CLOUDFLARE

解決方案簡述

Cloudflare + Microsoft 365 網路釣魚防護

為安全工作空間通訊提供自發的多通道保護

棄用傳統閘道並升級網路釣魚防護

21 世紀初期，引入了安全電子郵件閘道 (SEG) 來應對不斷增長的電子郵件路由和篩選需求。儘管 SEG 多年來成功履行了使命，但它的基本設計使其無法跟上網路釣魚威脅範圍和複雜程度快速增長的步調。

不斷更新最初為內部部署伺服器構建的手動規則集和原則，只會增加維護 SEG 所需的時間和精力。這不僅導致成本和複雜性增加，而且仍然無法攔截最危險的威脅，例如，商業電子郵件入侵 (BEC) 攻擊。導致開支增加和有效性降低的原因如下：

- **新興的網路釣魚策略和 zero-day 威脅：**新型網路釣魚攻擊越來越多地採用詐騙性策略，旨在規避靜態篩選器和傳統控制。這就導致 SEG 很難封鎖缺少已知入侵指標的新威脅。
- **複雜的部署：**SEG 需要大量的設定和持續的調整來應對新出現的威脅，同時還需要多個附加模組以充分利用各種功能。
- **耗費時間的事件回應：**當可疑或惡意活動繞過已部署的 SEG 控制時，調查與回應的過程可能既冗長又繁瑣，涉及到各種各樣的介面和工作流程。

部署高功效、低觸控保護

隨著組織繼續採用 Microsoft 365 來增強混合員工的通訊和協作，務必在利用 Microsoft 原生安全功能的同時，整合基於機器學習的補充解決方案，以自動封鎖和隔離最危險的威脅。此策略不僅顯著降低了網路釣魚風險，還簡化了工作流程；最大程度減少了持續安全管理所需的時間和精力。

91%

的網路攻擊從網路釣魚電子郵件開始[1]

排名第 1 的

攻擊手段，用於實施欺詐和取得存取權[2]

500 億美元

這是過去十年 BEC 攻擊造成的損失[3]

488 萬美元

這是 2024 年資料外洩的平均成本[4]

1. 2020 年 Deloitte 研究
2. Microsoft SIR 報告
3. 2023 年 FBI IC3 PSA
4. 2024 年 IBM 資料外洩成本

Microsoft 的電子郵件安全功能

移除 SEG 重疊以降低風險和成本

分析師一致認為，整合各種功能以最大程度減少重疊功能有助於組織降低成本和複雜性。然而，他們也建議組織仔細評估原生功能，以確保它們滿足所有使用案例。

隨著 Microsoft 繼續擴建其基本電子郵件安全功能，與 SEG 重疊的功能不斷增加，這為組織提供了一個機會，可以利用 E3 或 E5 授權中已經包括的功能來簡化安全營運。透過這種轉變，組織可消除複雜而昂貴的 SEG 部署，可以重新分配一部分預算，用來整合輕量型解決方案，從而有效解決最危險的網路釣魚威脅。

Cloudflare 電子郵件安全性提供一個低觸控的整合式解決方案，它使用機器學習威脅分析擴充了 Microsoft 365，從而實現 BEC 和多通道攻擊偵測自動化。

與 SEG 功能重疊的領域包括：

- **電子郵件檢疫**
  針對垃圾郵件和大量郵件採用基於規則的原則，針對已知惡意程式碼採用基於簽名的偵測。
- **URL 和附件保護**
  針對所有電子郵件連結的基本重寫功能，以及針對附件的沙箱功能。
- **調查和威脅搜尋**
  電子郵件搜尋、事件調查和關聯、搜尋以及補救。
- **資訊保護**
  針對電子郵件、檔案和端點的加密、封存和 DLP 原則。
- **意識與訓練**
  針對終端使用者的網路釣魚攻擊模擬和訓練。

Exchange Online Protection

每個方案中都包含此服務，該服務還提供基本的電子郵件檢疫，用來篩選大量郵件、垃圾郵件和惡意程式碼。

- 反垃圾郵件
- 基於簽名的惡意程式碼防護

Microsoft Purview (DLP)

可設定的資料丟失預防規則和強制執行。與 Microsoft 資訊保護整合。

- 適用於電子郵件和檔案的 DLP
- 適用於 Teams 的 DLP
- 適用於端點的 DLP

Defender for O365 方案 1

其他安全控制，用於針對惡意連結和附件提供基本防護。

- 安全連結（URL 重寫）
- 安全附件（沙箱）
- 內部電子郵件保護

Defender for O365 方案 2

包括方案 1 中的全部功能，以及用於威脅搜尋、調查、訓練和回應的其他功能。

- 威脅搜尋
- 跨網域事件關聯
- 網路攻擊模擬訓練

E3 授權

E3 授權 + 合規性

E3 授權 + 合規性 + 安全性

E5 授權

● 完整　● 受限　● 無

	SEG	M365	Cloudflare
威脅預防			
允許/封鎖清單	●	●	●
已知惡意寄件者	●	●	●
已知惡意 URL/附件	●	●	●
垃圾郵件/大量郵件篩選	●	●	●
機器學習（內容分析）	●	●	●
Zero-Day 惡意程式碼/勒索軟體	●	●	●
惡意連結	●	●	●
URL 重寫（點擊時間分析）	●	●	●
適應性連結隔離	●	●	●
企業電子郵件入侵 (BEC)	●	●	●
員工假冒	●	●	●
廠商假冒	●	●	●
員工入侵 (ATO)	●	●	●
廠商入侵	●	●	●
DMARC 管理	●	●	●
惡意應用程式偵測（OAuth 網路釣魚）	●	●	●
Web 內容安全性	●	●	●
安全意識與訓練	●	●	●
威脅回應			
直觀的單一介面	●	●	●
自動化威脅分類	●	●	●
快速搜尋與調查	●	●	●
自動撤銷	●	●	●
隨需報告	●	●	●
受管理的偵測和回應服務	●	●	●
資料保護			
加密	●	●	●
封存	●	●	●
電子郵件 DLP	●	●	●
雲端 DLP（協作應用程式）	●	●	●
網路 DLP	●	●	●

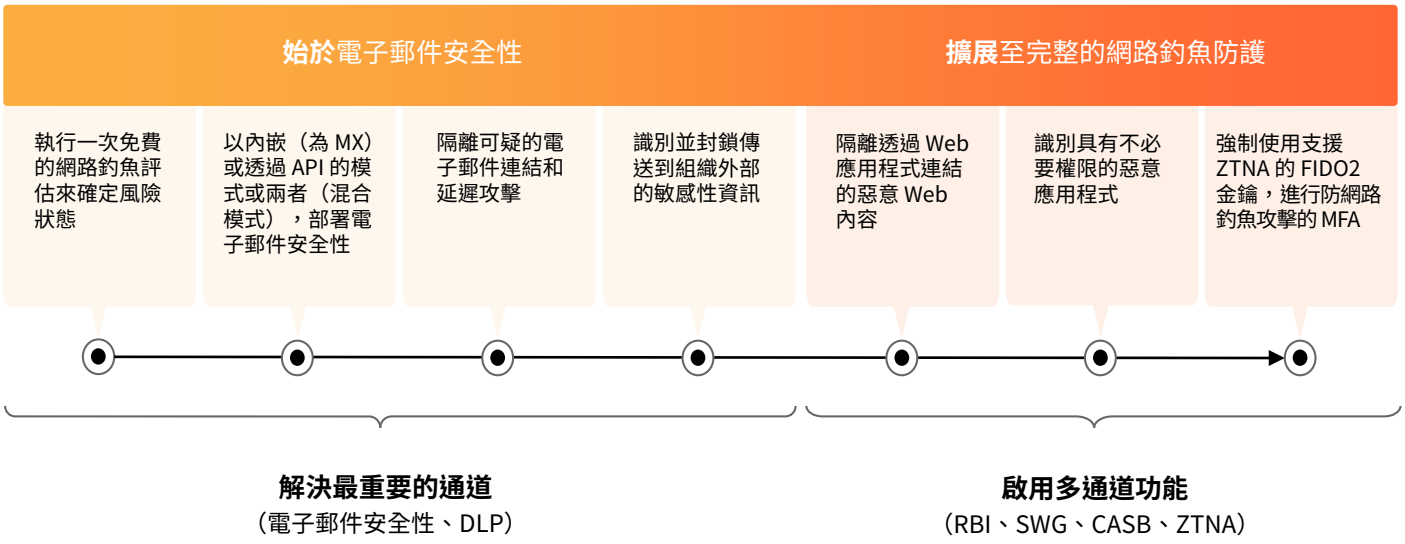
優點

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)，以監控收件匣中是否存在送達時含有網路釣魚威脅的電子郵件。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

