

# 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.

# 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 phishing



### HIGH VOLUMES OF USER-REPORTED PHISH

Security awareness training result in more user-submitted phishing reports



### OVERLOADED SOC TEAMS

All phishing must be investigated, taking up time and resources

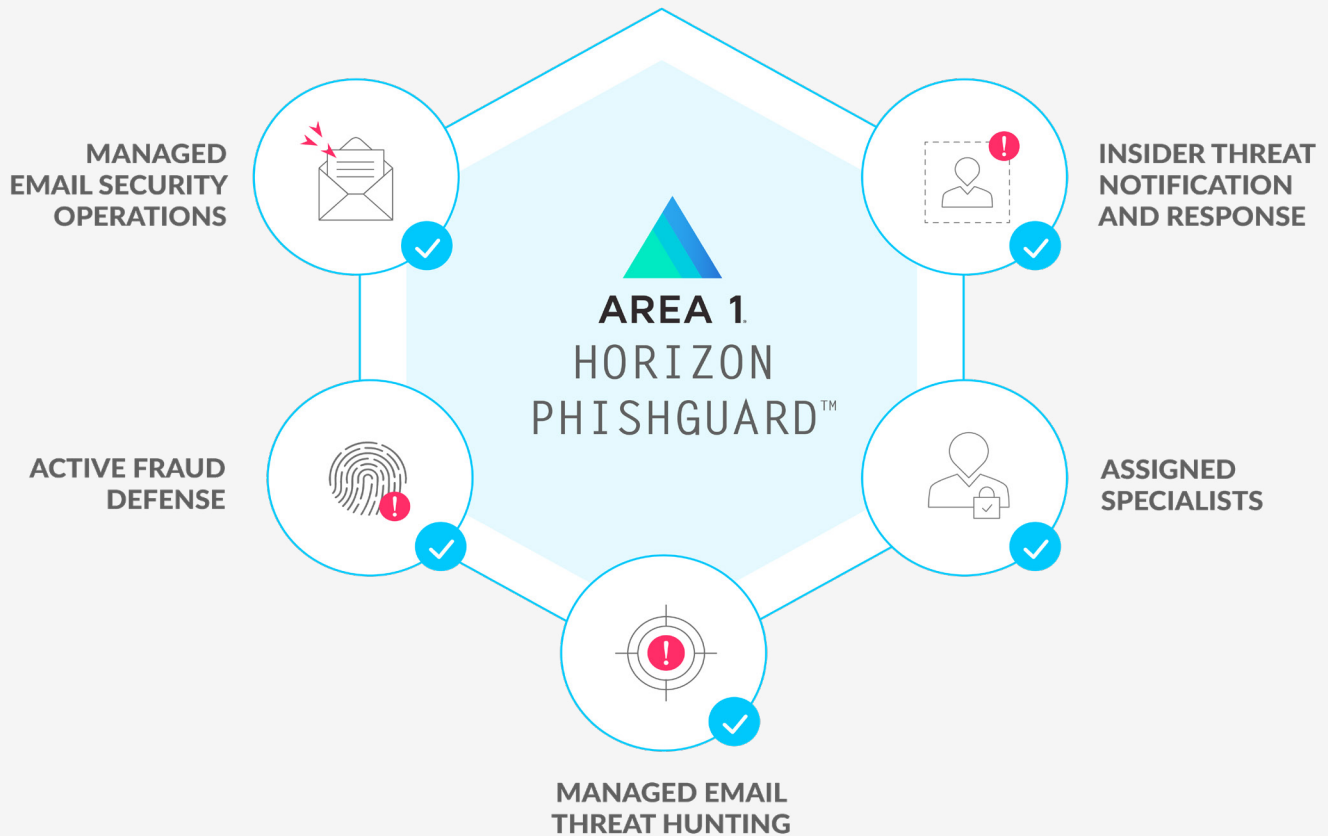
A fundamentally insecure method of communication, email is the single largest method by which modern fraud is perpetrated. With the rising popularity of cloud-based email simultaneously providing a ready-made, inexpensive and scalable infrastructure for attackers, the problem continues to exacerbate. 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 phishing. All user-reported suspicious messages as well as legitimately malicious phishing 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.

## 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.

## Horizon PhishGuard™ Services and Benefits

<p><b>1</b> <b>MANAGED PHISH SUBMISSIONS AND RESPONSE</b></p> <p>Manage phish submission processes, analyze suspicious messages and provide incident response within the customer email environment</p>	<p><b>2</b> <b>ACTIVE FRAUD NOTIFICATIONS AND RESPONSE</b></p> <p>Notify customers of potential fraudulent communications, automatically block and quarantine malicious BEC messages, retract confirmed malicious messages</p>	<p><b>3</b> <b>INSIDER THREAT NOTIFICATIONS AND RESPONSE</b></p> <p>Conduct insider threat notifications and provide a report of potential internal malicious behavior</p>
<p><b>4</b> <b>MANAGED QUARANTINES</b></p> <p>Manage quarantined messages based on disposition, best practices and priorly agreed-upon terms; release quarantined messages at customer's request</p>	<p><b>5</b> <b>CUSTOM SIGNATURES</b></p> <p>Create custom blocking signatures (e.g. YARA signatures) based on a threat analysis of customer environment and assist with implementation</p>	<p><b>6</b> <b>EMAIL THREAT HUNTING</b></p> <p>Investigate customer email environment and provide any indicators of compromise and campaign-specific indicators</p>
<p><b>7</b> <b>ACTIVE SERVICE MONITORING</b></p> <p>Real-time monitoring of customer email environment</p>	<p><b>8</b> <b>ASSIGNED SECURITY ANALYST</b></p> <p>Assigned security analyst for customer organization to provide periodic review of findings</p>	<p><b>9</b> <b>ASSIGNED TECHNICAL ACCOUNT MANAGER</b></p> <p>Assigned technical account manager for customer escalation and periodic customer account review</p>



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](http://www.area1security.com), follow us on [LinkedIn](#), or subscribe to the [Phish of the Week](#) newsletter.