白皮書

CLOUDFLARE

SASE 入門：網路基礎架構保護與優化指南

安全存取服務邊緣 (SASE) 在一個全球網路上整合網路和安全服務，從而簡化傳統的網路架構。本白皮書探討網路安全如何演進到 SASE，概述了 SASE 解決方案中所含的各種服務，並介紹了導入 SASE 的建議實踐步驟。

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

介紹

安全存取服務邊緣 (SASE) 這個術語是 Gartner 於 2019 年創造的，其最初定位為數位化轉型過程中的一個關鍵進步：高度可自訂的網路與安全服務無縫併入到全球雲端平台結構中。Gartner 預計其採用率將於 2023 年達到 20%，並且指出對 SASE 功能的需求將「重新定義企業網路和網路安全架構，並重塑競爭格局」。[1]

此後，這個詞就像野火一樣在 IT 和企業安全領域廣泛傳播。網路安全提供者和 SD-WAN 廠商爭先恐後地將自身定位成 SASE 領導者，擺在企業面前的是各種匆忙組裝、雜亂無章的網路和安全服務，這些雖然採納了 SASE 框架，但通常並未完全將之融入在內。

若要真正採用 SASE，不僅需要捆綁現有的單點解決方案，還要全面重新考慮企業網路基礎結構。維護牢固的內部部署網路邊界已不足以保護分散於各地的行動式員工，而同時使用多種安全服務來保護混合基礎結構可能會代價高昂，而且給 IT 團隊帶來部署和管理方面的麻煩，並留下巨大的安全性漏洞。

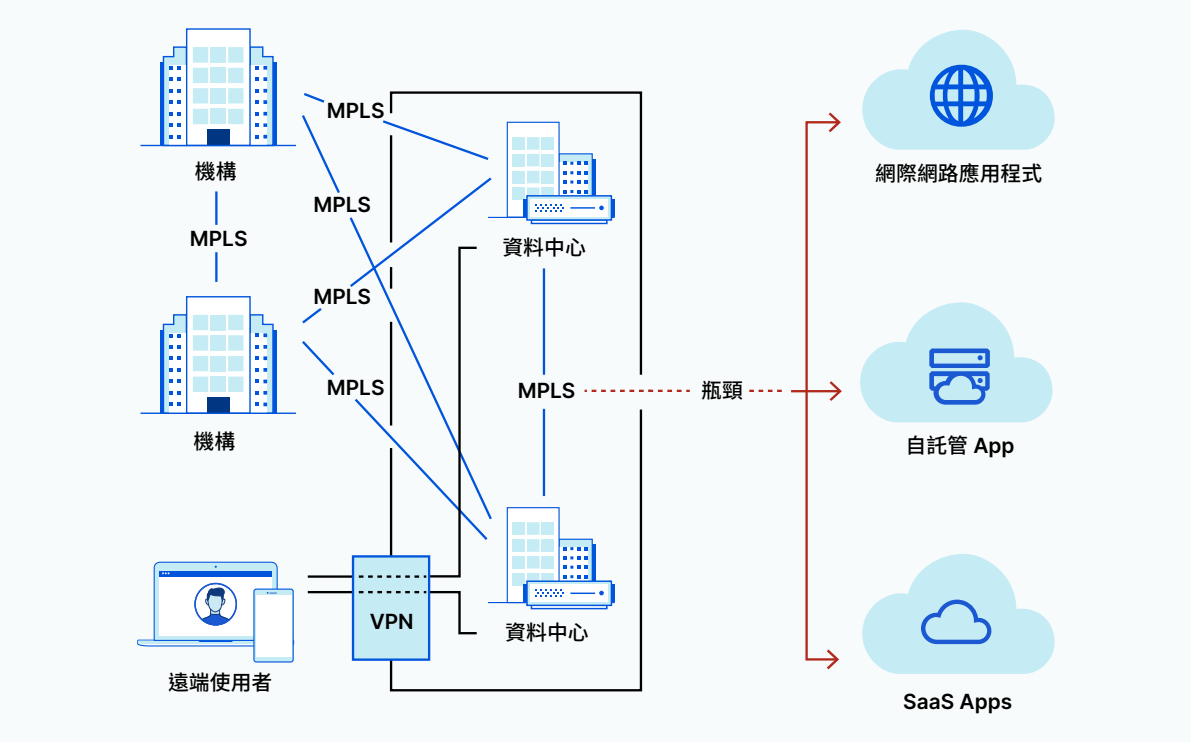
SASE 通過將網路邊界從集中式資料中心轉移到用戶來解決這些挑戰。通過整合網路連接和網路安全服務，並從基於 Zero Trust 原則的單一雲原生平台交付，SASE 消除了服務之間的安全空隙，為 IT 團隊提供了對網路活動的更大可見性，並簡化了雲遷移過程。

SASE 的起源 —— 舊模型

要瞭解 SASE 所代表的關鍵轉變，必須要審視網路基礎結構和安全性的逐步發展。

在雲端運算得到廣泛採用前，企業資源、資料和應用程式都存在於由硬體防火牆和 DDoS 設備保護的內部部署設施中。企業辦公室中的員工使用由網路防火牆篩選私密連線來存取內部資源。從遠端位置連接的用戶通常使用 VPN，這容易造成延遲，為避免過度擁擠和補丁漏洞的高昂開銷，以及糟糕的行動體驗。

這種設定掩蓋的是對開放網際網路的恐慌；網際網路這一工具最初是為了韌性而建構，極少考慮到企業效能和安全需求。事實證明，網際網路本身容易遭受攻擊，因此組織選擇自行建立私人網路，使用物理防火牆硬體和 DDoS 設備保護資料、應用程式和公司資源 (這種保護通常效果欠佳)，全部流量透過集中式資料中心進行檢查和篩選。



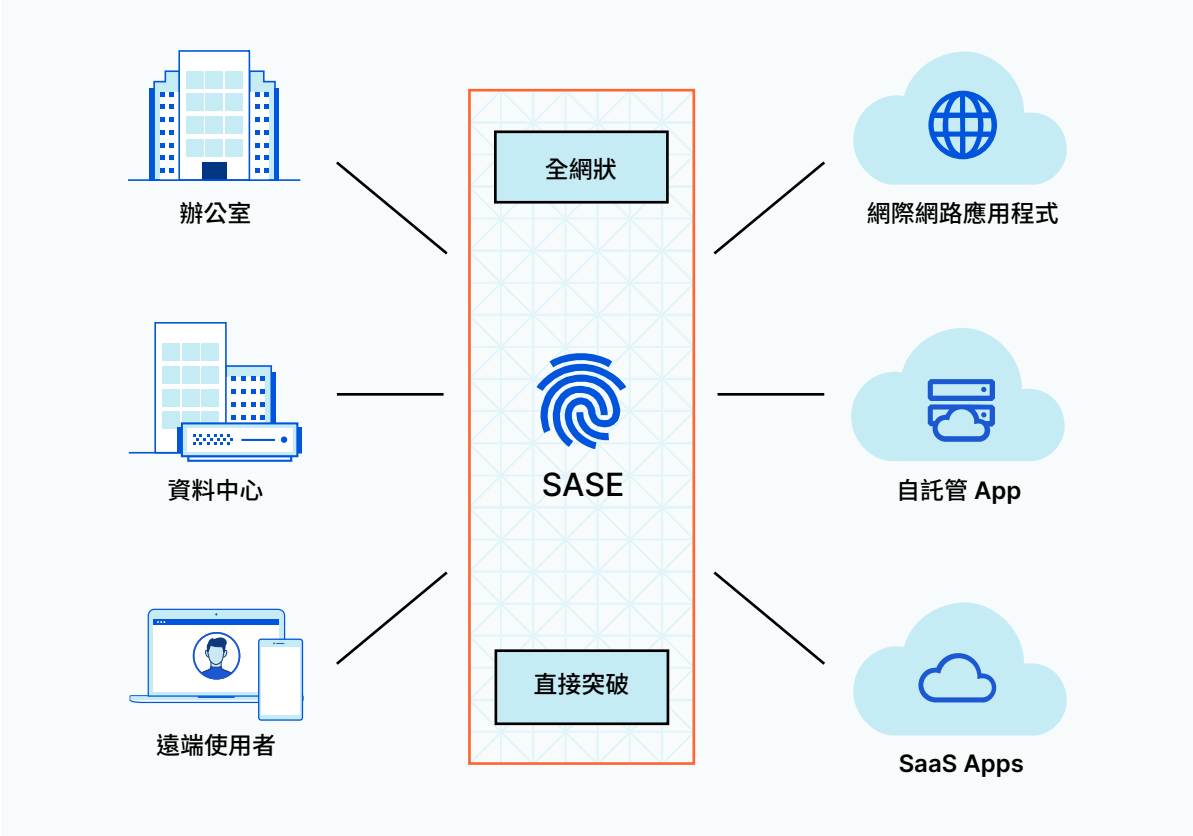
這種網路安全模型既昂貴又複雜，並且仍然使組織容易受到資料外洩和內部威脅的侵害。攻擊者一旦突破網路邊界，就可傳播勒索軟體、控制使用者帳戶[2]，並竊取寶貴的客戶資料，在組織內部造成嚴重破壞。[3]

隨著雲端和 SaaS 服務的問世，組織能夠更加自由和靈活地重新構想其網路基礎結構，因為應用程式、資料和員工不再需要全部駐留在內部部署設施中。

SASE 的起源 —— 新模型

但是，這種自由帶來了新的安全挑戰。IT 團隊不僅要負責保護部署於內部和雲端的服務，還要保護越來越多的行動和遠端員工。[4]要成功做到這一點，通常需要維護昂貴的硬體，還要對來自多家廠商的單點安全服務進行分層，其實施比較耗時，管理難度也很高。

網路安全性的下一個演進可能不會與保護傳統的「輻射式」基礎結構的硬體相像，也可能有別於混合雲端架構所需的複雜解決方案。相反，這看起來會像一種 SASE 框架，能夠合併網路和安全服務並將其作為整合服務來提供。



SASE 不依賴低效的硬體設備或將孤立的安全服務拼湊在一起，而是提供一種簡化的網路安全方法。它以網際網路邊緣取代複雜的回傳，讓企業能夠一次性完成對流量的路由、加速、驗證、過濾、隔離和檢查。通過結合全網狀 WAN 連線性、 Zero Trust 訪問策略和網路層威脅防護，SASE 淘汰了傳統 VPN 和 MPLS 電路以及硬體防火牆、代理和 DDoS 保護裝置，賦予組織對其網路安全配置的更大可見性和控制。

定義 SASE 的範疇 —— 核心能力

SASE 是一種基於雲端的安全模型，將軟體定義的廣域網路與核心網路安全服務捆綁在一起，並從雲端邊緣提供這些服務。大多數 SASE 產品具有五大功能：

建構和管理網路

藉助軟體定義的廣域網路 (SD-WAN)，組織可以建立公司私人網路，無需硬體路由器或多通訊協定標籤交換 (MPLS) 電路的支援。這種基於軟體的虛擬架構為企業建立和維護其網路基礎結構提供了更大的靈活性，但這也伴有一些內建的安全性漏洞。

篩選流量

安全 Web 閘道 (SWG) 可從 Web 流量中篩選不需要的內容，阻止未經授權的使用者行為，並執行公司安全性原則，從而預防網路威脅和資料外洩。這通常包括 URL 篩選、反惡意軟體偵測和封鎖以及應用程式控制等功能。

保護資料

雲端存取安全代理 (CASB) 為雲端託管服務 (例如，SaaS、IaaS 和 PaaS 應用程式) 執行多項安全功能。標準 CASB 透過存取控制和資料丟失防護來保護機密資料、揭示影子 IT，並確保遵守資料隱私法規。

將使用者與應用程式相連

Zero Trust 網路存取 (ZTNA) 要求即時驗證各個使用者對每個受保護應用程式的存取，以保護內部資源並防禦潛在的資料外洩。透過採用「Zero Trust」方法，任何實體都不會自動得到信任，只有透過身份驗證後才會受到信任，即便這些實體已在私人網路的邊界之內，也是如此。

保護應用程式和基礎結構

雲端防火牆 (FWaaS) 藉由一系列安全功能 (包括 URL 篩選、入侵預防和統一原則管理) 保護雲端基礎結構和應用程式免受網路攻擊。

定義 SASE 的範疇 —— 一流能力

儘管傳統的 SASE 解決方案包括上述五項服務，但這張清單其實更像是一個起點，而非一組嚴格的要求。SASE 的核心是融合兩個基本且獨立的功能：基於軟體的網路架構和基於雲端的安全服務。在這基礎上，不同廠商可以酌情增減其他服務。

雖然 SD-WAN 幫助客戶管理網路連接的最後一英里，但其不能直接確保使用者和應用程式之間連接的安全性、效能和可靠性。它充其量只能通過多個全球網路和串聯多種安全服務來優化端到端連接，此舉既複雜又昂貴。如果 SASE 提供商擁有從頭構建的 WAN 即服務，無論是否使用 SD-WAN，都能讓客戶僅管理一個預設內建安全、效能和可靠性的全球網路。SWG、CASB 和 ZTNA 共同顯著降低了安全風險，但在所有用例中，這些服務的結合仍然留下許多威脅和資料保護方面的漏洞。如果 SASE 提供商擁有從頭構建的遠端瀏覽器隔離，且在每一個資料中心與 SWG、CASB 和 ZTNA 原生集成，就能夠消除這些漏洞。

SASE 方法的優勢

隨著 SASE 的不斷發展，不同廠商和組織的 SASE 實施可能會大相徑庭。不過，相比於內部部署和混合型網路安全設定，大多數 SASE 解決方案具有幾個關鍵優勢：

實施更加流暢

透過整合網路和安全服務，SASE 消除了導入雲端式服務和設定內部部署設備的需求，也不需要投入時間、金錢和內部資源來更新這兩種資源以防禦最新的威脅。

等待時間得以減少

SASE 透過一個廣闊的邊緣網路來路由傳送網路流量，在盡可能靠近使用者的位置處理流量，從而減少等待時間並提升效能。路由最佳化可以根據網路擁塞和其他因素幫助確定最快的網路路徑。

原則管理更簡單

SASE 允許組織在所有位置、使用者、裝置和應用程式中設定、監控、調整和實施存取原則。從單個入口網站中識別並緩解攻擊和傳入威脅，而不必使用多個單一用途的安全工具來分別進行監控和管理。

全球網路

SASE 框架構建在單個全球網路之上，使組織能夠將其網路邊界延伸到任何遠端使用者、分支機構、裝置或應用程式，並在整個網路基礎結構中獲得更大的可見性和控制力。

根據身分的網路存取

SASE 在很大程度上依賴於 Zero Trust 安全模型，該模型基於以下因素組合授予使用者身分和存取權限：使用者位置、時刻、企業安全標準、合規性原則，以及對風險/信任的持續評估。這種級別的安全性相比於過於寬鬆和天生易受攻擊的 VPN 有顯著的進步，可以防止內部和外部資料外洩並抵禦其他攻擊。

SASE 入門

如果企業已經花費大量時間、資源和金錢來精心部署內部設定，管理由雲端安全服務構成的複雜網路，或者仍在為迎接遠距工作之未來而調整，採用 SASE 可能會令其望而生畏，但不必如此。

您可以按照以下五個實踐步驟來開始採用 SASE：

1. 保護您的遠端員工。

實施 ZTNA 解決方案將減少對 VPN 的依賴甚至取而代之，保護企業資料和資源免受內部和外部威脅，同時改善使用者體驗。通過將安全 web 閘道和雲防火牆置於邊緣，無需通過中央資料中心回傳，就能節選、隔離和檢查流量。

2. 將分支機構置於雲端邊界內。

在分支機搆部署 Zero Trust 架構，淘汰本地安全設備（統一威脅管理等）。本地設備成本維護成本高昂，而且在瞬息萬變的威脅環境中效果不佳。

3. 將 DDoS 防護移到邊緣。

淘汰 DDoS 設備，使用雲原生的網路層 DDoS 保護，即時檢測和緩解威脅，保護企業網路免受攻擊。

4. 將應用程式遷移到雲端。

隨著組織規模擴大，將自行代管的應用程式從自有資料中心遷移到雲端，確保對所有流量應用一致的網路安全性原則。

5. 用統一的雲原生策略執行取代本地安全設備。

通過將策略執行轉移到邊緣，在一個面板中監控和管理所有流量、攻擊模式和安全性原則，從而降低維護網路硬體設備的成本和複雜性。

CLOUDFLARE 的 SASE 是 CLOUDFLARE ONE

Cloudflare One 是一個 Zero Trust 網路即服務平台，無論使用者在哪裡，都能將使用者動態連接到企業資源，在接近使用者的地方提供基於身份的安全控制。

通過 Cloudflare One 的網路服務，基礎結構團隊可：	通過 Cloudflare One 的 Zero Trust 服務，IT 安全團隊可：
• 將 Cloudflare 全球網路用作自己的 WAN。 • 以一個雲原生網路防火牆取代傳統硬體裝置。 • 提高應用程式效能，降低最終使用者延遲。	• 無需 VPN，即可安全、簡單地連接到資源。 • 阻止橫向行動、勒索軟體、惡意軟體和網路釣魚。 • 改善最終用戶體驗，優化管理工作，尤其是入門時間。

為什麼選擇 Cloudflare？

部署和管理簡單輕鬆

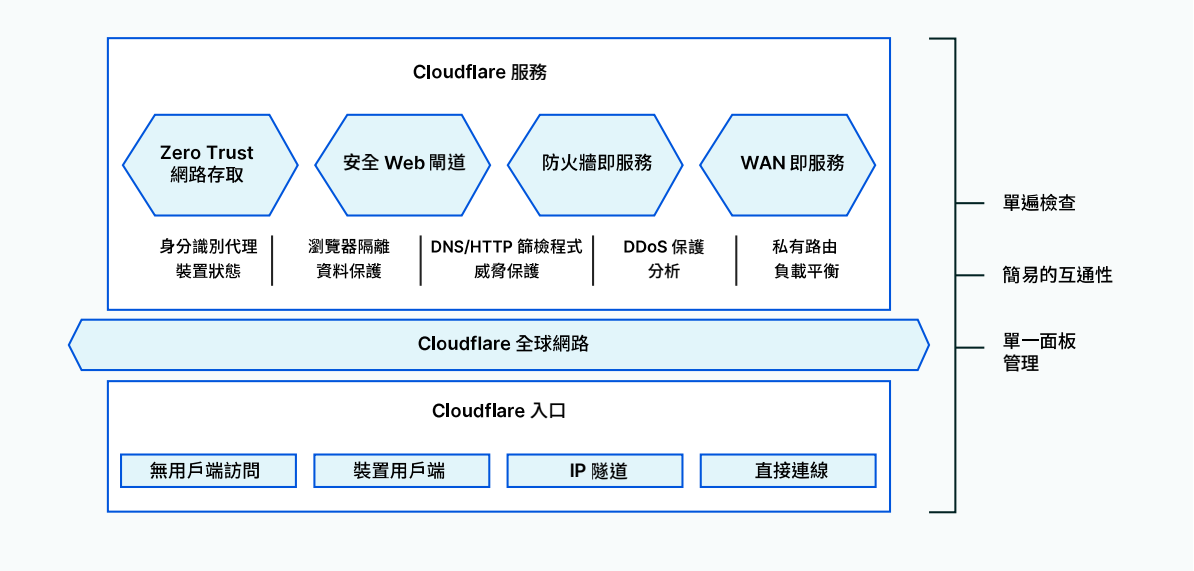
每一項 Cloudflare One 服務都運行於我們全球遍佈 250 多個城市的資料中心上。不必為了採用 SASE 模型而手動集成多個獨立的產品。

在世界任何地方獲得一致的安全性和速度

每一個 Cloudflare 資料中心都能提供一次通過流量檢查和路由，為世界任何地方的使用者提供相同的保護，不會因為延遲或「長號效應」而犧牲速度。

連接到原有服務

Cloudflare 運營世界上最強大、對等連接最多的網路，Cloudflare One 支援已經在使用的身份、端點和雲提供商。使用簡易，一次集成。



CLOUDFLARE 的 SASE 是 CLOUDFLARE ONE

Cloudflare One 提供您所需的安全和連接工具，在這個隨處工作的世界中連接使用者、應用程式和分支機構。

<table>
<tr><th colspan="2">Cloudflare One</th></tr>
<tr><td>Zero Trust 網路存取
通過執行基於身份和上下文的規則並限制橫向行動，比 VPN 更快、更安全地將任何使用者連接到任何應用程式和私人網路。

核心 SASE 能力：
• 將使用者與應用程式相連
• 保護資料</td><td>WAN 即服務
用我們的全球專用骨幹網取代您的傳統廣域網路架構，以更快的效能、內置安全性和更高的韌性實現任意對任意連接。

核心 SASE 能力：
• 建構和管理網路</td></tr>
<tr><td>安全 Web 閘道
通過無限制的 SSL 檢查來實施 DNS、HTTP、網路和瀏覽器隔離規則，阻止已知和未知的網際網路威脅，並輕鬆控制資料流。

核心 SASE 能力：
• 節選和檢查流量
• 保護資料</td><td>防火牆即服務
通過對所有傳入和傳出流量執行狀態檢查規則，控制訪問——並阻止 DDoS 攻擊和其他威脅，同時維持快速效能。

核心 SASE 能力：
• 保護應用程式和基礎結構</td></tr>
<tr><td colspan="2">Cloudflare 全球網路
我們的網路容量超過 90 Tbps，覆蓋全球 250 多個城市，擁有 9800 多個互連，並提供 100% 正常執行時間 SLA，與 95% 的聯網人口延遲不超過 50 ms。</td></tr>
<tr><td>無用戶端訪問
短短幾分鐘即可配置任何使用者和裝置（包括協力廠商和自帶裝置），以基於瀏覽器的安全方式訪問自託管和 SaaS 應用程式，而非僅僅使用 HTTP。</td><td>IP 隧道
通過使用 GRE 隧道或我們自己的 Tunnel 連接器，通過 BGP Anycast 路由公告接入整個雲端或本地環境中的公共和私有 IP 子網。</td></tr>
<tr><td>裝置用戶端
配置 Windows、macOS、iOS、Android、ChromeOS 和 Linux 裝置，以基於安全用戶端的方式訪問任何應用程式、私人網路絡或網際網路目的地。</td><td>直接連線
將您的網路基礎結構從公共網際網路在物理或虛擬意義上遷移到 1600 多個託管設施中，獲得更可靠、更安全的體驗。</td></tr>
</table>

使用 CLOUDFLARE ONE 帶來的業務成果

↓91%

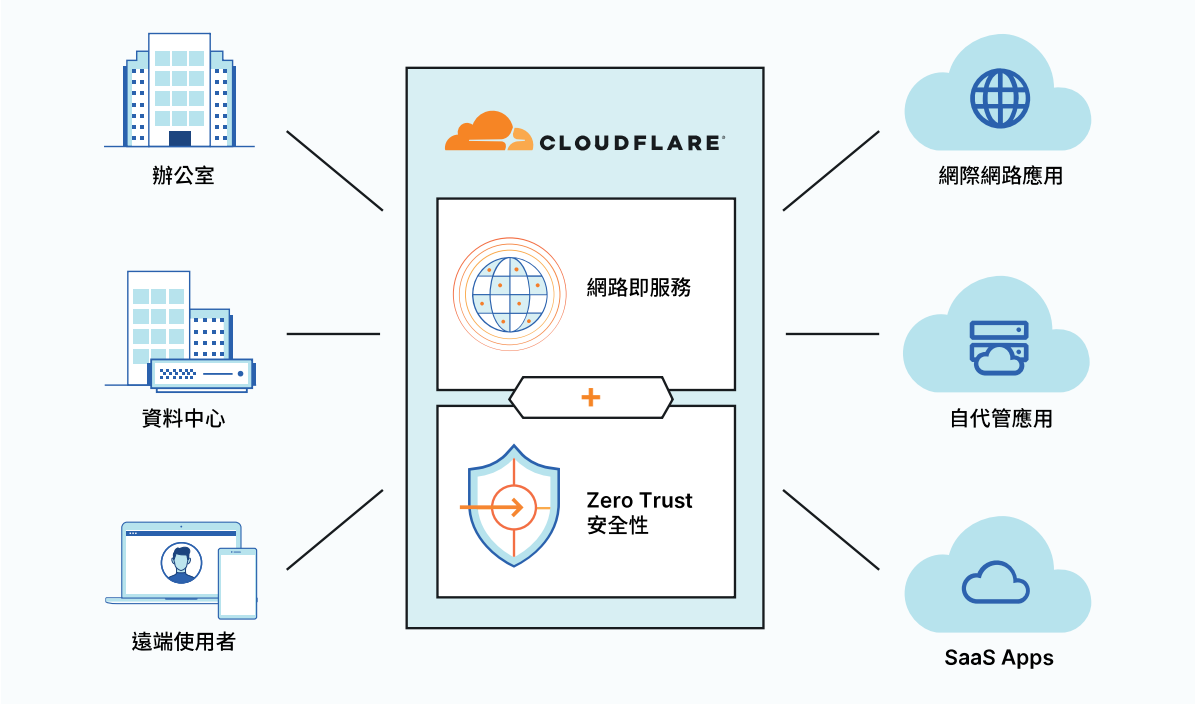
通過從最終使用者系統隔離高風險瀏覽，從網路隔離應用程式訪問，可將攻擊表面減少高達 91%。

10 → 1

將多達 10 款獨立產品整合到一個平台上，降低總體擁有成本，加速您的業務

↑60%

通過用 Cloudflare 代替 VPN 來將用戶連接到資源，接入新員工和承包商的速度加快多達 60%。



進一步瞭解 Cloudflare One

按一下此處

參考文獻

1. Gartner，「網路安全的未來在雲端」，分析師 Neil MacDonald、Lawrence Orans 和 Joe Skorupa 於 2019 年 8 月 30 日發表。Gartner。Gartner.

2. Twitter Inc.，「關於我們安全事件的更新」。Twitter。2020 年 10 月 27 日存取時的資料。

3. Marriott International News Center，「萬豪國際向客人通告酒店系統事件」。Marriott。2020 年 10 月 27 日存取時的資料。

4. Bursztynsky Jessica，「Dropbox 是三藩市最新一家永久化遠距工作的技術公司」。CNBC。2020 年 10 月 27 日存取時的資料。