

# 十大生產力提升

96% 的網路安全主管表示，制定 Zero Trust 策略是其當務之急。<sup>1</sup>  
瞭解 Zero Trust 如何為組織提供價值。

## Zero Trust 釋放整個組織的生產力

### 對於 IT 和網路安全管理員

65%

的 IT 決策者和網路安全專業人員表示，Zero Trust 提升了 IT 網路安全團隊的生產力。<sup>2</sup>

↓ 80%

相較於 VPN 存取，使用 Zero Trust 解決遠端工作 IT 工單所花費的時間減少<sup>3</sup>

↑ 50%

在實作 Zero Trust 的五個範例組織中，網路安全團隊的平均營運效率提升<sup>4</sup>

35%

報告增強式 SecOps 的可能性有所增加（在成熟實作 Zero Trust/SASE 的組織中）<sup>6</sup>

↓ 29%

相較於傳統架構，使用 Zero Trust 平台對解決方案複雜性及整合點數減少<sup>7</sup>

### 生產力 驅動因素

- 精細化控制，無需額外開支
- 簡化了初始部署、持續原則管理以及使用者和應用程式中的擴展
- 透過將點服務整合到單一 Zero Trust 雲端平台上，降低了複雜性
- 減少了使用傳統系統修正問題和修復弱點所花費的時間

### 對於終端使用者

53%

的 IT 決策者和網路安全專業人員表示，Zero Trust 提升了使用者體驗<sup>2</sup>

↑ 60%

相較於透過 VPN 存取應用程式，佈建 Zero Trust 對新員工入職上線的時間提速<sup>3</sup>

85%

的 IT 主管一致認為，改進員工體驗可提高收入<sup>5</sup>

3天

透過為前線工作者提供安全的 BYOD 和對重要資源的 Zero Trust 存取，每年可節省的時間<sup>4</sup>

65%

的員工認為，如若他們可以使用更好的技術，工作效率就會更高<sup>8</sup>

### 生產力 驅動因素

- 網路安全檢查更透明且干擾更少
- 員工、承包商、供應商和協力廠商上線/離線速度加快
- 簡化了驗證工作流程，無需透過內部部署設備回傳流量
- 減少了因連線、存取或網路安全原則相關問題造成的閒置時間

## 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	在任何位置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 釋放團隊生產力

請求諮詢

### 還沒準備好進行諮詢嗎？

- 探索 Zero Trust 如何降低風險並提高技術效率：[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. 「Microsoft Zero Trust 採用報告」，2021 年 7 月 [\(連結\)](#)
2. 「有關雲端 Zero Trust 安全性的全球研究」，Ponemon Institute LLC，2022 年 7 月 [\(連結\)](#)
3. Cloudflare 案例研究 [\(連結\)](#)
4. 「Microsoft Zero Trust 解決方案的總體經濟影響™」，Forrester Research，2021 年 12 月 [\(連結\)](#)
5. Amy Loomis 和 Alan Webber，「透過將客戶體驗和員工體驗聯繫起來，實現底線價值」，IDC Research，2022 年 1 月 [\(連結\)](#)
6. 「網路安全成果研究」Cisco，2021 年 12 月 [\(連結\)](#)
7. 「實現網路安全價值」，Palo Alto Networks，2022 年 9 月，[\(連結\)](#)
8. 「改進數位員工體驗的需求：技術如何提高員工留存率和生產力」，Ivanti，2022 年 [\(連結\)](#)