Zero Trust 如何降低風險和提高技術效率

縮減開支 — 增加安全性

量化 Zero Trust 最佳做法的財務和安全性影響

降低網路風險

95% 使用包括內建 Zero Trust 原則的 SASE 架構，受攻擊面減少[1]

72% 的 IT 主管表示，其採用 Zero Trust 的首要理由就是「強化資料安全性」[2]

61% 的 IT/網路安全專業人員認為，「使用身分和風險狀態進行更強大的驗證」是一種優勢[3]

↓23% 相較於未部署 Zero Trust 的阻止，已部署的組織的平均資料外洩成本下降[4]

驅動因素

- 針對每一項要求實施以身分和相關內容為基礎的控制，減少過度信任
- 增強了所有使用者、應用程式和裝置的可見度，並加快補救速度
- 減少了威脅的橫向移動

提高技術效率

700 萬美元 在五個組織中採用 Zero Trust，傳統網路安全的平均開支降低[5]

20 美元/FTE 使用以雲端為基礎的 Zero Trust 平台取代備援網路安全服務，每個月可節省的成本[5]

↓80% 佈建和保護新基礎架構所需的工作量減少[5]

39% 的組織所使用的網路安全技術已過時，可透過 Zero Trust 實現現代化[6]

網路安全複雜性的主要後果[7]

#1 成功的資料外洩或網路攻擊會造成財務損失

#2 無法在市場機會允許的情況下盡快創新

#3 缺乏營運彈性

驅動因素

- 透過將傳統單點解決方案整合至單一雲端平台，降低了複雜性
- 簡化了網路安全工作流程，無需透過內部部署設備回傳流量
- 在混合工作團隊中實施一致的原則

Zero Trust 對您的組織而言是一種策略性思維轉變

傳統 IT 網路安全：邊界決定信任		ZeroTrust：沒有邊界，始終驗證
保護邊界，在網路內安全無虞（即「城堡加護城河」）	保護	承擔風險，降低影響（加密、檢查、微分段）
在邊界僅記錄登入資料	可見度	隨時隨地記錄每次登入和要求
預設允許，依據網路位置的靜態存取	控制	預設拒絕，依據身分和上下文的最小權限

開始使用 Zero Trust 降低網路風險

要求諮詢

還沒準備好進行諮詢嗎？

- 探索 Zero Trust 如何提高團隊生產力：**閱讀簡介**
- 進一步瞭解同儕組織如何處理混合式工作：**閱讀簡介**
- 探索與廠商無關的藍圖以實現 Zero Trust：**閱讀白皮書**

1. 基於 Cloudflare 客戶體驗
2. 「Capterra 的 2022 年 Zero Trust 問卷」，2022 年 8 月（連結）
3. 「有關雲端 Zero Trust 安全性的全球研究」，Ponemon Institute LLC，2022 年 7 月（連結）
4. 「資料外洩成本報告」，IBM，2022 年（連結）
5. 「Microsoft Zero Trust 解決方案的總體經濟影響™」，Forrester Research，2021 年 12 月（連結）
6. 「網路安全成果研究」，Cisco，2021 年 12 月（連結）
7. 「2022 年全球數位信任深入解析」，PWC，2022 年 9 月（連結）