

Openfind™ MailGates BEC 郵件詐騙防護解決方案

商務電子郵件詐騙事件急速攀升 企業損失金額龐大

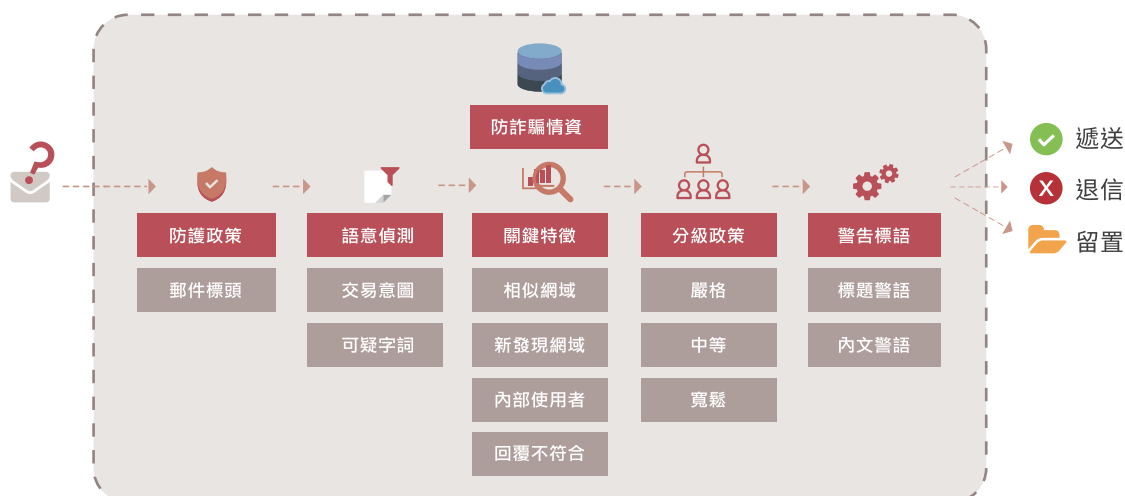
商務電子郵件詐騙事件近年來迅速增加，2018 年企業因郵件詐騙損失現已超過 120 億美元。美國聯邦調查局透過其網路犯罪通報中心 (Internet Crime Complaint Center, IC3) 發布最新的商業電子郵件詐騙統計估算，每次事件平均損失金額為 160,000 美元。

BEC (Business Email Compromise) 是犯罪組織針對企業精心策劃的複雜騙局，在大多數情況下，詐騙者會將目標鎖定在財務人員身上，利用取得的資訊偽裝成企業高階主管或往來供應商進行詐騙。由於這類信件並非病毒信，無法透過防毒機制加以偵測阻攔，收件者必須更加謹慎處理。電子郵件身份驗證機制 (如 SPF、DKIM 及 DMARC) 可阻絕假冒網域的電子郵件，但無法偵測其他類型的偽冒信，例如相似網域信件之詐騙攻擊。這也是為何企業用戶需要更進階的郵件詐騙防護機制之原因。

整合防詐騙智慧中心情資進行郵件行為分析 協助企業解決詐騙信問題

MailGates BEC 防護解決方案，整合 MailCloud 防詐騙智慧中心情資，透過郵件標頭防護政策與郵件行為分析等機制，幫助用戶解決難以防範的詐騙信問題。管理者可彈性設定郵件標頭安全政策保護往來合作夥伴，若偵測到異常郵件行為，可依組織政策將信件標記警語或删除。郵件行為分析引擎，是根據 MailCloud 防詐騙智慧中心情資所制定的專家系統，可偵測電子郵件中關鍵特徵值，並根據用戶的信件往來紀錄，以判別是否為可疑信件。

BEC 防護機制如何運作



當一封郵件通過 MailGates 時，BEC 防護引擎會檢查幾個關鍵項目：

1. 郵件身分驗證，檢查 SPF / DKIM 及 DMARC 等驗證機制，阻絕假冒網域的電子郵件。
2. 郵件標頭偵測，比對郵件中 Envelope-From、From 與 Reply-To 等標頭是否符合郵件安全政策。
3. 郵件行為分析，檢查郵件各項特徵值，例如：偽造內部使用者名稱 (Forge Internal User)、未曾往來的網域 (New Observed Domain)、郵件回覆位址與寄件者不符 (Reply-To Mismatch)、顯示名稱詐騙 (Display Name Spoofing) 及相似網域 (Cousin Domain) 偵測等。
4. 郵件意圖分析，檢查電子郵件內容是否具有急迫性、交易意圖或匯款請求，並透過機器學習 (Machine Learning) 模型提升攔截精準度。

如果郵件未通過這些組合驗證，管理者可設定郵件安全政策將郵件退回、留置隔離區或標記警語提醒收件者該封信是可疑的。

BEC 威脅關鍵指標

01 偽造的郵件網域名稱

04 未曾往來的網域

02 偽造的寄件者顯示名稱

05 與合作廠商相似的電子郵件網域

03 寄件者與回覆地址不相符

06 信件內容具有急迫性與交易意圖

MailGates BEC 防護解決方案主要特色：

No	項目	說明
1	郵件身分驗證機制	支援 SPF、DKIM 及 DMARC 等標準驗證機制，避免網域冒用攻擊。
2	整合全球詐騙威脅情資	包含 Sophos 全球威脅情資及 MailCloud 防詐騙智慧分析中心情資。
3	彈性化郵件標頭安全政策	比對郵件中 Envelope-From、From 與 Reply-To 標頭內容，避免郵件標頭偽造攻擊手法。
4	防止偽造顯示名稱	比對郵件中顯示名稱是否為偽造，範例： Sam<Sam@internal.com>公司內部使用者 Sam<Sam@external.com>意圖假冒之信件
5	防止相似網域詐騙	檢查寄件者網域與合作夥伴之相似性，範例： mailcloud.com.tw → mailcloud.com.tw l → 1 (數字) openfind.com.tw → openfind.com.tw m → rn mail2000.com.tw → mail2000.com.tw o → 0 (數字)
6	偵測郵件意圖是否具風險性	透過AI防詐騙辨識模型，分析郵件內文是否具交易意圖或匯款請求。
7	彈性化組合驗證機制	根據大數據分析統計，動態調整各項驗證機制權重，以達成最佳化檢測效果。
8	AI 防詐騙學習模型回饋機制	提供詐騙信回報機制，回饋 MailCloud 防詐騙智慧分析中心，改善 AI 防詐騙學習模型。

支援郵件系統

Mail2000 | Microsoft Exchange | IBM Notes | Sendmail | Postfix

支援郵件雲端服務

Google Workspace | Microsoft 365 | Exchange Online

用戶端建議需求

Microsoft Edge | IE 11 | Firefox 最新版 | Chrome最新版