DATASHEET

Mimecast Advanced BEC Protection

Block business email compromise with an AI-powered email security solution, providing integrated protection for your communications.

The Problem

Email is how business gets done, whether exchanging sensitive information or facilitating major transactions. With so much dependence on email, it becomes the perfect target for Business email compromise (BEC) that seeks to exploit these high-value moments. BEC lures are constantly evolving requiring tools that do not rely on signatures or heuristics, resulting in the use of AI based solutions. The challenge of making these technologies working together is the complexity and overwhelming amount of data to interpret, whilst constantly requiring tuning and human oversight due to the high number of false positives generated by AI only solutions.

The Solution

To prevent BEC attacks, security teams need to integrate multiple proven methods. A comprehensive BEC solution leverages threat feeds, email authentication protocols and advanced AI-driven detection capabilities.

To confidently identify anomalies and suspicious emails, Mimecast's advanced email security includes authentication protocols, reputation checks, threat feeds, proprietary signatures and AI to stop attacks at the point of detection. But with Mimecast, AI is more than just a last line of defense. Billions of signals across our platform strengthen our AI detection to continuously identify and block advanced BEC attacks, adapting to evolving threats.

Our protection doesn't stop there. Mimecast's unified detection capabilities protect against any type of email-based attack – not just BEC.

$2.9 BILLION
in losses due to BEC in 2023*

25%
of financially motivated attacks utilize BEC**

Mimecast Value

- **Detect payloadless attacks.** Stop advanced business email compromise threats with advanced AI.
- **Strengthen defenses with integrated protection.** One platform to protect collaboration – regardless of the attack.
- **Gain visibility into threats targeting your users.** Empower admins to make informed decisions with actionable insights.

* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
** https://www.verizon.com/business/resources/reports/dbir/

Feature	Details
Social Graph	• Analyzes relationship strength between the sender and the recipients within the organization • Analyzes reputation strength of inbound/outbound communication and user reported messages • Domain verification of Freemail, recently registered domains and typo squats of common brands
Message Analysis	• Detection of threat-specific language within emails related to specific BEC threat categories, such as requests for help with a task, fake wire transfers, urgency, communication channel switches, gift card, banking, and finance scams • Focus on understanding the context, nuances, and implications of the message to accurately interpret the true intention.
Subject Line Analysis	• Detection of threat-specific language within the subject line related to specific BEC threat categories • Focus on understanding the context, nuances, and implications of the subject line to accurately interpret the true intention.
Administration	• Organized, consolidated view of critical information • Detection explanation offering detailed evidence and impacted users • View top targeted users displaying those who frequently receive BEC threats • Search across threats to determine scale and severity • Customizable BEC policies and actions to support organizational risk tolerance
Policy Modeling	• Evaluate the impact of sensitivity level adjustments • Compare actioned emails to determine the status of each sensitivity level

Advanced BEC Protection Use Cases

Defend against BEC threats
Eliminate BEC threats by identifying anomalous activity and building a social graph of user interactions, analyzing risky phrases and semantic intent to determine an email's purpose.

Comprehensive BEC protection
Defending against BEC threats cannot rely solely on AI to identify patterns and abnormalities. It requires an approach that combines AI with proven indicators from signatures and threat feeds, ensuring attacks are stopped at the point of detection rather than relying solely on AI as the last line of defense.

Understand what is blocked and why
Being able to easily triage a BEC detection is important. Every detection from Mimecast's Advanced BEC Protection lists not only the policy that triggered the detection but also the risky characteristics that led to the verdict. As a result, administrators spend less time determining the cause.

Policy modelling made simple
Constantly tuning BEC policies is unsustainable. Through the historical analysis of messages, identify the impact of a policy change and determine the potential messages caught via each level of sensitivity.