HUNT EMAIL THREATS AT **SPEED.**

COFENSE VISION™

YOUR **PROBLEM.**

Mitigating a phishing attack requires speed and precision. If you don't quickly eliminate the whole problem, trouble continues to breed. Email search and quarantine tools are slow and inflexible, offering limited search scope like 'Sender' and 'Subject.' It's difficult to find the entire attack fast enough and account for the way tactics, techniques, and procedures morph to avoid exact matching for each recipient.

OUR **SOLUTION.**

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

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

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 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.

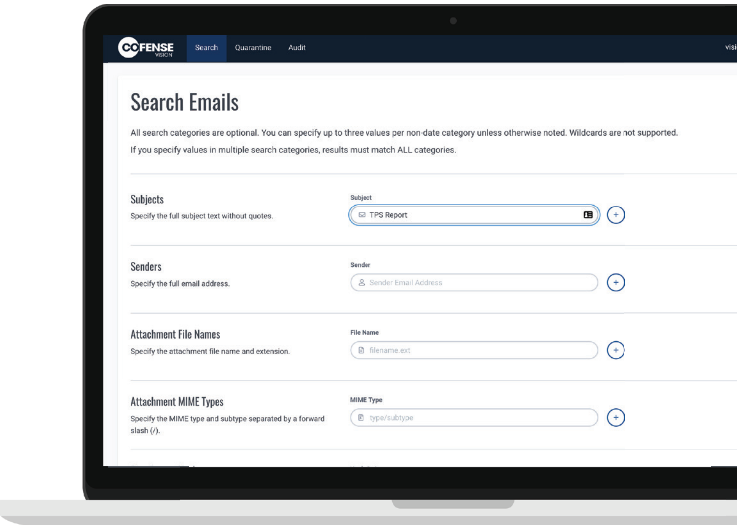
Speedy searches no longer require privileged rights to the mail environment. Cofense Vision extensively audits and logs all actions. You can see who is searching for what and remain in compliance.

HOW **COFENSE VISION** WORKS.

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

GETTING STARTED.

Cofense Vision can be deployed on premises, in AWS, or in Azure. To get started, we share the Cofense VM Image with your company’s PAAS account, where your instance setup is typically less than an hour. All of the Cofense Vision functionality is available in a fully RESTful and documented API as well as an elegant and modern user interface. Email ingestion supports both industry standard SMTP and journaling.



Search Emails

All search categories are optional. You can specify up to three values per non-date category unless otherwise noted. Wildcards are not supported.

If you specify values in multiple search categories, results must match ALL categories.

Subjects
Specify the full subject text without quotes.
Subject: TPS Report

Senders
Specify the full email address.
Sender: Sender Email Address

Attachment File Names
Specify the attachment file name and extension.
File Name: filename.ext

Attachment MIME Types
Specify the MIME type and subtype separated by a forward slash (/).
MIME Type: type/subtype

USER INTERFACE.

The new Cofense Vision UI allows analysts to search by combinations of fields, enabling them to quarantine some or all messages in seconds. With the user interface, the analyst can search for recipients, senders, subject, MIME type, attachments, and many other elements, essentially creating a cluster. The analyst can quarantine one or hundreds of malicious emails with a single click. Cofense Vision also removes the need for hard-coded credentials in scripts.

THE **API**.

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.

INTEGRATION WITH COFENSE TRIAGE.

Cofense Vision integrates with Cofense Triage™ for maximum visibility. The integration allows you to search for recipients, senders, subject, MIME type, attachments, and many other elements to find all emails in a campaign. You can then quarantine verified phish from all user inboxes.

Cofense Vision also helps identify users that received suspicious emails but did not report them. When Cofense Vision is configured as an integration in Cofense Triage, super users and operators with the appropriate permissions can search for exact matches to reported emails in Cofense Triage, then quarantine unreported emails directly from Cofense Triage.

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175