執行簡述

在邊緣辨識、連線及保護行動和 IOT 裝置

簡介

連線到企業網路的 IoT 裝置數量令人吃驚，對 IT 人員帶來了挑戰，他們必須權衡智慧建築的優點，並考慮大量未知裝置上線進入其環境、卻沒有正確一套工具來自動辨識、剖析、驗證及套用原則於這些裝置的風險。

Aruba 最新發表的產品利用 4 步驟方法，提供邊緣的 IoT 連線能力，讓上述挑戰都能迎刃而解。辨識網路上的一切、將行動與 IoT 裝置連線到智慧型交換器、利用業界領先的原則管理保護網路，以及透過我們的合作夥伴生態系統進行創新，以提供端對端的安全性。

IOT 帶來挑戰

行動裝置的爆發式增長與智慧建築的發展趨勢，給 IT 和企業領導者帶來了重大挑戰。

欠缺能見度 — 對於您網路上的一切，您真的都清楚明瞭嗎？

安全始於瞭解網路上的一切 — 也就是：未受管理的智慧型手機、惡意的端點、IoT 裝置。這些都會增加攻擊面，威脅企業安全。如果能看到網路上的一切，IT 就可以更清楚地瞭解公司網路的使用情況以及哪些人在使用。IT 必須能辨識並剖析每一個連線到網路的裝置，無論裝置從何處連線。隨著不明的無線與有線 IoT 裝置淹沒我們的網路，達成上述目標日趨艱難。所有的裝置在一連線時，都必須加以剖析和評估，接著指派到某個類別，並會根據裝置類型、擁有權狀態或作業系統自動授與或拒絕存取權。

有線成為新的隱憂。

對企業與工業領域中的組織來說，有線 IoT 裝置數量的預期成長率從 35% 到超過 50% 不等，實際取決於行業，如移動偵測器、醫療設備、工廠流程控制器等，在此僅列舉一二供參考。過去，對於網路存取控制 (NAC) 的討論，大多集中在如何確保無線網路安全，因為大部分的裝置都是這種連線方式。工作階段的安全連線成為需求，因為無線竊聽和不明的使用者可以透過存取點範圍內的任何位置和不安全的 SSID 建立存取。

對於確保無線網路安全的看重，意味著有線網路沒有得到保護，因為交換器裝設在上鎖的門後面，普遍就認為有線網路沒有無線網路的那些弱點。遺憾的是，隨著有線網路的成長，許多交換器之間的一致性受到衝擊，導致連接埠敞開，人人都能存取。會議室和印表機區域的連接埠就是存在安全性「非有即無」的典型例子。在許多 IoT 裝置透過有線進行連線之下，現在也應該同等看待有線基礎架構的安全。

傳統的有線基礎架構未針對 IoT 進行最佳化

在舊有的交換環境中，沒有行動工作者，IoT 還沒有闖出名堂 (沒有語帶雙關的意思！)。資產都位於防火牆的後方，IT 只需確認周圍保持穩固即可。如今，進入 IoT 世代，有線基礎架構必須與無線基礎架構一樣具備智慧，目前的交換器需要整合安全性和智慧型網路管理，如此一來，這些裝置才能安全且無縫地進行連線。

保護網路需要自動化工作流程

在每天有數千個不明的行動和 IoT 裝置連線到企業網路的情況下，要手動指派及實施考量到每個裝置的原則，無疑是緣木求魚。整個流程必須自動化，才能將 IT 手動作業降至最低，進而降低風險。靜態裝置與基礎架構本身也應該加以剖析並接受自動檢查，以找出可疑的變動。如果某個裝置行為可疑，在完成風險評估之前，都應該自動將它隔離。

始終搶先駭客一步，所費不貲

我們幾乎每天聽聞有大量資料外洩的事件發生。公司在安全性方面投入大量的金錢和時間，要自行單打獨鬥，以始終搶先駭客一步，幾乎難如登山。Aruba 的合作夥伴生態系統將業界最佳的安全合作夥伴匯集在一起，提供端對端的安全解決方案。

ARUBA 針對邊緣的安全 IOT 連線能力制定的藍圖

1. 辨識並剖析多廠商有線與無線網路上的不明裝置

如果說，網路安全性始於知道網路上的一切，那麼組織最重要的是具備辨識並剖析所有裝置的能力。Aruba 的 ClearPass 系列提供獨一無二的競爭優勢，因為他們可以獨立應用裝置的形式或透過全方位的原則實施解決方案獲得即時的無代理程式剖析功能。

無論網路是否啟用 AAA 功能，這兩種解決方案都可以讓您透過動態或靜態 IP 位址，持續辨識有線與無線網路上的端點和網路裝置。全方位的儀表板視覺化功能，讓查看端點總數，以及依類別、系列和裝置類型區分數目，變得輕而易舉。

全新的 Aruba ClearPass Universal Profiler 是獨立虛擬應用裝置，在幾分鐘內，即可完成部署並執行，專為尚未準備好導入完整 NAC 解決方案的組織而設計，也適用於尚未部署 NAC 的遠端區域或管制區域。Universal Profiler 提供簡單且具成本效益的方式，來辨識並剖析網路上的一切。

Aruba ClearPass Policy Manager 是虛擬或實體應用裝置，包括全方位的剖析、非 AAA 和 AAA 有線與無線原則實施、訪客存取、BYOD 上線啟用、端點評估功能、報告，以及內建協力廠商安全性與使用者體驗導向的解決方案整合功能。

2. 利用自動化的智慧連線 IoT 裝置

在智慧建築的潮流下，當今的企業需要更具智慧的有線基礎架構。ArubaOS-Switch 的最新增強功能可以為智慧型邊緣帶來力量與安全，進而針對行動和 IoT 裝置進行最佳化。這些增強功能透過能辨識及指派角色給已連線的 IoT 裝置，以排定業務關鍵應用程式的優先順序和保護網路，實現了跨無線與有線網路的統一角色型存取。

Aruba 第 3 層交換器也能夠根據使用者及連接埠，建立連接 Mobility Controller 的有線流量通道，如此一來，便可以套用原則、延伸進階服務，並且對流量加密來確保 LAN 安全。為了滿足分散式企業因應 IoT 與連網裝置快速成長的需求，具成本效益的 Aruba 2540 (還有其他 Aruba 交換器) 支援零接觸佈建和選購的雲端式管理，可讓企業簡化並大幅降低網路部署與管理成本。

3. 利用智慧型原則保護網路

只要您擁有裝置能見度，自動實施原則就能派上用場。Aruba ClearPass Policy Manager 可以協助您洞悉網路上的一切，然後跨多廠商有線與無線基礎架構，實施原則和自動化工作流程。ClearPass 提供剖析、原則實施、訪客存取、BYOD 上線啟用等功能，實現 IT 卸載、增強的威脅防護，及無縫的使用者體驗。在更加重視有線基礎架構的安全之下，OnConnect 功能使用現有的交換器通訊協定，協助您在諸如會議室、IP 電話和印表機區域等易受攻擊的地方，將有線連接埠關閉。

4. 加速創新來改善邊緣的安全性

Aruba 的技術生態系統包括領先業界的安全解決方案，這些解決方案整合了 ClearPass Exchange，能確保邊緣和核心位置獲得端對端的安全性。我們的合作夥伴對 IoT 安全性的最新重視：

- Niara 使用與裝置類型關聯的已知流量模式，辨識可疑行為，然後要求 ClearPass 從網路移除該裝置。
- 當有人嘗試使用假裝置攻擊網路時，Attivo 允許 IT 建立「假虛擬」的 IoT 裝置。一旦虛擬裝置被看出正在執行有害的行為，他們就會要求 ClearPass 將裝置拉出網路。

結論

隨著組織日漸擁抱 IoT 進入主流運作，IoT 裝置的上線啟用和管理成為成功的關鍵。公司需要策略來確保行動和 IoT 裝置在邊緣進行安全連線，以便在確保網路和公司資產安全無虞的同時，汲取與智慧建築相關的價值和效率。Aruba 的 4 步驟 IoT 連線方法，讓辨識網路上的一切、透過智慧型有線與無線基礎架構連線裝置、利用自動化原則管理保護網路，以及使用我們的合作夥伴生態系統大幅提升端對端安全性以始終搶先潛在風險一步等所有挑戰，全都迎刃而解。

a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | 電話：1.408.227.4500 | 傳真：1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com