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

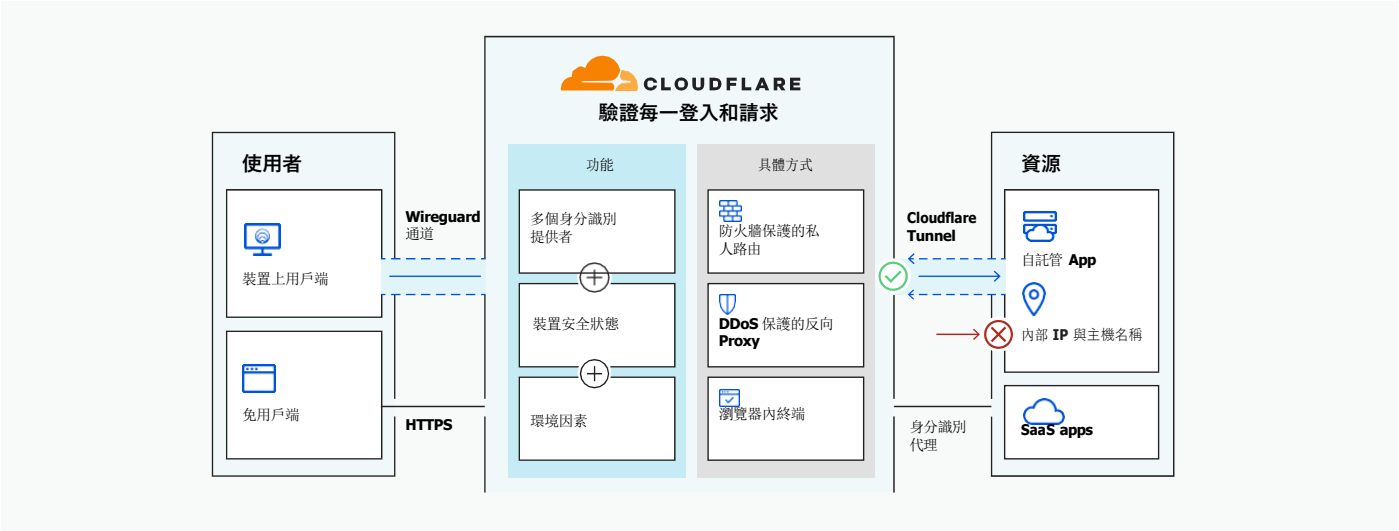
記錄在受保護應用程式中發出的任何要求，不只是登入和登出。在 Cloudflare 中彙總活動記錄，或將其匯出到您的 SIEM 提供者。

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

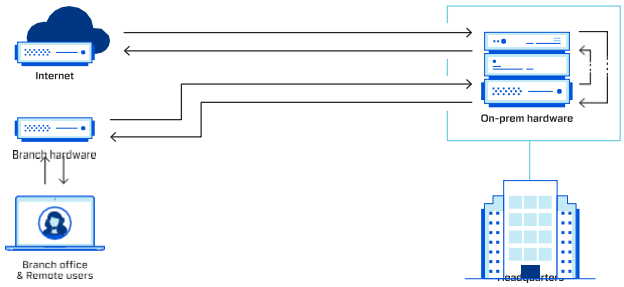
Gateway 的日誌提供對您的 Internet 和 Web 流量的可見性——跨所有用戶、設備和位置。

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

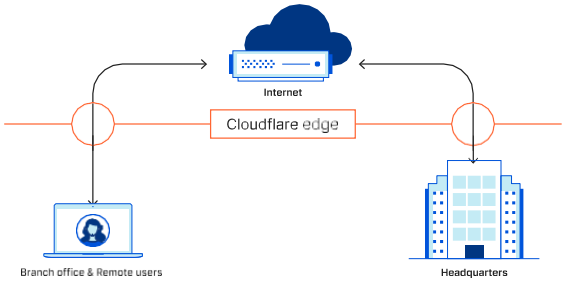
傳統方法

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

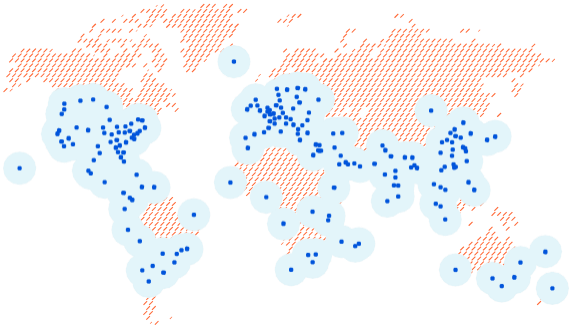
Cloudflare Gateway 用 Cloudflare 的全球網絡取代了過時的硬體。 用戶無需骨幹網路，而是連接到 Cloudflare 在全球 200 個城市的數據中心之一，Cloudflare 在該數據中心應用安全策略和過濾.



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

CLOUDFLARE

PRODUCT BRIEF

Cloudflare Browser Isolation

內建於網際網路零信任

將零信任擴展到網際網路

攻擊面大，控制有限

如今，網站瀏覽器是使用最廣泛的企業應用程式—代表著巨大的攻擊面。

然而從歷史上看，保護用戶免受基於瀏覽器的威脅一直不完善。 應用控制來保護用戶與敏感訊息的交互方式變得更加困難。

完善零信任

將零信任應用於瀏覽意味著默認情況下不應信任任何程式碼或在設備上互動運行。

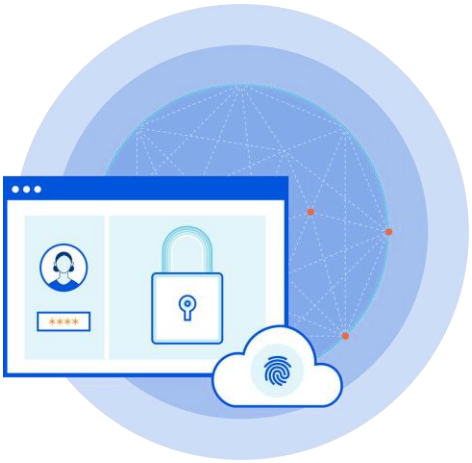
Cloudflare Browser Isolation 在我們的邊緣運行所有程式碼——使用戶免受不受信任的 Web 內容的影響，並保護瀏覽器互動中的資料免受不受信任的用戶和設備的影響。

不是一般的遠端瀏覽器

- 相容性適用於任何網頁、任何瀏覽器。
- 效能提供低延遲的網頁流。

保護使用中的資料免受不被信任的用戶和設備的侵害，並保護設備和用戶免受勒索軟體和網路釣魚的侵害

— 甚至是 zero-day 攻擊



現在試用 – 無須安裝

內建,非外加安全性

內建於Cloudflare

我們的瀏覽器隔離是與我們網路上的其他零信任服務一起從頭開始構建並運行在我們 275 個以上的地點。

Web 瀏覽連線盡可能靠近用戶，以確保極速般的用戶體驗。

原生整合

不同於其他提供商，Cloudflare 將瀏覽器隔離與我們所有的零信任服務原生整合。

使用單一管理介面:

- Secure web gateway (SWG)
- Zero trust network access (ZTNA)
- Cloud access security broker (CASB)
- Cloud email security (計畫中)
- ...其他

減少攻擊面

零信任瀏覽可阻止未分類、危險甚至低風險網站上的惡意程式碼感染用戶的設備。

簡易部署

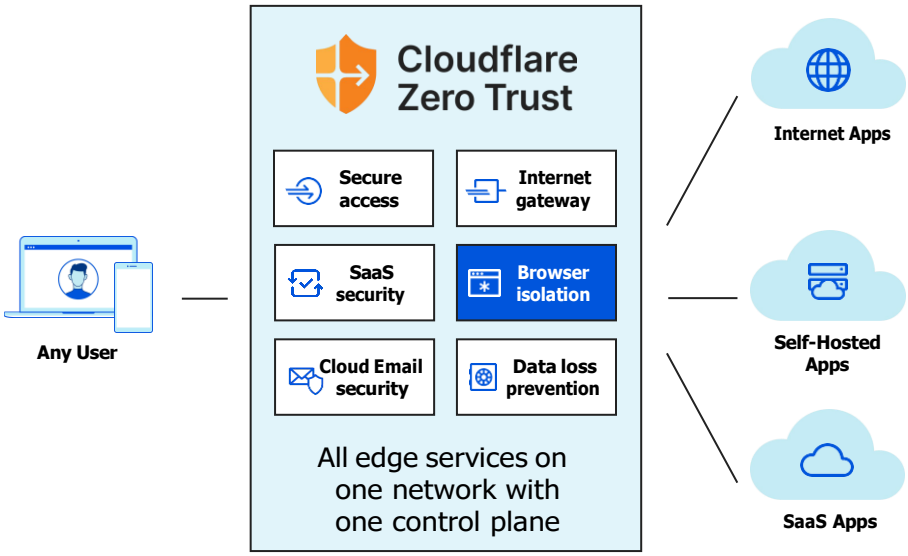
在管理應用程式存取的同一位置設置零信任瀏覽策略。

保護資料

透過控制應用程式或危險站台內的用戶操作（鍵盤輸入、複製、列印、上傳/下載）來阻止資料遺失和網路釣魚。

Browser Isolation: 零信任的基礎

隔離是零信任的核心原則。 只需使用 Cloudflare 的零信任平台單擊幾下，即可輕鬆將可見性和控制擴展到瀏覽器中。



隔離變得平易近人

從歷史上看，瀏覽器隔離作為一種獨立的解決方案存在，由於成本高且複雜，只有大型企業才買得起。

借助 Cloudflare，與 ZTNA、SWG 和其他 SSE 服務的原生整合讓您可以輕鬆地開始您的安全現代化之旅，然後再通過瀏覽器隔離進一步擴展零信任。

本地 vs. 遠端瀏覽

本地瀏覽

不受信任的網頁程式碼和網路釣魚站台在端點設備上本地執行。 用戶可以隨意將敏感資料輸入釣魚網站，他們的設備和資料直接暴露在未打補丁或零日威脅之下。

遠端瀏覽

未經過濾的程式碼或站台可以在不斷打補丁的遠端瀏覽器中執行。 控制用戶交互以防止惡意軟體和網路釣魚攻擊，並隔離零日攻擊在最終用戶的設備之外。

Cloudflare 的方法

Network Vector Rendering (NVR)

不同於頻寬密集的像素推送或脆弱的內容清洗和重建技術，NVR 將安全繪製命令流傳輸到設備，而不會傳輸任何惡意網頁程式碼或影響最終用戶體驗。

我們的全球網路

其他服務商在公有雲供應商中託管遠端瀏覽器。 Cloudflare 將瀏覽器定位在更靠近您的用戶位置，以在任何地點獲得與本地瀏覽無異的體驗。

主要功能

- 在遠離用戶的雲端執行所有瀏覽器程式碼
- 無像素推送
- 快如閃電的網絡（與全球 95% 網際網路用戶相差約 50 毫秒）
- 與所有現行瀏覽器的相容性
- 使用或不使用設備用戶端部署
- 阻擋資料離開企業應用程式並獲得Shadow IT 可見性
- 運用我們的網路防火牆和零信任規則的情資阻止威脅
- 100% 運行時間 SLA

立即體驗更快、更安全的瀏覽體驗

Try Browser Isolation now