aruba
a Hewlett Packard Enterprise company

釋放 **SASE** 的潛能：

從邊緣到雲端，提供全方位的安全網路

遠端工作使企業加速邁入雲端的腳步。
您對於提升網路效能與縮小安全漏洞有何規劃？
您的架構須做出哪些改變？

啟用 SASE 架構以整合安全性與網路，為貴公司提供更完善的防護

孤島式網路與安全性基礎架構已經無以為繼

嘗試遠端工作後，有 53% 的人想維持遠端工作型態

雲端、邊緣和 IoT 正在重新定義資料和應用程式的位置

越來越多企業應用程式存在雲端之中

使用者和裝置現已不受傳統企業邊界侷限

傳統的安全性與網路模式為何不管用了

各自為政的資安方案、網路孤島和以硬體為中心的侷限方法意味著：

- 複雜度更高，彈性與效率更低
- 恢復能力與災難復原受到阻礙
- 錯失良機，陷入落後競爭對手的逆境
- 難以符合雲端使用方式以及支援在家工作者的需求

為何您需要零信任邊緣方案

零信任邊緣解決方案能夠實現強大的身分驗證、身分識別和角色型存取控制，並跨資料中心、雲端和邊緣間做出適當的使用者和裝置區隔。

透過零信任、身分識別和角色型原則架構使 SASE 更臻完善，從邊緣到雲端都能確保使用者、裝置、應用程式和資料的安全。

Forrester 2021

零信任邊緣和 SASE 有何優勢？

- 將資安融入網路的 DNA 中
- 提供安全的企業服務與應用程式存取方式，保障遠端工作者的安全
- 優先處理支配分支 WAN 的企業應用程式流量
- 根據業務需求，確保使用者和 IoT 裝置的安全並做好區隔
- 協助企業防範客戶、員工、包商和裝置透過 WAN 光纖連上高風險環境所帶來的危機
- 針對零信任邊緣解決方案涵蓋的安全性與網路服務組合，可進行集中管理、監控與分析

您是否應開始零信任邊緣旅程？貴公司可以思考 3 個問題

1. 您的應用程式在雲端有多安全？
2. 是否難以確保邊緣裝置和使用者的安全？
3. 53% 的工作者維持遠端工作型態，您是否準備好因應之道？

為安全性與網路服務導入零信任邊緣模式：

安全存取服務邊緣 (SASE) 即為零信任邊緣

閱讀完整的 **Forrester** 報告以瞭解以下資訊：

- 孤島式網路、安全性基礎架構和營運為何正快速消失
- 何種類型的零信任邊緣方案適合貴公司
- 如何評估多廠商和單一廠商選擇

閱讀報告

aruba
a Hewlett Packard Enterprise company