White Paper

Your SEG Won’t Save You

Moving Email Security to Inside the Mailbox

IRONSCALES
SAFER TOGRTHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Contents

Advanced email phishing attacks remains the most problematic cyber security issue that companies face today. An estimated 90% of successful cyberattacks can be traced back to a phishing email. Global losses from business email compromise (BEC) attacks cost organizations billions of dollars every year. And because cyber criminals are enjoying so much success, these attacks aren't going away any time soon. If anything, the pace of attacks will continue to accelerate. As a result, security teams are overwhelmed, and employees are stressed out because they don't want to be the one who falls for the next phishing attack.

In an era of sophisticated and targeted attacks, each phishing attack affects multiple mailboxes across multiple organizations and requires managing an array of defensive tools to quickly detect and remediate phishing attacks. For this to become reality, CISOs and other information security managers must implement a multi-pronged approach including proven, post-delivery capabilities to bolster their defenses. In today's complex threat landscape, secure email gateways (SEGs) no longer sufficient protection against modern types of phishing attacks and must be reinforced from inside the mailbox. Just as no security professional would ever suggest a firewall alone is enough to protect enterprise infrastructure, simply having a SEG in place is likewise insufficient to defend against advanced phishing attacks.

The rise and fall of the SEG

When SEGs first emerged and bad actors were less technically savvy, this technology provided an adequate layer of protection to block basic email phishing threats and spam. Not so today. Sophisticated attackers have created targeted phishing and BEC techniques that bypass SEGs with ease. The modern bad actor can easily assess which SEG an organization uses and find ways to slip through basic spam filters or even bypass the perimeter entirely. Once these dangerous threats have landed in user mailboxes, they are well beyond the reach of the SEG and its basic scanners and spam filters.

That's not to say the SEG has no role in today's complex threat landscape. On the contrary, the SEG remains a critical, legacy workhorse focused on stopping spam and malicious attachments. However, protecting the perimeter – even with enhanced cloud prefiltering and modest anti-phishing capabilities – is no longer sufficient. Organizations must complement their SEGs with another layer of endpoint protection – and this one needs to operate from inside the mailbox itself.

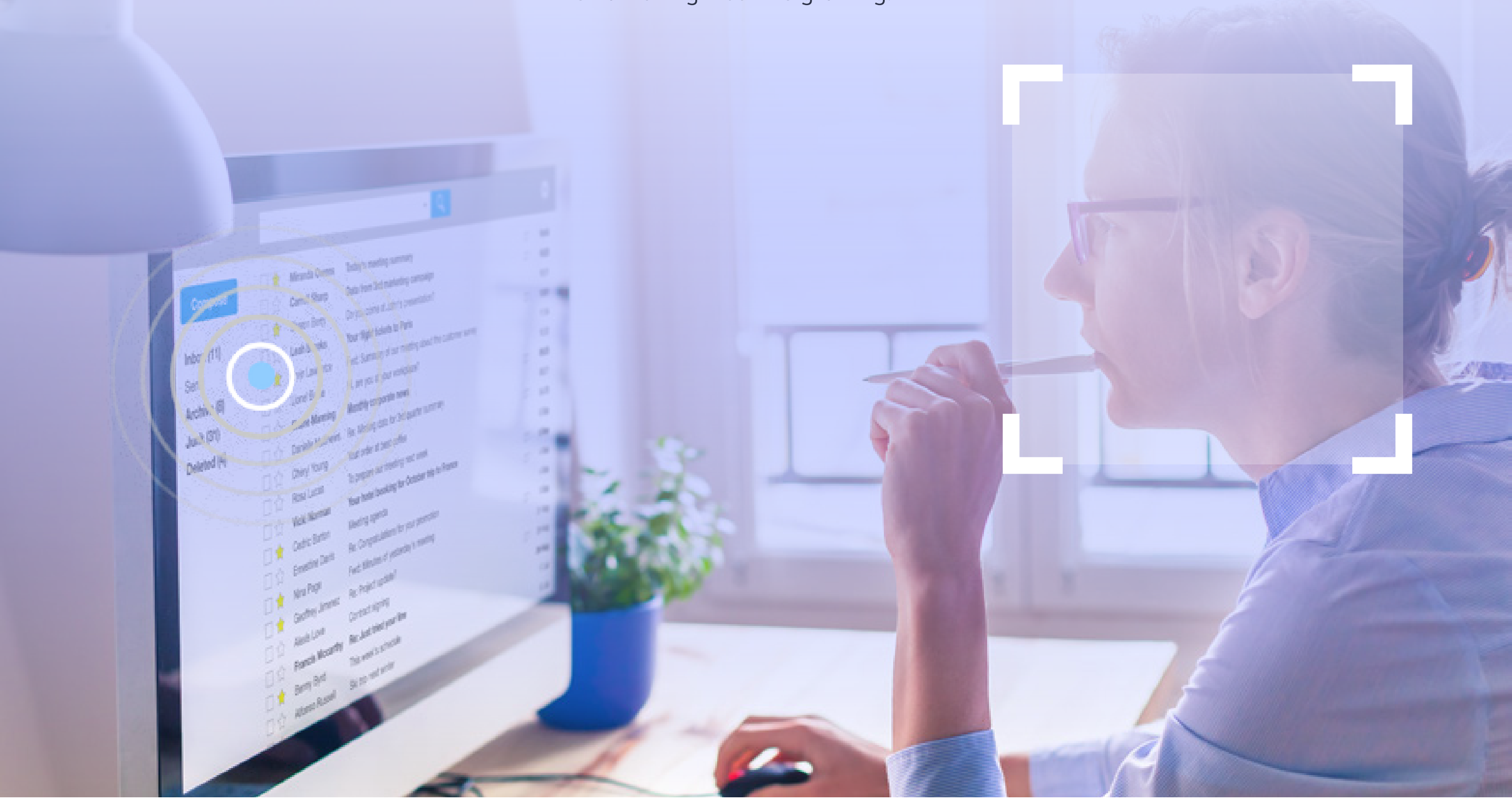
90%

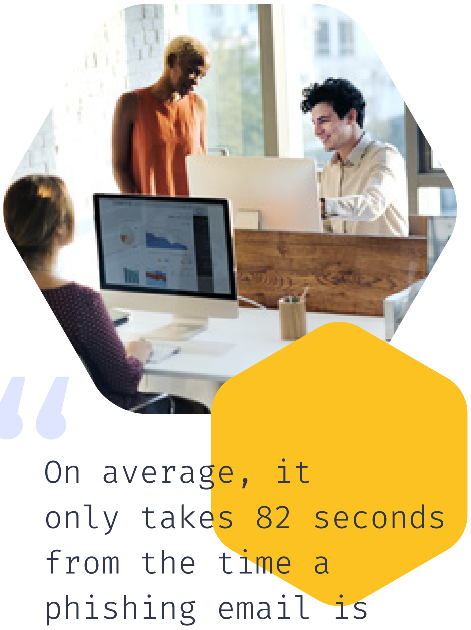
of successful cyberattacks can be traced back to a phishing email.

Bypassing the SEG

Threat actors are constantly developing new, inventive methods – from social engineering and identity deception to BEC – to trick their targets, compromise accounts, and steal valuable credentials. For example, attackers may use different file extension names to bypass SEG attachment controls and deliver their payloads. SEGs only see what they know: e.g., known signatures, malicious attachments, and web links. With 40% of all attacks containing unknown elements, it's not surprising that many targeted phishing and BEC attacks still pass through SEG defenses should concern every information security professional.

At the same time, those vendor-provided signatures mentioned above typically lag the actual threats, providing an ineffective defense against phishing email attacks. Outdated signatures from SEGs aren't created in real time and can take up to 250 days from the time a phishing email attack is first reported to the time a signature is made available to enterprise technical staff – assuming it receives a high enough priority by the vendor to warrant a signature. Furthermore, the trend toward sophisticated, polymorphic phishing email attacks makes traditional signature-based approaches only marginally useful. Plus, many SEGs don't scan every URL. Instead, they focus only on the type of URLs people click. But with more phishing attacks using single-use URLs, the risk of falling victim is growing.





“

On average, it only takes 82 seconds from the time a phishing email is first distributed until it successfully lures its first victim.

A race against time

Inundated with the time-consuming tasks of manually responding to phishing attacks and attempting to mitigate those risks in the first place, security teams are drowning. They're also fighting a losing battle – attempting to respond faster than end users can click on a malicious link. On average, it only takes 82 seconds from the time a phishing email is first distributed until it successfully lures its first victim.[1] When cyber risks are multiplying unabated, SOC teams can't afford to waste a minute.

No solution will ever stop 100% of attacks. The realistic challenge then becomes how to respond to a phishing incident once emails land in the mailbox.

The days of manual search-and-delete incident response are over. Enterprises need automated, post-delivery detection and response capabilities to address threats their email gateways missed. Automated anti-phishing solutions powered by machine intelligence can analyze messages at the mailbox level and provide one-click remediation of a phishing attack across the organization. As a result, security teams can reduce the time from discovery to remediation from days or weeks to a matter of minutes or even seconds.

Even standards-based protocols lack sufficient protection

In a perfect world, standards-based protocols like Domain-based Message Authentication, Reporting, and Conformance (DMARC) would provide adequate protection against phishing attacks based on domain-name spoofing. Unfortunately, we don't live in a perfect world. DMARC requires both senders and receivers to be compliant, and that's not always the case. Moreover, many phishing attacks that slip past native email gateways don't involve exact domain name spoofing but instead use techniques such as domain lookalikes – and DMARC doesn't protect against impersonation attacks like these.

In a recent analysis of more than 100,000 email phishing attacks that successfully evaded SEGs, less than 1% were based on exact domain name spoofing.[2] It's worth noting that exact domain name spoofing represents only one of the many easily implemented weapons for email phishing attacks in the attacker's arsenal.

SOURCES

[1] Verizon, 2018 Data Breach Investigations Report

[2] IRONSCALES research

The future is autonomous

In a world where incoming threats are growing exponentially, no company can ever deploy enough security analysts to cover the increasing workload. Analysts predict that by 2022, 30% of security operations playbooks will be fully automated, up from just 10% in 2019.Thus, autonomous decision-making and email-threat defense are inevitable. Through real-time external sharing and querying, an autonomous security ecosystem would enable an anti-phishing platform to probe endpoint security, tracing the path and current location of incoming threats. Likewise, such a platform could automatically move to block a suspicious threat, such as a fraudulent URL, at the gateway, based on user reports.

As companies of all sizes move to cloud-based email and as cyber criminals continuously refine their methods and begin using artificial intelligence and machine learning (AI/ML), a new approach to securing against phishing attacks is needed. This new approach requires email security solutions that are fast to implement, easy to manage, and rely on a combination of AI/ML and end user training to defend against the higher quantity and advanced quality of phishing attacks. Perimeter-level security will no longer be enough to protect the enterprise from phishing attacks. SEGs simply won't be able to stop sophisticated, targeted attacks before they slip through controls and into end users' mailboxes. The time has come to reinforce or even replace SEGs with mailbox-level protection.

About IRONSCALES

Not All Email Security Solutions are Equal

Defending against today's advanced threats requires a new approach to email security. IRONSCALES' best-in-class email security platform is powered by AI, enhanced by thousands of customer security teams and is built to detect and remove threats in the inbox. We offer a service that is fast to deploy, easy to operate and is unparalleled in the ability to stop all types of email threats, including advanced attacks like BEC, ATO and more.

To learn more about IRONSCALES' award-winning anti-phishing solution, please sign up for a demo today at **https://srccybersolutions.com/contact-us**

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks and launched globally. Legacy technologies like secure email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

www.srccybersolutions.com
+91 120 232 0960 / 1
sales@srccybersolutions.com