

## SOLUTION BRIEF

# Secure Office 365 with Agari

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

The benefits of moving to Office 365—easily communicating and collaborating 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 cybercrime attack vector and the entry point for 96% of the world’s breaches<sup>1</sup>. While Office 365 provides 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 continue to be a leading way attackers are bypassing the Secure Email Gateway (Exchange Online Protection included). In fact, during the 2nd half of 2017, over 96% of organizations were targeted by a BEC attack<sup>2</sup>. Unfortunately, the majority of these attacks targeted O365 organizations. 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:

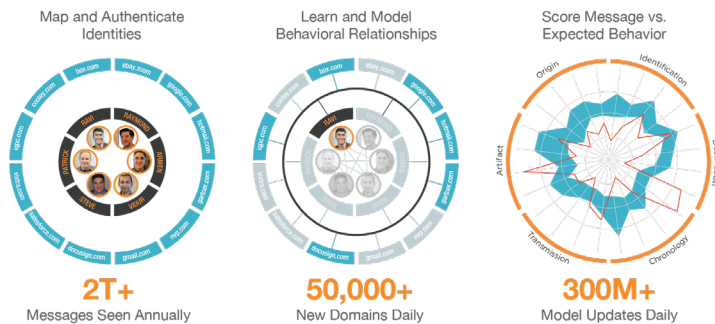
- Stopping new and existing spam attacks
- Stopping well-known or commonly used viruses and malware
- Managing unwanted or unsolicited bulk email such as newsletters or marketing campaigns
- Managing email routing or quarantine policies to keep the inbox organized

### 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 Advanced Threat Protection™ leverages Agari Identity Graph™, 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.



### AT A GLANCE

As you move to Office 365, secure your email with the next generation of Advanced Threat Protection for email. Agari Advanced Threat Protection leverages global telemetry sources, unique algorithms, and a real-time scoring pipeline to continuously model email sending and receiving behaviors across the Internet.

### HOW AGARI SECURES OFFICE 365

**Integrates seamlessly** via journaling or routing policies to scrutinize every message considered clean by Exchange Online Protection

**Subjects each message to multiple phases** of identity, behavioral, and trust modeling to expose the true identity and trustworthiness of the message

**Empowers security teams** to customize policies for high risk executives leveraging Azure Active Directory while enforcing protections via O365 mailbox APIs

**Fortifies EOP** with AI-driven URL analysis and attachment analysis to stop credential phishing and advanced email threats

### AGARI STOPS

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

“Agari Advanced Threat Protection is the most granular business email compromise solution I have seen.”

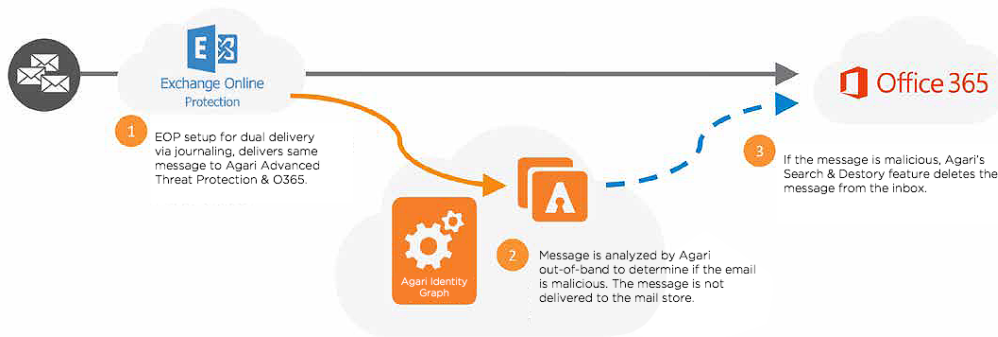
— Email Security Administrator, Fortune 1000 Organization

## 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<sup>3</sup>, making this attack technique the most effective. Anti-phishing and 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 Agari Identity Graph engine, making it possible to detect and prevent account takeover-based email attacks.

## Seamless Integration with No Added Operational Burden

Agari Advanced Threat Protection deploys hidden behind EOP, providing attackers no indication as to how O365 is protected. Agari Advanced Threat Protection 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

  
Over 2 trillion  
emails per year

  
Sender and recipient  
associations and  
situational awareness

  
Over 3 billion  
global inboxes

  
Threat intelligence  
data across  
multiple partners

## The Company We Keep

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

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

<sup>1</sup>Verizon Research Report, 2018 Data Breach Investigations Report, 2018.

<sup>2</sup>Agari, Business Email Compromise (BEC) Attack Trends Report: H2 2017, 2018.

<sup>3</sup>Osterman Research Report, Best Practices for Protecting Against Phishing, Ransomware and Email Fraud, 2018.