保護混合式工作

為網路內外的所有使用者減少風險並提升可見度

保護所有使用者透過任意裝置、在任何地點進行的所有連線

隨時隨地工作的未來：全球疫情蔓延多年，再加上即將到來的經濟衰退，混合式工作似乎已成為常態。無論是以遠端方式還是在辦公室內工作，IT 和網路安全團隊都必須為所有使用者和裝置提供一致的保護與體驗，而以地點為中心的傳統工具（如 VPN 和基於 IP 的控制）無法滿足目前的工作需求。

針對現代員工的現代網路安全：為了應對這一情況，許多組織都在重新塑造其 IT 及網路安全架構，採用依照分散式員工的需求進行擴展的雲端交付式安全性，並遵循 Zero Trust 最佳做法。

Cloudflare 可輕鬆確保任何連線的安全，這樣使用者便能夠透過任意裝置、在任何地點安全高效地存取應用程式或網際網路。

根據 Gartner® 的報告：

到 2026 年，75% 的工作者的工作地點仍會在家裡和傳統辦公室之間切換，這比 2021 年疫情最嚴重時的 77% 略有下降。[1]

基於一組邊界安全設備的網路安全設計無法滿足現代數位企業及其混合式數位員工隨時隨地辦公的動態需求。[2]

目錄（依頁面）

網路安全現代化機會

在不使用 VPN 的情況下進行安全應用程式存取

由於使用者如此分散，透過 VPN 等內部部署設備回傳流量會降低效能，並造成威脅在整個企業網路內橫向傳播的風險。

相反，恢復所有要求的可見度並在更靠近使用者的位置強制執行基於身分的控制才能保持生產力。無需回傳。

簡化 SASE 網路安全

員工比以往任何時候都更加依賴不受傳統企業網路控制的 SaaS 應用程式。

為應對這一情況，組織需要對其 SaaS 應用程式具有更全面的可見度和控制，以便設定存取原則、套用資料保護控制措施、緩解影子 IT 以及掃描應用程式中的設定錯誤。

保護使用者和資料免受網際網路威脅

勒索軟體、網路釣魚及其他網際網路威脅一直存在，並且變得越來越複雜。

針對輸出流量採取基於雲端的檢查和隔離可讓使用者遠離惡意軟體。此外，管理員還可以套用控制措施來防止將敏感性資料送達未受管理的本機裝置。

成熟企業的混合式工作

對於成熟的企業，充滿信心地對混合式工作的網路安全進行現代化改造

挑戰：複雜的傳統環境

各個組織正在嘗試辦公室內工作模式。但在這些混合式情境中維持一致的安全保護及使用者體驗頗具挑戰性。

這些公司往往歷史較為悠久，既存的（通常十分複雜）內部部署及舊版投資較為龐大。在經濟衰退的不利形勢下啟動一個全新的網路安全專案可能風險過高，難度也很大。

機會：更簡單易行的現代化之路

各個組織應以自己的步調著手進行數位化轉型，而無需無限的預算、昂貴的「概念驗證」、複雜的實作階段或菊鍊式服務。

為了協助這些成熟的企業滿足混合式工作需求，Cloudflare 設計了比其他 Zero Trust 服務提供者（如 Zscaler）更輕鬆快速的部署方式。

範例使用案例

電信

狀況：擁有 100 多年歷史，年收入達 200 多億美元的歐洲電信公司希望由單個廠商來部署網際網路篩選，並對最近遷移到多雲端環境的傳統應用程式進行存取驗證。

解決方案：公司選擇了 Cloudflare 來整合服務，並使用統一平台來保護其 10 萬多名員工的應用程式及網際網路存取。

媒體與廣告

狀況：媒體企業集團（全球收入超過 100 億美元，員工超過 10 萬名）的內部基礎架構面臨著網路威脅，包括勒索信。

解決方案：Cloudflare 利用基於身分的 Zero Trust 規則為數百個 Web 及非 Web 應用程式提供安全保護。公司在 3 個月內針對 5 萬名員工推出安全保護，並計畫在 9 個月內擴展到全體員工。

聯邦政府

狀況：美國國土安全部 (DHS) 正在牽頭對聯邦辦公室、儲存單元以及基礎架構中的網際網路威脅防護進行投資。

解決方案：DHS 選擇了 Cloudflare 和 Accenture Federal Services 來開發一個聯合解決方案，將 DNS 查詢篩選到將在聯邦機構中使用的惡意且有風險的目的地。

能源

狀況：一家位居《財富》雜誌 500 強的天然氣提供者尋求增強式保護，以協助其分散式資料中心及 1,500 多名員工抵禦日益增加的產業相關網路威脅。

解決方案：公司選擇了 Cloudflare 來取代 Zscaler，理由是其在保護應用程式及網際網路存取方面具有更出色的可靠性和一致性，並且從更長期的角度來看，採用具有遠端瀏覽器隔離功能的進階控制更為輕鬆簡便。

客戶引述

Cloudflare 是我們 Zero Trust 之旅的力量倍增器。

John McLeod
資安長
National Oilwell Varco

在 Cloudflare 的支援下，Ziff Media Group 能夠安全順暢地將我們的內部工具套件交付給世界各地使用任何裝置的員工，而無須進行複雜的網路設定。

Josh Butts
產品與技術副總裁
Ziff Media Group

藉助 Cloudflare，我們能夠降低開發環境中對 VPN 和 IP 允許清單的依賴。

Alexandre Papadopoulos
網路安全總監
INSEAD

數位原生公司的遠端工作為先的員工

對於數位原生公司，優先考量敏捷式網路安全以支援遠端工作靈活性

挑戰：擴展雲端安全性並實現自動化

許多組織正在採用遠端工作為先的招工形式。這些組織往往是更加年輕的早期雲端採用者，它們擁有有限的內部部署基礎架構，且商業模式基於安全、快速且可靠的數位服務。

實現隨時隨地工作的靈活性是一個獨特的優勢，但這要求網路安全工具能夠同等靈活，讓使用者能夠隨時移動並採用個人裝置開展工作。

機會：可縮放的組合安全性

由於要棄用的傳統 IT 較少，這些數位原生公司可以利用我們的網際網路原生基礎架構和部署彈性，在其網路安全現代化方面保持敏捷性。

透過我們的可組合服務、API 優先的設計和單一面板管理，您可輕鬆入門並調整網路安全。我們全球網路的速度、規模及可靠性能夠滿足完全遠端工作員工的各種需求。

範例使用案例

B2B SaaS

狀況： 澳大利亞圖形設計平台 Canva（2021 年價值為 400 億美元）在疫情前部署了 Cloudflare，來簡化協力廠商使用者的存取，並避免實作 VPN 的麻煩。

解決方案：隨著時間的推移，Canva 對其整體不斷增長的員工推出了 Zero Trust 應用程式存取原則，此外，還擴充了網際網路篩選及檢查。

金融科技公司與區塊鏈

狀況：在管理的資產不斷增長、以遠端工作為先的員工不斷增加，而又同時面臨網路威脅的情況下，BlockFi（一個由區塊鏈技術支援的系列數位財富管理平台）迫切需要提升網路安全性。

解決方案：藉助 Cloudflare，BlockFi 能夠過渡到基於身分的驗證來進行應用程式存取，並徹底拋棄耗時的 IP 型控制措施。

社交媒體

狀況：全球社交媒體平台遭遇了一次備受矚目的利用內部應用程式存取和 VPN 設定的外洩。

解決方案：為了應對這一情況，公司決定針對 13,000 名員工和承包商採用 Cloudflare 的 Zero Trust 網路存取 (ZTNA) 解決方案，並淘汰 VPN 部署，以徹底改變其遠端存取的方法。

電子商務

狀況：全球電子商務平台（收入超過 40 億美元，員工超過 15,000 名）尋求為遠端使用者提供更好的保護，以在網路外瀏覽網際網路和存取敏感性 SaaS 應用程式。

解決方案：公司部署 Cloudflare 來對 DNS 篩選等威脅防護功能進行分層，同時增強對 SaaS 應用程式使用情況的瞭解。

客戶引述

Delivery Hero 始終致力於為客戶提供出色的體驗。在 Cloudflare 的協助下，我們的內部團隊亦能享受同樣的體驗：在全球擁有安全的工作環境，並且能夠輕鬆地構建快速、可靠且尊重隱私的應用程式。

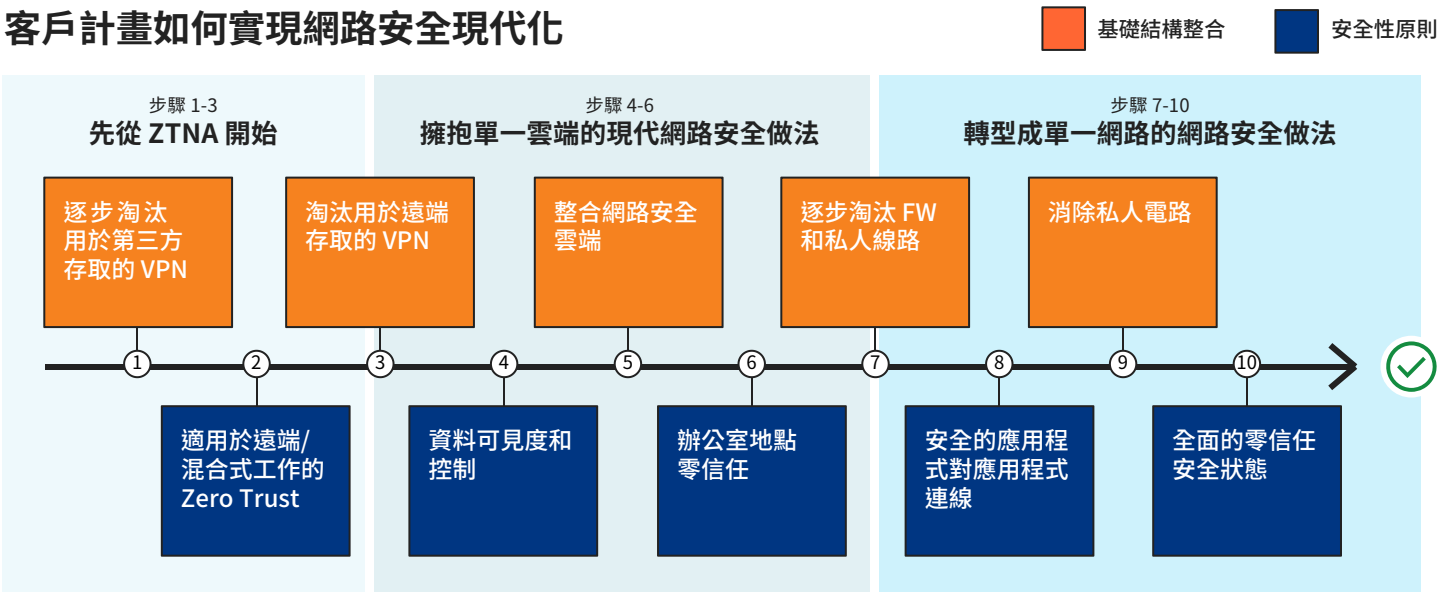
Christina von Hardenberg
技術長，Delivery Hero

Cloudflare 對於保護快速增長的遠端員工至關重要。採用 Zero Trust 進行應用程式存取增強了管理員的可見度和精細化控制，這是之前的傳統工具無法做到的。

Marccio Alcaide
IT 安全主管，Facily

混合式工作的說明性藍圖

客戶計畫如何實現網路安全現代化



網路安全現代化藍圖

上方的藍圖說明了組織在對其網路安全進行現代化改造以適應混合式工作時所採取的方法。此藍圖有兩大目標：

1) **頂端列（橙色）**：將連線功能和網路安全基礎架構從單一功能產品和硬體整合到一個雲端原生平台。
2) **底端列（藍色）**：獲得可見度和控制，從而對在任何地點使用任意裝置的使用者和資源採用 Zero Trust 安全性。

階段 1 - 5：保護應用程式及網際網路存取

對許多組織而言，適應混合式工作意味著首先對員工存取企業資源的方式進行現代化改造。

階段 1：通常來說，第一步是為特定使用者（例如承包商、開發人員、合作夥伴或新收購的團隊）卸載 VPN 流量並過渡到網際網路原生控制。藉助 Cloudflare，組織能夠輕鬆保護可透過瀏覽器存取的自託管應用程式，無須在端點上部署任何軟體。

階段 2：這一新型工具能夠提供必要的可見度，以便基於角色、MFA 和硬體金鑰要求以及身分和裝置狀態構建特定於應用程式的原則。

階段 3：隨著團隊對這一方法建立信心，他們完全淘汰了 VPN 並利用 Zero Trust 來保護非 Web 和傳統私人網路。

階段 4：然後重點轉向提高 SaaS 應用程式的可見度和控制，包括緩解影子 IT、管理租用戶和防止資料外流。

階段 5：在這個階段，組織已經從單一平台管理內部及 SaaS 應用程式，因此將尋求擴展對輸出網際網路存取的控制，並整合 DNS 篩選器和安全 Web 閘道等威脅防護工具。

階段 6-10：將連線轉移到雲端

對於大多數組織來說，剩餘的藍圖階段還在規劃中，但他們希望將所有網路連線和網路安全轉移到一個統一的雲端網路上。

階段 6：在這一階段，組織尋求將一致的 Zero Trust 延伸到任何網路位置（如總部、分支機構、資料中心和衛星辦公室）來支援混合式工作。

階段 7：隨著將越來越多的辦公室流量傳送至 Cloudflare 以確保安全，組織可以逐步淘汰傳統的內部部署防火牆和其他私人網路設備。

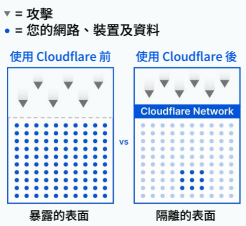
階段 8：這些進階使用案例側重於保護混合式多雲端環境中的應用程式對應用程式連線，以協助網路基礎架構團隊做好準備，在**階段 9** 結束電信 MPLS 合約。

階段 10：儘管現代化永不會真正結束，但現在的目標是將 Zero Trust 延伸到所有使用者、裝置、資料、應用程式和環境。

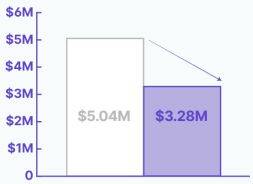
業務和網路安全成果

Zero Trust 以 5 種方式為企業節省時間與金錢

減少攻擊面
91%↓



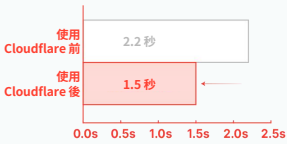
減少外洩成本
35%↓



加速員工佈設
60%↑

減少IT 工單負擔
80%↓

減少使用者延遲
39%↓



其他商務驅動因素

釋放員工生產力

對於管理員

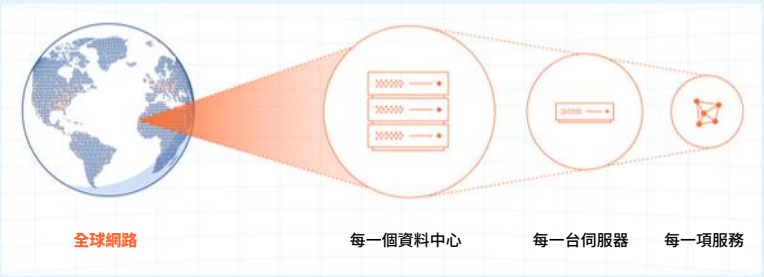
- 藉助單一管理介面簡化設定，以設定應用程式及網際網路存取的原則
- 透過同一管理介面，設定與身分識別提供者、端點保護、雲端提供者及網路入口的所有整合

對於終端使用者

- 藉由不同尋常的網路安全，獲得順暢的驗證和原生瀏覽體驗

減少在傳統服務上的花費

- 取代或擴充虛擬私人網路 (VPN) 設備，轉而採用 Zero Trust 網路存取 (ZTNA)
- 從內部部署 Web 代理或防火牆過渡到雲端原生第 3-7 層網路安全服務
- 藉助遠端瀏覽器隔離 (RBI)，從虛擬桌面基礎架構卸載使用案例
- 換掉傳統的安全電子郵件閘道，以獲取現代雲端電子郵件安全性



以一致的速度和規模，為所有遠端或辦公室使用者提供保護

所有的安全性、效能和可靠性功能都經過精心設計，能夠在我們如今遍佈超過 275 座城市的網路中每一個 Cloudflare 資料中心的每台伺服器上執行。

加速您的 Zero Trust 藍圖

立即嘗試　聯絡我們

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

REV: PMM-2022JUL

[1] *支援混合式工作的最佳網路做法*，Gartner，Karen Brown、Andrew Lerner、Mike Toussaint，2022 年 4 月 8 日
[2] *2022 年 SASE 聚合的策略藍圖*，Gartner，Neil MacDonald、Andrew Lerner、John Watts，2022 年 6 月 24 日