# 電子郵件連結隔離

隔離電子郵件連結以縮小攻擊面並簡化作業

## 套用瀏覽器隔離保護和控制來降低網路釣魚風險

### 挑戰：複雜的多通道網路釣魚

多通道網路釣魚可巧妙的規避篩選規則，藉此跨越電子郵件和進行 Web 傳遞。此類常見類型包括：

- **延遲的網路釣魚：**電子郵件內初始良性的連結在傳遞之後被惡意目的地裝備成武器。
- **雲端服務網路釣魚：**危險的 HTTPS 連結與常見的雲端服務（例如，Google Drive、Box）極為類似

若要阻止此類威脅，必須裝備新式電子郵件保護，以對所有連結套用 Zero Trust「從不信任，始終驗證」審查。

### 解決方案：電子郵件連結隔離

整合遠端瀏覽器隔離 (RBI)
功能與雲端電子郵件安全性 (CES)
套用該審查來增強網路釣魚
保護。Cloudflare Area 1
客戶可開啟
Cloudflare 瀏覽器隔離
來抵禦這些
多通道威脅。

管理員可控制隔離網頁上的使用者互動（例如，限制鍵盤輸入和檔案上傳）來防止網路釣魚影響，例如，憑證收集或機密資料竊取。

此外，在隔離瀏覽器中開啟電子郵件連結，也可以透過在遠離本機裝置的雲端執行所有程式碼，來抵禦惡意軟體。

### 分析師們是這樣說的：

*「在內部解析的基於電子郵件的 URL 通常用於對員工進行網路釣魚。隔離這些 URL 可以降低網路釣魚攻擊的成功率。」*

*「大多數攻擊透過公共網際網路傳遞，即透過 Web 瀏覽或電子郵件連結誘騙使用者造訪惡意網站。只需從終端使用者桌面移除（或者更強烈的方式，即隔離），瀏覽器就會大大改進企業安全狀態，包括防止勒索軟體攻擊。」*

*「針對特定的高風險使用者（例如，財務小組）或使用案例（例如，轉譯基於電子郵件的 URL）評估並試用瀏覽器隔離解決方案，特別是在組織不願冒險的情況下。」*[1]

Gartner®

閱讀更多

## 整合 CES 與 RBI 的商業優勢

### 增強網路釣魚保護

電子郵件隔離不僅可以阻止網路釣魚連結中的有害程式碼在本機執行，還會套用資料保護控制來防止敏感性資訊落入宵小之手。

### 釋放 IT 和網路安全生產力

只需按幾下即可針對任意網站開啟電子郵件隔離。

IT 和網路安全團隊無需設定繁瑣的篩選原則，從而避免了「過度封鎖」（和限制使用者生產力）以及「封鎖不足」（並讓威脅進入）的風險。

## 範例使用案例：阻止延遲的網路釣魚

### 問題：延遲的網路釣魚可規避偵測

憑藉適當的策略和動機，延遲的網路釣魚活動可以繞過傳統的保護措施。

**活動設定：** 攻擊者可以先使用適當的電子郵件認證（SPF、DKIM、DMAR）和良性網頁，透過新建立的網域傳送一封看似真確的電子郵件。

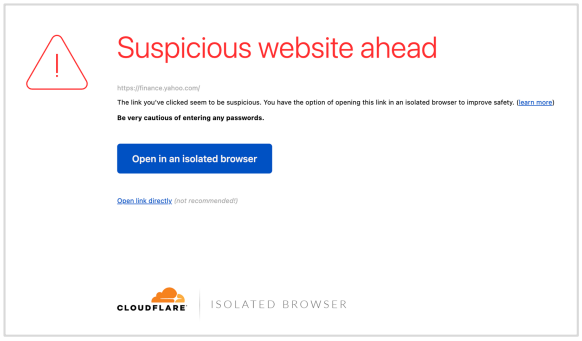
**成功傳遞至收件匣：**這些電子郵件可透過安全電子郵件閘道、基於驗證的篩選器或其他服務（依賴基於聲譽的訊號和其他決定性技術），來規避偵測。

**轉向惡意連結：**成功傳遞電子郵件後，攻擊者可透過變更攻擊者控制的網頁將連結轉向惡意目的地。例如，通常會轉向用來收集憑證的虛假登入頁面。

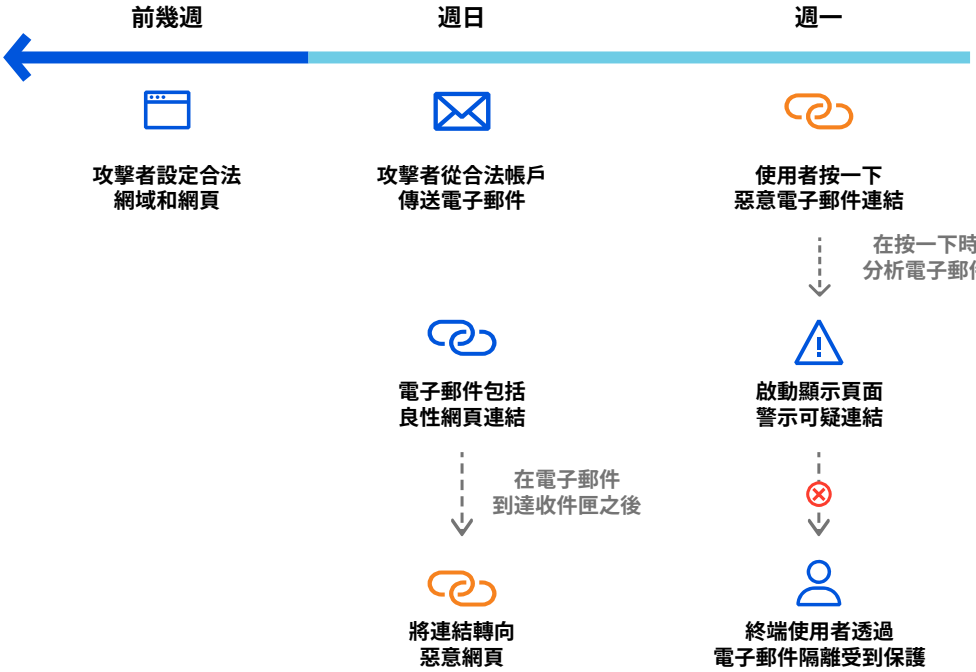
### 解決方案：隔離傳遞後的可疑連結

電子郵件連結隔離為傳遞後保護提供了一個關鍵層。Cloudflare 會分析電子郵件內使用者按下的任何連結。如果認為連結可疑或有風險，則 Cloudflare 會顯示一個警告啟動顯示頁面 *（請參閱下圖）*，如果使用者瀏覽了網頁，則會隔離該網頁。

管理員會阻止惡意程式碼在本機裝置上執行，並且可以套用資料保護控制，例如，限制檔案上傳和下載、防止使用者鍵盤輸入或以唯讀模式開啟頁面。




## 延遲的網路釣魚活動時間表




### Cloudflare 在按一下時分析每個連結

**安全連結：**明確地將使用者重新導向至此網站。

**惡意連結：**封鎖使用者使其無法導覽。

**可疑連結：**強烈阻止使用者進行導覽，並呈現一個啟動顯示警告頁面，建議他們在隔離瀏覽器中檢視連結。

# 整合雲端電子郵件安全性與 Cloudflare Zero Trust

## 使用 Zero Trust 的現代網路安全

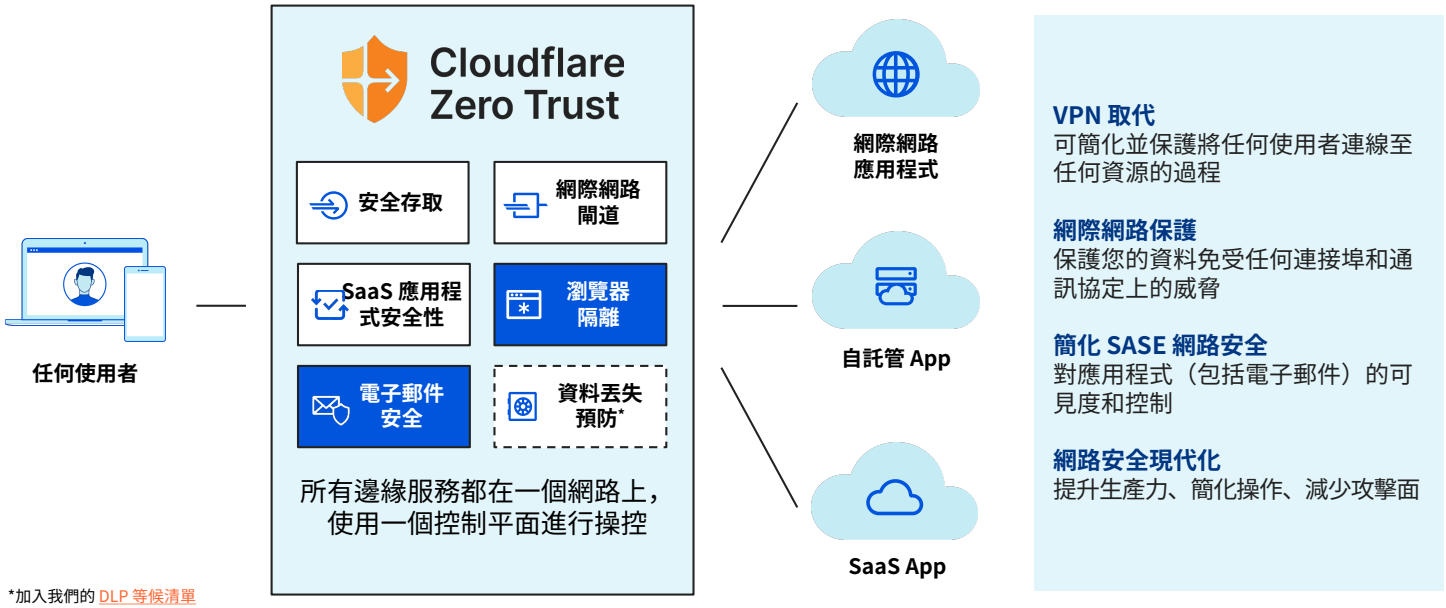
Cloudflare Zero Trust 可在遠端和辦公室使用者連線至企業應用程式和公共網際網路時，提升可見度、消除複雜性並降低風險。

2022 年 4 月 1 日，Cloudflare 完成了對 Area 1 Security 的收購，其願景是對 Zero Trust 平台的保護功能進行擴充，讓使用者免受電子郵件、Web 和網路環境中的網路釣魚攻擊。在此閱讀更多資訊。

## 電子郵件安全性：Zero Trust 的核心

Cloudflare Area 1 Email Security 透過消除來自電子郵件的盲目信任，預先阻止網路釣魚和企業電子郵件入侵 (BEC) 攻擊，增強了 Zero Trust 功能。

從不信任包括內部寄件者在內的任何寄件者。取而代之的是，確保包括電子郵件在內的所有使用者流量都經過驗證、篩選、檢查並與網際網路威脅隔離。在 Cloudflare 的 Zero Trust 服務中整合電子郵件安全性，並與 RBI、CASB 等強強聯合。




*加入我們的 DLP 等候清單

**VPN 取代**
可簡化並保護將任何使用者連線至任何資源的過程

**網際網路保護**
保護您的資料免受任何連接埠和通訊協定上的威脅

**簡化 SASE 網路安全**
對應用程式（包括電子郵件）的可見度和控制

**網路安全現代化**
提升生產力、簡化操作、減少攻擊面

### 雲端電子郵件安全性 (CES)

- 網路釣魚事件回應時間減少 90%。
- 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。
- 透過分析通訊的內容、上下文和社交圖，消除來自電子郵件的盲目信任。
- 善用與 Microsoft、Google 和其他環境的整合來增強內建安全性

### 遠程瀏覽器隔離 (RBI)

- 以「唯讀模式」開啟有風險的網站，藉此來控制使用者互動（例如，鍵盤輸入、複製和貼上、上傳/下載），從而阻止憑證入侵。
- 在 Cloudflare 的網路上執行所有瀏覽器程式碼，使本機裝置免於惡意程式碼的攻擊。
- 提供順暢而快速的終端使用者體驗。全球 95% 的網際網路使用者在 50 毫秒內即可連線至遠端瀏覽器，我們從中繪製精確的頁面複本，而不是典型的像素串流。

**立即要求網路釣魚風險評估**

**聯絡我們**

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com

REV: PMM-2022JUN

[1] *Gartner 網路安全性技術成熟度曲線報告，2021 年* /GARTNER 和 HYPE CYCLE 是 Gartner, Inc. 及/或其附屬公司在美國和其他國家/地區註冊的商標和服務標識，在此使用已獲許可。