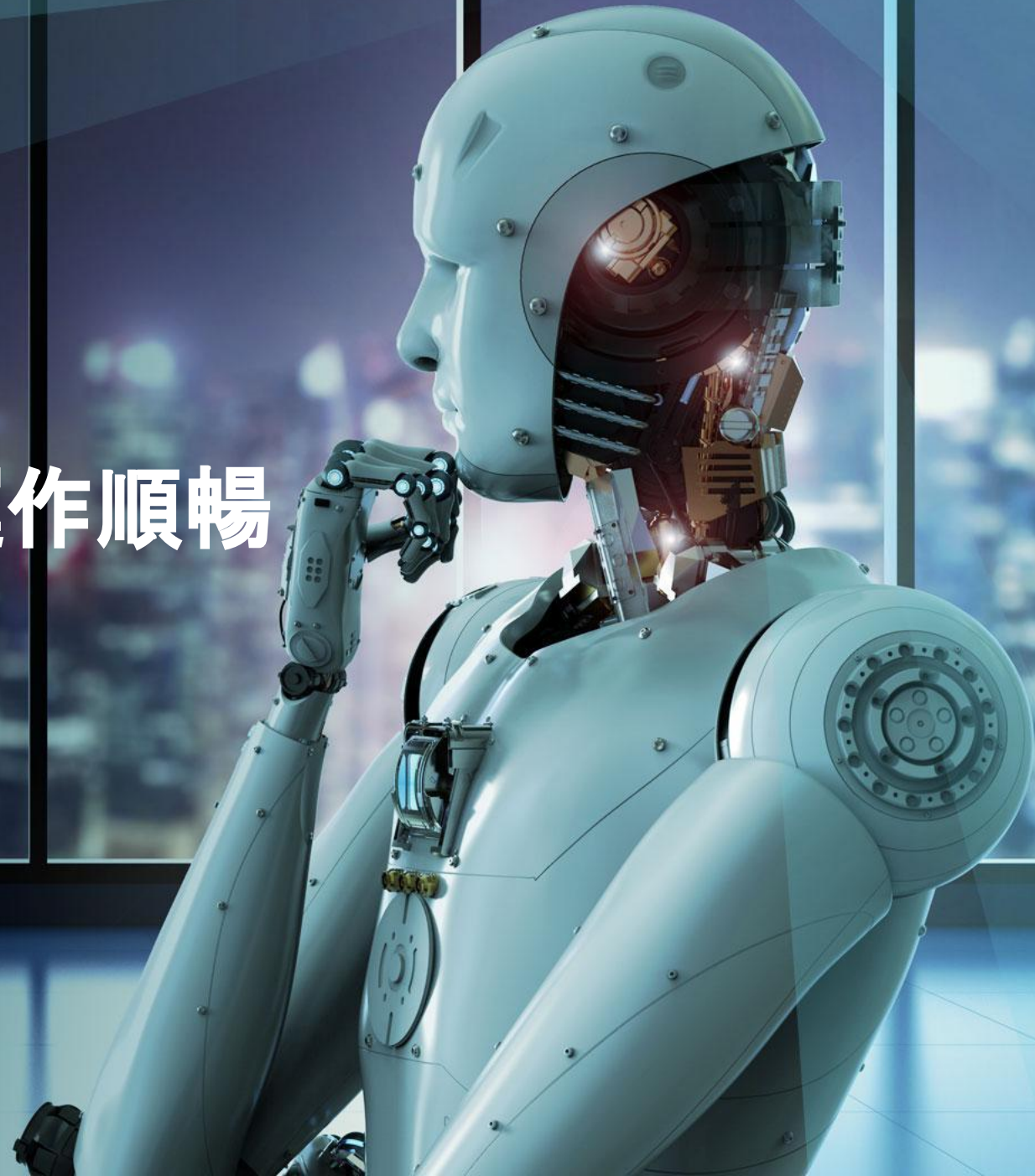


如何利用 AI 協助日常網路運作順暢

Marty Chang

Fortinet 技術顧問

mchang@fortinet.com





資安/網路 維運中心



FortiAnalyzer

Central Log & report



FortiNAC

IoT Access Control



FortiSandbox

File Analysis



FortiAI

Virtual Security Analyst™



FortiSIEM

SIEM / UEBA



FortiXDR

XDR



FortiManager

Central Device Mgmt.



FortiAuthenticator

User Access Mgmt.



FortiTester

Network Tester



FortiDeceptor

Honeypot



FortiSOAR

SOAR



FortiPAM

PAM



雲端服務 / 雲端託管

Cloud mgmt.

FortiGate Cloud | FortiLAN Cloud |
FortiExtender Cloud | FortiManager Cloud |
FortiAnalyzer Cloud | FortiClient EMS Cloud |
FortiToken Cloud | FortiSOAR Cloud

Cloud services

FortiPresence | FortiMail Cloud | FortiPhish |
FortiGSLB | FortiConverter | Fortinet SOCaaS |
FortiSASE | FortiPenTest | FortiWeb Cloud |
FortiSandbox Cloud | FortiVoice Cloud |
FortiMonitor



終端行動用

384629

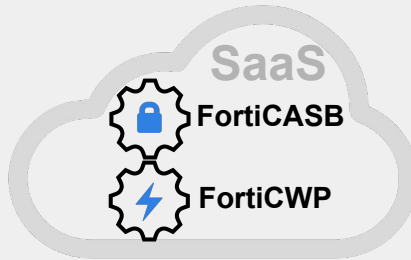
FortiToken

2 Factor OTP Token



FortiClient / FortiEDR

VPN, ZTNA, EPP, and SASE Client



Secure SD-WAN

IPsec / SSL VPN

SASE



FortiGate

Security Gateway

ZTNA



FortiDDoS

L7 D/DOS Mitigator



FortiADC

Load Balancer



FortiMail

Mail Sec. Gateway



FortiWeb

Web App. Firewall



FortiIsolator

Browser Isolation



FortiProxy

Secure Web Gateway



外點/分公司



FortiWiFi

Secure WiFi Access



FortiExtender

3G/4G/5G WAN



FortiSwitch

Switch



FortiAP

Wireless Access Point



FortiRecorder

Surveillance Manager



FortiVoice

IP PBX



FortiCamera



FortiFone

區域內網

業界最完整且全面的資安佈局



資料中心

AI、5G普及 資安攻擊急速加劇



2025年2月馬偕紀念醫院 遭勒索軟體攻擊事件

【資安週報】0303~0307，彰基醫院遭勒索軟體CrazyHunter攻擊，預期可能出現系統化攻擊狀況，全臺關鍵CI醫院拉警報

二二八年假後3月初的資安新聞中，彰化基督教醫院也和不久前的馬偕醫院，一樣遭遇CrazyHunter這支勒索軟體攻擊，引發全國關注，衛生福利部指出這已是系統性攻擊情形；在網路威脅態勢方面，我們最新一期封面故事解析網路威脅態勢日益複雜的現況，並從資安經濟學與AI資安角度，帮助大家展望2025年網路安全態勢



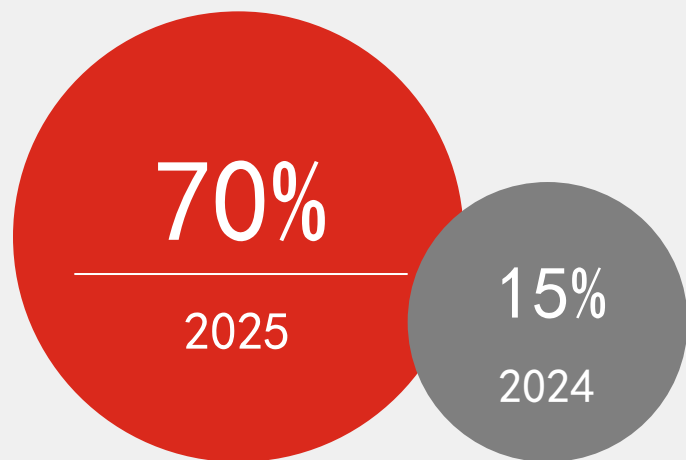
Fortinet 公布 《2024 全球資安威脅預測》

經典攻擊靠 AI 進化、漏洞擄客現身、從內部滲透，
攻擊者將更輕鬆扣下板機

全方位整合與自動化網路資安領導廠商 Fortinet® (NASDAQ : FTNT) 旗下FortiGuard Labs威脅情資中心今 (14) 日公布《2024 全球資安威脅預測》報告顯示，透過「網路犯罪即服務 (Cybercrime-as-a-Service , CaaS) 」的攻擊案例增加，加上生成式人工智慧的出現，威脅者比過往任何時候都更容易發動攻擊。同時，攻擊者各自仰賴的工具不斷演進，更一再提升攻擊行動的複雜性，目前已經可以發動更具針對性且更隱匿的攻擊，並且有能力規避一些強大的安全防護，其攻擊週期中每個戰術循環也變得更加靈活。

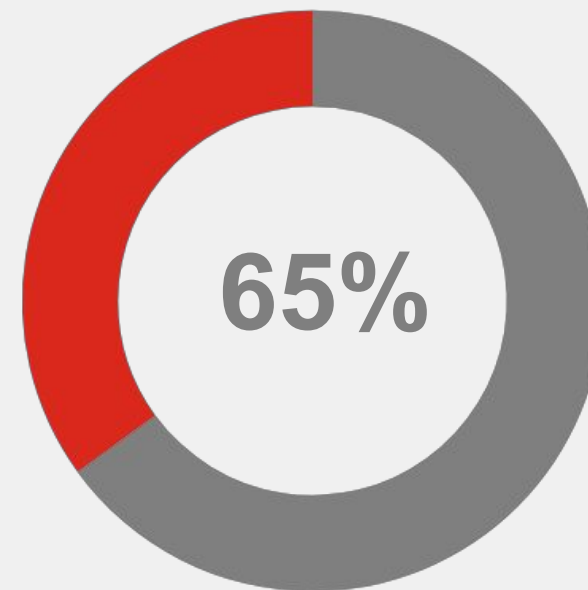
網路維運的變革已經展開了 ...

Gartner: 生成式 AI 在提高營運效率和競爭優勢方面發揮變革性力量



供應商
(Vendors)

- 網路供應商透過生成式AI, 與機器人對話互動, 來增強網路運營能力
- 根據 Gartner 數據, 使用新一代AI 工具的供應商將從今年的 15% 增加到明年的 70%

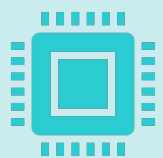


管理者 (Customers)

- 設定配置和故障排除等維運作業仍然有65% 透過人工手動執行, 這凸顯了透過GenAI 實現自動化來提升效率的龐大契機。

GenAI 的 iPhone 時刻已經來臨，將成為網路維運的基石

Gartner：生成式 AI 的目標，提高營運效率，提升 IT 團隊技能水平，並改善用戶體驗



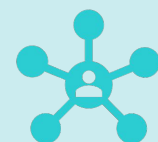
到 2025 年時，**20%** 的初始設定配置將使用 GenAI 協助，而在 2023 年時，這個比例趨近於 0%。



到 2026 年時，**60%** 的網路營運人員將依賴 GenAI 進行持續性網維管理，而在 2024 年初時，這個比例還不到 5%。



GenAI 可以減少多達 **25%** 的故障排除時間、安裝時間和到場檢視時間。



網路效能和可用性的改進 可以將最終用戶的工作效率提高達 **25%**。

FortiAI 能為我們做些甚麼？



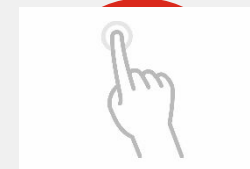
提升洞察力

建構整個維運環境的知識庫，從網路、用戶、傳輸數據的應用以及資安態勢



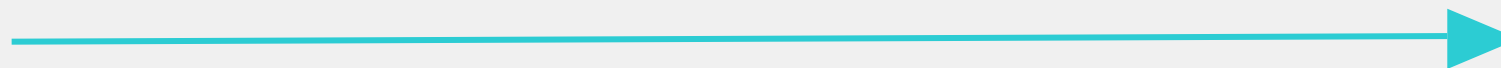
協助決策制定

依據洞察後狀態推薦管理者接續的行動制定，以上是基於維運環境的分析並執行最佳實踐執行



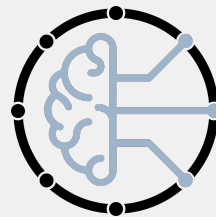
自動化腳本執行

通過管理者同意後的自動化腳本來執行決策後的推薦行動



FortiAI Ops

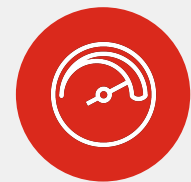
預知問題，減少障礙，優化環境
將資源投注在更關鍵的商務之上



簡單的交給你！
複雜的就交給 AI
吧！



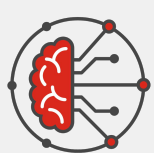
節省時間



提高回應速度

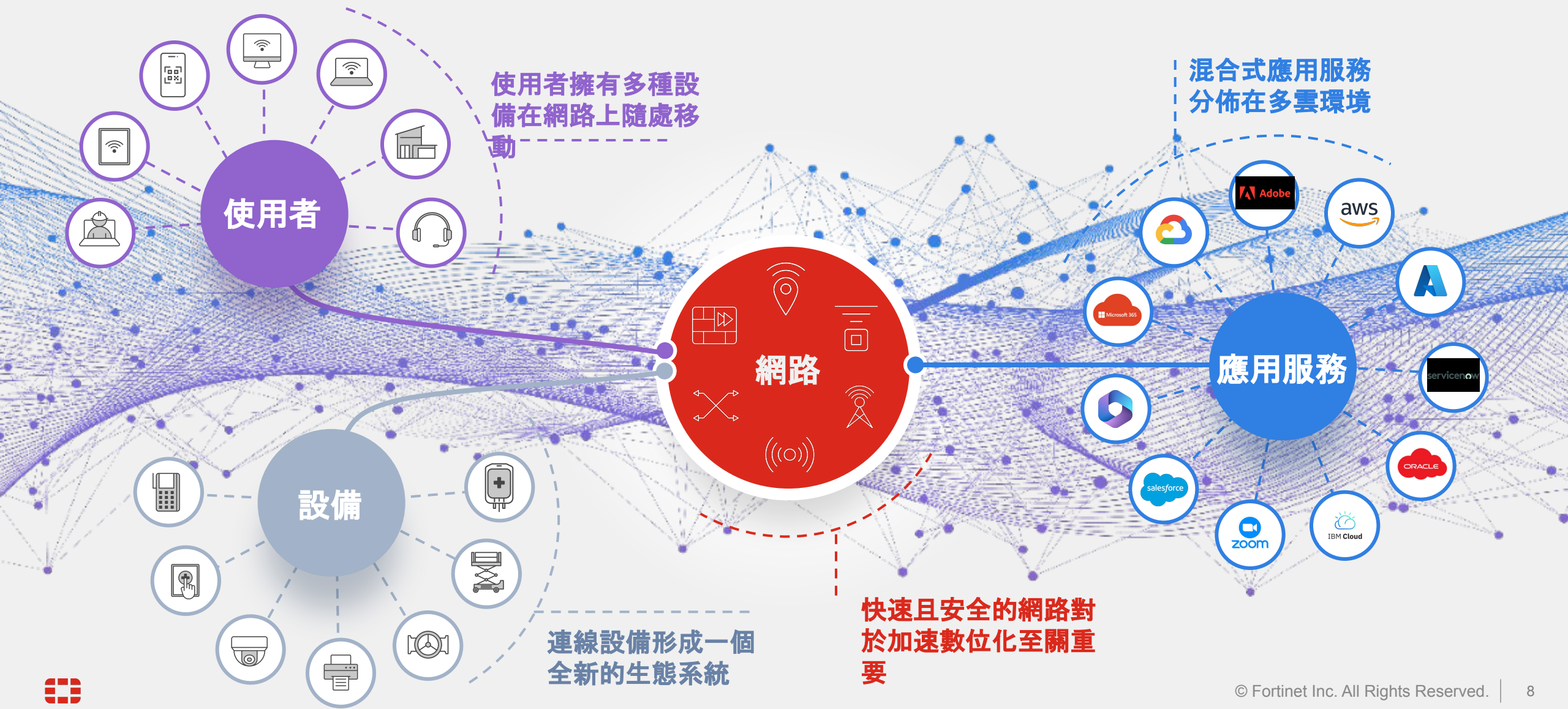


增加生產力



當網際網路變得越趨複雜...

駭客攻擊已成家常便飯





網路面臨的挑戰

微分割讓網路營運變得複雜



人工營運繁瑣



缺乏可視性



找出根本原因



企業受到的衝擊



時間的浪費

部門將時間花在繁瑣的工作上，
而非戰略性計畫



失去生產力

員工花時間處理網路問題



造成金錢的損失



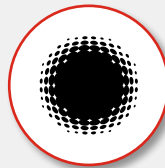


網路營運常面臨的挑戰



營運團隊

需要高度專業技術的
調查和耗時的修復



數據過多，無法監控



需要跨有線、無線和 SD-WAN
領域的專業知識



耗時的故障排除過程



問題的分類，在不同領域和
情境下有所不同



效能不佳的線路服務



網路營運大趨勢



網路營運中心 自動化流程處理

網路供應商的領導者正被要求提供安全的網路並實現自動化，以支持組織的數位轉型。

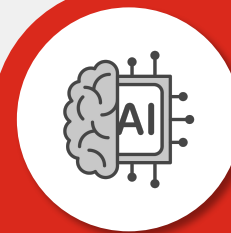
Gartner Hype Cycle for Enterprise Networking, 2022



應用服務 識別管控

到 2026 年，至少 **60%** 的領導者將使用 DEM (數位化體驗管理) 從用戶的角度來評估應用服務和終端性能，而 2021 年這個比例不足 20%。

Gartner, Market Guide for Digital Experience Monitoring, 28 March 2022



AI Ops 人工智能導入

IDC 預測，到 2027 年，AI 驅動的自動化將可確保數位基礎設施配置、性能、成本和安全的一致性，透過減少 **70%** 的人為操作來提高服務水平目標。



人工智能帶給我們怎樣的幫助？

網路營運中的人工智能與機器學習 (AI / ML)

記錄分析



機器學習建立
營運基準線

狀態監控



發現網路異常態勢
與問題癥結點

危機預警

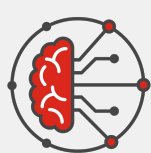


關聯性分析, 識別問題
確定根本原因 (RCA)

提供對策

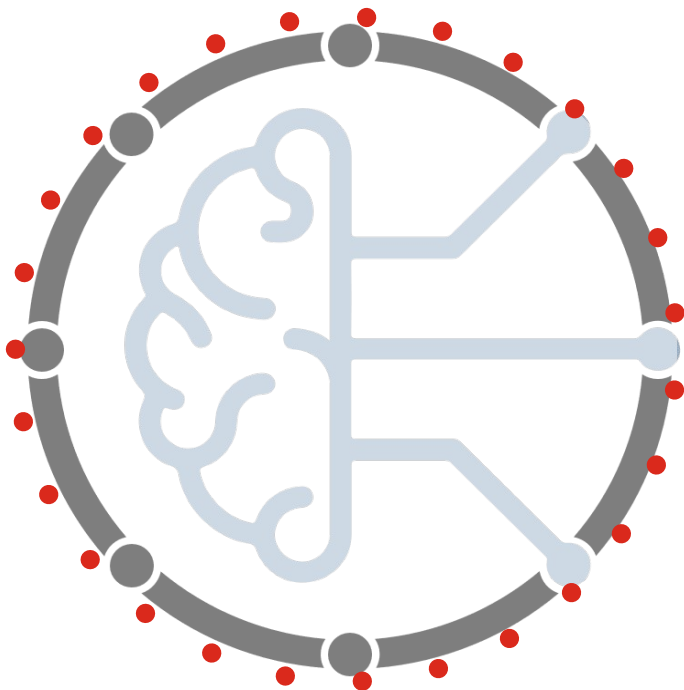


AI 提供專業建議
快速解決問題



FortiAIOps 概觀

AI / 機器學習在安全織網的應用



Incident API



Stats API



FortiOS



SD-WAN



FortiAP



FortiExtender



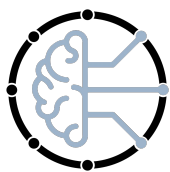
FortiSwitch

FortiAIOps 是一種人工智能與機器學習 (AI / ML) 解決方案, 提升可視性、識別異常行為、發現問題根本原因, 執行網路營運中心 (NOC) 優化。





FortiAI Ops 效益

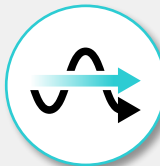


AI Ops



Ops Team

輕鬆的分析各個網路節點資料
建立網路流量基準線
提供最佳的改善方案



減輕網路技術的依賴



快速找到問題癥結點



減少復原所需時間



增進網路與應用服務可靠度



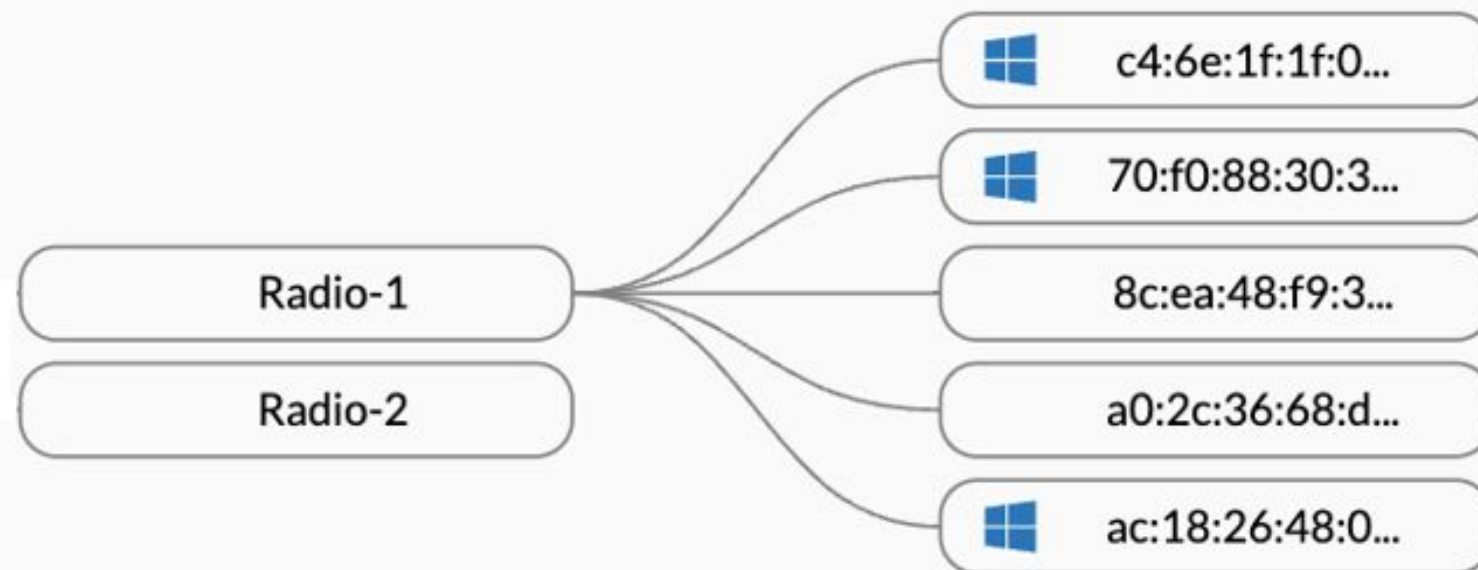
提升使用者體驗



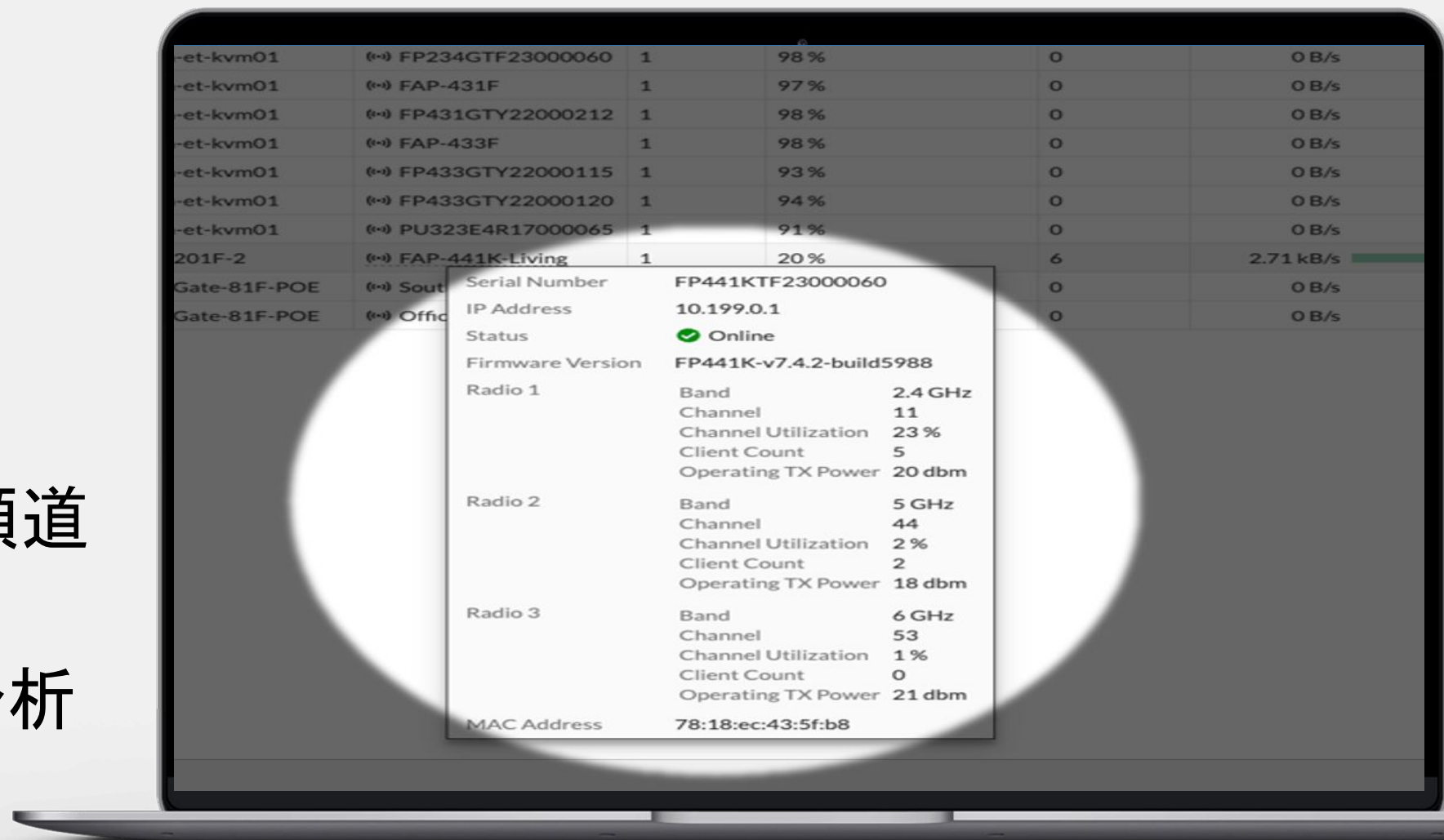
直覺化的操作介面



- 簡單易懂的拓譜圖
- 依據無線頻段列出無線網路用戶清單



- 無線趨勢分析
 - 頻道使用率
 - 雜訊程度
 - 流量統計
- 整體無線網路頻道使用率
- 單一 AP 深入分析



-et-kvm01	(=) FP234GTF23000060	1	98 %	0	0 B/s
-et-kvm01	(=) FAP-431F	1	97 %	0	0 B/s
-et-kvm01	(=) FP431GTY22000212	1	98 %	0	0 B/s
-et-kvm01	(=) FAP-433F	1	98 %	0	0 B/s
-et-kvm01	(=) FP433GTY22000115	1	93 %	0	0 B/s
-et-kvm01	(=) FP433GTY22000120	1	94 %	0	0 B/s
-et-kvm01	(=) PU323E4R17000065	1	91 %	0	0 B/s
201F-2	(=) FAP-441K-Living	1	20 %	6	2.71 kB/s
Gate-81F-POE	(=) Sout			0	0 B/s
Gate-81F-POE	(=) Office			0	0 B/s

Serial Number

IP Address

Status

Firmware Version

Radio 1

Radio 2

Radio 3

MAC Address

FP441KTF23000060

10.199.0.1

Online

FP441K-v7.4.2-build5988

Band 2.4 GHz

Channel 11

Channel Utilization 23 %

Client Count 5

Operating TX Power 20 dbm

Band 5 GHz

Channel 44

Channel Utilization 2 %

Client Count 2

Operating TX Power 18 dbm

Band 6 GHz

Channel 53

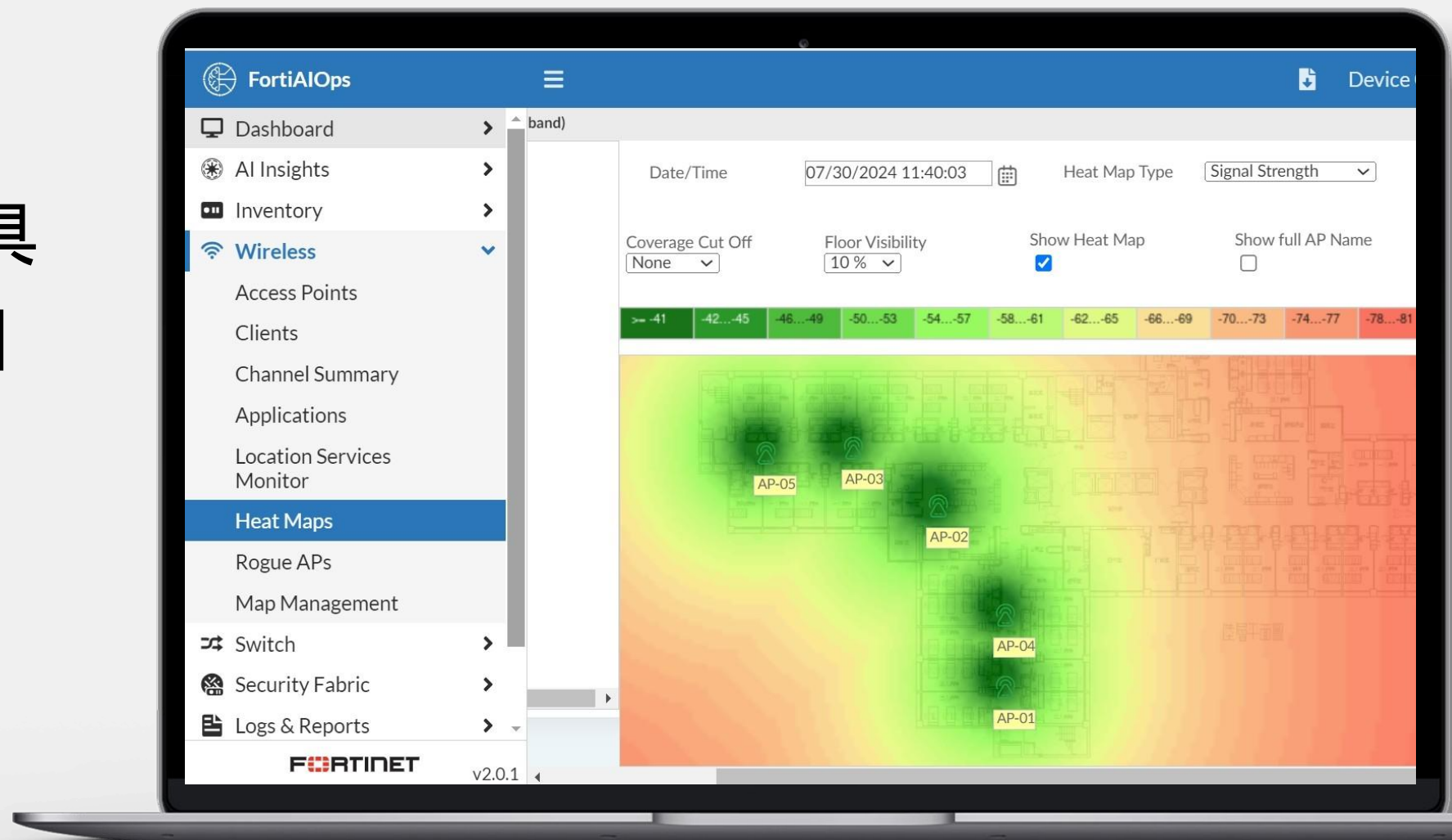
Channel Utilization 1 %

Client Count 0

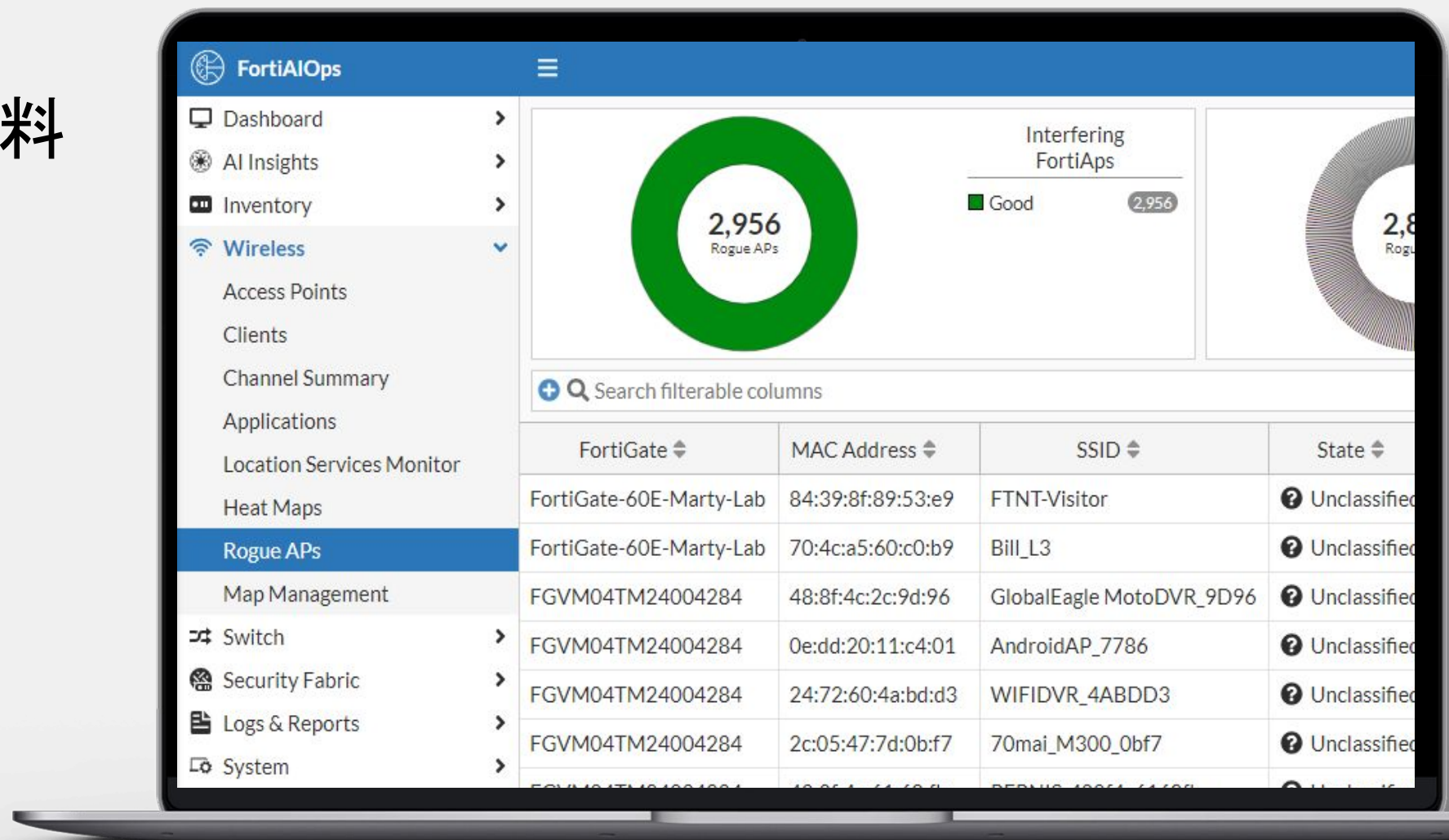
Operating TX Power 21 dbm

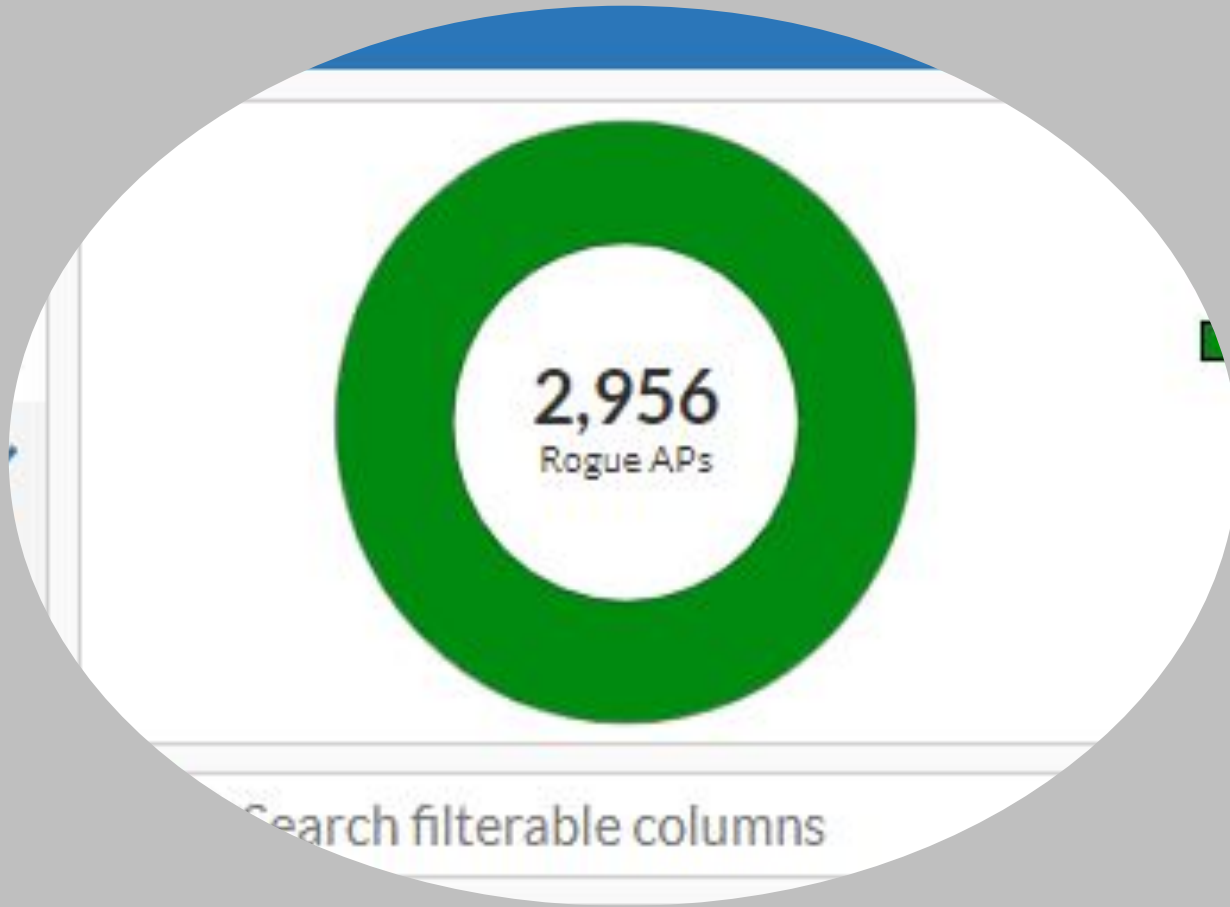
78:18:ec:43:5f:b8

- 無線網路
Site-Survey 工具
- 無線網路熱感圖



• 干擾 AP 統計資料



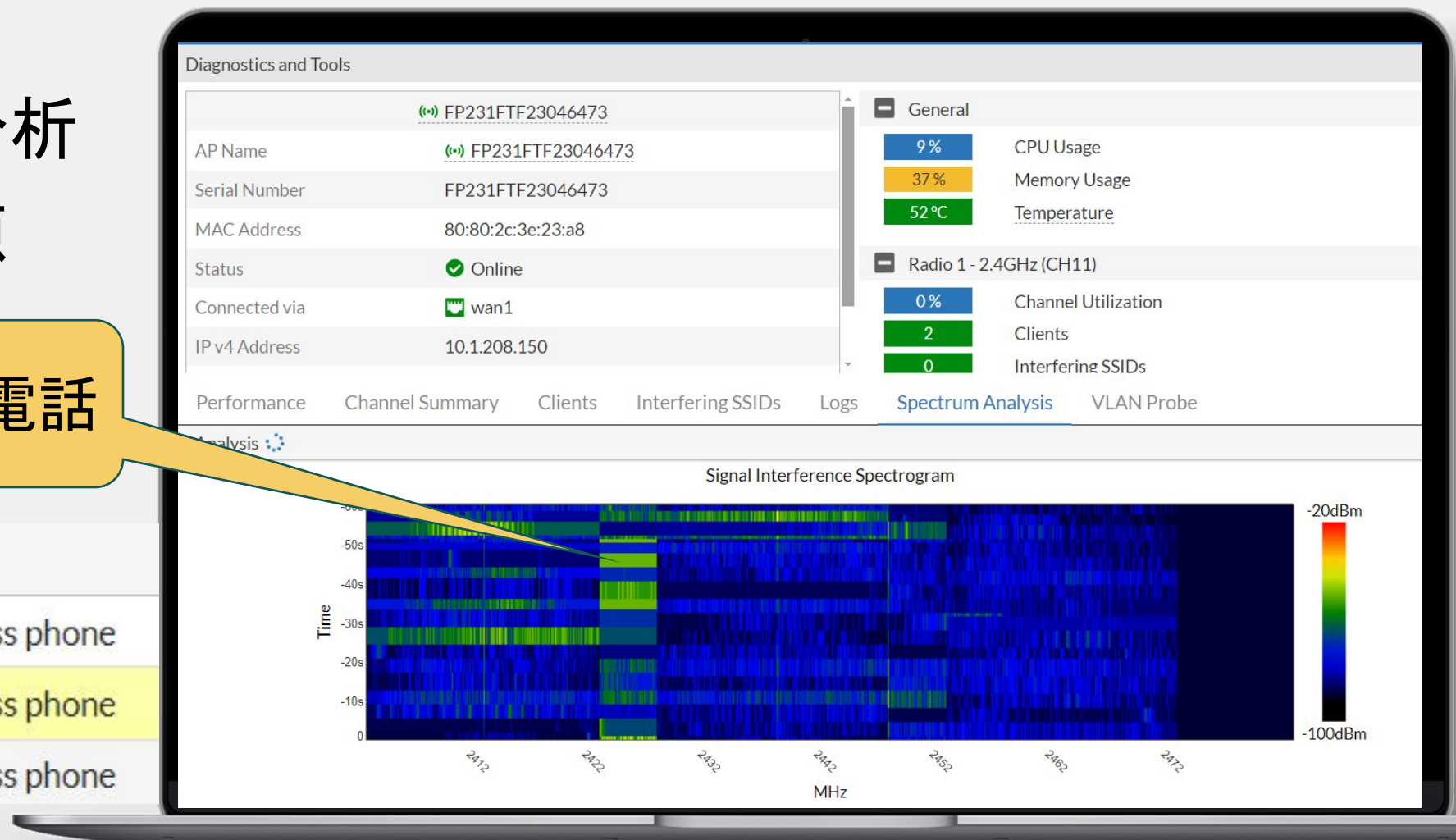


附近干擾 AP 高達 2900 多個

- 無線網路頻譜分析
- 一眼找出干擾源

2.4GHz 家用無線電話

Frequency	Type
2402	WiFi, DSSS cordless phone
2427	WiFi, DSSS cordless phone
2452	WiFi, DSSS cordless phone





AI / 機器學習





FortiAI Ops

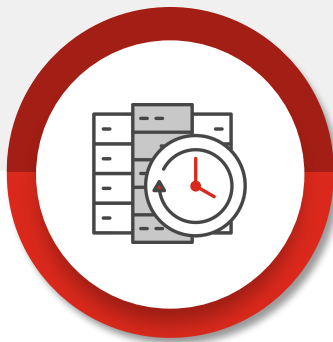
AI / 機器學習基準線的建立



自動收集
FortiGate
FortiSwitch
FortiAP
SD-WAN
使用資訊



收集資料，
以七天為基
礎，建立各
項基準線



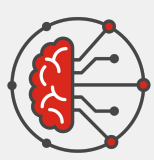
比對目前資
料與過去七
天歷史資料
差異處



透過 AI 運算
找出受影響
的設備與受
影響的應用
服務



AI 提供專業
的建議快速
解決問題



如何利用 AI 解決問題



Emma：今天無線網路很慢耶！



您好，這裡是控八控控—控控控



傳統方式解決問題

費時又費力，需要跨有線、無線和 SD-WAN 領域的專業知識

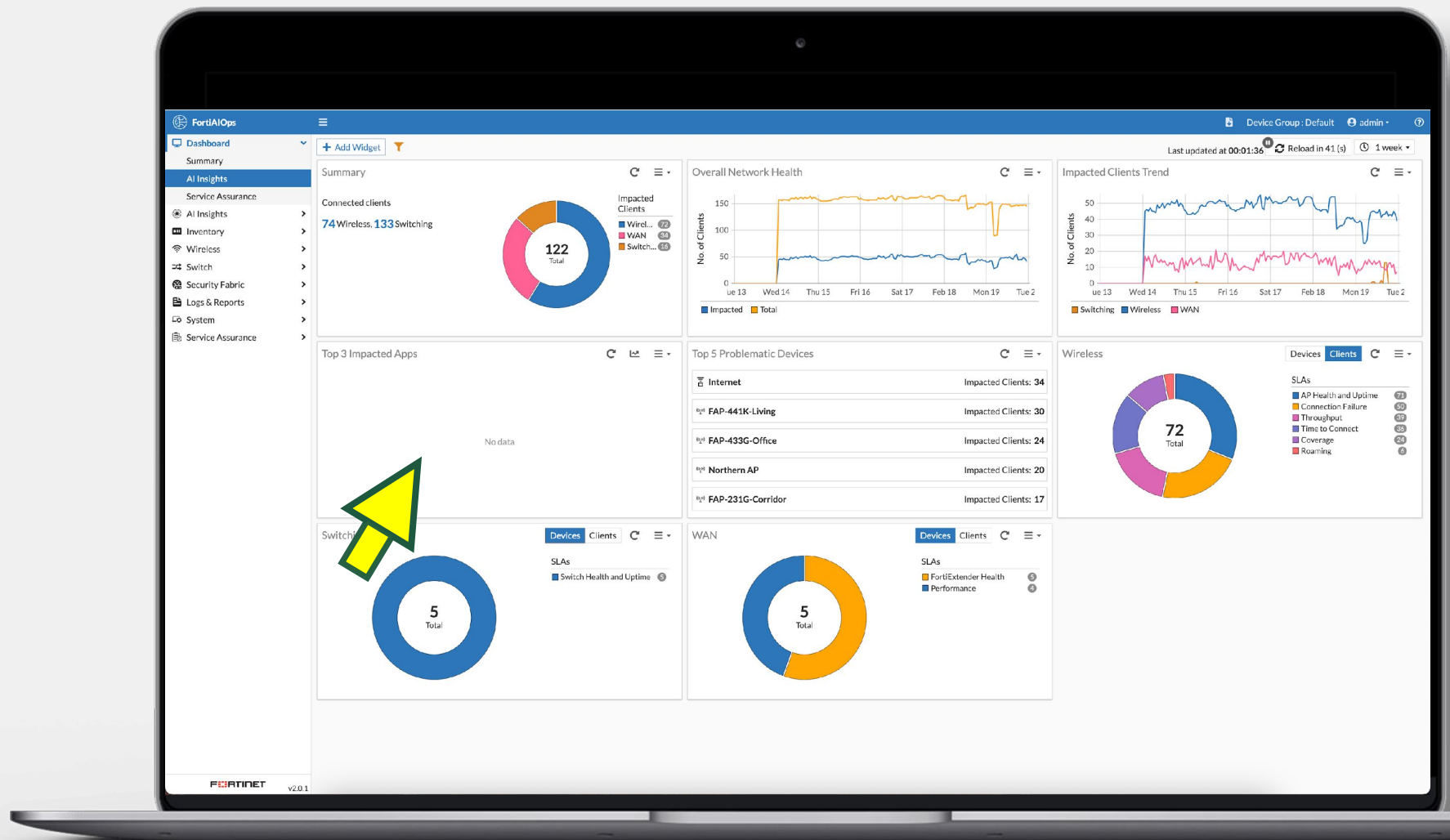
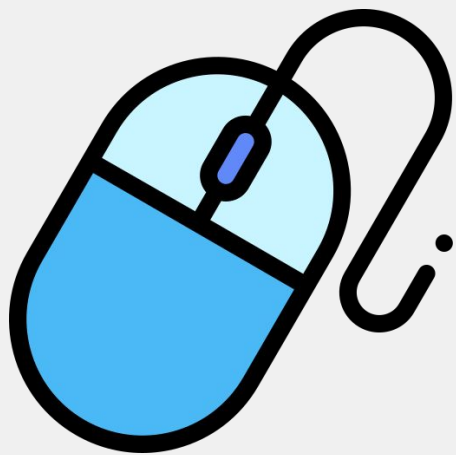




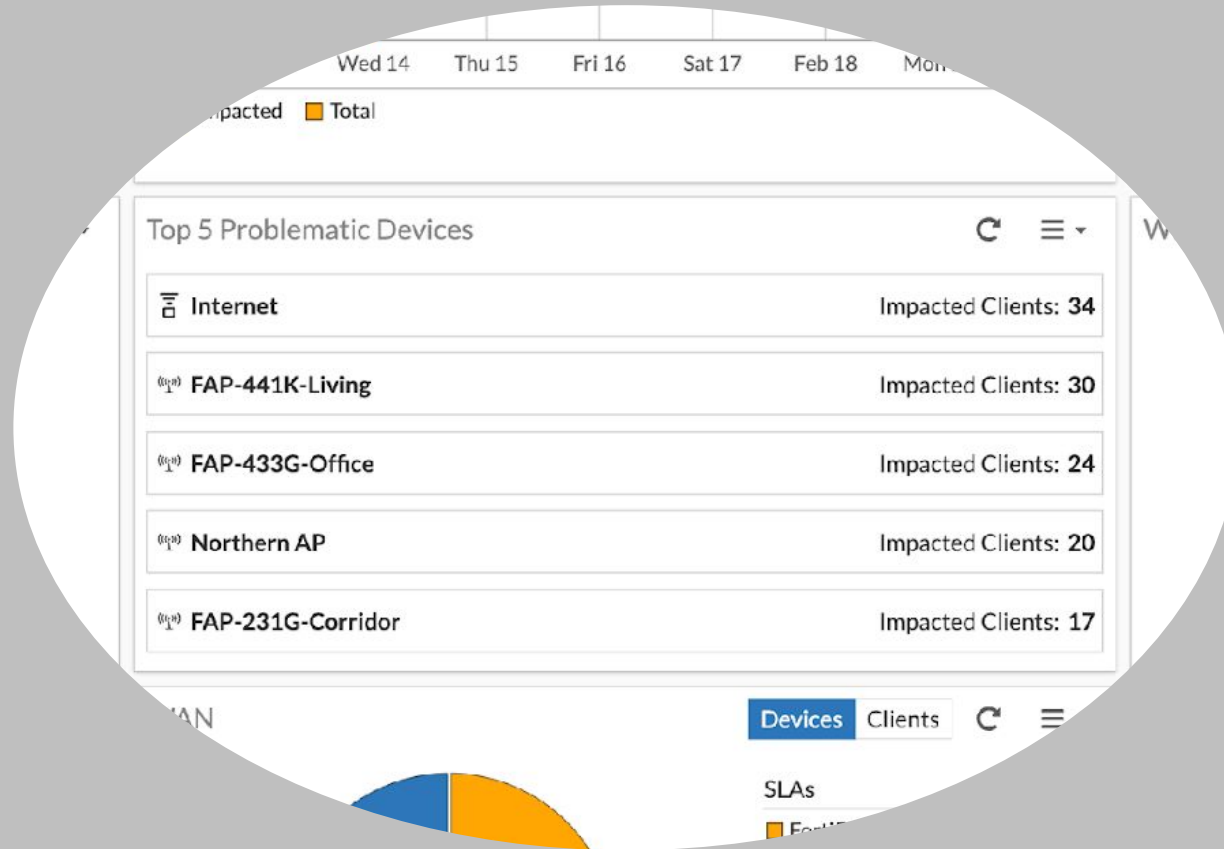
透過 AI 解決問題

省時又省力, AI 直擊問題核心

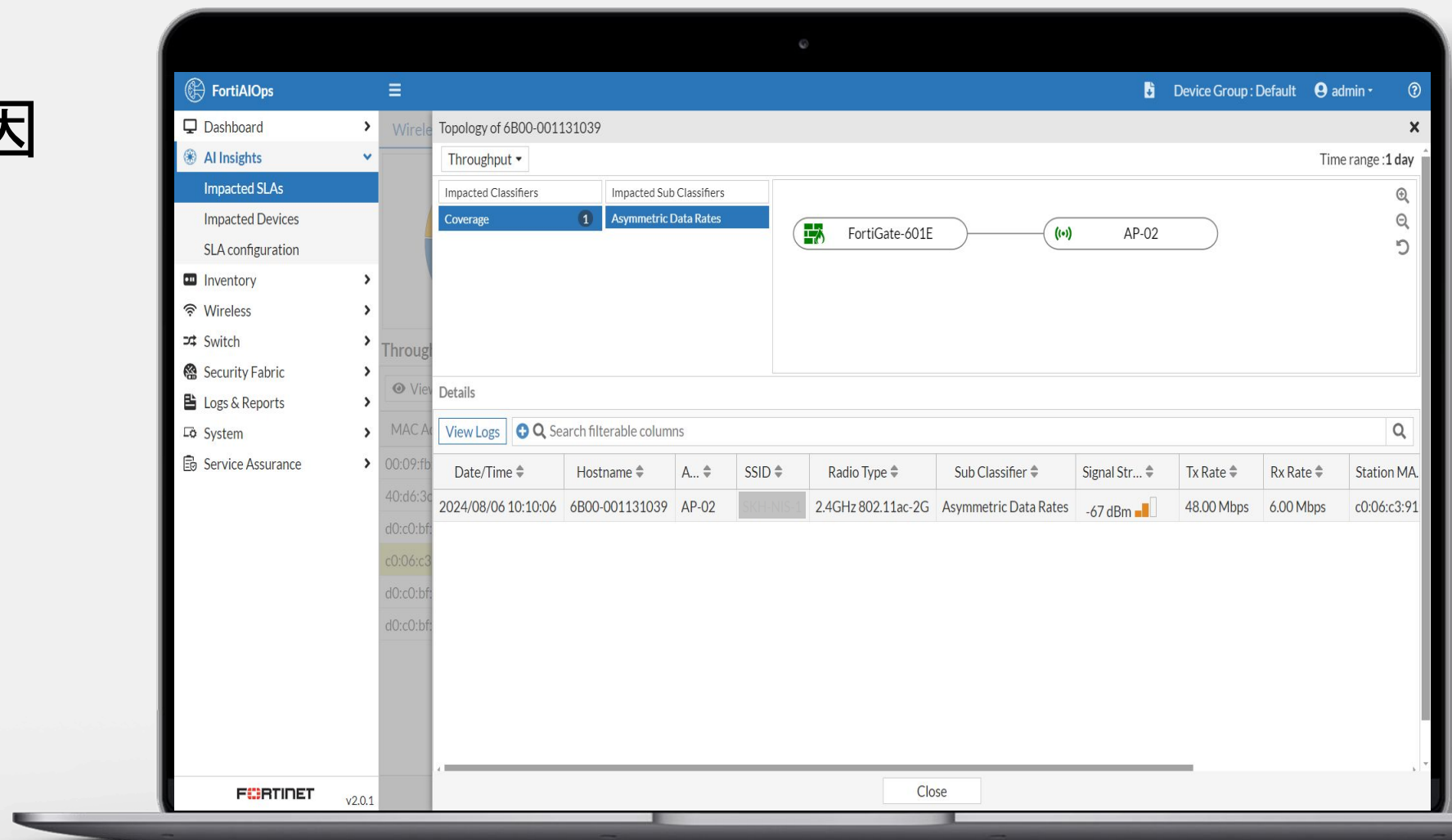
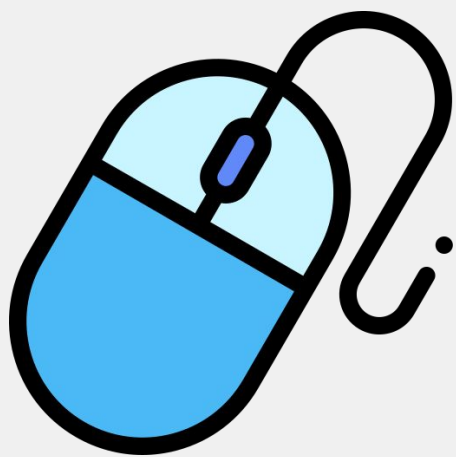
- 透過點擊滑鼠
- 快速找到問題



找出受影響的使用者



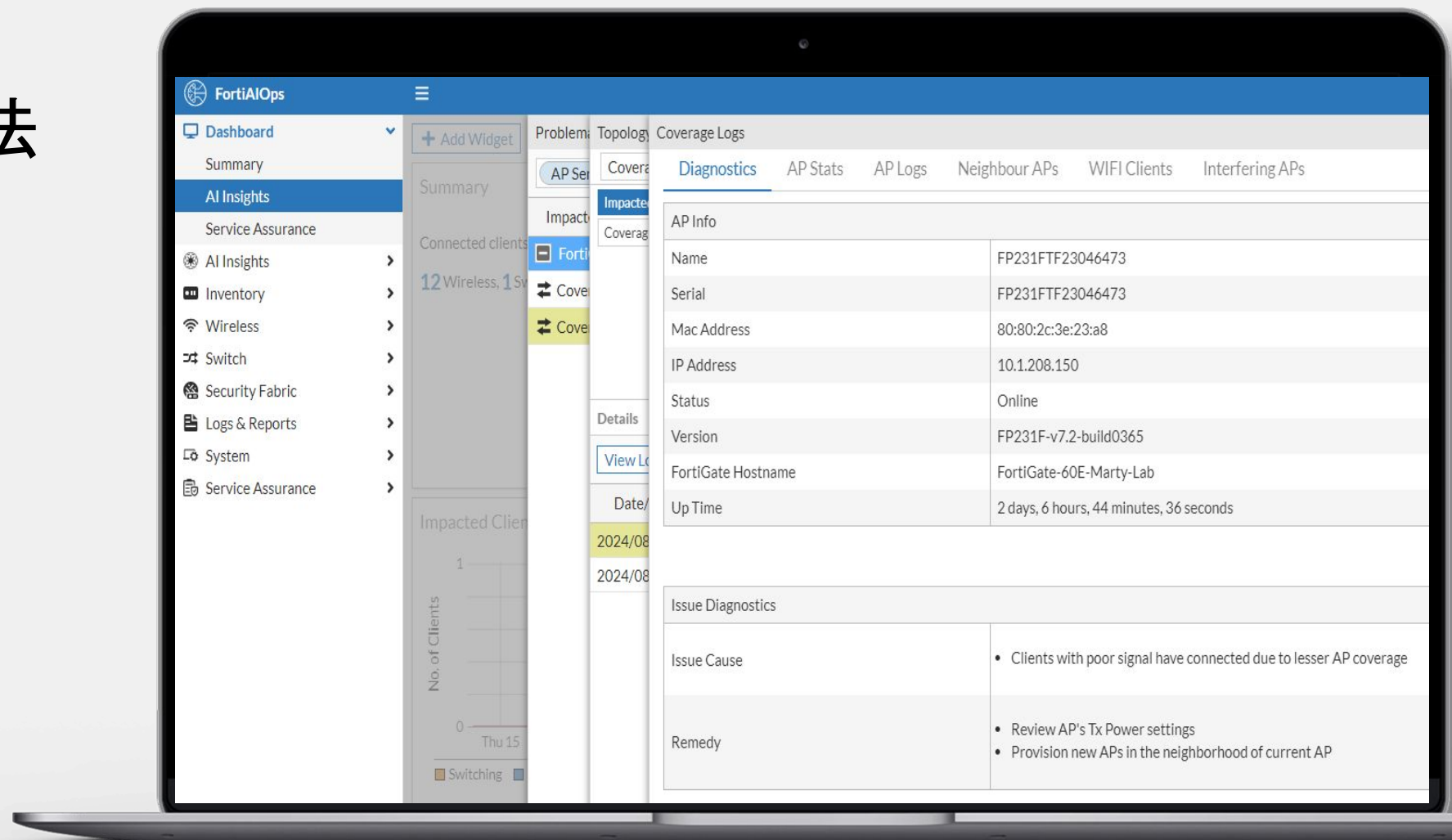
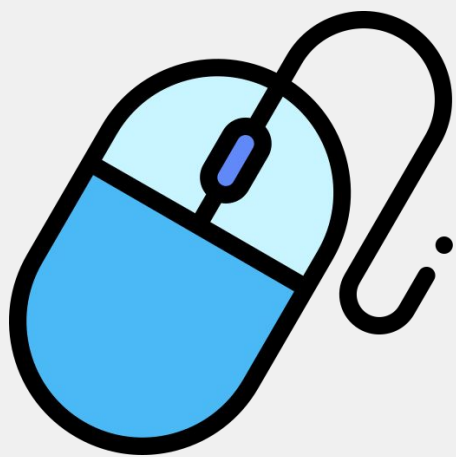
• 透過 AI 判斷原因



AI 自動判斷：無線訊號傳送速率不對等

Radio Type ▾	Sub Classifier ▾	Signal Str... ▾	Tx Rate ▾	Rx Rate ▾
2.4GHz 802.11ac-2G	Asymmetric Data Rates	-67 dBm 	48.00 Mbps	6.00 Mbps

• 利用 AI 提供解法



AI 建議：調整 AP 傳送功率或增建新 AP

- Review AP's Tx Power settings
- Provision new APs in the neighborhood of current AP



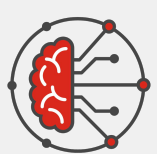
如何利用 AI 解決問題



Lucy：有無線網路但上不了網
耶!



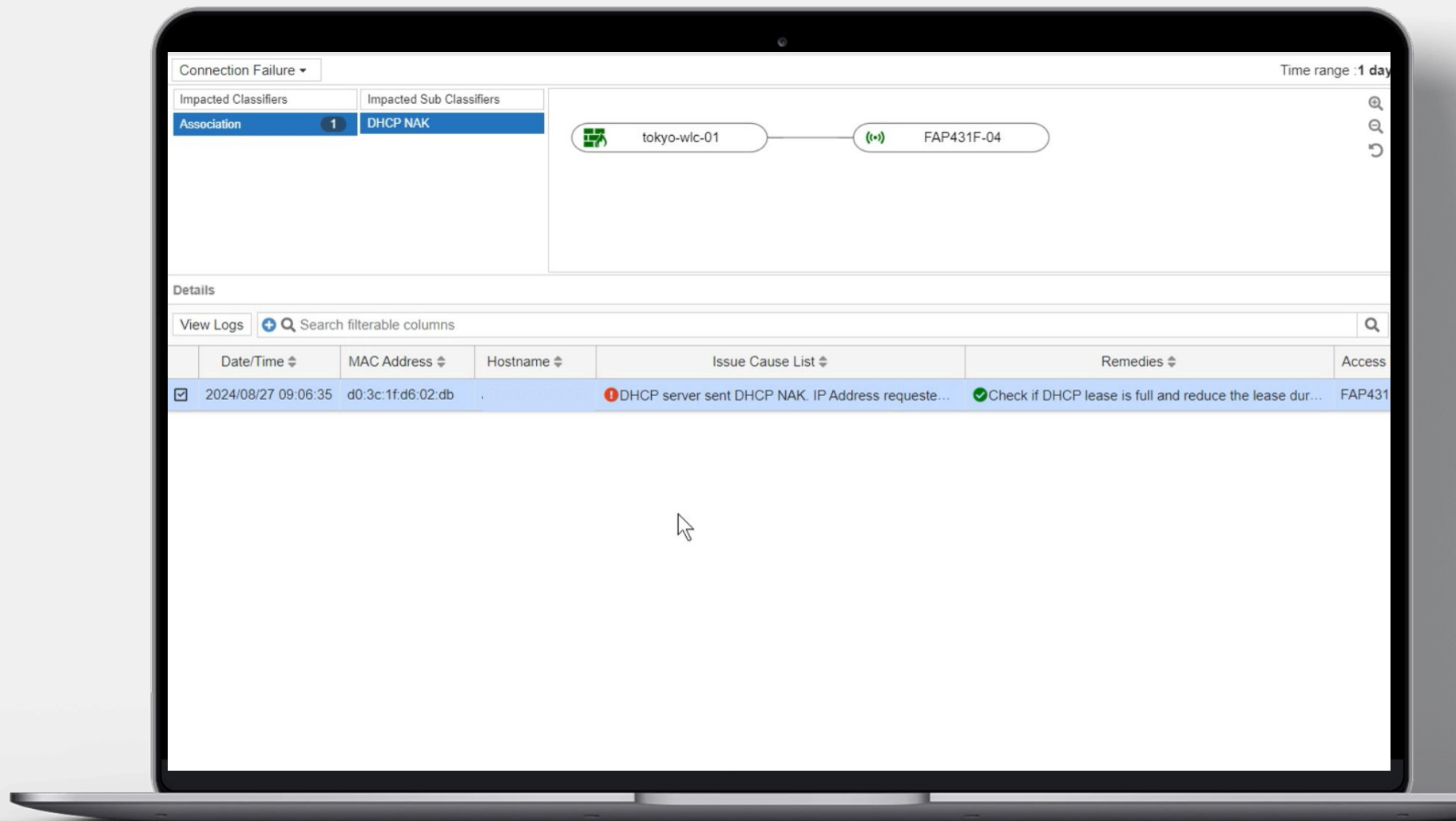
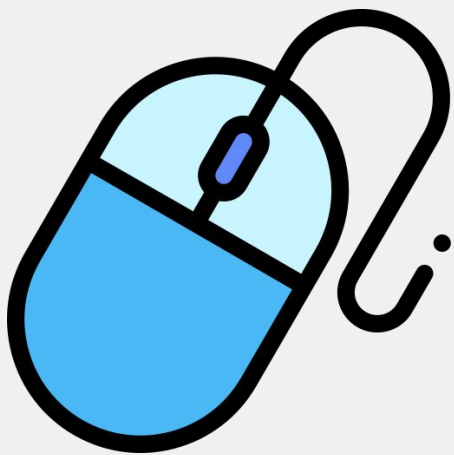
您好，這裡是控八控控—控控控

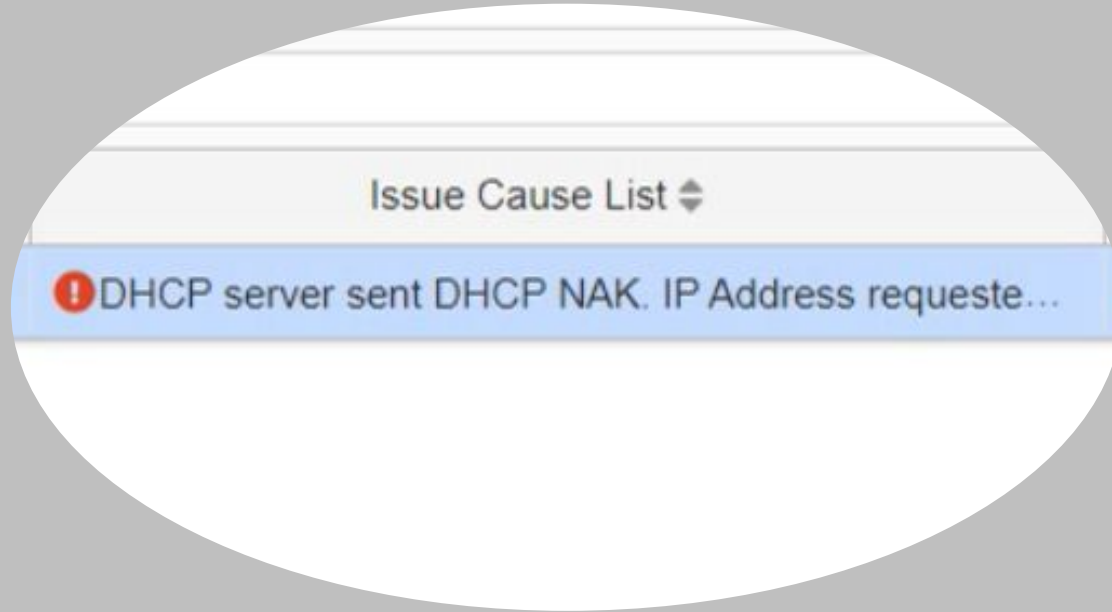


FortiAI Ops

找出無法上網問題

- 透過 AI 判斷原因

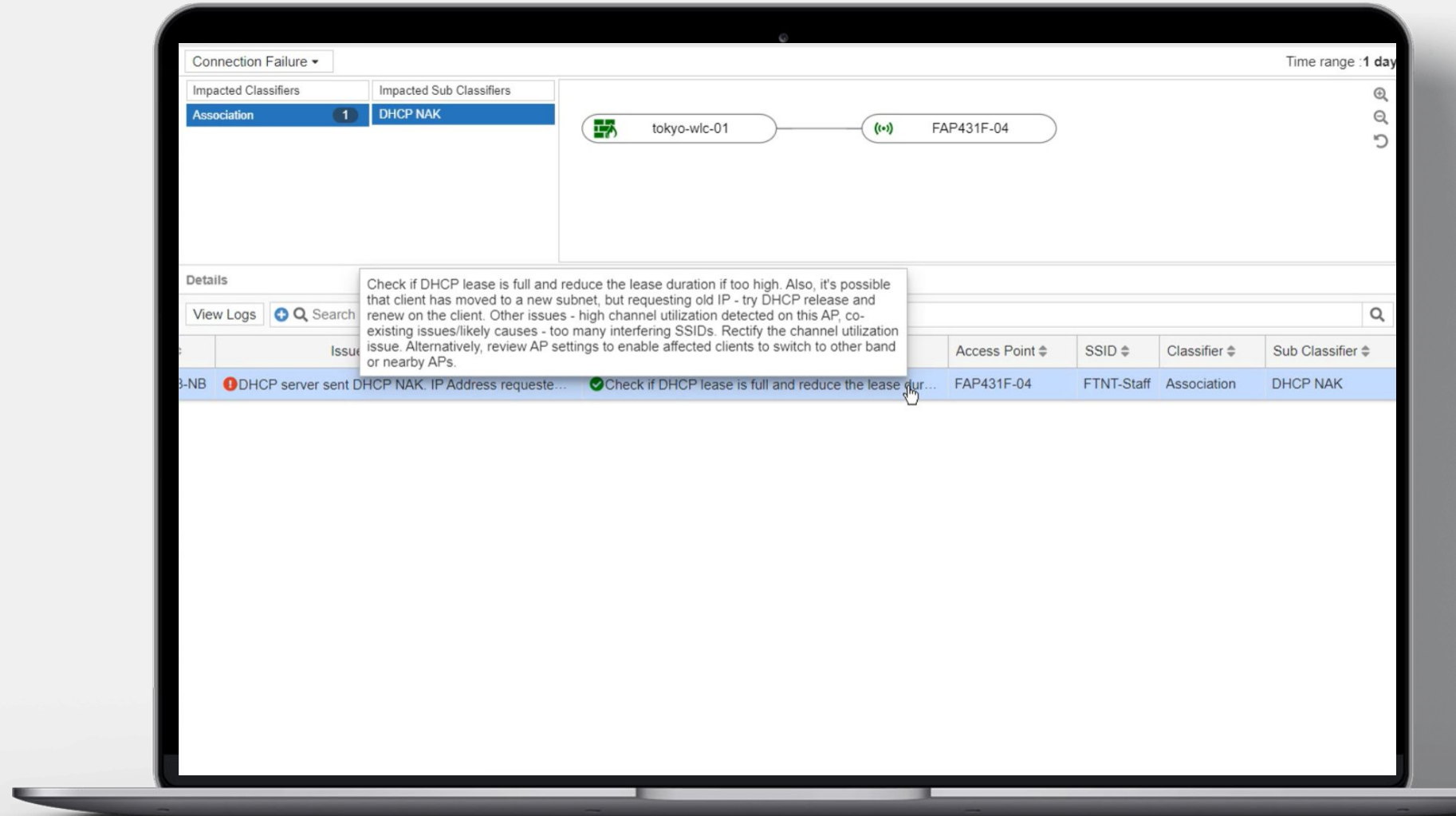
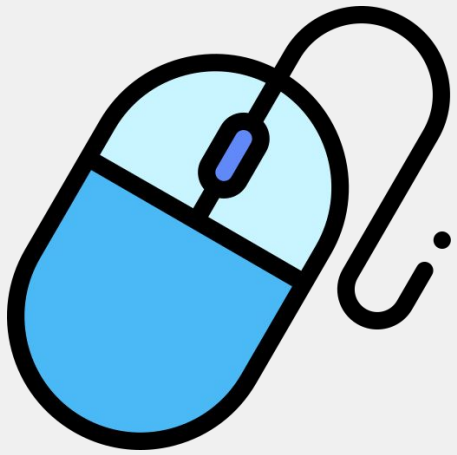


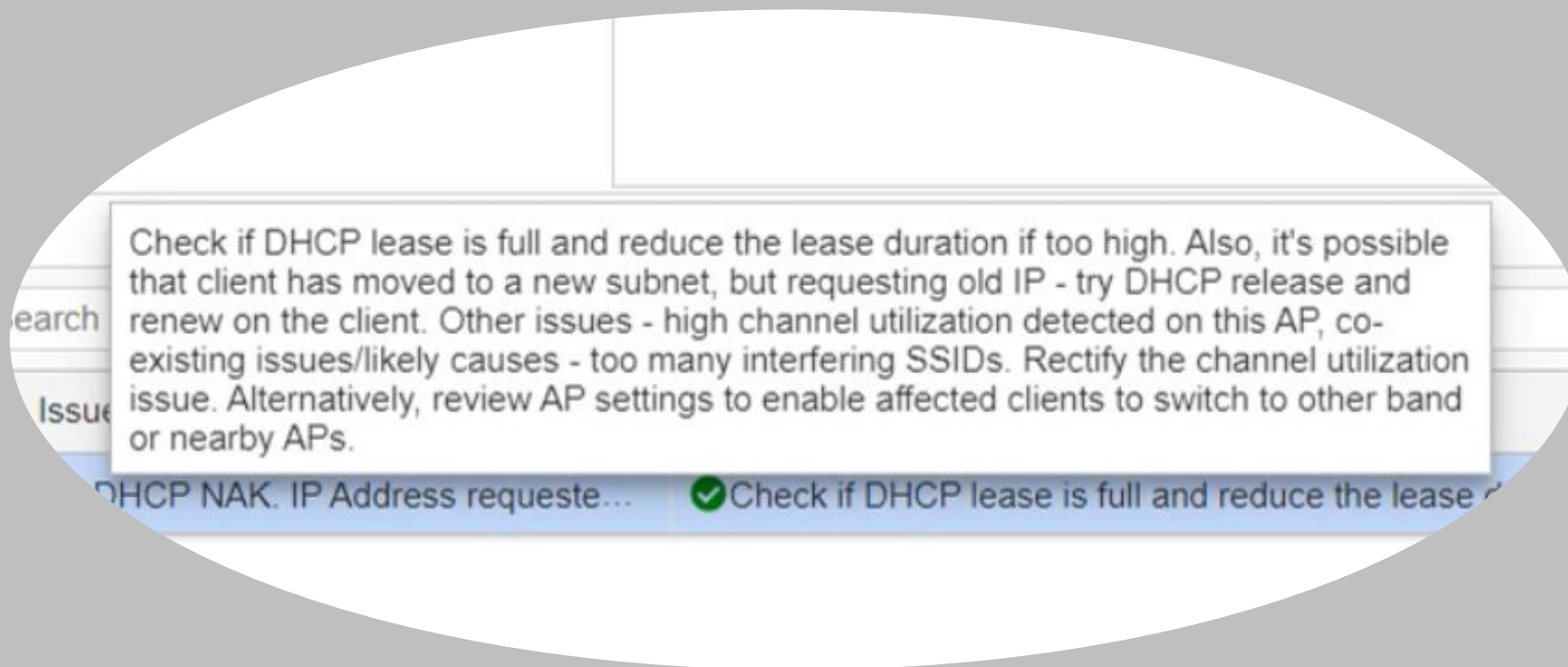


AI 自動判斷: DHCP 伺服器拒絕請求



- 利用 AI 提供解法





AI 自動判斷：檢查 DHCP 使用狀況，增加可配發的 IP 或調整 DHCP 租約期



如何利用 AI 解決問題

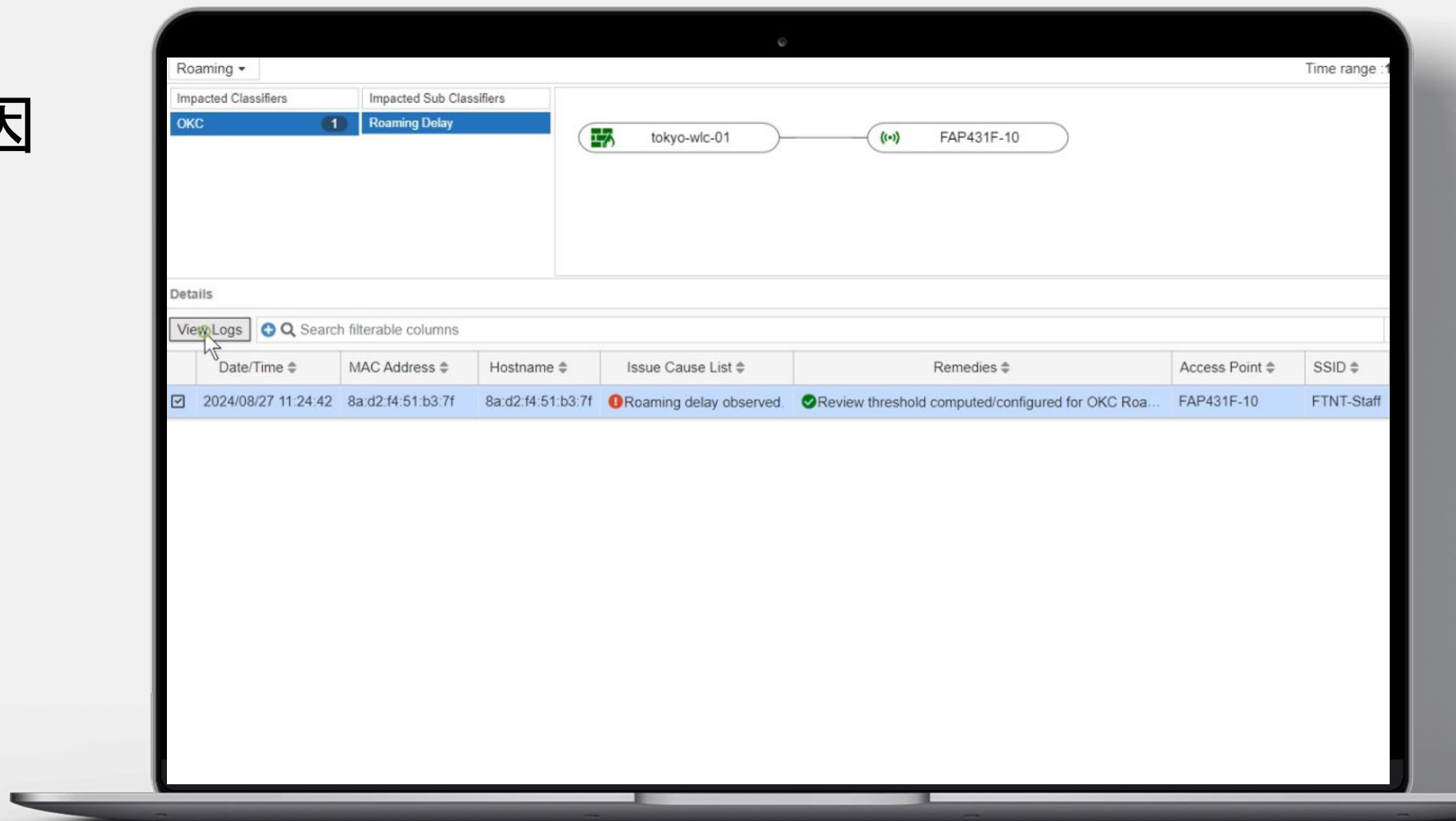
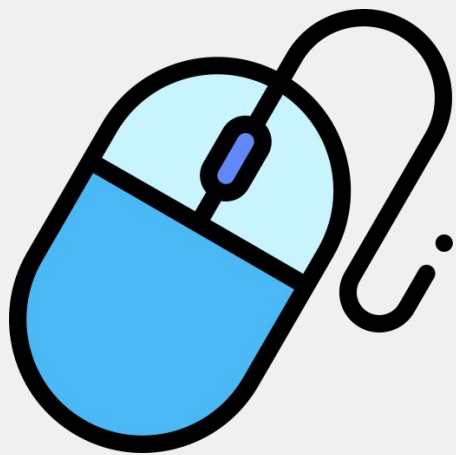


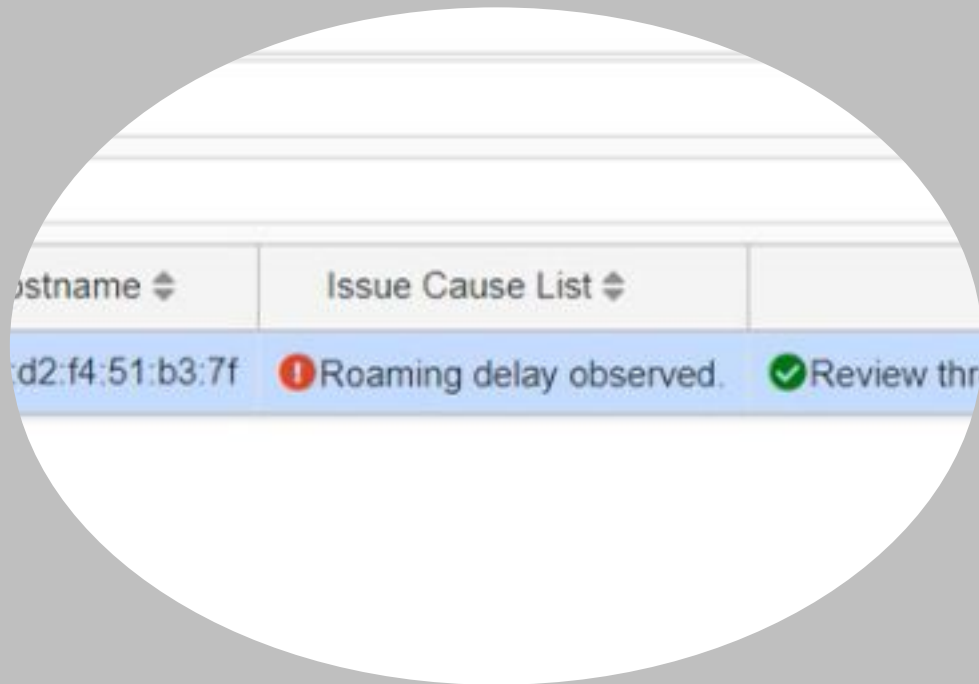
Marty：今天無線網路怪怪的!



您好，這裡是控八控控—控控控

• 透過 AI 判斷原因





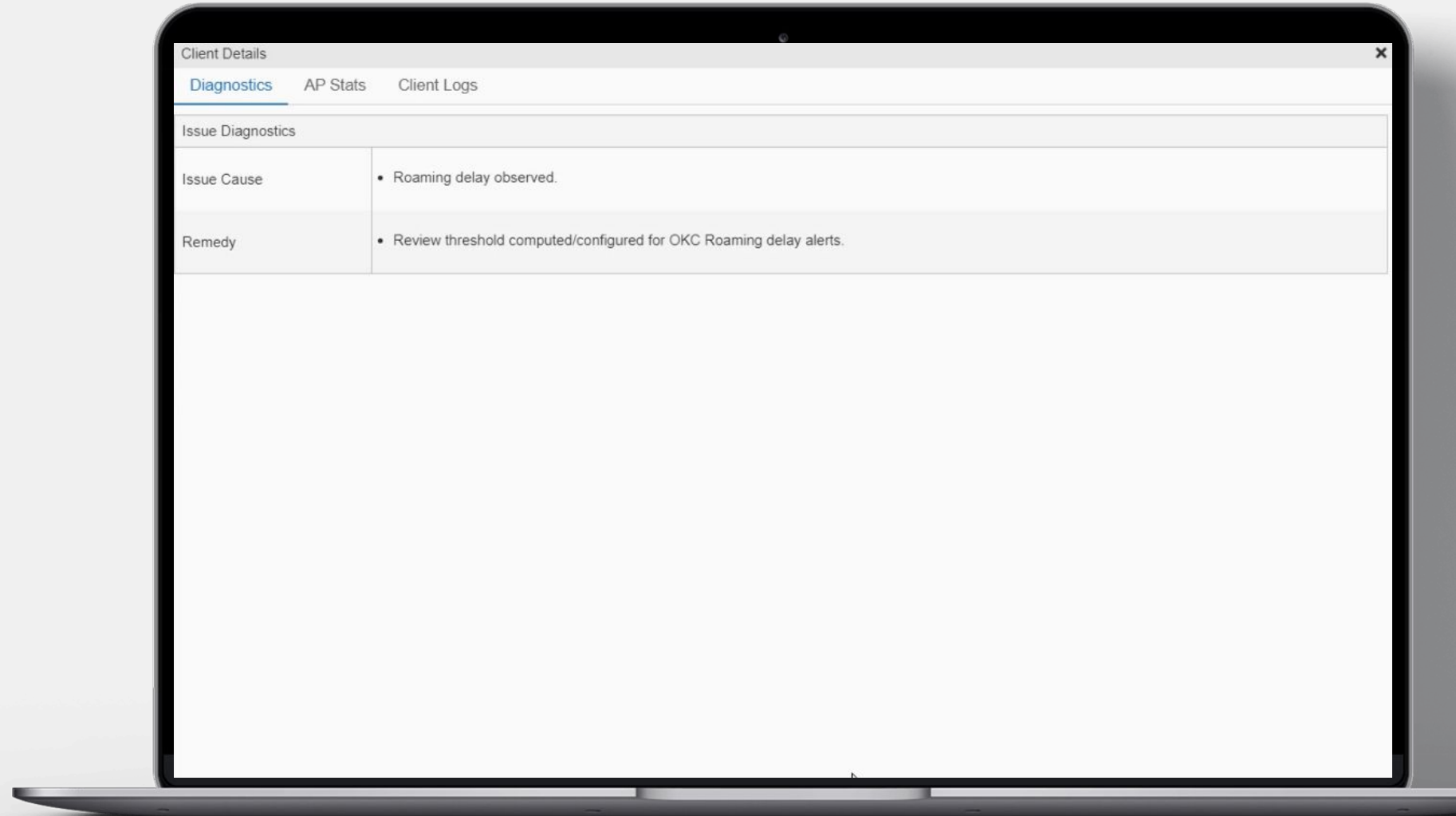
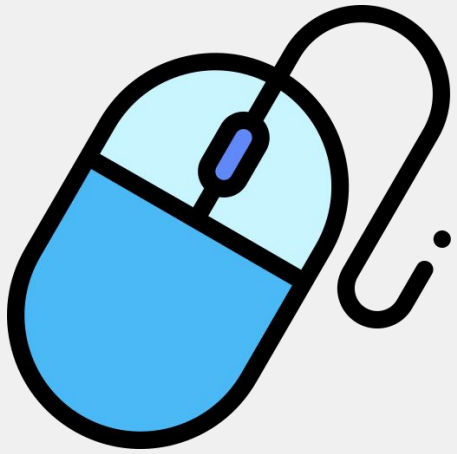
AI 自動判斷：無線漫遊發現異常



FortiAI Ops

找出無線網路漫遊問題

• 利用 AI 提供解法



- Review threshold computed/configured for OKC Roaming delay alerts.

AI 建議：檢查無線漫遊積極度設定



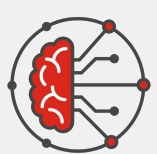
如何利用 AI 解決問題



Ella：今天無線卡卡的耶！



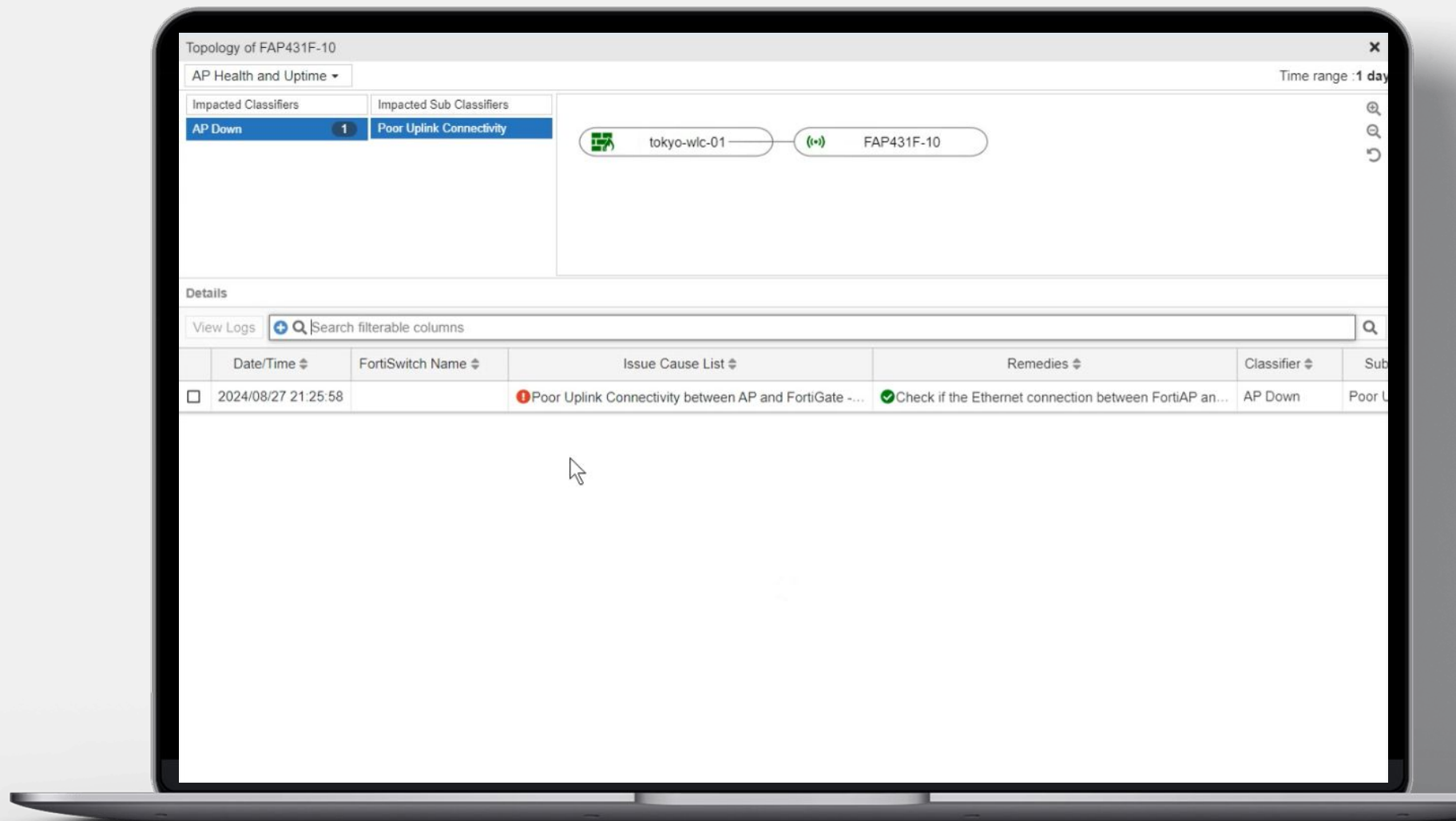
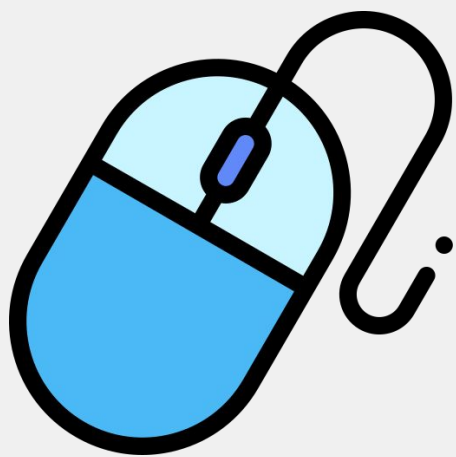
您好，這裡是控八控控—控控控



FortiAI Ops

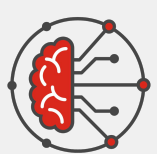
找出有線網路問題

- 透過 AI 判斷原因





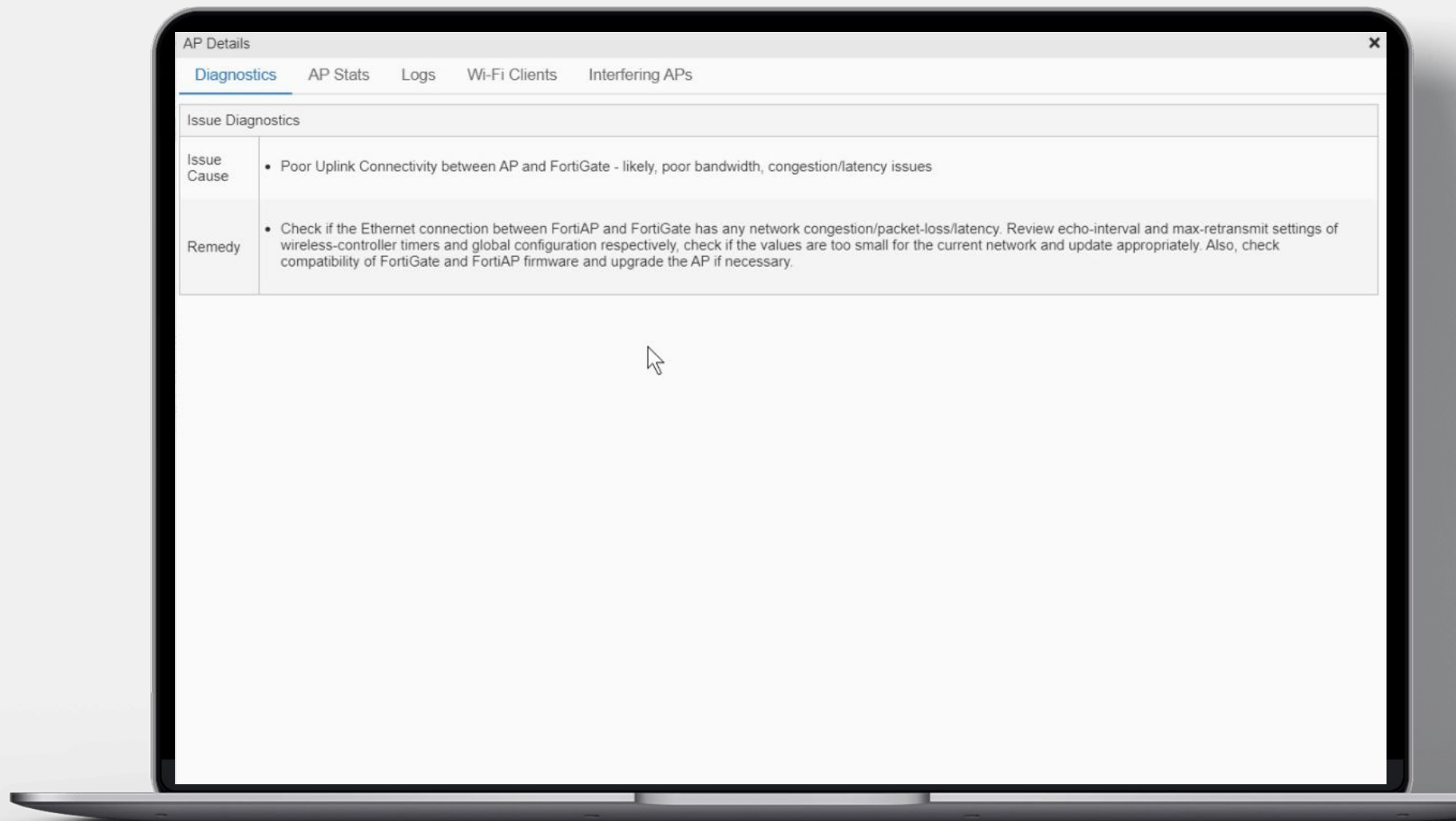
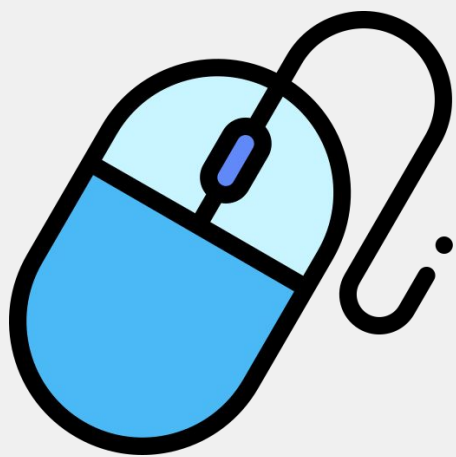
AI 自動判斷: AP 與控制器中間的線路不良



FortiAI Ops

找出有線網路問題

• 利用 AI 提供解法



Issue Diagnostics	
Issue Cause	• Poor Uplink Connectivity between AP and FortiGate - likely, poor bandwidth, congestion/latency issues
Remedy	• Check if the Ethernet connection between FortiAP and FortiGate has any network congestion/packet-loss/latency. Review echo-interval and max-retransmit settings of wireless-controller timers and global configuration respectively, check if the values are too small for the current network and update appropriately. Also, check compatibility of FortiGate and FortiAP firmware and upgrade the AP if necessary.

AI 建議：

檢查 AP 與控制器之間的交換器連線速率是否正常，有沒有封包遺失，AP 與控制器間的韌體是否匹配。



FortiAIOps

將 AI / 機器學習融入安全織網中



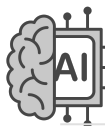
持續監控

- 趨勢分析 / 歷史基準線
- 網路流量可視化



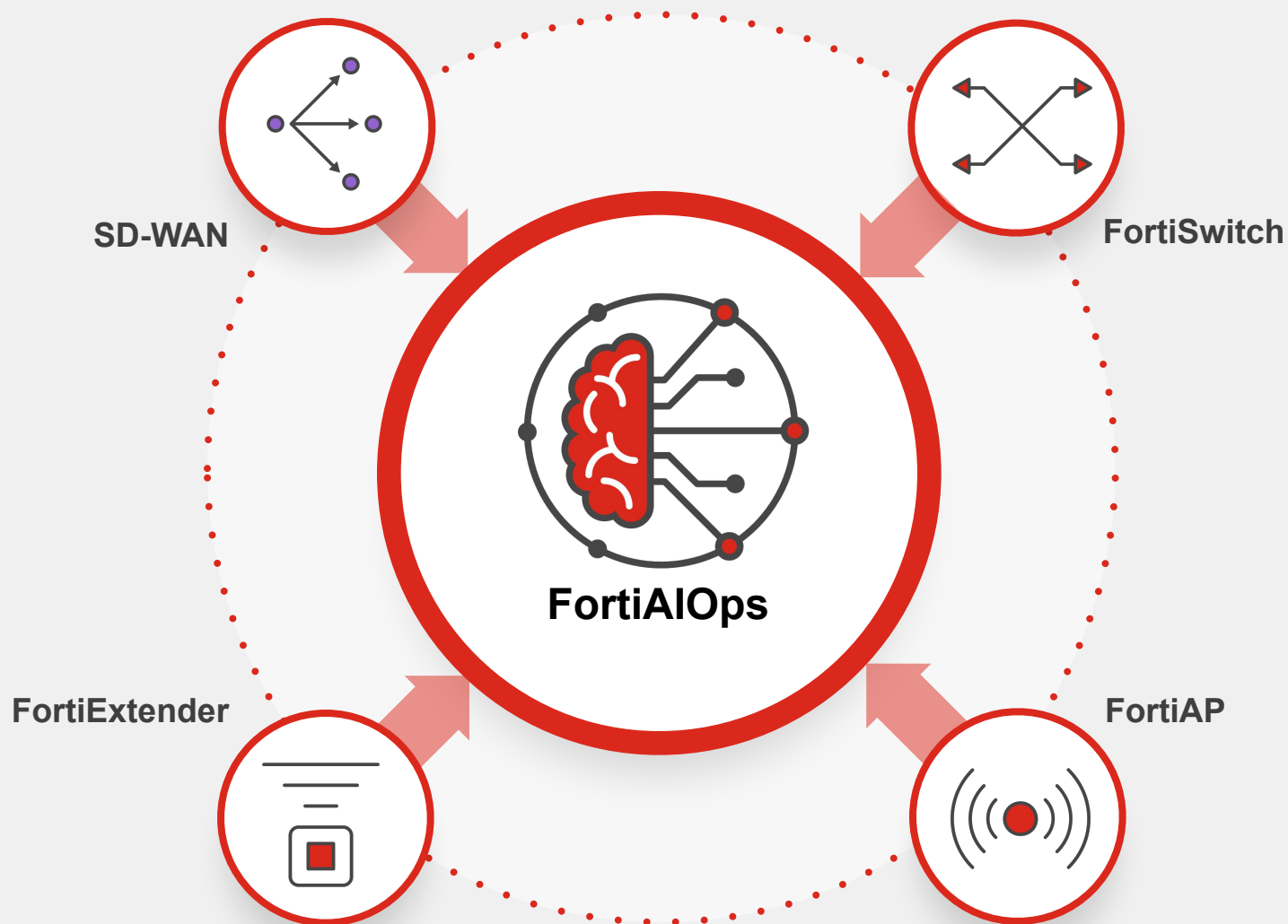
智能除錯

- 無線網路服務不中斷
- 無線網路頻譜分析
- 無線網路熱感圖
- 網路線品質測試
- 視訊軟體品質監控



AI / 機器學習

- 動態學習網路品質曲線
- 問題判斷與分類
- 建議改善措施



FORTINET[®]