DARKTRACE | Microsoft

Multi-layered Email Security for Microsoft: A Guide to Ending Business Email Compromise

Content

Abstract

Email remains the cornerstone of business communication and the most exploited entry point for cybercriminals. As Business Email Compromise (BEC) tactics evolve, threat actors leverage AI-powered techniques to launch targeted, sophisticated attacks that bypass traditional security measures. To stay ahead, security teams must shift from reactive defense to a proactive, AI-driven strategy.

This whitepaper explores:

- **How BEC attacks are becoming more sophisticated with AI**
- **Why traditional email security measures are no longer enough**
- **How Microsoft and Darktrace combine forces to deliver a multi-layered, AI-driven defense**
- **The benefits of an integrated approach to email security**

The rising threat of BEC in a Microsoft-driven world

BEC remains a top cyber threat and a multi-billion-dollar problem that continues to outpace other cyber threats in financial impact. In 2023 alone, BEC accounted for over $2.7 billion in adjusted losses (FBI Internet Crime Report 2023). As attackers leverage AI-driven techniques, traditional email security is no longer enough to stop sophisticated phishing and social engineering tactics.

Indeed, BEC attacks have evolved beyond basic phishing scams, leveraging AI-powered social engineering to deceive even the most cautious employees. With Microsoft 365 offerings and Exchange as dominant enterprise platforms, attackers frequently target these environments. While Microsoft offers robust security, the growing sophistication of AI-driven BEC attacks demands a more proactive defense.

To stay ahead, organizations need a layered, AI-powered defense that extends beyond the inbox. This is where Darktrace / EMAIL comes in to improve protection by detecting and neutralizing threats in real-time. Microsoft and Darktrace combine attack-centric and behavior-centric security to protect user identities, detect threats early, and secure modern email environments.

How BEC attacks are weaponizing AI

In the past, BEC attacks primarily relied on straightforward impersonation techniques such as exploiting compromised credentials or spoofing email addresses. However, generative AI, particularly Large Language Models (LLMs), has fundamentally changed the cybersecurity landscape and the way cybercriminals conduct BEC attacks.

These models enable attackers to craft highly convincing, context-aware emails that mimic the style and tone of legitimate communications, making them far more difficult to distinguish from genuine messages.

The key advancements AI brings to BEC attacks include:

- Flawless, context-aware email crafting: AI can draft emails that seamlessly blend into ongoing conversations or align with company-specific communication styles.
- Multilingual attacks: Attackers can generate phishing emails in multiple languages, even if they are not fluent in the target language, lowering the barrier to entry for malicious actors and high-quality attacks.
- Advanced evasion tactics: AI tools are capable of generating sophisticated emails that can easily evade rule-based security systems, which typically rely on known patterns, threats, or predefined keywords.

For example, tools like ChatGPT can automatically generate fake invoices from vendors that seem perfectly aligned with legitimate transactions. These emails are also harder to spot because AI automatically:

- Avoids misspellings and grammatical errors
- Creates multiple variations of email text
- Translates messages that read well in multiple languages
- Impersonates individual writing styles
- Creates deepfake audio and video content that strengthens impersonations

Why legacy email security falls short

Legacy email security solutions are designed to catch known threats and attack patterns, typically focusing on suspicious links, attachments, or email domain anomalies, capabilities which are offered natively in your Microsoft deployment. However, AI-driven BEC attacks are more nuanced, often lacking obvious indicators of compromise. They primarily rely on social engineering, psychological manipulation, impersonation, and account compromise, areas where legacy security tools struggle to keep pace.

Traditional SEGs face similar limitations, relying on static indicators like blacklists and signature-based detection. This approach struggles to catch more dynamic threats and often ignores behavioral anomalies at the account level. While some SEG providers have adopted API-based deployments and AI-driven analysis, these updates do not fundamentally improve outdated detection methods.

This is where Darktrace / EMAIL, powered by Darktrace's Self-Learning AI, fills the gap. By continuously analyzing the behavior of email interactions, sender relationships, and user activity patterns, Darktrace identifies subtle deviations that signal an attack, often before the content even raises suspicion. This approach allows organizations to detect and neutralize threats in real-time, even when the email content itself appears benign or harmless.

Additionally, Darktrace was designed from the ground up to build off of the benefits of Microsoft instead of duplicating its capabilities. This synergy eliminates mail latency, ongoing configuration maintenance, and the need for duplicate costs across your IT estate. The solution seamlessly integrates insights from email, messaging, and other productivity tools into your SOC workflow, providing a proactive and unified security platform that adapts to evolving threats and ensure comprehensive protection.

For CISOs, adopting this two-pronged approach not only strengthens their security posture but also optimizes resources, leading to a more efficient, scalable, and future-proof email security strategy.

Beyond the inbox: A holistic approach to email security

BEC attacks don't start and end with an email. They exploit vulnerabilities across an organization's entire security infrastructure. To effectively combat these threats, organizations must adopt a defense-in-depth strategy that goes beyond traditional email protection and encompasses the broader security ecosystem. This approach includes:

- Identity access protection: Ensuring that strong authentication mechanisms, zero-trust principles, and anomaly detection are in place to safeguard user credentials and prevent unauthorized access.
- Behavioral AI detection: Leveraging AI to continuously learn normal email communication patterns and identify deviations that may signal a potential attack.
- Proactive incident response: Automating threat containment and remediation to neutralize attacks before they escalate, minimizing business impact.
- Seamless integration: Ensuring that all security solutions work together, enabling a unified response to threats and eliminating gaps between siloed systems.

Better together:

Microsoft Defender for Office 365 and Darktrace / EMAIL

Darktrace / EMAIL is designed to seamlessly integrate with Microsoft's security ecosystem, ensuring that security solutions work together without overlapping workflows or devalued investments. Hosted on Microsoft Azure, Darktrace / EMAIL enhances Microsoft's native protection by adding advanced, AI-driven layers to secure email communications across all dimensions of an organization's operations.

Key capabilities of this integrated solution include:

- **Extended inbox security:** Moves beyond inbox protection to safeguard user identities, account access, and outbound email threats, ensuring comprehensive protection.
- **Leading phishing & BEC protection:** Uses behavioral AI to detect and neutralize zero-day threats, including sophisticated phishing and BEC attacks, before they reach their target.
- **Optimizing ROI on security investments:** Enhances existing Microsoft security investments by eliminating duplicate workflows, reducing manual tuning and maintenance, and freeing security teams to focus on higher-priority threats, all while minimizing the need for additional security platforms and optimizing budget efficiency.

By combining the strengths of Microsoft and Darktrace, organizations can adopt a proactive, AI-driven defense that stays ahead of evolving threats. Real-time, intelligent analysis detects and neutralizes threats before they cause harm, while seamless integration with Microsoft's security framework strengthens visibility and ensures compliance, allowing organizations to maintain oversight while adhering to regulatory requirements. This powerful collaboration delivers comprehensive protection, securing inbound and outbound emails, safeguarding user identities, and reinforcing defenses across all communication channels.

Take the next step towards AI-powered email security

Darktrace and Microsoft have built a partnership that customers can trust, with the majority of Darktrace's 10,000 customers relying on Microsoft technologies. This award-winning collaboration offers an integrated, best-in-class email security solution that combines attack-centric and business-centric approaches, delivering complete, contextual, and continuous protection.

Get started with Microsoft & Darktrace

Explore the Darktrace / EMAIL solution brief

Watch the webinar: Beyond Spam Filters and Firewalls: Preventing BEC in the Modern Enterprise"

Schedule a demo to see how Darktrace / EMAIL strengthens your Microsoft security investments.

■ **About Darktrace**

Darktrace (DARK.L), a global leader in cybersecurity artificial intelligence, is on a mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to help transform security operations and improve cyber resilience. Breakthrough innovations from its R&D Centers have resulted in more than 200 patent applications filed. Darktrace employs 2,400 people around the world and protects over 9,700 organizations globally from known, unknown and novel cyber-threats.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com