Security Service – Workshop

自由系統資安解決方案—OT資安健檢服務

IoT/OT Security PoC

FREEDOM SYSTEMS

Freedom Systems Inc.

為何企業應該及早啟動 IoT/OT Security 前瞻計畫？

資安攻擊升溫

COVID-19以來，全球針對企業—尤其是製造業—*遭駭客鎖定進行目標式勒索與DDoS攻擊*的災情頻傳。

政令法規改革

美國總統拜登簽署改善網路安全的行政命令(NIST 800-207)，*督促企業提出資安能力證明*；台灣金管會也明訂上市櫃公司於2022~2023年完成設立資安長與資安專責單位。

智慧工廠趨勢

工業4.0時代來臨，工控場域導入愈來愈多物聯網與自動化設備，意味著以後企業IT和OT將逐漸匯流，資訊安全問題將橫跨IT/OT領域並需要統一管理。

工控領域之資安威脅影響擴大

機敏資訊
遭到不當洩漏

- **沙烏地阿拉伯國家石油公司(Saudi Aramco)**遭駭客攻擊資料大量外洩，內含該公司1.4萬名員工資訊、各個系統的專案規格、內部分析報告/合約/價目表、以及客戶名單與合約。
- **台灣電腦品牌大廠**被REvil病毒團體勒索要求5000萬美元（約新台幣14億元）贖金，遭竊資料包含其財務表格、銀行結餘、銀行通訊文檔。

營運中斷
因資安事件停擺

- **Garmin** 遭駭客攻擊產線停工 2 天，用戶的 App 出現無法更新的狀況。傳言支付了 1,000 萬美元（約新台幣 2.9 億元）的「贖金」才解鎖攻擊。
- **日本光學製造商HOYA**遭到網路攻擊，使得該公司泰國工廠的部分生產線關閉，公司約有100臺電腦感染密貨幣挖礦的惡意軟體，並會竊取公司使用者帳密。

民生安全
裝置惡意竄改

- **美國佛羅里達州奧爾德斯瑪市的淨水廠設施**，遭到駭客惡意入侵系統，將水中的氫氧化鈉濃度從百萬分之100調高111倍，差點對成千上萬的奧爾茲瑪居民造成嚴重影響。
- **醫療設備商GE Healthcare**旗下放射裝置出現資安漏洞，允許駭客遠端關閉裝置、警報、變更設定，可能會使護理人員錯過病患監護裝置的重要警報，甚至竊取患者數據。

IoT/OT面臨的資安挑戰

- IoT/OT資安危機可能導致：

機敏資料外洩、
數據回傳異常

設備與生產線停擺

感染惡意程式
成為殭屍網路

人員或環境安危

- 傳統OT裝置的資安隱患：

不支援Agent-based Solution
例如一般EDR產品

可視性(Visibility)相當有限

採用專有通訊協定，
一般IT資安設備難以正常識別流量

大量的IoT/OT裝置
大幅增加攻擊面(attack surface)

「可視性 (Visibility)」是打造IoT安全防護的首要關鍵

透過部署 Microsoft Defender for IoT，企業能夠強化對IOT環境的掌控能力抓出潛在威脅

1

掌握整體環境

掌握整體環境Device Inventory – 區分一般端點(Endpoint)、工控設備(OT)、IoT裝置(IoT)

2

找出弱點與漏洞

工控環境設備或IoT裝置弱點漏洞檢測，並提供建議的安全性改善措施

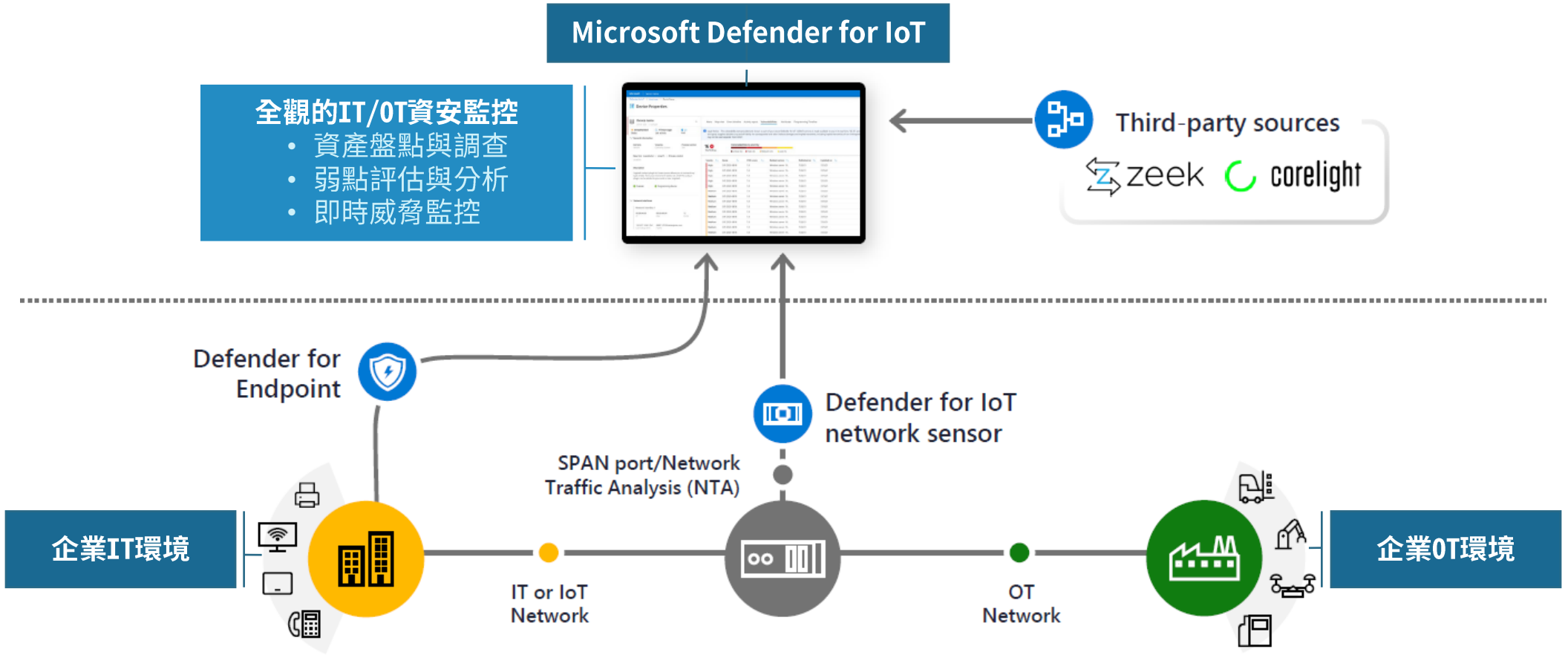
3

抓出威脅、預判風險

過往IoT與ICS威脅，就隱藏在工業網通的暗處。
將ATT&CK for ICS架構完整包覆，不只抓出現存威脅，更預測未來潛在風險。

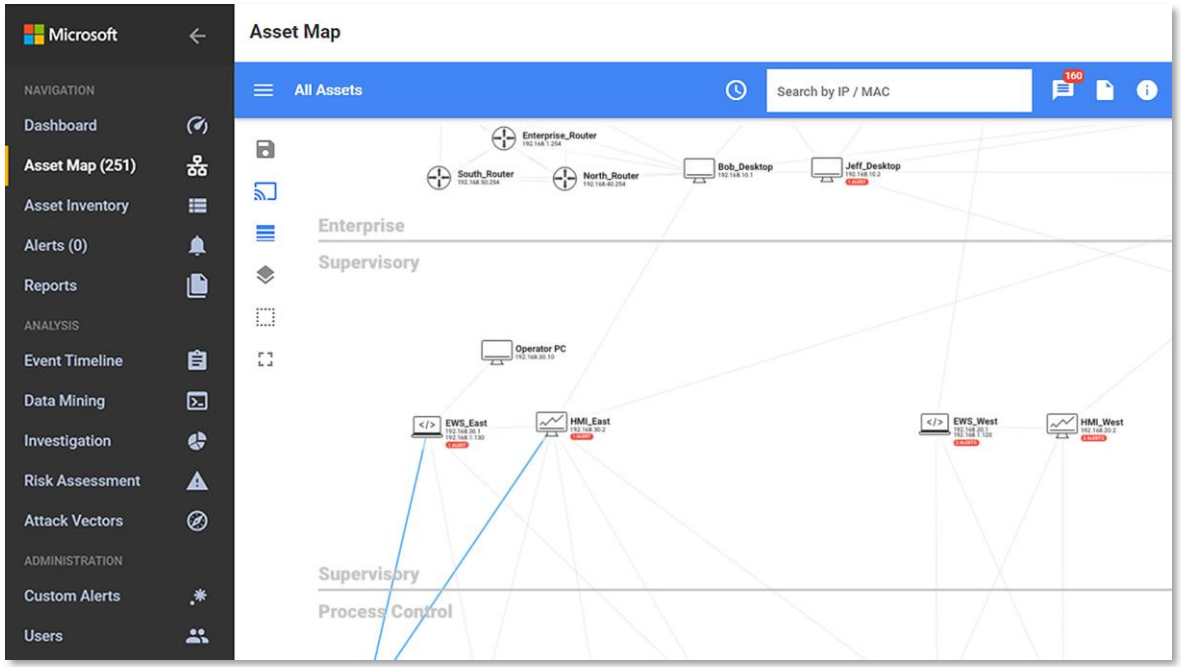
» 查看更多 Defender for IoT 產品說明

串聯所有端點，就地部署 Microsoft Defender for IoT



» 查看更多 Defender for IoT 產品說明

監視和偵測受控與非受控 IoT 資產的安全性威脅！



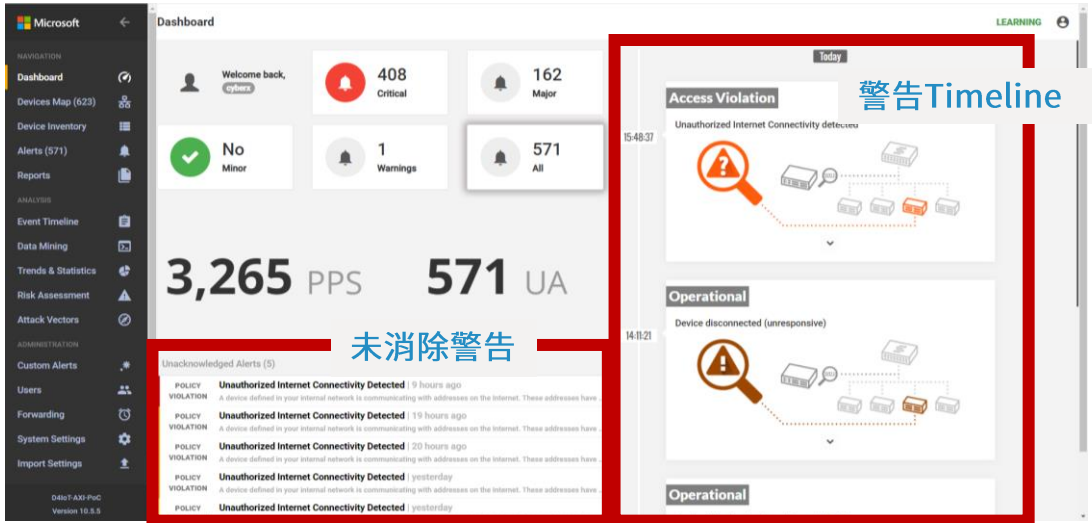
完整了解整體 IoT/OT 環境的資產和風險

使用 IoT/OT 感知行為分析和威脅情報
持續監視威脅和弱點

與 Microsoft SIEM 和 XDR 的互通性，使用
自動化、跨網域安全性和內建 AI 來阻止攻擊

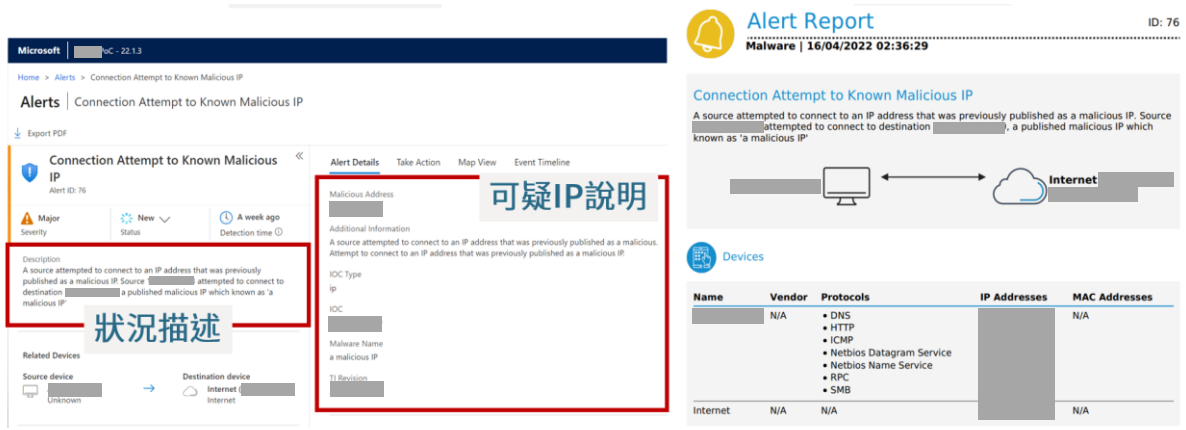
彈性的部署選項，包括內部部署、
Azure 連線或混合式

Quick View: Defender for IoT 重點功能

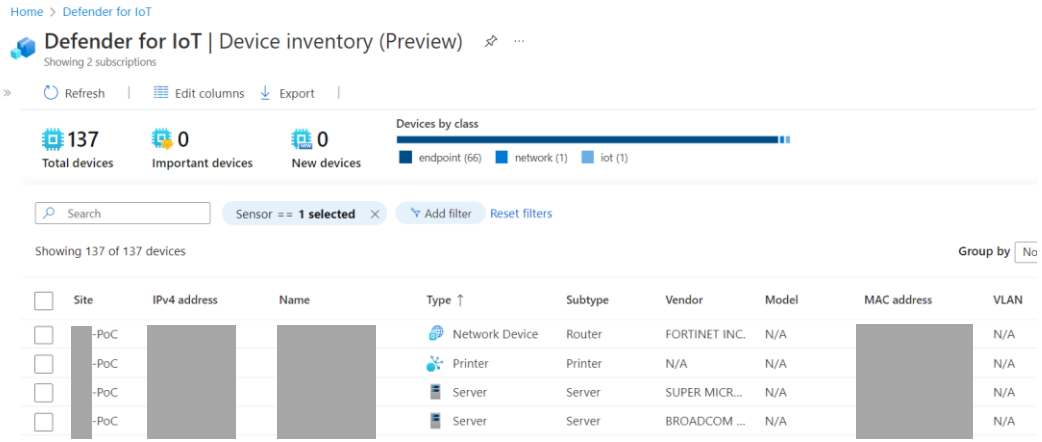


- Dashboard

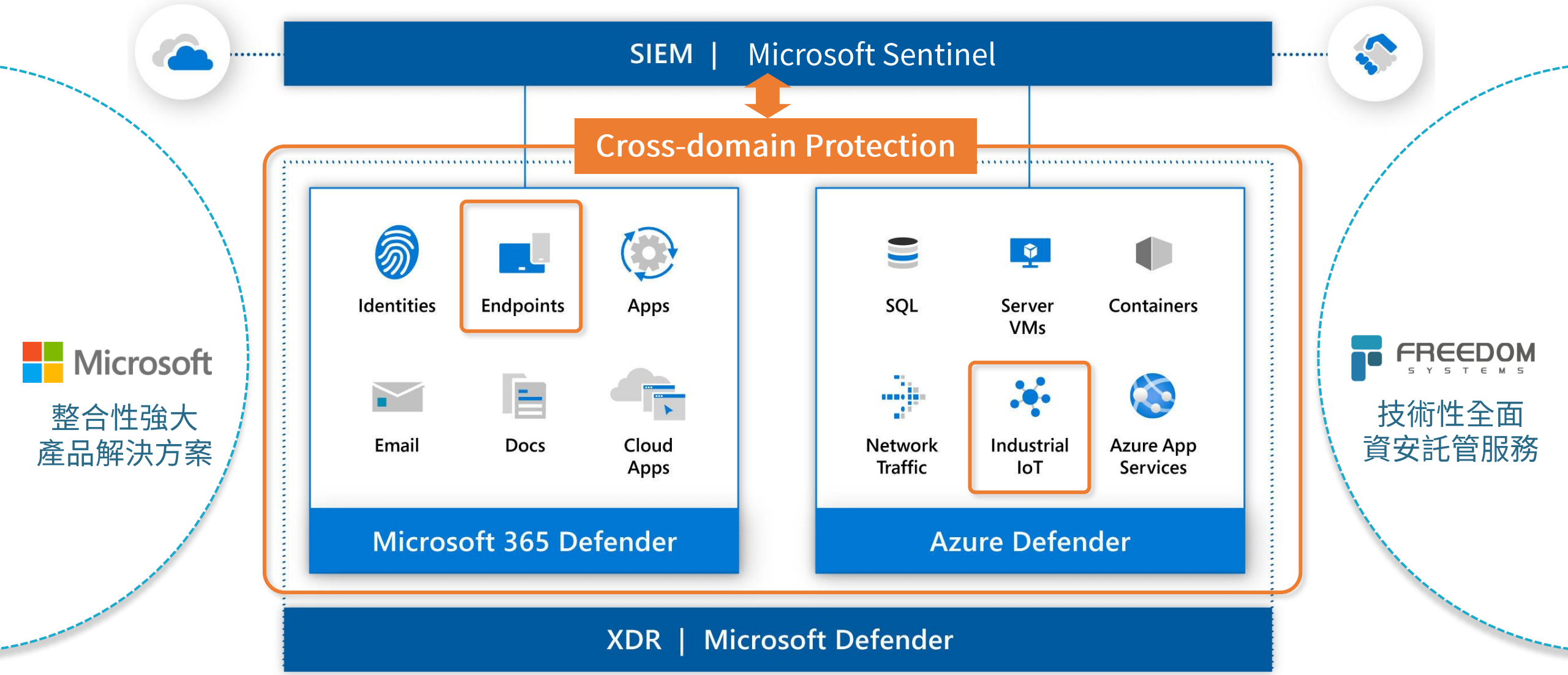
- Device Map



- Sensor Alert Details



- Device Inventory



Microsoft

整合性強大
產品解決方案

FREEDOM SYSTEMS

技術性全面
資安託管服務

自由系統 IoT 資訊安全健檢服務：4-week workshop

1 場域環境評估與訪查

- 確認場域網路架構、設備數量規模、比對通訊協定等基礎架構
- 組織管理、需求確認等問題訪談

3 網路流量異常監控及偵測

- 檢查安裝後的各Port網路流量以及狀態，劃分裝備級別
- 檢查警示(Alert)資訊並輔助統學習

Week 1 — Week 2 — Week 3 — Week 4

2 Microsoft Defender for IoT 機器部署

- 根據欲部署範圍規劃架構並配置授權
- 後臺啟用 Defender for IoT 並完成設備初始設定、防火牆規則設定

4 服務結果報告與安全性建議

- 檢視裝置安全分數、攻擊向量、網路運作問題、高風險裝置及漏洞(CVE)等結果報告

※總體服務所需時間為粗略估計，可能視組織產業、規模與個案情況而有調整。

自由系統資安與技術資格認證

自由系統已取得 Microsoft大中華區資安(E5)最佳合作夥伴、2021台灣微軟最佳合作夥伴，以及Microsoft Advanced Specialization – Identity and Access Management、Threat Protection等進階專長認證，並擁有各大資訊廠商的合作資格。

(ISC)²®

CISSP® Certified Information Systems Security Professional

CISSP®認證被譽為資訊安全界的最高標準，偏重資安管理概念，主要訴求對象是中高階資安主管，例如CSO(安全長)、CISO(資安官)，或者是資安顧問等

SSCP® Systems Security Certified Practitioner

SSCP®認證是針對具有資訊安全技術能力且具實務經驗者而設，此證照以公正客觀的標準，界定了企業組織中實際負責運作及落實資安政策相關從業人員的實務工作範圍、角色與職務

CCSP™ Certified Cloud Security Professional

CCSP®認證是二大安全組織-(ISC)2及CSA(雲端安全聯盟)兩大國際原廠聯手打造的頂級雲端資安認證。透過此認證，主要用於表彰其持有者於資訊及雲端安全的專業與能力，藉此以協助組織維持重要雲端基礎設施的正常運作、免於危害

Microsoft Partner
Microsoft
Gold Security
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices
Gold Small and Midmarket Cloud Solutions

Winner Microsoft Partner
2021 Partner of the Year
Taiwan
Microsoft

Hewlett Packard Enterprise Business Partner
Business Partner

cisco Select Partner

vmware PARTNER
PROFESSIONAL SOLUTION PROVIDER

veeam GOLD pro partner

DELL PartnerDirect Preferred

Adobe Certified Reseller

Symantec. Specialist Partner
Small and Midsize Business Segment

FireEye Product Specialist

自由系統的獨到之處與服務效益

即時且高效率地調查、遏制並修補重大資安事件

危機管理與即時應變

事件發生當下，沒有應對經驗的企業容易無所適從。您需要具有豐富處理經驗的團隊進場協助、主導陣營，能就事件相關的溝通事宜給予建議，包含與主管溝通、與IT及其他廠商協作。

蒐集調查威脅情報

若企業沒有資安團隊，往往當事件噴發時無法有效判讀威脅，也無從排除。專家就像解籤師，能透過工具比對數據紀錄、第三方資源等情報，進行有效率的調查、定義問題，找出攻擊的源頭。

以顧問式服務為本位

解決問題才是我們與客戶的共同目標。您不需要擔心廠商銷售不適用的產品，或是解決方案難以在組織落地。從問題洞察到技術維運全部交予一站式的服務，將資安管理納入企業永續經營方針。

專業判讀

判讀事件內容、定義緊急優先程度

即時處理

事件回應及應變處理

動態優化

環境結構調整、工具設定調整

自由系統資安服務客戶案例

Learn More→

研華在2020年底決定開始重新檢討既有資安管理，加強己身的資訊架構體質、降低被攻擊的風險，與縮短被攻擊後的反應時間。自由系統憑藉專業實力在眾多優秀Security Partners之中脫穎而出，成為研華的資安顧問，並分成三步驟確實進行資安健檢：1. 協助分析現況之風險，與現存之攻擊 2. 導入資訊安全工具，並提供資安維運服務3. 提出架構改善建議(AD、Email、Firewall)，並協助執行。

有察於地端server版本老舊，除了日常使用與維運問題，更擔心造成系統資安漏洞。自由系統的首要之務是協助艾訊評估比較升級地端server或上雲端的資訊成本、風險和生產效益，並規劃並執行地端email server移轉上雲端。除了Microsoft 365授權及導入，交給自由系統支援每月技術維運及教育訓練，更與微軟合作進行Security Workshop PoC，使用Microsoft Defender For Endpoint為艾訊降低端點資安風險。

台灣人壽為了因應大量資料處理，並有效從中發掘潛在資安事件，委託自由系統及微軟聯手抵禦資安潛在風險。導入Azure Sentinel後，藉由AI的高度學習及運算能力，以及視覺化的儀表板，將台灣人壽每日60十億位元組的資料，壓縮在半小時內檢視、回應及處理完成，協助內部資安人員更有效進行資源分配及利用。

為確保產業領先地位，瑞昱決心積極佈局資訊安全規劃，以降低經營風險及可能面臨的災損。自由系統透過佈署Microsoft Defender for Identity，優化企業內部的監控機制，若偵測到可疑的駭客橫向移動或攻擊行為，將可在第一時間示警並進行停權及環境檢查，搶在駭客發動更嚴重的攻擊前阻斷其動作。後期陸續使用Azure Security及Microsoft Defender來強化鞏固安全防護，也強化風險警示。

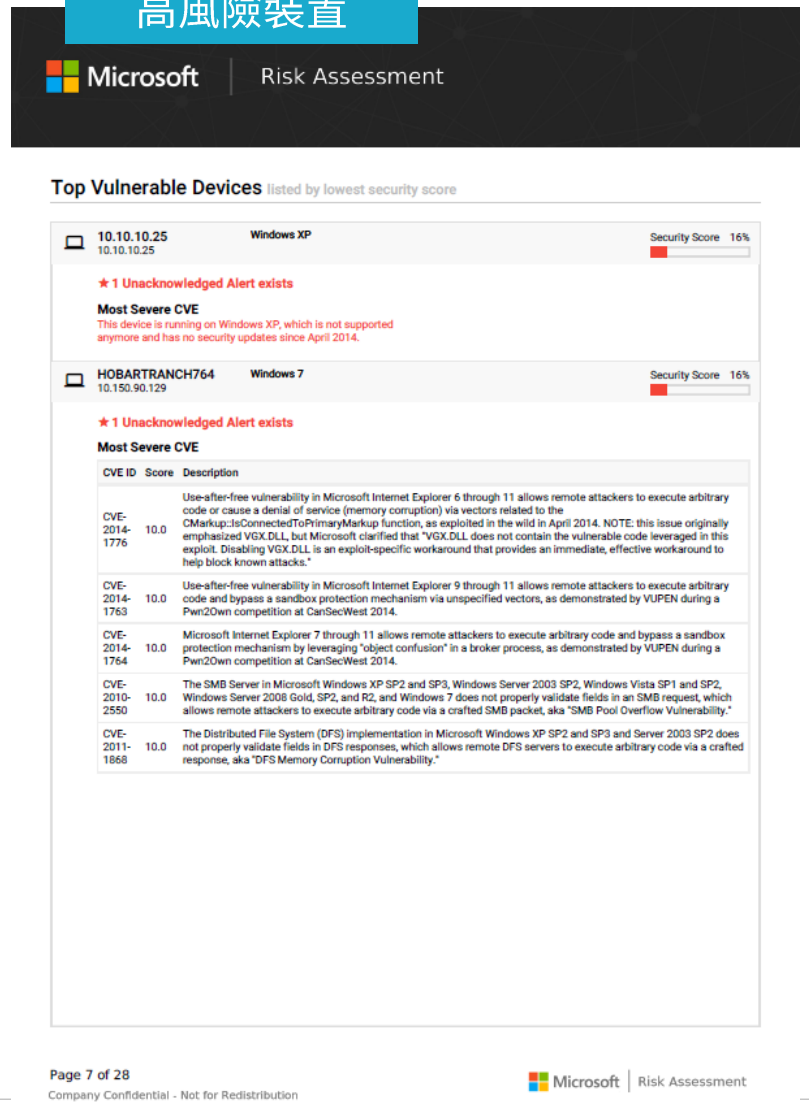
Appendix

健檢報告樣本與官方授權價格

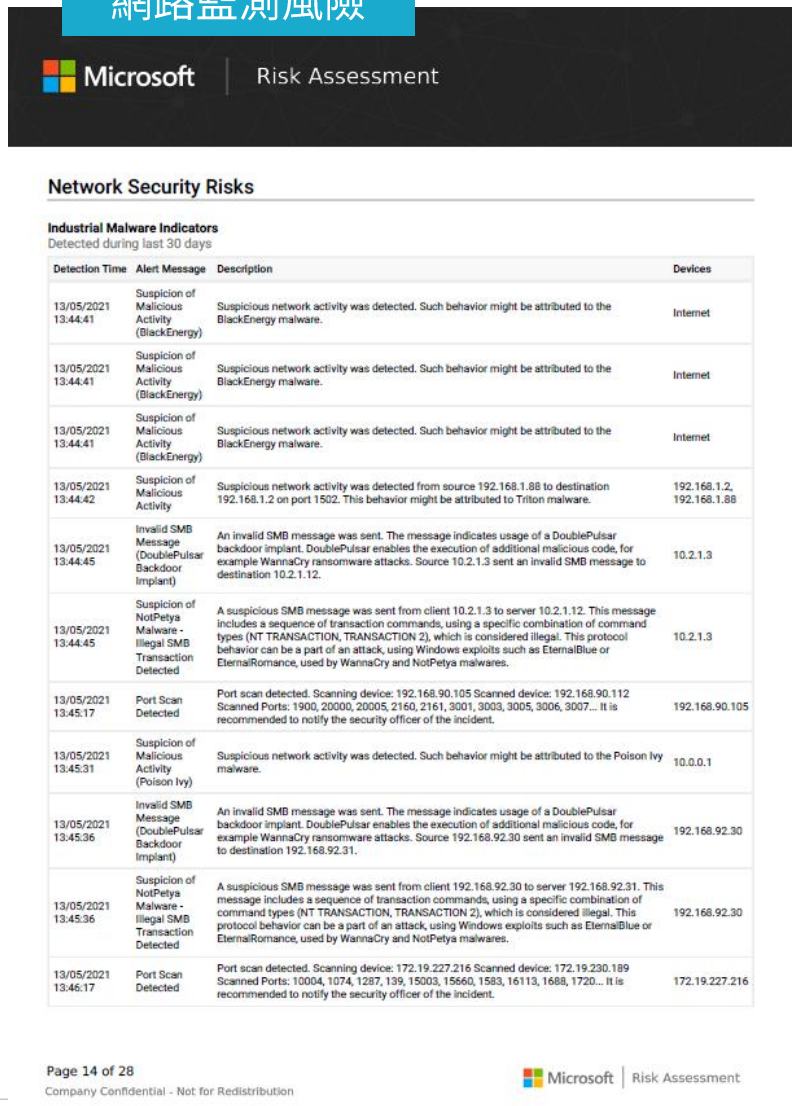
資訊安全健檢報告-官方樣本（一）

總體安全概覽

高風險裝置



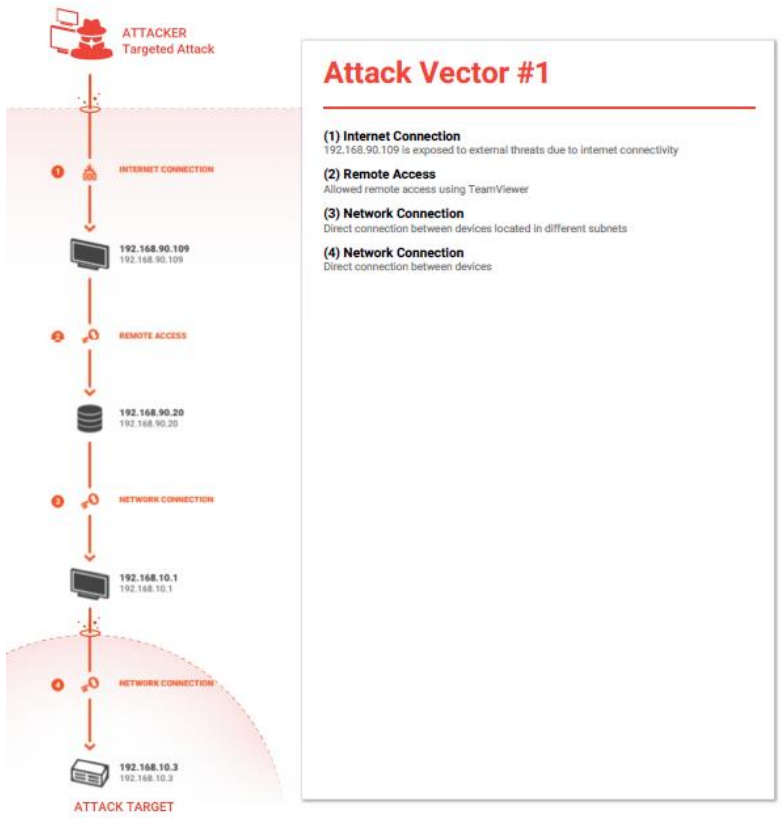
網路監測風險



資訊安全健檢報告-官方樣本（二）

簡易攻擊分析

Microsoft | Risk Assessment



Attack Vector #1

(1) Internet Connection
192.168.90.109 is exposed to external threats due to internet connectivity

(2) Remote Access
Allowed remote access using TeamViewer

(3) Network Connection
Direct connection between devices located in different subnets

(4) Network Connection
Direct connection between devices

資安改善建議

Microsoft | Risk Assessment

Mitigation

Please note, the following enhancements are available:
★ Firewall policy import
★ Further device information import

☐ **Check any Internet Connections ensuring all are allowed. Consider removing unnecessary connections or using an offline-proxy or a Unidirectional Security Gateway** — **14%** Maximum Security Impact

Internal Address	Authorized	External Addresses
10.10.10.25	Yes	8.8.8.8
10.150.90.129	Yes	34.226.68.35 , 54.144.111.231 , 64.74.103.155
10.150.90.250	Yes	199.167.52.141 , 54.225.164.101 , 54.243.77.59
172.19.230.189	Yes	51.104.166.192
172.29.0.111	Yes	68.87.71.230 , 68.87.73.246
192.168.0.107	Yes	144.208.124.152 , 198.54.117.211 , 198.54.117.216
192.168.66.235	Yes	166.161.16.230
192.168.90.10	Yes	207.234.209.181
192.168.90.105	Yes	8.8.8.8
192.168.90.109	Yes	157.56.176.213 , 173.193.174.199 , 173.194.65.188 , 212.179.17.163 , 216.58.198.238 , 216.58.213.99 , 216.58.214.46 , 23.53.50.135 , 66.235.148.140 , 81.218.16.237 , 81.218.16.251
192.168.90.12	Yes	66.22.111.2
192.168.92.30	Yes	8.8.8.8

☐ **Upgrade firmware to the latest version (Devices: 6)** — **12%** Maximum Security Impact

Name	Address
10.48.1.100	10.48.1.100
192.168.10.120	192.168.10.120
192.168.10.3	192.168.10.3
192.168.10.4	192.168.10.4
192.168.110.6	192.168.110.6
192.168.90.122	192.168.90.122

☐ **Install an Antivirus solution to increase protection of the workstations** — **10%** Maximum Security Impact

Microsoft Defender for IoT 官方授權定價 ※方案價格如有異動，請以微軟官方公告為準。

適用於 IoT 的 Microsoft Defender (先前稱為適用於 IoT 的 Azure Defender)

適用於 IoT 的 Defender 可為 IoT/OT 環境提供一貫的安全性，並能依據您要保護現有的 IoT/OT 環境，或要保護經由 IoT 中樞所佈建及管理的新 IoT/OT 裝置，提供兩組不同的功能。

無代理程式監視

適用於 IoT 的 Defender 無代理程式監視功能在前 30 天內，可免費在首 1，000 個裝置使用。在此之後，將會自動按照下列價格向顧客收費。將適用於 IoT 的 Defender 警示和事件內嵌至 Microsoft Sentinel 不需要任何費用。

組織將依據將保護的裝置數目 (以 100 為增量) 每月計費，而且他們可以選擇每月或年度訂用帳戶選項。每月選項是專為裝置數量可能會隨著時間變更的組織所設計。使用此選項時，您可以隨著組織中裝置數量的增加，將裝置新增到您的訂用帳戶，或者視需要減少裝置數量。這最適合著重定價模型彈性的組織。對於基於預算考慮，著重每月費用之可預測性和一致性的組織，我們提供年度訂用帳戶選項，以確保每月費用在年度訂閱期間每個月都相同。

解決方案	訂用帳戶選項	價格
適用於 IoT 的 Defender 無代理程式監視	每月	每 100 部受監視的裝置每月 **NT$4,114**[1]
	年度	每 100 部受監視的裝置每年 **NT$49,362**

[1]若客戶選擇連線到雲端以將資料傳送給 Microsoft Sentinel，必須先將適用於 IoT 感應器的 Defender 連線到 IoT 中樞，而這會衍生額外的費用。如需了解定價，請參閱 Azure IoT 中樞定價頁面。

保護經由 IoT 中樞佈建的新裝置

適用於 IoT 的 Defender 也能為**經由 IoT 中樞所佈建及管理的新裝置** (例如安裝有適用於 IoT 的 Defender 安全性代理程式的裝置) 提供安全性。這些安全性功能前 30 天免費。30 天期滿之後，所有使用量將自動依據下列定價計費。

解決方案	價格
適合 IoT 中樞管理之裝置使用的適用於 IoT 的 Defender - 依裝置	**NT$0.0294**/月
適合 IoT 中樞管理之裝置使用的適用於 IoT 的 Defender - 依訊息	**NT$5.877**/25,000 筆交易

Defender for IoT Supported Protocol

- Cisco: CAPWAP Control, CAPWAP Data, CDP, LWAPP
- IETF: ARP, DCE RPC, DNS, FTP (FTP_ADAT, FTP_DATA), GSSAPI (RFC2743), HTTP, ICMP, IPv4, IPv6, LLDP, MDNS, NBNS, NTLM (NTLMSSP Auth Protocol), RPC, SMB / Browse / NBDGM, SMB / CIFS, SNMP, SPNEGO (RFC4178), SSH, Syslog, Telnet, TFTP, TPKT, UDP
- ISO: CLNP (ISO 8473), COTP (ISO 8073), ISO Industrial Protocol, MQTT (IEC 20922)
- Mitsubishi: Melsoft / Melsec (Mitsubishi Electric)
- Rockwell Automation: ENIP, EtherNet/IP CIP (including Rockwell extension), EtherNet/IP CIP FW version 27 and above
- Schneider Electric: Modbus/TCP, Modbus TCP–Schneider Unity Extensions
- Protocols supported by Microsoft Defender for IoT - Microsoft Defender for IoT | Microsoft Docs

讓自由系統陪伴您成長，共同打造IT績效

IT is not an issue, call us!

FREEDOM SYSTEMS

+886-2-2655-0668

sales@freedom.net.tw

www.freedom.net.tw