IRONSCALES

The SEG Breakup Guide:

Why MSPs Are Moving On

Introduction

Break ups are never easy. Whether it's ending a relationship with a company, friend, business associate, romantic partner, or even a technology. We can't speak to some of these categories, but when it comes to cybersecurity, your technology stack should be evaluated on an ongoing basis to ensure you are getting the most ROI. Moore's Law was coined in 1965 by Gordon Moore (the co-founder of Intel), and it states that every 18-24 months, computers get twice as powerful and almost half as expensive. Once again, that was in 1965.

Within the MSP market, owners and operators often get attached to certain technologies for a slew of reasons ranging from a well-made UI to integration capabilities to pure comfort. It's one thing to keep the keys to a 30-year-old vehicle that still gets you from point A to point B, but **this isn't a personal matter.** Your organization has a responsibility to deliver quality security services to your customer base. You have a responsibility to find the best technology for your business and end users. Which is why **we need to have a discussion about your Secure Email Gateway (SEG).**

Most security practitioners we speak with understand the SEG isn't keeping up with today's attacks, but few of them have a plan to solve the problem. The SEG may have worked well in the past, but modern threat actors are incorporating a level of sophistication and frequency that these legacy technologies simply can't combat. **AI-generated scams and social engineering techniques expose the inherent weaknesses of static, rule-based SEG defenses**. It's one thing to have a gut feeling, but it's something entirely different to have the data to back it up.

In 2025, we analyzed customers using both a SEG and our Adaptive AI Integrated Cloud Email Security (ICES) solution to uncover what MSPs have long suspected. The data confirms what most MSPs have long suspected: SEGs miss an *average* of **67.5 phishing emails per 100 mailboxes every month.** These missed threats are not just blip on the radar screen —they translate to real risks, increased operational burdens, and financial costs for MSPs and their clients.

The purpose of this white paper is to provide informative and educational cybersecurity guidance for MSPs aligned with, and contextualized to, the email security market. This white paper will walk you through the different eras of email security, the data from the latest IRONSCALES study, risks posed by using a SEG today, and best practices for breaking up with your SEG.

TABLE OF CONTENTS

Chapter 1: The Evolution of Email Security

How Did We Get Here? An Homage to Email Security Solutions of the Past

19th Century: *Antivirus and Spam Filters: The Early Defenses*

The earliest forms of email security relied on antivirus software and spam filters. Antivirus engines scanned email attachments for known malware signatures, while spam filters attempted to block unwanted emails based on sender reputation and keyword analysis. These tools provided a necessary first layer of defense, but their limitations became clear as attackers found new ways to evade detection.

- **Strengths:** Effective at detecting known viruses and blocking mass spam campaigns by deploying IP/domain based filters.
- **Weaknesses:** Heavily dependent on signature-based detection, which means new threats often went unnoticed until they were identified and cataloged (often too late).
- **Operational Impact:** Created a false sense of security, as businesses often assumed that having antivirus and a spam filter was enough to prevent email-based threats.

As email attacks evolved beyond simple malware attachments and spam messages, security teams needed more advanced solutions that could detect emerging, sophisticated threats in real time.

1990s and 2000s: The Rise of the Secure Email Gateway (SEG)

The origins of the **SEG** can be traced back to the explosive growth of email usage in the 1990s. As businesses embraced email as a primary form of communication, attackers quickly recognized it as a lucrative vector for delivering spam, malware, and viruses. This surge in abuse gave rise to the first generation of email filtering technologies—what would eventually become SEGs.

Early innovators like **Brightmai**l (founded in 1998), **Postini** (1999), and **IronPort Systems** (2000) developed dedicated solutions to sit at the email perimeter. These systems scanned inbound and outbound emails for threats, relying heavily on **static rules, signature matching, and IP reputation** to detect and block malicious content. Over time, these companies were acquired by major players**—Symantec**, **Google**, and **Cisco**, respectively—who integrated SEG functionality into broader security platforms.

SEGs quickly became a default security layer for enterprises and growing SMBs, especially as compliance regulations began mandating data protection for electronic communications. They were often deployed as hardware appliances on-premises, or as early managed cloud-based services.

Capabilities of Early SEGs:

- **Blocking known threats:** Effective at protecting against spam, viruses, and malware using signature-based detection.
- **Policy enforcement:** These capabilities helped organizations meet compliance requirements (e.g., content filtering, DLP).
- **Customizable rulesets:** Administrators were given access to granular control over email flow.

Weaknesses & Growing Pains:

- **Static filtering:** Struggled to detect novel, socially engineered phishing attacks that didn't carry obvious malicious payloads.
- **Zero-day threat detection:** An ongoing struggle to detect novel attacks and fileless malware using a SEG which lacked behavioral analysis.
- **High maintenance burden:** Regular updates, tuning of filtering rules, and false positive management became operationally intensive.

Impact on MSPs

SEGs have and will always be a blessing and a challenge. While they offered a tangible value-add to clients, **managing SEG appliances or hosted instances was labor-intensive**. Constant monitoring, rule updates, quarantines, and end-user support required significant effort for MSPs managing client environments.

2000s and 2010s: *Native Email Security in Microsoft 365 & Google Workspace*

As cloud adoption accelerated in the late 2000s and 2010s, organizations increasingly migrated to **Microsoft 365** (M365) and **Google Workspace** (GWS) for their productivity and email needs. Alongside these platforms came **native email security features**—built-in tools designed to protect users from common threats like spam, viruses, and known phishing scams.

These native defenses—such as **Microsoft Defender for Office 365** and **Google's Gmail security features**—introduced **basic filters** for spam, malware, and malicious links. They also incorporated **reputation-based filtering** and **sandboxing** to scan attachments and URLs before delivery.

With a similar story to the SEG, while effective at stopping high-volume, low-sophistication threats, these tools were not designed to detect more **targeted, subtle, or identity-based attacks**—which became more prevalent throughout the 2010s.

Capabilities of Native Cloud Email Security:

- **Baseline threat protection:** Blocks known spam, viruses, and malicious links using signature-based and reputation-driven filters.

- **Attachment and link scanning:** Sandboxing of suspicious files and analysis of embedded URLs to prevent drive-by malware.

- **Basic phishing detection:** Uses heuristic analysis to flag known phishing tactics, spoofed domains, and impersonation attempts.

Limitations & Threat Gaps:

- **Lacks advanced behavioral analysis:** Native tools typically don't analyze user behavior, communication patterns, or conversation context—leaving blind spots for socially engineered threats.

- **Misses Business Email Compromise (BEC):** Since BEC attacks often don't include malicious payloads, they can slip through native filters undetected.

- **Vulnerable to AI-generated phishing:** Emerging threats that use generative AI or novel attack methods can easily bypass rule-based systems.

- **Frequent target for attackers:** Because M365 and GWS dominate the business productivity market, attackers **design their phishing campaigns specifically to evade these built-in tools.**

- **Misses VIP impersonation threats:** Native tools can't spot context-driven spoofing like fake "CEO" emails with no payloads, letting high-risk attacks slip through.

Impact on MSPs

Native email security presents a double-edged sword:

- **Low barrier, high expectations:** Clients often assume that because M365 or GWS includes security by default, they're fully protected—creating a false sense of security.

- **Pressure to respond post-breach:** When native tools fail to detect a phishing attack or account compromise, your business is often left cleaning up the mess—damaged reputations, credential resets, forensic work, and user training.

- **Opportunity for value-added services:** These limitations create an ideal opening for MSPs to educate clients on the need for layered security—and to upsell more advanced security solutions.

- **Ongoing need for Security Awareness and Training (SAT):** Because native tools don't proactively stop all threats, user education and phishing simulations often fall to the MSP as part of a broader security stack.

2010s & 2020s: *Integrated Cloud Email Security (ICES)*

As cyber threats grew more targeted, adaptive, and socially engineered, traditional SEGs began to fall behind. Attackers no longer relied on obvious malware or spam tactics—instead, they weaponized trust, using impersonation, business email compromise (BEC), and zero-day phishing techniques that easily bypassed static filters.

To counter this shift, a new generation of email security emerged: **Integrated Cloud Email Security (ICES).**

Unlike SEGs, which sit outside the email environment and filter messages before delivery, ICES solutions operate natively within cloud platforms like M365 and GWS. They analyze emails at the moment of delivery and continuously afterward, providing visibility into threats that bypass initial defenses and enabling real-time remediation of malicious or suspicious emails already in users' inboxes.

How ICES Improves Email Security:

- **Inbox-level protection:** Works inside the cloud email environment, not just at the perimeter, offering a second layer of defense after email delivery.
- **AI-driven detection:** Uses natural language processing, behavioral analytics, and threat intelligence to identify impersonation, account compromise, and insider threats.
- **Automated response:** Remediates threats across all user inboxes—removing or flagging malicious emails—without waiting on manual IT intervention.
- **Continuous learning:** Incorporates feedback either through human influence or evolutionary AI models that learn and recognize new attacker behavior and emerging threats.

Impact on MSPs

ICES solutions represent both a **relief** and an **opportunity** for MSPs struggling to find the appropriate email security solution.

- **Reduced Operational Overhead:** ICES solutions dramatically cut down or eliminate manual rule creation, policy tuning, and false positive investigations—freeing up valuable resources for business-critical tasks.
- **Proactive Threat Mitigation:** Instead of waiting for end users to report suspicious emails (or worse, fall for them), MSPs can now automate post-delivery remediation, improving response times and minimizing damage.
- **Stronger Differentiation:** Offering advanced, AI-powered ICES protection positions MSPs as forward-thinking security partners—not just IT support vendors. It's a clear value-add in a crowded market.
- **Scalability for Modern Workplaces:** With more clients moving to M365 and GWS, ICES integrates seamlessly into their cloud stack—no hardware, no gateways, and no disruption to email flow.

Chapter 2: IRONSCALES 2025 Study

The Hidden Gaps in SEG Protection

IRONSCALES analyzed email traffic across nearly 2000 customer environments who were utilizing a SEG as well as IRONSCALES email security solution for email protection. We did this with the sole intention of measuring the effectiveness of SEGs against modern threats. First, we'll discuss the details of this analysis and then I'll explain the insights we gleaned from the data.

Parameters:

- **Customer Environments Evaluated:** 1,921
- **Average Organization Size:** 548 mailboxes
- **Duration of Study:** 30 days of real-world email traffic (no lab tests)

Results:

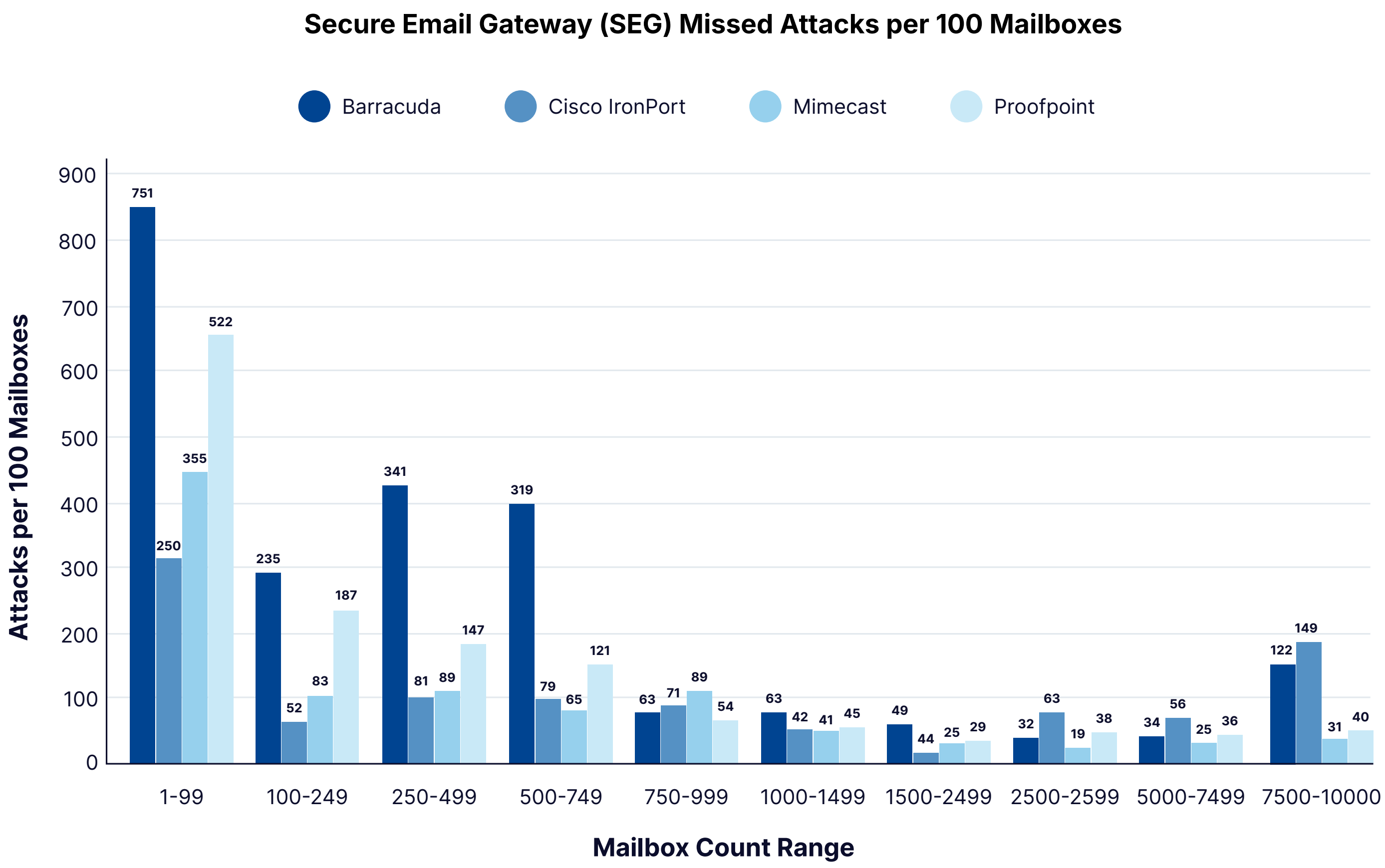
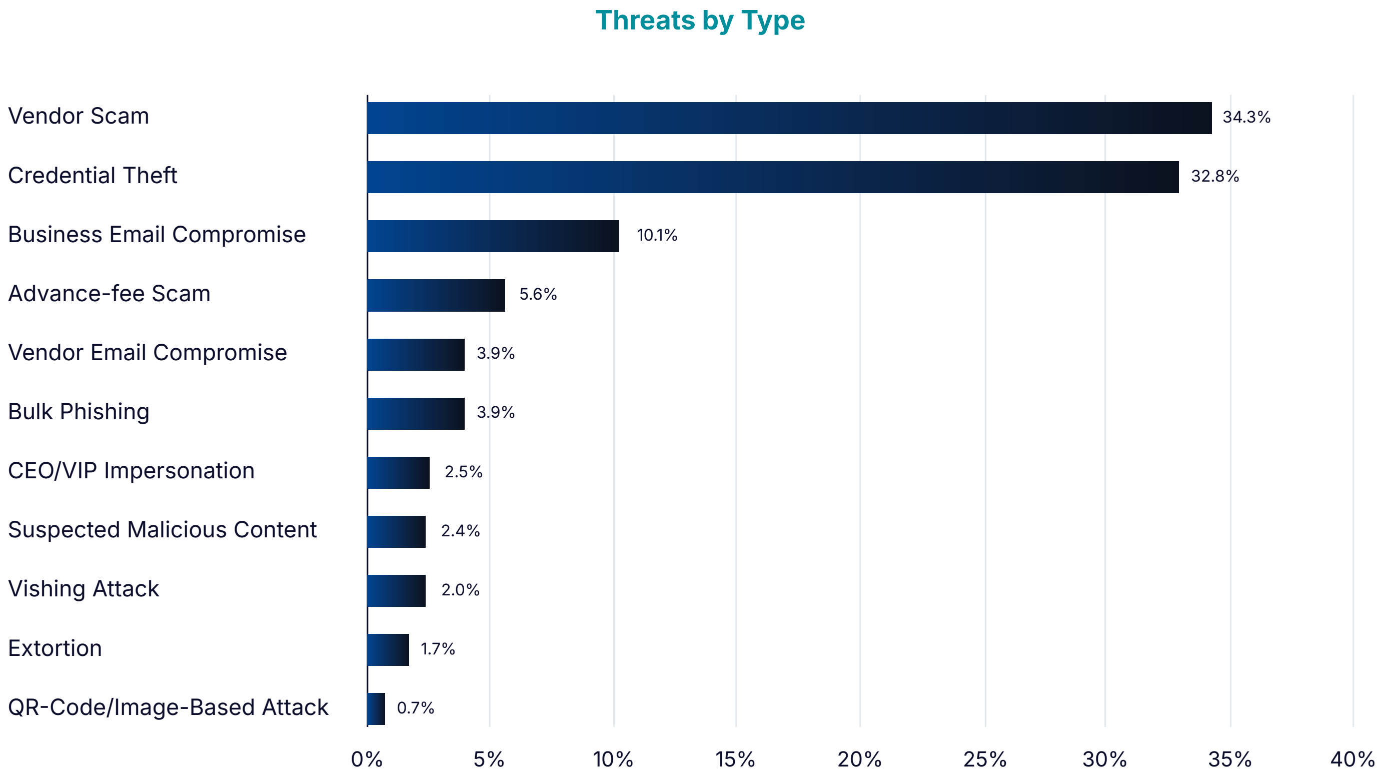


Figure 1: SEG missed attacks per 100 mailboxes across different organization sizes

Refined by Threat Type



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%

Additional information around the types of attacks each of these SEG vendors experienced and the full IRONSCALES study is referenced within the work cited and appendix at the end of this white paper.

Key Findings

On average: **67.5 phishing emails** bypass SEGs per **100 mailboxes every month.**

- **Small businesses appear to be most at risk,** with up to **7.5x more missed attacks** than large enterprises.
- At 30-42%, **Vendor scams** represent the most frequent category of missed attack across all SEG providers.
- At 21-41%, **Credential theft** is the second most commonly missed attack type.
- Missed Attacks by SEG provider (over 30 days):
    - **Barracuda:** Missed an average of *101 attacks per 100 mailboxes.*
    - **Proofpoint:** Missed an average of *68.4 attacks per 100 mailboxes.*
    - **Cisco IronPort:** Missed an average of *51.6 attacks per 100 mailboxes.*
    - **Mimecast:** Missed an average of *38.4 attacks per 100 mailboxes.*

Summary

Our analysis of these four leading SEG providers reveals a hard truth MSPs can't afford to ignore: **the SEGs many MSPs are still relying on are consistently failing to detect real phishing attacks that land in client inboxes.** Barracuda missed the most, but even the "better performers" like Mimecast still let through dozens of phishing emails per 100 mailboxes each month. When we look at the types of attacks that are most prevalent—Vendor Scam and Credential Theft—it starts to paint a clear picture. SEGs are built for static detection, not dynamic, real-world deception tactics which today's attackers have evolved to weaponize at scale.

This isn't just a security gap for your business—it's a service delivery risk, a client trust issue, and an operational bottleneck that turns into lost time, lost profit, and in worst-case scenarios, lost customers.

Chapter 3: The Business Impact for MSPs and Their Clients

Why SEGs Are Holding MSPs Back

If you rely on a SEG to protect your clients, you're exposing your business to operational, financial, and reputational risk. Traditional SEGs create challenges in scalability, client trust, financial liability, and market competitiveness.

According to the 2024 Verizon Data Breach Investigation Report, almost 100% of socially engineered phishing attacks took place using email as their initial attack vector of choice.[4] Threat actors are not wasting time with other mediums and are prioritizing email for their most sophisticated attacks. The following is a list of what's at stake if a phishing email slips through your SEG:

1. **Growth & Profitability Constraints**
   You need efficiency to scale, but SEGs introduce hidden operational burdens. Constant rule updates and policy tuning bog down internal resources, increasing operational overhead and diverting valuable IT resources from growth initiatives. Without AI in email security, you will find it increasingly difficult to scale effectively, as security incidents demand more hands-on management, preventing your business from expanding without adding significant costs.

2. **Reputation & Trust Erosion**
   You are in business because you are a trusted partner in cybersecurity, but that trust is fragile—one phishing failure can permanently damage a provider's credibility. Clients expect you to keep them secure, and if your SEG fails, the responsibility falls directly on your organization. A reactive approach—waiting for a breach before upgrading defenses—signals negligence, making clients question whether you're truly staying ahead of evolving threats.

3. **Financial Culpability Risks**
   When security failures occur, your business does not just lose trust—it can also face direct financial consequences. Legal liability from breaches can result in costly lawsuits and client compensation claims, putting you at risk. Additionally, recurring security incidents drive up cyber insurance premiums, cutting into margins and making it more expensive to operate.

4. **Competition & Client Retention Challenges**
   In a 2024 MSP Benchmark Survey Report by Kaseya, 36% of the almost 1000 security experts surveyed highlighted acquiring new customers as their top concern.[2] Maintaining a competitive advantage has never been more important. If you fail to evolve your security stack, or stay in a technology relationship longer than you should, you risk falling behind competitors offering superior protection.

The Hidden Risks of Relying on a SEG for Clients

SEGs have long been the default choice for email security, but modern phishing tactics are exposing their hidden vulnerabilities. When these legacy defenses fail, clients face significant risks in multiple areas—business continuity, compliance, relationships, and financial impact. Here's how SEG shortcomings put your clients at risk:

1. **Business Continuity Disruptions**
   If your client's environment is compromised from a missed phish, everything stops including operations, partnerships, and their growth. SEGs operate on static rule-based filtering, meaning advanced phishing techniques, such as AI-generated attacks and vendor impersonations, often slip through. With an average of 67.5 phishing emails bypassing SEGs per 100 mailboxes each month, most of which are sophisticated attacks, your clients are more at risk for business disruption when you use a SEG.

2. **Compliance & Cyber Insurance Challenges**
   Many industries require businesses to maintain strict compliance with data protection regulations or cyber insurance policies. When SEGs fail to catch phishing threats, organizations become vulnerable to regulatory fines, lawsuits, and policy exclusions from cyber insurers. Weak defenses can also lead to increased premiums or outright denial of coverage.

3. **Damaged Business Relationships**
   Trust is everything in business. A single phishing incident—especially one that results in business email compromise (BEC) or vendor fraud—can erode relationships with customers, partners, and employees. SEGs are particularly weak against socially engineered attacks, which often involve impersonation of trusted contacts. **Vendor scams were the #1 missed attack type that SEGs fail to stop in our study**, creating a direct risk to business credibility.

4. **Financial Fallout from Cyberattacks**
   The average cost of a data breach has now surpassed $4.88 million,[1] with phishing being one of the leading attack vectors. Ransomware incidents, fraudulent transactions, and legal proceedings stemming from email attacks all compound the financial burden. One missed attack—especially for an SMB—can lead to the end of your client's business.

Chapter 4: The Future of Email Security: AI and Beyond

The shift from traditional SEGs to ICES marks a turning point in email security. With cybercriminals leveraging AI to craft more convincing phishing campaigns, AI is no longer optional for security teams, it's now fundamental to stay ahead of today's attackers. The combination of **behavioral detection, automated remediation, and adaptive learning** is the key providing today's MSP owners and their clients with an effective and proven protection against the next generation of email threats.

$2.22M

The average cost savings in millions for organizations that used security AI and automation extensively in prevention versus those that didn't.[1]

Legacy SEGs were built to filter spam and known threats—not to counter today's reality of sophisticated, socially engineered phishing attacks. Our latest analysis confirms this through the data: virtually all of the missed attacks were persuasive, socially engineered phishing attempts—credential theft, vendor scams, BEC attacks, and more—that lacked traditional indicators like malicious links or attachments. Today's email-based threats require a different approach: detection and response directly inside the inbox. By integrating natively with Microsoft 365 and Google Workspace via API (no MX record changes required), our platform sees what others miss and remediates threats in real time—often before users even realize there was a risk.

What sets IRONSCALES apart is our use of Adaptive AI, dynamic social graphing, and feedback from a global community of over 25,000 security analysts. Our platform builds a behavioral baseline for every mailbox, analyzing tone, communication patterns, and sender intent to detect impersonation and deception-based threats that SEGs simply can't catch. This approach not only blocks advanced phishing attacks, but also dramatically reduces remediation time—from minutes to seconds.

As you continue to modernize your email security strategy, the question is no longer *if* AI-driven email security is needed—but *when* it will be time to fully embrace it.

Chapter 5: A Step-by-Step Guide to Breaking Up with Your SEG

Breaking up is hard to do—especially when it's with the security solution you've relied on for years. AI is no longer optional for security teams, it's now fundamental to stay ahead of today's attackers. It's time to upgrade your email security.

Whether you're a team of five or fifty, migrating away from a SEG shouldn't be a blind leap—it's a calculated move toward something that works *with* your team, not against them.

Before you initiate the breakup, here are the strategic questions MSPs should ask themselves to ensure a clean, smart, and future-ready transition:

Business Category	MSP Questions	IRONSCALES Insights
Business Size + Client Type	• How many mailboxes do you manage? • Do you serve SMB, Mid-Market, or Enterprise clients?	The scale of your operations will dictate your approach. A larger MSP may require a phased migration, while a smaller MSP can transition more quickly.
Industry Verticals + Compliance	• Are your clients in regulated industries (Healthcare, Financial Services, Legal, Manufacturing)? • Do you need to meet specific compliance concerns (HIPAA, GDPR, PCI DSS)?	Not all ICES solutions are built to handle industry-specific compliance mandates—choose one that aligns with your needs.
Integration Capability	• What security tools and platforms are already in place? • Can the new solution integrate with your PSA, RMM, SIEM, or MDR tools?	A seamless transition requires an ICES that enhances your current security infrastructure rather than complicating it.
Internal Readiness + Technical Expertise	• Does your team have the necessary expertise to manage a new security platform? • Will you need additional training or onboarding support?	A well-prepared internal team will ensure a smoother adoption process.
Client Communication + Education	• How will you introduce this transition to your clients? • Will there be training sessions, FAQs, or direct support available for customers?	Keeping clients informed and involved reduces friction and builds trust.

Business Category	MSP Questions	IRONSCALES Insights
Financial and Operational Considerations	• What is the long-term cost of staying with your SEG versus transitioning to ICES? ◦ Consider the reduction in manual remediation, phishing-related incidents, and operational costs.	MSPs must weigh the total cost of ownership, including licensing, maintenance, and staffing resources.
Success Metrics + Post-Migration Monitoring	• How will you measure the effectiveness of the transition? • Key benchmarks should include: ◦ Phishing detection improvements ◦ Reduction in incident response times ◦ Client satisfaction and feedback ◦ Overall security posture enhancement	Set clear KPIs and continuously assess performance to ensure the switch is delivering expected results.

ICES at IRONSCALES

What sets us apart in the crowded ICES market is our approach to detection: **Adaptive AI + Human Insights (HI)** working in tandem, not isolation. While many vendors boast automation, IRONSCALES goes further—pairing AI that learns from behavioral patterns across inboxes with real-time feedback from a community of over 15,000 organizations.

Our AI constructs individualized social graphs per mailbox, spotting anomalies others miss, while our human-in-the-loop (HITL) model ensures rapid tuning against zero-day and socially engineered threats. But intelligence isn't enough without control.

That's why we give our MSP partners centralized, multi-tenant visibility and granular policy control across every client tenant—without relying on complex MX record changes or disruptive reconfigurations. This means faster deployment, better protection, and less operational drag.

Why Thousands of Global MSPs Choose IRONSCALES

- **More Profit, Less Phish:** No quotas, no minimums, and no long-term commitments so you can grow on your terms.
- **Operational Efficiency:** AI-driven email security, multi-tenant management, and rapid time-to-value (TTV) to reduce internal workload and scale faster.
- **Sales & Enablement Support:** Tailored marketing, sales training, and onboarding resources built specifically for MSPs.
- **Feedback-Driven Innovation:** We prioritize input from every MSP partner. Your voice shapes our product for the better.

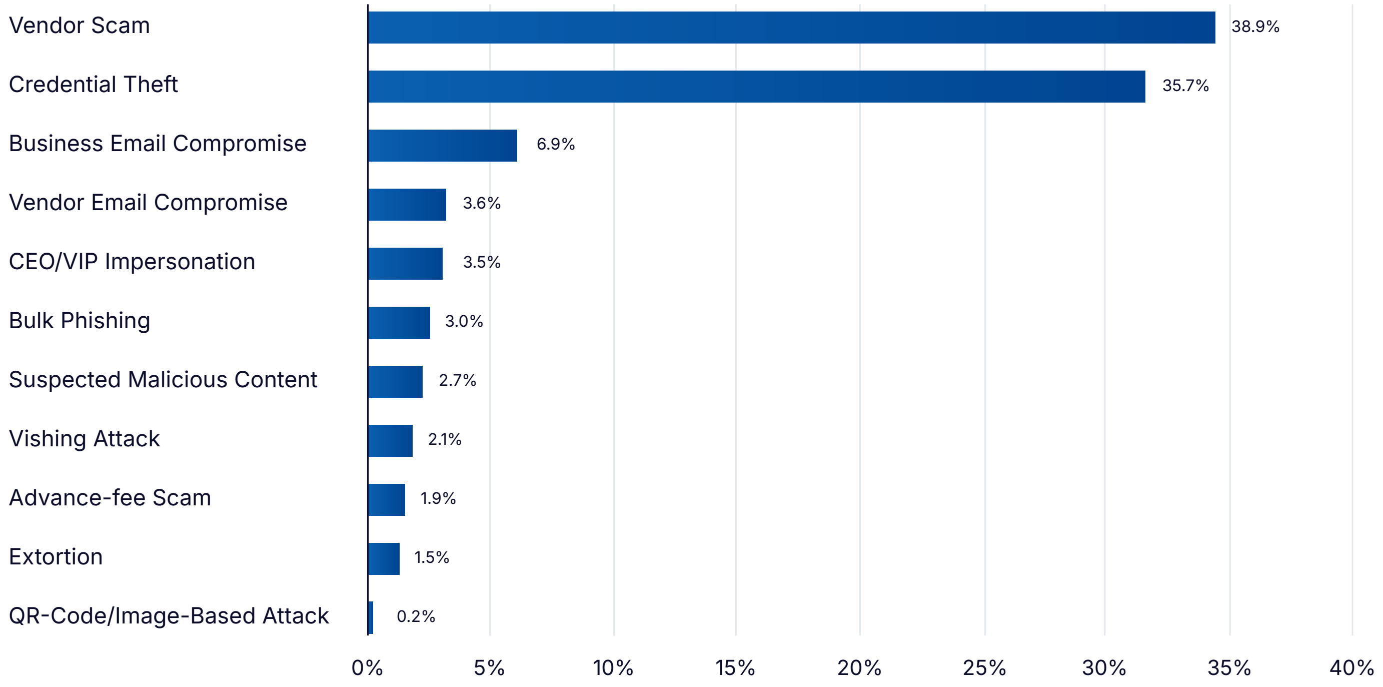
Conclusion

MSPs can no longer afford to rely on outdated, static security measures. Attackers are leveraging AI, automation, and multi-channel deception tactics that render SEGs ineffective. The longer an MSP waits to transition, the more risk they introduce to their clients and their own business.

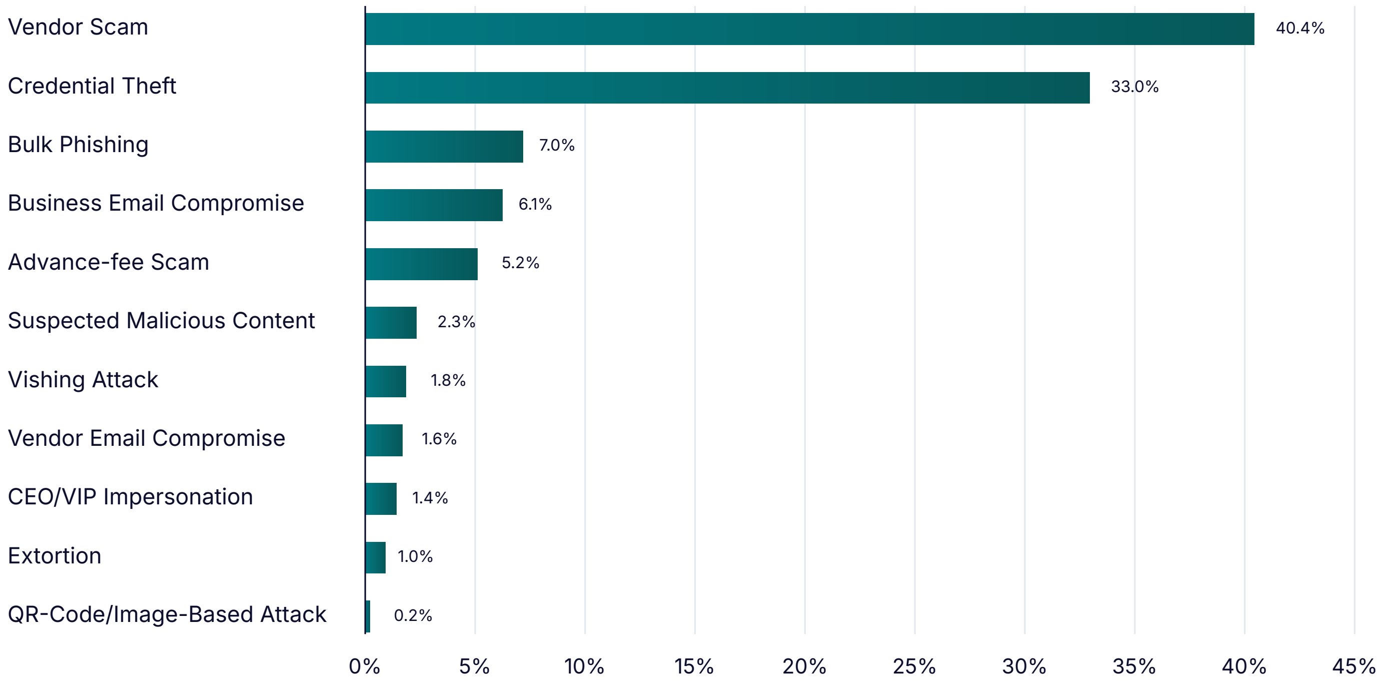
Ditching your SEG isn't just a security upgrade, it's your chance to lead and grow. MSPs that make the move unlock new revenue streams, boost profitability, and deliver stronger protection their clients actually notice. **It's time to break up with your SEG.**

Appendix

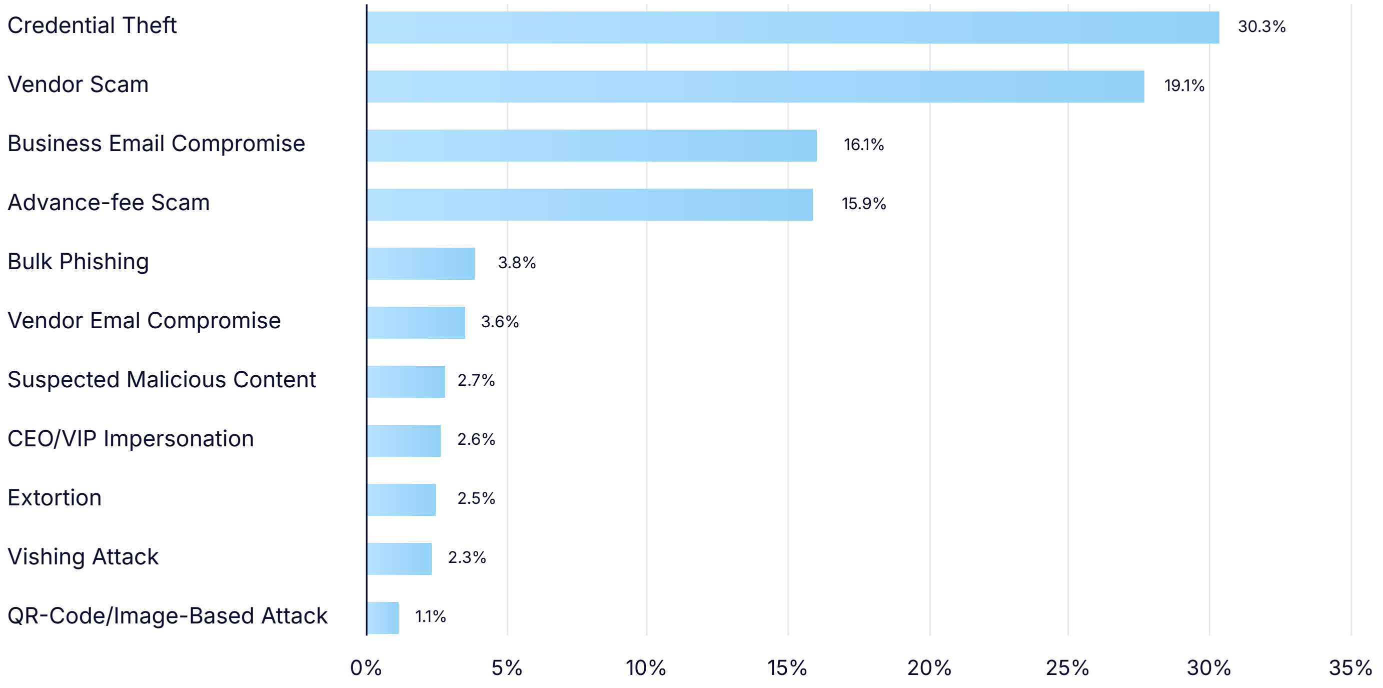
Barracuda - Misses 101 Attacks



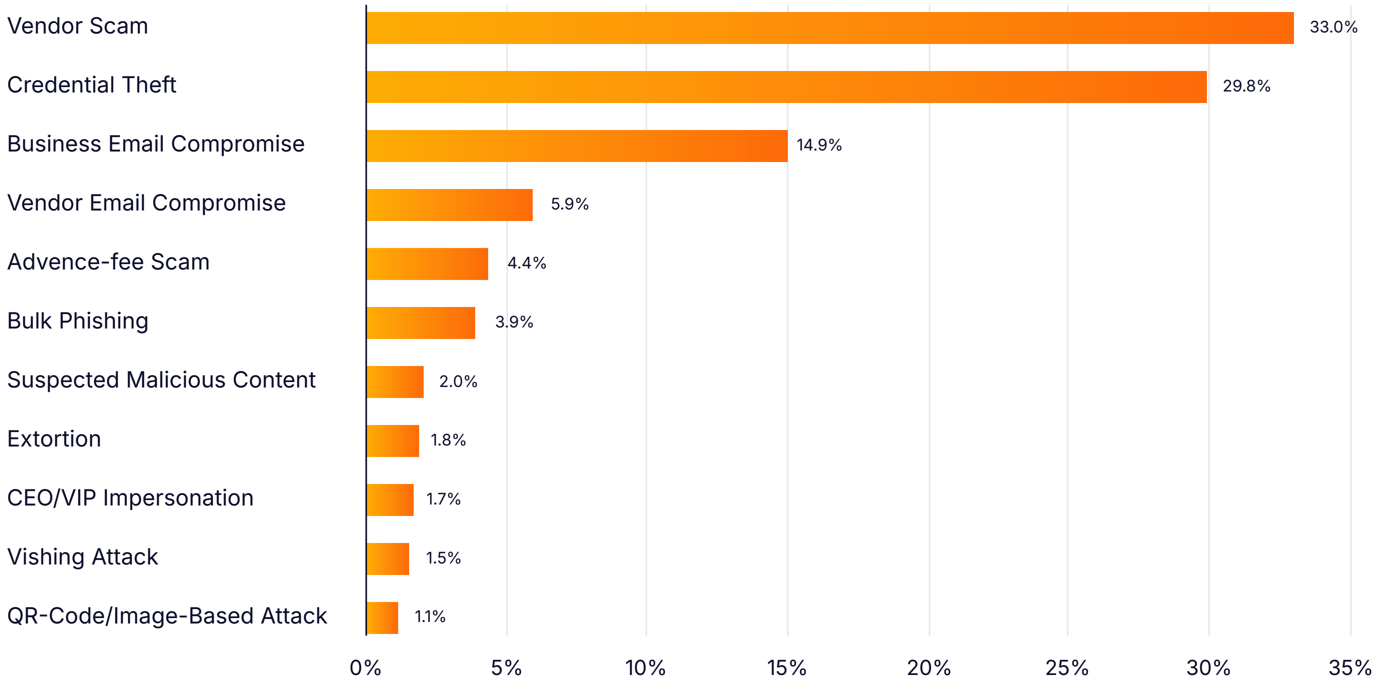
Cisco - Misses 51.6 Attacks



Mimecast - Misses 38.4 Attacks



Proofpoint - Misses 68.4 Attacks



Works Cited

1. IBM. *Cost of a Data Breach 2024 Survey*. IBM, 2024, https://www.ibm.com/reports/data-breach.
2. Kaseya. *2024 MSP Benchmark Survey Report*. Kaseya, 2024, https://www.kaseya.com/wp-content/uploads/dlm_uploads/2024/03/Whitepaper-2024-MSP-Benchmark-Survey_Kaseya.pdf.
3. Moore, Gordon. *Moore's Law*. University of Texas, https://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf.
4. Verizon. *2024 Data Breach Investigations Report (DBIR)*. Verizon, 2024, https://www.verizon.com/business/resources/reports/dbir/.
5. IRONSCALES, The Hidden Gaps in SEG Protection White Paper. IRONSCALES, 2025, https://secure.ironscales.com/hidden-gaps-in-seg-protection-white-paper

Secure Your Inboxes. **Unburden** Your Team. **Empower** Your People.

The IRONSCALES™ platform is the leading cloud email security solution for the enterprise and the industry's only solution that uses adaptive AI and human insights (HI) to stop advanced phishing. Its award-winning, self-learning platform continuously detects and remediates attacks like BEC, ATO, and VIP impersonation that bypass traditional security solutions. Powerful, simple, and adaptive, IRONSCALES helps enterprises protect better, simplify operations, and empower the organization. IRONSCALES is headquartered in Atlanta, Georgia, and is proud to support more than 15,000 global enterprises. To learn more, visit www.ironscales.com or follow us on X @IRONSCALES.

IRONSCALES

IRONSCALES.COM