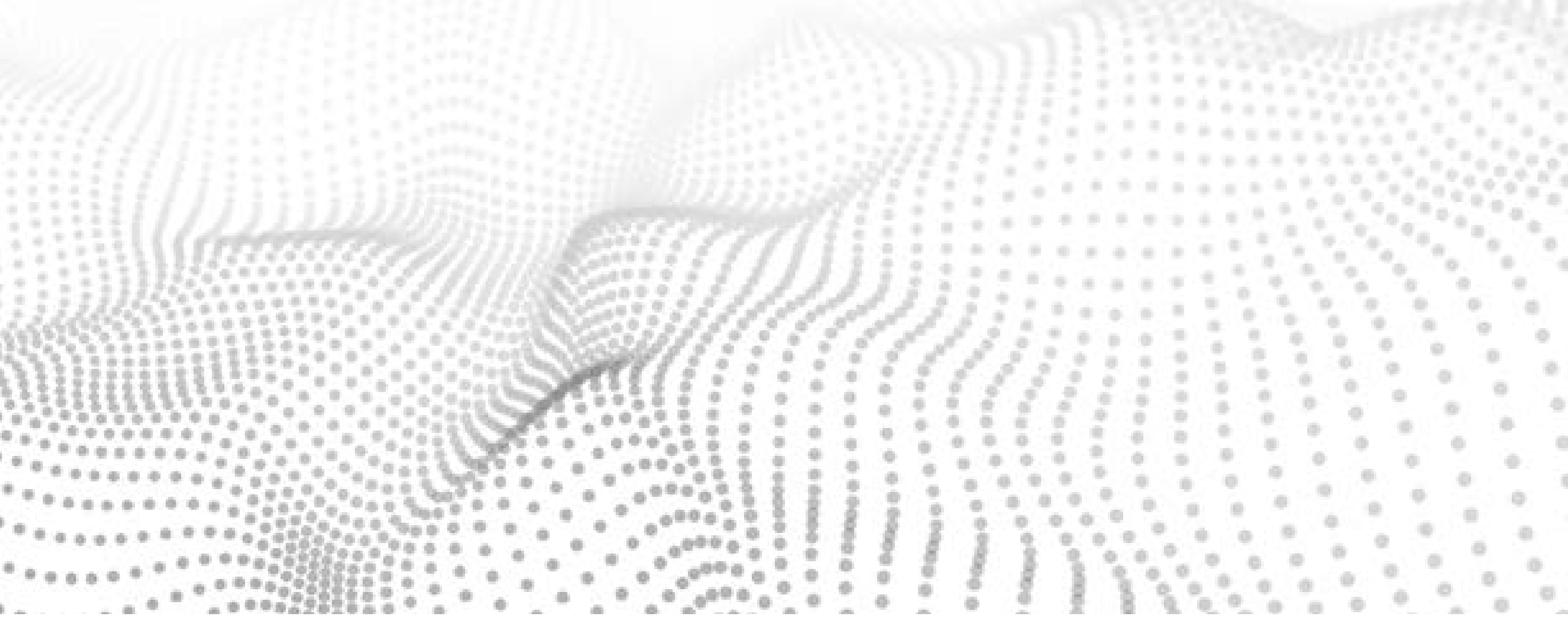
PHISHME®
COFENSE

Intelligence-Driven Phishing Defense



Traditional Phishing Defense Needs To Evolve

Phishing is among the most dangerous attack vectors. According to the 2024 Verizon Data Breach Investigations Report, 78% of all data breaches start with a phishing attack. With modern advancements such as artificial intelligence (AI) and machine learning (ML), cybercriminals are gaining new powers to evade email defenses. In this heightened threat environment, organizations need to employ two key components to ensure a sound phishing protection strategy:

1. **Perimeter filtering:** Every organization should have a competent perimeter defense program, such as a secure email gateway (SEG), to filter out as many malicious emails as possible. However, as we will discuss in this eBook, even AI-powered ones are far from perfect.

2. **Intelligence:** Organizations need intelligence to see, remediate, and mitigate the email threats that inevitably get past perimeter defense measures.

The Real Danger Zone: Unseen Post-Delivery Phishing Threats

Perimeter defenses, such as SEGs or equivalent AI-/ML-driven tools, are built to prevent as many malicious emails as possible from being delivered to your employees' inboxes. While this layer of defense is indispensable, significant numbers of phishing attacks get through. In fact, Cofense global threat Intelligence derived from 11 million annual post-SEG suspicious email reports indicates that 15% of known phishing attacks bypass perimeter defenses. A small sample of the nearly 1 million verified phishing attacks seen by Cofense Intelligence that were missed by perimeter defenses are published openly for review.

This is particularly concerning because, according to research conducted by the Cyentia Institute measuring multiple cybersecurity risk indicators, 12% of employees, on average, are high-risk and susceptible to phishing. In other words, your organization will always have a segment of employees who will click on the wrong emails.

On top of that, these threats and potential compromises remain unseen for far too long. Average dwell times reported in the 2024 M-Trends report tell us that, when malicious emails are delivered or employees have clicked and become compromised, it will take your security team ten days just to find out.

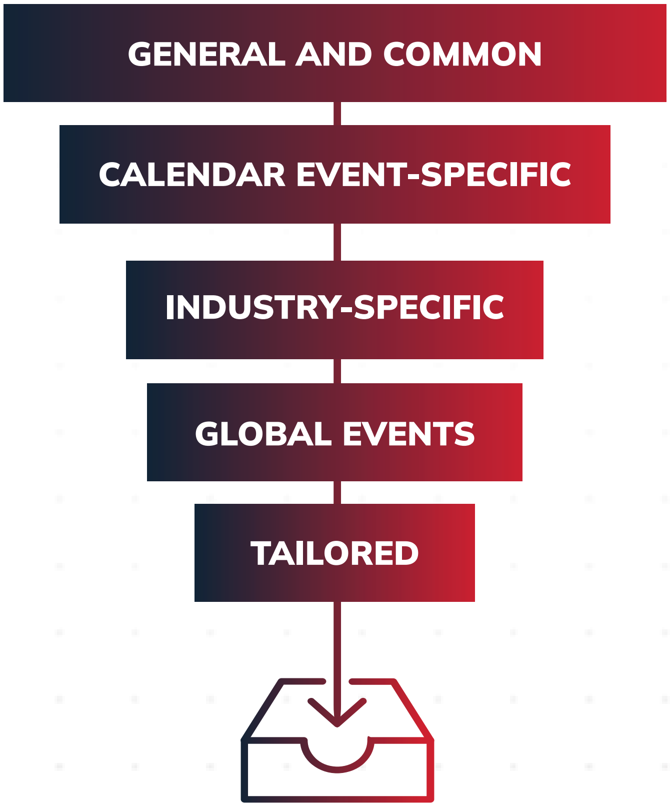
Taken together, these factors make unseen post-delivery phishing attacks a high danger zone.

Why Defensive AI and Email Security Perimeter Tools Miss Attacks

Perimeter filtering defenses must cope with high volumes of the most common malicious emails on behalf of many customers across a wide variety of industries. As a result, whether based on statically defined rulesets, large language, or other MML models, filtering defenses are designed as broad, general-purpose solutions.

However, the attacks aimed at your organization are not the same. In fact, there is a custom shape to the types of attacks hitting any given organization. As seen in Figure 1, that shape can be visualized as an upside-down pyramid. At the top are the broad, general-purpose, volumetric attacks. These are the attack types that broad rulesets and models deal with best. Below that are increasingly targeted and tailored attacks. For example, there are attacks that are category-specific, tailored to different times in the calendar, different industries, as well as global events like elections or natural disasters. Finally, there are highly targeted attacks aimed just at your company and your people. The more tailored the attacks, the less likely broad filtering will catch them.

Types of Phishing Threats



GENERAL AND COMMON

CALENDAR EVENT-SPECIFIC

INDUSTRY-SPECIFIC

GLOBAL EVENTS

TAILORED

Figure 1

Offensive AI Is Making Things (Far) Worse

Prior to the advent of AI, highly tailored attacks had to be handcrafted. This required time and capital, and thus, only the best-funded cybercriminals could execute them. Offensive AI has changed the game, making it far easier, faster, and cheaper to research, personalize, and execute phishing campaigns at scale.

While defensive AI exists and is very useful for improving perimeter filtering, it can never keep up with offensive AI. Unlike software vendors, threat actors are unconcerned by the regulations, data privacy laws, and corporate budgets to which a typical organization needs to adhere. Further, unlike defensive AI software, attackers carry no technical debt and can simply discard what doesn't work.

Defensive AI models must conduct regular, multi-week retraining. Offensive AI moves so fast that Cofense Intelligence regularly sees large spikes in attacks getting through AI-based SEGs during these retraining periods.

Unleash Your Human Intelligence To Defend Against Post-Delivery Email Threats

Since broad-based perimeter defense tools aren't sufficient, how do you protect your organization from the post-delivery threat? The answer is human intelligence.

Unlike broad AI models, employees working in your organization possess deep contextual and intuitive knowledge of what is normal or atypical. They know the people in your organization and their work and communication habits, as well as corporate policies and practices.

When trained properly, not just on basic awareness but to recognize real threats that bypass perimeter defenses, employees can become cyber-resilient assets that identify and report the suspicious emails getting through your perimeter defenses. This creates a strong culture of reporting, allowing you to unlock a valuable source of real-time, actionable intelligence about your organization's post-delivery email threat environment.

Further, when relieved of spam overhead and equipped with powerful and easy-to-use analytics, SOC analysts can utilize this human intelligence to perform effective and rapid threat hunting and remediation.

Gain Human-Vetted Intelligence at Scale

While empowering your employees to act as a vital layer of defense in your email security strategy is essential, the truth remains that you can only go so far with your own employees. After all, your employees have day jobs. **Phishing detection will never be their top priority.**

But what if you could take your 5,000 employees and multiply them by 10, 100, or 1,000? Or more?

This level of human-vetted intelligence at scale is what Cofense has built over many years. Our global threat intelligence sources real-time reporting of suspicious emails by a network of over 35 million Cofense-trained employees from companies around the world. Like your employees, these reporters are using threat-relevant training and their contextual knowledge to find and flag phishing attacks that evade perimeter defenses.

However, scaling intelligence goes beyond the number of trained employee reporters. Cofense operates a global team of expert phishing analysts who use this collective employee intelligence to perform timely, in-depth threat analysis

How Human-Vetted Intelligence Transforms Post-Delivery Defense

There are a variety of ways that an intelligence-driven approach improves your ability to defend against post-delivery threats:

- Transform security awareness training (SAT) content from generic to threat-relevant. This empowers your employees to recognize the real threats they're going to see in their inboxes, making it easier and more natural for them to report suspicious emails.
- Leverage the indicators of compromise (IOCs) detected by scaled human intelligence and feed them into analytics, automation, and remediation tools to improve analyst effectiveness.
- Apply ML that is trained not on broad data sets but on company-specific spam data to filter out noise from analyst workloads with extremely low false positives and false negatives.
- Utilize comprehensive post-delivery phishing threat intelligence, including both high-level landscape information and details, to aid post-compromise risk identification and mitigation.

Cofense Intelligence-Driven Phishing Defense Solutions

Cofense is the world's largest and most authoritative source of post-delivery phishing intelligence. Cofense offers human-vetted intelligence at scale, sourced by the world's largest network of reporters—over 35 million strong. Cofense protects 70 million employees working for the world's largest companies.

Cofense Intelligence is deeply integrated into a full-cycle suite of SAT, email analytics, auto-quarantining, threat landscape, and detailed intelligence reporting solutions. These solutions unleash the power of your employee and analyst insights and augments them with our global phishing intelligence.

Cofense is the only cybersecurity company leveraging expert-supervised AI for phishing detection and response—delivering human-vetted intelligence and real-world raining to help enterprises stay ahead of modern threats. Built to augment existing email defenses, Cofense identifies attacks that bypass perimeter filters, remediates them in minutes, and continuously strengthens the human layer through simulations modeled on active phishing campaigns. Informed by insights from over 35 million trained users, Cofense enables faster containment of threats and measurable reductions in risk. Organizations like Visa, Siemens, and Blue Cross Blue Shield rely on Cofense to reduce exposure, meet regulatory demands, and build lasting resilience against the most persistent cyber threat: phishing.

Smarter phishing defense. Stronger human security. cofense.com

Scan the QR code
or visit cofense.com.