SOLUTION BRIEF

CLOUDFLARE
AREA 1 SECURITY

Cloudflare Area 1's PhishGuard: A Force Multiplier for CISOs and Security Teams

Integrated managed email security, insider threat hunting and fraud defense

The challenge:

Detecting sophisticated threat actors who specialize in Business Email Compromise (BEC)/Email Account Compromise (BEC/EAC), ransomware/extortion, and workstation/network compromise is extraordinarily difficult. Phishing — the no. 1 vector for perpetrating cyber attacks — is also costly and difficult to remediate. According to the FBI, exposed dollar losses due to BEC/EAC reached $43 Billion worldwide between June 2016 and December 2021[1].

Nation states also recruit highly skilled workers to obtain sensitive and/or proprietary information through highly nuanced methods, which can avoid detection and raise suspicions. Cloudflare Area 1's Insider Threat team offers years of experience identifying these activities.

Spikes in user-reported suspicious emails stretch cybersecurity resources even further. The transition to remote work has tasked cybersecurity teams with as many as double the number of incidents[2] - and many lack sufficient internal resources to proactively monitor for — and manage — fraud attempts.

The Cloudflare Area 1 PhishGuard solution:

PhishGuard acts as an immediate force multiplier for your security team and SOC to neutralize phishing campaigns before they cause damage. Free up security investigation cycles, gain valuable data for your executive team, and gain valuable threat intelligence with PhishGuard.

Cloudflare Area 1's PhishGuard works within your environment and VAR/MSSP infrastructure to provide end-to-end services that deliver:

Managed email security provides dedicated resources for end-to-end phishing and targeted attack management and response.

Insider threat program leverages custom multi-lingual ML models and detections to track nation state-sponsored intellectual property theft targeting operations and infrastructure.

Fraud defense provides customized notification and responses for BEC fraud and insider threats, as well as tailored threat hunting for your email environment.

[1] FBI Alert Number I-050422-PSA. "Business Email Compromise: The $43 Billion Scam." FBI Internet Crime Complaint Center, https://www.ic3.gov/Media/Y2022/PSA220504. Accessed 19 May 2022.

[2] Rogers, Kate and Spring, Betsy. "'We are outnumbered' — cybersecurity pros face a huge staffing shortage as attacks surge during the pandemic." CNBC, https://www.cnbc.com/2020/09/05/cyber-security-workers-in-demand.html. Accessed 25 May 2022.

Modern email fraud and Business Email Compromise (BEC) — an expensive problem

Current email security challenges

Fraud via email

Email is the #1 vector for perpetrating fraud, and BEC alone has cost organizations over $43 billion

Missed phish

Legacy email security tools and cloud email suites miss phish

High volumes of user-reported suspicious email

Security awareness training results 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 cyber fraud is perpetrated. With the rising popularity of cloud-based email simultaneously providing a ready-made, inexpensive and scalable infrastructure for attackers[3], the problem continues to challenge security professionals.

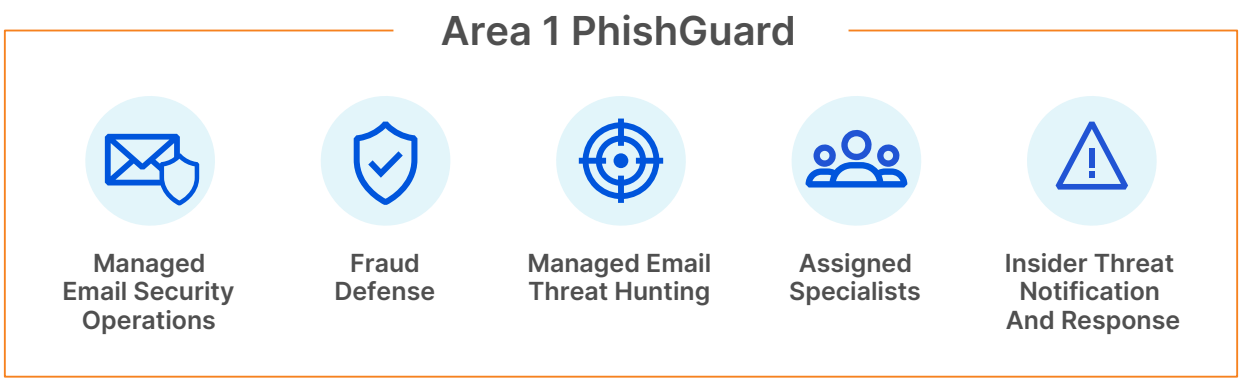
Security awareness programs, which are mandatory across certain industries, have also trained users to report any and all suspicious emails, resulting in SOC teams inundated with both user-reported and actual phish. All user-reported suspicious messages — as well as legitimately malicious phish — must be investigated, extending overall response times and filling up SOC queues.

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 often missed by legacy secure email gateways and native cloud email defenses. These must be detected early in the attack lifecycle so action can be taken before damage is done.

With no industries safe, fraud conducted through email phishing is a widespread problem, requiring all hands on deck to manage. Yet organizations of all sizes are often shorthanded in the security resources needed to monitor and stop fraud attempts.

[3] Tung, Liam. "Microsoft disrupted this large cloud-based business email scam operation." ZDNet. https://www.zdnet.com/article/microsoft-disrupted-this-large-cloud-based-business-email-scam-operation/. Accessed 10 June 2022.

The Cloudflare Area 1 PhishGuard approach



PhishGuard builds upon Area 1's unique preemptive email security approach with actively-monitored services that include fraud notifications, insider threat notifications and proactive email-based threat hunting.

PhishGuard extends our resources and security expertise to your enterprise security team, as well as cybersecurity VARs and MSSPs.

Key services include:

- Managed fraud response, custom signatures for your email environment, insider threat response, and proactive email threat hunting
- Proactive fraud/BEC notifications so your organization can take action early in the attack lifecycle
- Managed phish submission, response and quarantines for the Area 1 email security platform

Cloudflare Area 1 PhishGuard features and benefits

- **Managed phish submissions and response**
  Manage phish submission processes, analyze suspicious messages and provide incident response within the customer email environment
- **Active fraud notifications and response**
  Notify customers of potential fraudulent communications, automatically block malicious BEC messages and retract confirmed malicious messages
- **Insider threat notifications and response**
  Conduct insider threat notifications and provide a report of activities warranting further investigation
- **Active service monitoring**
  Real-time monitoring of customer email environment
- **Custom signatures**
  Create custom blocking signatures (e.g. ML, YARA signatures) based on a threat analysis of customer environment and assist with implementation
- **Email threat hunting**
  Investigate customer email environment; provide any indicators of compromise and campaign-specific indicators and identify new/novel attacks
- **Assigned security analyst**
  Assigned security analyst for customer organization to provide periodic review of findings
- **Assigned technical account manager**
  Assigned technical account manager for customer escalation and periodic customer account review

Led by a team of researchers and analysts with security experience from the National Security Agency, Department of Defense and top security consulting firms, PhishGuard adds proactive security services to our preemptive email security technology.

Scale your security team and prevent fraud targeting your organization with Cloudflare Area 1's PhishGuard service. To learn more, reach out to your account team or contact area1sales@cloudflare.com.