

A monochromatic blue-tinted photograph of a cowboy on a horse, seen from behind, herding a large group of horses across a grassy field. The sky is filled with large, fluffy clouds. A small dog is visible in the lower right corner of the herd.

The Good. The Bad. And the Ugly of Email Security.

Why You Need Mailbox-Level Protection



IRONSCALES

IF you've spent any time at all in the cybersecurity world, you know firsthand that Warren Buffett isn't just blowing smoke about the dangers of cyber threats when he's said,

“Cyberattacks are “the number one problem faced by mankind.”

You see the obvious signs all around – from the blaring headlines about the latest security threats to the staggering volumes of attempted phishing attacks faced by your security team every day.

And the problem isn't getting any better.



IRONSCALES



An estimated **9** out of every **10** successful cyberattacks can be traced back to a phishing email(s).

Global losses from business email compromise (BEC) attacks have cost organizations more than **\$26 billion since 2016.**

More than **40% of phishing** email attacks are polymorphic – meaning they undergo at least one permutation designed to evade traditional email security controls.

The average cost of a data breach for global enterprises reached nearly **\$4 million.**

In an era of sophisticated and targeted attacks

every phishing email attack affects multiple mailboxes at multiple organizations and requires hundreds of successful detections by the email security capabilities of enterprise defenders.

CISOs and other information security managers need to implement a multi-pronged approach that includes a proven, post-delivery capabilities to bolster their defenses against these threats. Secure email gateways (SEGs) are no longer sufficient protection against today's challenging threat landscape and must be reinforced with endpoint protection inside the mailbox.

Protecting the gateway isn't enough. Nobody would suggest that just because you have a firewall, you don't need endpoint anti-virus protection. Likewise, just because you have a SEG in place doesn't mean you don't need email security protection inside the mailbox.

Whether deployed as a cloud or a hosted, on-premise solution, SEGs emerged to provide native capabilities, including:



Anti-spam and Anti-virus filters



Anti-malware blocking for attachments, including sandboxing with dynamic analysis of executable and non-executable files provided by the vendor or through integration.



Content filtering and Basic anti-phishing filters



URL inspection on receipt of a message and at time of click



Data protection through DLP and encryption



IRONSCALES



Back in the early days when SEGs emerged, bad actors were less technically savvy and SEGs provided an adequate layer to block basic email phishing threats and spam.

Not so today. Sophisticated attackers have created new targeted phishing and business email compromise (BEC) techniques that bypass SEGs. The modern bad actor can easily see which SEG an organization uses and find ways to slip through basic spam filters or bypass the perimeter entirely.

And 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. So, if you're looking to modernize and strengthen your email security posture, a SEG alone won't protect your enterprise from today's advanced phishing attacks.



IRONSCALES

In today's complex threat landscape


the SEG continues to play an important role as a legacy workhorse. However, protecting the perimeter – even with enhanced cloud prefiltering and modest anti-phishing capabilities – is no longer sufficient. You must complement your SEG with another layer of endpoint protection inside the mailbox itself

Sophisticated attacks are bypassing traditional SEGs. Strengthen your email security with mailbox-level email security that provides protection from the inside out.

SEGs will never stop all phishing emails. Need proof? A recent study found that SEGs miss 99.5% of all non-trivial email spoofing attacks and that results in attacks landing in users' email inboxes. We think that statistic should concern every information security professional.

Threat actors are constantly coming up with new, inventive methods – from social engineering and identity deception to BEC – to trick their targets, compromise accounts and steal valuable credentials. For example, attackers use different file extension names to bypass SEG attachment controls and deliver their payloads.

SEGs only see what they know: 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 SEGs' defenses.



99.5% of all non-trivial email spoofing attacks bypass secure email gateways (SEGs) and land in users' mailboxes.

At the same time, these vendor-provided signatures typically lag behind the actual threats, providing an ineffective defense against phishing email attacks. Outdated signatures from SEGs aren't created in real-time and can often take up to 250 days from the time a phishing email attack was first reported, to the time a signature was made available to enterprise technical staff, assuming it receives a high enough priority by the vendor to warrant a signature. In addition, the trend towards 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 actually click. But with more phishing attacks using single-use URLs, the risk is growing. Cybercriminals only need one set of legitimate credentials to break into a network type of URLs people actually click. But with more phishing attacks using single-use URLs, the risk is growing.



IRONSCALES

SEGs have very limited post-email delivery detection

Security teams are inundated with time-consuming tasks of manually responding to phishing attacks and mitigating these risks. They're fighting what often seems like a losing battle to respond faster than it takes users to click on a malicious link.

At a time when cyber risks are growing, SOC teams can't afford to waste a minute. On average, it only takes 82 seconds from the time a phishing email is first distributed until it successfully lures its first victim. No solution is ever going to be capable of stopping 100% of attacks. The challenge becomes how to respond to a phishing incident once emails land in the mailbox. The old days of manual search-and-delete incident response are over.

Enterprises need automated, post-delivery detection and response capabilities to address threats that weren't caught by their email gateways.

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.

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



IRONSCALES

Standard-Based Protocols Aren't Enough to Protect You Against All

In a perfect world, standards-based protocols like Domain-based Message Authentication, Reporting, and Conformance (DMARC) would provide the adequate protection you need against phishing email 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. Besides, many phishing attacks that slip past native email gateways actually don't involve exact domain name spoofing but use techniques such as domain lookalikes. DMARC doesn't protect against these kinds of impersonation attacks.

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. 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..

Less than 1% of email phishing attacks that bypassed SEGs were based on email domain name spoofing.






Today's complex threat landscape demands a multi-pronged email security strategy

Most security teams today rely too much on technical controls like SEGs, but they are doomed to fail if they don't factor users and security analysts in the equation. The world of cybersecurity technology is extremely fragmented with tools for awareness, SEGs, spam filters, anti-malware and incident response operating in separate silos. Attacks are exploiting this weakness, resulting in major threats slipping through the cracks.

To close the gaps, enterprises need to adopt Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA) architecture and implement a unified platform that supports threat prediction, prevention, detection and incident response.

A person wearing a dark cowboy hat and a dark jacket is silhouetted against a bright background of a mountain range. The person is looking out over the landscape. The mountains are covered in green trees and have some rocky peaks. The sky is blue with some white clouds.

The future is autonomous

IN a world where incoming threats are growing exponentially, no enterprise can ever deploy enough security analysts to cover the increasing workload. By 2022, Gartner predicted that 30% of security operational 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 to trace the path and current location of incoming threats. Likewise, a platform could automatically move to block a suspicious threat, such as a fraudulent URL, at the gateway based on multiple user reports.



IRONSCALES

A holistic email security platform

Modern email security requires a comprehensive platform built on a CARTA strategy combining advanced technologies, human intelligence, and user behavior. An integrated mailbox-level email security platform based on CARTA provides end users and security professionals with the right training, tools, threat intelligence and one-click resolution to strengthen your email security posture and hunt, log, alert, analyze and remediate phishing attacks.

Look for a modern email security solution with one-click resolution and the ability to hunt, log, alert, analyze and remediate phishing attacks, including:



Protection against advanced malware, credential theft, phishing websites, Impersonation, social engineering and payload-less advanced threats.



Gamified, personalized awareness and training to simulate attacks to help employees identify and report attacks.



AI-powered incident response and remediation for phishing emails that have landed inside the inbox inside the inbox.



Better security team collaboration with real-time actionable threat intelligence and detection.



A virtual AI-powered security analyst to speed decision making with automated thresholds, analysis, threat mitigation and remediation.



IRONSCALES

Perimeter-level security isn't enough to protect your enterprise from phishing attacks. SEGs simply aren't capable of stopping sophisticated, targeted attacks before they slip through these controls and into end users' mailboxes. Reinforce your perimeter email security with mailbox-level protection.

Contact us today to schedule a demo at www.iron scales.com/demo.



IRONSCALES

About IRONSCALES

IRONSCALES is the leader in email security and anti-phishing technologies. Using a multi-layered and automated approach starting at the mailbox-level to prevent, detect and respond to today's sophisticated email phishing attacks, IRONSCALES expedites the time from phishing attack discovery to enterprisewide remediation, reducing the time from detection to response from hours or days to just seconds or minutes, by significantly reducing the workload on incident responders.

Headquartered in Tel Aviv, Israel, IRONSCALES was founded by a team of security researchers, IT and penetration testing experts, as well as specialists in the field of effective interactive training, in response to the phishing epidemic that today costs companies millions of dollars annually. It was incubated at the 8200 EISP, the top program for cybersecurity ventures.