

SOLUTION BRIEF

Agari Phishing Defense™

Eliminate Advanced Email Attacks that Bypass Existing Defenses

New and emerging email threats employ identity deception to easily bypass existing security controls such as secure email gateways, sandbox environments, URL rewriting processes, and imposter classifiers. These technologies are predicated on a failed security paradigm of attempting to model known bad signals, whether by volume, static sender identities, or content.

Anatomy of a Business Email Compromise Attack

Received: from smtp relay.b.hostedemail.com
From: Shelly Jones (CFO) <shelljones@mailbox.com>
Subject: Fwd: Wire Payment
To: Donna Lessig <donna.lessig@bankdomain.com>

Donna,

Are you able to process an international wire before cutoff?
Details below. Please let me know when it's done.

Shelly

-----Original Message-----

Subject: Wire Transfer
From: Martha Long <marth.longg@bankdomain.com>
To: Donna Lessig <donna.lessig@bankdomain.com>

Donna,

As we discussed earlier, I've attached the wiring instructions for the \$1.2M payment. This is urgent and has Jamie's approval. I'll provide you with the supporting material later.

Martha Long

- 1 Message originates from public cloud server with no negative sending history.
- 2 Sender uses display name deception or domain spoofing.
- 3 Socially engineered spoofed content suggests a history of prior interaction and approval.
- 4 Lack of active payload prevents detection by traditional content-based or sandboxing approaches.

Attackers know they can easily evade these protections by impersonating trusted individuals, partners, or brands while avoiding the use of malicious content. This is why Agari Phishing Defense takes a different approach—modeling the email-sending behavior of all legitimate senders across the Internet. By combining advanced machine learning techniques, Internet-scale telemetry, and real-time data pipelines, this method allows only email from your organization's unique set of trusted customers, partners, and employees to be received. With Agari, you escape the legacy approaches that simply can't react fast enough to stop the newest types of attacks.

AT A GLANCE

Agari Phishing Defense stops phishing, BEC and other identity deception attacks that trick employees into harming your business.

BENEFITS

Stop business email compromise from tricking unsuspecting employees and partners.

Prevent impersonation of your CEO and other high-profile executives.

Detect account takeovers before they result in financial or information loss.

Block brand impersonations from being used in credential phish attacks.

THE AGARI ADVANTAGE

The Agari Identity Graph™ uses predictive science to model trustworthy communications, based on 300+ million daily updates.

Best-in-class BEC protection combines advanced display name protection, and look-alike domain detection to stop attacks.

Partner fraud prevention models supply chain partners, auto-generating and continuously updating policies to prevent fraud.

Account takeover ID models ATO threat behavior to block attacks originating from compromised email accounts.

Intelligent content inspection integrates signature-less, URL, and file analysis to detect malicious content that evades SEGs and other legacy systems.

Email forensics and enforcement provides customizable policies to enforce actions or report malicious activity to security operations teams.

Continuously protect your organization with human vetted threat intel combined with proven predictive modeling continuously protect your employees.

Microsoft hybrid support secures mailboxes in Microsoft 365 and Exchange on-premises through a single administration console.

Detecting Deception With Machine Learning

Agari Phishing Defense, powered by the Agari Identity Graph™, leverages three phases of machine learning modeling:

IDENTITY MAPPING

Determines which identities the recipient perceives is sending the message.

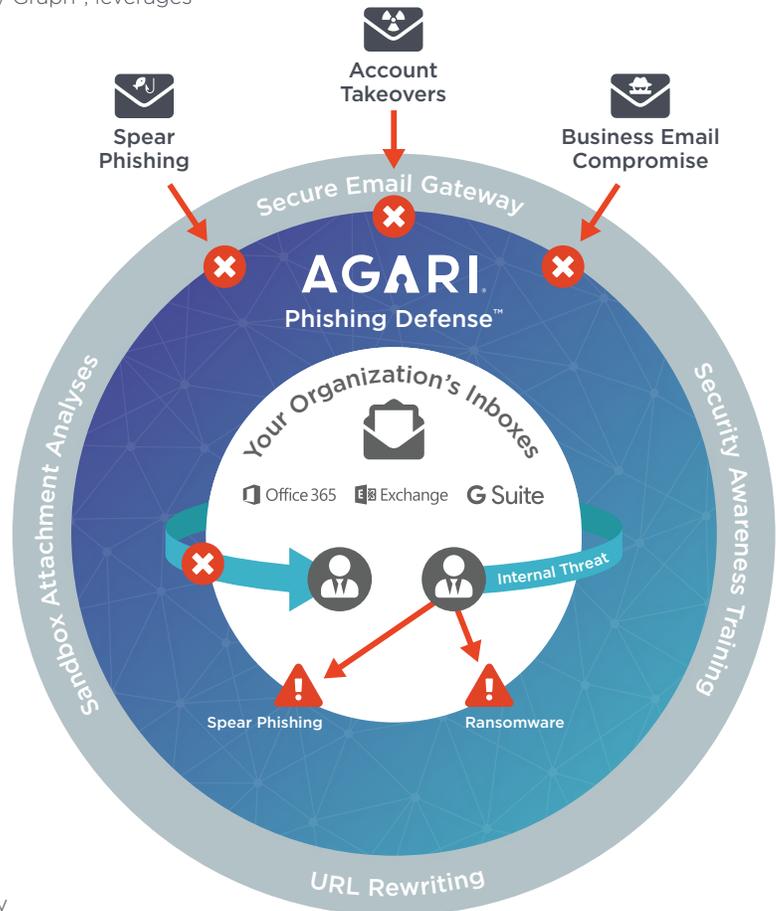
BEHAVIOR ANALYTICS

Based on the perceived identity, analyzes the expected sending behavior for anomalies relative to that identity.

TRUST MODELING

Measures relationships to determine expected sending behavior; highly engaged relationships (such as between coworkers) have strict behavioral anomaly thresholds since they have higher overall risk if spoofed.

By incorporating each phase, the final Identity Graph score determines whether the message should be accepted. Those that are accepted are delivered to the inbox, while malicious emails are filtered out.



Remove Latent Threats, Even After Delivery

Agari Continuous Detection and Response technology brings together Agari Phishing Defense and Agari Phishing Response™ to automatically remove latent email threats and provide visibility into the attack blast radius. The technology takes threat intelligence sourced from the world's top SOC teams, the Agari Cyber Intelligence Division (ACID), and best-of-breed threat intelligence feeds to search for indicators of compromise (IOCs) in employee inboxes and then remove them in order to prevent or mitigate data breaches.

Simultaneously Scan Incoming, Outgoing, and Internal Employee-to-Employee Traffic

Agari Phishing Defense deploys as a lightweight sensor via the cloud or on-premise.

- 1 Sensor receives a copy of all incoming, outgoing, and internal messages within your email environment.
- 2 Leveraging the Agari Identity Graph, Agari Phishing Defense scans and determines if the message is untrusted.
- 3 Pre-configured policies immediately block or redirect the message for further incident investigation.

The Company We Keep

Top 3 Social Networks | 6 of the Top 10 Banks | Top Cloud Providers



© 2021 Agari Data, Inc. All rights reserved.
Agari, Secure Email Cloud, Agari Identity Graph, Agari Phishing Defense, Agari Brand Protection, Agari Phishing Response, Agari Active Defense and the Agari logo are trademarks of Agari Data, Inc.
v12.01.14.21

[Learn More: www.agari.com/products](http://www.agari.com/products)