Harnessing AI against BEC

The $3B threat to business

mailguard

Executive Summary

While many security solutions focus primarily on malware, malicious links, and known indicators of compromise, Business Email Compromise often contains none of these signals.

MailGuard's AI-powered threat detection architecture was specifically designed to identify socially engineered attacks, executive impersonation attempts, payment fraud, and trust-based deception before they reach employee inboxes.

This is where many of the most financially damaging cyberattacks begin.

Business Email Compromise (BEC) is the most financially damaging cybercrime facing organisations today.

In 2025, the FBI IC3 reported:

- **$3.05 billion** in BEC losses, and
- **24,768 incidents**

These attacks are quiet, targeted, and increasingly evade traditional email security.

The FBI noted in it's IC3 report that *'AI technology enables the creation of convincing synthetic content, such as social media profiles and personalized conversations, often in mass quantities... this developing technology makes it possible to create high-quality content.*

AI-enabled synthetic content is becoming increasingly difficult to detect and easier to make, which allows criminal actors to potentially conduct successful fraud schemes against individuals, businesses, and financial institutions.'

And specifically with regard to AI, it said, *'Chat generators can quickly create official-sounding emails mimicking a company's CEO or other officials. These emails can contain phishing links or directions to wire funds...'*

Noting that '*There are multiple BEC tactics, and not all are AI-enabled.*' For instance, many sophisticated BEC attacks are highly targeted and socially engineered, and don't contain malware or obvious links, just convincing language designed to trick employees.

"MailGuard is designed to work with Microsoft, not replace it.

We stop threats that traditional, native security can miss, before they reach your users."

Craig McDonald
CEO & Founder, MailGuard

Why Microsoft 365 + MailGuard Is Better Together

Microsoft Defender for Office 365 provides essential native protection, but like all broad-based tools, it has limitations against BEC:

- **It relies on pattern and reputation analysis,**
- **May lag in identifying zero-day or personalised threats , and**
- **Does not flag clean-looking executive impersonations .**

While other vendor solutions integrate with Microsoft 365 to enhance email security, they often operate alongside Microsoft's native defences rather than being deeply embedded. This leads to overlapping functionalities and potential gaps in threat detection, particularly concerning fast-breaking zero-day attacks.

MailGuard has partnered with Microsoft since 2001, leveraging over two decades of expertise. It employs proprietary AI & ML models to detect and neutralise sophisticated threats faster than Microsoft 365 alone, ensures an enhanced, unified defence, and minimising overlaps to improve the overall efficacy of threat detection and response.

"It's the type of innovation that we want to see."

Satya Nadella
Chairman & CEO, Microsoft

"Every company has at least one employee who will click on anything. That's pretty hard to protect."

Brad Smith
Vice Chair & President, Microsoft

The Threat landscape: FBI IC3 2025 Data

Threat Type	Complaints	Total Losses
BEC (Business Email Compromise)	24,768	$3,046,598,558
Investment Scams	72,984	$8,648,617,756
Tech/ Customer Support Fraud	47,794	$2,134,675,818
Personal Data Breach	67,456	$1,314,923,988
Phishing/ Spoofing/ Ransomware	195,172	$248,163,231

Real-World FBI Examples

- A real estate firm nearly lost **$956,000** in a BEC scam. The FBI recovered **$955,000** within 48 hours.
- Another organisation transferred **$6.6M** to a fraudulent vendor account. Only **$5.1M** was recovered.

Beyond Traditional Email Security

Many organisations still associate email security with blocking spam, malware, malicious attachments, and suspicious links.

While these threats remain important, some of today's most damaging attacks look entirely legitimate.

Business Email Compromise, payment fraud, supplier impersonation, executive impersonation, payroll fraud, and credential theft attacks are designed specifically to exploit trust rather than technology.

In many cases there is no malware.

No malicious attachment.

No suspicious URL.

Only a carefully crafted message designed to influence a decision.

This shift has changed the nature of email security.

The challenge is no longer simply identifying malicious code. It is identifying deception.

Modern organisations rely on trusted communications to move money, approve transactions, share sensitive information, and make critical business decisions.

Cybercriminals increasingly target those trusted processes because they understand that manipulating people is often easier than compromising systems.

This is where MailGuard provides a critical layer of protection.

By analysing behavioural signals, impersonation indicators, communication context, and emerging attack patterns, MailGuard helps identify sophisticated socially engineered attacks before employees have an opportunity to engage with them.

mailguard

How BEC Works — and Where MailGuard Intercepts

Typical Attack Flow:

Step 1) Spoofed Email Sent

Step 2) Executive Receives Message

Step 3) Urgent Request Sent to Finance or HR

Step 4) Funds or Credentials Transferred

Step 5) Laundered via Cryptocurrency or Offshore Account

MailGuard stops the threat between Step 1 and Step 2 — before inbox delivery.

"BEC is one of the most financially damaging online crimes.

It exploits human behaviour — not technical vulnerabilities — which makes it hard to detect using traditional tools."

Microsoft Security Team

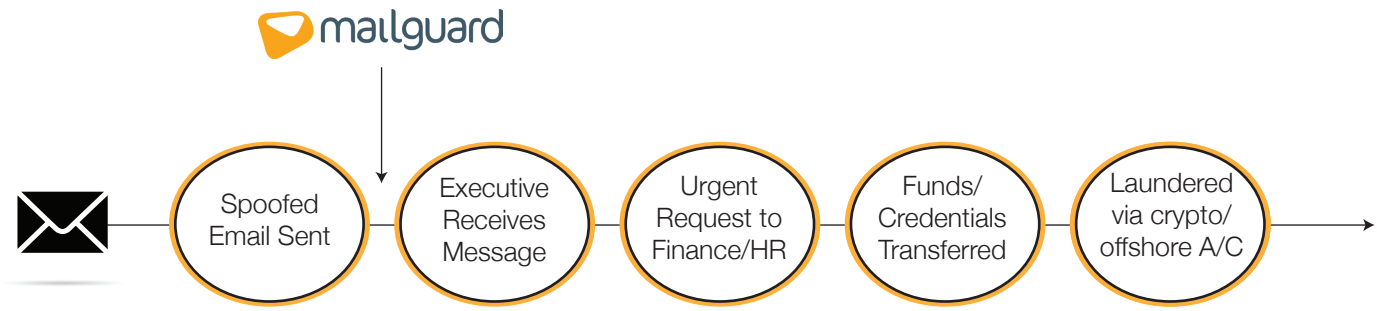

Figure 1. How BEC works - and where MailGuard intercepts

How MailGuard Detects BEC & Social Engineering

Traditional email security often focuses on identifying technical indicators of compromise.

Business Email Compromise and socially engineered attacks rarely provide those indicators.

Instead, MailGuard evaluates a broad range of behavioural, contextual, and impersonation signals to identify deception before employees interact with a message.

MailGuard continuously assesses:

- Sender authenticity and identity signals
- Executive and supplier impersonation indicators
- Language patterns commonly associated with fraud
- Unusual communication behaviour
- Domain reputation and emerging threat intelligence
- Global attack patterns observed across protected organisations

Supporting this capability is MailGuard's proprietary AI-powered, threat detection architecture, combining:

- Advanced Large Language Models (LLMs)
- Bayesian classification engines
- Meta fingerprinting technology
- Real-time global threat replication
- Human-led threat intelligence and validation

This combination allows MailGuard to identify sophisticated attacks that may otherwise appear legitimate to both employees and traditional email security controls.

We do not wait for threats to become widespread.

We work to stop them on first encounter.

Examples of Attacks MailGuard is Intercepting

Not all email threats arrive carrying malware.

Many of the most financially damaging attacks are designed to appear as legitimate business communications.

MailGuard routinely detects and blocks attacks including:

Executive Impersonation

Emails appearing to originate from a CEO, CFO, Managing Director, or other senior executive requesting urgent action, financial transfers, or sensitive information.

Supplier Payment Fraud

Messages impersonating trusted suppliers and requesting changes to banking details, payment instructions, or invoice processing procedures.

Credential Harvesting

Emails designed to capture usernames, passwords, and multi-factor authentication information through deceptive login requests or account verification workflows.

Payroll and HR Fraud

Attempts to redirect payroll deposits, update employee banking information, or obtain sensitive personnel records.

Partner and Customer Impersonation

Sophisticated attacks that leverage trusted commercial relationships to manipulate decision-making and bypass normal scrutiny.

These attacks are successful because they exploit familiarity, urgency, authority, and trust.

MailGuard is specifically designed to identify those signals before the message reaches the inbox.

Why These Attacks Often Evade Traditional Security Controls

Many security solutions were designed to detect malicious files, known indicators of compromise, and previously identified attack techniques.

Business Email Compromise operates differently.

Attackers increasingly use legitimate-looking emails, realistic business language, trusted brands, and convincing impersonation techniques to avoid triggering traditional security controls.

These attacks often:

- Contain no malware
- Include no malicious attachments
- Use legitimate email services
- Mimic normal business workflows
- Appear to originate from trusted individuals
- Create urgency that encourages immediate action

Because the attack is centred on human decision-making rather than technical exploitation, traditional detection methods can struggle to identify the threat.

MailGuard's approach focuses on detecting deception itself.

By analysing intent, context, behaviour, and impersonation indicators, MailGuard helps stop sophisticated fraud attempts before trust is transferred, credentials are disclosed, or funds leave the organisation.

What Leaders & Boards Should Be Asking

- “If an attacker impersonated our CFO right now via email, would we detect it before the inbox — or only after it’s been opened?”
- “How many credential theft attempts have actually reached our employees this month — and how do we know?”
- “Are we still relying solely on Microsoft 365 or post-delivery detection to stop threats — even after they’ve landed?”
- “Have we reviewed a live threat snapshot for our domain in the past 30 days — showing what Microsoft Defender may have missed?”

The MailGuard Threat Detection Advantage

Beyond traditional email security, MailGuard outpaces Microsoft Defender for Office 365 and other email security peers by delivering faster, more precise threat detection.

With proprietary AI & ML-powered architecture, real-time global threat intelligence updates, and optimized workflows for immediate response, it delivers deep protection of employee inboxes against advanced, emerging threats.

A multi-layered AI & ML-driven security approach, leverages:

- Proprietary models including Gen-AI-based LLM, Bayesian classifiers, and meta fingerprinting for advanced threat detection.
- Optimized workflows allowing real-time threat response and security fine-tuning.
- Low-latency replication, meaning instant deployment of global threat intelligence updates before attacks reach inboxes.

"That ability to laterally move, faster than the adversary... especially around threat protection and social engineering. That's the type of innovation that we want to see."

Satya Nadella, CEO & Chairman, Microsoft

"Threats were still getting through Microsoft — MailGuard picked them up."

IT Manager, Porsche

"We've seen email-based attacks surge. MailGuard and Defender 365 together have helped us stay protected."

CISO, Silk Logisitics Holdings

Trusted by Leaders Globally.

Not simply commodity filtering, MailGuard is a global leader in stopping advanced zero-day email threats, many of which are missed by Microsoft 365 and other 3rd party vendors.

Business leaders achieve peace of mind with a solution trusted by global leaders that ensures their email is secure. Benefitting from A$35M+ in R&D, including proprietary AI & ML-powered threat detection, to boost cybersecurity and inbox confidence.

AI-powered email threat detection and agile architecture intercepts and blocks advanced, sophisticated BEC and socially engineered threats, hours faster, and on first encounter.

"You are being led by what I see as one of the world's best at protecting secure infrastructure and securing your business."

Steve Miller

VP, Microsoft Australia & New Zealand

"I support MailGuard's mission, as a solution designed to intercept threats before user engagement. It's fast, focused, and built with intent in mind."

Don Good

Former Deputy Assistant Director, FBI Cyber Division

Final Word: Protecting Trust Before It Is Exploited

The most damaging cyberattacks facing organisations today are increasingly difficult to recognise because they appear legitimate.

They do not rely on exploiting vulnerabilities in software.

They rely on exploiting trust.

A trusted supplier.

A trusted executive.

A trusted business process.

A trusted communication channel.

As attackers increasingly use AI to scale deception, organisations require security solutions capable of identifying not only technical threats but also the subtle indicators of manipulation and fraud.

MailGuard was built to address this challenge.

Working alongside Microsoft 365 and other leading email platforms, MailGuard provides an additional layer of intelligence focused on detecting Business Email Compromise, payment fraud, executive impersonation, credential theft, and other socially engineered attacks before they reach employee inboxes.

Because once trust is transferred, the damage has often already begun.

The strongest email security strategy is not simply about stopping malware.

It is about protecting the trust that modern organisations depend upon every day.

"Our analysts have recognised MailGuard as a global innovator and a bright spot in cloud email security."

Gartner

mailguard

Pioneering Email Security. Built in Australia. Trusted Worldwide.

MailGuard is a global leader in email threat detection. A pioneer in cloud email security since 2001, MailGuard invented the concept of pre-filtering email threats before inbox delivery, laying the foundation for the Secure Email Gateway (SEG) category.

Today, MailGuard protects organisations globally with AI-powered threat detection.

Seamlessly deployed inline with Microsoft's ecosystem and Google, among other email providers, at the heart of our platform is MyGuard, our proprietary AI threat engine developed with over A$35 million in R&D.

MyGuard combines:

- Gen-AI powered LLMs
- Bayesian and fingerprint-based classifiers
- Real-time behavioural heuristics

…to stop advanced threats on first encounter before they reach staff inboxes, including those that bypass Microsoft and other cloud email security vendors.

MailGuard is ISO/IEC 27001:2022 certified, trusted by over 5,500 organisations, including governments, law firms, banks, hospitals, and ASX-listed companies.

Recognised for our unmatched speed in detecting zero-day email threats, we have consistently stopped sophisticated exploits, like QR code phishing, Dropbox-based malware, and Azure AD Guest Invite fraud, months ahead of Microsoft, and other leading platforms.

In an era of rising cyber regulation and board-level accountability, MailGuard enhances your Microsoft 365 or Google security stack with minmal disruption, easy activation, and elite-speed protection, fulfilling your fiduciary and operational responsibilities.

mailguard

Let's Connect

Craig McDonald
CEO & Founder
craig@mailguard.com.au

MailGuard Pty Ltd.
(A GlobalGuard Company)
Level 14, 333 Collins Street
Melbourne VIC 3000

info@mailguard.com.au

+61 3 9694 4444

Support
Australia: 1300 306 510
United States: 888 848 2822
United Kingdom: 0800 404 8993

mailguard