



# Traditional Email Security is NOT Enough.

How to build a layered defense to combat advanced phishing threats.

**COFENSE.COM**

© Cofense 2022. All rights reserved



# The Problem

## Over 50% of phishing emails bypass existing email security EVERY month.

Every hour of every day, phishing emails are evading traditional email security controls like secure email gateways (SEGs) as well as native capabilities offered from email providers.

In 2021, The Cofense Phishing Defense Center analyzed millions of user-reported emails. Some of the most difficult to identify emails are sliding past traditional email controls and landing in the inboxes of users.

**67%**

of malicious emails evading controls were credential phish

**10%**

increase in credential phish from previous year

**0%**

of those are stopped by perimeter controls






Once delivered to the inbox, phish tempt users to click and give up network or personal credentials, activate malware, or fall for scams like business email compromise (BEC) or wire transfer fraud. Additionally, there has been a growing trend of phishing campaigns containing HTML attachments. During 2021, Cofense Protect recognized a 150% growth rate in HTML attachments in phishing attacks. This represents about 30% of all credential phishing attacks detected by the platform.<sup>1</sup>

Since SEGs are missing so many phish, there's a good chance other technologies—firewalls, anti-virus, and EDR – also aren't spotting these threats. Such gaps can leave you vulnerable for hours, days, or even longer.

**Bottom line:** You can't rely on SEGs alone. They are the first line of defense, not the last one.

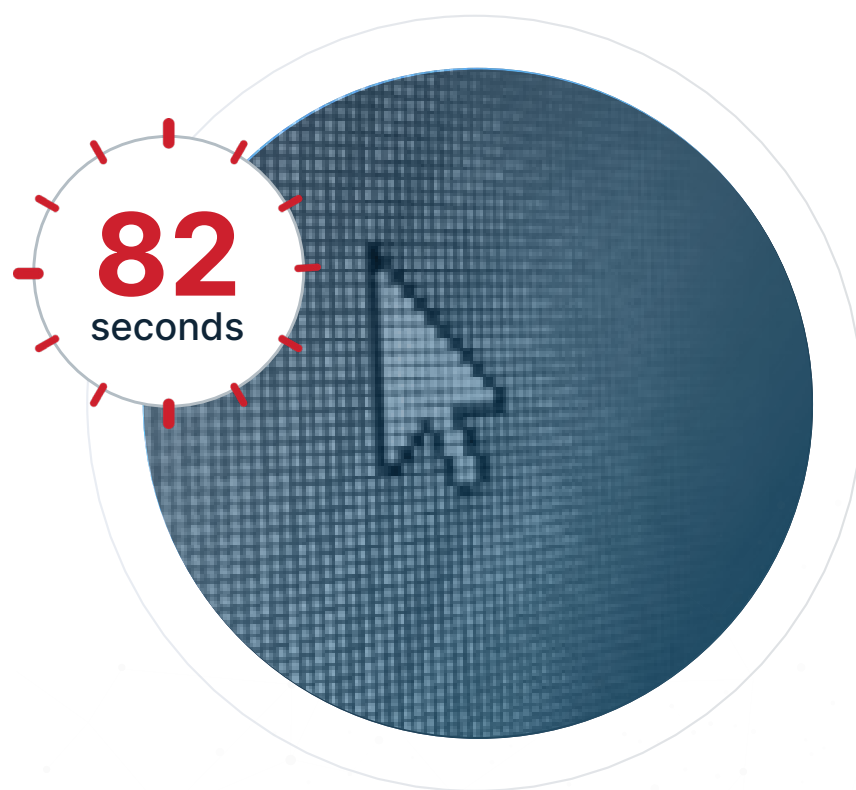


## To Understand The Problem and How You Can Solve It, Let's Look At:

-  What is a SEG?
-  How do SEGs work?
-  Why native email security & SEGs are not enough.
-  The painful consequences of failure.
-  And finally, the gap in security and phishing protection your team needs to fill—your last line of defense against threats when the clock is ticking.

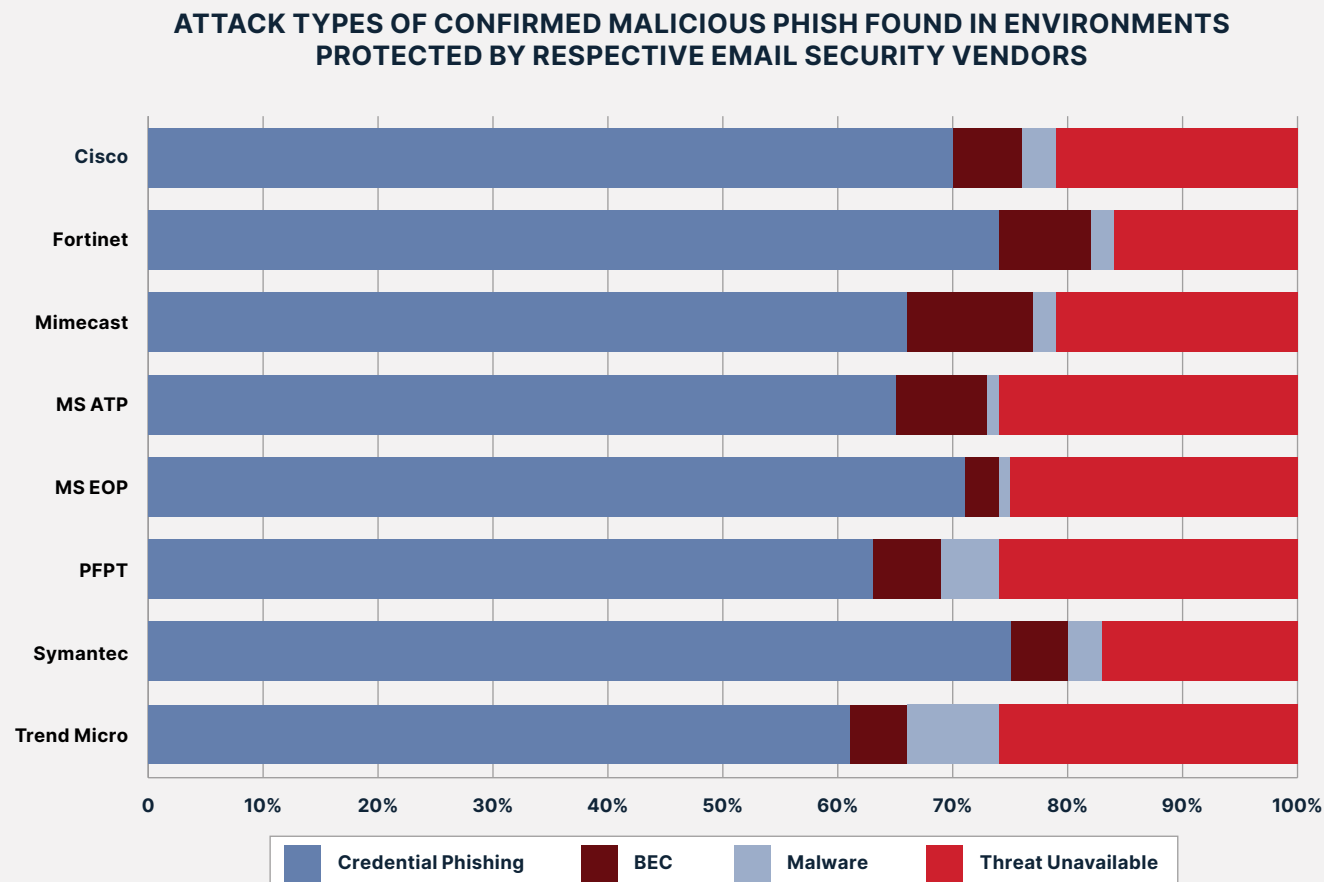
## 82 Seconds

That's the average time it takes for users to click on a phishing campaign.<sup>2</sup>








# What is a SEG?

Secure email gateways - AKA email gateways - are the most common types of perimeter technology used to stop phish from reaching the inbox with some organizations deploying multiple SEGs and spending millions of dollars annually. Unfortunately, **they don't stop advanced phishing attacks**. Threat actors have adapted their tactics and use multiple stages in their delivery of either malware or credential stealing to get users to engage.



## How do SEGs Work?

SEGs guard against phish by:

-  Validating senders.
-  Validating content.
-  Detecting known tactics, techniques, and procedures.
-  Executing attachments in sandboxes.
-  Wrapping URLs for click-time analysis.

**Unfortunately**, unlike firewalls and other security technologies, SEGs receive no regulatory or compliance oversight. That's right, SEGs get zero validation testing against the problem they're meant to solve—phishing, the #1 global cyber-threat.

In 2021, Cofense analyzed the performance of commonly used email security solutions in customer environments and found that BEC, credential theft, and other URL based phishing attacks evaded these solutions at high rates.

BEC, Cred Theft & Other Types of Phishing Attacks Evade Existing Email Security tools at High Rates				
Microsoft E3	Microsoft E3	Proofpoint	Cisco Ironport	Mimecast
Attacks Containing Malicious URLs that Reach Inbox				
94%	40%	49%	61%	82%

**Your SEG alone is NOT enough and phishing attacks are slipping through the net.**

# Why Native Email Security & SEGs Are **NOT** Enough

As we have seen, traditional email security controls can handle the basics of perimeter phishing defense. But today's modern and sophisticated attacks are anything but basic. They prey on the emotions of your end users' and are evolving more quickly than some technologies can keep up.

## 1 Attackers Constantly Innovate

You configure your email security to thwart the latest Tactics, Techniques, and Procedures (TTPs). Threat actors then innovate relentlessly to stay ahead and email security vendors often have limited visibility into live, active phishing threats. Attackers are shifting to using harder to detect tactics with goals like stealing user credentials to gain access to sensitive information or effectively deploying ransomware to make a quick buck.

In 2021, the Cofense Phishing Defense Center analyzed millions of user-reported emails. Among them we saw noticeable trends in the attack types that were making it past existing controls:



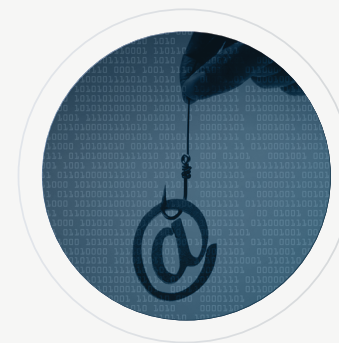
**67%**

**Credential Phish**



**7%**

**Business Email Compromise**



**3%**

**Delivered Malware**

## 2 SEG Vendors Are Reactive

You are not the only one having trouble keeping up. As phishers refine their tactics, SEG vendors scramble too.



### **Not Scalable**

Can't keep pace with attacker TTPs



### **Coverage issues**

Try to fill many holes, attackers need just one



### **Maintain Productivity**

Keep legitimate emails flowing

## 3 Business Can't Wait

Tuning your SEG to the latest TTPs takes time. But email must flow freely for your business to operate. Too often, you're forced to choose between speed and organizational security. Sooner or later, speed wins out and phish land in the inbox.



# The Painful Consequences of Failure

To recap: you tune your SEG to stop the latest TTPs. It performs as configured, but soon attackers respond with something the tech has never seen. Now you're back to square one, with cunning human adversaries outsmarting machine controls. When this inevitably happens, the damage can be severe.

## The Time and Losses Are Severe



**\$4.24M**

Average cost of a breach<sup>3</sup>



**287**

Average number of days to  
identify and contain a data  
breach<sup>4</sup>



**\$180**

per record cost of personally  
identifiable information<sup>5</sup>



## Serious Threats Get Through



Malware like Emotet, Ad Wind, Agent Tesla, Predator



BEC Attacks, Credential Theft, Cryptocurrency and NFT Themes

## SEGs Miss Phish Every Day

Phishing attacks are responsible for more than 80% of reported security incidents. According to CISCO's 2021 Cybersecurity Threat Trends report, about 90% of data breaches occur due to phishing. Spear phishing is the most common type of phishing attack, comprising 65% of all phishing attacks.



# Your Best Defense Against Phishing Attacks

## Gaps You Need to Fill

Because SEGs are so porous, you need something to back them up and a consistent way to find and remove threats that reach the inbox. We are talking defense-in-depth, combining human intuition and purpose-built automation.

## Visibility Into Active Threats

Reliance on the intelligence provided by your SEG is not enough. Timely, accurate, and actionable phishing insights are required to effectively protect your organization. Leveraging the insights of the people and technology both inside and outside your own organization ensures that you are better prepared to fend off both known and unknown evolving phishing campaigns.

## Security Awareness

When human attackers deliver threats to the inbox, humans need to respond, starting with end users. Besides educating users on phishing, your security awareness program needs to let them practice in a real-world setting: their inboxes. Phishing simulations are your best bet. Make sure the training is positive, not punitive, and that scenarios mirror threats your organization faces.



## Email Reporting

Your security teams can't stop a threat in the inbox unless it's reported. A 'Report Phishing' button on the email toolbar makes it easy. With a single click, end users get involved. As employees get more practice, both in training and real situations, they'll sharpen their intuition—something tech controls like email gateways lack.

## Email Analysis

When security teams try to respond manually to email reports, they usually fall behind. There are simply too many emails, most of them harmless. Automation can cut through noise and identify real threats, plus prioritize them so analysts can budget their limited time.

## Search and Quarantine

Thanks to well trained users and advanced automation, your SOC has identified a phishing email in a handful of inboxes. But who else received the phish? Again, you'll rely on automation to search all inboxes ASAP and quarantine the threat before lasting damage is done.

## Quick Review

1. Phishing attacks bypass perimeter controls daily and routinely.
2. Native email security & SEGs only work as well as they're configured—they are machines, after all.
3. Your email, SEG vendor and your security team can't keep pace with phishing attackers—they adapt and innovate too quickly.
4. Sooner rather than later, human attackers will figure out a way around your security filters and technology, regardless of who makes them.
5. When phish reach the inbox, humans are the key to any phishing defense.

---

## Contact Us

Let us show you how to level up your email security strategy. Visit [cofense.com](https://www.cofense.com) or schedule a live demonstration today!

**Book a Demo Now!**

---

## Sources

1. [Cofense 2022 Annual State of Phishing Report](#).
2. [Cyber DB, 2018](#).
- 3, 4, 5. [IBM Security's 2021 Cost of a Data Breach Report](#)

## About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of nearly 32 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, visit [www.cofense.com](https://www.cofense.com) or connect with us on [Twitter](#) and [LinkedIn](#).

