

COFENSE PHISHING DETECTION & RESPONSE (PDR)



Cofense augments traditional perimeter defenses by identifying and quarantining advanced phishing threats that often go undetected.

The Problem.

It takes just one malicious phishing email bypassing your perimeter to expose sensitive data, and harm your reputation. Your first line of defense at your email security perimeter is often your secure email gateway, and in many cases, it's bolstered by a second layer of protection like an Integrated Cloud Security Solution.



The Cofense Phishing Defense Center (PDC) saw, on average,

**1 malicious email every
42 seconds throughout 2024**

Our Solution.

Cofense enhances your SOC team's ability to detect, investigate, and remediate phishing threats that bypass traditional perimeter defense solutions. This critical layer identifies missed phishing emails (false negatives) using expert-supervised AI and real-time intelligence sourced from a global network of over 35 million trained users. PDR equips analysts with clear, high-confidence alerts, reducing alert fatigue and expediting response times, ensuring your organization stays ahead of the most persistent phishing threats. While these solutions do a reasonable job of defending against costly and malicious phishing attacks, traditional perimeter defenses can still miss up to 50% of more sophisticated threats.



Scan the QR code or visit **cofense.com** to learn how to catch more phish with Cofense.

COFENSE PHISHING DETECTION & RESPONSE (PDR)



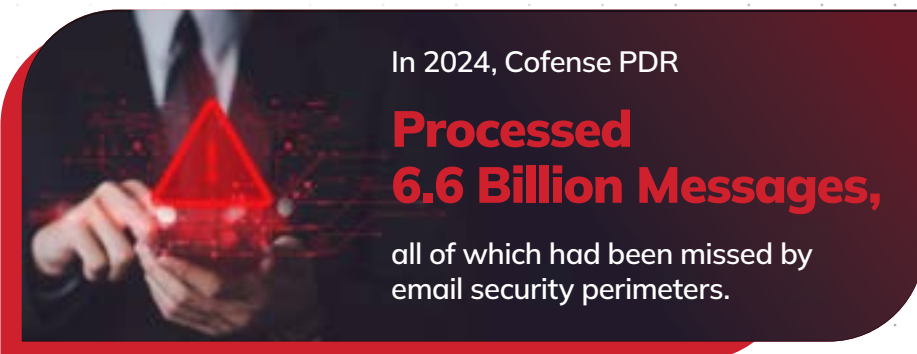
Why Choose Cofense PDR?

- **Catch What the Gateway Missed:** Eliminate false negatives using expert-supervised AI and real-time intelligence.
- **Act in Seconds, Contain the Threat:** Rapidly identify and quarantine phishing threats across all inboxes.
- **Reduce Analyst Workloads:** Automate threat clustering and risk prioritization to streamline SOC workflows.
- **Strengthen Organizational Resilience:** Stay protected with industry-leading, phishing-specific intelligence and proactive incident management.

Exclusive Features of Cofense PDR

Rapid Quarantine with Deep Search Indexing -

Cofense's email indexing swiftly identifies and removes phishing threats across all inboxes, far outpacing legacy tools.



In 2024, Cofense PDR

**Processed
6.6 Billion Messages,**

all of which had been missed by email security perimeters.

Intelligence purpose-built for phishing -

Supervised AI analyzes user-reported phishing emails with 99.998% accuracy.

Smarter clustering, faster triage -

Automatically cluster polymorphic phishing attacks, streamlining workflows and reducing analyst workload.

Behavioral context for targeted response -

Identify which users are interacting with phishing emails, enabling precise incident response using behavioral data.

Custom-tuned spam filtering -

The AI Spam Filter, uniquely trained on your environment, filters out irrelevant alerts to focus on legitimate threats.

Seamless integration into existing SOC workflows -

Smoothly deploy advanced phishing defenses within your current security stack using out-of-the-box workflows.

Cofense is the only cybersecurity company leveraging expert-supervised AI for phishing detection and response—delivering human-vetted intelligence and real-world training 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](https://www.cofense.com)

