Cloudflare Area 1 電子郵件安全

先發制人地保護您的使用者免受網路釣魚、企業電子郵件入侵 (BEC) 和電子郵件供應鏈攻擊。

網路釣魚是組織最常面對且造成最多損失的網路威脅之一。

Cloudflare Area 1 是一個能在攻擊到達使用者收件匣之前就識別威脅並將其封鎖的雲端原生電子郵件安全平台，能夠更有效地防禦可躲過現有防禦措施的魚叉式網路釣魚、BEC 和其他進階威脅。

Area 1 深度整合 Microsoft 和 Google 的環境和工作流程，以加強雲端電子郵件提供者的內建安全性。

Area 1 是我們 Zero Trust 服務的一部分。

阻止針對性的網路釣魚威脅

Area 1 能防禦各式網路釣魚攻擊，包括大規模的攻擊活動和經歷數月縝密規畫的高度針對性電子郵件供應鏈入侵嘗試。

網路釣魚

Verizon 2021 DBIR 將網路釣魚稱為最常見的入侵手法。Area 1 能透過大規模網路爬行、小型模式分析和增強偵測的組合，在網路釣魚攻擊抵達使用者收件匣的數天前就先行將其擋下。

BEC 和社交工程威脅

BEC 意指攻擊者透過冒充或入侵受信任的實體以竊取錢財和資料。Area 1 透過分析電子郵件通訊內容和上下文來阻止這種「大海撈針」式的威脅 。

電子郵件供應鏈攻擊

攻擊者透過入侵廠商電子郵件、觀察郵件模式和攔截現有對話來執行發票詐騙。Area 1 能透過分析郵件對話、訊息情緒和社交圖表來阻止這些精心策劃的攻擊。

敲詐和勒索軟體電子郵件

Gartner 估計有 40% 的勒索軟體攻擊都是從電子郵件開始的。Area 1 能在勒索軟體電子郵件抵達使用者收件匣前就主動進行阻擋，同時在惡意郵件擴散前就將其移除。

超越傳統電子郵件閘道

先發制人

透過提前識別攻擊者的基礎結構和傳遞機制，於攻擊週期的最初階段即阻止網路釣魚。

上下文相關

運用進階偵測技術（語言分析、電腦視覺和社交圖表等）讓 BEC、廠商電子郵件詐騙和其他無承載威脅無所遁形。

全面

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

連續不斷

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。

優點

增強原生電子郵件安全

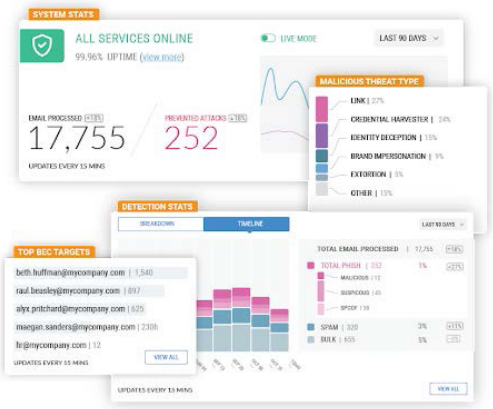
阻止躲過內建安全層的進階網路釣魚和 BEC 攻擊。在不影響電子郵件生產力的情況下，運用雲端電子郵件環境的深層整合。

採用雲端優先架構

採用現代化且可擴充的架構，揮別傳統電子郵件閘道笨重且不靈活的缺點。減少重複原生電子郵件安全功能的安全層支出。

為您的 SOC 團隊節省時間

幾分鐘內即可完成部署，無需任何硬體、代理程式或設備。不再需要花費時間建立和調整原則。透過 SIEM 和 SOAR 整合加快 SOC 調查。



請求網路釣魚風險評估

請求在您的即時電子郵件生產流量上執行 Area 1，並即時查看哪些電子郵件攻擊通過了現有的安全控制。

該評估不需安裝硬體或軟體，也不會影響郵件流程。

如要請求評估，請點擊此處。