IRONSCALES

The Hidden Gaps in SEG Protection

A Data-Driven Analysis of SEG Effectiveness and Missed Threats

Executive Summary

You already know your Secure Email Gateway (SEG) isn't catching everything it's supposed to catch. Now, the data confirms it.

Our comprehensive analysis of what security teams across nearly 2,000 of our 15,000+ customer environments have experienced reveals that for every 100 mailboxes, an average of 67.5 additional phishing emails bypass legacy security solutions monthly. These aren't hypothetical threats or simulated tests; they're real-world attacks landing in employee inboxes after evading detection by industry leading SEGs.

This protection gap isn't just a security risk, it's an operational drain. Each phishing incident takes 27.5 minutes to resolve, costing $36.29 per event, consuming nearly one-third of IT security teams' time.

The data shows notable performance variations across SEG vendors, with missed attack rates ranging from 38.4 to 101 per 100 mailboxes monthly. Smaller organizations face disproportionately higher risk, with companies under 100 mailboxes experiencing up to 7.5x more missed attacks than larger enterprises.

Vendor scams and credential theft consistently represent the largest categories of missed attacks (30-42% and 21-41% respectively), reflecting attackers' shift toward social engineering tactics that exploit human psychology rather than technical vulnerabilities.

This paper quantifies the risks, operational burdens, and financial impact of SEG failures, and outlines a better approach to email security.

TABLE OF CONTENTS

Introduction

Unique Visibility at the Inbox Level

Serving over 15,000 customers globally, IRONSCALES has a distinctive vantage point for analyzing email security effectiveness. Unlike perimeter defenses like SEGs that operate upstream, we operate at the inbox level where email is actually delivered. This placement gives us unprecedented visibility into what upstream defenses are missing—we see exactly what gets through existing security layers and lands in user inboxes. This is the differentiator: we're not speculating about SEG performance, because we can see and count the actual misses in real time.

This analysis is based on 30 days of real-world email traffic across 1,921 customer environments, representing a diverse subset of our global customer base. This comprehensive dataset provides unprecedented insight into the actual effectiveness of SEGs commonly used by all size organizations today.

Scope of the Study

- **1,921 customer environments evaluated**
- **Average organization size: 548 mailboxes per environment**
- **Data gathered from 30 days of real-world email traffic, not lab tests**

Unlike theoretical tests or vendor claims, our data comes from actual emails landing in real inboxes, giving you confidence that these are genuine attacks bypassing real defenses.

Purpose of This Paper

This paper is not about claiming that "SEGs are bad." Rather, it validates what many security teams already suspect, their SEG is letting too much through. For prospects, it confirms "you're not imagining it, others see this problem too." For our customers, it provides proof that we are delivering on our promise; catching what others miss.

By analyzing 30 days of attack data from organizations using both SEGs and IRONSCALES, we can quantify exactly how many attacks SEGs are missing, and the types of attacks that give them the most trouble.

1. Why SEGs Are Missing More Than You Think

Attackers have evolved beyond rule-based defenses. AI-generated phishing, social engineering, and tailored attack techniques are now designed to bypass static filtering methods.

Empirical Data - The Scale of Missed Phishing Attacks

Across the customer environments analyzed, we observed a consistent pattern of missed phishing attacks, an average of **67.5 additional phishing emails bypassing SEG defenses per 100 mailboxes each month**. This data is not theoretical—it represents actual phishing emails that bypassed SEG as well as Microsoft 365 (M365) & Google Workspace (GWS) protection, and were identified by our security solution.

The data demonstrates that smaller organizations are disproportionately affected. Organizations with fewer than 100 mailboxes experience significantly higher rates of missed attacks across all SEG vendors. This suggests that smaller organizations, which often lack dedicated security resources, are particularly vulnerable to SEG failures.

SEGs are missing an average of 67.5 phishing emails per 100 mailboxes every month.

Breaking down the data by vendor shows that some SEGs miss significantly more than others, and that attack types vary by provider. The table below details how frequently each SEG fails to block phishing attacks and which attack types are slipping through most often.

SEG Vendor	Missed Attacks per 100 Mailboxes (Monthly)	Leading Attack Types
Barracuda	101	Vendor Scam - 38.9% Credential Theft - 35.7%
Proofpoint	68.4	Vendor Scam - 33.0% Credential Theft - 29.8%
Cisco IronPort	51.6	Vendor Scam - 40.4% Credential Theft - 33.0%
Mimecast	38.4	Credential Theft - 30.3% Vendor Scam - 19.1%

While vendor performance varies, a key factor affecting SEG effectiveness is organization size. The chart below illustrates how smaller organizations experience significantly higher rates of missed attacks across all SEG providers.

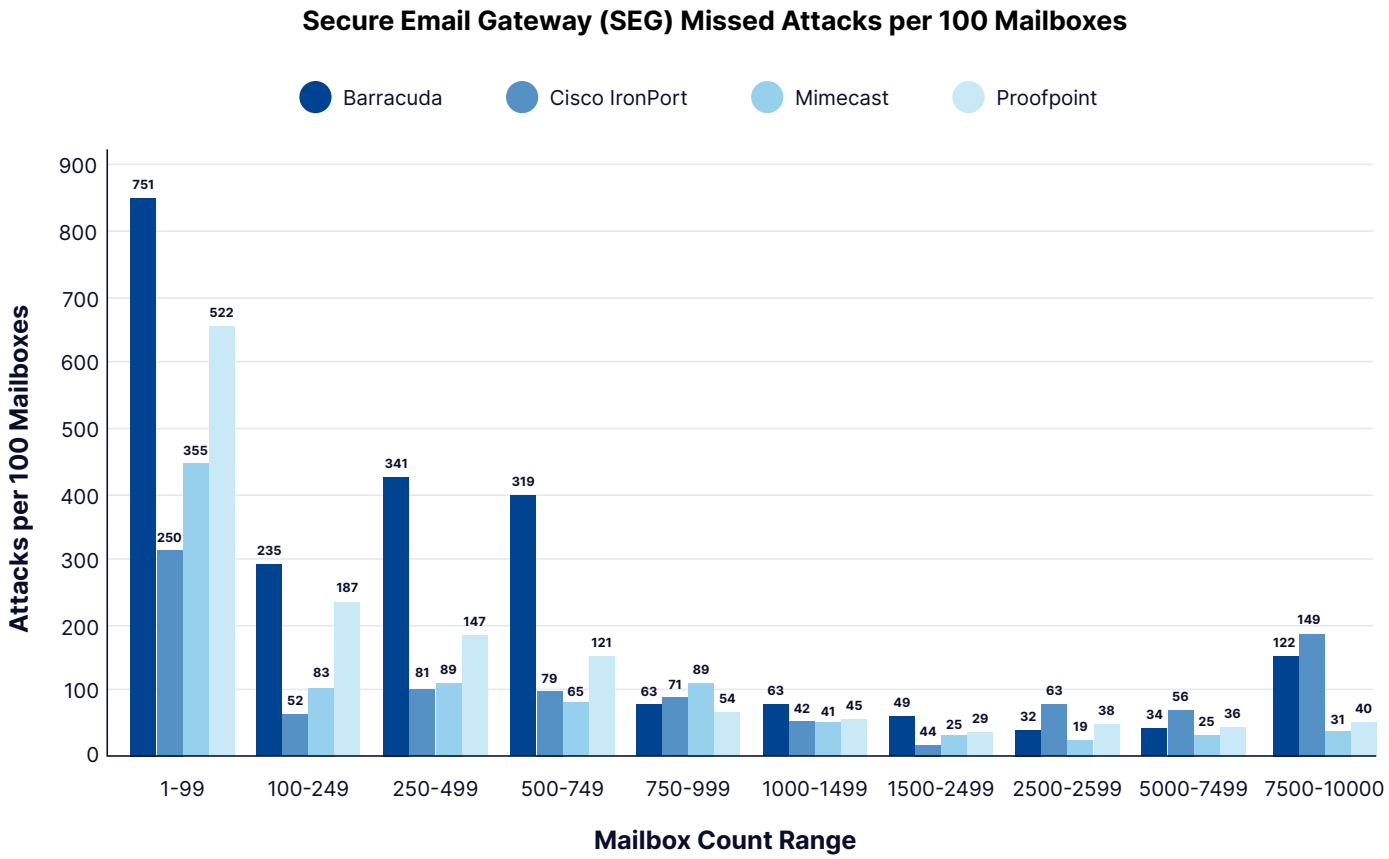

Figure 1: SEG missed attacks per 100 mailboxes across different organization sizes

Key Findings:

1. **Higher Risk for Small Organizations:** Organizations with fewer than 100 mailboxes experience significantly higher rates of missed attacks across all SEG vendors, with Barracuda showing the highest rate at 751 missed attacks per 100 mailboxes.

   Note: While our data strongly suggests SEG effectiveness is a major factor, smaller organizations may also face compounding risks due to limited security resources, fewer trained security personnel, and weaker email hygiene. These factors could further contribute to the higher rate of missed attacks in this segment.

2. **Mid-Size Organizations:** Experience the lowest rates of missed attacks across all vendors, suggesting better SEG effectiveness or potentially different attack patterns targeting these organizations.

3. **Vendor Performance:** Across all organization sizes, Mimecast shows the lowest average rate of missed attacks (38.4 per 100 mailboxes), followed by Cisco IronPort (51.6), while Barracuda has the highest average rate (101).

4. **Large Enterprise Anomaly:** Organizations in the 7,500-10,000 mailbox range show an unexpected increase in missed attacks compared to the mid-size ranges, particularly with Cisco IronPort (149) and Barracuda (122).

Attack Type Distribution - What SEGs Are Missing

When analyzing the types of attacks that bypass SEGs, clear patterns emerge. The data reveals that while all SEGs struggle with phishing threats, the types of attacks they miss vary widely. Some providers allow more credential theft attempts, while others let through high rates of vendor scams or invoice fraud. The table below breaks down these attack patterns by SEG provider.

Missed phishing attacks by attack type across different SEG providers.
Higher percentages indicate more missed attacks of that type.

	Barracuda	Cisco IronPort	Mimecast	Proofpoint
Advance-fee Scam	3.9%	4.7%	10.1%	5.8%
Bulk Phishing	3.7%	5.3%	3.8%	6.2%
Business Email Compromise (BEC)	1.7%	1.9%	6.8%	2.1%
Credential Theft	41.2%	34.7%	22.5%	21.6%
Extortion	4.8%	1.5%	5.1%	1.7%
QR-Code & Image-Based Attacks	0.1%	0.3%	2.1%	1.1%
Invoice Phishing	5.6%	4.6%	4.7%	9.9%
Suspected Malicious Content	1.6%	2.0%	2.3%	2.1%
Vendor Email Compromise (VEC)	2.4%	1.3%	2.1%	2.5%
Vendor Scam	30.1%	39.0%	26.6%	42.4%
CEO/VIP Impersonation	2.9%	1.0%	2.4%	1.3%
Vishing Attack	2.0%	1.8%	2.5%	1.5%

Figure 2: Attack type distribution by SEG provider (averaged across all organization sizes)

For attack type definitions, see Appendix A: Phishing Attack Types Defined

These results show clear trends: Vendor scams are the most common missed attack type, followed closely by credential theft. Attackers are increasingly using Quishing (QR-code phishing) and image-based techniques to evade SEG detection, exploiting gaps in their filtering methods.

Key Insights:

- Vendor Scam represents the largest category of missed attacks across all SEG providers (30-42%)
- Credential Theft is the second most common missed attack type (21-41%)
- Emerging threats like Quishing / Image-Based Attacks and Vishing are beginning to appear in the mix of missed threats

These findings highlight a critical reality: SEGs are particularly vulnerable to socially engineered attacks that don't rely on traditional indicators like malicious attachments or suspicious links. The prevalence of vendor scams and credential theft attempts suggests that attackers are focusing on techniques that exploit human psychology rather than technical vulnerabilities—precisely the types of attacks that traditional, rule-based systems struggle to detect.

What Happens to These Missed Attacks?

Recent industry research reveals the real-world impact of these missed phishing emails:

- **10.4% of users click on phishing links** when they receive a phishing email
- **6.5% submit credentials** after clicking
- This means **62.3% of clickers fall for the scam and submit their credentials** [1]

These aren't hypothetical numbers, they represent what happens when phishing emails evade your SEG and land in employee inboxes.

The implications are sobering: If SEGs let through an average of 67.5 phishing attacks per 100 mailboxes monthly (as discovered from our analysis), and 10.4% of users click, that means approximately 7 users per 100 mailboxes are at risk of compromise each month. With 6.5% ultimately submitting credentials, an organization with 1,000 mailboxes could suffer about 50 compromised accounts per year from attacks that their SEG security missed entirely.

The Operational & Financial Cost of SEG Failures

The impact of missed phishing attacks goes far beyond security risk. According to Osterman Research's 2022 study "The Business Cost of Phishing" [ii]

- **Phishing-related activities consume one-third of IT and security teams' available time**
- **This equates to $52,666[iv] per IT/security professional annually just to handle phishing**

Each phishing email takes 27.5 minutes to resolve, costing $36.29 per incident.

[1] The 62.3% figure represents the percentage of users who submit their credentials after clicking a phishing link. It is calculated by dividing the percentage of users who enter credentials (6.5%) by the percentage who click a phishing link (10.4%). In other words, when a user clicks on a phishing email, there is a 62.3% chance they will fall for the scam and provide their login credentials.

For an organization with just five security professionals, that's over $263,330 annually spent on managing phishing threats, and this doesn't include the potential costs of successful breaches.

Beyond these direct operational costs, SEGs demand constant tuning and policy management to keep pace with evolving threats. This maintenance burden falls particularly hard on smaller organizations with limited IT security resources. In fact, our data strongly supports the hypothesis that smaller organizations lack the personnel and specialized skills required to properly configure and maintain SEGs—explaining why companies with fewer than 100 mailboxes experience up to 7.5x more missed attacks than larger enterprises with dedicated security teams.

Default configurations often fall short, forcing teams to spend additional time maintaining rules, investigating misses, and fine-tuning filtering policies, all adding to the operational overhead.

2. The Threat Landscape Is Evolving Faster Than SEGs Can Adapt

Attackers are early adopters and innovators. They exploit AI, automation, and multi-channel deception, and they usually do it faster than security teams can respond. Traditional SEGs, built on static rules and reputation filtering, are struggling to detect these evolving tactics.

AI-Powered Phishing & Polymorphic Attacks

Generative AI has dramatically lowered the barrier to creating sophisticated phishing campaigns. Attackers can now:

- Generate grammatically perfect, convincing emails that bypass language-based detection
- Automate the creation of tailored, personalized messages that appear legitimate
- Develop polymorphic attacks that mutate with each deployment, evading signature-based detection
- Craft context-aware social engineering content based on target research

Tactics like QR-code phishing and multi-channel attacks expose the blind spots of SEG-based security.

> ***Threat actors adopt new technologies rapidly, leveraging AI and automation to bypass traditional defenses faster than security teams can respond.***

Emerging Attack Vectors

Threat actors are expanding their tactics beyond traditional phishing emails to include:

- **QR Code Phishing**
  Embedding malicious QR codes in emails that bypass URL scanning
- **Image-Based Attacks**
  Using images containing text to circumvent content analysis
- **Multi-Channel Attacks**
  Combining email, SMS, and voice phishing in coordinated campaigns
- **Business Email Compromise (BEC)**
  Sophisticated impersonation attacks that rarely contain malicious links or attachments

SEGs that focus on scanning links and attachments will continue to struggle to detect these emerging threats. Email security simply can't rely on conventional phishing indicators.

The Business Cost of SEG Failures

The financial impact of these missed phishing attacks is substantial:

- **Business Email Compromise accounts for 24-25% of all financially motivated breaches** with a median loss of $50,000 per incident according to the Verizon Data Breach Investigations Report[v]
- **BEC incidents have nearly doubled over the last two years** as attackers refine their techniques
- **The average cost of a data breach now exceeds $4.88 million** (IBM Security, 2024[vi]), with phishing as a leading initial attack vector

For many organizations, just one successful phishing attack can cause irreparable damage. Defending against modern threats requires an approach that evolves alongside attackers, not one that reacts after the fact.

3. API-Integrated, Adaptive Protection Is the Future

Email security must evolve beyond perimeter-based filtering. Adaptive protection continuously learns, detects emerging threats, and stops phishing attacks that bypass conventional defenses. IRONSCALES offers critical advantages over perimeter-based defenses with its Adaptive AI approach that evolves alongside the threat landscape.

Why Adaptive Protection Delivers Better Results

IRONSCALES provides several key advantages that traditional SEGs simply cannot match:

1. **API-based integration** with Microsoft 365 and Google Workspace that deploys in minutes without changing MX records or disrupting mail flow, unlike traditional SEGs.

2. **Self-learning AI builds a detailed social graph** through natural language processing (NLP) to establish normal communication patterns for every inbox in your organization, creating a personalized baseline.

3. **Adaptive AI detection evolves continuously,** using the social graph to perform real-time reputation, content, and behavioral analysis that identifies even the subtlest signs of malicious threats.

   Note: Even with advanced AI defenses, a small percentage of never-before-seen attacks can still evade detection. That's why our approach incorporates human analysts and customer-driven feedback (human-in-the-loop), ensuring continuous improvement and rapid AI/ML model adaptation.

4. **Human-in-the-loop feedback** from our community of over 25,000 security professionals (an average of 1.6 per customer organization) continuously improves our detection capabilities through a powerful machine learning feedback loop.

5. **Automated remediation** and response automatically classifies, clusters similar messages, and remediates threats, reducing remediation time from minutes to seconds.

   Note: While SEGs provide a foundational layer of security, our findings highlight their limitations against modern, socially engineered threats. Security teams should consider augmenting their SEG with adaptive, inbox-level detection to catch what traditional filtering systems miss.

Real-World IRONSCALES Impact

Organizations implementing IRONSCALES have seen dramatic improvements in their email security posture:

- **Fortitude Re** detected and remediated 13,000 phishing emails that bypassed their existing defenses, saving an estimated $78,000 in operational costs—a figure based on the customer's own cost calculations, factoring in salary, time, and remediation efforts.

- **Sonic Automotive** reduced phishing remediation time from 25 minutes to just 20 seconds per incident, stopping 177,000 phishing threats in 9 months that their existing security stack missed.

- **Concentrix** uncovered 179,659 phishing emails in 90 days that evaded their traditional email security, saving 8,782 analyst hours (equivalent to four full-time security professionals).

These results demonstrate the tangible value of IRONSCALES Adaptive AI protection that works to close critical gaps and reduce the operational burden on security teams.

4. Strategic Implications for Security Leaders

The data presented in this paper reveals a clear and quantifiable security gap in traditional email defenses. As phishing tactics evolve and attackers employ increasingly sophisticated social engineering techniques, the limitations of conventional security approaches have significant implications for organizational risk posture and security team operations.

Quantifying the Protection Gap

The evidence shows that relying solely on SEGs or native email security leaves organizations exposed to a substantial volume of phishing attacks:

1. **Consistent detection failures across vendors** – phishing emails regularly bypass legacy solutions, leaving organizations exposed.
2. **Disproportionate risk for smaller organizations** – companies with fewer than 100 mailboxes face substantially higher rates of missed attacks
3. **Predictable attack patterns** – vendor scams and credential theft consistently represent the largest categories of missed threats

Operational Impact Assessment

The operational burden created by these security gaps demands strategic consideration:

1. **Resource consumption** – each phishing email requires 27.5 minutes to resolve at $36.29 per message
2. **Team capacity reduction** – phishing-related activities consume approximately one-third of security team time
3. **Maintenance overhead** – SEGs require ongoing tuning and policy management to maintain effectiveness
4. **Financial risk exposure** – with Business Email Compromise losses averaging $50,000 per incident

Future-Focused Security Strategy

As the threat landscape continues to evolve, security leaders should consider these strategic priorities:

- **Assess detection capabilities & protection layers** – evaluate existing security performance using objective metrics and explore layered defense approaches to close detection gaps.
- **Integrate automation for faster remediation –** implement technologies that cut response time from minutes to seconds, reducing security team workload.
- **Prioritize security investments strategically –** align resources with quantifiable business impact to maximize operational efficiency.

Security teams increasingly need tools that provide nuanced detection capabilities—particularly socially engineered attacks. Solutions that combine behavioral analysis, machine learning, and automated remediation offer the most promising approach to addressing the email security gaps documented in this paper.

- **SEGs fail to block a significant number of phishing attacks, exposing organizations to ongoing risk.**
- **The operational burden is high. IT teams spend significant time manually remediating missed phishing emails.**
- **Modern threats require adaptive AI-based inbox-level security, not just perimeter-based filtering**

Given these findings, security leaders should evaluate their SEG's performance by measuring how many attacks bypass their existing defenses. Solutions that operate at the inbox level, such as API-integrated detection and response, provide a critical layer of protection against evolving threats.

These findings provide a data-driven case for reevaluating email security strategies. Security leaders should assess their SEG's real-world performance and consider solutions that strengthen inbox-level protection against evolving phishing threats.

Additional Resources

Email Security Gap Calculator – see how many email attacks organizations like yours are missing based on size and SEG vendor

The Business Cost of Phishing (Osterman Research, 2022) - Detailed analysis of operational impact of email attacks

Appendix: Phishing Attack Types Defined

Phishing attacks take many forms, each with unique tactics designed to bypass security defenses. Below is a reference guide to the attack types analyzed in this report.

Attack Type	Definition
Advance-Fee Scam	Scammers request upfront payments or fees under false pretenses, promising rewards that never materialize.
Bulk Phishing	High-volume, generic phishing emails sent indiscriminately to large numbers of recipients, aiming to steal credentials or distribute malware.
Business Email Compromise (BEC)	Attackers impersonate executives or employees to deceive recipients into transferring funds or sharing sensitive data.
Credential Theft	Phishing emails designed to trick users into revealing login credentials by impersonating trusted entities.
Extortion	Threats to expose personal or corporate data unless the victim complies with demands, often involving ransom payments.
Quishing or Image-Based Attack	Phishing emails using QR codes or embedded images instead of clickable links. These images often spoof genuine transactional emails to bypass keyword-based security filters.
Invoice Phishing	Fraudulent emails disguised as invoices from vendors, tricking recipients into making unauthorized payments.
Suspected Malicious Content	Emails containing no explicit malware or malicious links but designed to manipulate recipients into harmful actions (e.g., transferring funds, revealing credentials).
Vendor Email Compromise (VEC)	Attackers hijack a supplier or business partner's email account to send fraudulent invoices or payment requests.

Attack Type	Definition
Vendor Scam	Fake emails impersonating vendors or service providers to request payments, refunds, or sensitive information.
CEO / VIP Impersonation	Attackers pose as high-profile executives, board members, or influential figures to manipulate recipients into urgent actions, such as transferring money or sharing sensitive data.
Vishing Attack	Social engineering via phone calls or attached voicemail messages. These may include malicious instructions (e.g., requesting financial transfers) or malware-laden audio files (e.g., ransomware disguised as a voicemail alert).

Methodology Note: The data in this whitepaper is based on analysis of 30 days of email traffic across 1,921 customer environments with an average size of 548 mailboxes per organization. All figures represent actual phishing emails that bypassed existing security controls and were subsequently identified by IRONSCALES.

i. Fortra. (2023). Phishing Benchmark Global Report 2023: Gone Phishing Tournament. Retrieved from https://terranovasecurity.com/gone-phishing-tournament/
ii. Osterman Research. (2022). The Business Cost of Phishing. Retrieved from https://ironscales.com/resources/white-papers/business-cost-of-phishing
iii. The estimated cost per phishing incident has been updated to reflect current (March 2025) salary and benefits data for IT and security professionals. The original figure of $31.32 was calculated using 2022 salary data, which has been adjusted for wage inflation and increased demand for cybersecurity expertise.
iv. The annual cost per IT/security professional dedicated to handling phishing has been revised upwards to $52,666. This adjustment accounts for the increased composite salary and benefits for IT and security roles as of March 2025. The original figure of $45,726 was based on 2022 salary data, which no longer accurately reflects current compensation levels in the cybersecurity field.
v. Verizon. (2023). Data Breach Investigations Report (DBIR). Retrieved from https://www.verizon.com/business/resources/reports/dbir/
vi. IBM Security. (2024). Cost of a Data Breach Report. Retrieved from https://www.ibm.com/security/data-breach