AREA 1

Microsoft Partner

Microsoft

Partner of the Year

Google Cloud

CLOUD EMAIL SECURITY

Harden your Office 365 and Gmail security with total anti-phishing protection

PROBLEM

- Targeted phishing attacks are still breaching Office 365 and Gmail defenses
- Gateway-based architectures aren't built to handle cloud-based environments, missing phish as a result

SOLUTION

- **Best-of-breed cloud email attack prevention** against BEC, credential harvesting, ransomware and other threats
- **Cloud-native application that scales** with your environment - no hardware, no constant "tuning" to keep up with threats

SOLUTION OVERVIEW

Even as the cloud delivers phenomenal productivity advantages, it also delivers a menacing security gap in the form of vulnerability to phishing campaigns.

Over 95 percent of cybersecurity damages begin with a phishing attack. This phishing epidemic costs billions — $1.7 billion was lost in 2019 due to Business Email Compromise (BEC) alone — damaging organizations' brand image, confidential data, and even their financial solvency.

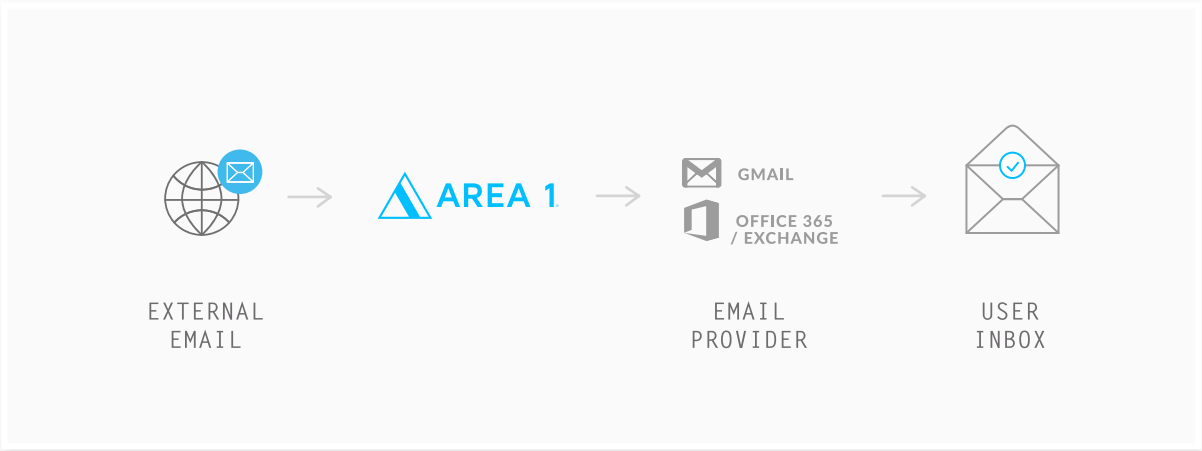
The defenses arrayed against attacks by both Office 365 and Gmail are proving inadequate to the mission, and regularly fail to stop phish. Gmail and Office 365 spam filters are not architected to proactively hunt or even recognize linkless, file-less phish such as BEC.

At the same time, secure email gateways (SEGs) with their box-first and hosted architectures aren't designed to handle the scalability and performance requirements of their cloud email provider counterparts. And their constant "tuning" requirements cost security teams time and security leaders money.

Area 1 Security's cloud-native service continuously and proactively seeks out phishing campaigns and infrastructure before they hit inboxes — far and away the most effective defense strategy.

AREA 1

Deployed in minutes, Area 1 Security exposes and stops emerging phishing threats:



Phishing continues to be such a serious challenge that Gartner has called out BEC and phishing as a top security project even after adopting basic security measures. Furthermore, Gartner cautions in its Market Guide for Email Security that legacy email security vendors often fail to innovate at the speed of attackers or fail to deploy updated versions in time.

Area 1 Security's cloud-based and preemptive solution overcomes these challenges. Area 1 proactively discovers and blocks advanced threats and phishing attacks. Its completely cloud-based platform means all customers always get the latest protections against threats.

Area 1 integrates quickly with email providers and existing security systems like security information event management solutions (SIEMs). With flexible deployment options, Area 1 can be deployed inline or in BCC or journaling mode without affecting existing infrastructure.

As a cloud-native service, deployment can be completed in a matter of minutes. By fortifying existing email providers' baseline security, Gmail and Office 365 users can be confident that phishing campaigns will be preemptively neutralized.

On average, Area 1 discovers malicious sites and payloads under construction a full 24 days or more before they launch, preemptively analyzing attacks and blocking them from employee inboxes. While the defenses of email providers and SEGs work against spam and known email viruses, only Area 1's preemptive model can deal effectively with the growing spectrum of targeted phishing attacks.

AREA 1

Area 1 Horizon Anti-Phishing Service

Your Cloud Email Security Partner

1 BEST-OF-BREED ATTACK PREVENTION

Phishing, targeted attacks, BEC, ransomware, spam, virus, backscatter attacks, etc.

2 QUICK VISIBILITY & DEEP CONTEXT

Rapid-scale message tracing & detections search; industry's fastest indexing and retrieval rate

3 OPERATIONAL SIMPLICITY & CLOUD NATIVE

Cloud-first, API-first architecture with deep hooks into existing operational tools & playbooks

4 ENTERPRISE-GRADE EMAIL HYGIENE

Enforce inbound TLS, email authentication, and partner communications policies

5 MULTI-MODE DEPLOYMENTS

Flexibility with inline or out-of-band modes; API / connector for easy search and retrievals

6 HIGH SCALE CLOUD MTA

On-demand scalability with the highest levels of service assurances & adaptive message pooling

Area 1's proactive monitoring of threat actor activity, combined with our 6.4+ PB attack data warehouse, enables continuous protection against the most ingenious campaigns. The Area 1 service updates and enhances machine learning detection at the pace of threat actor evolution, critically bolstering and refining your defenses. We dynamically analyze suspicious web pages and payloads, continuously adapting to new bad-actor tactics.

Unlike SEGs, Area 1 is specifically built to perform complex phishing campaign deconstructions, such as imposter analysis and conversational context analysis, and is the industry's best phish-blocking engine.

AREA 1

Do phishing attacks continue to land in your Office 365 and Gmail inboxes?
To see what Area 1 catches that your email providers miss, visit ***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.