DATASHEET

ENTERPRISE PROTECT

Eliminate advanced email attacks that bypass existing Secure Email Gateways

AT A GLANCE

Agari Enterprise Protect is the next-generation advanced threat protection solution that uses identity-based threat detection with machine learning to stop advanced attacks.

TARGETED EMAIL THREAT PROTECTION

- Identity Deception
- Spear Phishing
- Ransomware
- Business Email Compromise

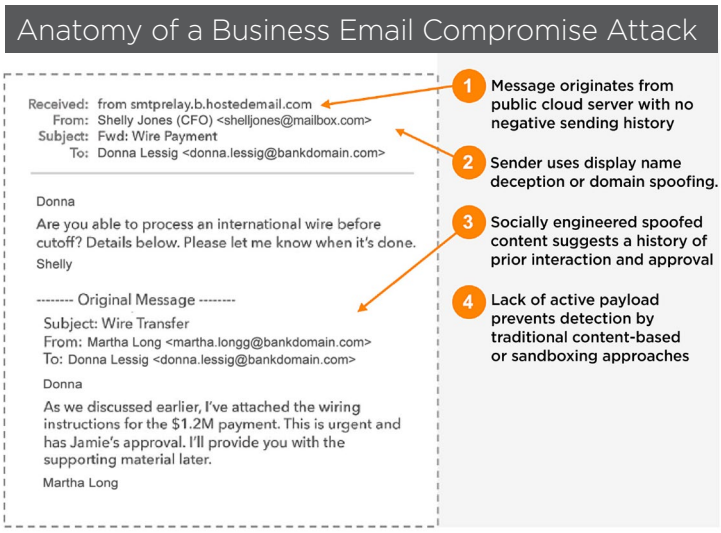
HOW WE'RE DIFFERENT

- **Identity Intelligence –** The only solution that automatically and reliably detects all three forms of identity deception (display name deception, domains spoofing, and look-alike domains) to stop advanced email attacks.
- **Beyond "Imposter Classifiers" –** Applies Rapid DMARC, identity mapping, trust modeling, and behavior analytics to identify trusted email communication between employees and external entities.
- **Unique Global and Local Visibility –** Leverages insights from an organization's local traffic, DMARC authentication data, and Agari's Trust Analytics built on massive, Internet scale data sets including over 2 trillion emails yearly.
- **Cloud-native Architecture –** Built from the ground up to leverage the scale and efficiency of cloud email.
- **Flexible Deployment –** Fortifies all cloud-based and on-premise secure email gateways.

"Advanced threats (such as ransomware and business email compromise) are easily bypassing the signature-based and reputation-based prevention mechanisms that a secure email gateway (SEG) has traditionally used."

Gartner (ID:G00320003)

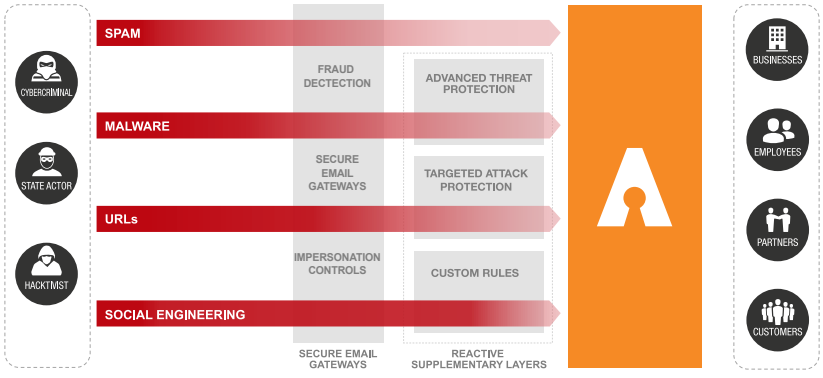
MODERN EMAIL ATTACKS RELY ON IDENTITY DECEPTION



The most damaging and successful attacks impersonate key executives targeting their own employees

YOUR SECURE EMAIL GATEWAY NEEDS AGARI

Low-volume, targeted email attacks are easily bypassing existing secure email gateways and their added layers, such as cloud-based sandboxing, URL rewriting, impersonation controls, and more. These technologies attempt to stop attacks by looking for malicious content within the message body, attachment, and URLs or comparing messages against reputation-based databases. Unfortunately, attackers can easily evade these protections by impersonating trusted individuals, partners or brands and avoiding the use of malicious content. Agari Enterprise Protect takes a different approach. We focus on stopping identity deception, which is part of every advanced email attack. Using multiple machine learning models that integrate identity mapping, trust modeling, and behavioral analytics linking the Internet's infrastructure, DMARC authentication data, and local sender/recipient associations. We allow only email from your unique set of trusted customers, partners, and employees to be received. With Agari, you escape the legacy approaches that can't react fast enough to stop the most advanced attacks.



HOW WE DO IT

Detecting Deception with Machine Learning

Agari Enterprise Protect uses multiple patented machine learning models that integrates:

- **Identity Mapping:** Extracts perceived user or brand identity and maps to an existing model
- **Trust Modeling:** To determine sender-receiver relationships and risk tolerance threshold for anomaly detection
- **Hierarchical Behavior Analytics:** To detect deception anomalies based on local and global machine learning models of expected behavior

Based on this Identity Intelligence, Enterprise Protect can accurately and effectively stop advanced attacks with no user intervention.

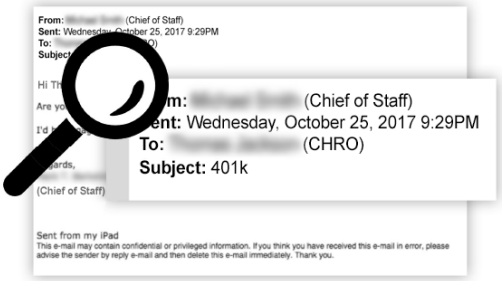
ENTERPRISE PROTECT IN ACTION

Customer: Top healthcare provider

Defenses: Proofpoint Gateway with Targeted Attack Prevention

Attacker Goal: Gain access to victim's 401k account

Tactic: Sent carefully crafted email from Chief of Staff to CHRO. Correct display name, no malicious attachments or links



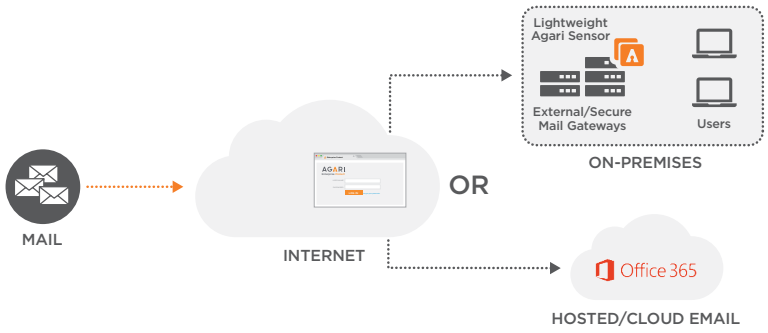
Caught by Secure Email Gateway?
NO

Caught by Targeted Attack Prevention?
NO

Caught by Agari?
YES

ENTERPRISE PROTECT DEPLOYMENT

- Lightweight sensor deploys in cloud or on-premise
- Search and Destroy can delete messages from the inbox for breach prevention or copy emails for forensic analysis
- Agari Trust Analytics determines whether message is trusted or untrusted
- Admin can log into portal or integrate via RESTful API for access to alerts and forensic intelligence



THE COMPANY WE KEEP

Top 5 social networks | 6 of the top 10 Banks | Top cloud providers

