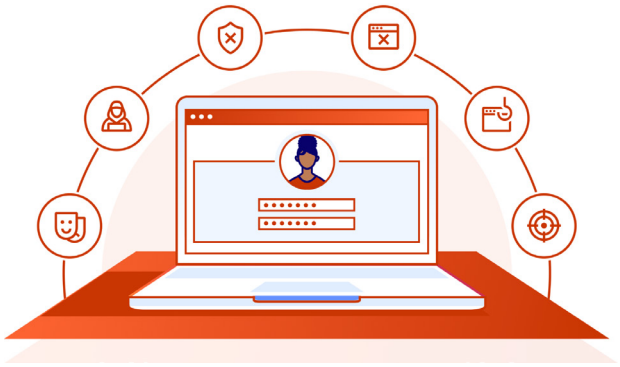
保護員工免遭多通道網路釣魚的威脅

超越收件匣範圍的分層保護



概觀

網路釣魚攻擊不再局限於電子郵件

雖然電子郵件仍然是網路釣魚活動中最普遍、最有效的傳遞機制，但攻擊者越來越多地運用巧妙的策略，在用於日常通訊和協作的多個通道（即各種應用程式）中攻擊和利用使用者。這些攻擊往往採用巧妙混淆的連結來欺騙使用者，並將其目標轉向惡意內容和不安全的環境。

更多通道 = 更多利用員工的方式

在電子郵件和其他協作應用程式內透過欺騙性連結攻擊員工可讓攻擊者繞過傳統的偵測方法，同時以增加真實感的方式吸引使用者。這會提高員工點擊惡意 Web 內容、洩露認證或外洩敏感性資訊的風險。電子郵件安全性僅有助於處理源於收件匣的攻擊，當這些攻擊傳播至其他應用程式時，必須採用更廣泛的安全解決方案才能將其封鎖。

挑戰

多通道威脅可以繞過傳統的電子郵件篩選

多通道攻擊利用複雜的連結混淆和各種各樣的協作應用程式，誘騙使用者點擊惡意內容或外洩敏感性資訊。這種類型的攻擊很難應對，原因如下：

- **連結混淆**（URL 重新導向/縮短程式）
- **基於影像的 URL**（QR 碼）
- **延遲攻擊**（傳遞後啟用）
- **分散式參與**（跨各種工作應用程式）

89%

的安全決策者對多通道威脅感到擔憂[1]

#1

惡意連結是偵測數量最多的網路釣魚威脅[2]

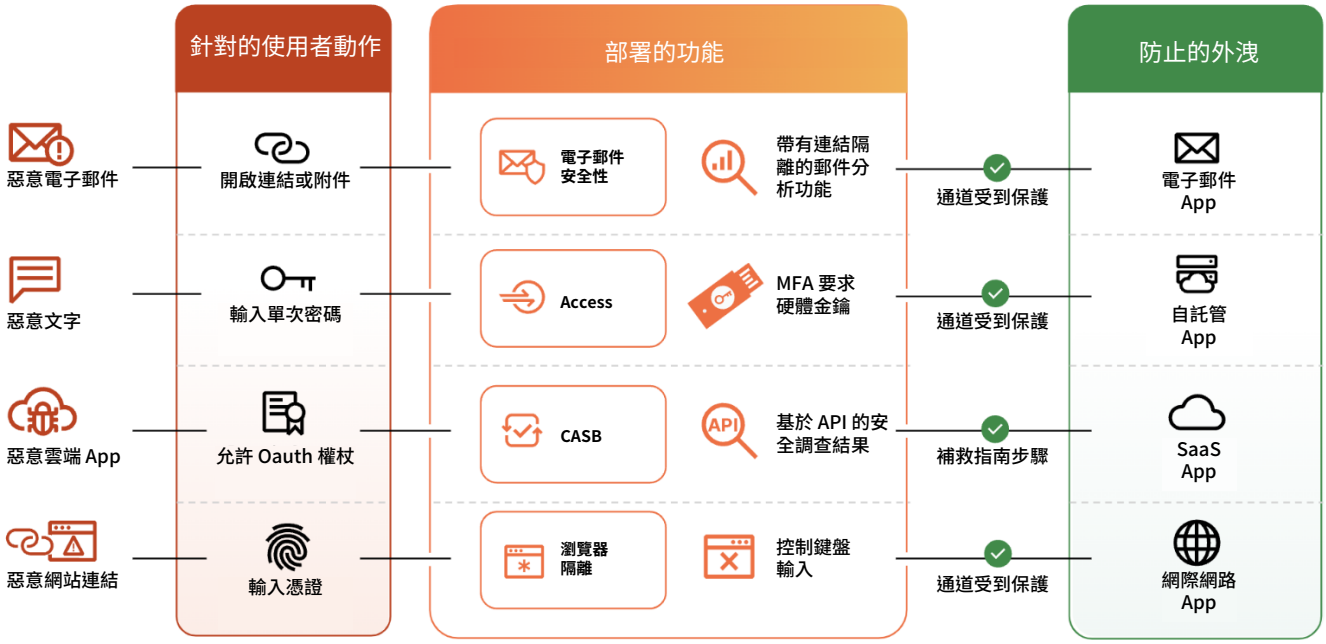
81%

的組織在過去 12 個月內經歷了一起多通道攻擊[1]

解決方案

在每一個網路釣魚暴露點提供統一的安全性

阻止多通道攻擊需要一個平台，它能夠解決員工工作流程和應用程式內互動中存在的所有漏洞。而這正是 Cloudflare 提供最完整的網路釣魚解決方案的原因，該解決方案專注於為員工和應用程式提供無縫保護。藉助 Cloudflare One 平台，組織可以充分利用原生整合的電子郵件安全性 (ES) + Zero Trust 服務，為電子郵件、自託管應用程式、SaaS 應用程式和網際網路應用程式部署分層保護，從而提供縱深防禦來阻止詐騙性付款和資料外洩。



先發制人，阻止電子郵件傳播的威脅

透過採用 AI/ML 技術的內容分析，偵測商業電子郵件入侵 (BEC)、惡意程式碼以及其他源自電子郵件的威脅，以實現自動化保護。

防止因認證盜竊而導致的外洩

如果認證被盜或外洩，則條件式存取 + 硬體金鑰要求會充當最後一道防線，來阻止外洩。

封鎖並隔離基於連結的規避性攻擊

讓使用者免遭針對性攻擊，這些攻擊會在常用的傳訊應用程式中，透過巧妙混淆且很難發現的連結誘騙員工。

阻止電子郵件傳播的威脅 (ES)

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。透過使用 Cloudflare 擴充或取代目前的電子郵件防禦系統，組織可以自動緩解複雜的網路釣魚攻擊，這些攻擊利用內嵌的電子郵件連結、附件以及被冒充或遭入侵的帳戶，來竊取敏感性資訊和實施金融詐騙。

Cloudflare 的輕量型、雲端原生解決方案可以在幾分鐘內完成部署，為 Microsoft 和 Google 的內建電子郵件功能提供補充。由於自動化程度提高，並且只需最小調整即可獲得最佳結果，Cloudflare 顯著減少了持續電子郵件安全管理所需的時間和精力。

企業電子郵件入侵 (BEC)
採用 AI/ML 技術的內容分析會解構每一條訊息，來評估交談記錄、書寫模式、情緒以及其他變數，從而確定寄件者的真實性。

勒索軟體和惡意附件
使用針對有效負載的 ML 偵測模型、未簽名偵測、電腦視覺、遠端擷取以及其他形式的分析，識別加密和未加密的惡意負載。

惡意電子郵件連結
結合使用進階技術（用於解構和深入剖析複雜的 URL）與適應性連結隔離，以確保為員工提供安全、順暢的 Web 體驗。

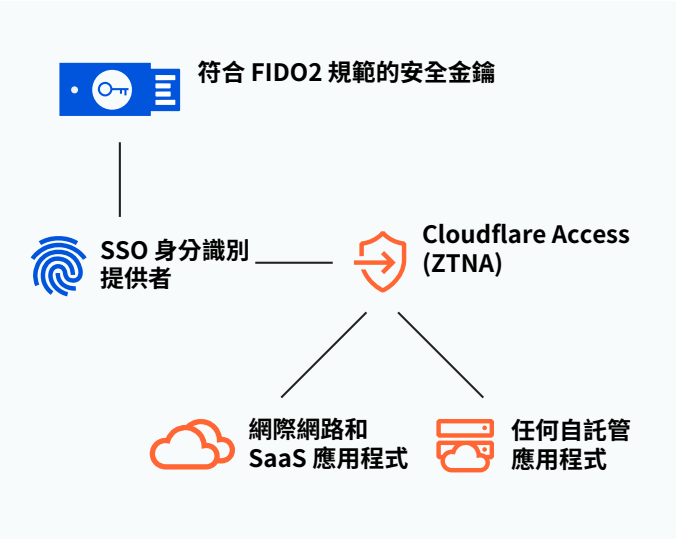
緩解 OAuth 網路釣魚攻擊 (CASB)

OAuth 網路釣魚利用合法的身分識別提供者和授權工作流程，誘騙使用者為惡意應用程式授予權限。Cloudflare One 平台不僅能夠偵測出此類應用程式，還會提供補救指導來快速緩解這些威脅。

防止因認證外洩而導致的洩露 (ZTNA)

儘管很多組織實施了大量的預防措施來避免員工認證落入宵小之手，但真相卻令人痛苦，即預防措施永遠不可能做到 100% 萬無一失。如果認證不幸被盜或無意中外洩，必須有最後一道防線來防止全面的洩露。

使用 Cloudflare Access 作為每一種資源（包括自託管或非 Web 資源）的彙總層，組織可以一致地強制執行符合 FIDO2 規範的驗證，來進行防網路釣魚攻擊的 MFA。這樣，即使員工認證外洩，組織仍然能夠確保其資料受到保護。



隔離基於連結的攻擊 (ES + RBI + SWG)

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、社交和雲端磁碟來傳遞這些連結，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 瀏覽器隔離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。

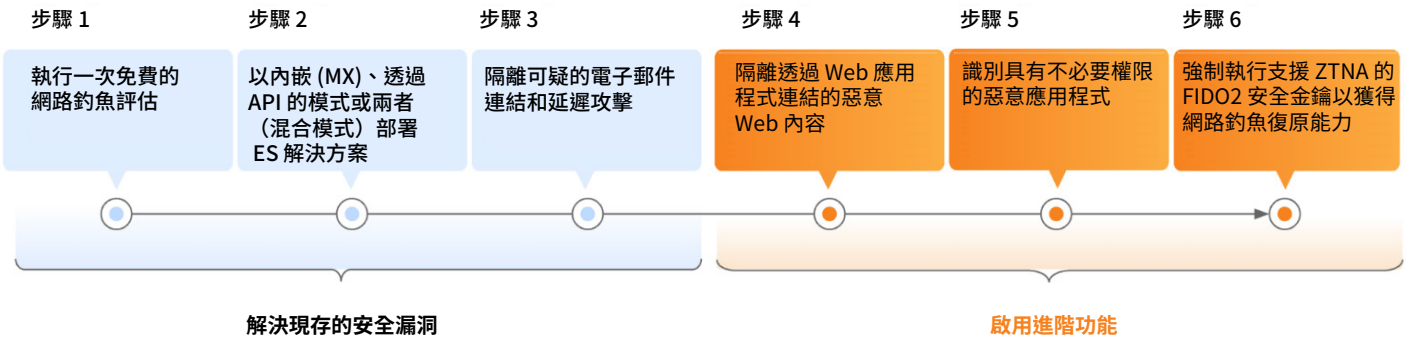
優點

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 One 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；然後輕鬆啟用其他 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（O365 收件匣），瞭解在過去 14 天內哪些網路釣魚威脅成功送達，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。

瞭解哪些網路釣魚威脅正在突破您的防禦系統

執行一次追溯掃描　申請 PRA

CLOUDFLARE

1. 2023 年 Forrester 商機快照：來源
2. 2023 年網路釣魚威脅報告來源