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, manage your risk by using the security provider that applies multiple machine learning models built against massive, Internet scale data, to stop advanced email attacks.

HOW AGARI SECURES OFFICE 365

1. Detects all forms of identity deception (display name deception, domain spoofing, and look-alike domains) to stop advanced email attacks
2. Leverages local and global data including sender and recipient relationships to model trusted email communications
3. Integrates seamlessly with Office 365 mailbox APIs and Azure Active Directory for accurate detection and prevention
4. Fortifies Exchange Online Protection as a secondary antispam layer to stop missed spam attacks

STOP TARGETED ATTACKS

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

"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 security to stop spam, known viruses, and malware, it won't secure you against the most sophisticated email attacks such as Business Email Compromise or spear phishing that rely on identity deception.

THE IDENTITY DECEPTION GAP

According to Agari research, business email compromise continues 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]. BEC attacks exploit a victim's trust as the attacker purports to be someone the victim either knows or has had a previous relationship with. Due to the fact that the only way to identify these attacks is to determine whether the sender is trusted, makes detecting them nearly impossible. The success rate for attacks using identity deception is so great that it is used in nearly all advanced email attacks. To stop these attacks a new model focused on determining sender trust and message authenticity is required, of which Exchange Online Protection was never designed for.

Exchange Online Protection (EOP) works best for:

- ✓ Stopping new and existing spam attacks
- ✓ Managing unsolicited bulk email such as Newsletters
- ✓ Detecting large-scale scattershot attacks that use
  - Malicious attachments
  - Malicious URLs

Agari fortifies EOP by stopping:

- ✗ Business Email Compromise and spear phishing
- ✗ Low-volume, targeted email attacks that use identity deception
- ✗ Social engineering-based attack that contain no malicious content
- ✗ Spam attacks missed by Exchange Online Protection

DETECTING DECEPTION WITH MACHINE LEARNING

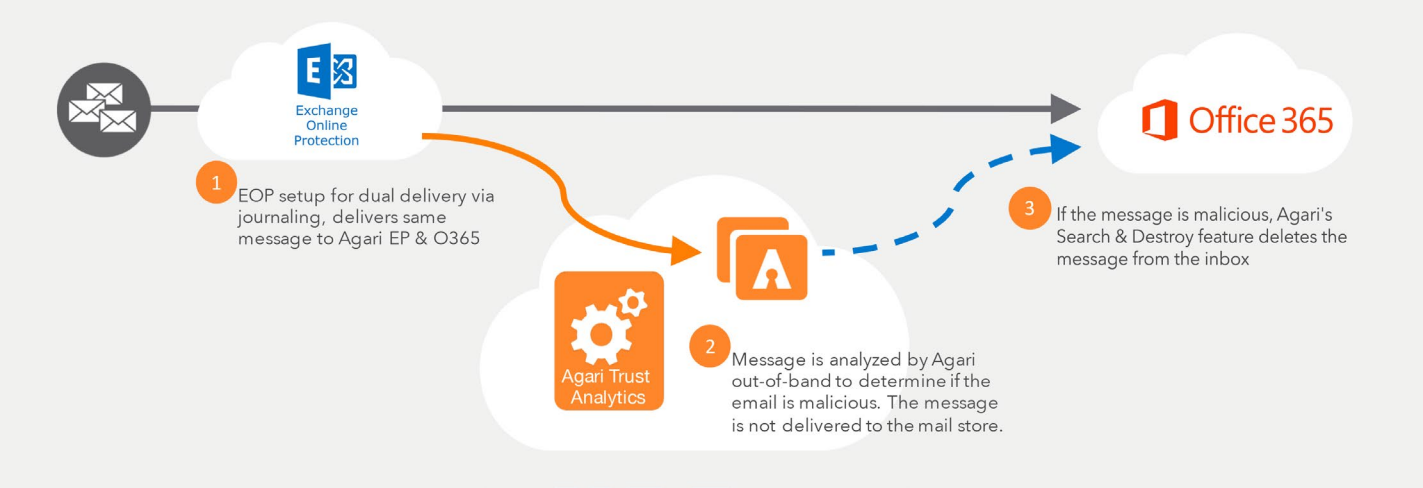
Agari Enterprise Protect uses multiple patented machine learning models that integrate identity mapping, trust models and behavioral analytics linking the Internet's infrastructure, DMARC authentication data, and local sender/recipient relationships to detect and prevent identity deception.

RULES AND REPUTATION-BASED DETECTION COMES UP SHORT

According to Gartner, "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 – ID:G00320003". Legacy detection approaches simply cannot keep up with the proactive and reactive countermeasures used by cybercriminals. From launching multi-stage attacks to leveraging email sending infrastructures with high scoring reputations, Microsoft faces an uphill battle in an area that they have never been interested in winning.

SEAMLESS INTEGRATION WITH NO ADDED OPERATIONAL BURDEN

Agari Enterprise Protect deploys hidden behind Exchange Online Protection providing attackers no indication as to how Office 365 is protected. EP provides seamless integration via journaling and Azure Active Directory to eliminate time consuming manual tuning. In addition, offers Search & Destroy to delete or move messages from the user's inbox for breach prevention or forensic analysis.



TRUSTED, PROVEN, AND SCALABLE

Enterprise Protection was built from the ground up to leverage the scale and efficiency of the cloud to dynamically adapt to the changing threat landscape. The machine learning models and algorithms developed to protect against advanced email attacks were built from Internet scale data sets with insights into the following:

- Over 2 trillion emails per year
- Sender and recipient associations and situational awareness
- Over 3 billion global inboxes
- Threat intelligence data across multiple partners

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