競爭比較面面觀

專為現今中型企業所設計的 6 點式防護

領先業界的網路安全技術

現今的中型企業必須大方採納技術以獲得競爭優勢，這一點相當關鍵。可惜的是，能夠創造商機的同一種技術同樣也會開啟新的攻擊面向和漏洞，足以對企業帶來威脅。如果沒有適當的防護能力，網路就會成為攻擊入侵裝置、資料和其他層次的主要進入點。Aruba 深知安全才是優先要務。以下列出 Aruba 為了維持網路安全而設計的創新安全功能，不妨花點時間了解有何不同：

功能	Aruba	競爭優勢	其他供應商	弱點
全天候安全監控	是	Aruba 將專用雙頻AP作為感應器，可同時在兩個頻段支援全天候安全性掃描，提供有效監測並降低網路攻擊。	受限	其他雲端供應商大廠使用專用第三頻，按其設計限制，只能各花 50% 的時間掃描各頻段。第三頻通常為 1x1 MIMO，只能監測到一部份的威脅態勢，且需花更久時間辨識攻擊 (如果徹底執行)。
內嵌式政策執行防火牆 (PEF)	是	Aruba 的多層政策執行防火牆適用於無線連線用戶端及應用程式的安全性、流量轉送與網路效能政策，帶來安全的高通訊品質。	否	其他廠商缺乏內建政策執行防火牆。他們還需要取得專用的硬體、授權和支援。
內建網頁內容過濾功能	是	Aruba 提供訂閱型的網頁內容過濾功能，無需另行購買設備即可套用。	否	網頁內容過濾解決方案有賴硬體裝置，這類裝置需要另外付費才能取得。
內建無線入侵與惡意抵禦功能	是	Aruba 的內建無線入侵防護功能已完成大規模執行測試，可持續地快速辨識惡意裝置並降低威脅。	受限	標準無線入侵防護功能在辨識惡意裝置時速度緩慢，無法遏制威脅，而適用的無線入侵防護功能又需要額外硬體和授權。
支援 WPA3 與 Enhanced Open	是	Aruba 安全專家對於開發這些使用於 WPA3 和 Enhanced Open 的新型加密協定助益良多。因此，Aruba 成為第一家將相關產品出貨的廠商 (2018 年 11 月)。	極少	儘管標準已於 2018 年 10 月頒佈，卻少有廠商實施與取得 Wi-Fi 認證。
使用者/裝置可見度與政策執行	是	Aruba 獲獎肯定的 ClearPass 政策管理平台是業界最頂級的使用者與裝置驗證與授權、政策執行及漏洞回應解決方案。	否	儘管市場上也有其他進階安全平台，但這些平台的部署難度過高，需要額外授權及/或訂閱才能取得基本服務，且只能有限地提供多廠商支援。

想要進一步了解 Aruba 的中型企業解決方案嗎？請按這裡。

CL_6PointProtection_072419