Cofense Protect MSP®/™

Computer Vision Phishing Detection

Next Generation Anti-Phishing

End-User Benefits

Rev. 2.20

July 2021

Table of Contents

Phishing is the #1 Attack Vector 3
Zero-Second Detection 4
Brand Impersonation 4
Person Impersonation 4
Attachments Scanning 4
Employee Training 4
Computer Vision and AI 4
Cofense Protect MSP Stops All Phishing Attacks 5
Integration With Cofense Phishing Simulations 5
Gets Smarter Every Day 5
Super-Fast Protection 5
Getting Help 6
About Cofense 7

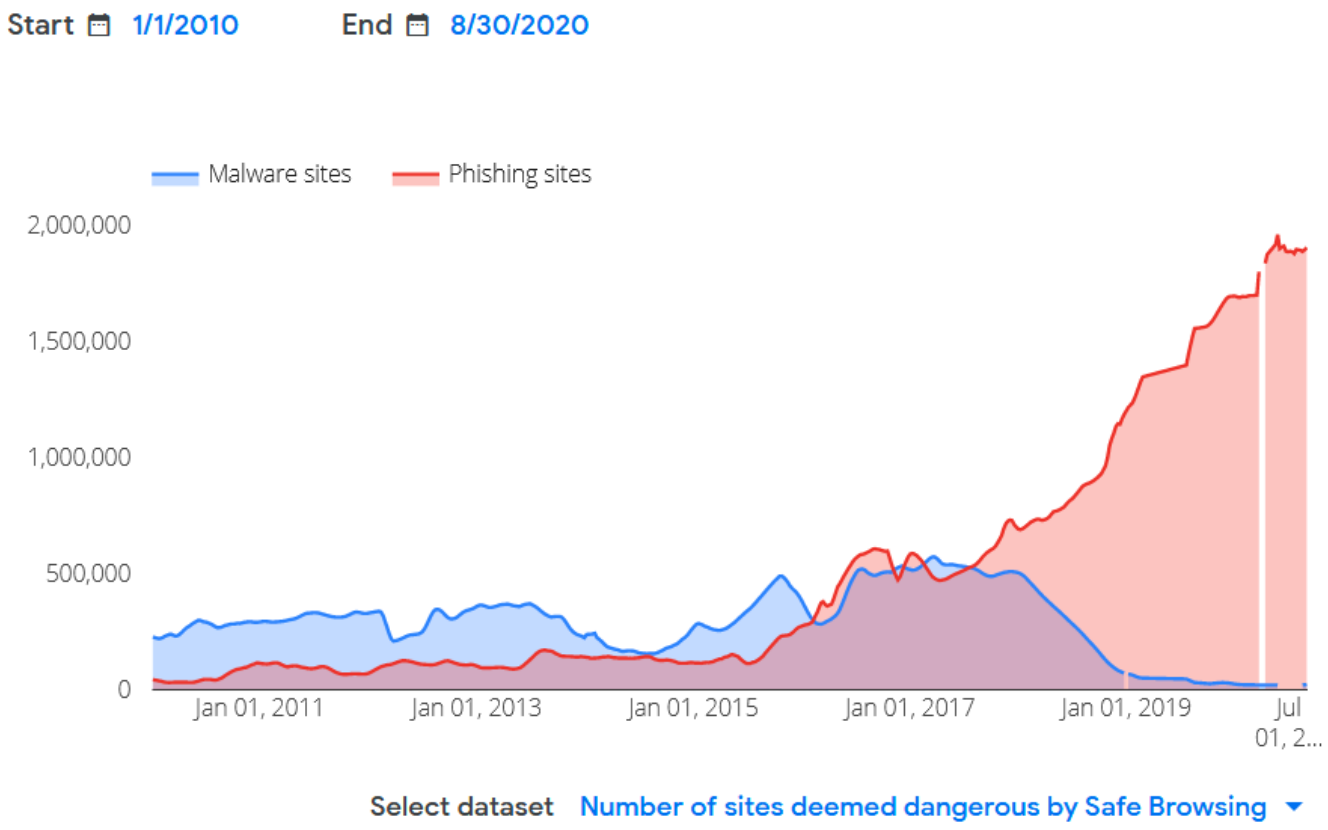
Phishing is the #1 Attack Vector

Phishing is the most effective, prevalent, and inexpensive method to carry out a cyber-attack.

Organizations deploy multiple layers of security technologies to prevent, detect, and respond to cyber threats. But even with these controls in place, organizations are still far more likely to be compromised via a phishing attack than by any other attack method.

Phishing is exploding and has increased more than 1000% in the last few years, based on the Google Safe Browsing report.

These attacks are used to steal financial information, intellectual property, extort ransom payments and, in many cases, can put a company out of business.



Zero-Second Detection

Cofense Protect MSP is an anti-phishing solution that combines Computer Vision and AI to detect phishing emails and pages in real-time. Cofense Protect MSP is the only solution that stops new phishing emails, websites and even attachments in real time - before they have been reported or added to the blacklist, which provides more than 10x higher detection rate compared to the market leaders.

Cofense Protect MSP is a cloud-native, advanced phishing detection and email analysis technology. It is built to stop advanced attacks that circumvent basic detection mechanisms baked into the Microsoft O365 and Google Workspace offerings.

Cofense Protect MSP is a one-stop defense solution for all phishing-related attacks, such as spear phishing, Business Email Compromise or BEC attacks (CEO fraud), scam, and ransomware attacks delivered via phishing.

Brand Impersonation

Cofense Protect MSP detects new, just created, phishing and fraud websites which lead to credential thefts pages or malware. Cofense Protect MSP is the only solution that also discovers mediator pages containing phishing and malware links, which are created to fool other security solutions.

Person Impersonation

Cofense Protect MSP automatically detects BEC, impostor and fraud emails whether sent using spoofing, address or name impersonation, utilizing several techniques, including visual analysis of email assets.

Attachments Scanning

Cofense Protect MSP scans email attachments and detects links hidden in those documents (PDF, MS Office, text files, cloud documents) which point to phishing websites and malware, as well as detect phishing delivered in inline attachments.

Employee Training

Integrated with our top-notch detection engine, the training module continuously builds employee phishing awareness by sending relevant, real-data simulation emails with contextual data based on ongoing attacks.

Computer Vision and AI

Computer Vision is an AI technology that utilizes advanced perception analysis algorithms to simulate how humans see. Cofense Protect MSP uses this technology to detect phishing attacks by visually representing, inspecting, and drawing conclusions on emails, URLs, landing pages, and attachments. Cofense Protect MSP pairs computer vision with machine learning algorithms and advanced training, to create a resilient and ever-evolving phishing detection capability that will mitigate phishing threats in real-time.

Cofense Protect MSP Stops All Phishing Attacks

Cofense Protect MSP can stop all phishing attack types and as new ones emerge, they easily can be added to the Cofense Protect MSP detection engine.

Type of Attack	Protection From
Phishing links	Brand phishing pages Phishing kits Generic phishing Mediator pages Client-side attacks
Imposter emails	Internal impersonation (Business Email Compromise, CEO fraud) External contacts impersonation (BEC) Brands impersonation Impersonation via SaaS
Attachments	Phishing links inside attachments Inline HTML attachment and scripting Cloud document phishing

Integration With Cofense Phishing Simulations

Businesses using Cofense Protect MSP get industry leading Cofense PhishMe simulations for maximum effectiveness. Customers benefit from training based on real attacks. There are no other AI and computer vision threat detection solutions which also carry a training component. Combined with the zero-second phishing attack protection, SMBs now can offer their employees the best phishing attack prevention available.

Gets Smarter Every Day

The machine learning algorithms continuously ingest the crowd-sourced Cofense Intelligence data feed from over 27M humans, making the quarantining of phishing emails even faster.

Super-Fast Protection

Cofense Protect MSP is a zero-second protection product. Malicious links in the message are disabled, further protecting your employees from phishing attacks because of accidental clicking.

Cofense Protect MSP customers are onboarded with sub-one minute deployment.

Cofense Protect MSP is integrated with popular email cloud providers such as Google Gmail and Google Workspace and Microsoft Office 365 family (Office 365 & Exchange Online), as well as with MS Exchange with On-Premises deployment. Customers

Getting Help

From the Cofense Resource Center, you can access product documentation and knowledge base articles, post feature requests, and submit support tickets. Based on your location, use the appropriate portal link below:

- EMEA or META: https://supportintl.cofense.com
- Other locations: https://support.cofense.com

About Cofense

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. For additional information, please visit: http://www.cofense.com/.