



## ENTERPRISE PROTECT

The only solution that stops targeted email attacks by determining the authenticity of every in-bound email

### What Sets Us Apart

- › Evaluates risk associated with every in-bound email by assessing its authenticity, i.e., did it come from where it purports to come from?
- › Uses proprietary Agari Email Trust Platform and associated global email telemetry data, a cloud-based Big Data analytics approach to predictive threat detection
- › Creates a unique sender model for every sender domain encountered, both globally and specific to your organization
- › Does not depend on presence of suspect embedded URLs, potentially malevolent attachments, or reputation scores from third parties

Agari Enterprise Protect relies on our unique Agari Email Trust Platform™ and proprietary global email telemetry data to detect low-volume, targeted email attacks that go undetected by existing email security systems. It is an essential complement to your extant cyber-security infrastructure, and guards your organization against today's most sophisticated and insidious email-based attacks—those crafted to target specific individuals, collectively known as “spear phishing.”

### WHY YOU NEED AGARI ENTERPRISE PROTECT

All phishing attacks are based on identity deception. Criminal methods have evolved to the point at which they are capable not only of convincingly spoofing trusted brands, but impersonating specific individuals within them - letting attackers gain the trust of individuals within your organization. Indeed, some of the most nefarious and successful spear phishing attacks have impersonated CEOs or CFOs of the same company of the attacked employee.

The diagram shows an email header and body with four numbered callouts:

- 1** Message originates from public cloud server with no negative sending history (points to the 'Received' line: from smtprelay.b.hostedemail.com)
- 2** Sender can use a real address or look-alike (points to the 'From' line: Traci Wheeler <traci.wheeler@jpmchase.com>)
- 3** Socially engineered spoofed content suggests a history of prior interaction and approval (points to the 'From' line of the 'Original Message' block: From: Marianne Lake marianne.lake@jpmchase.com)
- 4** Lack of active payload prevents detection by traditional content-based or sandboxing approaches (points to the 'Subject' line of the 'Original Message' block: Subject: Wire Transfer)

**Email Header:**

```
Received: from smtprelay.b.hostedemail.com
From: Traci Wheeler <traci.wheeler@jpmchase.com>
Subject: Fwd: Wire Payment
Date: Mar 30, 2015 9:03PM EDT
To: Tamara Lawson <tamara.lawson@jpmchase.com>
```

**Body:**

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

----- Original Message -----  
Date: Mar 30, 2015 7:30  
Subject: Wire Transfer  
From: Marianne Lake marianne.lake@jpmchase.com  
To: Traci Wheeler traci.wheeler@jpmchase.com

Traci,  
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.  
Marianne Lake

## SIMPLY THE BEST

Agari Enterprise Protect is simply the best spear phishing defense available because it:

- Can identify suspicious emails coming from apparently reputable sources even on first attacks of the most sophisticated, socially engineered kind, with a high degree of accuracy and reliability
- Improves continuously over time as it models your organization's unique inbound traffic patterns and mix of correspondence from partners, vendors, and customers
- Is the only solution that works by evaluating the sender's authenticity and determining the level of risk associated with any given email

These attributes combine to make Enterprise Protect an essential element in any cyber-defense infrastructure, in addition to any other defensive systems that have been deployed.

## DEPLOYING AGARI ENTERPRISE PROTECT

Enterprise Protect works with hosted or on-premises email infrastructure, including with Gmail, Microsoft O365, and industry-leading secure email gateways. A SaaS portal provides control and reporting. A lightweight data Collector is deployed on-premises or hosted in your or Agari's cloud.

## GET STARTED TODAY!

The best time to protect your organization from spear phishing with Agari Enterprise Protect is today. Engage in a no cost Proof-of-Value demonstration. To get started, contact your Agari Sales Representative or Sales Engineer.

Agari Enterprise Protect provides visibility and insights into risk

