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和端點保護平台協同工作，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%1
- 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。

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。

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。

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。

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。

記錄使用者在任何應用程式中的活動

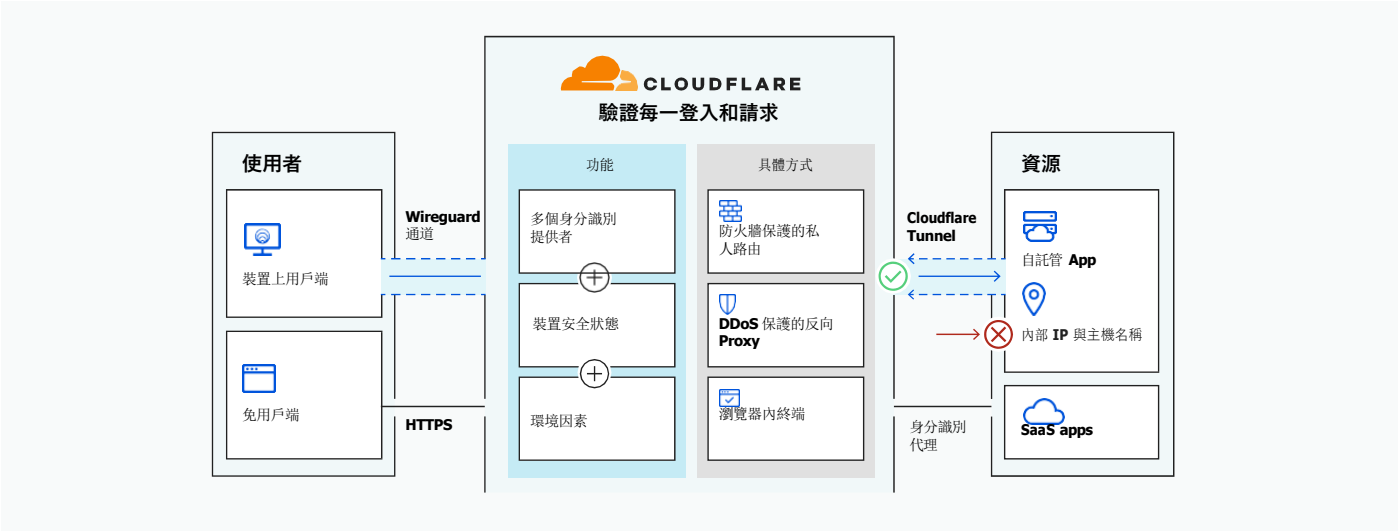
記錄在受保護應用程式中發出的任何要求，不只是登入和登出。在 Cloudflare 中彙總活動記錄，或將其匯出到您的 SIEM 提供者。

1Zero 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**

Cloudflare Gateway

保護使用者和資料免受 Internet 上的威脅 – 無須骨幹網路

您如何阻止敏感資料離開您的組織？ 保護員工網際網路流量的傳統方法依賴於將流量從分支機構回傳到集中的公司安全邊界的網路設備。 了解 Cloudflare Gateway 如何利用 Cloudflare 強大的全球網路在不犧牲性能的情況下檢查和保護從每台設備到網際網路上每個目的地的每個連接。

功能

阻止 Internet 上的已知和未知威脅

使用我們龐大的威脅情報庫在域名或 URL 級別阻止對潛在風險站點的訪問，其中包括 100 多個類別的預設清單，可幫助您輕鬆阻止對惡意或風險站點的訪問。

控制進出組織的資料流

使用可以阻止用戶將文件上傳到站點，具檔案類型控制的資料外洩防護 (DLP)。 透過阻止用戶下載特定類型的文件來防止惡意下載。

SaaS 應用程式控制

發現未經批准的 SaaS 應用程式使用，並使用 Gateway 的策略引擎來阻止對未經批准的應用程式的訪問。

將用戶身份和角色整合到 Cloudflare Gateway 中，以限制對企業 SaaS 應用程式的特定子網域和功能的訪問。

監控整個網路的流量

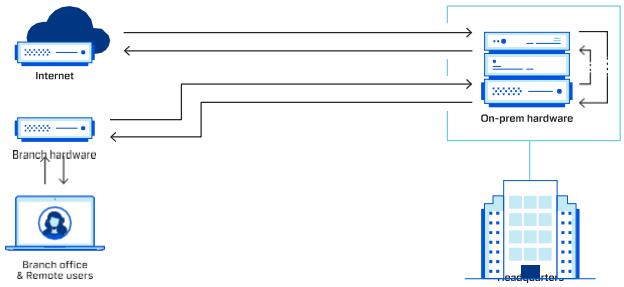
Gateway 的日誌提供對您的 Internet 和 Web 流量的可見性——跨所有用戶、設備和位置。

您可以將 Gateway 的日誌導出到您的 SIEM 或選用的雲存儲平台。

運作方式

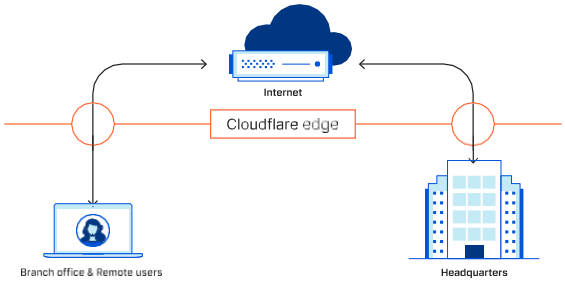
傳統方法

團隊需要連接到 Internet 才能完成工作。 傳統方法試圖迫使網際網路流量通過無法擴展且只會減慢用戶速度的硬體。



使用 Cloudflare Gateway

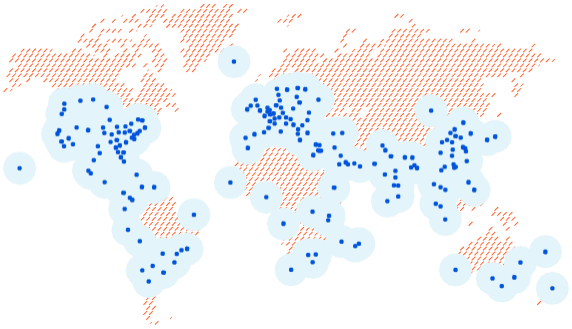
Cloudflare Gateway 用 Cloudflare 的全球網絡取代了過時的硬體。 用戶無需骨幹網路，而是連接到 Cloudflare 在全球 200 個城市的數據中心之一，Cloudflare 在該數據中心應用安全策略和過濾.



Cloudflare 優勢

只有 Cloudflare 具有處理每個請求的安全和保護的規模和經驗。

- 來自保護超過 2500 萬個 Web 資產的威脅情報
- 安全性由世界上最快的 DNS 解析器 1.1.1.1 提供支持
- 網路遍布 100 多個國家的 200 多個城市



“Algolia 的發展速度非常快。我們需要一種方法來了解整個公司網路，同時又不會拖慢我們員工的工作速度。Gateway 為我們提供了一種簡單的方法來做到這一點。”

Adam Surak
基礎設施與安全總監

algolia

How DLP Works

遷移到雲端使得追蹤和控制敏感資訊比以往更加困難。
員工正在使用越來越多的工具來操作大量資料。 同時，IT 和安全經理很難確定誰應該有權存取敏感資料、資料的儲存方式以及數據被允許去往的地方。

資料遺失防護使您能夠根據資料的特徵（例如關鍵字或模式。 當流量進出公司基礎設施時，會檢查流量的指標敏感資料。 如果發現指標，則根據客戶的規則允許或阻止流量。

輕鬆、快速地控制 受監管的資料類別	**高級訂製 不斷變化的數據需求**	**無縫集成 現有的資料分類工具**
合規要求是越來越嚴格和廣闊的。 快速啟用要解析的預定義 DLP 設定文件，員工網路流量和阻止共享受監管的數據，例如 PII、PHI 和其他財務資訊（包含銀行/信用卡號碼）。	敏感資料的定義可能會有很大差異。取決於產業和經營地點。 將精細控制應用於其他資料類型，例如秘密、代碼、憑證和 IP，透過創建具有上下文自訂 DLP設定文件分析和精確數據匹配。	對於安全團隊來說，保持徹底敏感資料的庫存數量，對於安全團隊來說是巨大的提升。因此需要像MIP一樣的資料分類工具。我們整合的自動檢索敏感度標籤並填充進入 DLP 設定檔。增加敏捷性，而不是增加複雜度。