AGARI

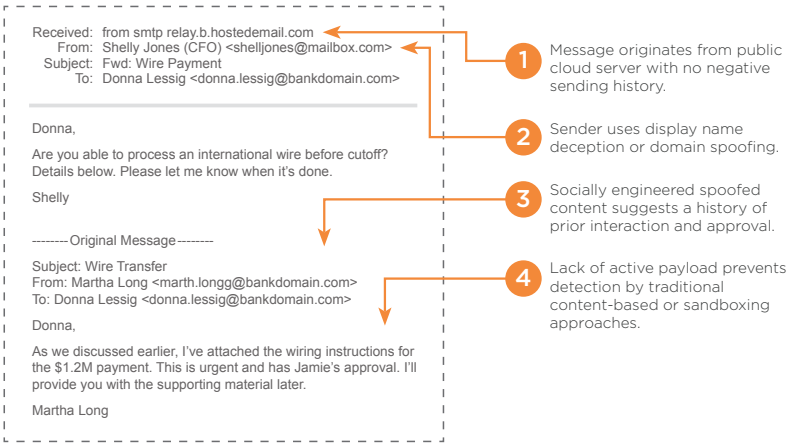
SOLUTION BRIEF

Agari Advanced Threat Protection™

Eliminate advanced email attacks that bypass existing defenses.

Modern Email Attacks Rely On Identity Deception

Anatomy of a Business Email Compromise Attack



Why Your Secure Email Gateway Needs Agari

Modern and sophisticated identity-based email attacks are easily bypassing existing security controls such as Secure Email Gateways, attachment sandboxing, URL rewriting, and imposter classifiers. These technologies are predicated on a failed security paradigm of attempting to model known bad signals, whether by volume, sender identity, or content.

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 Advanced Threat Protection 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 Advanced Threat Protection stops 99.987% of all advanced email threats including business email compromise, executive spoofing, and account takeover-based attacks.

BENEFITS

Stop business email compromise from tricking unsuspecting employees.
Prevent impersonation of your CEO and other executives.
Detect account takeovers before they result in financial or information loss.
Block zero-day attacks from becoming a serious problem for your organization.

THE AGARI ADVANTAGE

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

Best-in-class BEC protection combines Rapid DMARC, 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 trusted partner fraud.

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

Intelligent content inspection combines AI-based impersonation analysis, URL, and file analysis to detect malicious content that evades SEGs.

Email forensics and enforcement provides customizable policies to enforce actions or report malicious activity to Security Operations teams via automated alerts or API integration.

Detecting Deception With Machine Learning

Agari Advanced Threat Protection, 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 tighter 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.

Continuous Detection and Response

Agari's continuous detection and response technology brings together Agari Advanced Threat Protection and Agari Incident 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 intel feeds to search for indicators of compromise (IOCs) in employee inboxes and then remove them in order to prevent or mitigate data breaches.

Agari Advanced Threat Protection Deployment

Agari Advanced Threat Protection deploys as a lightweight sensor via the cloud or on-premise.

1. Sensor receives all messages considered clean by the Secure Email Gateway.
2. The Agari Identity Graph determines if the message is malicious, based on the criteria identified above.
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

Microsoft HSBC aetna facebook citi CHASE Google

Learn More: www.agari.com/products