

# Zero Trust 網路存取及私人路由

## 防止橫向行動，減少對 VPN 的依賴

信任對應應用程式存取的網路控制（例如 VPN 和 IP 位置限制）可能會擴大攻擊面、限制可見度，並讓最終使用者感到失望。Cloudflare 的 Zero Trust 網路存取與身分識別提供者協同工作，強制執行預設拒絕、Zero Trust 規則，以限制對企業應用程式、內部 IP 空間和主機名稱的存取。由 Cloudflare 廣泛且高效能的 Anycast 網路支援，讓使用者連線比 VPN 更為快速。

自從在內部部署 Zero Trust 網路存取以來，Cloudflare 已獲得了以下效益：

- 攻擊面縮小 91%<sup>1</sup>
- IT 工作量減少，節省了 2 倍成本
- 在 VPN 相關工單服務上所花費的時間縮短了 80%
- 工單數量減少了 70%
- 新員工就職每年節省超過 300 個工時，讓生產力更為提升

### Access 有何成效



#### 保護任何應用程式

Cloudflare 與身分和應用程式都無關，讓您能夠利用偏好的身分識別提供者保護任何應用程式，不論是 SaaS、雲端還是內部部署應用程式。



#### 限制企業資源之間的橫向移動

透過 IP 防火牆和 Zero Trust 規則，甚至可以將強大且一致的認證方法應用於傳統的應用程式。



#### 靈活地連接使用者，無論是否有用戶端

協助 Web 應用程式和 SSH 連線，無需用戶端軟體或終端使用者設定。對於非 Web 應用程式、RDP 連線和私有路由，則是在不同的網際網路和應用程式存取使用案例間運用一個綜合型用戶端。



#### 強制執行裝置感知的存取

在授予資源存取權限之前評估裝置狀態，包括是否存在 Gateway 用戶端、序號和 mTLS 憑證，以確保只有安全的已知裝置可以連線到您的資源。整合來自端點保護平台 (EPP) 提供者的裝置狀態，包括 Crowdstrike、Carbon Black、Sentinel One 和 Tanium。



#### 跨多個身分識別提供者啟用聯合身分驗證

整合您所有的企業身分識別提供者（Okta、Azure AD 等），以實現更安全的遷移、收購和第三方使用者存取。啟用一次性 PIN 碼，用於臨時存取，或納入社交網路身分識別來源，如 LinkedIn 和 GitHub。



#### 記錄使用者在任何應用程式中的活動

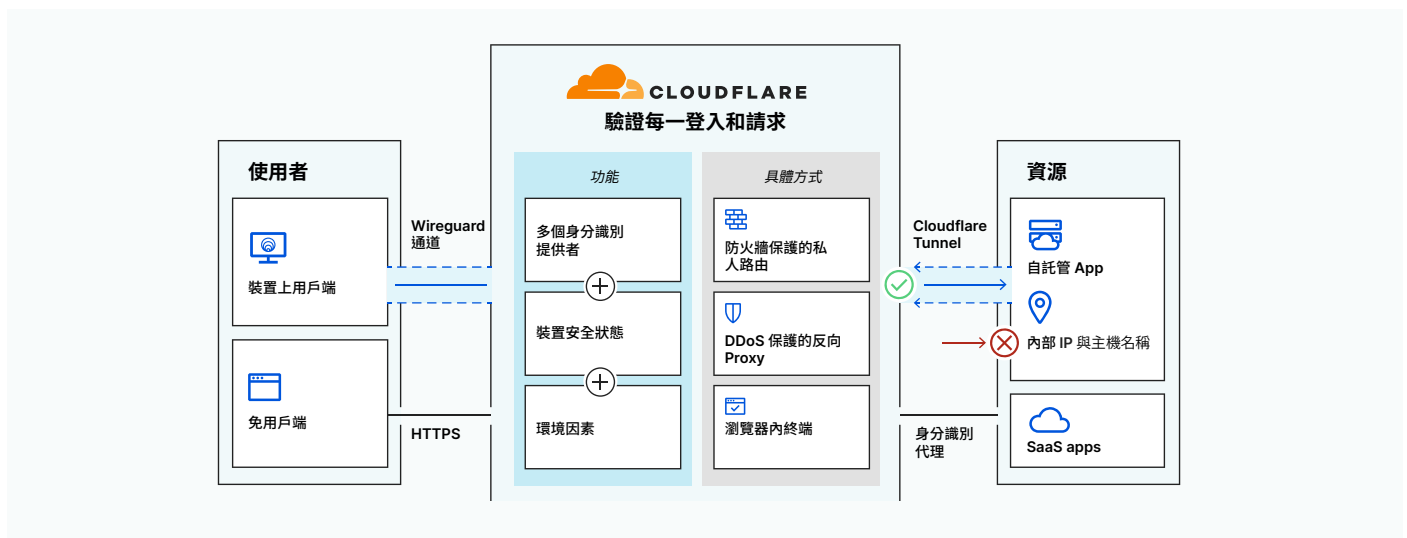
記錄在受保護應用程式中發出的任何要求，不只是登入和登出。在 Cloudflare 中彙總活動記錄，或將其匯出到您的 SIEM 提供者。

<sup>1</sup>Zero Trust 網路存取與網際網路瀏覽相結合時

## Cloudflare 的不同之處

- **無可比擬的效能**能夠透過 Cloudflare Anycast 網路中以情報為導向的最佳化路由來路由請求。平均而言，Web 應用程式的存取速度提升了 30%，且 TCP 連線的往返時間減少了 17%。我們每秒可收到 2500 多萬個 HTTP 個請求，且每秒可建立 3.9 萬個新的 TCP 連線，並透過分析這些請求和連接中的網路資料來取得情報。
- **更簡易的管理**將 Zero Trust 網路存取、安全 Web 閘道、遠端瀏覽器隔離等功能結合到單一控制平面，提供從頭開始打造的管理員體驗，而不是從多個廠商合併和拼湊的體驗。
- **單遍檢查**能夠在全球範圍內快速且一致地驗證、過濾、隔離和檢查流量，因為世界各地超過 250 個地點的每個資料中心都部署了所有 Cloudflare 服務。

## 了解詳情



使用者不使用 VPN，而是透過用戶端或 Web 瀏覽器接入企業資源。請求透過 Cloudflare 的邊緣進行路由傳送和加速後，整合來自身分識別提供者、裝置和其他上下文的訊號，對 Zero Trust 規則進行評估。過去，RDP 軟體、SMB 檔案檢視器和其他厚重的用戶端程式需要依靠 VPN 才能進行私有網路連線；現在，團隊可以透過 Cloudflare 網路以私有方式路由任何 TCP 或 UDP 流量，並進行一次性加速、驗證和篩選，藉此有助於提升效能和網路安全。

「Cloudflare Access 使我們無需開發自己的身分識別與存取管理 (IAM) 系統。我們不需要將使用者權限功能建置在由 Access 保護的應用程式中。我們全心投入；公司每一個人都有席位。」

Jim Tyrrell  
Canva 基礎結構主管



「Delivery Hero 始終致力於為客戶提供出色的體驗。在 Cloudflare Access 的協助下，我們的內部團隊亦能享受同樣的體驗：擁有安全的工作環境，而且無需 VPN 就能從全球各地存取我們的所有應用程式。」

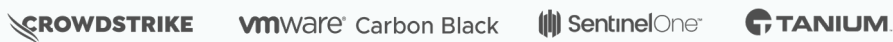
William Carminato  
Delivery Hero 工程部資深總監

**Delivery Hero**

## 身分識別與存取管理 (IAM) 整合



## 端點保護平台 (EPP) 整合



## 主要特色

| 📁 統一原則                     |     |
|----------------------------|-----|
| 自訂應用程式、私人網路和網際網路存取原則       | 無限的 |
| 透過企業和社交媒體 IdP 的身分驗證        | ✓   |
| 使用協力廠商整合與 Cloudflare 的裝置狀態 | ✓   |
| 以 CSV 為基礎的企業裝置序號清單大量匯入     | ✓   |

| 👁️ 增加可見度                |      |
|-------------------------|------|
| 活動記錄保留                  | 6 個月 |
| 基於身分的國家/地區、州/省與裝置詳細資訊視圖 | ✓    |
| 將記錄推送至雲端儲存空間或 SIEM      | ✓    |

| 🔒 安全連線                                         |                     |
|------------------------------------------------|---------------------|
| 基於用戶端加密的網際網路連線 (WARP 用戶端)                      | Win、Mac、iOS、Android |
| 對自行代管和 SaaS 應用程式的無用戶端安全存取                      | ✓                   |
| 用於自託管應用程式和內部 IP 與主機名稱的專用連接 (Cloudflare Tunnel) | ✓                   |

| 🔗 簡易的互通性                      |   |
|-------------------------------|---|
| 端點和行動管理整合                     | ✓ |
| 適用本機或 VPN 連線能力的分隔通道           | ✓ |
| 非受管理裝置的用戶端自行註冊                | ✓ |
| 可定制的應用程式啟動器                   | ✓ |
| 同時支援多個身分識別提供者的驗證              | ✓ |
| 用於支援 SAML 和 OIDC 的通用和自訂連接器    | ✓ |
| 用於自動化服務的基於權杖的認證               | ✓ |
| 適用於 IoT 和其他 mTLS 使用案例且基於憑證的授權 | ✓ |

| 🚀 效能毫髮無損                                        |      |
|-------------------------------------------------|------|
| 正常運作時間 SLA                                      | 100% |
| 最快速的網路之一 (自超過 250 個 PoP 不到 50 毫秒)               | ✓    |
| 速度最快，隱私優先的 DNS 解析器 (透過超過 250 個 PoP 為 7 至 31 毫秒) | ✓    |
| 快如閃電的原則更新 (至超過 250 個 PoP 不到 500 毫秒)             | ✓    |
| 快如閃電的遠端瀏覽器 (無像素推送 — 在我們的網路上執行；非第三方雲端)           | 附加服務 |

有興趣瞭解更多內容嗎？

請瀏覽 [www.cloudflare.com/zh-tw/products/zero-trust/access/](https://www.cloudflare.com/zh-tw/products/zero-trust/access/) 以建立帳戶，最多 50 位使用者可免費註冊。