白皮書

ZTNA（零信任網路存取）可以取代你的 VPN 嗎？比較三種遠端存取方法

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

索引

介紹	3
方法一：傳統 VPN	4
方法二：Zero Trust（零信任）網路存取	7
Cloudflare 的遠端存取方法	9
用 Zero Trust 網路存取取代傳統的 VPN	11
附錄	12

介紹

安全、無縫的遠端存取是經營的命脈，可提高遠端用戶的工作效率，並減少了 IT 團隊讓用戶加入應用程式並加以維護，使其敏捷及耐用所花費的時間。然而，遠端存取對許多企業來說是個挑戰。

有段時間，VPN 提供了一種簡單的方法，可在短時間內讓遠端用戶連接到公司網路。然而，隨著勞動力變得更加分散，企業需要讓遠端使用者在更長的時間內保持安全的連結，這種方法的缺陷就變得明顯，包括性能緩慢、網路安全風險增加以及擴充性問題。

隨著遠端存取需求的增長，越來越多企業從傳統的 VPN 轉向更安全、更高效的遠端存取解決方案。零信任網路存取 (ZTNA) 會在特定應用程式、私有 IP 和主機名四周建立安全疆界，把默認允許的 VPN 連線替換為基於認證和情境授予存取權限的默認拒絕策略。

2020 年，有大約 5% 的遠端存取主要採取 ZTNA 服務。由於傳統 VPN 存取的侷限，加上對更精確的存取和工作階段控管的需求，預計在 2024 年這一數字將躍升至 40%。[1]

雖然 ZTNA 對企業來說具有一些明顯的優勢和擴充功能，但許多企業發現它尚無法完全替代 VPN 基礎結構。但隨著 ZTNA 變得更加強大且 VPN 的問題變得更嚴重，這種情況正在迅速改變。本文比較 VPN 和 ZTNA 遠端存取解決方案，以闡明它們的優點和侷限性，同時說明遷移物件時最重要的考慮因素。本文解釋 Cloudflare 如何提供 ZTNA 服務，並推薦一組行動步驟，可將傳統 VPN 基礎結構過渡到為遠端用戶提供更快、更安全的 Zero Trust 連線。

[1] Riley, Steve, MacDonald, Neil, and Orans, Lawrence. "Market Guide for Zero Trust Network Access." Gartner Research, https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access. 2021 年 6 月 21 日取得。有關詳細資訊，請參見表 1。

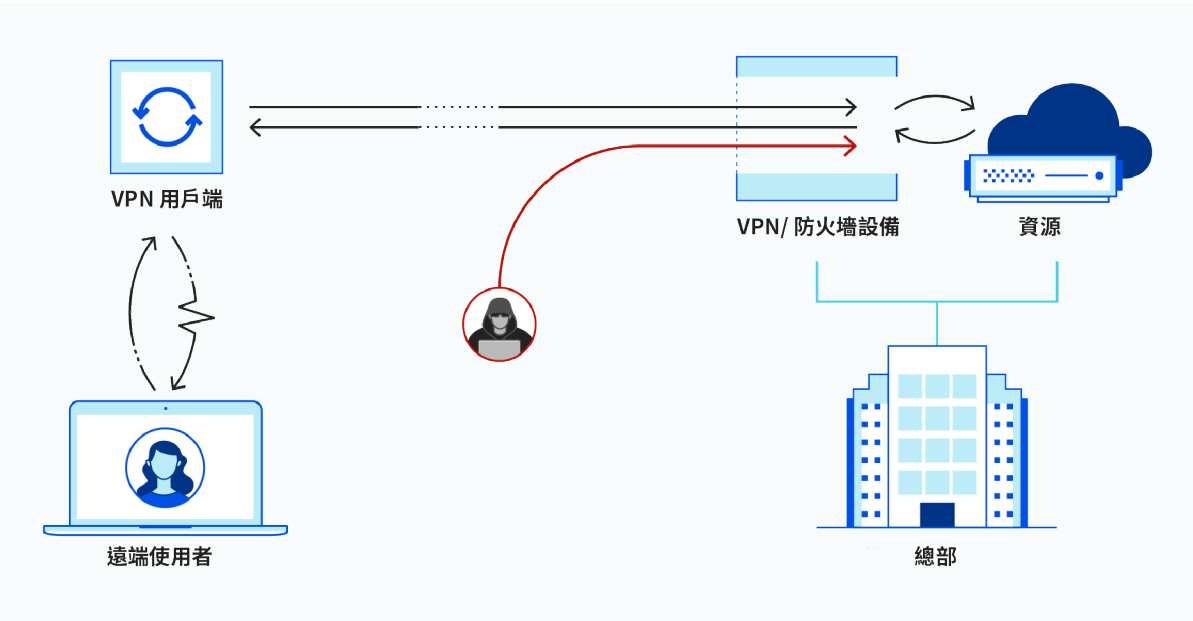
方法一：傳統 VPN

數十年來，企業藉由 VPN，讓遠端使用者能連接到具有一定隱私和網路安全措施的企業網路。若透過公共網路存取敏感性資訊，可能遭受任何攻擊者窺探或竊取；而 VPN 不同之處在於，讓用戶透過加密連線安全地存取內部資源。

兩種最常見的 VPN 實施模式，是基於客戶端的 VPN 和無客戶端的 SSL-VPN。每種模式都有其優缺點：

基於客戶端的 VPN 透過加密隧道，將遠端用戶連接到專用網路。這種連線是透過軟體應用程式或客戶端建立，要求用戶以使用者名稱和密碼執行一次身份驗證，以便長期存取該網路內的任何資源。	**優點：**連線之後可自由橫向移動，用戶可以存取應用程式、連接內部主機，輕鬆快速存取多種資源。 **挑戰：** • **並非為漫遊用戶和行動裝置而設計**。當用戶四下漫遊時，隨著無線網路在不同位置的變化，他們的筆記型電腦和行動裝置也會無縫地重新連線。但是 VPN 客戶端不擅長流暢地處理這些重新連線，需要用戶反覆強制 VPN 客戶端重啟和重新執行身份驗證，因而導致生產力降低並產生 IT 報修單。 • **可見性差**。使用這種方法，VPN 基礎結構會終止資料中心內部防火牆後的 VPN 客戶端加密隧道。儘管這些連線有紀錄，但沒有應用程式特定的集中日誌可以顯示用戶存取了哪些應用程式或他們在應用程式中執行了哪些操作。

無客戶端 SSL-VPN 入口允許一些遠端用戶連接到專用網路中一些基於瀏覽器的應用程式。這些連線之所以可行，是使用運行 VPN 服務的網路設備中內建的網路伺服器。	**優點：**無需在設備上使用客戶端，任何網路瀏覽器都可以使用門戶網站的 SSL 憑證建立加密的 HTTPS 連線，可支援使用非託管設備的承包商。 **挑戰：** • **安全問題。**資料中心大多數 VPN 設定都授予用戶完整的存取權限，這給不希望非正式員工（如承包商）不受限制存取敏感資源和應用程式的企業來說，是個問題。 • **並非為支持大量並行用戶而生。**不同於現代的雲端服務，入口網站的網頁伺服器無法彈性擴充以滿足更高的需求，必須安裝更多網路設備並進行負載平衡才能擴充入口，這通常價昂、複雜且低效，因為設備的其餘功能可能未充分利用。 • **無客戶端 SSL-VPN 入口讓防火牆連接埠和網頁伺服器暴露在攻擊下。**為了讓託管入口的網頁伺服器能存取內部應用程式，管理員必須打開入站防火牆連接埠，讓它們暴露在外部攻擊下。開放的連接埠和網頁伺服器本身都必須採取防護，避免 DDoS 和網路應用程式攻擊，這需要更複雜的配置和更高的成本，才能確保這種連線方式的安全。



儘管 VPN 為遠端用戶提供了基本層級的隱私，但網路安全或擴充性並非設計的主要目的。以往，企業使用 VPN 讓一些遠端用戶在短時間內連接到公司網路。然而，隨著遠端工作變得越來越普遍，VPN 的問題開始成倍地增加：

- **用戶經歷到效能緩慢。**若 VPN 基礎結構無法處理工作者製造的流通量及同時連線，用戶的網路連線就會變慢。此外，當 VPN 距離用戶和他們要存取的應用程式伺服器都很遠時，這段旅程就會造成等待時間。
- **企業網路容易受到攻擊。**VPN 通常使用城堡和護城河模型，用戶只要連接上網路就可以不受限制地存取所有企業資源。由於沒有內建限制存取關鍵基礎結構和資源的方法，企業被迫配置昂貴、複雜的安全服務，例如下一代防火牆和網路存取控制，否則就容易受到惡意橫向移動的影響，導致更嚴重的資料外洩。

託管 VPN 服務的挑戰

一些供應商已將運行 VPN 服務的網路設備轉移到公有雲端中，作為一個或多個資料中心的虛擬機運行。此 VPN 不一定與附加安全服務捆綁（或以菊鍊方式連接）。

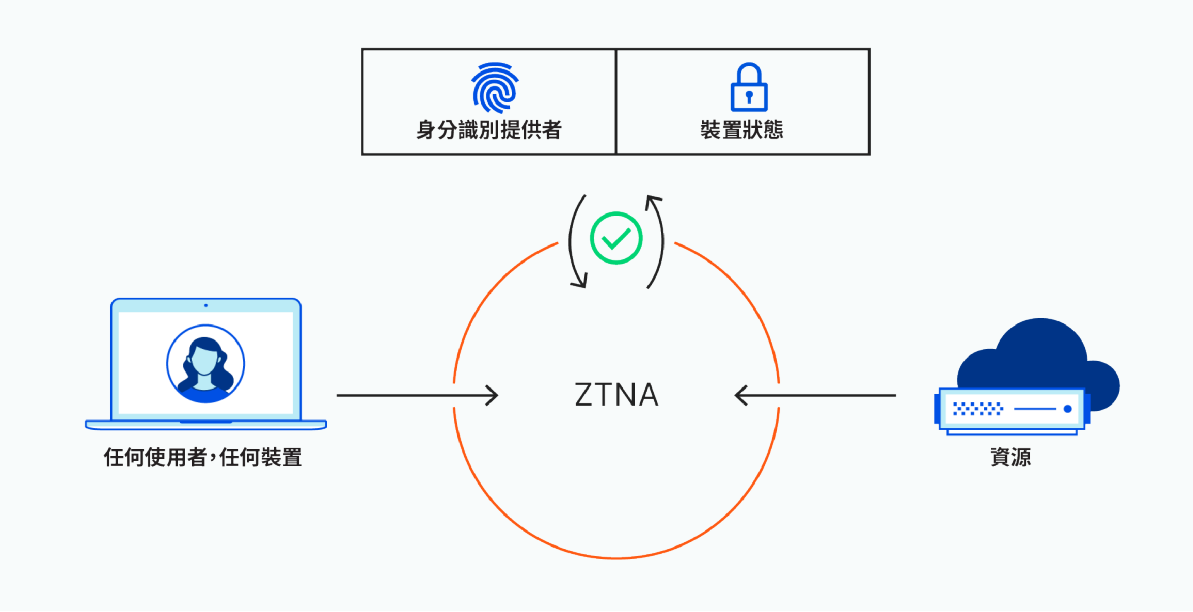
把 VPN 放在雲端似乎可以解決硬體 VPN 設備固有的擴充性問題。然而，這也帶來了一些重大的安全性和擴充性的挑戰。

例如，若有一個組織代管完整的 NGFW（下一代防火牆），將 VPN 與防火牆及附加網路安全功能結合。既然 NGFW 是捆綁的服務，因此不可能根據需要獨立擴充特定的功能。要擴充一項功能就需要擴充整個服務；因此必須啟動更多 VM，以便對每個 VM 中正在執行的少量運算進行負載平衡。這不僅是一種不切實際且笨拙的解決方案，而且隨著企業的遠端存取需求不斷擴大，可能會產生高昂的成本。

方法二：ZERO TRUST 網路存取

Zero Trust 網路安全規避了 VPN 固有的許多挑戰。它的基本原則是，網路內外任何用戶或設備都不被默認為可信任。為了降低資料外洩、內部攻擊和其他威脅的風險及影響，Zero Trust 方法.....

- 驗證每一個登入和要求，
- 對所有用戶和設備要求嚴格的驗證，
- 根據身份認證和使用情境，限制每個用戶和設備可以存取的資訊，
- 並添加端對端加密，以隔離網路內的應用程式和資訊。



與 VPN 一樣，ZTNA 可以用多種方式配置：

1. **無客戶端（或由服務啟動）的 ZTNA** 使用現有瀏覽器而不是客戶端來建立安全連線並驗證用戶設備。過去，無客戶端 ZTNA 一直僅限於使用 HTTP/HTTPS 通訊協定的應用程式，但其兼容性正在快速發展。[2]
   - **優點：**無客戶端 ZTNA 使用反向 Proxy 連線來防止直接存取應用程式，阻止用戶存取他們可能無權查看的應用程式和資料，並允許管理員在管理時有更大的控制權和靈活性。
2. **基於客戶端（或由端點啟動）的 ZTNA** 先在用戶設備上安裝軟體，然後才在控制媒介和經授權的應用程式之間建立加密連線。
   - **優點：**基於客戶端的 ZTNA 讓管理員可以更深入地瞭解存取應用程式的用戶其設備狀態、位置和風險脈絡，因而能建立及採取更精細的策略。同時，這種方法不限於 HTTP/HTTPS，因此可用於存取更廣泛的非 HTTP 應用程式，例如那些透過 SSH、RDP、VNC、SMB 和其他 TCP 連線的應用程式。

[2]截至 2021 年 6 月，Cloudflare 的 ZTNA 解決方案支援無客戶端存取 SSH 和 VNC 應用程式，並計劃在未來支援 RDP。

採行 ZTNA 的挑戰

儘管 ZTNA 與傳統 VPN 相比具有明顯的優勢，但它並非保護遠端用戶存取網路的完美方法。當企業權衡採用 Zero Trust 方法的利弊時，他們可能會遇到以下一種或是多種的挑戰：

並非真正雲端原生的解決方案。

如果供應商不提供基於雲端的 ZTNA——意味著客戶必需在自己的資料中心部署軟體——那麼用戶將失去即時擴充和無限通量等關鍵優勢。

供應商可能不提供基於客戶端及無客戶端的 ZTNA 服務。

這對需要將用戶連接到非 HTTP 應用程式（如遠端桌面、SSH 應用程式或文件共享）的企業而言，其價值有限。

配置可能既複雜又耗時。

不提供支援策略編排和自動化（透過 Terraform 之類的工具）的供應商，可能會讓管理員面臨更多手動工作——還不包括識別提供者內已然必須的配置。

CLOUDFLARE 的遠端存取方法

保護和擴充遠端存取應該是一個無縫的過程，不會對安全解決方案造成負擔、造成性能下降或產生不必要的成本。Cloudflare 讓團隊能夠處理所有遠端存取的使用方式，並具有以下優點：

- **用戶和管理員可輕鬆、無風險地上手。**Cloudflare 可輕鬆與現有識別提供者和端點保護平台整合，以便採行 Zero Trust 策略，限制對企業應用程式和資源的存取。
- **靈活部署基於用戶端和無用戶端 ZTNA（零信任網路存取）**。Cloudflare 針對到 Web、SSH、VNC（即將包括 RDP）應用程式的連線提供無用戶端支援，並針對非 HTTP 應用程式以及到內部 IP 的私人路由提供基於用戶端的支援。

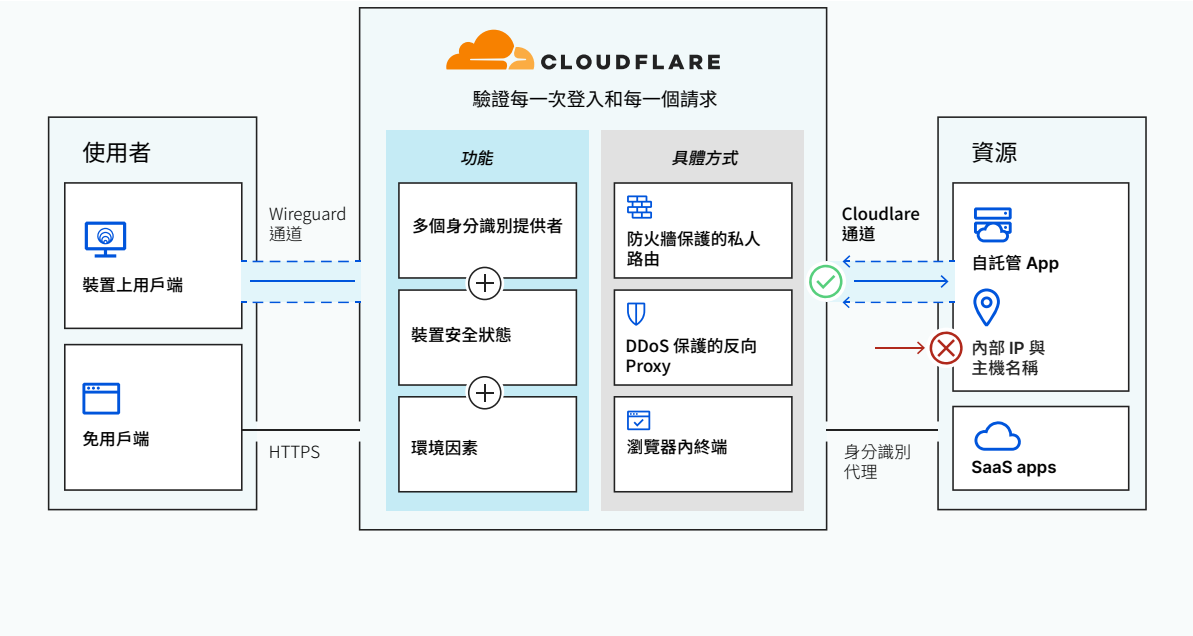


表 1：Cloudflare 如何解決遠端存取的挑戰

問題	解決方案	Cloudflare 實施
不容易擴充	全球邊緣網路	擴充性問題困擾著非雲端原生的 VPN 和 ZTNA 服務，使遠端用戶難以存取應用程式和資料。 Cloudflare 的全球 Anycast 網路不僅讓用戶連線速度比使用 VPN 更快，而且不論遠端工作者有多少，都可以根據需要，確保他們能安全、快速地連接到公司資源，不需要管理員額外花時間進行配置。
與行動裝置的兼容性不佳	輕量的客戶	使用 IPSec 和 SSL 通訊協定的 VPN 和 ZTNA 解決方案，在行動和漫遊裝置上通常表現很差。 Cloudflare WARP 客戶端利用更現代的 Wireguard 通訊協定，在用戶空間中運行，以支援更廣泛的操作系統選項，並提供比傳統選項更快的使用者體驗。Cloudflare 的 WARP 客戶端可以在 Windows、MacOS、iOS、Android（即將包括 Linux）設備上進行配置。
沒有內建 DDoS 保護，或保護不足	內建領先業界的 DDoS 保護	如果沒有適當的內建 DDoS 保護，企業往往被迫以菊鍊形式連接額外的安全服務，這可能會造成配置問題、擴充性問題和網路安全挑戰。 Cloudflare 的 67+ Tbps 網路為任何 ZTNA 模式提供內建的 DDoS 保護，保護網路免受最大規模的巨流量攻擊。
通訊協定限制	支援非網路應用程式	✓ 模式兼容性：適用於 SSH/VNC 應用程式的無客戶端 ZTNA；適用於所有其他非網路應用程式的基於客戶端 ZTNA。
沒有整合的網路防火牆	內置網路防火牆	隨著企業網路的發展，企業必須平衡的網路安全硬體堆棧也在增長，導致成本、性能和安全性顧此失彼。 Cloudflare 使管理員能在邊緣執行網路防火牆策略，讓他們能夠精密地控管允許哪些資訊進出網路，並提高流量如何流經網路的可見性。 ✓ 模式相容性：基於用戶端的 ZTNA
缺乏精密的控管	內建安全網路通道 (SWG)	未經批准而使用應用程序可能會給企業帶來嚴重的網路安全問題；如果沒有嚴格的政策，用戶可能會訪問和篡改敏感資料和其他公司資源。 Cloudflare 將 ZTNA 與 SWG 結合，允許管理員對應用程式中的用戶和設備存取權限進行更精細的控管，因此用戶和以職能區分的團體只能存取他們需要的資源。 ✓ 模式兼容性：基於客戶端的 ZTNA

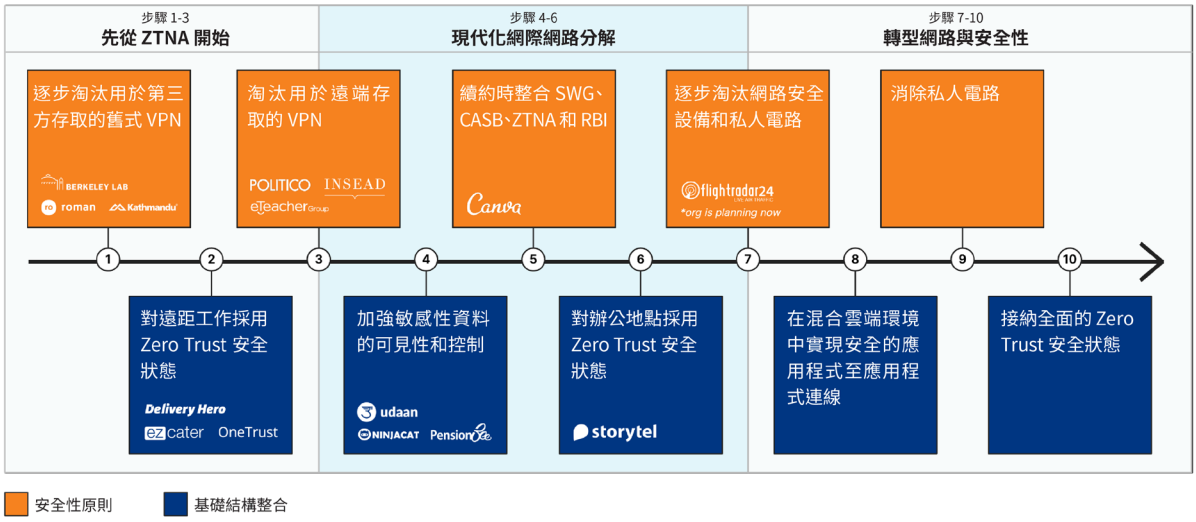
用ZERO TRUST 網路存取取代傳統的 VPN

在過渡到無 VPN 網路安全這段漫長而痛苦的過程中，Zero Trust 方法的承諾，對於 IT 安全領導者來說可能覺得很空洞。但是用 Zero Trust 網路存取替換您的 VPN 是可能的，且無需對支援的通訊協定或功能性妥協。

建議的遷移路徑，會根據推動這項計畫的業務優先等級而有所不同：

- 如果您優先考慮更快連接到應用程式，請首先為**非網路應用程式部署基於客戶端的 ZTNA**。
- 如果增強應用程式存取規則的安全性更重要，請從 **Web 應用程式開始**。

替換您的 VPN 只是全面網路轉型的第一步。由於過渡到 SASE 模型可能令人無法招架，因此我們根據客戶過去採用的方法，拆解出一條通向 Zero Trust 網路安全的常見路徑：



詳細了解 Cloudflare 的 Zero Trust 平台如何幫助您減少對 VPN 的依賴，並最終取而代之。

瞭解更多

查看 VPN 和 ZTNA 在實際使用上的比較，以及 Cloudflare Access 如何增強應用程式存取的安全性。

觀賞示範

附錄

讓現代化將您的網際網路帶來突破

實施 ZTNA 是部署安全存取服務邊緣 (SASE) 模型的重要步驟。**Cloudflare One** 是一個全面的網路即服務 (NaaS) 解決方案，可為各種規模的團隊簡化和保護企業網路。借由 Cloudflare One，組織可以：

- **接納 Zero Trust 存取。**將寬廣的網路安全疆界替換為逐一驗證每個請求對每個資源的存取。無論使用者位於何處，身份是誰，都會對公司應用程式的每個連線執行 Zero Trust 規則。
- **保護網路流量。**當網路上的威脅快速移動時，用來阻止它們的防禦措施也需要更加主動。Cloudflare One 可保護遠端員工免受網路上的威脅，並藉由在任何站點上實施 Zero Trust 瀏覽器隔離來實踐策略，以防止有價值的資料離開您的組織，同時提供流暢、閃電般快速的用戶體驗。
- **保護和連接辦公室和資料中心。**企業網絡變得過於複雜，這意味著用戶流量通常必須經過多個躍點才能到達需要去的地方。藉由 Cloudflare One，企業可以由一致、統一的雲端平台保護辦公室和資料中心。

想了解有關 Cloudflare One 的更多資訊，請觀賞 10 分鐘的介紹和展示。

轉化您的網路

即將推出的 Cloudflare Zero Trust 和 WAN 即服務將融合為一，使您的員工能夠持續訪問公司資源——無論他們在哪裡工作。

如今，您用的 VPN 和 WAN 產品允許您的員工存取位於您的專用企業網路中的資源，但它們也迫使您以不同的方式管理連接和安全策略。

現在，Cloudflare 提供了一個統一的控制平面，讓您可以更靈活地將相同的 Zero Trust 網路安全策略應用於您的所有工作者和工作場所中，而無需處理多個單點產品。

想瞭解更多，請上 https://www.cloudflare.com/cloudflare-one/.

© 2022 Cloudflare Inc.保留一切權利。Cloudflare 標誌是 Cloudflare 的商標。
所有其他公司與產品名稱可能是各個相關公司的商標。