COFENSE VISION®

# Quarantine Email Threats at Speed.

## Your Problem.

**Phishing reports are the tip of the iceberg.** When a phishing attack evades your secure email gateway (SEG), reports to your security team may not expose the entire threat. Your SOC needs to find every instance of the campaign quickly, before it turns into a major breach.

An auto maker **automatically detected 4,500 phishing emails in seconds**—stopping an unreported phishing attack in its tracks.

## Our Solution.

**Cofense Vision is the fastest way to stop the entire phishing attack,** including emails not reported by users. With a single click, quarantine every instance of the malicious email and stop the attack in its tracks. Cofense Vision copies and stores only the metadata from all emails in your organization's environment, so the SOC can look for a phishing campaign without creating more work for the email teams. The solution also provides a compliant, auditable workflow.

**Cofense Vision enables security teams to automatically quarantine phishing threats from all user inboxes without disrupting or waiting on the IT mail team.**

### Proactively Stop Attacks.

Apply the insights provided by 32 million global reporters through a specially curated Cofense Intelligence feed designed to detect and remove email threats from your environment before they're even reported.

### Search Faster.

Cofense Vision stores potential Indicators of Phishing in an offline environment optimized for threat hunting. This ensures searches are fast, not impacted by the throttling controls of Microsoft Exchange and Office 365, without relying on mail teams.

### Quarantine Quickly.

Cofense Vision enables security teams across the enterprise to quarantine an email threat with a single click. Quarantined messages are moved to a mailbox hidden from the user but visible to the mail team and can be "unquarantined" in minutes.

### Stay Compliant.

Speedy searches no longer require privileged rights to the mail environment. Cofense Vision extensively audits and logs all actions. You can see who is searching for what and remain in compliance.

## How Cofense Vision Works.

Cofense Vision provides "search and destroy" capabilities to cybersecurity operators defending against phishing attacks.

### Phish-Focused Threat Hunting.

Cofense Vision indexes email and is optimized for phishing threat hunting, deployable on-premises, within AWS or Azure, or as a SaaS solution. Unaffected by Microsoft EWS throttling and separate from your mail team's production environment, your SOC team can search, find, and neutralize threats in minutes.

### Powerful Search.

Not just limited to subjects and senders like other "solutions," Cofense Vision supports complex queries to find the most dangerous polymorphic attacks evading SEGs. Find campaigns based on domains, URLs, attachment names and hashes, and other elements frequently found in advanced phishing attacks.

### Flexible Management & Integrations.

Users wanting to integrate Cofense Vision with their existing security stack, such as SOAR and SIEM platforms, have access to all Cofense Vision functionality, including client management, configuration, and logging through the fully documented Cofense Vision API. The API provides additional audit, search, and quarantine capabilities not currently available from the Cofense Vision user interface. Take advantage of Vision's robust quarantine capabilities without disrupting your existing workflow or process.

### IOC Wildcard Matching.

IOCs are extremely dynamic in nature—always evolving ever so slightly to try and evade detection. With automated IOC Wildcard Matching, Vision helps you keep up with these slight changes that often go unnoticed resulting in an up to tenfold increase in visibility of IOCs—providing exponentially more value than before.

## Cofense Vision SaaS Now Available.

It's now easier than ever to take advantage of capabilities such as instantaneous, organization-wide removal of malicious emails and increased visibility of email threats provided from over 32 million global reporters.

With Cofense Vision SaaS, experience faster time to value and eliminate friction by completely offloading infrastructure responsibilities to Cofense. Organizations utilizing this SaaS deployment model achieve:

- Rapid deployment
- Performance monitoring
- Fast troubleshooting
- Minimal dependencies

Recently, a global industrial technologies company had Vision up and running, ingesting emails, in less than 3 hours. On top of a speedy deployment, they were able to minimize maintenance costs, reduce dwell time, and incorporate automated information sharing via a robust API.

### 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 close to 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. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defense, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn.

COFENSE

**W:** cofense.com/contact **T:** 703.652.0717

**A:** 1602 Village Market Blvd, SE #400
Leesburg, VA 20175