Proofpoint Threat Protection

保護團隊安全，抵禦現代威脅

主要優勢

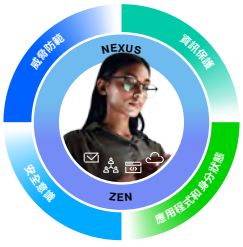
- 快速偵測及封鎖現代電子郵件威脅
- 透過持續 AI 更精準阻擋新興威脅
- 深入探索人為風險與安全威脅
- 提高作業效率
- 強化團隊防護力，推動安全行為轉變

電子郵件是網路安全威脅的主要威脅媒介。當今網路威脅層出不窮，各種惡意軟體、網路釣魚攻擊與社交工程詐騙手法不斷進化，專門鎖定您的團隊作為攻擊目標。根據 2023 年 Verizon 資料外洩調查報告，74% 的資料外洩事件源自人為因素[1]。透過 Proofpoint Threat Protection，您的組織能全面抵禦現代網路威脅，確保團隊安全。

網路犯罪持續擴張，風險前所未有

高回報、低風險讓網路犯罪迅速崛起，成為快速成長的非法產業。根據 Cybersecurity Ventures 預測，全球網路犯罪造成的損失將在 2025 年突破每年 10.5 兆美元[2]。網路犯罪組織與一般企業運作模式無異，其核心動機正是巨大的財務利益。惡意攻擊者透過電子郵件竊取重要的個人與企業資訊、進行身分竊取，並發動金融詐騙攻擊。作為現代商業運作的基石，電子郵件已成為頭號威脅媒介，精準鎖定您的團隊發動攻擊。更嚴峻的是，這些威脅不斷進化，防禦難度日益提升。這就是為什麼即使是最先進、最複雜的組織，保護團隊免受現代威脅仍極具挑戰。但 Proofpoint 能助您一臂之力。

這套解決方案組合是 Proofpoint 整合式 Human-Centric Security 平台的一環，專注於降低四大關鍵人為風險。



1 Verizon 〈*2023 年資料外洩調查報告*〉，2023 年。
2 Steve Morgan〈*網路犯罪雜誌*〉。「Cybercrime To Cost The World 10.5 Trillion Annually by 2025」〈*到 2025 年，全球網路犯罪損失將達每年 10.5 兆美元*〉，2020 年 11 月。

87%

的財星前 100 大企業信賴 Proofpoint，保護團隊安全，抵禦現代威脅。

資料來源：Proofpoint，2024 年

透過 Pre-delivery 偵測，快速阻擋電子郵件威脅

使用我們的 Pre-delivery 偵測技術，您可以全面掃描企業郵件，精準識別並攔截已知與未知威脅。這表示尖端威脅在進入企業系統前即被攔截，而非 Post-delivery 才應對。這些威脅包括：

- 進階憑證式網路釣魚
- 惡意軟體
- 勒索軟體
- 企業電子郵件入侵 (BEC)
- 惡意 URL
- QR 代碼攻擊
- 附件式攻擊
- 以及更多攻擊手法

當這項技術與我們的自動化 Post-delivery 偵測與補救機制相結合時，您的組織即可透過單一且全面的解決方案，全方位保護團隊安全。

AI 導向的多層次偵測，精準識別威脅

我們採用多層次偵測架構，結合了威脅情報、機器學習、行為 AI、沙箱分析、內容分析與語意分析 (LLM)。這些技術相互整合，精準偵測多種類型的現代威脅。透過此架構，實現 99.99% 的高精準偵測率，並提供更深入的威脅解析。不同於單層次偵測的電子郵件安全解決方案，我們的多層次架構能更精準攔截惡意郵件，同時確保合法郵件順利送達，不影響企業運作，大幅降低漏報與誤報的風險。

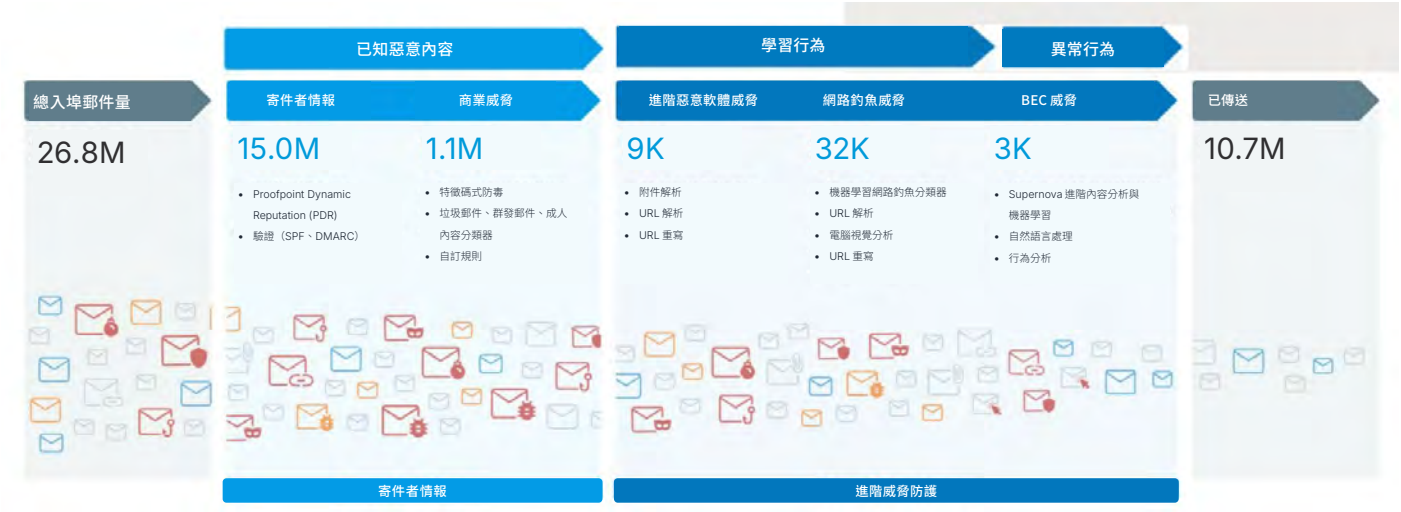


圖 1：Proofpoint AI 導向的多層次 Pre-delivery 偵測實戰應用。

全面掌握人為風險與威脅動態

Proofpoint 提供獨特洞察，讓您清楚識別 Very Attacked People™ (VAP) 及其所面臨的威脅。有了這些關鍵資訊，您即可精準部署應變控制措施。這些措施包括瀏覽器隔離、安全意識訓練、進階驗證等。透過分析人為風險，您能精準掌握團隊安全狀況，包括受攻擊頻率、潛在弱點與存取權限。此外，Proofpoint 每年分析 3 兆封以上的電子郵件，涵蓋超過 23 萬家客戶、合作夥伴及供應商的安全生態系統。我們的威脅情報與研究可為您提供早期預警與遙測防禦，助您應對前所未見的新興威脅。

提高作業效率

透過 Proofpoint，您可以自動偵測並移除已送達的惡意電子郵件。這項自動化機制可加速威脅分類與處理流程，並移除含有惡意負載的郵件，讓您更迅速、更高效地識別與應對安全威脅。無論這些惡意郵件是來自內部遭入侵的帳戶，還是經由其他使用者轉發或接收，Proofpoint 都能提供自動化警報、威脅比對分析，並呈現可執行的威脅洞察。這不僅大幅縮短威脅處理時間，還能減輕團隊負擔，提升整體運作效率。此外，使用者可透過電子郵件警告標籤或網路釣魚電子郵件警示按鈕，一鍵即可回報可疑郵件。若使用者回報的郵件被確認為惡意郵件，則系統將自動隔離該郵件及所有相同副本。使用者將收到電子郵件通知，確認該郵件為惡意郵件並已自動移除。這種封閉迴路通知機制有助於強化使用者行為，鼓勵持續回報類似郵件。

強化團隊防護力，推動安全行為轉變

Proofpoint 透過改變不安全行為並培養可持續的安全習慣，進一步降低人為風險。我們運用豐富的威脅情報，多方面強化您的安全計畫。這包括設計真實環境的網路釣魚模擬、提供威脅引導式訓練，針對高點擊率使用者與最易受攻擊對象進行培訓，以及自動化調查使用者回報的可疑電子郵件。我們透過個人化學習體驗，幫助您提升使用者的參與度。自我調適方法幫助您的團隊有效吸收所學，並培養長期且正向的安全習慣。我們透過追蹤實際的行為改變，並與同業標準對比，幫助您更有效向管理層傳達人為風險現況及安全計畫成效。

圖 2：Proofpoint 可清楚掌握 Very Attacked People™ (VAP) 的人為風險。

Proofpoint 代管服務供應項目

Proofpoint 為 Proofpoint Threat Protection 提供以下代管服務：

- **Managed Email Threat Protection**—提供專業主動防禦、持續監管與高層安全洞察，確保您的電子郵件安全解決方案穩健運行。我們也負責日常安全作業檢查與主動應用最新威脅情報。
- **Managed Abuse Mailbox**—減少人工審查使用者回報電子郵件的負擔。我們的團隊負責分析所有未分類郵件，並提供明確的處置判定。
- **Managed Security Awareness**—強化並升級您的使用者安全教育策略。我們引導您的安全計畫策略，重點關注行為改變與建立更具韌性的安全文化。

如需詳細資訊，請造訪 proofpoint.com/tw/products/protect-people。

若要深入瞭解，請前往 www.proofpoint.com