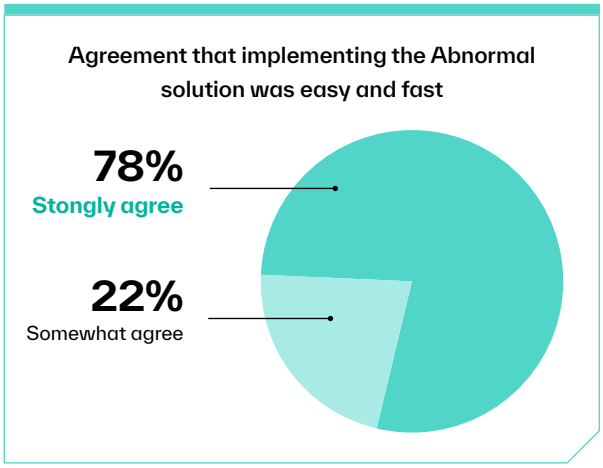
Of the organizations in the survey, **22% indicated that their email security expenses decreased more than 30%.** An additional 61% found that expenses "decreased somewhat." The remaining 17% indicated that email security expenses stayed about the same. No organizations experienced an increase in email security expenses.



Ease of Tool Implementation

Some new technologies require difficult and lengthy implementation processes that offset or postpone benefits. To determine if that was a factor in this case, we asked respondents to describe their agreement with the statement "Implementation of the Abnormal solution was easy and fast."

Twenty-two percent of the respondents indicated that they "somewhat agree" with that statement and many more, **78%, said that they "strongly agree."** No respondents indicated that they somewhat or strongly disagreed.



The easiest product I've ever implemented.

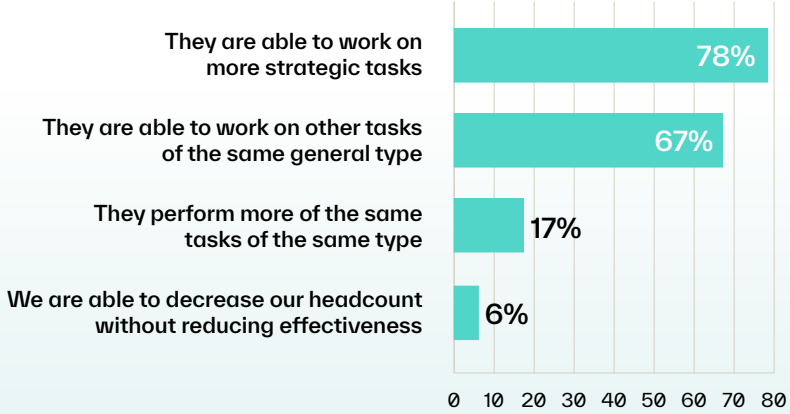
- **SENIOR DIRECTOR OF INFORMATION SECURITY AND INFRASTRUCTURE,** LEADING MEDIA COMPANY

Impact on Security Teams

We anticipated that some security practitioners might want to know what happened to the email and cybersecurity team members who were freed up from routine tasks. So we asked the survey respondents how those people's time was reallocated. They were allowed to select more than one answer.

The results: **in 78% of organizations, team members were switched to work on more strategic tasks,** and in 67% of organizations, some worked on other tasks of the same general types as the ones they had been doing before. Examples include analyzing root causes that formerly nobody had time to investigate and creating stronger email security policies. At 17% of organizations, the team members performed more of the same tasks of the same type, such as responding to more user reports. Only six percent of the organizations used any of the time savings to reduce headcount.

How the time saved by email and security team members was reallocated



Nobody wants to manage a SEG. We took the people who had been doing that and created a new team for mobile security and handheld devices. They loved the change.

- **DIRECTOR OF INFORMATION SECURITY,** FORTUNE 500 RETAIL COMPANY

Putting the Pieces Together

	SEG	ABNORMAL BEHAVIOR PLATFORM	REDUCTION	
Administration and Management of Email Security Tools (Figures Are Per 1,000 Mailboxes)				
Full-Time Equivalent Employees	1.4	.6	.8	59%
Investigating and Responding to User-Reported Emails (Figures Are Per 1,000 Mailboxes)				
Hours Spent Per Week	5.6	.5	5.1	
Cost Per Week ($65/Hour)	$362	$34	$328	
Annual Cost	$18,827	$ 1,753	$ 17,074	91%
Investigating False Positive Email Attack Alerts (Figures Are Per 100 Alerts)				
Hours Spent Per 100 Alerts	16.6	1.3	15.3	
Cost Per 100 Alerts ($65/Hour)	$1,076	$83	$993	92%
Increased Productivity with Less Graymail (Figures Are Per 1,000 Employees)				
Hours Per Day	70.4	–		
Cost Per Day ($50/Hour)	$3,518	–		
Annual Cost	$703,513	–	$703,513	100%

Conclusion

As SEGs fall farther behind new generations of email-based threats, many organizations are exploring behavioral AI-driven solutions—either as replacements or to augment their existing defenses. Until recently, however, there's been little concrete data comparing the performance of these solutions.

Based on the survey and interviews conducted by AimPoint Group, it is clear that email security solutions such as Abnormal deliver substantial improvements over SEGs in several operational areas while improving security efficacy.

These benefits extend well beyond those that can be easily quantified. Panelists, all of whom have managed both a major SEG and the Abnormal platform, frequently mentioned how much their teams appreciated being relieved of routine, repetitive tasks. This shift allowed them to focus on more strategic, higher-impact work. Many also highlighted how their own roles as cybersecurity leaders were transformed by a solution that "just works"—without the need for constant tuning, monitoring, and second-guessing.

A consistent recommendation from many panelists was the value of running a proof of concept with the Abnormal platform operating behind an existing SEG. Doing so quickly reveals the threats SEGs fail to catch—threats that Abnormal detects with precision—while also demonstrating the benefits of simplified management, fewer false positives, and the broader operational enhancements outlined in this report.

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 Replacing the SEG Could Benefit Your Organization?

See Your ROI ›

Request a Demo ›

ABNORMAL.AI