

How to protect your business from Business Email Compromise (BEC) scams

The Landscape

25%

of motivated attacks are BEC ¹

\$50,000

The median loss from BEC scams ¹

60 seconds

The time it takes to fall for a phishing attack ²

The risk?

Small businesses have limited resources to combat high-volume or complex email scams.

5 critical layers to defend against BEC

Discover how a multi-layered AI-powered approach protects against BEC.

Checklist:

- Prefiltering** – block known bad emails, let known good emails through to end users
- AI-powered** – Natural language processing (NLP) and ML capabilities analyze email content, identifying subtle anomalies and suspicious activity.
- Integrated detection** – Multiple signals and technologies create a comprehensive view of threats, enabling blocking at the point of detection.
- Continuous learning** – Limit manual intervention with models that continuously learn and improve.
- Security Awareness Training** – Enable your employees to be more security conscious, and identify and remediate riskier users.

[Learn how to protect against business email compromise](#)

1: FBI Internet Crime Report 2023 2: 2024 Data Breach Investigations Report