# 確保物聯網正常運作

## 盡在 VMware Edge Network Intelligence

VMware Edge Network Intelligence 隸屬於廣大的 VMware Secure Access Service Edge (SASE) 產品組合，可協助企業：

- 透過提供以每部裝置為基礎的作業保證，以簡化管理物聯網裝置管理的作業複雜性
- 因應與使用物聯網裝置相關的複雜網路安全挑戰

邁向邊緣運算的趨勢和數量不斷激增的物聯網 (IoT) 裝置，始終為數位化轉型經濟的重要課題。鑑於物聯網具備降低成本、提高效率，以及進一步提供日常作業能見度的潛力，各行各業皆前仆後繼地推動相關使用情境。根據預測，在 2027 年，全球物聯網連線數量可望自 2022 年的 146 億攀升至 300 億以上[1]。在採用物聯網裝置方面，企業和 IT 領導階層面臨著兩大重要考量：作業複雜性和網路安全威脅。

### 物聯網裝置大舉提高複雜性

導入物聯網裝置，會提高 IT 和網路團隊的作業複雜性。手動上線新的物聯網裝置並追蹤其效能，不僅曠日廢時、耗費人力，更難以大規模作業。由於這些裝置往往極為重要 (例如醫院病床旁的監視器、零售門市內的保全攝影機)，勢必需要確保其持續作業且安全無虞。但在一些企業中，功能團隊和 IT 作業團隊並未擬定明確的架構，用以規範哪個團隊為裝置的所有者，並負責維護其作業狀態。

### 保護物聯網裝置為一大挑戰

在企業環境中新增物聯網裝置，會帶來重大的網路安全挑戰，包括：

- **暴露在重大弱點之下：**鑑於裝置類型和製造商琳瑯滿目，加上威脅態勢持續進化，物聯網裝置有可能帶來風險。此外，如果裝置製造商並未設有足夠的內建裝置安全功能，或裝置未經適當強化和修補，企業就有可能暴露在重大弱點之下，並容易遭受潛在的網路攻擊。

[1]《Ericsson 公司行動化報告 - 2022 年 6 月》(Ericsson Mobility Report – June 2022)

- **能見度不良：**隨著物聯網裝置數量不斷增加，手動進行管理和監控的難度也隨之提高。缺乏裝置作業狀態和行為 (例如裝置正在與哪些外部主機互動，及這些主機的數量) 的能見度，可能會直接影響生產力，並帶來新風險。
- **缺乏足夠的風險隔離機制：**由於環境內的物聯網裝置種類繁多，將裝置予以分類、評估其風險，並將其置放在適當的網路區段中，因而成為必要之舉。舉例來說，存取企業應用程式的終端使用者流量，應與位於企業作業中心的物聯網裝置流量進行邏輯隔離。缺乏足夠的網路分段，攻擊者就有機會輕鬆橫向移動，藉此破壞整體網路。

## VMware Edge Network Intelligence 簡介

VMware SASE™ 可協助 IT 團隊解決在分散式環境中進行作業，以及管理物聯網裝置作業的各項挑戰。VMware Edge Network Intelligence™ 為 VMware SASE 中不受限於廠商的 AIOps 解決方案，可透過確保裝置效能、安全性和自我修復的方式，著手推展物聯網裝置作業。


圖 1：VMware Edge Network Intelligence 可提供涵蓋物聯網生命週期的洞悉

VMware Edge Network Intelligence 能為企業帶來以下優勢：

### 物聯網裝置監視清單管理

免除終端使用者的物聯網裝置探索、分類和追蹤責任，好讓他們能著重進行業務作業。VMware Edge Network Intelligence 是一款無代理程式解決方案，可運用以機器學習 (ML) 為基礎的階層式裝置分類系統，並使用每個所偵測裝置詳盡的行為特徵，以自動為其建立監視清單，並將其劃分為裝置群組。

## 深入瞭解

- VMware Edge Network Intelligence：sase.vmware.com/products/edge-network-intelligence
- VMware SASE：sase.vmware.com

### 確保重要裝置正常運作

協助企業使用者順暢進行重要的裝置作業，讓他們無需診斷和疑難排解裝置問題。VMware Edge Network Intelligence 可讓使用者指定哪個物聯網裝置群組具有重要性，並針對其裝置作業提供深入的能見度。VMware Edge Network Intelligence 會建立效能基線，以及在效能與基線產生偏差時，向 IT 作業團隊即時發出警示，藉此達到上述目的。此外，這款解決方案也會使用企業內的相似裝置和相同產業內的同屬性項目，為裝置效能和行為建立基準。

### 物聯網安全性

協助 IT 作業和資安團隊管理環境內的物聯網裝置安全性需求。VMware Edge Network Intelligence 可監控群組和個人層級的裝置行為，並擷取各項資訊，例如網路中的裝置地點、進行通訊的內部和外部主機數量，以及通訊所使用的通訊協定類型。系統會根據與可疑 URL、未經授權的 IP 位址和高風險連線的互動，產生整體威脅設定檔。設定檔可與群組中的裝置進行比較，也能與不同用戶端環境中的類似裝置加以比較。

VMware Edge Network Intelligence 會掃描您的物聯網環境，以便與最新的威脅情報資料庫加以比對；該資料庫涵蓋超過 3,000 億個全球資料點，可即時偵測威脅，並盡可能減輕其所帶來的風險。這款解決方案也負責在多個垂直產業生產環境中，監控所部署的逾 3,000 萬部物聯網裝置。

## 為何應採用 VMware Edge Network Intelligence？

如果您正考慮為所屬 IT 環境進行物聯網裝置上線作業，或早已採用一系列的物聯網產品組合，VMware Edge Network Intelligence 可提供一站式服務，以管理您的所有作業和網路安全需求。VMware Edge Network Intelligence 能自動偵測、分類和監控裝置的效能及行為偏差，藉此協助您掌控自身的物聯網商業網路，並掌握其能見度。



文件編號：SDWAN-1025-Assure-IoT-Ops-ENI-so-0922