

# FORTRA

SOLUTION BRIEF

## Secure Microsoft 365 with Fortra Email Security

### Accelerate Your Move to the Cloud by Protecting Against Advanced Email Attacks

The benefits of moving to Microsoft 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. While Microsoft 365 provides security to stop spam, known viruses, or malware, it does not provide protection against today's modern, sophisticated identity-based attacks.

#### The Identity Deception Gap

Advanced attacks continue to be a leading way attackers bypass existing secure email gateways and other security protections. To stop these attacks, a new model focused on determining sender trust and message authenticity is required.

#### EXCHANGE ONLINE PROTECTION (EOP) WORKS FOR:

- Stopping spam attacks
- Stopping well-known 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

#### FORTRA EMAIL SECURITY FORTIFIES EOP BY:

- Enforcing and managing email authentication policies, such as DMARC, SPF, and DKIM
- Keeping employees safe by stopping today's sophisticated identity-based attacks
- 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

#### AT A GLANCE

As you move to Microsoft 365, secure your email with the next generation of advanced threat protection for email. Fortra Email Security leverages global telemetry sources, unique algorithms, and a real-time scoring pipeline to continuously model email sending and receiving behaviors across the Internet.

#### HOW FORTRA EMAIL SECURITY SECURES MICROSOFT 365

**Integrates seamlessly** via journaling 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 M365 mailbox APIs.

**Fortifies Exchange Online Protection** with AI-driven URL analysis and attachment analysis to stop credential phishing and advanced email threats.

#### FORTRA EMAIL SECURITY PROTECTS FROM

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

## Detecting Deception with Machine Learning

Fortra Email Security leverages its 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 sender and recipient identity characteristics, behavioral norms, and personal, organizational, and industry-level relationships to detect sophisticated identity deception attacks.

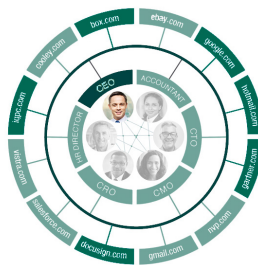
Map and Authenticate Identities



**2T+**

Messages Seen Annually

Learn and Model Behavioral Relationships



**50,000+**

New Domains Daily

Score Message vs. Expected Behavior



**300M+**

Model Updates Daily

***"Agari Phishing Defense is the most granular business email compromise solution I have seen."***

Email Security Administrator, Fortune 1000 Organization

## Prepare for the Most Dangerous Threats

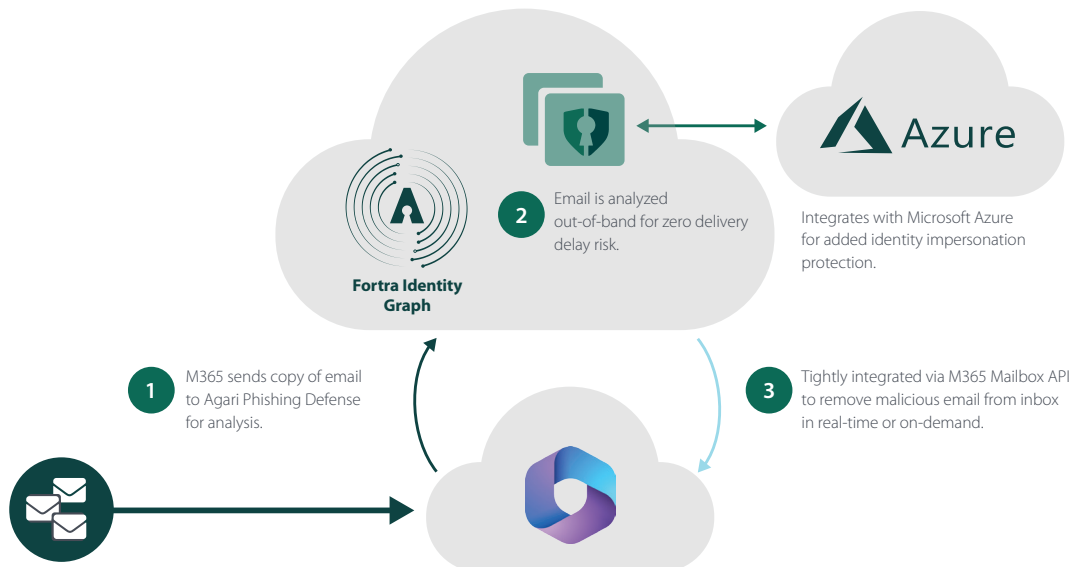
As Microsoft adds anti-phishing and anti-spoofing protection, both centered around BEC, cybercriminals are shifting tactics. Compromised accounts are quickly becoming the preferred method of attack, with cybercriminals launching attacks from legitimate accounts within an organization. Anti-phishing and anti-spoofing will not detect this type of attack because the email originates from a previously-established credible account, where deception is not needed. In contrast, Agari has built this behavioral model directly into the core Identity Graph engine, making it possible to detect and prevent account takeover-based email attacks, in addition to other advanced threats.

## Remove Latent Threats, Even After Delivery

Fortra's Continuous Detection and Response technology brings together Agari Phishing Defense and PhishLabs' Suspicious Email Analysis 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, and best-of-breed threat intelligence feeds to search for indicators of compromise in employee inboxes and then remove them in order to prevent or mitigate data breaches.

## Seamless Integration with No Added Operational Burden

Agari Phishing Defense deploys hidden behind EOP, so attackers have no indication as to how M365 is protected, and integrates via Graph API to ensure zero delivery delays. Integration with Azure Active Directory and M365 Mailbox APIs empowers security personnel to enforce prevention, regardless of organizational changes.



**Learn More:** [www.agari.com/products/phishing-defense](http://www.agari.com/products/phishing-defense)



### About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at [fortra.com](http://fortra.com).