CLOUDFLARE

解決方案簡述

確保分散式工作場所安全

在一個統一的控制平面上對任意辦公室位置的所有要求提供一致性保護

以雲端保障網路安全

藉助 Cloudflare 降低辦公室的複雜性和風險

由於員工有的在辦公室工作，有的在遠端工作，很多組織都會對今天如何確保辦公室安全進行重新評估 — 是依賴資料中心的設備，還是允許不安全的直接網際網路存取。

他們的新重點是為網路內外的使用者提供一致的保護和體驗。大多數時候，這意味著將控制權從 VPN、Web 代理和防火牆等不同工具轉移到單一的雲端交付安全性平台。

Cloudflare 看到，組織正在藉助兩個常見的使用案例實現辦公室網路安全現代化。

將分支機構和遠端存取併入單一實作中，可確保一致的原則並最大程度減少所需的廠商數量。部署 ZTNA 來擴充或取代傳統的 VPN，以限制對傳統技術的投資[1]。

Gartner

推薦使用案例：

使用 Zero Trust 取代 VPN，確保應用程式存取安全

對每個應用程式強制執行精細的識別身分原則，而不允許在企業網路內橫向移動。

- **第 1 步**：與身分識別提供者整合
- **第 2 步**：透過瀏覽器保護任何 Web 應用程式
- **第 3 步**：透過瀏覽器確保 SSH、VNC 和 RDP 環境安全

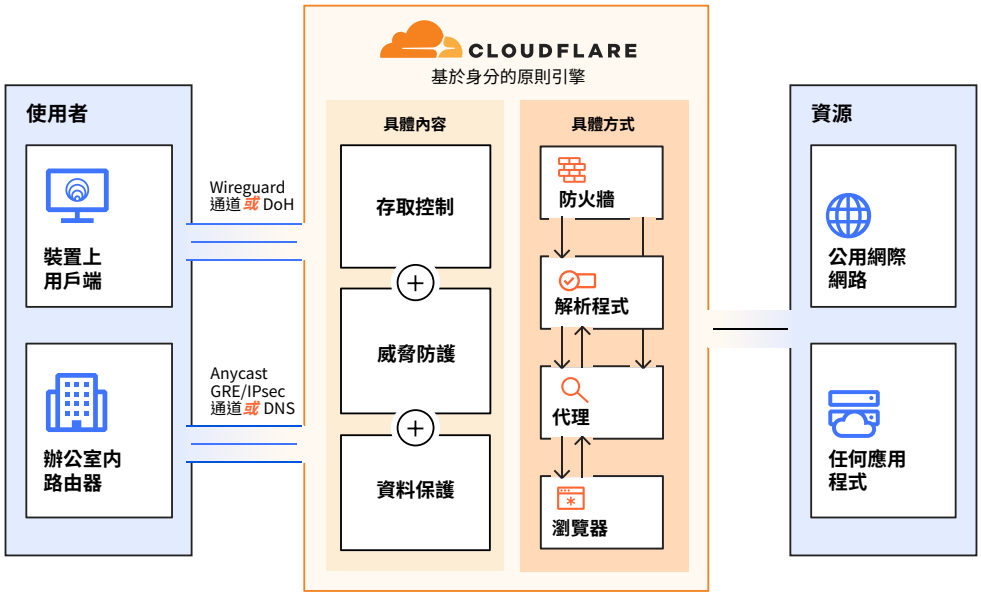
推薦使用案例：

篩選網際網路存取以實現一致的安全性和快速的價值實現

先進行 DNS 篩選，然後在所有位置進行更全面的檢查，來保護辦公室使用者。不再透過資料中心內部部署的網路安全設備回傳流量。

- **第 1 步**：將 DNS 流量指向 Cloudflare 的全球網路
- **第 2 步**：設定基於位置的 DNS 篩選，以防範勒索軟體、網路釣魚和其他網際網路威脅
- **第 3 步**：透過強制執行 HTTP、網路和瀏覽器隔離規則以及無限制的 TLS 1.3 檢查，來控制資料流。

運作方式



無用戶端部署以驗證存取並篩選來自辦公室位置的 DNS 查詢。

使用 Cloudflare 的裝置用戶端部署為每個使用者和每台裝置增強可見度和控制。

圖 1：藉助 Cloudflare Zero Trust 單遍完成對辦公室流量的驗證、篩選、隔離和檢查

任何來源的彈性入口

首先使用 Cloudflare 透過網路路由器進行 DNS 解析。隨著時間的推移，透過 GRE 或 IPsec 通道將第 3 層流量傳送至我們的全球網路 – 或使用現有的 SD-WAN 路由方法。

或者，部署 Cloudflare 的用戶端，在受管理裝置上進行 DNS 與 HTTP 篩選和檢查。

快速原則強制執行，可在全球範圍內擴展

所有的安全性、效能和可靠性功能都經過精心設計，能夠在我們覆蓋超過 275 個位置和 100 多個國家/地區的每一個資料中心的每一台伺服器上執行。

我們的網路規模可調整意味著，無論辦公室和終端使用者位於何處，始終可以透過單遍檢查在其附近以高速強制執行保護措施。

未來六到十二個月要探索的其他使用案例

重新控制 SaaS 應用程式

發現並緩解員工在辦公室和家裡使用的影子 IT 的風險。

使用從相同的單一 Cloudflare 儀表板啟用的 CASB 原則，防止資料外洩和違規。瞭解做法。

卸載 MPLS 流量

取代昂貴、老化且速度緩慢的私人 MPLS 連線。

使用 Cloudflare 的全球網路管理分支機構、資料中心和公有雲端服務內的流量，以簡化傳統的 WAN 架構。瞭解做法。

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。著作權所有，並保留一切權利。著作權所有，並保留一切權利。

 | + 886 8 0185 7030 | enterprise@cloudflare.com | cloudflare.com/zh-tw

REV:BDES-6043.2024AUG06