CLOUDFLARE

白皮書

網際網路原生轉型的參考架構

對如何保護使用者存取應用程式進行現代化改造

位於使用者與應用程式之間的安全堆疊是什麼？

使用 Cloudflare 前

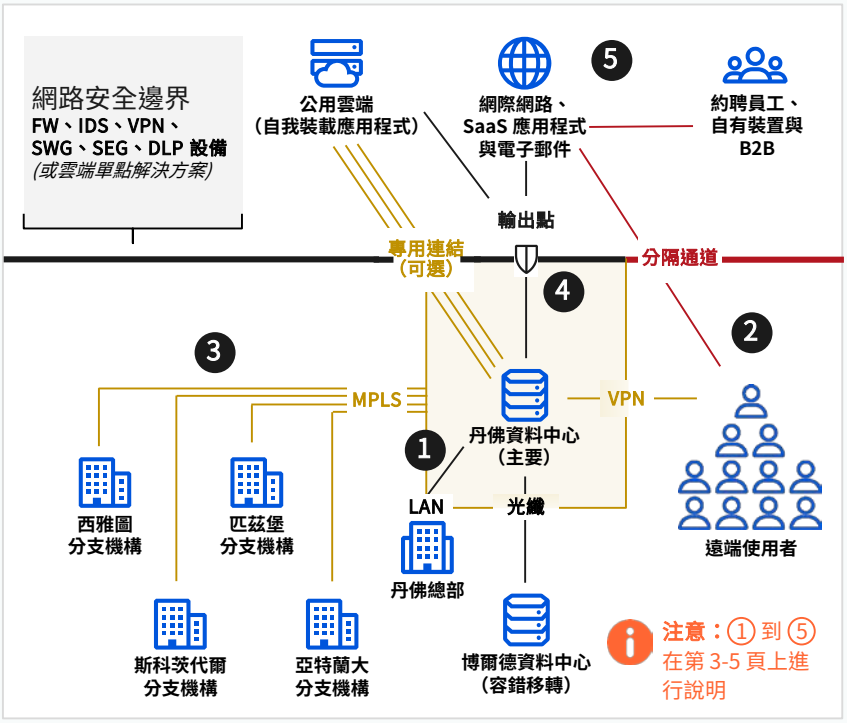
大多數組織依賴於擁有 20 多年歷史的中心輻射架構。內部使用者及應用程式與外部使用者及應用程式採用不同的連線及保護方式。存取權則取決於位置、裝置、角色或身分識別提供者（亦稱為IdP）。

使用 Cloudflare 服務

您的架構經過網際網路原生轉型，能夠符合未來需求，它採用 Zero Trust 原則，並透過一整套可輕鬆設定和運作的雲端原生服務，為所有使用者及應用程式提供始終如一的連線和保護。

✓受支援的使用案例及網路安全 ✕ 不受支援的使用案例及網路安全		內部 App	外部應用程式		
		自我裝載私人資料中心，共置或雲端 *（非 Web）*	自我裝載公用雲端 *（AWS、GCP、Azure）*	SaaS 及電子郵件 *（M365、GSuite）*	網際網路 *（FB、Reddit）*
使用 Cloudflare 前	內部使用者 *（辦公室和遠端）*	✓「受信任的」位置、裝置或員工角色 ✕「不受信任的」位置、自有裝置、約聘員工角色		✓企業 IdP ✕ 社交 IdP	不適用
	外部使用者	✕「不受信任的」IoT 裝置或 B2B 客戶角色		✕ 社交 IdP	不適用
	網路內連線性	「受信任的」直接 LAN	「受信任的」專用連結	一個「不受信任的」輸出點	
	網路外連線性	「受信任的」VPN	「不受信任的」VPN 分隔通道		
	存取安全堆疊	✓FW、IDS *（帶 LB、DNS）* ✕WAF、DDoS、ZTNA、SWG、SEG、RBI、DLP	✓FW *（帶 LB）*	✓SWG、SEG、DLP *（有時）* ✕ CES、CASB、RBI	
使用 Cloudflare 服務	內部使用者 *（辦公室和遠端）*	✓任何經過驗證的身分（以角色為基礎，可選）、任何裝置（以狀態為基礎，可選）、任何位置（以內容為基礎，可選）			
	外部使用者	✓透過任何 IdP（以內容為基礎，可選，例如，mTLS、OTP）驗證的任何身分			不適用
	網路內連線性	透過突破輸出點直接連線至 Cloudflare			
	網路外連線性	直接連線至 Cloudflare			
	存取安全堆疊	✓FW、IDS、WAF、DDoS、ZTNA、SWG、SEG、RBI、DLP *（帶 LB、DNS）*		✓SWG、SEG/CES、CASB、RBI、DLP *（採用 ZT 規則）*	

使用 Cloudflare 前：中心輻射架構



其他成本及複雜性

透過將流量回傳至一個集中的輸出點，來強制實施網路安全越來越低效。

難以採用全新技術

如果採用公用雲端及 SaaS 應用程式，則必須在網路安全或效能與使用者體驗之間進行取捨。

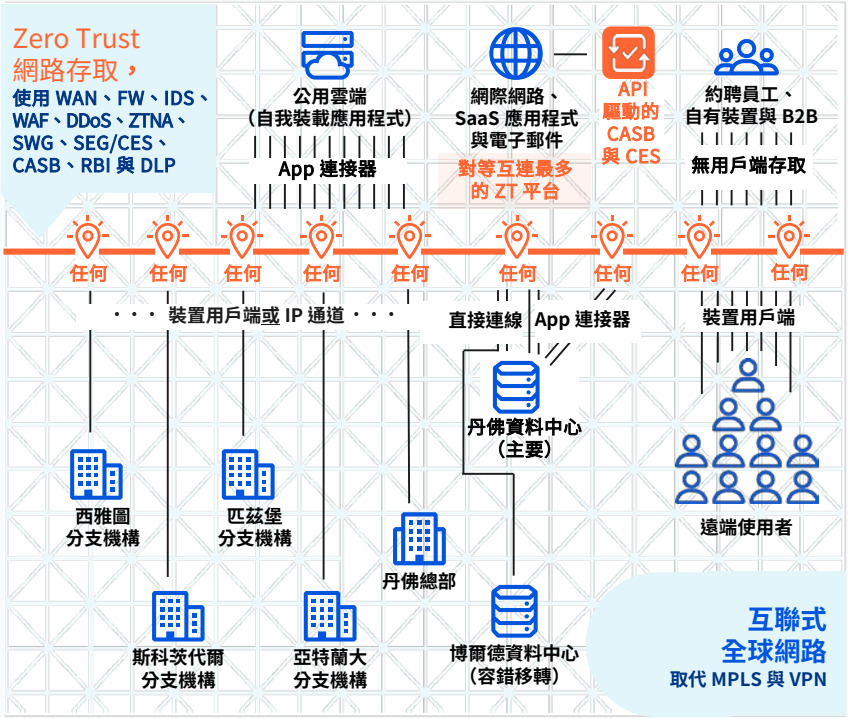
難以發展業務

在何處部署新硬體以及部署多少容量，才能確保所有使用者能存取所有應用程式，這很難做出決定。

對遠距工作不太友善的模型

疫情、氣候或地緣政治問題導致企業在重新思考其資源分配模型時產生摩擦。

使用 Cloudflare 服務：網際網路原生轉型



改善體驗，降低成本

將實施點分佈在所有使用者附近，從而減少對辦公室 MPLS 電路以及資料中心硬體的依賴。

減少外洩導致的損害

從概念上來說，所有使用者都是「離網」的，且僅存取明確允許的應用程式，從而消除了橫向移動攻擊。

混合工作團隊與多雲端就緒

簡單的反向 Proxy 及 API 設定可支援約聘員工、自有裝置、公用雲端、SaaS 應用程式與電子郵件的安全存取。

創新與收入增長速度加快

加速數位轉型，因為網際網路不僅更快速，更可靠、更安全，而且沒有容量限制。

注意：① 到 ⑤ 是第 2 頁圖表中的編號

① 企業網路優勢

使用 Cloudflare 前

以往，使用者、裝置、應用程式及資料都分在單一位置 — 總部。隨著企業在地理上的擴大，它仍然是中央樞紐。應用程式及資料在那裡託管和維護，因此使用者需要連線至該位置來完成工作。為了降低硬體成本，還需要將網路安全邊界集中在那裡。為了保護網路，所有流量都在一個位置進入和離開。然而，隨著使用者離這些應用程式越來越遠，它帶來了生產力瓶頸，並且需要許多昂貴而複雜的應急拼湊來解決這個問題。

使用 Cloudflare 服務

Cloudflare 不再將網路圍繞在實體安全及應用程式基礎結構周圍，而是成為您為使用者 — 在任何裝置、任何位置 — 及網路位置提供所有網路安全和網路功能的「第一個躍點」。使用者及網路可透過共用狀態連線至任何 Cloudflare 資料中心，其中 Anycast 會自動選取最低等待時間的路由。所有流量都會進入並離開一個自訂 Linux 伺服器，其中在單一行程中套用第 3 層防火牆及第 4-7 層 Zero Trust 原則。這不僅會簡化資料中心的現有硬體投資，還會將網路安全基礎結構分佈在世界各地靠近使用者、網路及應用程式的位置。

② 遠端使用者優勢

使用 Cloudflare 前

「安全」邊界之外的使用者必須重新連線，通常是透過在防火牆上終止的 VPN 連線。傳統上，這代表以下方面的難題：（1）使用者連線能力的一致性及效能，（2）網路上使用者的過度存取權，以及 （3） 防火牆中開啟的內送連接埠暴露於 DDoS 攻擊。隨著使用者網際網路流量的增加，企業不得不接受效能損失以及回傳成本增長，或者接受因在邊界周圍為遠端使用者流量建立分隔通道而導致的可見度及控制力損失。

使用 Cloudflare 服務

使用者因等待時間較短（<50 毫秒）的共用狀態連線而受益。然後，無論他們要存取內部應用程式還是外部應用程式，都會傳輸我們的網際網路原生骨幹，從而減少效能難題，提高一致性，並消除回傳使用者流量所帶來的架構容量限制和設計問題。如果正在分隔通道，則允許您從世界上的任何位置重新擷取所有使用者流量而不回傳，從而提高可見度及控制力，但不會對終端使用者體驗產生負面影響。

根據 Gartner® 的報告

「到 2025 年，至少 70% 的全新遠端存取部署將主要由 ZTNA 而不是 VPN 服務提供服務，而 2021 年底為不到 10%。」[1]

③ 分支機構優勢

使用 Cloudflare 前

隨著辦公室地點越來越分散，在為每個辦公室進行內部 WAN 及網際網路存取準備時很難做出決定：

- 如何在支援這兩種存取時確保一致性與可靠性呢？或者說，如何覆蓋 MPLS 電路（可能還有 SD-WAN）以透過集中式網路安全基礎結構為辦公室傳送網際網路流量。
- 面對全球供應鏈挑戰，採購並部署設備硬體來提高輸送量容量需要多長時間？
- 辦公室是否有互通性要求，例如每個辦公室都需要存取的共用或本機系統，來證明 MPLS 電路及軟體定義的路由器的昂貴和複雜性？

使用 Cloudflare 服務

Cloudflare 並未採用粗暴的 MPLS RIPout 方法，而是建議採用增量藍圖來提高可見度和控制力以及可靠性和效能。透過使用裝置用戶端與應用程式連接器軟體組合，或在現有路由器上設定 Anycast GRE 及 IPsec 通道，您可以根據需要使用更安全的 Zero Trust 原則及跨網路連線能力，同時支援透過內部 WAN 及網際網路存取應用程式，而無需構建權限過度寬鬆的網路原則。這會讓您從傳統的中心輻射網路中移除辦公室使用者（及 IoT 裝置），而不是讓他們獲得更棒的咖啡館式的體驗。所有辦公室都會立即獲得一條簡單快速的軟體定義的路徑來連線至網際網路，而無需使用昂貴的防火牆（或 SD-WAN）硬體。套用同樣全面的 IP 防火牆、DNS 篩選器以及安全 Web 閘道原則，這些原則用於從同樣簡單的管理介面為終端使用者獲取可見度及控制力，從而降低 TCO。

④ 網路安全邊界優勢

使用 Cloudflare 前

保護城堡的護城河通常是硬體衍生的。為了確保您的敏感性資料保留在內部，以及在使用者及裝置存取網際網路時提供保護，需要將網路安全基礎結構 — 通常包括防火牆、入侵偵測、VPN、安全 Web 及電子郵件閘道以及 DLP 設備 — 集中在需要將大部分流量留給網際網路的輸出點。隨著網路的擴展，以及使用者和應用程式不斷移出邊界，這種基礎結構成為採用新技術（例如，Microsoft 365）及網路典範的阻塞點。在這個輸出點的下游，透過資料中心傳輸企業 WAN 流量的 MPLS 電路以及硬體或軟體定義的 IP 通道也會具有基於硬體的頻寬限制，必須加以考量。

使用 Cloudflare 服務

隨著網路的擴展，應用程式使用的成熟和分散，以及使用者地理異構性日益顯著，Cloudflare 對這種中心輻射架構進行了轉型，以將原則實施分佈到網際網路邊緣，從而更靠近所有使用者及其所使用的應用程式。現在，Cloudflare 可提供由 FW、IDS、VPN、SWG、SEG 和 DLP 設備提供的服務以及 DDoS、WAF 和更新的技術（包括 ZTNA、CES、CASB 及 RBI）。由於它還是內外部使用者的「第一個躍點」終止點，因此您會獲得這一內聯套用的新型 Zero Trust 安全性的好處，從而確保高效且有效地完成轉型。

⑤ SaaS 應用程式及電子郵件安全性優勢

使用 Cloudflare 前

大多數企業採用 SaaS 的過程並未全部完成，特別是 Microsoft 365 及 Google Workspace，其中包括所有 Office 套件工具，包括電子郵件。SaaS 存在於邊界之外，因此既能代表提高的生產力，又能代表全新的挑戰。在使用者與 SaaS 應用程式之間傳輸中的資料通常沒有安全性，因為 VPN 分隔通道、TLS 檢查過於昂貴或不可擴展，或者因為它是外部使用者。而在所有 SaaS 應用程式的設定及待用資料設定檔中，通常沒有可見度及控制力或者不完整。在沒有任何網路入侵或惡意軟體下載的情況下，電子郵件仍然是攻擊者的首要攻擊方式，這是因為我們盲目地信任收件匣 — 讓所有人都成為了內部威脅。對於永久存在於邊界之外的內容，如何恢復一定的可見度呢？

使用 Cloudflare 服務

網路安全現代化架構 — 無論您將其稱之為 Zero Trust 架構 (ZTA)、安全服務邊緣 (SSE) 還是安全存取服務邊緣 (SASE) — 就是在應用程式及資料使用不斷分散的情況下統一安全狀態。Cloudflare 透過提供多種網路安全模式幫助實現這一願景；除了透過用戶端或無用戶端 SWG、ZTNA 及 RBI 部署組合提供的內聯 CASB 以外，我們還可以提供頻外 API 驅動的 CASB 及雲端電子郵件安全性 (CES)。這會在 SaaS 應用程式（包括 Microsoft 及 Google 套件）內進行深度掃描，只需按幾下即可進行設定檔探索，並且發現結果會防止資料滲漏並不斷地識別新風險 — 值得注意的是，可規避傳統安全電子郵件閘道方法的網路釣魚及 BEC 攻擊。

根據 Gartner® 的報告

「到 2025 年，30% 的組織將完全依賴於 Saas 應用程式來執行其任務關鍵型工作流程。」[2]

使用其他服務：多個拼湊起來的架構

許多產品提供碎片化的網路及網路安全基礎結構，無法快速擴展和發展，以將所有使用者端對端連線至應用程式。可見度及原則不一致，無法保護存取抵禦新型威脅。作業非常複雜，也不太靈活。使用者體驗大大降低。

遠端及外部使用者

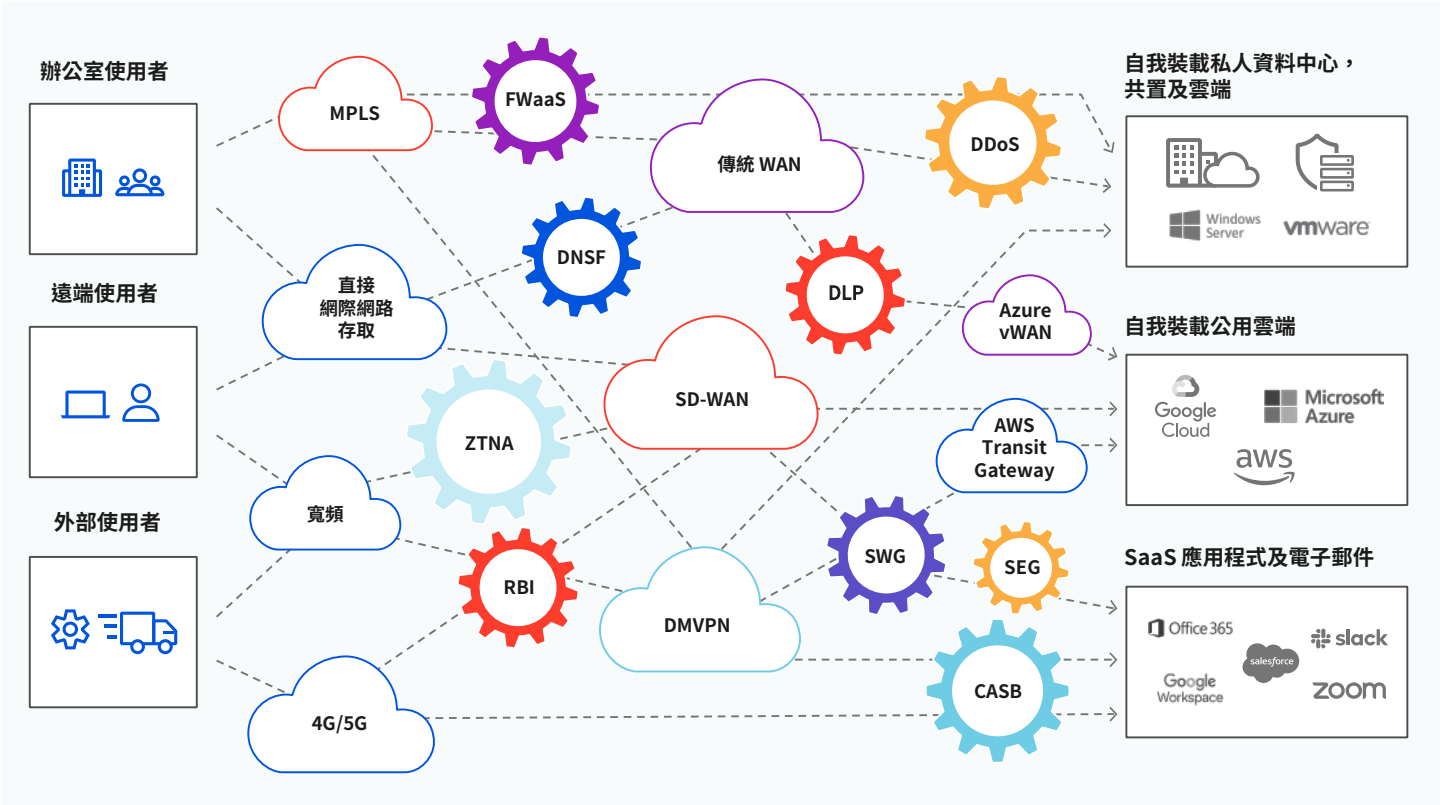
全新的網際網路連線能力擴展到了辦公室之外。全新的 Zero Trust 安全性與反向 Proxy 及隔離模式結合在一起，可確保不受信任的使用者、裝置及位置的存取安全。

公用雲端、SaaS 應用程式與電子郵件

全新的網際網路連線能力突破了辦公室的限制。全新的 Zero Trust 安全性擴展後，將 API 驅動與內聯代理模式相結合，以確保在私人網路以外安全地存取應用程式及電子郵件。

新型威脅

利用辦公室及資料中心內的過度信任。全新的 Zero Trust 安全性與正向 Proxy 及隔離模式結合在一起，可保護存取抵禦橫向移動攻擊。



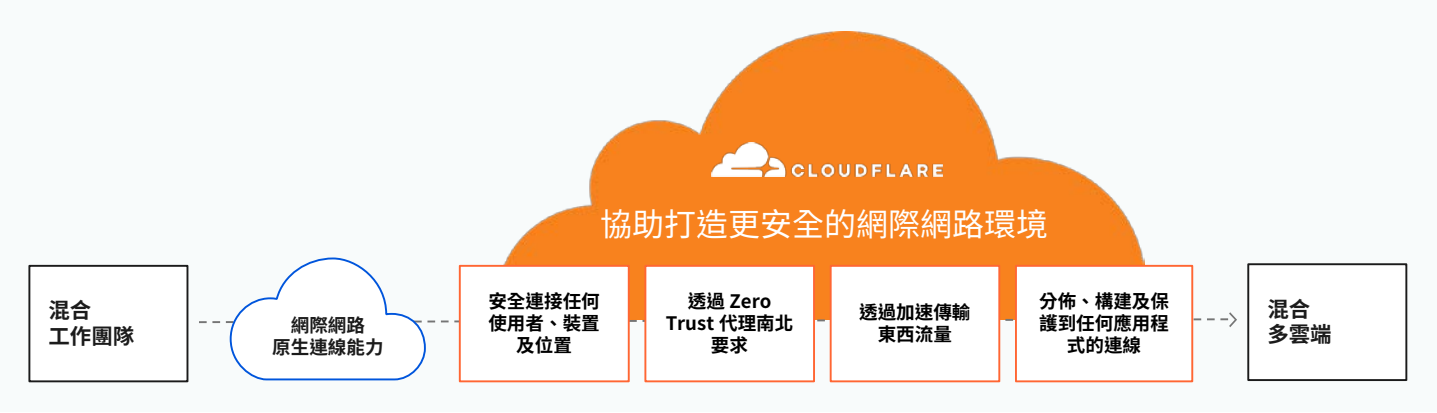
「到 2025 年，80% 的企業會採用策略，來使用 SASE/SSE 架構統一 Web、雲端服務及私人應用程式存取，而 2021 年為 20%。」[3]

Gartner

使用 Cloudflare 服務：一個可組合的統一架構

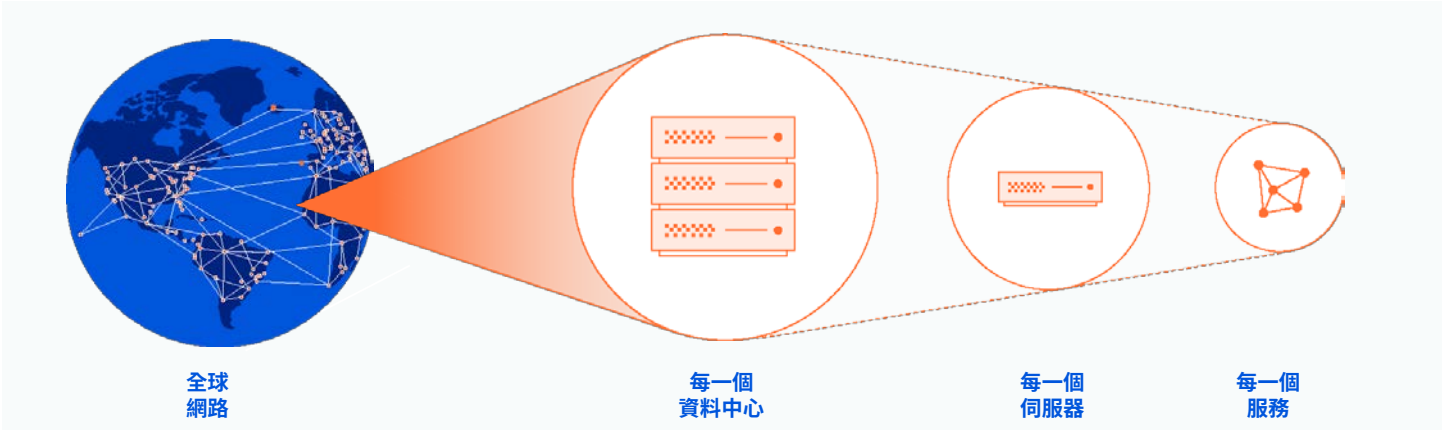
您的企業網路像網際網路一樣無處不在

所有連線及安全服務都與 Cloudflare 網路平台內的應用程式一起存在於雲端，並且準備就緒，隨時可啟動並順利地協同工作。現在，您的混合工作團隊中的任何使用者都可以在混合多雲端環境中一致地存取任何應用程式 — 而無需犧牲網路安全與效能。



一個網路，一個控制平面 — 無處不在

使用 Cloudflare 服務，您的企業網路運作起來比網際網路更快速、更可靠、更安全。在邊緣運作的每一項服務都可以在每一個資料中心執行，因此您的使用者在任何地方都能夠獲得一致且超快的體驗 — 無論他們身在芝加哥還是開普敦。這意味著所有客戶流量都在距離其來源最近的資料中心，在單一行程中處理，既沒有回傳，也沒有增加等待時間的服務鏈結。



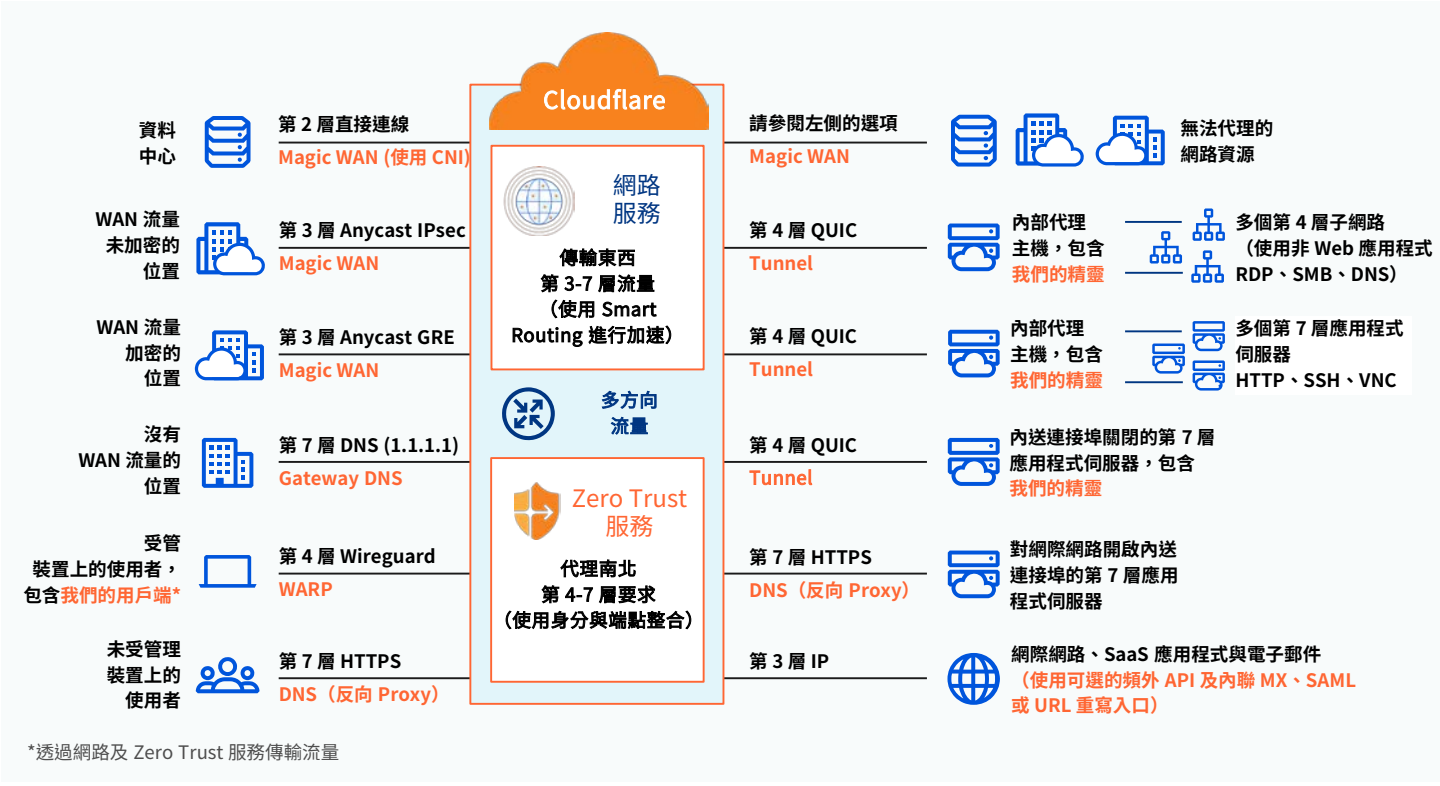
285+ 個城市，可供所有人使用
192+ Tbps 的 網路邊緣容量
11,500+ 個互連，連線至服務和雲端提供者，以及主要企業
~50 毫秒可與 95%的網際網路使用者連線

100% 正常運作時間 SLA（使用 Anycast）
在中等層級獲得 **FedRAMP** 授權
IPv6 及 TLS 1.3 處理和檢查無需犧牲網路安全

Zero Trust 網路即服務如何運作

可組合的入口實現端對端的任意連線性

Cloudflare 網路入口透過一個統一控制平面，來使用共用狀態連線。因此，使用網路互連的資料中心、使用 Anycast IPsec 或 GRE 通道的辦公室、使用 Wireguard 用戶端的使用者，以及使用 Cloudflare 通道的應用程式伺服器，可以透過每一項 Cloudflare 服務在彼此之間及網際網路之間傳輸及/或代理流量。



*透過網路及 Zero Trust 服務傳輸流量

Zero Trust 服務

- 存取控制：Access 與 Gateway（使用 CASB）
- 流量篩選：Gateway 與 Area 1 電子郵件安全性
- 內容檢查：Gateway 與 Area 1
- 威脅與資料保護：Area 1 與 Gateway（使用瀏覽器隔離、CASB 及 DLP）

網路服務

- 存取控制：Magic Firewall
- 流量路由最佳化：Magic WAN
- 入侵偵測：Magic Firewall
- DDoS 保護：Magic Transit

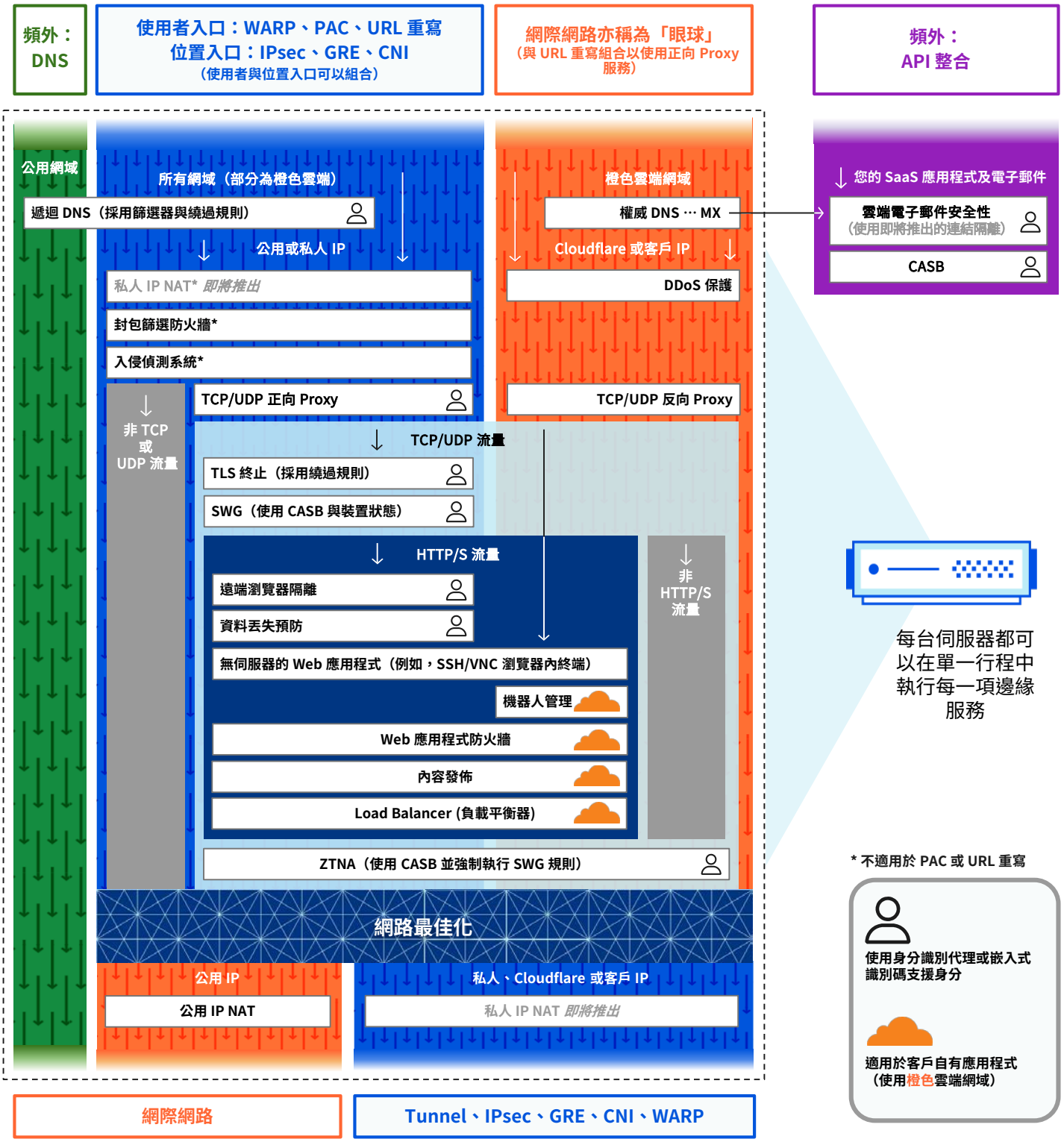
內建應用程式安全性與效能

客戶還會從與 Zero Trust 服務一起執行的應用程式服務中受益。依預設，授權內已啟用多項服務。

- 保護連接埠開啟的應用程式：第 7 層 DDoS 保護
- 防止約聘員工入侵應用程式：WAF
- 簡化應用程式入口流量：DNS
- 提高應用程式可靠性，無停機時間：LB
- 降低頻寬成本，改善使用者體驗：CDN

網路安全與使用者體驗無需折衷

我們的整個邊緣服務堆疊 — 加上頻外服務 — 都是為了協同工作而原生構建的。Zero Trust、網路及應用程式服務根據網域、IP 及通訊協定存在於適當的入口之間。要求與流量在距離其來源最近的超快單一行程中進行篩選、檢查、隔離和驗證；然後透過網際網路路由並加速傳輸至其目的地。



使用 Cloudflare 進行架構轉型的三個原因

部署簡便性

Cloudflare 客戶重視統一且可組合的平台，以便輕鬆設定和運作。他們不需要更花費時間且更容易發生錯誤之體驗的碎片化服務。

網路復原能力

Cloudflare 全球網路具備端對端流量自動化，能夠提供客戶信任的可靠性與效能。沒有人希望以手動方式連線到多個雲端網路，因為這樣會使網路安全有所折衷。

創新速度

Cloudflare 的架構將創新內容整合至客戶使用的相同網路中，以便快速發展。沒有人希望新服務以附加方式提供，或在採用新標準方面停滯不前，因為這樣會延遲他們的未來發展。

還沒準備好參加架構研討會？

不斷瞭解有關 Cloudflare One 的更多資訊

縮略字：

- BEC = 企業電子郵件入侵
- CASB = 雲端存取安全性代理程式
- CDN = 內容傳遞網路
- CES = 雲端電子郵件安全性
- DDoS = 分散式阻斷服務
- DLP = 資料丟失預防
- DNS = 網域名稱系統
- DNSF = DNS 篩選器
- FW = 防火牆
- IDS = 入侵偵測系統
- LB = 負載平衡器
- MPLS = 多通訊協定標籤交換
- RBI = 遠端瀏覽器隔離
- RDP = 遠端桌面通訊協定
- SD-WAN = 軟體定義的 WAN
- SEG = 安全電子郵件閘道
- SMB = 伺服器訊息區
- SWG = 安全 Web 閘道
- WAF = Web 應用程式防火牆
- WAN = 廣域網路
- VPN = 虛擬私人網路
- ZTNA = Zero Trust 網路存取

來源：

1. Gartner「新興技術：Zero Trust 網路存取的採用增長深入解析」，2022 年 4 月 8 日（連結）
2. Gartner「如何建立高效的 SaaS 控管」，2021 年 12 月 27 日（連結）
3. Gartner「2022 年 SASE 聚合的策略藍圖」，2022 年 6 月 24 日（連結）