Claroty Edge

快速簡單的解決方案，可在短時間內提供擴展物聯網（XIoT）的可視性

XIoT 的安全挑戰

有效的工業網路安全，需要管理企業整體工業環境中的營運技術 (OT)、物聯網 (IoT)，以及受 IT 管理與未受管理的資產。不過，基於許多原因，要獲得這種程度的可見性並不容易，包括：

- 標準的 IT 解決方案和掃描方法通常與工業網路不相容且不安全
- 傳統的工業資產清點解決方案需要的硬體通常成本高昂、功能複雜且部署耗時
- 許多工業網路分散在不同地方及或被實體隔離，因此很難透過網路收集資產內容
- 傳統的工業資產清點方法，例如被動式的數據收集和離線檔案解析，可能並非適用於所有網路和使用案例的所有情況，也可能不兼容或不適合

解決方案

Claroty Edge是一款非常彈性的在Windows電腦上直接運作的資料收集工具，短時間內即可提供工業網路的完整可見性，不需要改變網路架構，或在較低網路層使用任何實體設備。

這個快速簡便的解決方案可以部署在本地或整合到SaaS方案，用以揭示有關管理和未管理工業資產的深入詳細資訊，否則只能用其他不一定適用於所有情況下的網路和使用案例的方法來清點。

Edge 優勢總覽

完整可視性

Claroty Edge 可完全清點受管理和未受管理的 XIoT 資產，以及會對其造成影響的所有風險和弱點

零變更且無硬體需求

Claroty Edge 會安全地利用現有的架構，無須在較低網路層部署硬體

數分鐘即完成，不必等待數天

不到 10 分鐘內就能完成 Claroty Edge 部署，提供工業網路的完全可見性

非常彈性的部署

Claroty Edge的靈活的雲端和本地部署選項，解決方案完全適用於內部網路環境、實體隔離和雲端式網路。

主要功能及使用案例

XIoT 資產探索

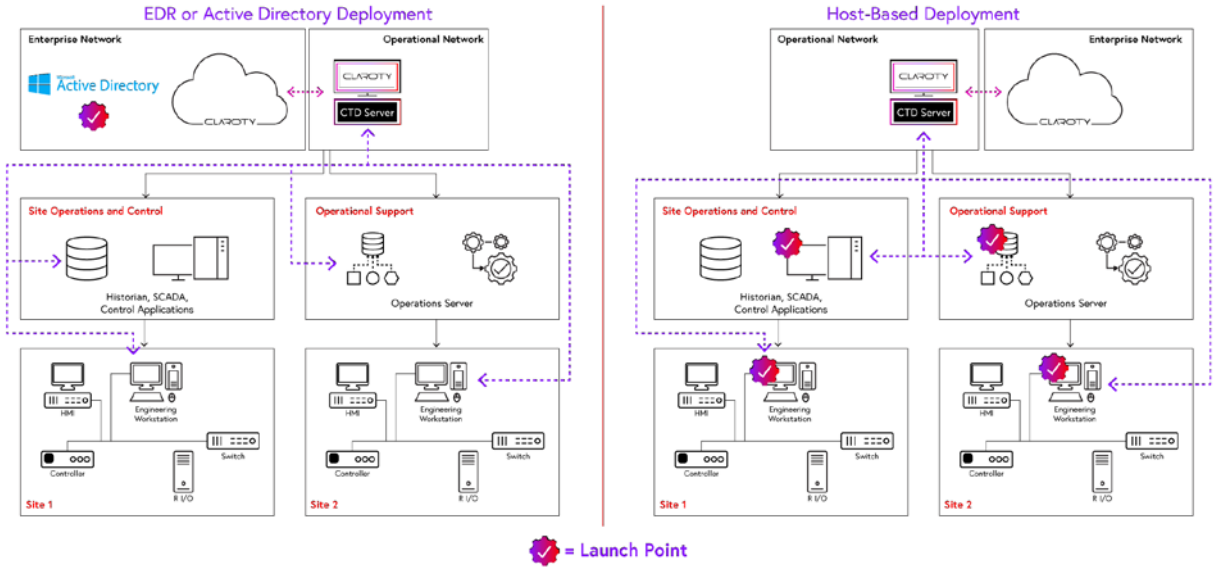
- 讓您幾乎即時完全掌握所有 OT、IoT 和 IT 的受管理和未管理資產
- 高度可視性可實現有效的工業網路安全，並是支援多種相關使用案例的強大基礎

風險與弱點管理

- 輕鬆辨識及管理會影響受管理和未管理資產的風險與弱點，例如缺少重大修補程式、資產停止支援(EoL)以及相關的CVE清單等等
- 這些功能可減少工業網路所面臨的風險，讓您能夠更妥善地保護工業網路

其他使用案例包括：

- **稽核與合規性：**輕鬆、快速且有效支援工業網路的稽核和合規性報告要求，讓您對報告更有信心、降低稽核失敗的風險，以及強化合規性和整體安全狀態。
- **併購盡職調查（M&A）：**以更輕鬆、快速和有效的方式，對目標公司的工業網路進行併購盡職調查，快速完成併購需求並獲得營運風險狀態的明確見解，並遵循 LOI 的規範。
- **事件回應：**立即幫助回應負責人完整清點遭到入侵的環境和風險弱點評估，以便最佳化事件回應工作，包括對工業網路的影響評估、範圍界定和鑑識。



關於 Claroty

Claroty讓工業、醫療保健及商業組織能夠保護其環境中的所有網路實體系統：擴展物聯網(XIoT)。公司的整合平台可以將客戶現有的基礎結構整合，提供可見性、風險和弱點管理、威脅偵測，以及安全遠端存取的全方位控制。

Claroty 獲得全球最大的投資公司和工業自動化供應商支援，目前部署在全球數百家企業的數千個站台。公司總部位於紐約，業務遍及歐洲、亞太地區和拉丁美洲。

智慧資安科技股份有限公司

服務專線　04-24523928 分機 300、301、302

電子信箱　servicedesk@unixecure.com.tw

台北據點　114 台北市內湖區基湖路 35 巷 13 號 8 樓

官方網站　facebook