CLOUDFLARE
AREA 1 SECURITY

解決方案簡述

Cloudflare Area 1 和 Google Cloud：

整合式雲端電子郵件安全性與先發制人的防網路釣魚

產業挑戰：

如今的網路釣魚攻擊（例如，無惡意軟體的企業電子郵件入侵 (BEC)、基於帳戶盜用的欺詐以及內部人員威脅）非常複雜，傳統的安全電子郵件閘道或電子郵件驗證很難偵測出來。

解決方案：

Cloudflare Area 1 Email Security 服務會主動爬行網路來探索網路釣魚活動，憑藉該早期探索，再加上關聯式電子郵件分析技術，保護您的收件匣免受網路釣魚攻擊 — 從而避免發生損害。

Area 1 在 Google Cloud Platform 基礎上建構，幾分鐘即可完成部署，以提供同類最佳、縱深防禦的防網路釣魚安全性階層。

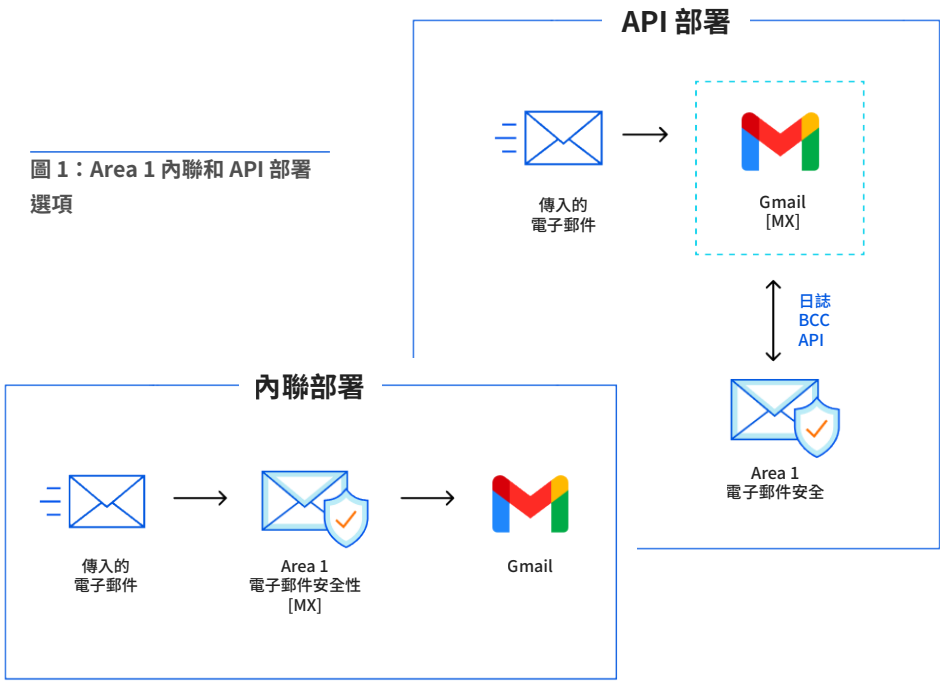

圖 1：Area 1 內聯和 API 部署選項

防禦針對排名第一的雲端應用程式（電子郵件）進行的現代攻擊。

先發制人地阻止網路釣魚攻擊、BEC、電子郵件欺詐和其他進階威脅。

透過 Cloudflare Area 1 和 Cloudflare 遠端瀏覽器隔離整合，隔離和防止多通道威脅。

探索遭入侵的帳戶和網域，以及攻擊者用來繞過 SPF/DKIM/DMARC 的新網域、類似網域和近接網域。

為什麼選擇 Cloudflare Area 1：

先發制人的網路安全

透過提前識別攻擊者基礎架構和傳遞機制，於攻擊週期的最初階段即阻止網路釣魚。

全面的保護

涵蓋全部電子郵件攻擊類型（URL、承載、BEC）、媒介（電子郵件、Web、網路、多通道）以及攻擊渠道（外部、內部、信賴的合作夥伴）。

關聯式分析

善用進階偵測技術（語言分析、電腦視覺和社交圖表等），讓 BEC、廠商電子郵件欺詐和其他進階威脅無所遁形。

持續的保護

從電子郵件寄出一直到寄達收件匣的每個環節，皆採用帶有威脅防護層級的縱深防禦。

為什麼選擇 Cloudflare Area 1 加 Google Cloud：

- **提高營運效率 —** 將傳統的安全電子郵件閘道取代為現代的雲端優先架構，藉此來降低複雜性。
- **無縫的彈性部署 —** 部署完全彈性的 Area 1 服務（只需不到 5 分鐘），並與 Google Cloud 的原生功能（例如，反垃圾郵件、DLP、加密和封存）無縫整合。
- **簡化的 SaaS 安全性 —** 除了整合式 Area 1 雲端電子郵件安全，Cloudflare Zero Trust 平台還提供適用於 Google 的雲端存取安全性代理程式 (CASB) 功能。輕鬆防止資料外洩和合規性違規，並取得一站式服務來阻止資料遺失、網路釣魚、勒索軟體、影子 IT 和組織內的橫向移動。

案例研究：標準普爾 100 消費者包裝商品領導者保護主管和使用者免受雲端電子郵件威脅

客戶挑戰	使用 Cloudflare Area 1 的結果
• Google Workspace 和現有網路安全基礎架構面臨威脅 • BEC 攻擊以資深主管和董事會成員為目標 • IT 團隊花費時間和資源不斷地調整電子郵件安全性規則和封鎖清單	• 在一年內封鎖了超過 8 百萬個針對性攻擊 • 現在，IT 團隊能夠為董事會會議提供更好的電子郵件安全性指標和報告 • 提高生產力並顯著降低網路安全風險

若要瞭解 Cloudflare Area 1 如何增強 Gmail 網路釣魚防禦，請要求自訂風險評估（按一下這裡）。