Cloudflare 電子郵件安全性

為安全工作空間通訊提供自發的多通道保護

防禦針對性網路釣魚攻擊

輕鬆封鎖並隔離其他解決方案遺漏的威脅

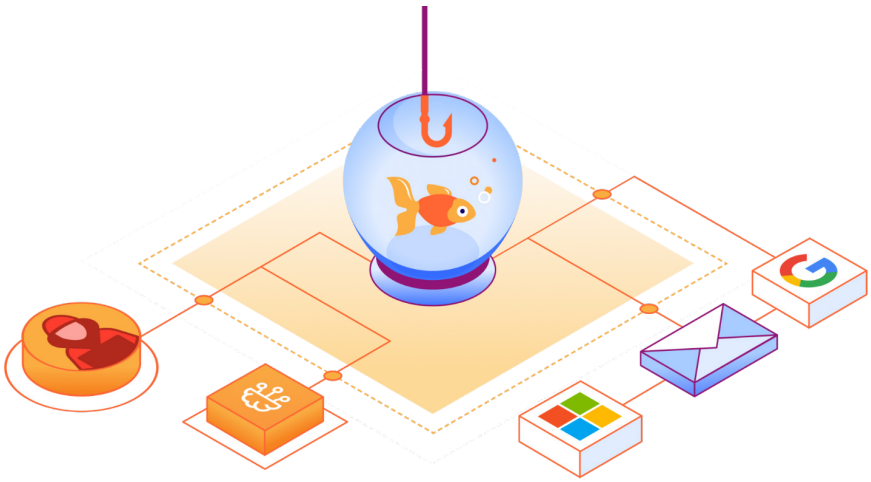
由於電子郵件是人們最常使用且最常遭到利用的商業應用程式，因此，保護使用者免受試圖透過電子郵件操縱其信任的網路釣魚攻擊比以往任何時候都更為重要。由於組織越來越多地透過 Microsoft 365 和 Google Workspace 來採用雲端電子郵件服務，以更好地支援混合工作人員，威脅執行者已轉向更具針對性的低流量攻擊，這些攻擊能夠規避如 Proofpoint 和 Mimecast 等傳統的安全電子郵件閘道 (SEG)。

正因為如此，Cloudflare 的雲端原生電子郵件安全解決方案經過獨特設計，能夠善用先發制人的活動情報、基於 ML 的內容分析，以及統一的 Zero Trust 平台來阻止網路釣魚威脅您的員工。

91%
的網路攻擊從網路釣魚電子郵件開始[1]

500 億
這是過去十年 BEC 攻擊造成的損失[2]

81%
的組織在過去 12 個月內經歷了一起多通道攻擊[3]



阻止商業電子郵件入侵 (BEC)

使用分層、基於 ML 的關聯式分析，來偵測被冒充和遭入侵的帳戶。

隔離延遲和多通道攻擊

讓使用者免受透過未知和混淆連結傳遞的惡意 Web 內容影響。

封鎖勒索軟體和惡意附件

防止勒索行為和惡意程式碼破壞您的組織。

更強的保護性和簡便性

實作分層網路安全，從而以較低的成本提供更強的保護

隨著網路釣魚攻擊的不斷激增，Microsoft 和 Google 繼續擴建原生功能，以支援基本的電子郵件和資料保護功能，例如，驗證、封存和用戶端加密。然而，威脅執行者卻改進了策略來執行更具針對性和規避性的攻擊，這些攻擊往往可以繞過原生安全控制，從而提高成功率。

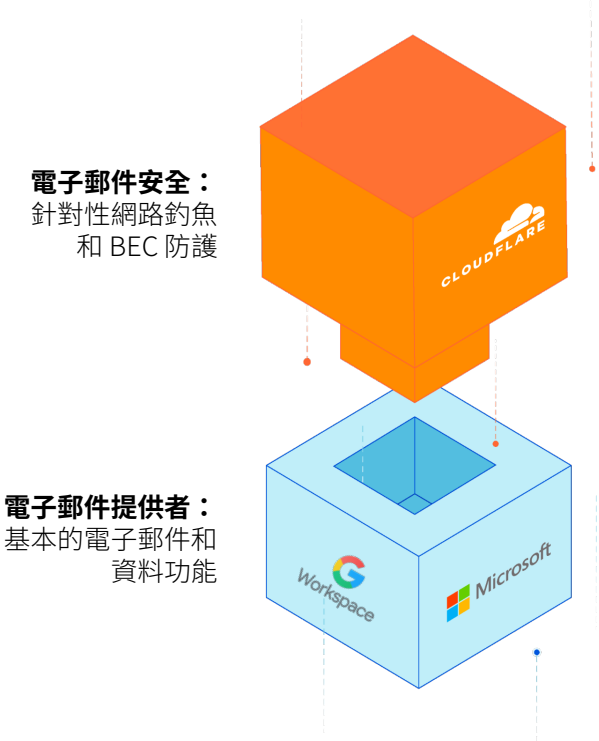
透過疊加實施 Cloudflare 解決方案，組織可以自動封鎖或隔離針對性網路釣魚攻擊，這些攻擊利用惡意連結、附件和遭入侵的帳戶來竊取敏感性資訊和實施金融詐騙。

擴充現有的電子郵件安全控制

Cloudflare 的雲端原生電子郵件安全解決方案可以在幾分鐘內完成部署，以增強現有的 SEG 部署，或為 Microsoft 和 Google 的內建電子郵件功能提供補充。幾乎無需調整，組織便能夠實現更強的網路釣魚防護，同時減少在持續安全管理上投入的時間和精力。

「自從 [在 M365 上] 實作 Cloudflare 以來，我們的使用者每天收到的惡意或可疑電子郵件數量減少了 50%。這就為我們騰出了好幾個小時的時間，可以重新用於其他目標。」

Werner Enterprises
（財富 1,000 強公司）



重新利用因自動化程度提高而省下來的時間

Cloudflare 的自動化輕量級解決方案可與 Microsoft 和 Google 工作流程無縫整合，同時為分析師活動提供單一而直覺化的 UI。

偵測功效達到 99.997%

將電子郵件提供者的原生功能與 Cloudflare 的網路釣魚和 BEC 防護相結合，可確保企業擁有全面的覆蓋範圍，從而將風險降至最低。

以更低的成本實現更大的價值

用 Cloudflare 的低觸控解決方案取代過時、昂貴且複雜的部署，可降低營運開銷、備援功能以及過度調整。

阻止複雜的 BEC 攻擊

報告損失達 500 億美元並在不斷增長

在過去十年中，BEC 攻擊造成了驚人的經濟損失，而令人吃驚的是，一些組織仍然沒有優先處理這種有效的金融詐騙形式。雖然 BEC 攻擊在網路釣魚威脅中所佔的比例要小得多，但 SEG 和雲端電子郵件提供者往往不會發現這類攻擊，從而導致更大的財務損失。這些有針對性的攻擊很難發現，因為它們會利用被冒充或遭入侵的帳戶和對話環境來偽裝成員工或受信任的廠商。

將 Zero Trust 原則延伸至電子郵件

當利用遭入侵的員工或廠商電子郵件帳戶時，攻擊者可以規避傳統的安全控制，這些控制僅會嘗試確認傳送者帳戶的合法性。Cloudflare 會進一步分析大量的行為屬性、書寫模式、情緒指標和交談歷史，以確定傳送者的真實性。Cloudflare 的 ML 支援的威脅模型和廣泛的網路情報提供了最有效的武器，可以抵禦用來獲取詐騙性付款的遭入侵帳戶。

圖 1：郵件分析

使用以 ML 為基礎的關聯式分析來偵測 BEC

準確識別 BEC 攻擊不僅需要對郵件進行結構分析。成功偵測還需要精細理解對話風格和意圖的變化。Cloudflare 龐大的網路遙測（每天超過 3T 的 DNS 要求）和不斷演進的 ML 模型為小型模式分析引擎提供支援，該引擎會解構電子郵件的所有方面來評估書寫模式、情緒、歷史背景以及大量的其他變數，幫助發現寄件者的真實性。

隔離基於連結的攻擊

基於連結的攻擊已成為竊取認證、載入惡意程式碼/勒索軟體以及擷取敏感性資訊的常用方法。結合使用電子郵件、聊天、簡訊、社交和其他應用程式來傳遞這些連結，使得確保員工和資料免遭針對性網路釣魚攻擊的過程更加複雜。

Cloudflare 透過在我們的全球雲端網路而非使用者的本機裝置上遠端轉譯所有 Web 程式碼，解決了基於連結的網路釣魚攻擊問題。這不僅緩解了惡意程式碼和瀏覽器 zero-day 攻擊，同時還可以精細化控制使用者動作（例如，停用鍵盤輸入）來防止認證收集和資料外洩。

消除網路釣魚風險而不拖慢員工效率

透過整合新一代瀏覽器隔離功能（基於我們獨特的網路向量渲染 (NVR) 技術構建），Cloudflare 能夠提供一款無縫、安全且可擴展的解決方案，來隔離潛在的惡意連結。與佔用大量頻寬的技術不同，NVR 會將安全繪製命令串流至裝置。這有助於消除惡意 Web 內容的風險，而不影響終端使用者體驗。藉助 NVR 以及 Cloudflare 的低延遲網路，組織不僅能夠隔離多通道威脅，還可確保員工的生產力無中斷。

快速調查與解決

直觀、低觸控的安全管理

憑藉更高的自動化程度以及獲得最佳結果所需的最低設定，Cloudflare 顯著減少了持續電子郵件安全管理所需的時間和精力。網路安全團隊可以立即完整檢視儀表板中的所有主要指標和趨勢，並且只需按一下，即可瞭解已標記郵件的更精細的詳細資料。透過深入剖析趨勢，可以快速發現頻繁的攻擊類型、成為攻擊目標的高管、已緩解的延遲攻擊以及其他關鍵資料點。

所有分析、遙測、值得注意的威脅以及入侵指標 (IOC) 都透過廣泛的 API 提供，以便輕鬆整合到現有的分析工作流程和協調工具中。

「我經常跟同事說，使用 Cloudflare 作為雲端 Saas 解決方案非常簡單輕鬆，而且我對它的高度準確性極為滿意。」

日本航空

受管理的偵測和回應 (PhishGuard)

Cloudflare 的受管理電子郵件安全服務 PhishGuard 可補充您現有的 SOC 團隊，以騰出安全調查週期，並提供有價值的威脅情報。PhishGuard 可透過協助調查、內部人員威脅評估、主動打擊欺詐以及複雜的補救需求，幫助消除網路釣魚活動。PhishGuard 擴展了網路安全資源和專業知識，可以主動通知潛在的欺詐和內部人員威脅，同時還可以執行基於電子郵件的威脅搜尋。

PhishGuard 功能和優點：

- 受管網路釣魚提交和事件回應，以加快解決問題。
- 主動式 BEC 和詐騙通知，讓組織可以在攻擊生命週期早期快速回應。
- 用於即時監控、定期帳戶審查以及持續威脅評估的專用資源。
- 基於對受管環境的威脅分析的自訂封鎖簽章。

1100+

小時，這是實現手動分流工作自動化後每年節省的時間

Cloudflare 的自動化解決方案可消除耗時的手動工作，從而縮短回應時間並釋放額外的週期。

50%

（在 M365 上）傳遞的惡意或可疑電子郵件減少

在 Microsoft 365 上實施 Cloudflare 解決方案，讓組織能夠發現針對性攻擊，並減少惡意電子郵件總數。

40

小時，這是七年來在電子郵件安全設定上花費的總時間

Cloudflare 的低觸控電子郵件安全幾乎無需前期設定和持續調整，可提供開箱即用的高偵測功效。

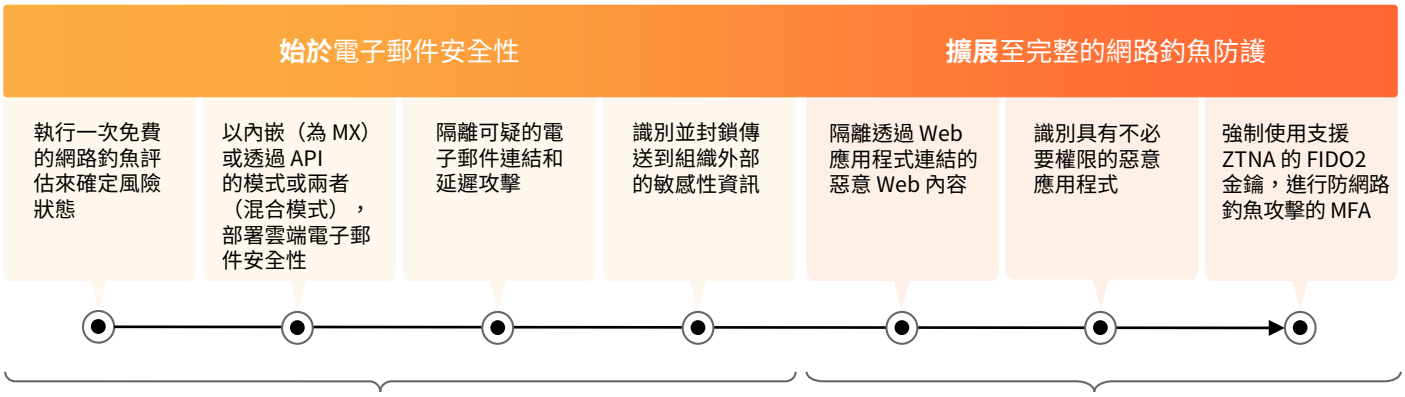
優點

完整的多通道保護

隨著網路釣魚活動快速擴展到電子郵件之外，現在，組織比以往任何時候都更迫切地需要實作網路釣魚解決方案，從而提供一個簡單快速的路徑來實現完整的多通道保護。

使用 Cloudflare 的統一安全平台，組織可以先部署領先業界的電子郵件安全性，以快速解決最重要的網路釣魚通道；然後輕鬆啟用 Zero Trust 服務，將防護擴展到所有通道，從而有效阻止已知和新出現的網路釣魚威脅。

- **低觸控、高功效保護：**
  只需極少調整，即可將網路釣魚風險降至最低，並提供領先業界的偵測功效。
- **更大的整合，更低的成本：**
  透過完全整合的單一平台解決所有網路釣魚使用案例，從而減少支出。
- **快速部署，易於管理：**
  確保即時保護，同時減少持續管理所需的時間和精力。



評估與比較

評估目前的電子郵件防禦系統，瞭解遺漏了哪些威脅

花幾分鐘時間執行一次免費的追溯掃描，瞭解哪些網路釣魚威脅在過去 14 天內僥倖逃過，或要求進行網路釣魚風險評估 (PRA)，監控收件匣中接收的電子郵件是否包含網路釣魚。與其他開箱即用的零調整提供者進行比較，看看哪款電子郵件安全解決方案可提供最快速且最簡單的保護。

執行一次追溯掃描　　申請 PRA

1. 2020 年 Deloitte 研究：來源
2. 2023 年 FBI IC3 PSA：來源
3. 2023 年 Forrester 商機快照：來源

