

比較 Cloudflare 與 Zscaler

何者能夠更好地推動轉型？

Zero Trust 佈建無需 如此困難

別侷限了自己的未來

Cloudflare 能夠協助您隨著網路未來的演變而快速敏捷地遷移。

快捷方便的佈建，極具彈性的網路架構以及快速創新能力，能夠為網路、安全性及應用程式的實質轉型提供更穩固的基礎。



客戶選擇 Cloudflare 而非 Zscaler 的三個原因



1. 快速部署的 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。客戶不需要花費時間在容錯性低的碎片化平臺上面。



2. 受信任的連線功能， 可靠地提供保護

Cloudflare 流量自動化的特點，能夠提供客戶信任的可靠性與效能。沒有人想要以手動方式連線到多個雲端網路的功能，因為這樣會使網路安全有所折衷。



3. 與時俱進， 能夠快速演變

Cloudflare 的架構將創新內容整合至客戶使用的相同網路中，以便快速演變。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。

挑選專為網路未來所設計的架構

如果選擇 Cloudflare 而不是 Zscaler，您將受益於建置用於在全球各地所有伺服器上執行所有邊緣服務的網路。我們將整個網路帶向雲端，並啟用具備單遍檢查的 Zero Trust，快速地將使用者、設備、工作負載、辦公室、雲端和資料中心連線到資源，無論其地點為何。部署和執行非常簡單，因此您可以掌控全局，以任何所需的步調對您的環境展開現代化改造，不需要無限的 IT 預算、一整套昂貴的 POC 和多種複雜的部署，您可以輕鬆實現目的。

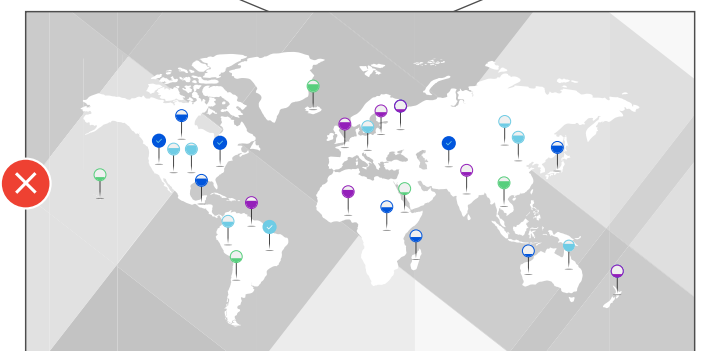
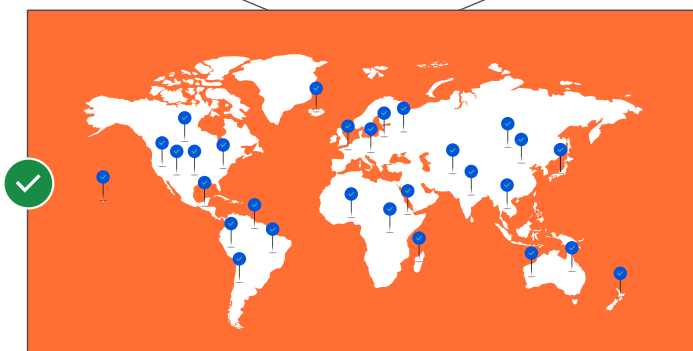
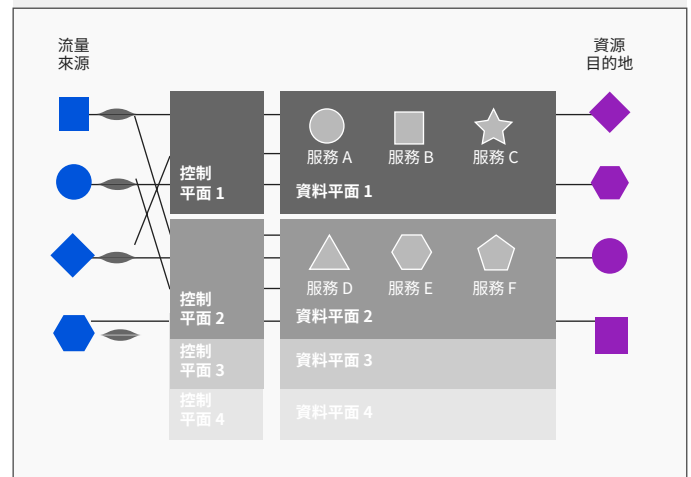
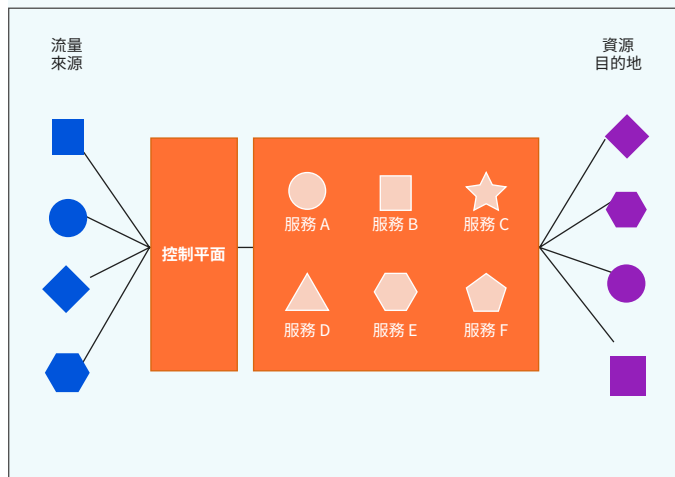
Cloudflare - 統一控制

統一控制平面提供單遍檢查和可靠的連線功能。

與

Zscaler - 碎片化

另一方面，零散且拼湊的架構增加了複雜性，而且還會產生額外風險。



在資料中心位置的相對採樣中，每項 Zscaler 服務都只在一小部分的位置執行，且僅一小部分的位置可供每個客戶使用。^{*}

^{*} 截至 2022 年 1 月：根據 cloudflarestatus.com 和 cloudflare.com/network，Cloudflare 在 250 多座城市擁有公共資料中心，且許多城市都有多個資料中心為其提供服務。根據 trust.zscaler.com 和 config.zscaler.com，Zscaler 在 55 座城市擁有 73 個公共資料中心，其中有 13 個資料中心位於未發佈的雲端中，並有 11 個資料中心停用自動地理鄰近性。所聲稱的其他 77 個資料中心似乎並未公開記錄。

快速追蹤您的歷程， 以保護任意連線

雖然各提供者之間的 Zero Trust 原則依舊相同，但實作和 ROI 卻迥然不同。

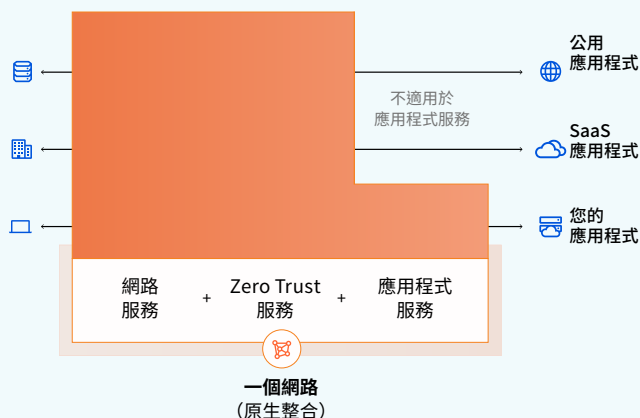
Cloudflare 統一透過單一網路和控制平面來連線和保護端對端，為您的 IT 從業者和終端使用者提供更好的體驗。

部署是否足夠簡易？

- 誰會挑選孤立的服務作為首選？沒有人。這就是所有 Cloudflare 入口及邊緣服務都切實協同合作的原因。
- 不要為了優質的支援而等待數週才開始採用。我們的服務平台是可組合的，因此您可以在數分鐘和數小時內解決實際的使用案例。
- 避免過度的虛擬機器部署後勤作業。透過僅限軟體使用的連接器和一次性整合，加快設定時間。

Cloudflare - 簡易

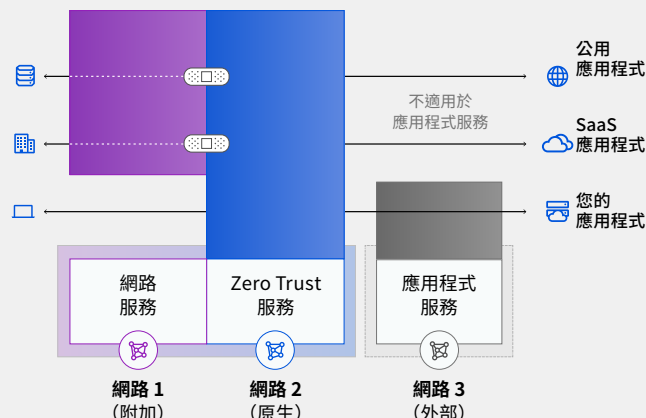
Cloudflare 的網路、Zero Trust 及應用程式邊緣服務已透過統一的後端架構完成原生整合。



與

Zscaler - 複雜

Zscaler 的網路和 Zero Trust 服務拼湊在一起，且並未全面涵蓋遠端使用者；另外，多家廠商間的應用程式服務完全孤立。



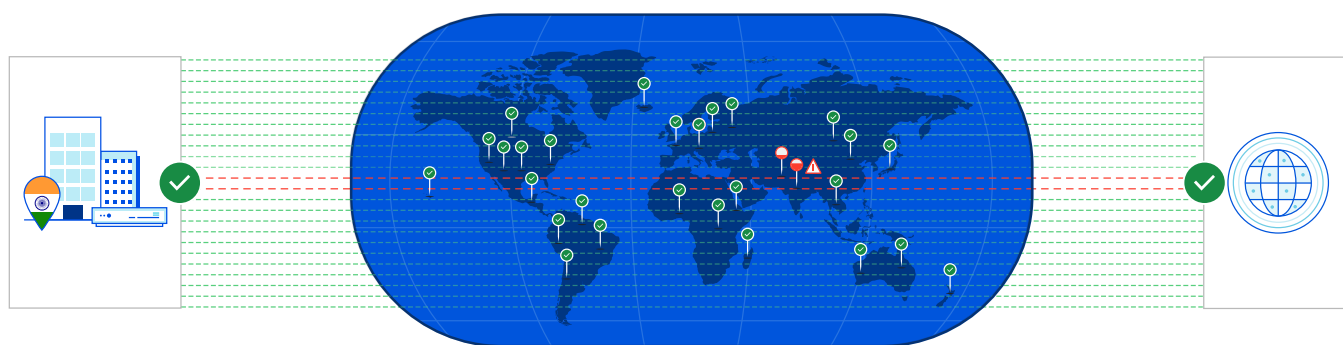
只有更好的網際網路才能夠始終如一地保護您的企業

如今，所有代理的網站中約有 20% 是透過 Cloudflare 網路路由，而這些網際網路流量都流經為您企業提供 Zero Trust 的相同代理。

我們的端對端流量自動化能夠確保可靠且可擴充的網路連線能力，從任何地點都能夠提供一致的保護。

網路復原能力是否足夠？

- 網路安全不應該像拼圖一樣。每個邊緣服務的建置方式應使其能夠在所有網路位置執行，且可供所有客戶使用。
- 我們為付費方案採用只有 Anycast 架構可以提供的 100% 正常運作時間 SLA。其他廠商之後無法將此功能新增到他們的平台。
- 直接的私人互連可讓您的流量遠離公共網際網路。這應該沒有商量餘地，但是 Zscaler 並未提供。



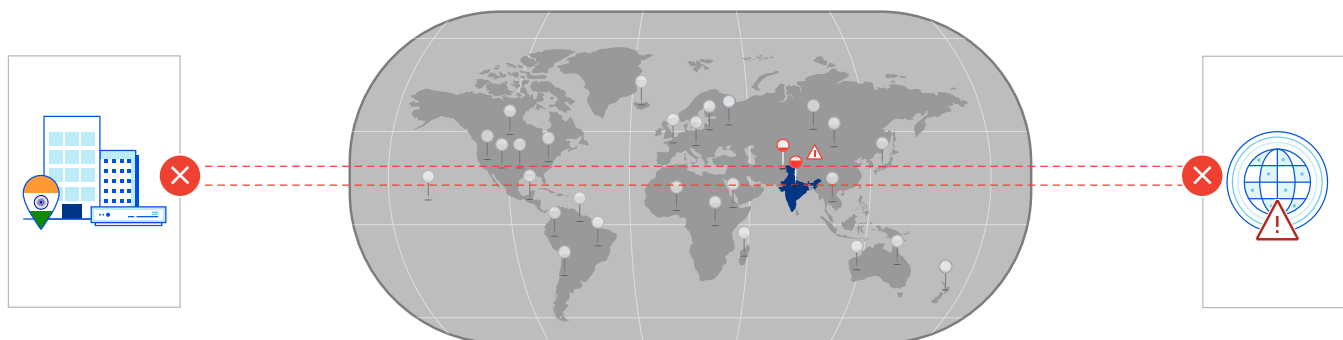
Cloudflare - 具備網路彈性

Cloudflare 網路的 Anycast 架構讓使用者安心無虞。如果發生地區問題，即會自動重新路由傳送流量，以保持邊緣服務的上線狀態。

與

Zscaler - 易受攻擊

服務位置受到限制時，即會因發生地區問題招致更多攻擊。如果主要和次要資料中心間同時發生預期或意外的服務中斷情況，Zscaler 服務即會經歷可避免的停機時間。



持續不懈地提前掌握現代企業的需求，保障您的未來

我們符合未來需求的架構有助於我們非常快速地建置和出貨，這是我們建立穩固名聲的根基；

請參閱我們的部落格一窺客戶見證！挑選具備變革速度快如閃電且由客戶主導的靈活提供者，才能開創新的網路、安全性和應用程式功能。

創新的步伐是否夠快？

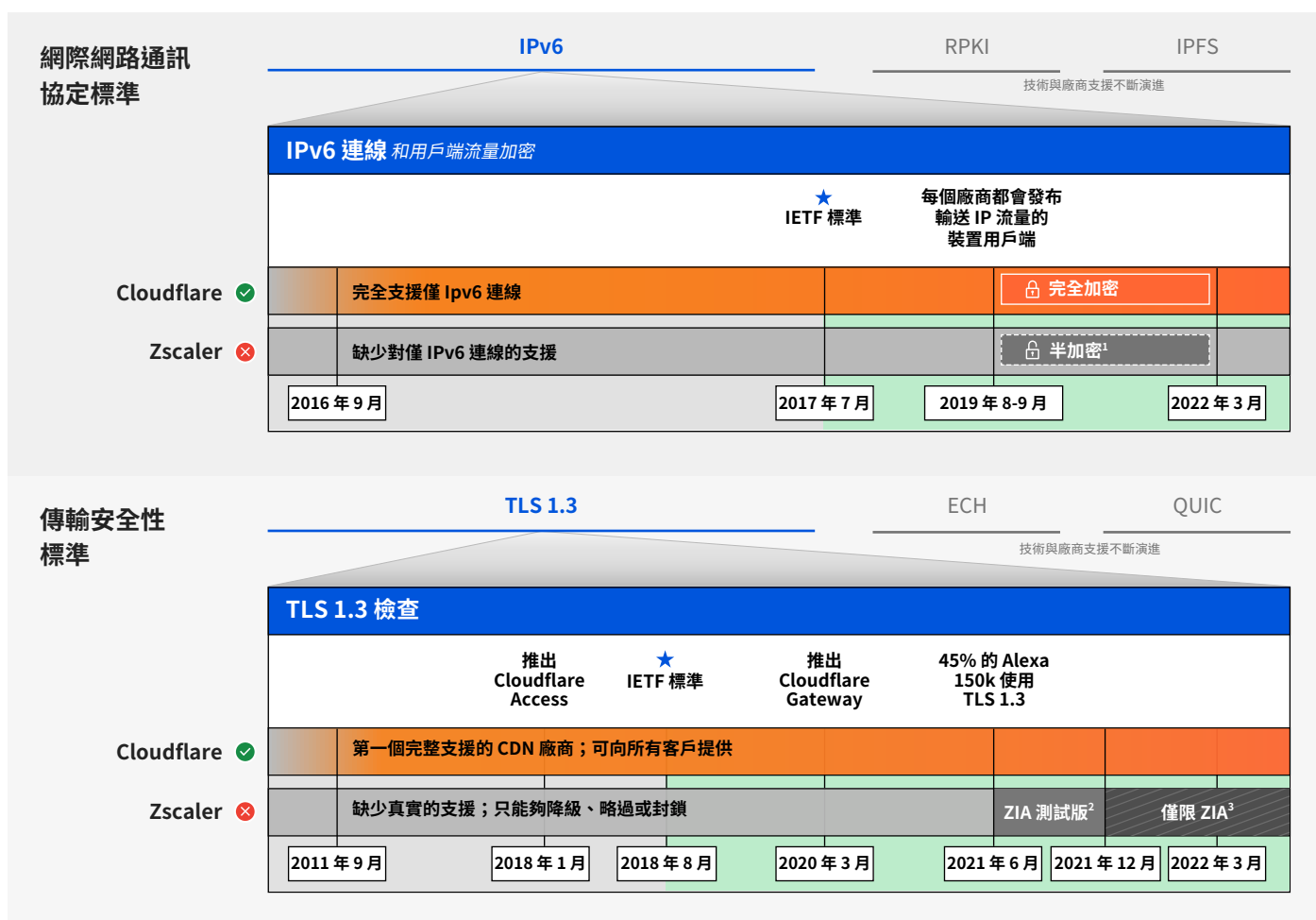
- 我們擁有的是一個可組合且利於開發人員使用的雲端平台，而不是多個碎片化的平台，因此可以隨著任何未來邊緣服務進行擴展。
- 我們能夠以快速且原生的方式採用新的網際網路和安全標準。
- 我們超凡的技術與成長的歷史不證自明，而且我們的基礎提供了最大的選擇性。

✔ Cloudflare - 創新

無論技術為何，您都需要快速創新和靈活性來保護未來。在採用全新技術方面，Cloudflare 執行速度之快可說是聞名遐邇。

✘ Zscaler - 停滯不前

在採用重要的全新技術（像是 TLS 1.3 或 IPv6 的全面整合支援）方面，您本不需要遲遲等待。



1. 裝置用戶端會對 ZIA 流量使用未加密的資料通道。只會將 TLS 控制通道加密。2. Zscaler 用於 ZIA 的測試版雲端僅擁有三個資料中心。

3. 僅適用於 ZIA 流量。對於 ZPA 流量，裝置用戶端會使用 TLS 1.2 通道來加密資料通道，但他們的雲端代理程式不會檢查應用程式加密的 TLS 1.3 流量。

參閱 Cloudflare 的
實現方式



Cloudflare

Zscaler

部署簡便性



服務接入

可組合且協同合作

多數是以獨立於其他的方式執行

網路安全與連線功能

端對端：使用者/工作負載對應用程式，加上 WAN 與應用程式

受限：
僅限使用者/工作負載對應用程式

網路與控制平臺

統一的單個網路，
單一控制平面

AWS/Azure 增強的網路，
多個控制平面

佈建要求

通常是無用戶端且無 VM 的軟體，
一次整合

通常為用戶端、VM 規模的後勤
作業，且重複整合

網路復原能力



全球連線

是：Anycast 架構

否：主動/主動本地終端

繞過公共網際網路

是：每個客戶都能夠以私人方式與
Cloudflare 網路互連

否：私人服務 VM 會繞過 Zscaler
雲端，而非網際網路

網路位置可用性

每個位置都可供所有客戶使用

只有一小部分的位置可供所有客戶
使用

服務可用性

每個邊緣服務的建置都能夠在所有
網路位置執行

每個服務都在一小部分的網路位置
執行

創新速度



雲端原生的架構

具備一致邊緣服務可用性的單一
雲端平台

具備碎片化服務可用性的多個雲端

利於開發人員使用的平台

可隨著任何未來邊緣服務組合和
擴展

已附加太長時間，多年之後
整合鬆散

新的網際網路和安全標準

快速採用，通常有助於設計

有些是數年後才引入

ZTNA 與 SWG 部署

分別在 4 和 2 年內建置

分別在 6 和 14 年內建置

既然可以在幾分鐘內就開始使用我們的免費方案，
為何要等待並付款來試用 Zscaler 呢？

看看有多簡單