aruba
a Hewlett Packard Enterprise company

彌補 IT 安全缺口：

2023 年零信任與 SASE 安全性架構的發展狀況

隨著混合式辦公風潮日益盛行、物聯網的使用越來越多，加上網路攻擊威脅無休無止，都讓企業面臨著前所未有的資安挑戰。新的挑戰正促使企業採用新的安全模式。零信任和 SASE (安全存取服務邊緣) 架構可以兌現以下承諾：

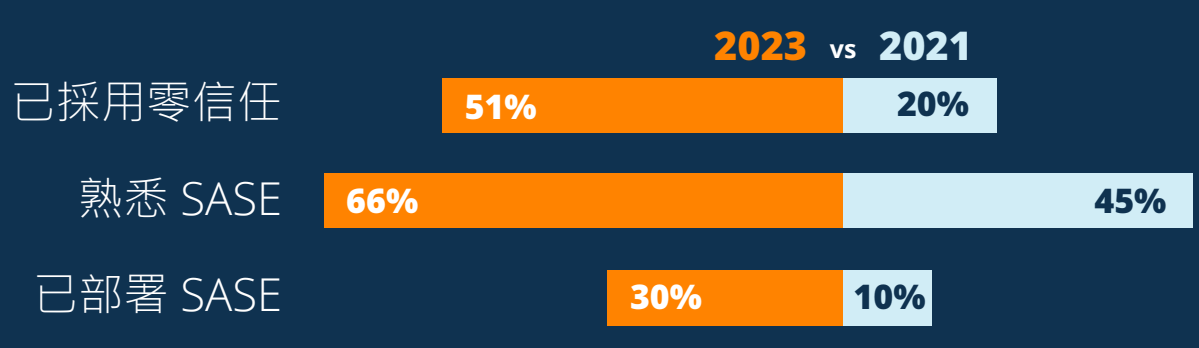
建構從邊緣到雲端的安全性

藉由動態強制執行最低權限原則來管理資源的存取權限，降低網路風險

隨時隨地提供對任意企業應用程式的安全存取

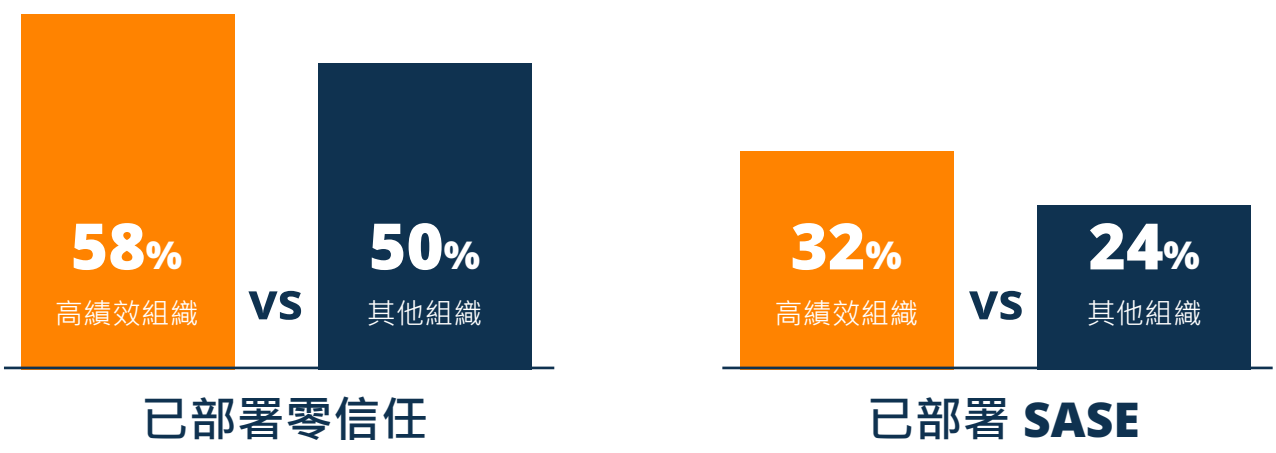
安全性架構正在發生怎樣的變化？

過去兩年，零信任和 SASE 安全性架構的採用速度不斷加快。您是否走在前端呢？



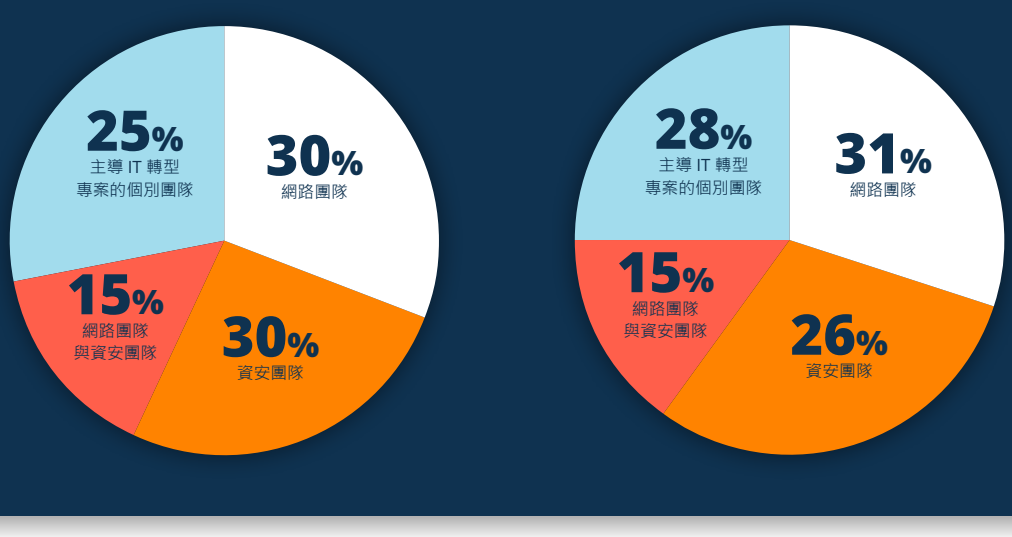
高績效組織的做法有何過人之處？

高績效組織更有可能部署零信任和 SASE 架構。



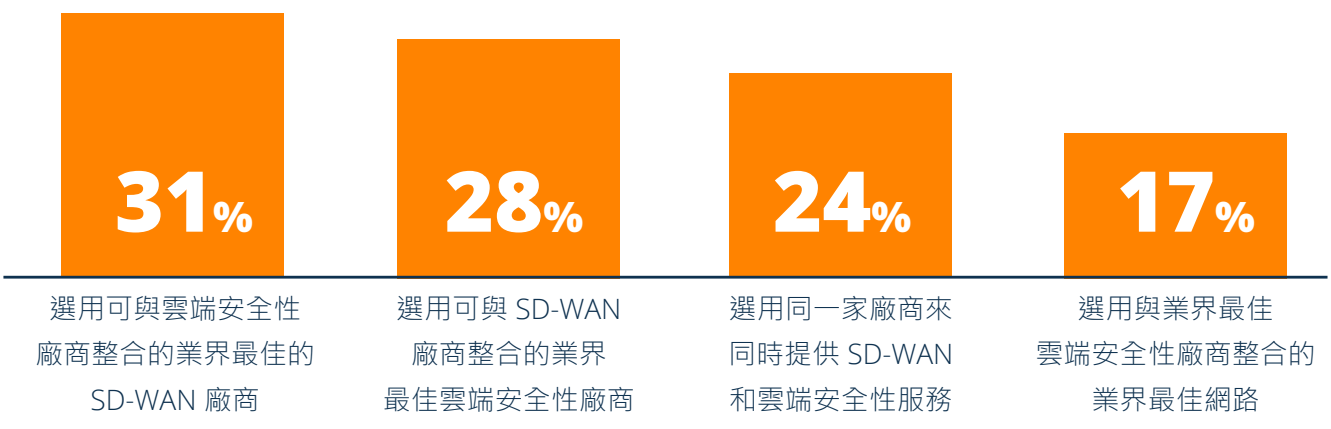
誰負責安全性架構的決策事宜？

在許多組織中，網路團隊會主導安全決策事宜，但新的決策小組也正在興起中：主導 IT 轉型專案的個別專案團隊。



考慮實作新的安全性架構嗎？

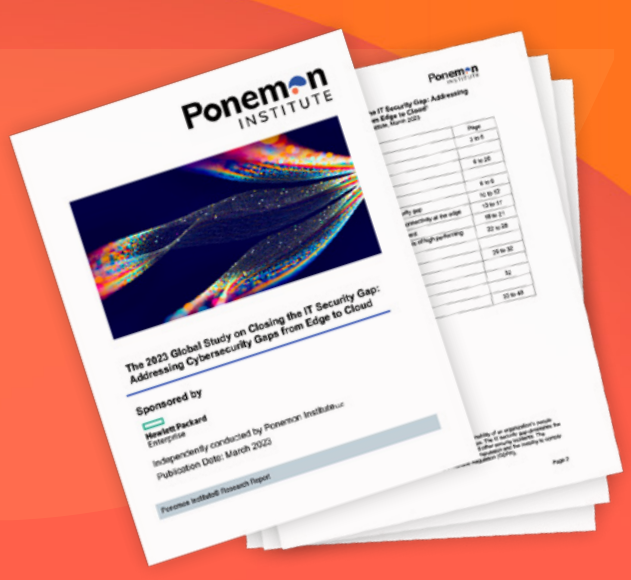
在提及部署 SASE 架構時，業界最佳 SD-WAN 和業界最佳雲端安全性的組合方案，以及單一廠商 SD-WAN 和雲端安全性方案，幾乎平分秋色，受到受訪者同等的青睞。



將進階的安全 SD-WAN 與業界最佳的 SSE (安全服務邊緣) 功能相結合，是將雲端型安全性服務整合到現有網路與安全性基礎架構的有效方式，而採用單一廠商方案則可能會提供更高的簡便性。

閱讀完整報告瞭解以下重點：

- 零信任和 **SASE** 解決方案的採用率和部署偏好情況
- 零信任和 **SASE** 在彌補 **IT** 安全缺口中所扮演的角色
- 可見性對於彌補 **IT** 安全缺口的重要性
- 相較於已部署高度有效網路安全性和實作的組織，您在零信任和 **SASE** 架構方面的進度如何



閱讀報告 →

aruba
a Hewlett Packard Enterprise company