SOLUTION BRIEF

AGARI

SECURE OFFICE 365 WITH AGARI

Accelerate your move to the cloud by protecting against advanced email attacks

OVERVIEW

As you move to Office 365, secure your email with the next generation of Advanced Threat Protection for email. Leveraging global telemetry sources, unique algorithms, and a real-time scoring pipeline to continuously model email sending and receiving behaviors across the Internet, detecting the new attacks of today and even more sophisticated ones of tomorrow.

HOW AGARI SECURES OFFICE 365

1. Integrates seamlessly with O365 via journaling or routing policies to scrutinize every message considered clean by Exchange Online Protection
2. Subjects each message to multiple phases of identity, behavioral, and trust modeling to expose the true identity and trustworthiness of the message
3. Empowers security teams to customize policies for high risk executives leveraging Azure Active Directory while enforcing protections via O365 mailbox APIs
4. Finally, fortifies EOP as a secondary antispam layer to stop missed spam attacks

AGARI STOPS

- Business Email Compromise
- Account Takeover-based Attacks
- Ransomware
- Spear Phishing

"Agari Enterprise Protect is the most granular Business Email Compromise solution I have seen"

Email Security Administrator, Fortune 1000 Organization

The benefits of moving to Office 365—easily communicate and collaborate inside and outside of the organization while working anywhere from any device at any time—are well known. However, along with the convenience of a highly available and easily accessible environment comes an increased security risk. Email is the preferred cyber-crime attack vector and the entry point for 95% of the world's breaches[1]. While Office 365 provides good enough security to stop spam, known viruses or malware, it won't secure you against today's modern, sophisticated identity-based attacks such as Business Email Compromise (BEC) or Account Takeover (ATO).

THE IDENTITY DECEPTION GAP

Advanced attacks such as Business Email Compromise and Account Takeover-based attacks continue to be a leading way attackers are bypassing Secure Email Gateways (Exchange Online Protection included). In fact, during the 2nd half of 2017, over 96% of organizations were targeted by a BEC attack[2]. Unfortunately, the majority of these attacks targeted O365 organizations and cybercriminals would have succeeded had it not been for Agari. To stop these attacks a new model focused on determining sender trust and message authenticity is required, of which O365 security was never designed for.

Exchange Online Protection (EOP) works best for:

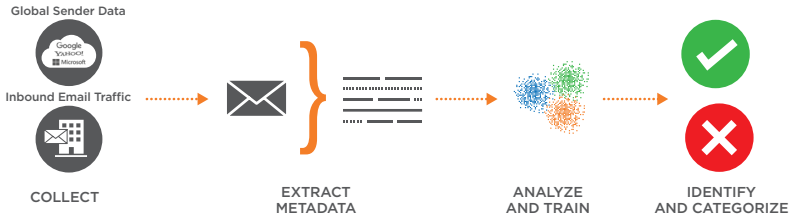
- ✓ Stopping new and existing spam attacks
- ✓ Stopping well-known or commonly used viruses and malware
- ✓ Managing unwanted or unsolicited bulk email such as newletters or marketing campaigns
- ✓ Managing email routing or quarantine policies to keep the inbox organized

Agari fortifies EOP by:

- ✗ Enforcing and managing Email Authentication policies such as DMARC, SPF, and DKIM
- ✗ Keeping employees productive by stopping today's sophisticated identity-based attacks such as BEC or ATOs
- ✗ Reducing Security Operational load by providing visibility and confirmation that attacks have been prevented
- ✗ Extending protection to trusted partners with insights into which senders have been compromised

DETECTING DECEPTION WITH MACHINE LEARNING

Agari Enterprise Protect leverages Agari Identity Intelligence™ (AI²), an advanced artificial intelligence and machine learning system that ingests data telemetry from more than two trillion emails per year to model email senders' and recipients' identity characteristics, behavioral norms, and personal, organizational, and industry-level relationships specifically focused on detecting the sophisticated identity deception attack.

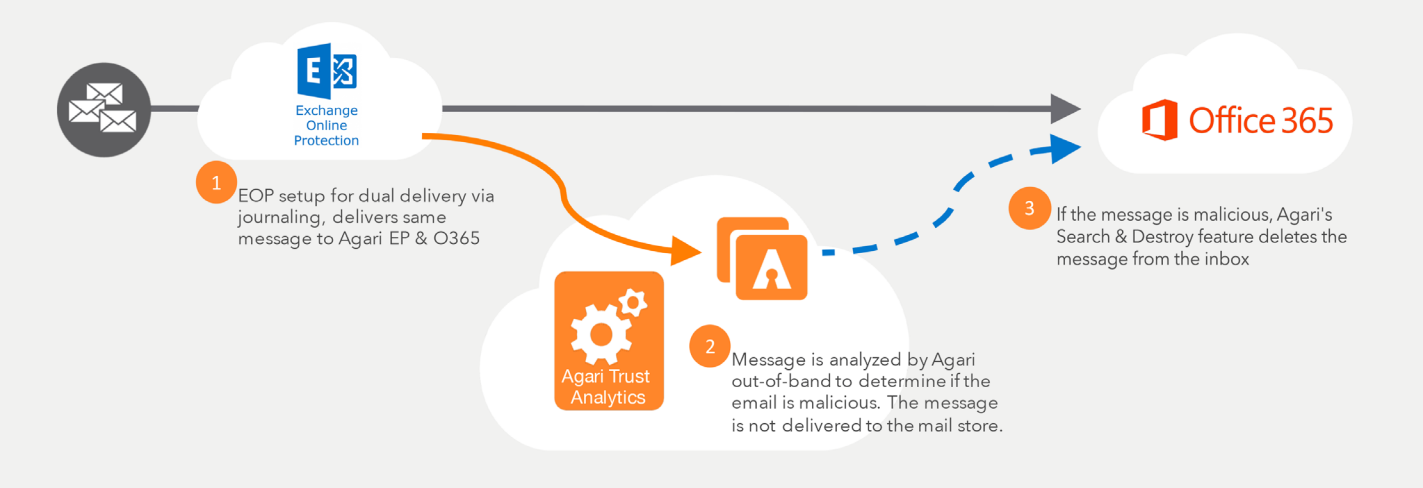


ANTI-PHISHING & ANTI-SPOOFING DETECTION COMES UP SHORT

As Microsoft finally adds Anti-Phishing and Anti-Spoofing protection, both centered around BEC, cybercriminals are shifting tactics. Based on a recent Osterman Survey, nearly half of the respondents were victims of a targeted attack that originated from a compromised account[3], making this attack technique the most effective. Anti-Phishing & Anti-Spoofing will not detect this attack because the email originates from a previously-established credible account, where deception is not needed. Agari has built this behavioral model directly into the core Identity Intelligence™ engine, making it possible to detect and prevent Account Takeover-based email attacks.

SEAMLESS INTEGRATION WITH NO ADDED OPERATIONAL BURDEN

Agari Enterprise Protect deploys hidden behind EOP providing attackers no indication as to how O365 is protected. EP integrates via journaling or routing policies to ensure zero delivery delays . Finally integration with Azure Active Directory and O365 Mailbox APIs empowers Security personnel to enforce prevention regardless of organizational changes.



TRUSTED, PROVEN, AND SCALABLE

The fundamental goal of Agari is to model the real-time email-sending behavior of all legitimate senders across the Internet. Using Internet-scale sources of email telemetry, patented algorithms, and a real-time scoring pipeline, the system continuously updates multiple individual, organizational, and class-based behavioral models that allow it to uniquely determine the trustworthiness of current and emerging forms of identity-based attacks

Telemetry from over two trillion emails per year

Over 300 million machine learning model updates per day

Insights from over 3 billion global inboxes

Analysis of over 50,000 domains daily

Contact Agari to start a free trial of Enterprise Protect on Office 365 at www.agari.com/free-trial

[1]Verizon , "2017 Data Breach Report"
http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf

[2] Agari Business Email Compromise Attack Trends Report, Jan. 2018

[3]"Best Practices to Protecting Against Phishing, Ransomware and BEC