CLOUDFLARE

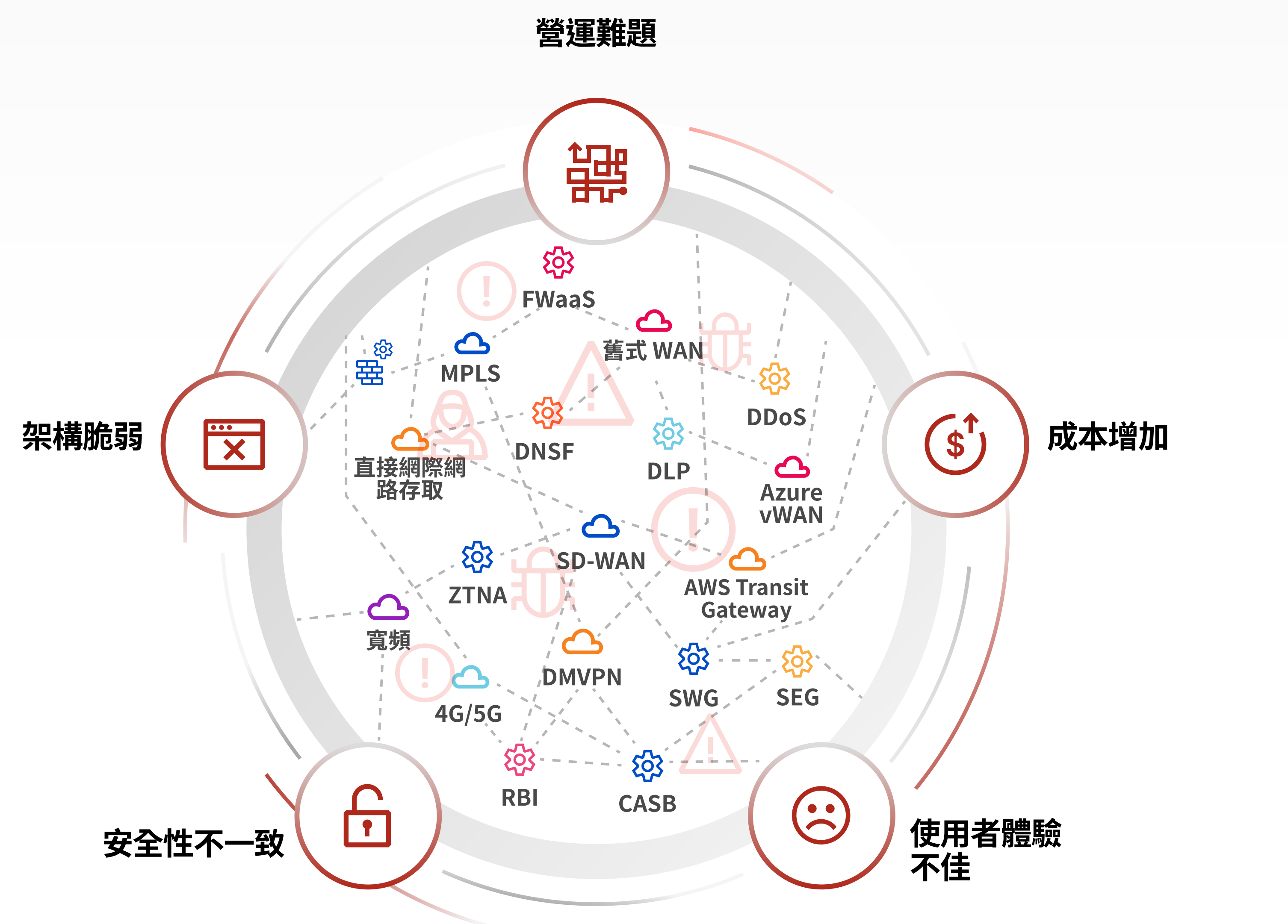
每條路徑都很重要

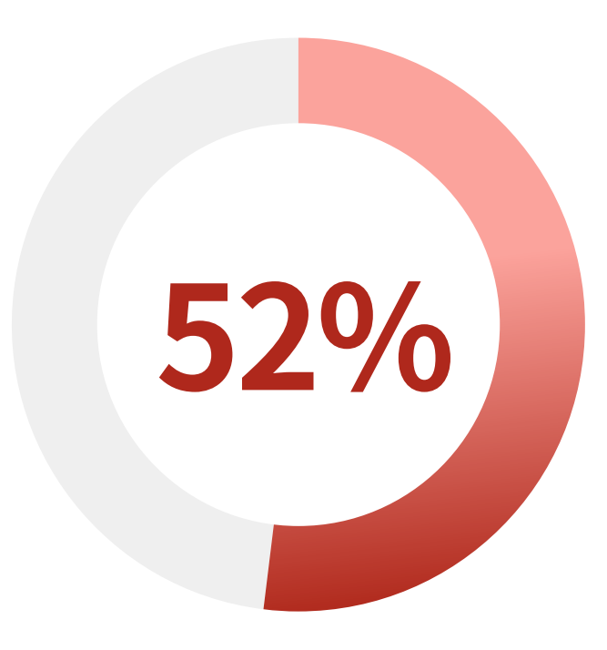
是否應重新規劃網路流量流程？

舊式企業網路僅專注於內部連線能力與安全性。然而，混合式工作、雲端部署的應用程式，以及快速的數位現代化投資，已徹底改變網路流動的地點和方式。

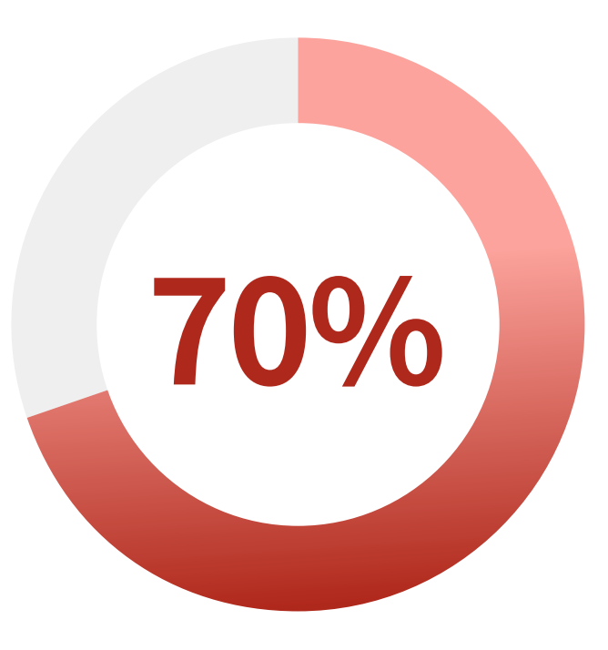
如果網路基礎架構無法滿足當今的業務需求會怎麼樣？

舊式企業網路經常遇到下列情況：





52% 的高階主管表示，**複雜性是安全運營的最大障礙**[1]



全球 70% 的 CEO 表示，**網路成熟度對**業務交付**產生了負面影響**[2]

平台化組織的平均投資報酬率為 101%，相較於未採用平台化的組織，後者的投資報酬率為 28%[1]

在傳統架構中，**使用數十種不同的解決方案來涵蓋四個網路流量流程**也會增加複雜性。

流量流程	所需產品	挑戰
來自網際網路的**傳入流量**	傳統上由內部部署防火牆、VPN、DMZ 基礎架構、網際網路服務提供者篩選所涵蓋	· DoS 和 DDoS 攻擊 · 零時差漏洞利用 · 網路釣魚 · 惡意程式碼
傳到網際網路和雲端應用程式的**傳出流量**	傳統上由內部部署的防火牆和代理伺服器所涵蓋	· 橫向移動 · 資料暴露 · 勒索軟體傳播 · 殭屍網路參與
園區與分支機構之間的 **WAN 網路**	傳統上由實體/虛擬化網路、SD-WAN、私人互連、MPLS 所涵蓋	· 更高的 CapEx/OpEx · 網路延遲 · 頻寬限制 · 不佳的使用者體驗
針對多重雲端中應用程式提供的**多重雲端**	傳統上由 DIY 產品涵蓋	· 可見度與原則強制執行問題 · 法規複雜性

必須**變更**

舊式網路

- 插入設備以新增功能或地理區域，這需要停機和服務中斷
- 連線並保護使用者和分支機構，以存取資料中心託管的應用程式
- 邊界內隱式「受信任」流量
- 經過最佳化，可支援辦公室工作人員

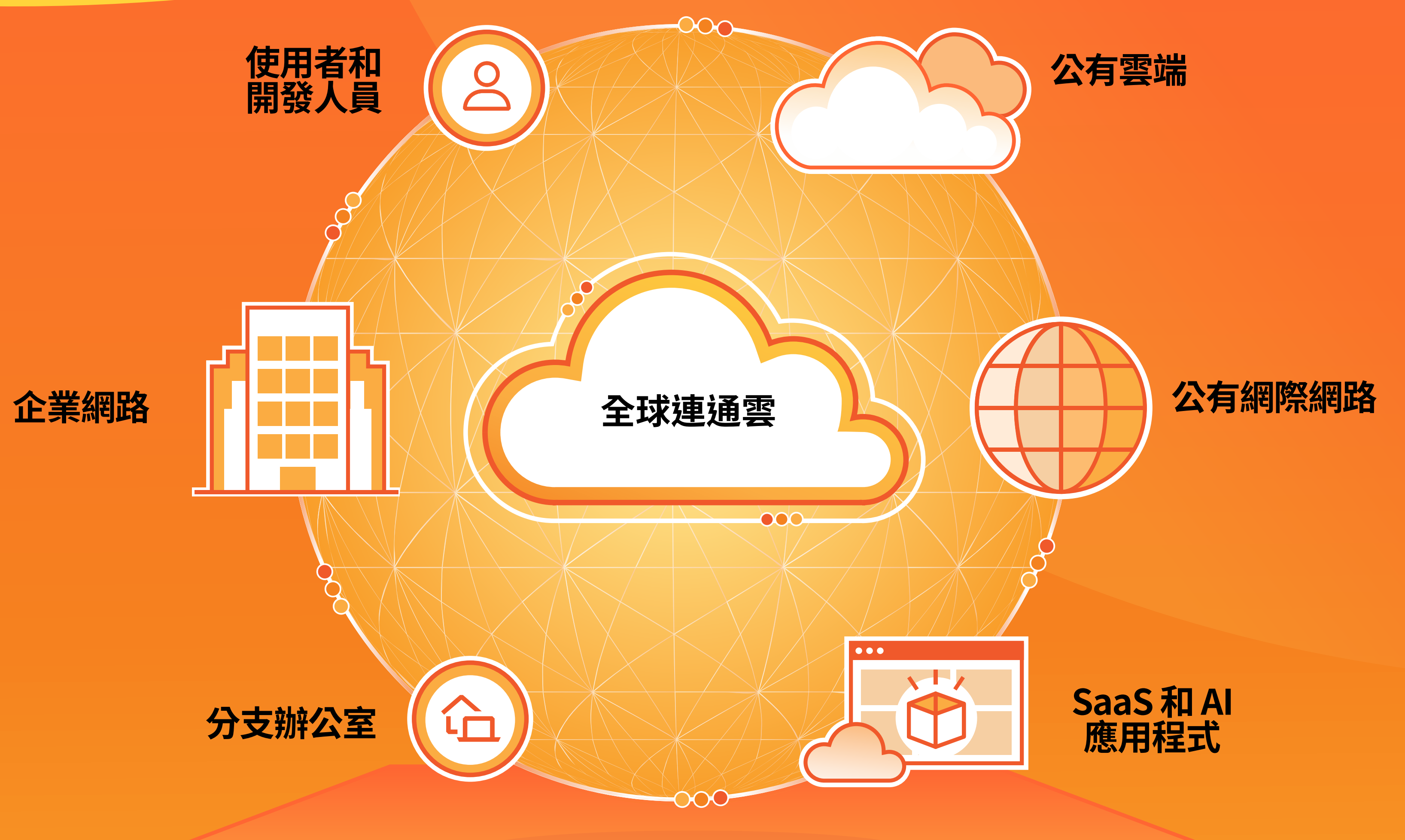
與

現代網路

- 部署組合式服務而非設備，減少複雜度與中斷
- 必須隨時隨地支援雲端、SaaS 和私人雲端應用程式
- 必須假設每個實體（包括分散式使用者、裝置、應用程式和資料）均為「不受信任」
- 不能假設使用者的位置，且必須支援使用者隨時隨地工作

如何在處理所有流量流程的同時滿足現代化要求？

全球連通云不是針對每個流量路徑使用不連貫的解決方案，而是從整體上解決了網路現代化問題。



傳入流量	傳出流量	WAN 網路功能	多重雲端流量
保護網路和應用程式免受 DDoS 及其他源自網際網路的威脅	保護使用者和辦公室免受威脅、強制執行一致的原則，並控制應用程式中的資料	連線並保護辦公室、使用者、裝置、資料中心和基礎架構	提供聯網功能，以在公有雲端/混合雲端環境中連線、保護及建置應用程式

Cloudflare 的全球連通雲使用組合式、可程式化架構，為您的使用者，以及在支援雲端的業務基礎架構和應用程式中，提供聯網與安全性服務。

- 無須延伸或擴展私人資料中心
- 使用雲端聯網與安全性服務，而非硬體設備
- 藉助 Zero Trust 減少對網路的過度信任

進一步瞭解如何利用 Cloudflare 來簡化和加速網路現代化

瞭解更多

---

1. Ali, Mohamad 和 Jenkins, BJ.「獲取網路安全紅利」IBM，https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform?。於 2025 年 6 月 26 日存取。

2. 「70% 的 CEO 表示，他們的網路正在減緩企業增長，全新 NTT 研究發現。」Business Wire，2022 年 10 月 20 日，https://www.businesswire.com/news/home/20221020005120/en/70-Of-CEOs-Say-Their-Network-Is-Slowing-Business-Growth-New-NTT-Study-Finds。新聞稿。

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

REV:BDES-7841.2025JUL31

CLOUDFLARE