CLOUDFLARE®
AREA 1 SECURITY

THE AREA 1 SECURITY DIFFERENCE

Area 1 Security is the only email security company dedicated to providing customers a clean inbox, free of threats. Our cloud-native platform provides preemptive, comprehensive, contextual and continuous security to stop phishing attacks before they reach inboxes.

CHALLENGE

Phishing, business email compromise (BEC), ransomware and account takeover attacks make up a small volume of threats (typically less than 1%) but cause the greatest financial damage. Our solution, Area 1 Horizon™, blocks these sophisticated, difficult-to-detect email-, web- and social media-based phishing attacks others miss to make a clean inbox a reality. We also amplify your resources by decreasing your SOC's incident triage time by more than 90%, improving your organization's response times and security posture.

AUGMENTING MICROSOFT 365 AND GOOGLE WORKSPACE SECURITY

Microsoft and Google's built-in capabilities work great for email hygiene and stopping high-volume, commodity attacks. However, low-volume and malware-less attacks (such as BEC, which have no links or malicious payloads) based on social engineering slip through, evading even the most sophisticated provider controls like Microsoft EOP/ATP. As a certified partner, Area 1 integrates seamlessly with Microsoft and Google email and collaboration features for best-in-class cloud email security.

ELIMINATING SECURE EMAIL GATEWAY (SEG) SECURITY GAPS, AND ELIMINATING SEGS

Similar to cloud email providers, traditional secure email gateways (SEGs) have a hard time detecting low-volume, high impact advanced phishing attacks. Many hosted SEGs also cannot handle the high traffic volumes and dynamic nature of cloud-based email. Area 1's cloud-native solution integrates seamlessly with cloud email providers to replace SEGs for a modern, cloud-first architecture and security.

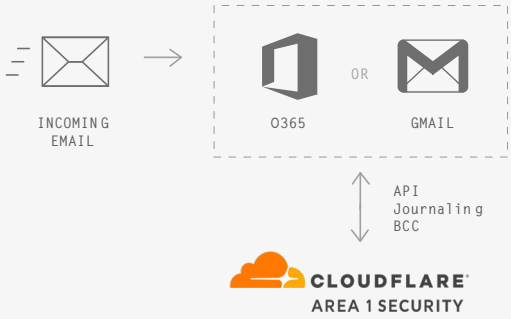
> "If you're looking for advanced email phishing protection, go for Area 1. Traditional email security gateways are limited. You need advanced detection techniques to counteract cyberattacks."
>
> - Messaging Manager, Fortune 50 Global Insurance

WHY AREA 1

- **PREEMPTIVE -** Stop attacks an average of 24 days before malicious campaigns launch.
- **COMPREHENSIVE -** Protection against a full range of attack types, channels and vectors.
- **CONTINUOUS -** Continuous security for the entire attack cycle — pre-delivery, at-delivery and post-delivery.
- **CONTEXTUAL -** Advanced detection techniques (e.g. natural language understanding/NLU, partner social graphing).
- **ACCOUNTABLE -** Enterprise-class scalability and reliability, ensuring a clean inbox with the industry's first and only pay-for-performance business model.
- **FLEXIBLE DEPLOYMENT -** *Transparent, multi-mode deployment options. Inline and API. Zero-touch deployment in under five minutes.*

SET UP A RISK-FREE ASSESSMENT IN UNDER 5 MINUTES

Area 1 Horizon™ is a fully elastic cloud-native service with no hardware or software to install. We offer flexible deployment options including multi-mode protection. Our solution can be deployed in under five minutes and requires no tuning or maintenance afterwards.



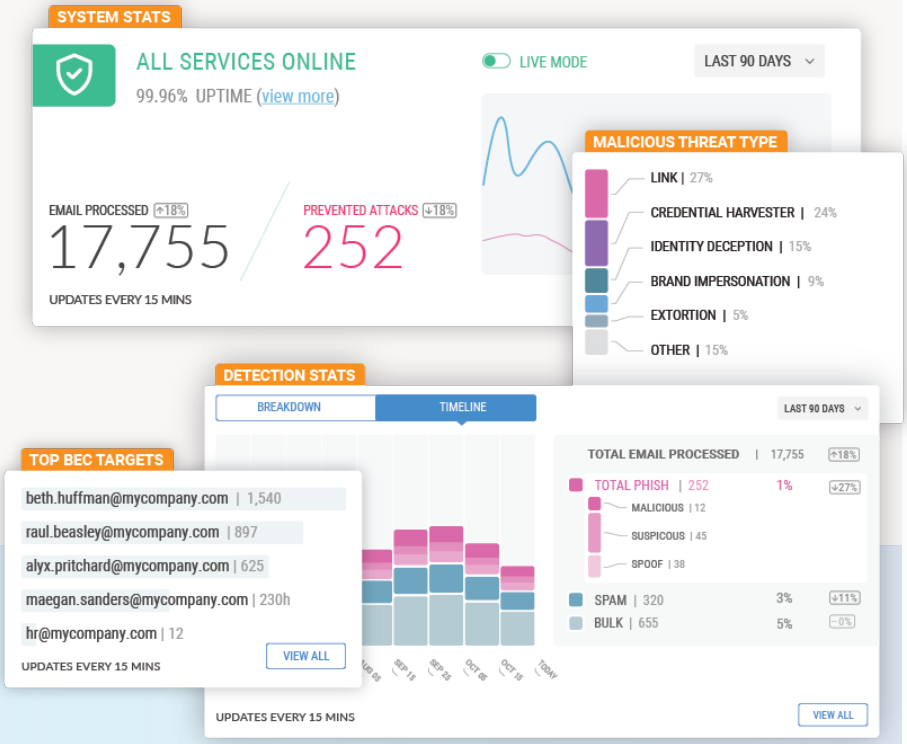
WHAT THREATS ARE BYPASSING YOUR EXISTING EMAIL SECURITY CONTROLS?

Area 1 Security stops sophisticated, highly targeted phishing attacks missed by traditional email security solutions, as well as commodity threats, to give customers a clean inbox. In fact, when deployed behind existing security defenses, we've seen our solution stop 30 percent more malicious campaigns than traditional email gateways and cloud email suites.

ORGANIZATION INDUSTRY	EMAIL SECURITY SYSTEM USED	MISSED THREATS	TOTAL EMAIL VOLUME
Insurance Software	Microsoft 365	***517,968***	103,099,539
Pharmaceutical	Proofpoint	***448,440***	432,611,141
Food and Beverage	Cisco Email Security (IronPort)	***105,603***	420,088,334
Education	Custom	***90,763***	420,088,334

AREA 1'S PHISHING RISK ASSESSMENT SHOWS YOU:

- **YOUR BIGGEST PHISHING THREATS,** such as missed Business Email Compromises (BECs)
- **SPECIFIC ATTACK GROUPS** targeting your organization and Indicators of Compromise
- **MOST TARGETED INDIVIDUALS** in your organization
- **RECOMMENDATIONS** to strengthen your domain configuration and email security



Contact us today to schedule your complimentary Phishing Risk Assessment.

A sample assessment report is available upon request.

CLOUDFLARE
AREA 1 SECURITY

Microsoft Partner
Microsoft

Partner of the Year
Google Cloud

HORIZON PHISHGUARD™

Managed Email Security and Active Fraud Defense

PROBLEM

- Email-based phishing attacks represent the No.1 vector for perpetrating cyber fraud.
- Security teams lack sufficient resources and time to monitor and respond to increasing user-submitted suspicious email reports and actual phishing incidents.

SOLUTION

- Area 1 Security's Horizon PhishGuard managed email security provides dedicated resources for end-to-end phish and targeted attack management and response.
- Our Active Fraud Defense services provide customized notification and responses for fraud and insider threats, as well as tailored threat hunting for your email environment.

Email-based cyber fraud has an immediate and direct financial impact to business and operations. Phishing, and Business Email Compromise (BEC) attacks in particular, has proven expressly expensive for victims. According to the FBI, BEC losses totaled more than $26 billion between 2016 and 2019 and made up over 40% of all internet crime-related losses in 2019.

Most modern financial fraud is initiated through email. Yet traditional email security is unable to stop these sophisticated, often link-less and malware-less attacks, and misses over 30% of phishing campaigns.

Many organizations do not have enough security resources to monitor and manage active fraud attempts in real time. In addition, each missed phish increases risk to end users and leads to a deluge of user-reported phish that security teams must investigate. Security teams must also be aware of stopped phish to track any targeted attacks and update their security environment or processes accordingly.

Area 1 Security's Horizon PhishGuard provides managed services to security teams, cybersecurity VARs and MSSPs for our Area 1 Horizon platform - the only preemptive Cloud Email Security solution. As part of the Horizon PhishGuard service, managed phish response and customized active fraud notifications extends Area 1 Security's expertise and resources to your own team. Horizon PhishGuard is also available to Area 1 Select and Elite Partners, as well as Area 1 MSSPs.

CLOUDFLARE
AREA 1 SECURITY

Modern Email Fraud and Business Email Compromise (BEC) — An Expensive Problem

CURRENT SECURITY CHALLENGES

ACTIVE FRAUD VIA EMAIL

Email is the #1 vector for perpetrating fraud, comprising $26 billion in losses

MISSED PHISH

Legacy email security tools miss phish

HIGH VOLUMES OF USER-REPORTED PHISH

Security awareness training result in more user-submitted phish reports

OVERLOADED SOC TEAMS

All phish must be investigated, taking up time and resources

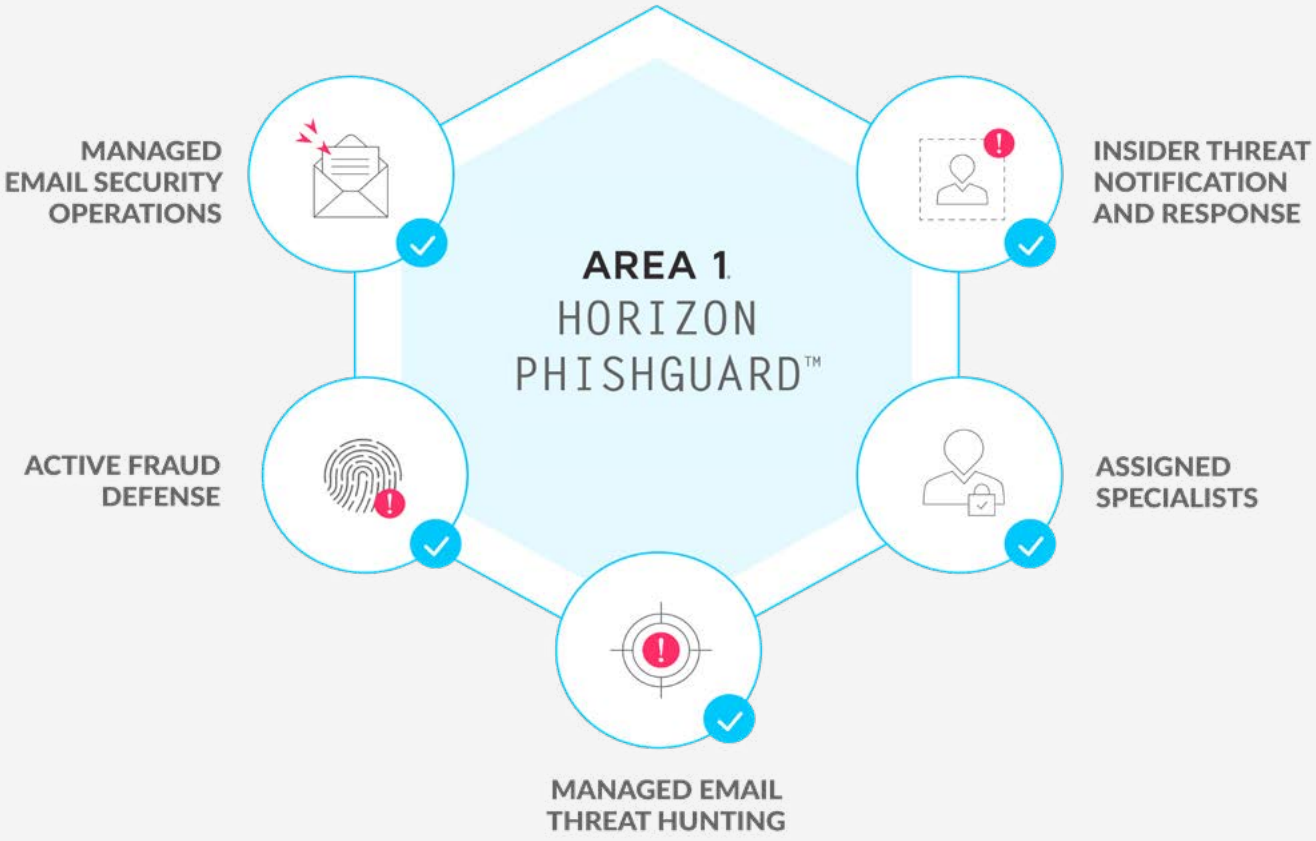
A fundamentally insecure method of communication, email is the single largest method by which modern fraud is perpetrated. With the rising popularity of cloud-based email simultaneously providing a ready-made, inexpensive and scalable infrastructure for attackers, the problem continues to exacerbate. The FBI cited BEC fraud as the most costly cyber crime, costing businesses over $26 billion in aggregate over three years.

With no industries or verticals safe, fraud conducted through email phishing is a widespread problem, requiring all hands on deck to manage. Yet organizations of all sizes are often short-handed in the security resources needed to monitor and stop fraud attempts. Security awareness programs, which are mandatory across certain industries, have also trained users to report any and all suspicious emails, resulting in SOC teams inundated with both user-reported and actual phish. All user-reported suspicious messages as well as legitimately malicious phish must be investigated, extending overall response times and filling up SOC to-do lists.

Exacerbating the challenge is the rise in BEC fraud attempts — via "long con" account compromise (Type 3 BEC) and supply chain phishing (Type 4 BEC) — all of which are missed by other defenses. These must be detected swiftly and alerts escalated so action can be taken before damage is done. Even with automation and an in-house security team, most organizations need additional help and resources to solve this problem.

CLOUDFLARE
AREA 1 SECURITY

WHAT IS HORIZON PHISHGUARD?



Area 1 Security's Horizon PhishGuard is an industry-first service for managed email security and active fraud defense.

Area 1 Horizon is the only email security platform capable of preemptively detecting and stopping phishing and targeted threats. Horizon PhishGuard builds upon our preemptive approach with actively monitored email security services including active fraud notifications, insider threat assessments and proactive email-based threat hunting.

Horizon PhishGuard extends Area 1's resources and security expertise and security expertise to enterprise security teams, cybersecurity VARs and MSSPs. Our email security service provides managed phish submission, response and quarantines for the Area 1 Horizon platform. As part of our Active Fraud Defense services, we provide proactive fraud notification so you can take action before damage is done. We'll also manage fraud response, create custom signatures for your email environment, conduct insider threat response, and perform email threat hunting. The Horizon PhishGuard service also comes with the benefit of a dedicated technical account manager and a dedicated security analyst for your organization.

CLOUDFLARE
AREA 1 SECURITY

Horizon PhishGuard™ Services and Benefits

1 MANAGED PHISH SUBMISSIONS AND RESPONSE

Manage phish submission processes, analyze suspicious messages and provide incident response within the customer email environment

2 ACTIVE FRAUD NOTIFICATIONS AND RESPONSE

Notify customers of potential fraudulent communications, automatically block and quarantine malicious BEC messages, retract confirmed malicious messages

3 INSIDER THREAT NOTIFICATIONS AND RESPONSE

Conduct insider threat notifications and provide a report of potential internal malicious behavior

4 MANAGED QUARANTINES

Manage quarantined messages based on disposition, best practices and priorly agreed-upon terms; release quarantined messages at customer's request

5 CUSTOM SIGNATURES

Create custom blocking signatures (e.g. YARA signatures) based on a threat analysis of customer environment and assist with implementation

6 EMAIL THREAT HUNTING

Investigate customer email environment and provide any indicators of compromise and campaign-specific indicators

7 ACTIVE SERVICE MONITORING

Real-time monitoring of customer email environment

8 ASSIGNED SECURITY ANALYST

Assigned security analyst for customer organization to provide periodic review of findings

9 ASSIGNED TECHNICAL ACCOUNT MANAGER

Assigned technical account manager for customer escalation and periodic customer account review

Led by our team of security researchers and analysts with security experience from the National Security Agency, Department of Defense and top security consulting firms, Horizon PhishGuard adds proactive security services to our preemptive technology suite. Scale your security team and prevent fraud targeting your organization with Area 1's Horizon PhishGuard service.

To find out more about Horizon PhishGuard™, reach out to your account team to set up a consultation.

About Area 1 Security

Area 1 Security is the only company that preemptively stops Business Email Compromise, malware, ransomware and targeted phishing attacks. By focusing on the earliest stages of an attack, Area 1 stops phish — the root cause of 95 percent of breaches — 24 days (on average) before they launch. Area 1 also offers the cybersecurity industry's first and only performance-based pricing model, Pay-per-Phish.

Area 1 is trusted by Fortune 500 enterprises across financial services, healthcare, critical infrastructure and other industries, to preempt targeted phishing attacks, improve their cybersecurity posture, and change outcomes.

Area 1 is cloud-native, a Certified Microsoft Partner, and Google Cloud Technology Partner of the Year for Security. To learn more, visit **www.area1security.com**, follow us on **LinkedIn**, or subscribe to the **Phish of the Week** newsletter.

CLOUDFLARE
AREA 1 SECURITY

Microsoft Partner
Microsoft

Partner of the Year
Google Cloud

ACTIVE FRAUD PREVENTION

Comprehensive Protection Against Phishing-related Financial Cybercrimes

PROBLEM

- Fraud and phishing attacks cause 95% of breaches and are difficult for traditional security tools to detect
- Legacy security solutions routinely miss over 30% of attack campaigns, creating more work for SOC teams

SOLUTION

- Area 1 Security is the only solution that preemptively stops phish across email, social, web and network attack vectors
- Area 1 extends protection to supply chain partners to comprehensively stop Types 1-4 BEC and active fraud in progress in progress

As cybercrime evolves, fraud — in particular phishing and business email compromise (BEC) — has risen to the top both in terms of prevalence and financial damage caused. The FBI recorded $3.5 billion in reported losses due to cybercrime in 2019. Much of this was due to financial fraud like BEC, rogue wire transfers, ransomware and spoofing. In fact, the most costly cybercrime in the U.S. was BEC, costing over $1.7 billion and making up over 40% of all internet crime related losses in 2019.

The latest forms of cyber fraud present a particular challenge to legacy email security systems. Traditional secure email gateways (SEGs) were built to handle commodity spam instead of today's targeted attacks, phish and BEC, resulting in missed detections. In fact, legacy solutions miss over 30% of attack campaigns. With 95% of breaches caused by phish, this creates a huge security gap and adds exponentially to security operation workloads.

To combat modern cybercrime, organizations need to adopt solutions with Active Fraud Prevention capabilities to comprehensively detect and stop attacks missed by SEGs.

[1] Federal Bureau of Investigation's Internet Crime Complaint Center (IC3). "2019 Internet Crime Report," Feb. 11, 2020. https://pdf.ic3.gov/2019_IC3Report.pdf

CLOUDFLARE
AREA 1 SECURITY

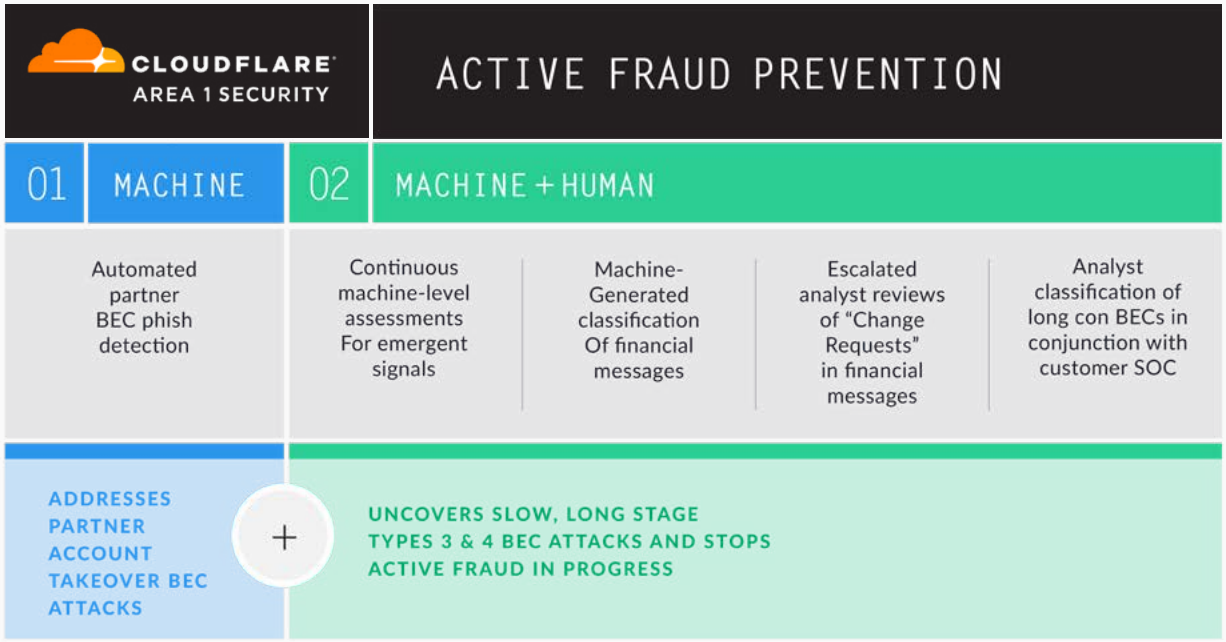
ACTIVE FRAUD PREVENTION

Stopping modern fraud attacks requires the ability to detect low-volume, targeted phish and BEC. As attackers increasingly use social engineering over malware for many of these attacks, detecting malicious intentions, even if there is no malware present, is key. Discovering fraud attempts, often conducted over a span of multiple conversations, over weeks and months, also calls for advanced machine learning algorithms.

Area 1 Security takes a machine + human approach for comprehensive Active Fraud Prevention across all threat vectors for fraud: email, social, web and network. Our approach allows us to stop all the threats anti-spam, anti-virus and advanced threat protection systems typically catch, but we also go above and beyond to preempt attacks and stop active fraud campaigns before they do harm.

In the first 12 weeks of service, Area 1 intercepted $233 million in Types 3 & 4 BEC fraud campaigns

Area 1 takes a machine + human approach to preemptively prevent phishing attacks as well as stop active fraud in progress:



Preempting attacks starts with Area 1's ActiveSensors™ for massive-scale web crawling and small pattern analytics engine (SPARSE™), which allow us to proactively discover and track attacker infrastructure. With these technologies, Area 1 is able to detect emerging attack infrastructure an average of 24 days before phishing campaigns go live.

Through our extensive research and detection of phishing campaigns, we've tracked and divided BEC evolution into three types. **Type 1 BEC** uses CXOs and display names as a lure through inter-organization impersonation. **Type 2 BEC** uses hijacked employee accounts as a lure in intra-organization impersonation. **Types 3 and 4 BEC** rely on account takeovers and spoofing of trusted supply chain partners respectively, making them the most difficult to detect and most financially damaging. Area 1 excels at detecting all four types of BEC, but we're particularly good at catching the sophisticated, long-con Types 3 and 4 BEC fraud commonly missed by legacy email security systems.

Our Active Fraud Prevention starts with Area 1's automated supply chain BEC phish detection, which addresses the vast majority of these partner account takeover-based BECs. We also take a combined machine/human approach designed to uncover the slow, drawn-out development of Types 3 and 4 BEC phish.

Area 1 conducts continuous machine level assessments of all messages for emergent signals of fraud. Messages are also auto-classified, surfacing categories of interest like financial messages. After multiple levels of machine-driven detection, we employ escalated analyst reviews of change requests in the small amount of financial messages with undetermined verdicts. Final joint confirmation with Area 1 security analysts and customer SOC teams results in precise verdicts with low false-positive rates. This process allows for scalable and accurate detections that stop active fraud campaigns in their tracks.

The methodologies and technologies we employ for preemptive and active fraud prevention can be summarized in the chart below.

1 CAMPAIGN SOURCE ANALYSIS

Preemptive crawling to discover and track attacker infrastructure

2 MESSAGE SENTIMENT ANALYSIS

Understanding what's being expressed within the message

3 PARTNER SOCIAL GRAPHING

Assessing supply chain partner reputation and vendor account takeover

4 CONVERSATIONAL CONTEXT ANALYSIS

Analyzing variations within an entire message thread for suspected fraud

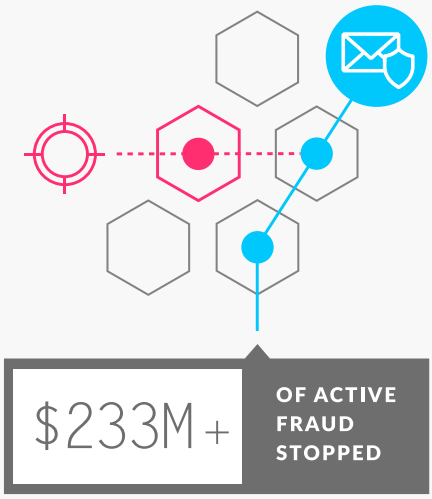
5 UNIVERSAL MESSAGE CLASSIFICATION

Surfacing Categories of Interest (COIs) for secondary assessments

6 VERDICT ESCALATIONS

Rapid escalations for analyst review and customer SOC confirmation

CLOUDFLARE
AREA 1 SECURITY



THROUGH THIS ADVANCED METHOD, AREA 1 HAS INTERCEPTED MORE THAN $233 MILLION IN TYPE 3 BEC FRAUD CAMPAIGNS TARGETING FORTUNE 500 COMPANIES IN JUST THE FIRST 12 WEEKS.

Since 2019, we have also caught more than 100 million phish missed by SEGs.

CLOUDFLARE
AREA 1 SECURITY

Area 1 Security is the only cybersecurity company able to comprehensively block phishing and fraud attacks before they do harm. To protect your organization from modern cybercrimes, try us out at ***www.area1security.com/try-area1***

About Area 1 Security

Area 1 Security offers the only pay-for-performance solution in the cybersecurity industry - and the only technology that comprehensively blocks phishing attacks before they damage your business. Phishing is the root cause of 95 percent of security breaches.

Area 1 Security works with some of the most sophisticated organizations in the world, including Fortune 500 banks, insurance companies, and healthcare providers to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture and change outcomes.

Learn more at www.area1security.com, join the conversation at @area1security or subscribe to the Phish of the Week for the latest industry news and insights on how to deal with phishing.