COFENSE INTELLIGENT EMAIL SECURITY

Unique Intelligence Enabling Organizations to Proactively Respond to Email Attacks

Proactive email security requires a vast amount of accurate intelligence that evolves with the threat landscape. Cofense synthesizes human intelligence, artificial intelligence, and email attack intelligence into the Cofense Intelligence Network and distributes across our portfolio of products to stop the most active and successful threat vector. Every month, intelligence from the Cofense Intelligence Network enables Cofense to quarantine up to thousands of emails per enterprise customer - even before they are reported by the customer's employee.

THE EMAIL SECURITY PROBLEM

An organization's email security posture is only as effective as the intelligence that powers it – and the intelligence powering traditional email security tools like Secure Email Gateways (SEGs) does not stack up. **Half of all email attacks, including Business Email Compromise (BEC) and credential theft, evade SEGs – and make up 91% of all cyberattacks.**[1] Threat actors are constantly iterating their tactics and techniques to bypass legacy technology and avoid Indicators of Compromise (IOC) Blocklists. These rapidly evolving IOCs allow email attacks to lurk in employee inboxes and evade detection – the average dwell time for attachment-based attacks is five days and a staggering 45 days for malicious links.[2]

1 (Deloitte 2020) 2 (Sheridan 2021)

The average dwell time for attachment-based attacks is

and a staggering

COFENSE INTELLIGENT EMAIL SECURITY

To efficiently mitigate the risks of email attacks, organizations must mature their email security posture from reactive to proactive with advanced technology powered by relevant, dynamic, and distributable intelligence. When evaluating a potential solution's intelligence, organizations should consider the following:

DECISION CRITERIA:

ACTIONABLE – Organizations should invest in intelligence that enables technology to stop threats not stopped by their other security investments.

RELEVANT – Organizations should look for intelligence on phishing attacks that reach employee inboxes.

RELIABLE – Organizations should look for intelligence that is based on real phish with minimal false positives.

TIMELY – Organizations should invest in intelligence that keeps up with the latest threat and feeds real-time into their email security technology.

HOW COFENSE SOLVES THE PROBLEM

Cofense's Phishing Detection and Response (PDR) Platform enables organizations to proactively stop the email attacks that pose the greatest threat to an organization. Cofense's automated technology and strategic services strengthen email security postures against phishing attacks and evolve with the threat landscape, all powered by Cofense's Intelligence Network.

The Cofense Intelligence Network is a combination of unique sources of intelligence that feeds powerful IOCs into Cofense's PDR platform in real-time to stop the email attacks that SEGs miss. This valuable, one-of-a-kind intelligence provides an unmatched level of effectiveness:

ACTIONABLE – Cofense's intelligence captures IOCs from threats evading SEGs.

RELEVANT – Cofense's intelligence pulls IOCs straight from malicious emails in employee inboxes.

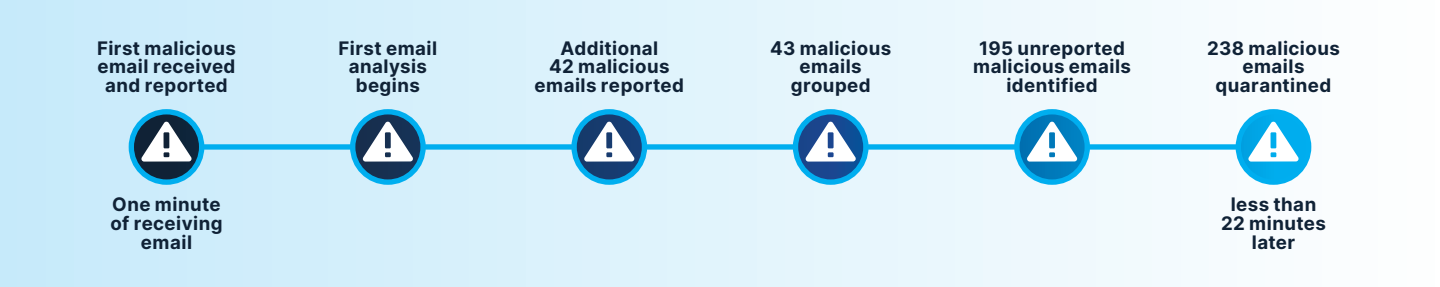
RELIABLE – All IOCs distributed by Cofense have been analyzed by our elite team to eliminate false-positives.

TIMELY – The newest attacks are detected and analyzed by Cofense and distributed into Cofense's technology in real-time.

Cofense synthesizes human intelligence, artificial intelligence, and email attack intelligence into the Cofense Intelligence Network and proactively evolves with the dynamic threat landscape.

WHY COFENSE'S INTELLIGENCE IS UNIQUE

When deployed, Cofense PDR, powered by the Cofense Intelligence Network, provides an unmatched level of effectiveness. A Cofense protected Manufacturing Company was targeted by a large credential phishing campaign. The Manufacturing Company deploys PDR, managed by the Phishing Defense Center (PDC), Cofense's phishing-dedicated Secure Operations Center (SOC) for customers. The first malicious email was reported within one minute of receipt and an additional 42 emails were received, reported, and analyzed. **Overall, a total of 238 emails were quarantined in under 22 minutes, stopping this attack in its tracks.**



Only Cofense provides organizations this level of effectiveness because of the unique combination of unique sources of intelligence. Cofense synthesizes human intelligence, artificial intelligence, and email attack intelligence into the Cofense Intelligence Network and proactively evolves with the dynamic threat landscape. Each of these sources, deployed through various products in the Cofense PDR platform, provides an important and necessary view into active phishing campaigns.

WHAT MAKES COFENSE SPECIAL...

A UNIQUE COMBINATION OF SOURCES OF INTELLIGENCE

Human Intelligence
>50% of threats reported in another environment first

Artificial Intelligence
88% of AI-detected threats never seen before

Email Attack Intelligence
"99.9% credibility rate" of IOCs validated by Cofense

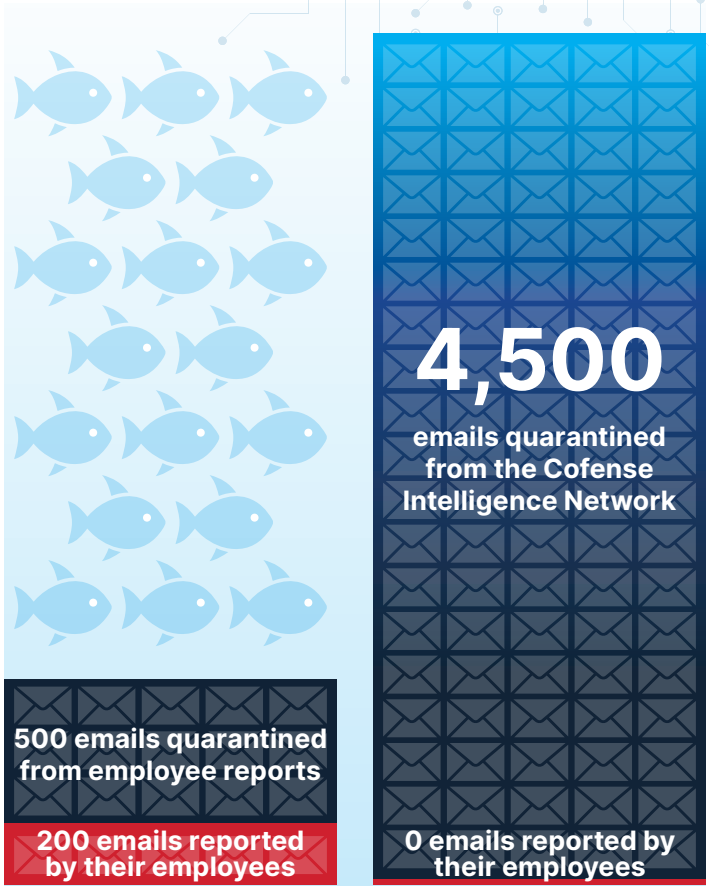
COFENSE INTELLIGENCE NETWORK

HUMAN INTELLIGENCE

Cofense's human intelligence derives from our network of over 32 million global users reporting real phish reaching their inboxes. Cofense Intelligence takes these human reported campaigns and provides that intelligence into our product suite and directly to customers, giving them a defensive head start against emerging attacks.

Sixty percent of the IOCs found in attacks reported to the PDC were reported in another PDC customer's environment first, immediately arming the organization with the necessary IOCs to stop the attack. These IOCs were found in emails reaching employee inboxes and evading SEGs, meaning Cofense sees IOCs other email security vendors don't.

For many organizations, the 60% of IOCs from the Cofense PDC stop 80-90% of their monthly quarantined emails. In one month, a 23,000 employee Healthcare Company had about 200 emails reported by their employees that resulted in about 500 emails being quarantined. However, an additional 4,500 emails were quarantined without being reported because of IOCs from Cofense. **Of the 5,000 quarantined emails that month, 4,500, or 88%, of them were detected and remediated because of the Cofense Intelligence Network.**



ARTIFICIAL INTELLIGENCE

Cofense's artificial intelligence stems from our patent-pending "Computer Vision" technology that reads emails like a human does. This intelligence is utilized in Cofense Protect, an easy-to-deploy product that blocks email attacks at the inbox.

Cofense Protect continuously improves effectiveness and stays current to the threat landscape because of Cofense's intelligence feed. In fact, 88% of the attacks identified by computer vision have never been seen before. One customer deployed Cofense Protect and blocked more malicious emails in the first four weeks than the number of malicious emails that were reported in the prior four months. **This resulted in a 94% reduction in volume of threats that required investigation, reducing risk for the organization and hours for their threat analysts.**

EMAIL ATTACK INTELLIGENCE

Cofense's email attack intelligence comes from our in-house Cofense Intelligence threat analysts reviewing every IOC from our human intelligence, our artificial intelligence, and various threat feeds Cofense tracks. These IOCs and all strategic intelligence produced are proprietary to Cofense and uniquely focus on attacks and tactics that are effective in reaching employee inboxes. Our intelligence analysts ensure every IOC released by Cofense and fed into our platform and our 20+ integrations is of the highest fidelity.

Many of our customers subscribe to our Intelligence product in addition to deploying our phishing awareness and simulation solution and incident response solution. **Our customers have told us they experience over a "99.9%" credibility rate.** In fact, one threat analyst at a large financial institution said "We process Cofense reports first because we know if you're reporting it, it's bad. Cofense Intelligence is the most accurate phishing threat info we receive and it's easy to consume."

COFENSE'S VALUE FOR YOUR ORGANIZATION

Organizations must evaluate both the technology and intelligence of a solution when investing in email security. A comprehensive email security solution is necessary to protecting an organization as email attacks make up 91% of all cyberattacks. However, most solutions don't stack up as half of all email attacks evade SEGs and reach employee inboxes. An email security solution is only as effective as the intelligence that powers it, and Cofense's PDR platform is powered by a powerful combination of unique sources of intelligence that enables organizations to detect and respond to email attacks. Human intelligence, artificial intelligence, and email attack intelligence are deployed together throughout the PDR platform to automatically remove attacks first seen by another Cofense customer, block attacks that have never been seen before, and reliably power automated technology without the worry of false positives.