解決方案概述

# 採用零信任安全的 Aruba ESP

## 為邊緣提供的安全功能

由於使用者變得越來越去中心化，且各種攻擊的精確程度與持續性越發增長，網路安全挑戰也逐年變得越發嚴峻。以防護網路邊界為主的傳統安全防護方式已不再是有效的獨立安全防護策略。現代網路安全防護必須因應不斷變化且多樣的使用者與裝置，以及更加普遍的、以過去網路基礎架構中「受信任」部分為目標的威脅。

零信任會從本質上將所有使用者、裝置、伺服器和網路區段視為不安全且可能帶有惡意，因此被認為是能更好地處理現代企業日新月異安全需求的有效模式。Aruba ESP 採用零信任安全，運用更嚴格安全最佳作法與控制項組合來處理以往受信任的網路資源，藉此改善整體網路安全態勢。


### ARUBA ESP：核心零信任原則

依考量的安全領域不同，零信任也會有很大的差異。儘管應用程式級控制已是零信任的重點，全面的策略也必須考量網路安全和不斷增加的連線裝置數量，包括居家環境工作。採用零信任安全的 Aruba ESP 結合了全方位掌控能力、最少存取微分割與控制項，以及持續監控及執行的功能。並確保相同的控制項套用至園區或分支機構網路，並延伸給在家或遠端工作者，藉此強化傳統的 VPN 解決方案。

在物聯網 (IoT) 時代，良好網路安全的基本原則往往難以實施。如有可能，所有裝置和使用者都應先識別身分並經過適當驗證，再授予網路存取權限。除了驗證之外，在使用者和裝置連上網路後，應只給予他們最少量的存取權限，讓他們能夠執行關鍵業務活動即可。這代表要授權哪些網路資源和應用程式可讓任何使用者或裝置存取。最後，所有使用者和應用程式間的通訊都應加密。

### 對全方位掌控能力的需求

隨著對物聯網 (IoT) 的運用不斷加深，全盤掌握網路上所有裝置和使用者的也變得越來越困難。缺乏掌控能力會導致難以套用支援零信任模式的關鍵安全控制項。自動化、以 AI 為基礎的機器學習和快速識別裝置類型的能力十分重要。

Aruba ClearPass Device Insight 使用主動與被動式探索和狀態剖析技術，藉此偵測並全盤掌握連線或嘗試連線至網路裝置的資訊。這包括筆記型電腦和平板電腦等一般使用者型裝置。Aruba ClearPass Device Insight 與傳統工具不同，能掌握現代網路中日漸普及，且種類越發多樣的物聯網 (IoT) 裝置資訊。

## 採用「最少存取權限」和微分割

具備掌控能力後，接下來的關鍵步驟是要採用與「最少存取權限」和微分割相關的零信任最佳作法。這代表盡可能為每個網路上的端點使用最佳驗證方式 (例如：對使用者裝置進行完整的 802.1X 和多因素驗證)，並採用相應存取控制政策，只授權存取該裝置或使用者絕對需要使用的資源。

Aruba ClearPass Policy Manager 可建立角色型存取政策，讓 IT 和安全團隊能透過單一角色與套用至網路上任意位置 (不論是有線或無線基礎架構、在分支機構或園區內) 的相關存取權限，讓這些最佳作法得以運作。完成剖析後，系統會自動為裝置指派合適的存取控制政策，並透過 Aruba 動態分割功能將其與其他裝置區隔開來。Aruba 的政策執行防火牆 (PEF) 是 Aruba 網路基礎架構中內嵌的完整應用程式防火牆，負責提供執行功能。Aruba 基礎架構也使用最安全的加密協定 (例如 WPA3 標準) 來加密無線網路連線。

ClearPass Policy Manager 也整合多種驗證解決方案，可使用多因素驗證，並在網路的各個關鍵點強制重新驗證。客戶也能透過 ClearPass 生態系統輕鬆整合其他解決方案，滿足與情境式資訊和其他安全遙測相關的零信任需求。

因此 ClearPass 能整合端點安全工具等多種解決方案，根據裝置態勢進行更智慧化的存取控制決策。存取控制政策也能根據使用的裝置類型、使用者連線的地點，以及其他情境式條件變更。

## 持續監控和執行

透過角色式存取控制執行精細分割後，下一個零信任最佳作法是持續監控網路上的使用者與裝置。這樣做可因應與內部威脅、進階惡意軟體或持續性威脅的風險，解決這些威脅能繞過傳統邊界防護的問題。

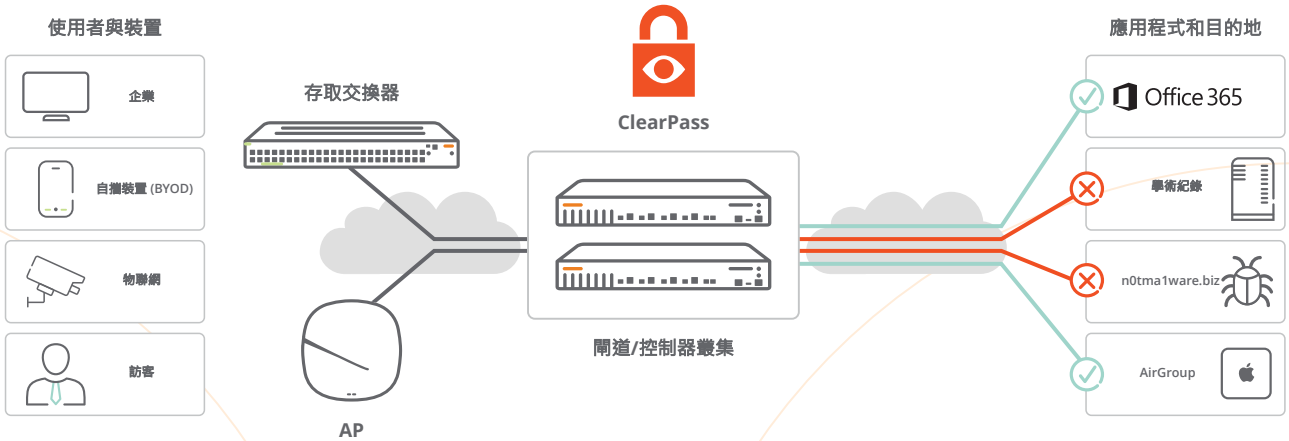


圖 1：Aruba ClearPass 自動指派透過動態分割執行的角色型存取控制政策


**圖 2：零信任安全是 Aruba ESP 的重要支柱**

### 利用 IDS/IPS 的威脅防禦

Aruba 威脅防禦功能可防禦大量威脅，包括釣魚攻擊、阻斷服務攻擊 (DoS)，以及越來越廣泛的勒索軟體攻擊。Aruba 9000 SD-WAN 閘道執行身分識別式入侵偵測和預防 (IDS/IPS)，並可配合 Aruba Central、ClearPass Policy Manager 和政策執行防火牆。身分識別式 DS/IPS 會根據簽名和模式，對分支辦公室 LAN (東-西) 和 SD-WAN (南-北) 流經閘道的流量執行流量檢測，藉此提供內嵌的分支機構網路安全性。Aruba Central 內的進階安全儀表板可為 IT 對提供掌握整個網路的能力、多種層面的威脅指標、威脅情報資料，以及建立關聯和事件管理功能。威脅事件會傳送至 SIEM 系統與 ClearPass 進行修復。

### 360 Security Exchange

ClearPass Policy Manager 整合了 150 多種最佳安全解決方案 (包括安全作業與回應 (SOAR) 工具組)，能根據來自多個來源的即時威脅遙測動態執行存取權限。使用者可根據新世代防火牆 (NGFWs)、安全資訊與事件管理 (SIEM) 工具和其他多種來源提供的警告，建立相應政策以做出即時存取控制決策。從限制存取權限 (例如：僅網際網路)，到徹底將裝置從網路中移除以進行修復，使用者可完全自行設定 ClearPass 行動。

## ARUBA EDGE SERVICES PLATFORM (ESP,邊緣服務平台)

為協助客戶充分運用邊緣的潛在機會，我們開發了業界第一個專為整合、自動化及保護邊緣設計的人工智慧平台：Aruba ESP。零信任安全是 Aruba ESP 的關鍵要素。結合 AIOps 和整合式基礎架構後，可讓組織降低成本、簡化作業並維護安全。

## 總結

現今的網路環境和威脅態勢需要使用不同的方式才能因應。過去以邊界為中心的網路安全功能並非為如今的行動工作者或日益增加的物聯網 (IoT) 裝置而設計。採用零信任安全的 Aruba ESP 提供全方位的功能組合，包括掌握情況、控制和執行的能力，藉此因應去中心化、物聯網 (IoT) 驅動網路基礎架構的需求。



SO_ZeroTrustSecurity_051120 a00097694enw