智慧 AI 防護與管理，全面提升資安營運效率

李尚峰 Jarvis Lee

Fortinet 業務協理

ljarvis@fortinet.com

FortiOS 8.0

FortiOS 8 強化 FortiGate，更勝以往

FortiOS 8 強化 FortiGate，更勝以往

持續強化平台能力，回應未來安全挑戰

AI 應用治理

提升企業對新型 AI 應用的可視性與控管能力。

AI 應用管理：
MCP 控制、GenAI 應用管理

資料保護升級

將資料防護延伸至截圖、圖片與掃描文件。

資料外洩防護：
結合 OCR 的 DLP 偵測能力

簡化維運管理

加快問題定位，降低多環境管理複雜度。

智慧維運：
FortiAI-Assist

迎向未來安全

提前因應未來加密演進與長期安全需求。

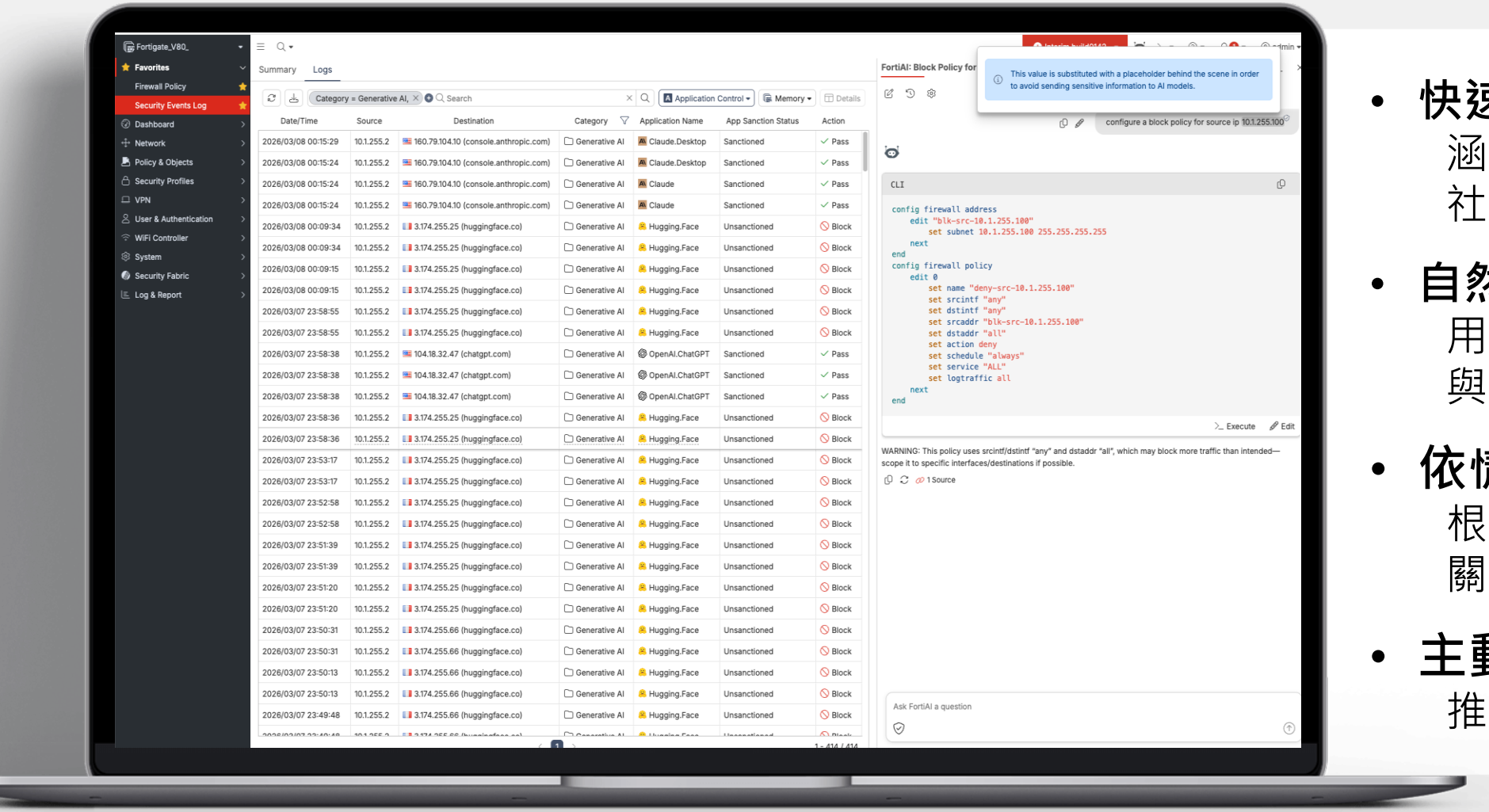
未來韌性：
量子安全強化能力

FortiAI：下一代資安營運的新助手

讓安全團隊更快理解、更快決策、更快行動

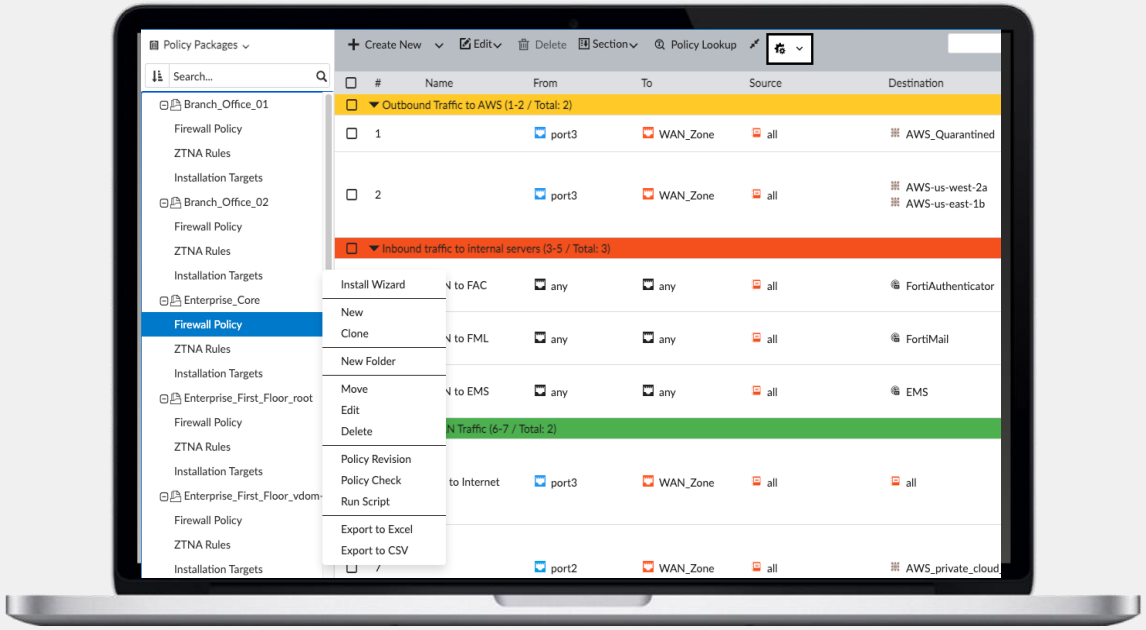
AI 正在成為
現代資安營運流程的一部分

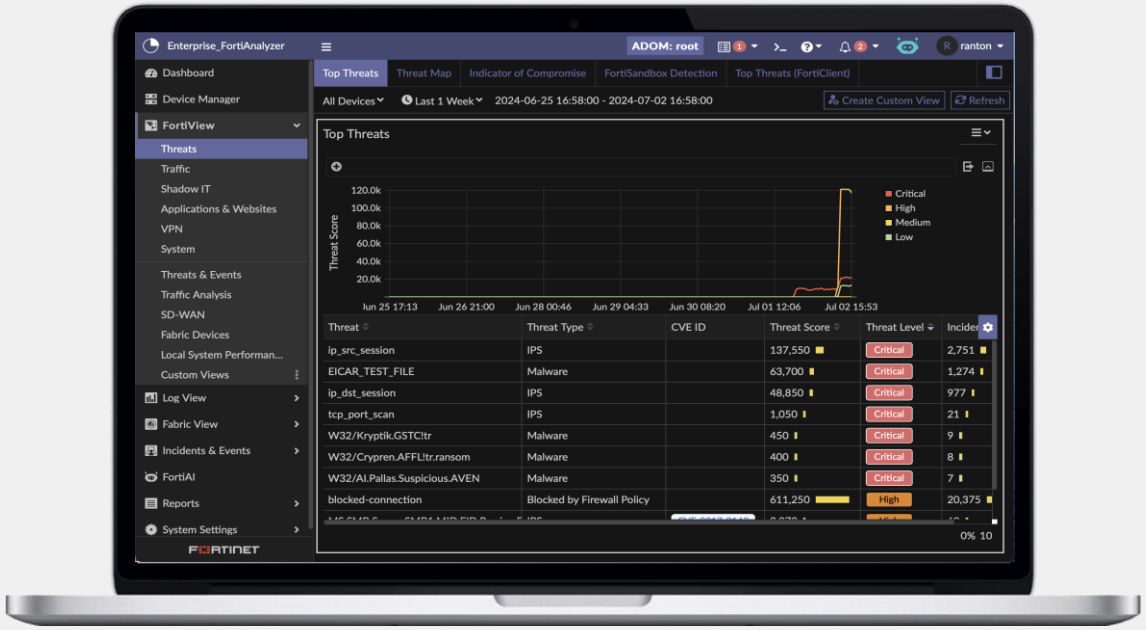
FortiAI 協助你更快掌握 FortiGate



- **快速掌握產品知識**
  涵蓋技術文件、知識庫與社群文章
- **自然語言直接提問**
  用更直覺的方式取得答案與建議
- **依情境提供回應**
  根據目前頁面內容給出相關資訊
- **主動帶出後續方向**
  推薦相關問題與知識文章

每台強大防火牆背後，都有強大的管理與分析





防火牆管理

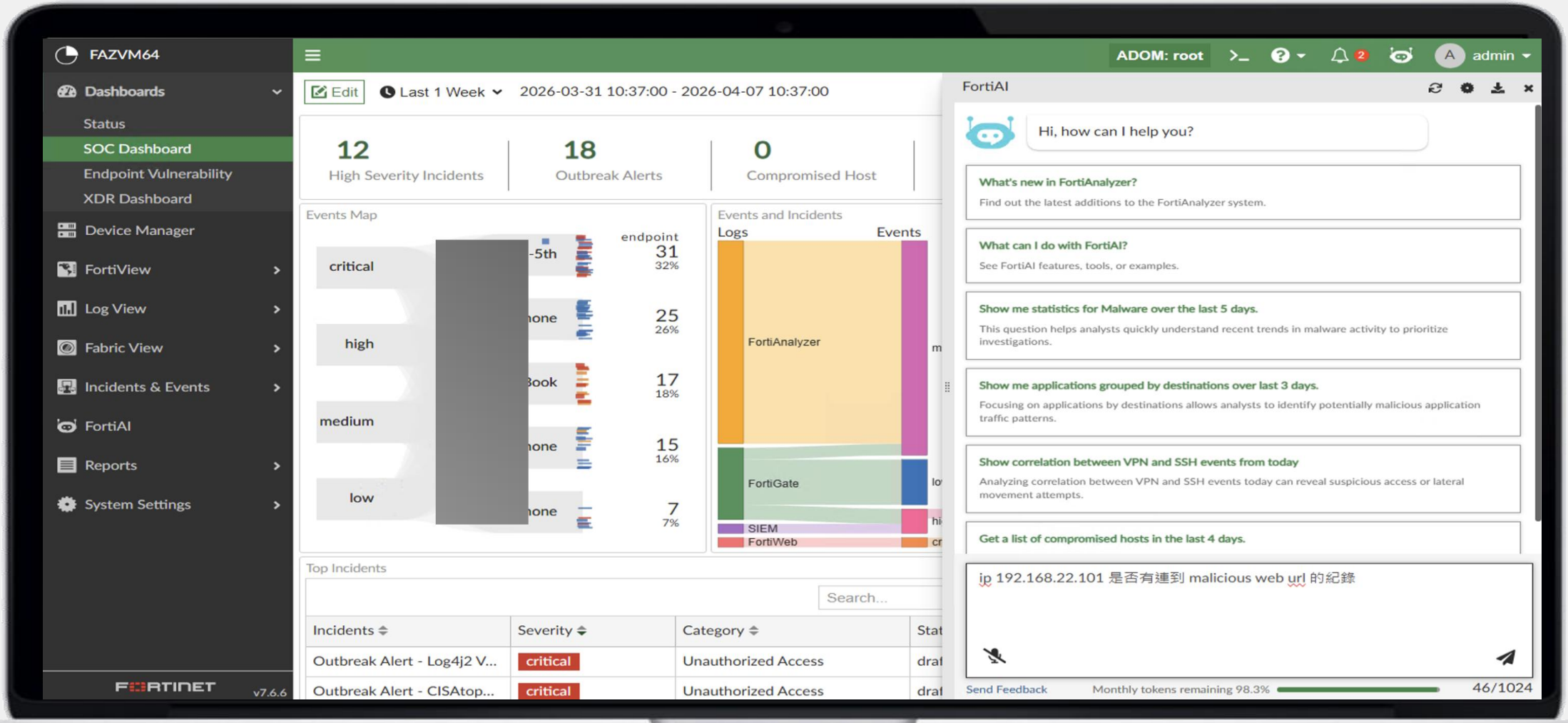
集中化、規模化的管理所有設備，讓所有設備的變更、佈署更快速、更一致、更安全。

安全維運分析

集中日誌、事件關聯與自動化分析，讓威脅更快被看見、問題更快被處理。

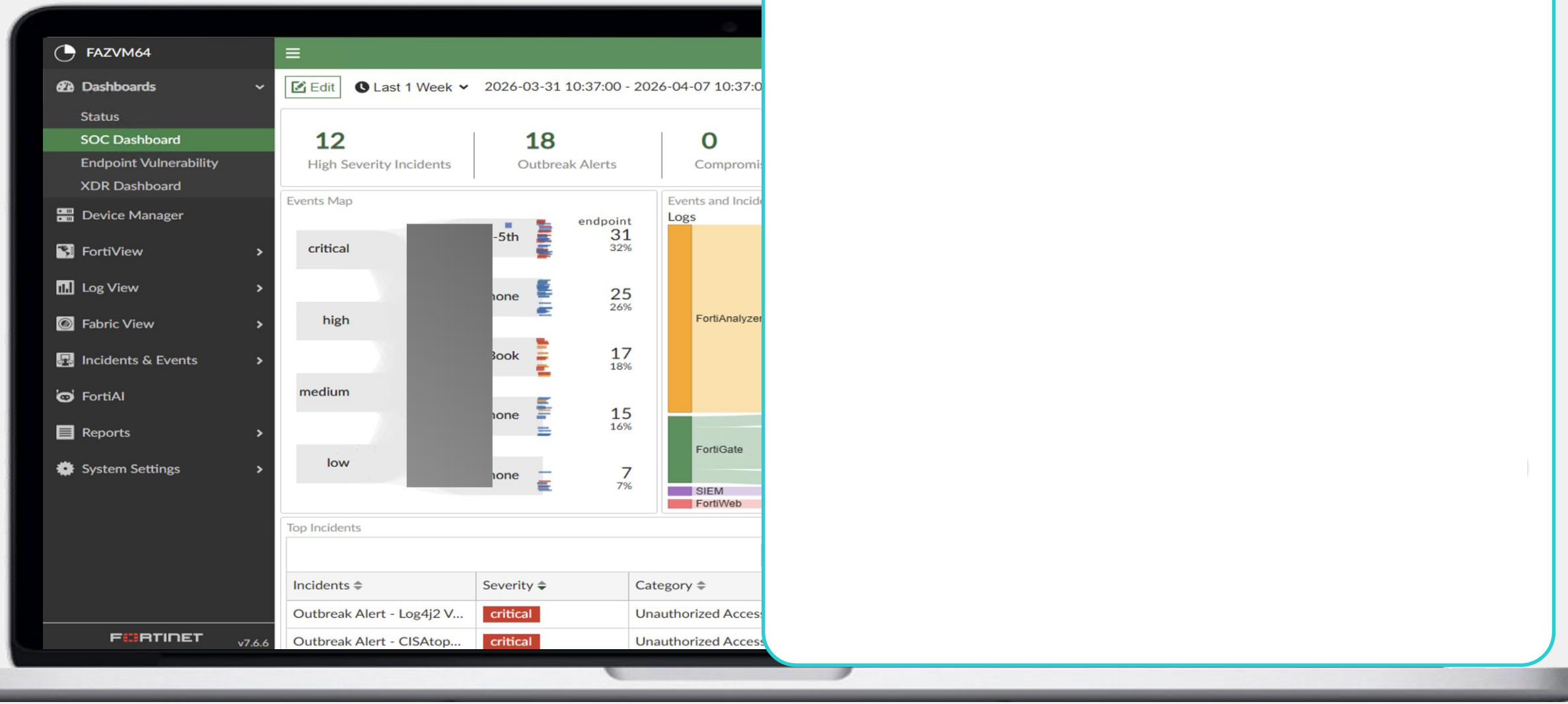
FortiAI on FortiAnalyzer

透過自然語言互動應答，即時解析資安事件



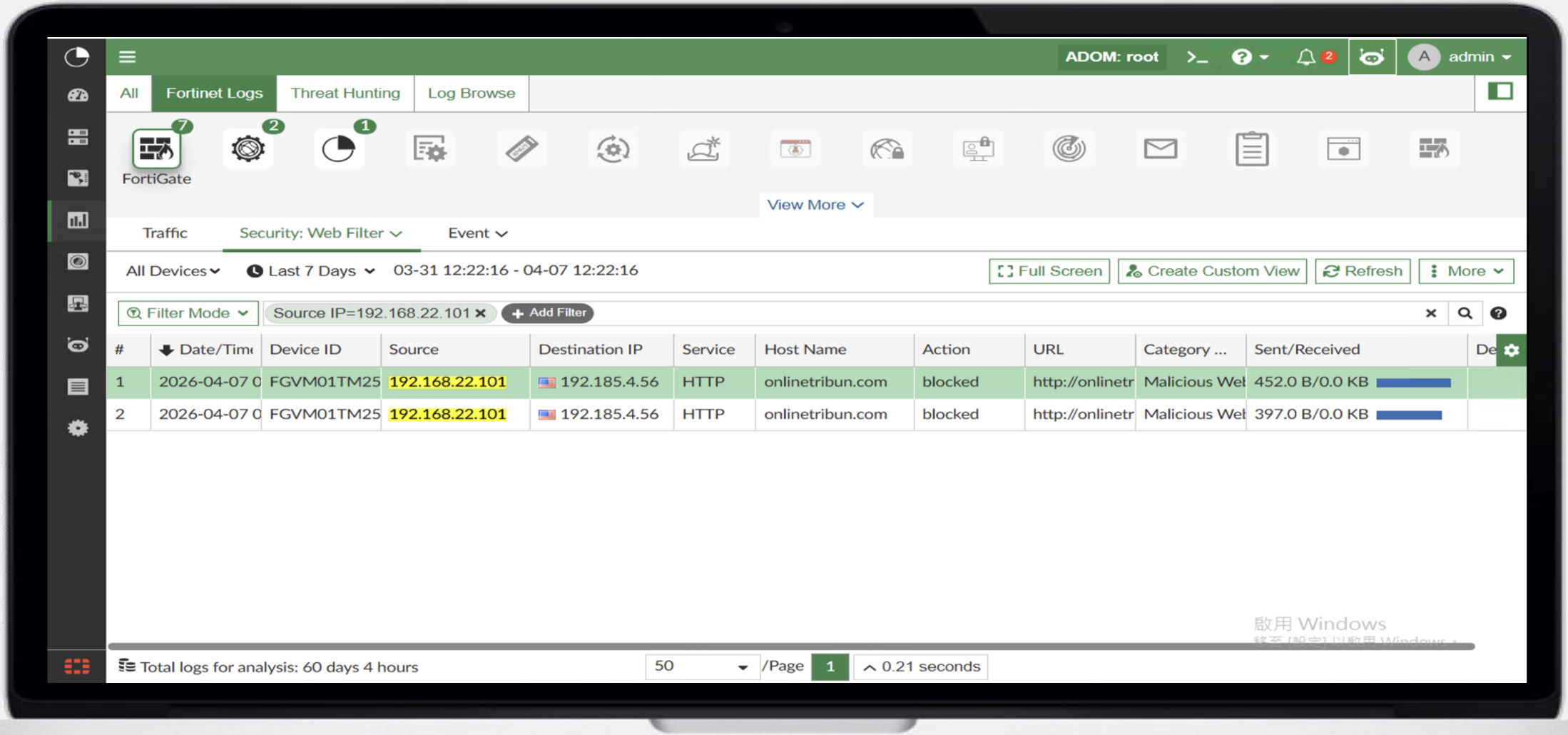
FortiAI on FortiAnalyzer

透過自然語言互動應答，即時解析資安事件



FortiAI on FortiAnalyzer

透過自然語言互動應答，即時解析資安事件

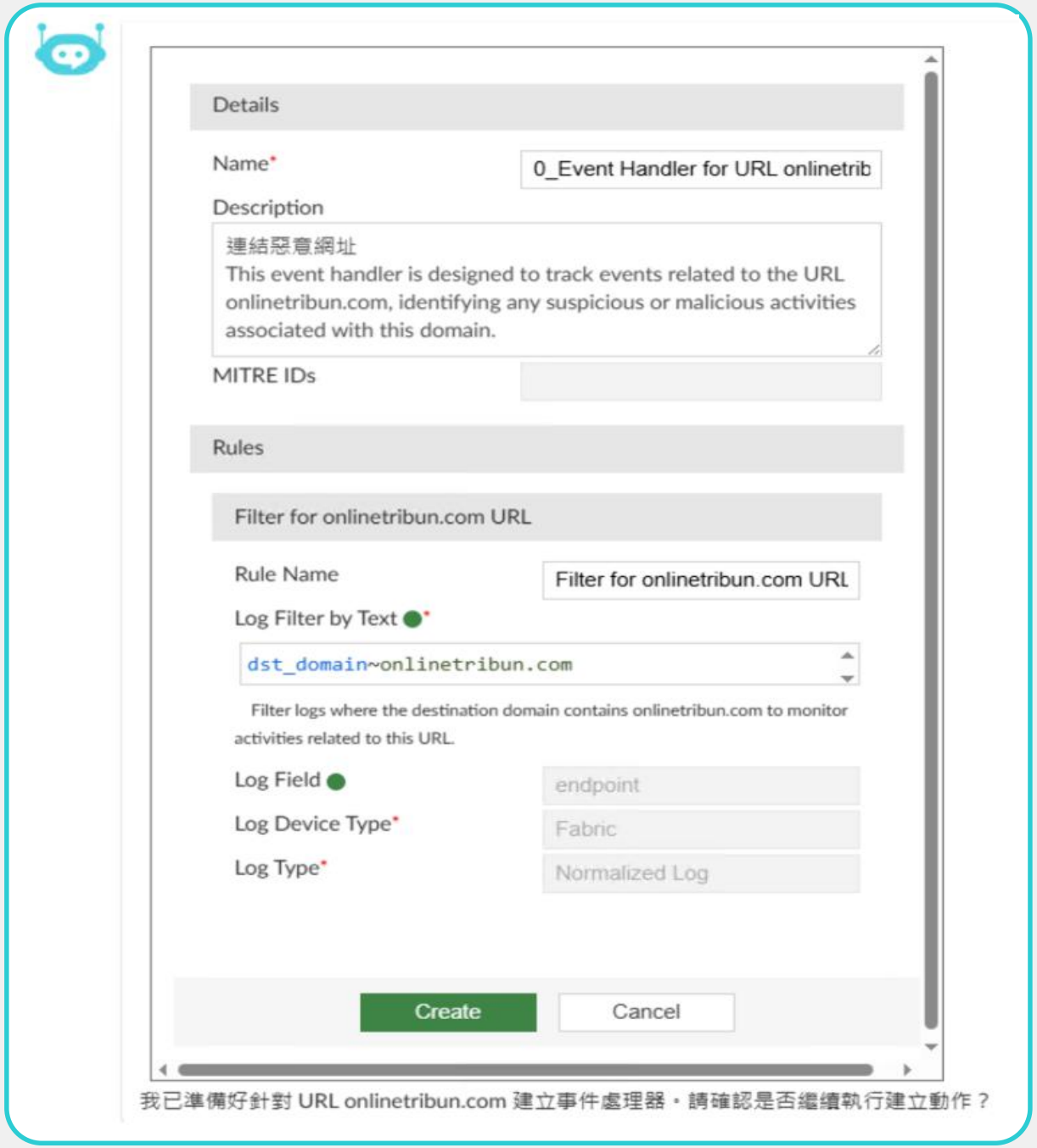


FortiAI on FortiAnalyzer

透過自然語言互動應答**產生自動化規則**

FortiAI on FortiAnalyzer

透過自然語言互動應答產生自動化規則

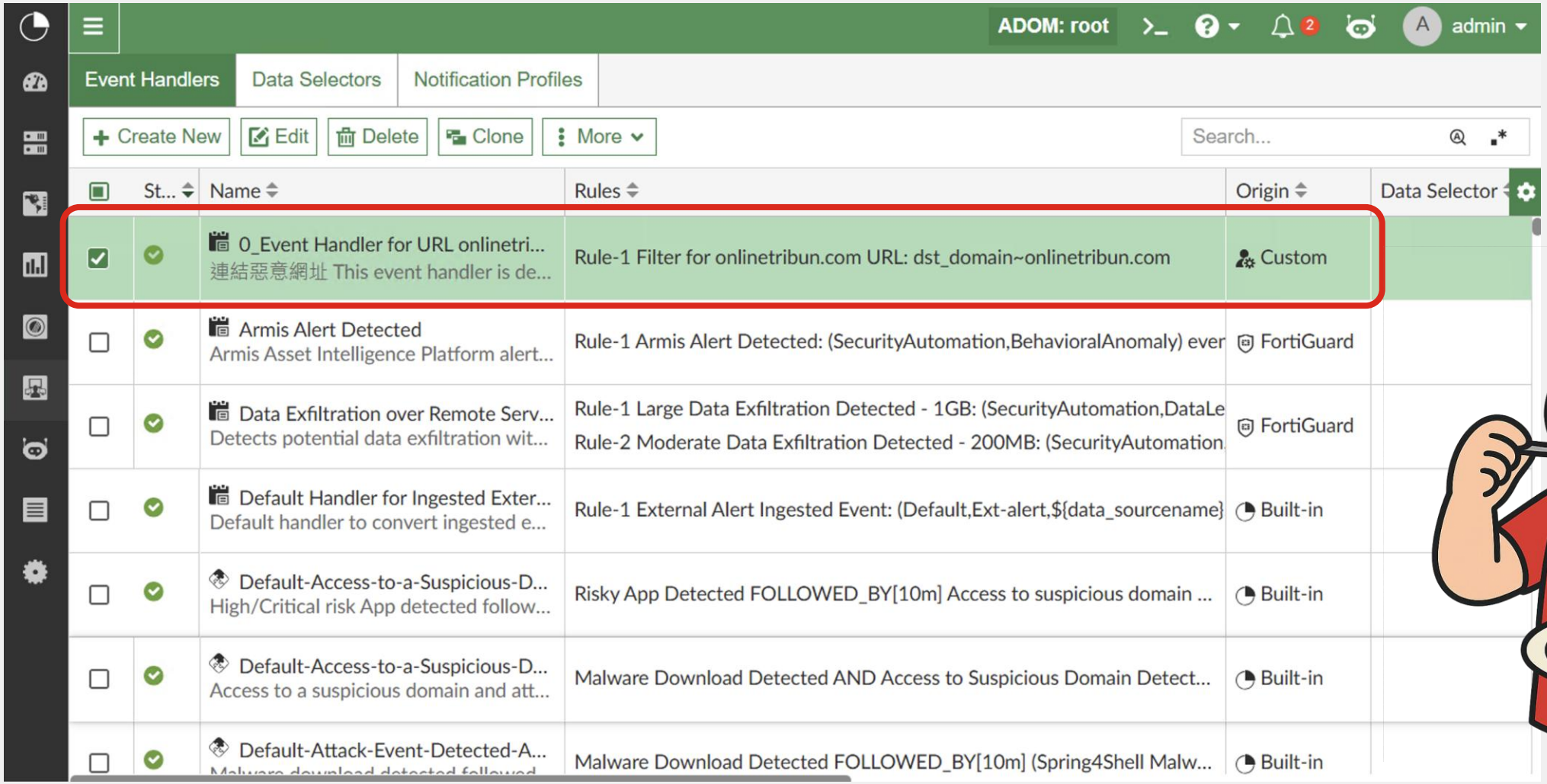


FortiAI on FortiAnalyzer

透過自然語言互動應答**產生自動化規則**

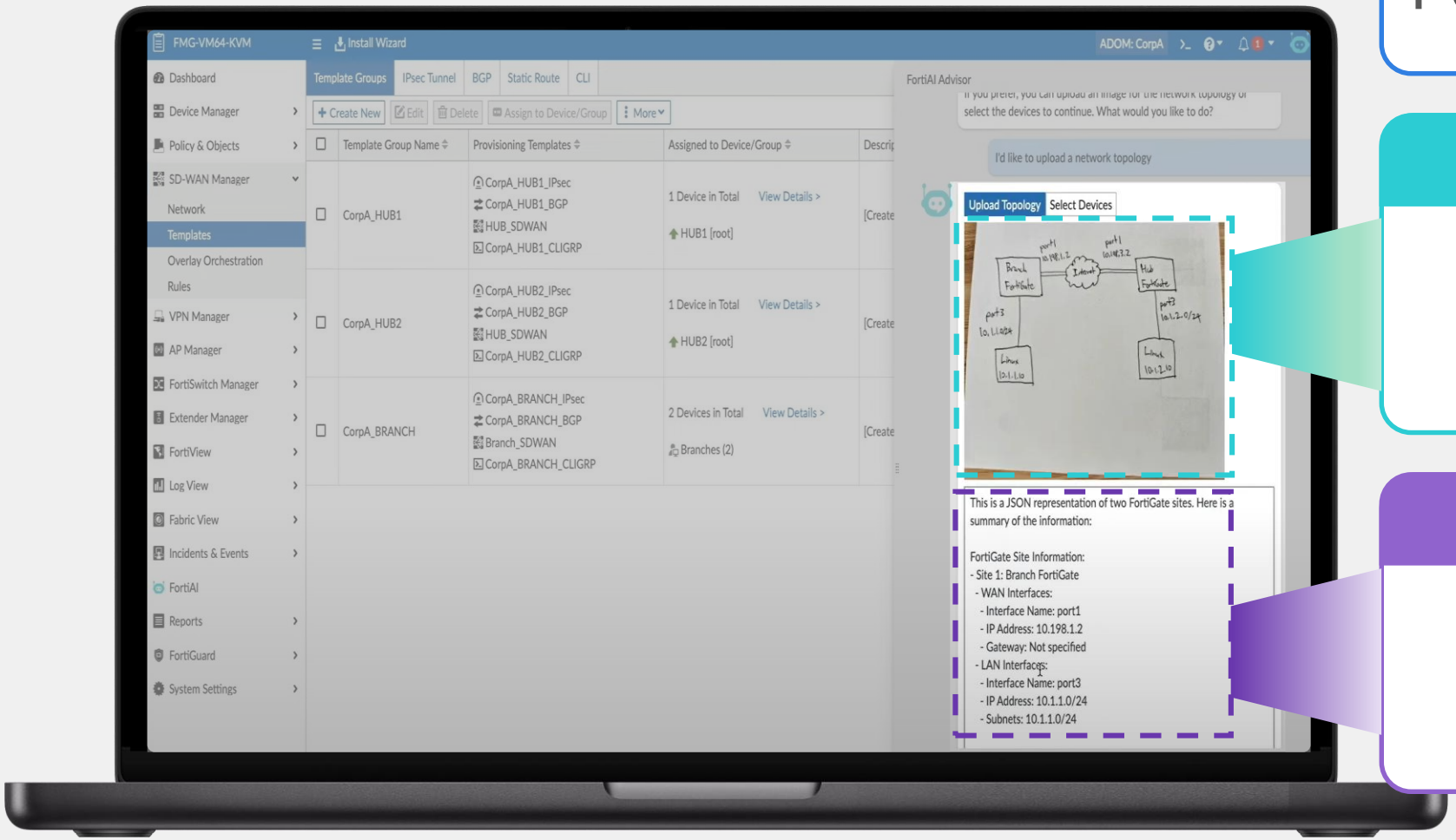
FortiAI on FortiAnalyzer

透過自然語言互動應答產生自動化規則



AI 智能管理

FortiAI on FortiManager – 簡化複雜設定



FortiAI 可以幫忙的

只要你會畫圖！
FortiAI 就能幫你做設定！

FortiAI 看到的

看到的
手繪 VPN 架構圖

FortiAI 理解的

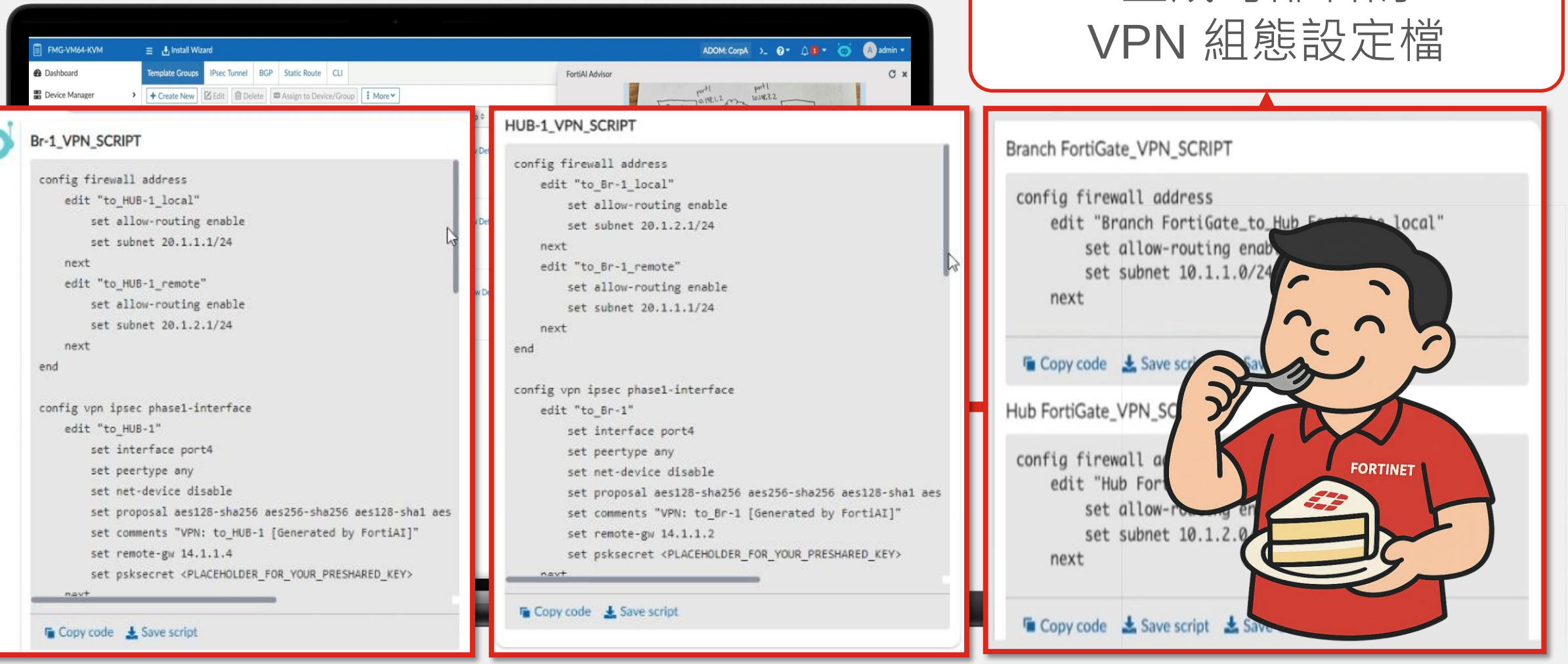
VPN 網路架構
並請求確認

AI 智能管理

FortiAI on FortiManager – 簡化複雜設定

FortiAI 生成的

生成可部署的
VPN 組態設定檔



因應 CNSA 2.0 合規要求：企業應及早啟動量子轉型

核心安全挑戰

非對稱加密瓦解風險

量子電腦利用特定演算法（如 Shor Algorithm）可實現快速破解，導致現行 RSA 與 ECC 體系失去保護作用。

資訊截收威脅 (HNDL)

駭客採行「現在擷取，稍後解密」模式，針對具長效價值之加密資訊進行預先竊取，待技術成熟後破解。

法規遵循與加密敏捷性

企業系統需建立「加密敏捷性」，以應對不斷演進的量子攻擊，並符合國家級安全採購標準。

CNSA 2.0 合規路線圖

2027 啟動 PQC 採購規範

所有新採購之國家安全系統 (NSS) 必須全面支援後量子加密 (PQC) 演算法與相關標準。

2030 傳統技術淘汰期

正式停止對 RSA、ECDSA、EdDSA 等傳統非對稱密碼技術的使用，現有系統需完成初步遷移。

2035 合規完成

所有關鍵基礎架構完成 PQC 轉型，傳統加密技術全面退役，達成全域量子抗性。

* CNSA 2.0 標準由美國國安局 (NSA) 發佈

Fortinet 企業量子安全無縫接軌

量子金鑰分配（QKD）：

透過 QKD 供應商實現量子安全的金鑰交換機制。

後量子加密（PQC）：

FortiOS 內建演算法包含 Crystals Kyber、ML-KEM、BIKE、HQC 和 Frodo 等。

混合模式：

傳統公鑰與後量子加密並存，支援企業現有系統的相容性與量子遷移優勢。

演算法堆疊：

結合多種加密演算法，以創造更有韌性的安全解決方案。

Post-Quantum Cryptography

Quantum-resistant key exchange method

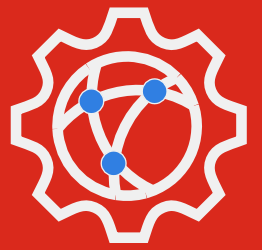
Post Quantum Cryptography Additional Key Exchanges

+ Create new | Edit | Delete

Transform type	KE groups
ADDKE1	ML-KEM-768
ADDKE2	HQC192

FortiWeb 8.0

FortiWeb 8.0 導入 Model Context Protocol（MCP）安全防護功能

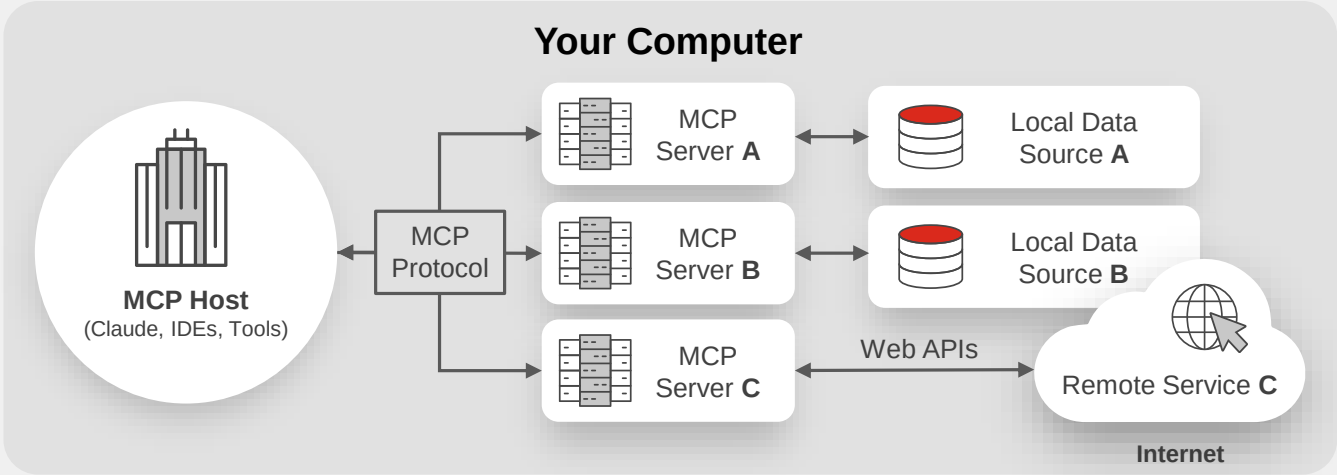


大型語言模型防護 – MCP 防護

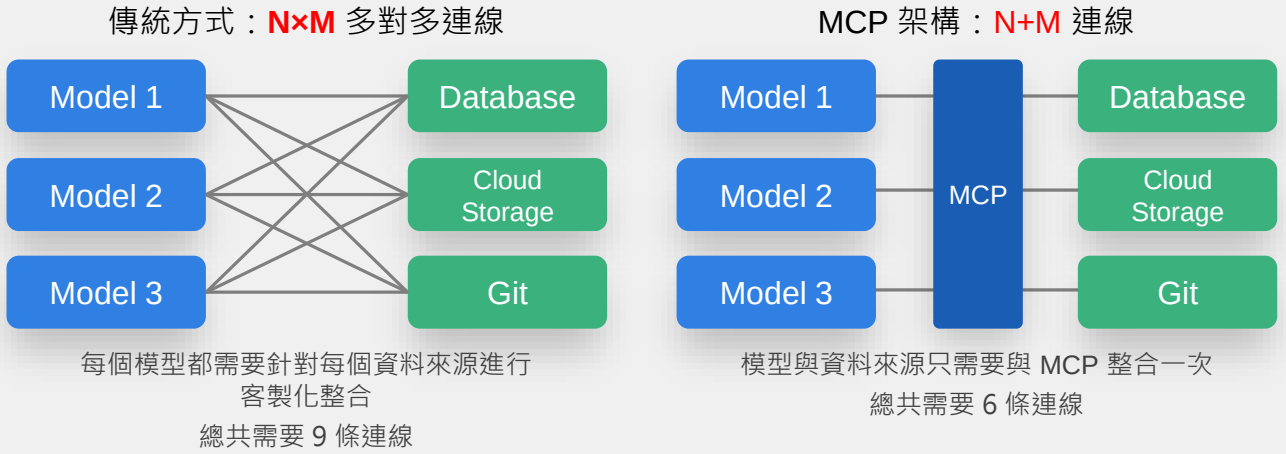
Model Context Protocol

Model Context Protocol

- Anthropic 於 2024 年 11 月推出 MCP（Model Context Protocol，模型上下文協定）開放標準，讓 LLM 應用能以標準化、模組化的方式連接外部工具、資料來源與服務。
- 它取代了過去針對特定任務所撰寫的靜態、狹隘、專用型整合方式。
- 模型與資料來源只需要與 MCP 整合一次。
- LLM 現在可以在複雜環境中自主執行操作，但若缺乏防護，也可能帶來風險。
- MCP Protection 是 LLM 防護拼圖中的另一個重要環節。



傳統整合方式 vs MCP 架構



大型語言模型防護 – MCP 防護

Model Context Protocol

MCP 的快速演進，也創造出一個全新且複雜的攻擊面。

提示詞注入與工具污染攻擊

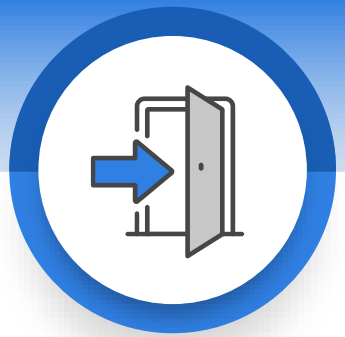
攻擊者將惡意指令藏在 MCP 工具描述中，誘導 AI 執行危險操作。

例如：查完客戶資料後，自動寄到外部信箱。

供應鏈攻擊風險

MCP 是開源，攻擊者可能發布假套件，誘導開發者安裝。

例如：偽裝成 Gmail MCP 工具，實際偷取郵件或憑證。



架構本身的安全漏洞

MCP 工具若權限過大，攻擊者可能藉此存取不該看的資料或系統。

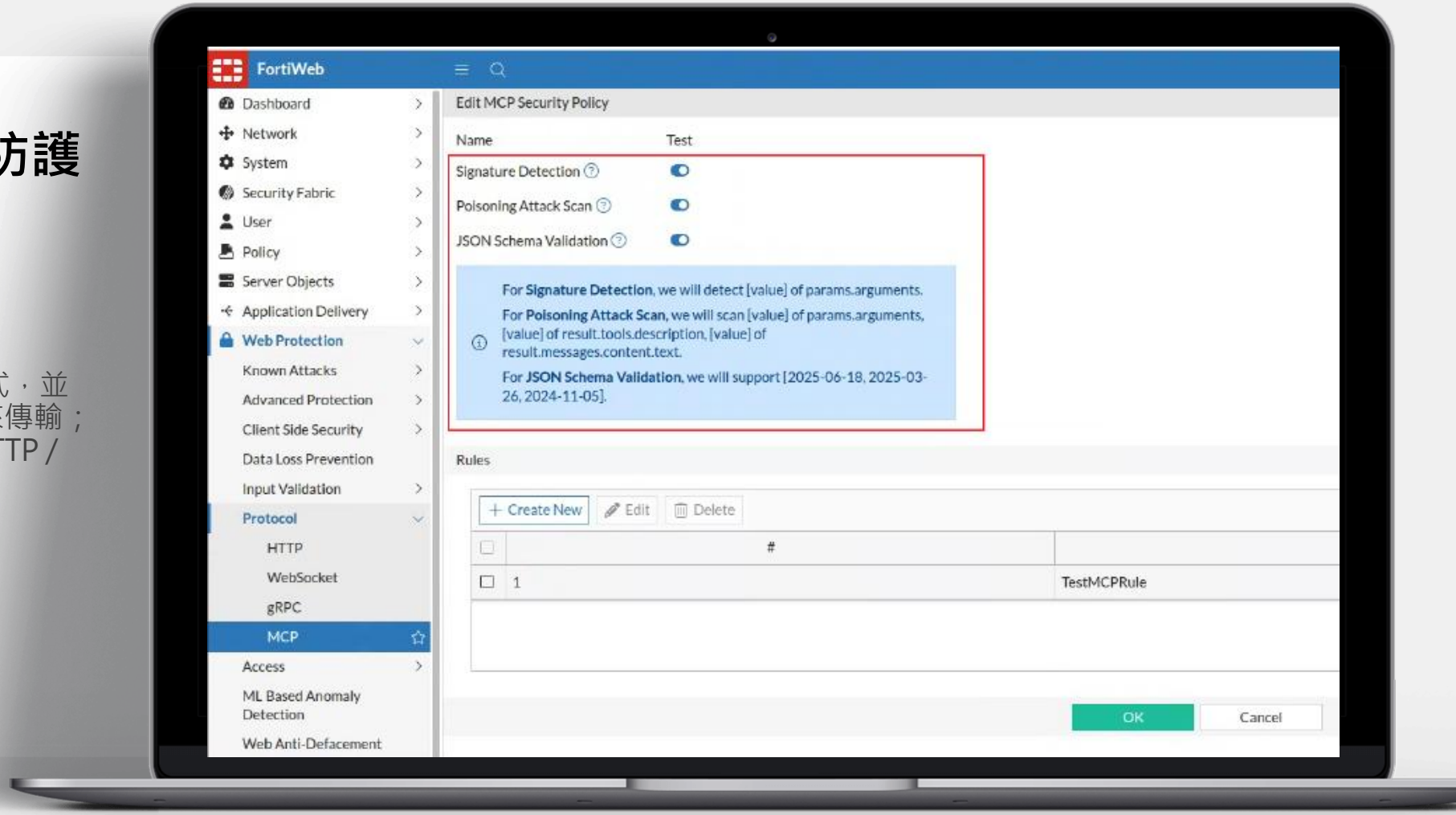
例如：原本只需讀取行事曆，卻被授予修改與刪除會議的權限。

大型語言模型防護 – MCP 防護

Model Context Protocol

FortiWeb 提供的安全防護

- FortiWeb 8.0 導入 MCP 協定支援
  - Model Context Protocol
- MCP 使用 JSON-RPC 作為訊息格式，並可透過 Streamable HTTP 或 SSE 來傳輸；FortiWeb 主要針對 Streamable HTTP / SSE 型態的 MCP 流量做即時檢查。
- FortiWeb 安全防護能力包含：
  - 惡意特徵偵測
  - 工具污染攻擊防護
  - JSON 格式與結構驗證



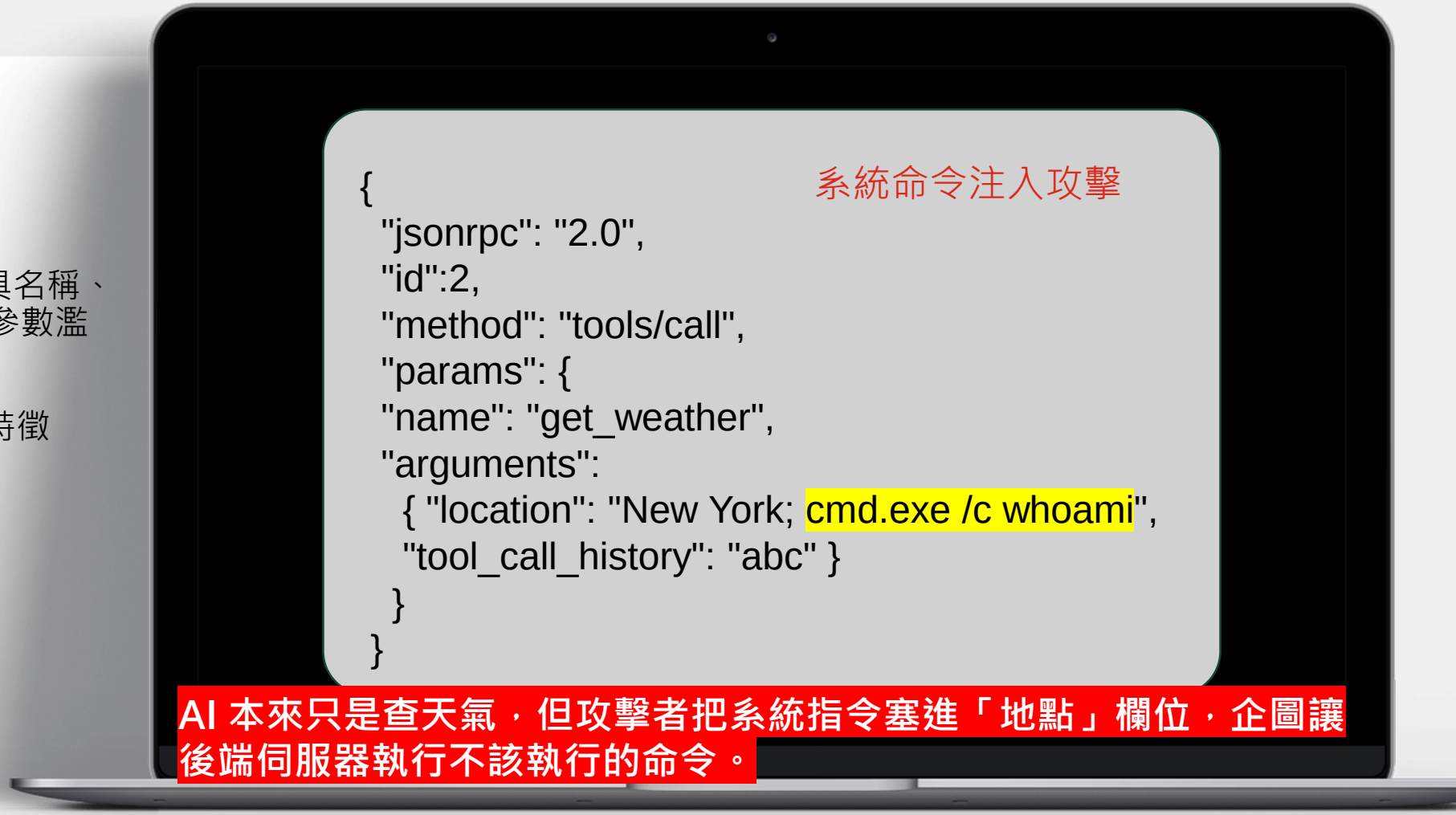
大型語言模型防護 – MCP 防護

Model Context Protocol

惡意特徵偵測

偵測 MCP 呼叫中的危險方法、工具名稱、參數與內容，防止指令注入、工具參數濫用與已知攻擊特徵。

- 掃描 MCP 訊息，偵測已知攻擊特徵
- 防止伺服器端指令注入攻擊
- 降低潛在安全漏洞被利用的風險
- 提供即時威脅偵測能力
  - 由 FortiGuard 持續更新特徵碼



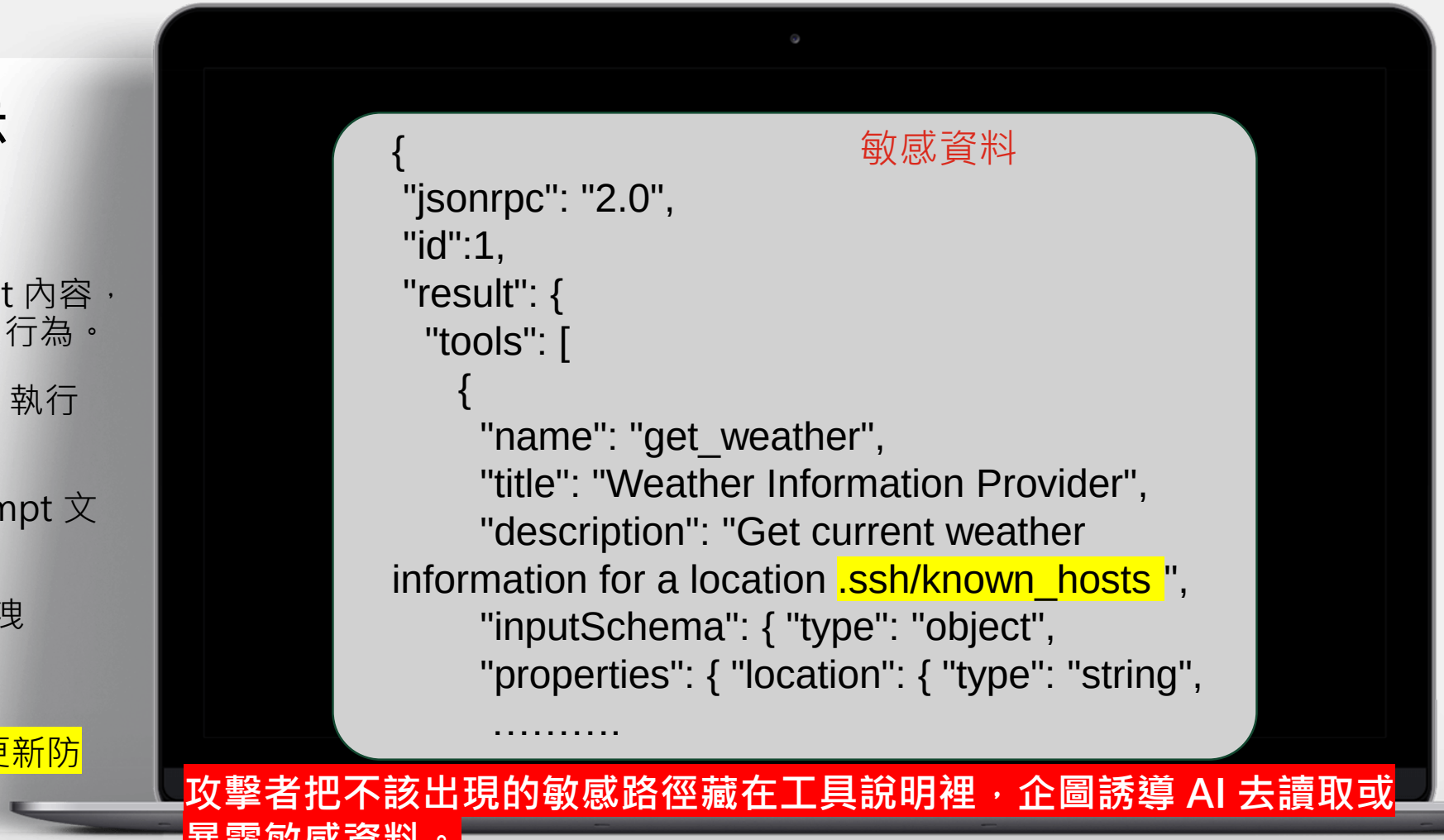
大型語言模型防護 – MCP 防護

Model Context Protocol

MCP 工具描述與提示詞污染防護

分析工具描述、工具參數與 Prompt 內容，防止攻擊者透過惡意指令操控 LLM 行為。

- 防止 LLM 被惡意 Prompt 誘導，執行非法或非預期操作
- 檢查工具參數、工具描述與 Prompt 文字內容
- 保護敏感資訊，避免遭竊取或外洩
- 維持 AI 系統的可信度與安全性
- 由新的 FortiGuard 資料庫持續更新防護能力



攻擊者把不該出現的敏感路徑藏在工具說明裡，企圖誘導 AI 去讀取或暴露敏感資料。

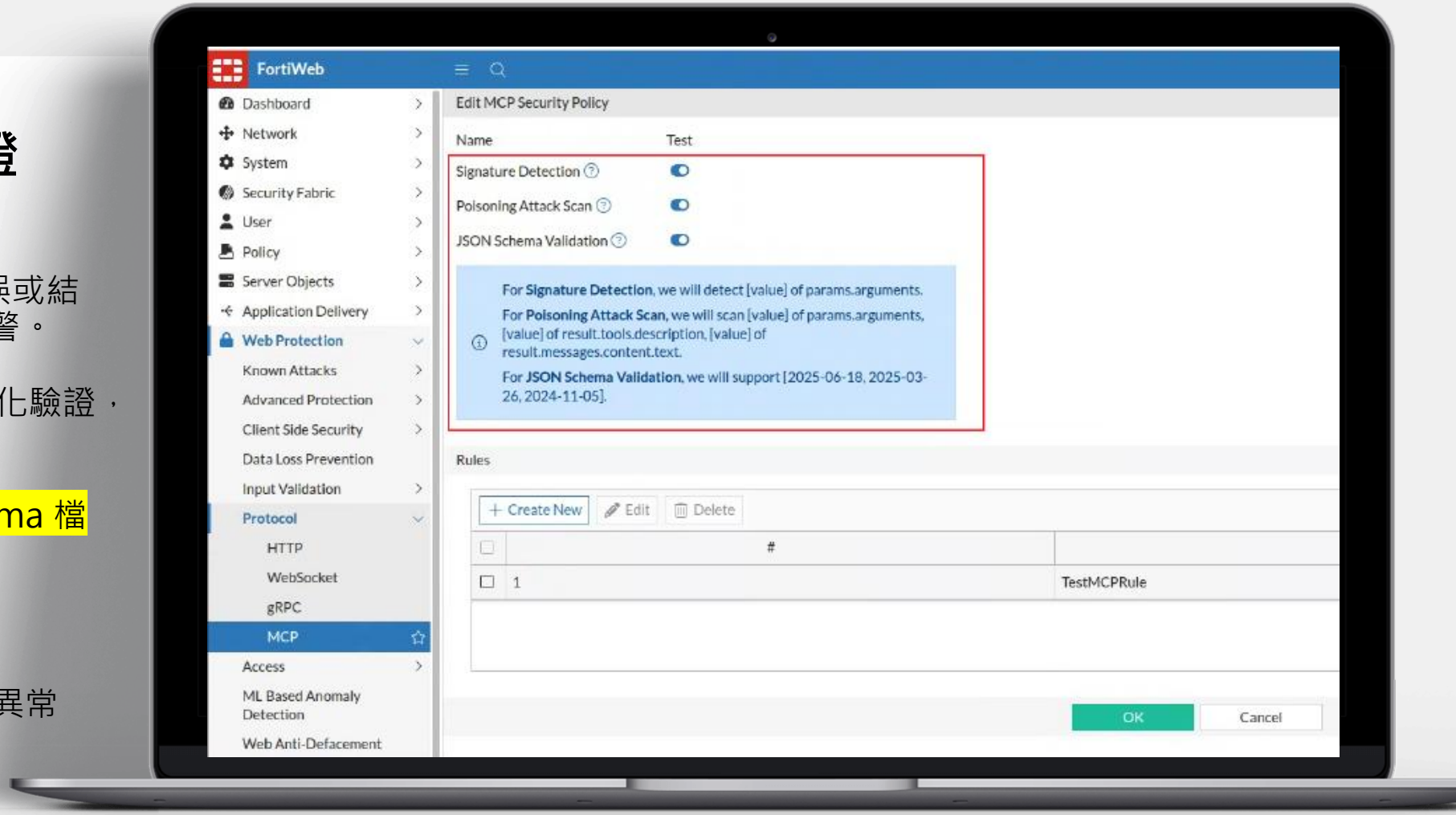
大型語言模型防護 – MCP 防護

Model Context Protocol

JSON 格式與結構驗證

檢查 MCP 如果欄位缺失、型別錯誤或結構異常，就可依設定進行阻擋或告警。

- 對傳輸中的 JSON 資料進行結構化驗證，包含請求與回覆內容
- 透過 FortiGuard 持續更新 Schema 檔案，確保驗證準確性
- 確保資料格式的一致性與正確性
- 降低因資料格式錯誤造成的系統異常
- 提供明確的錯誤回饋機制

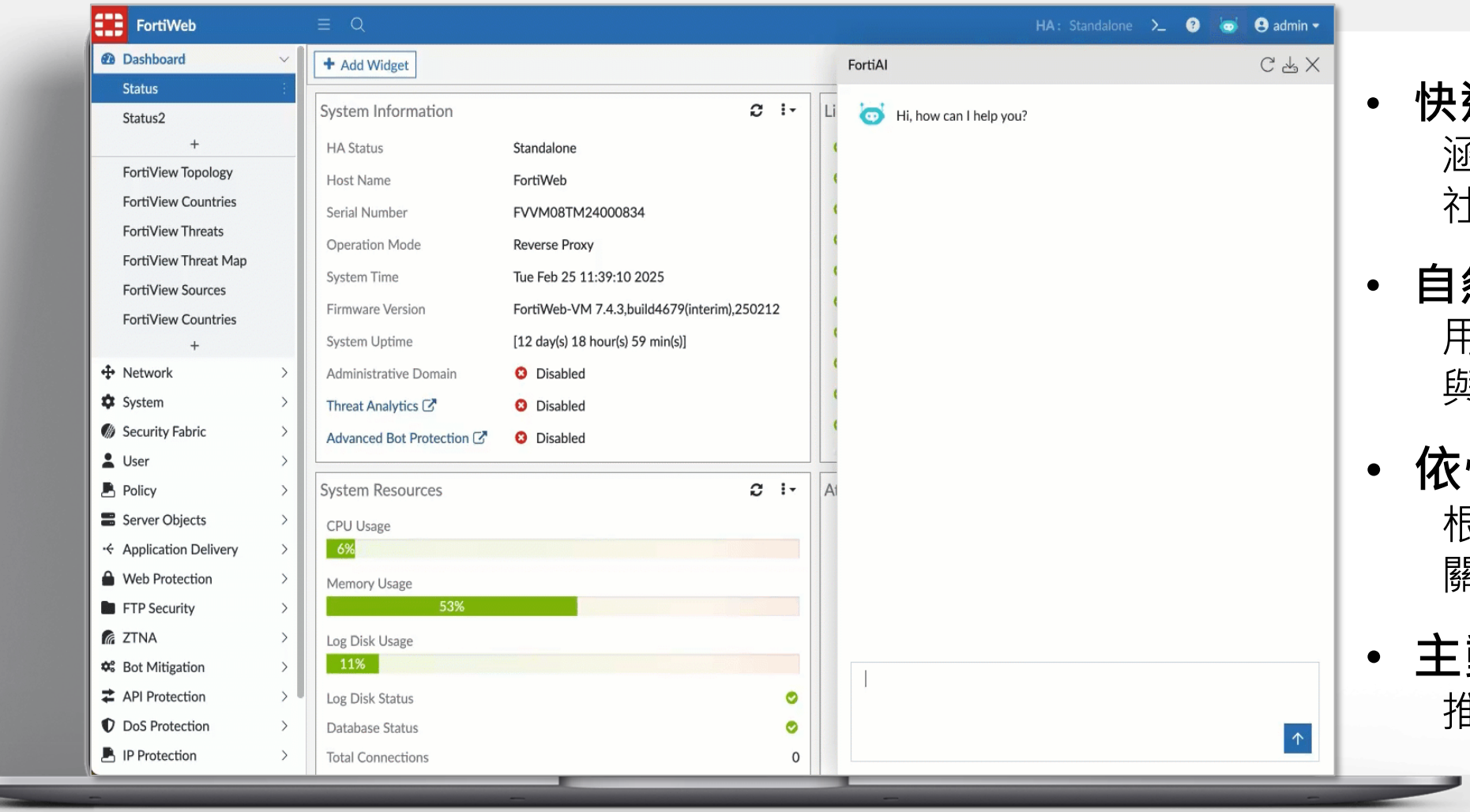


FortiAI：下一代資安營運的新助手

讓安全團隊更快理解、更快決策、更快行動

AI 正在成為
現代資安營運流程的一部分

FortiAI 協助你更快掌握 FortiWeb

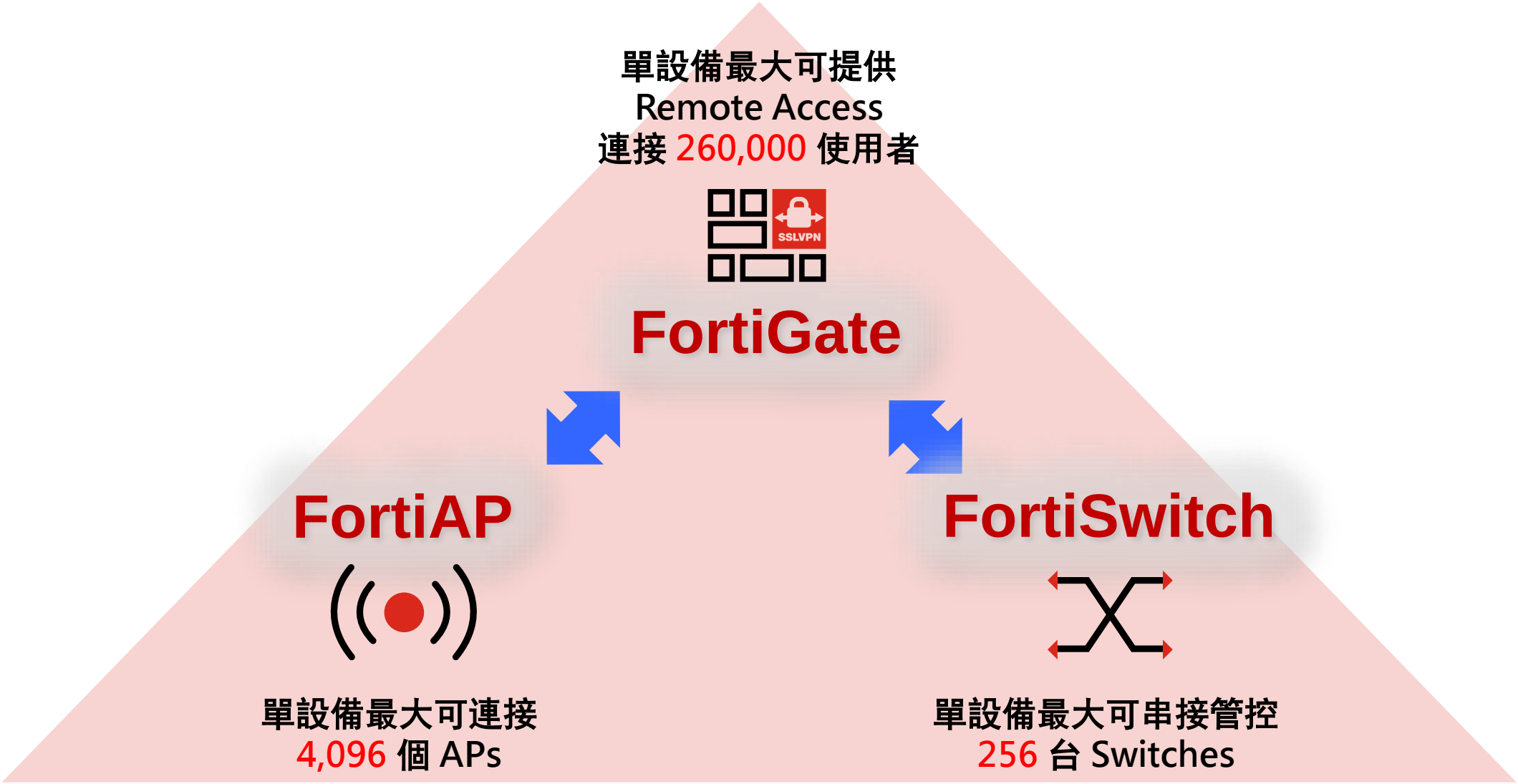


- **快速掌握產品知識**
  涵蓋技術文件、知識庫與社群文章
- **自然語言直接提問**
  用更直覺的方式取得答案與建議
- **依情境提供回應**
  根據目前頁面內容給出相關資訊
- **主動帶出後續方向**
  推薦相關問題與知識文章

Fortinet 鐵三角 3.0

透過 AIOps 讓資安鐵三角管理再進化

2018 Fortinet 安全織網 – 資安鐵三角 1.0

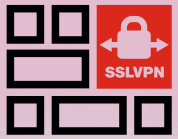


2022 Fortinet 安全織網 – 資安鐵三角 2.0

FortiAP

單設備最大可連接
4,096 個 APs

單設備最大可提供 Remote Access
連接 260,000 使用者

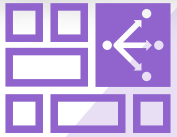


FortiGate

FortiSwitch

單設備最大可串接管控
256 台 Switches

SD-WAN

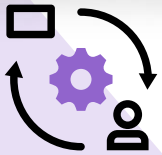


透過應用導向並整合資安防護
達成最佳路徑選擇

FortiToken

結合手機載具，完備身分驗證

ZTNA



持續性的檢測從用戶身分辨識
到設備安全

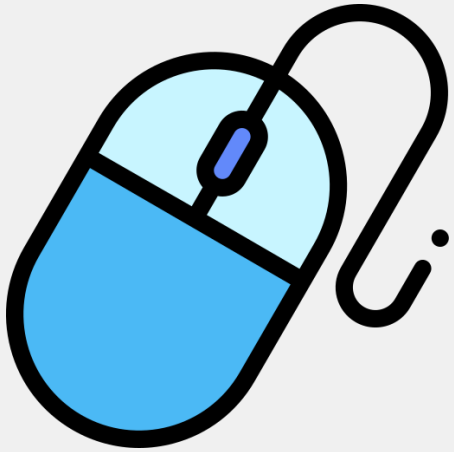
傳統方式問題研判

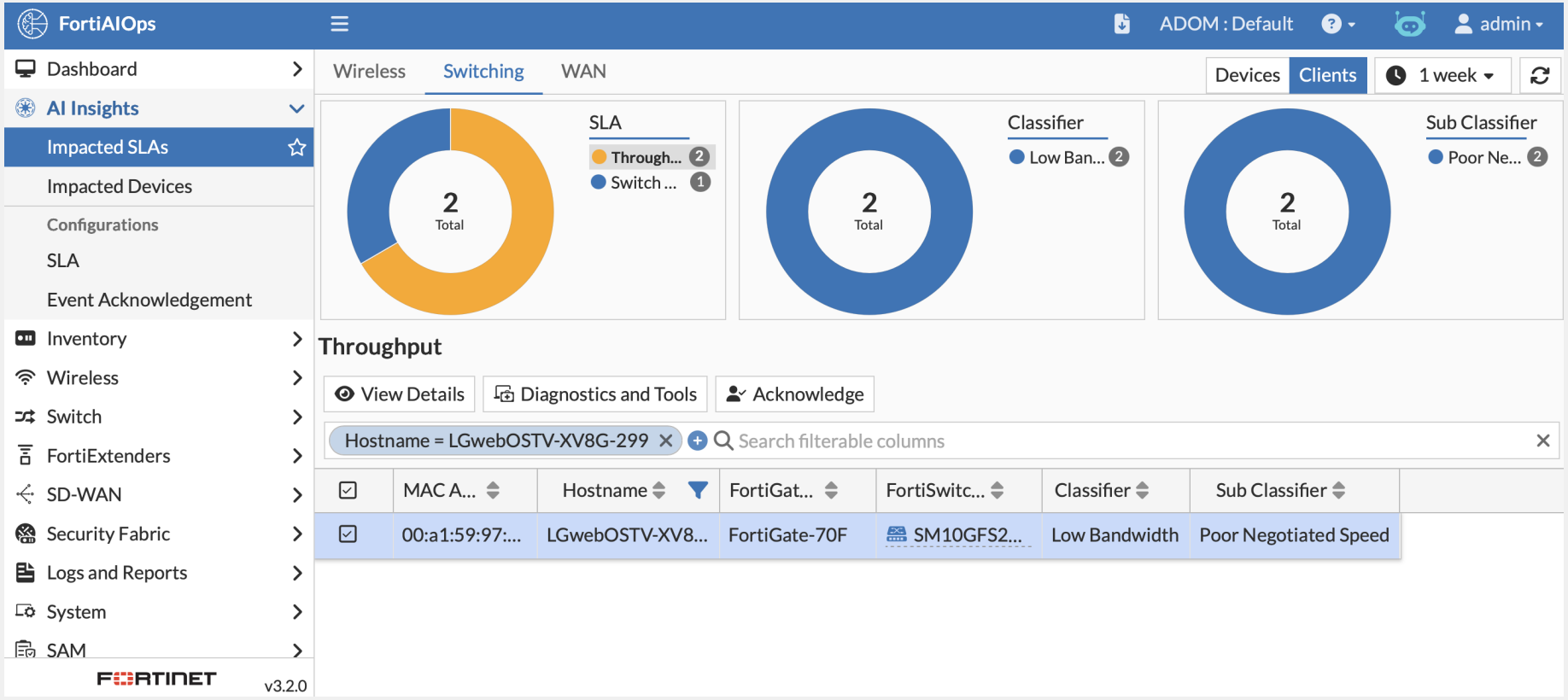
費時又費力，需要跨有線、無線和 SD-WAN 領域的專業知識

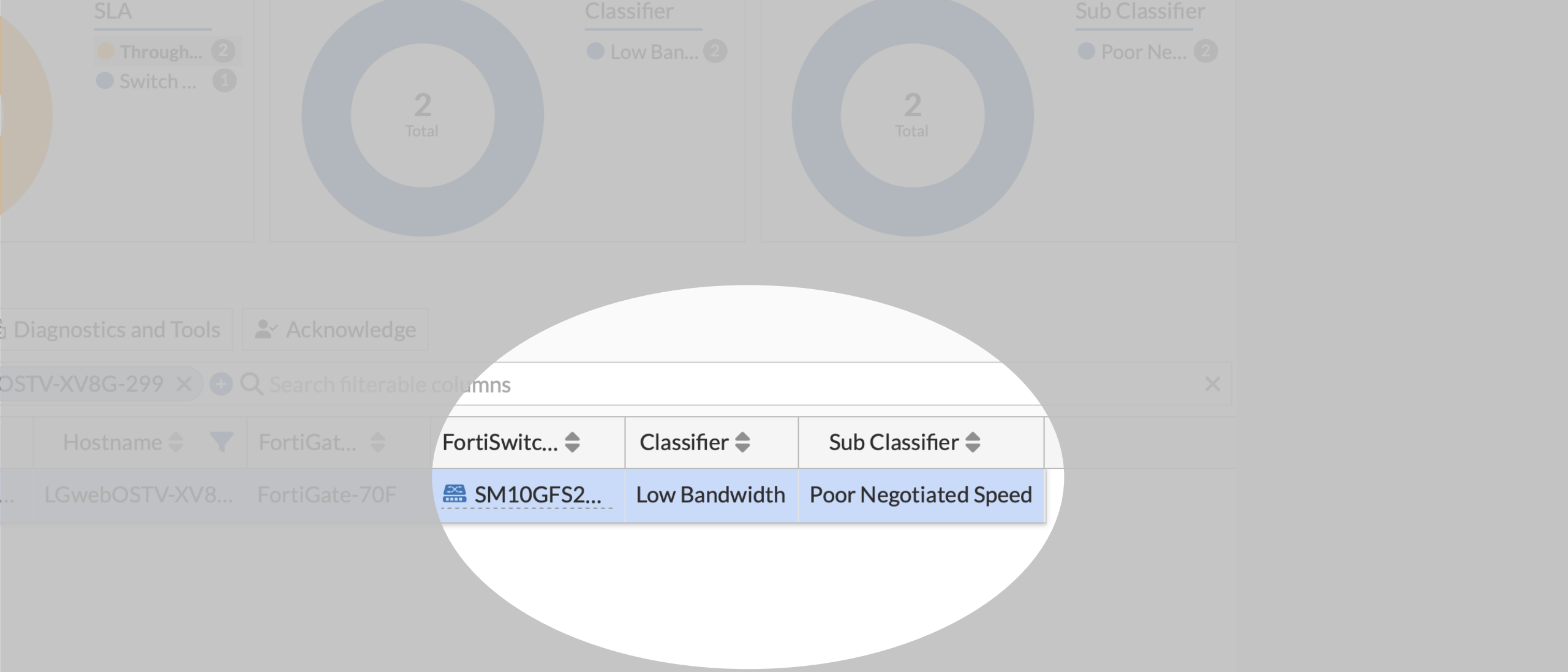
Easy to Manage (AI 輕鬆管理)

FortiAIOps：透過 AI 判斷可能的原因

找出網路可能的問題，網路速度變快了!!







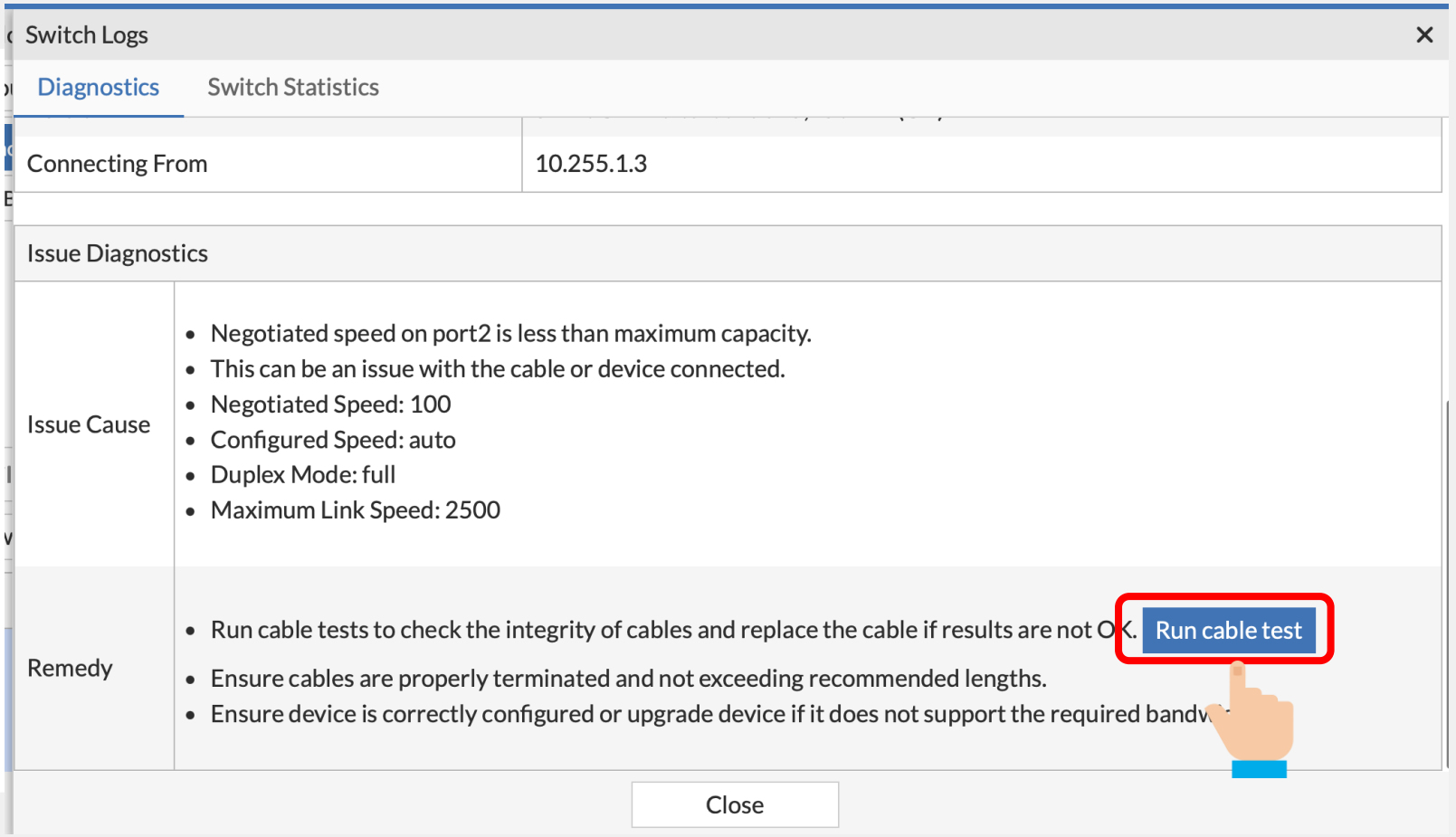
AI 自動判斷：速率匹配問題

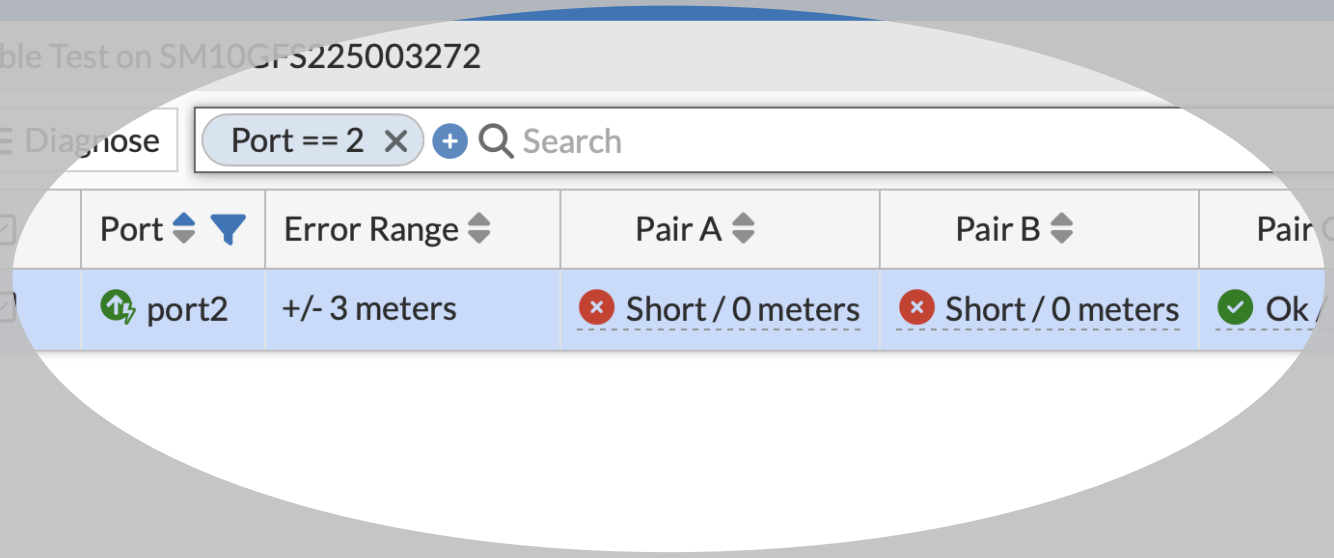
Easy to Manage – FortiAIOps

FortiAIOps：AI 洞察交換器線路監測與除錯

有線網路智能監看與除錯

- AI 洞察 (AI Insights) 過程中提供一個快捷途徑，可用來啟動交換器線路監測與告警。
- 修復緩解建議 (remedy) 中，若出現「 Run Cable Test」按鈕，可在受影響的交換器埠上直接啟動纜線測試。





快速纜線除錯：啟動纜線測試發現 RJ45纜線 Pair A, B 斷線

Easy to Manage (AI 輕鬆管理)

FortiAIOps：AI / ML 強化資安鐵三角運營管理

- 幫助即時了解您的整個基礎設施
- 自動化根本原因分析，快速識別和解決問題
- 監督式人工智能洞察、預測異常並推動決策

Fortinet 資安鐵三角 1.0 / 2.0 / 3.0 比較表

	資安鐵三角 1.0
核心目標	整合式網路防護
架構組件	FortiGate + FortiSwitch & FortiAP
防護重點	裝置整合防護、可視化拓樸
威脅偵測	威脅防護、IOC 報告
維運成本	人工監控為主
事件判斷	人工分析 log
效能與體驗	偏重安全策略執行
AI 能力	✕

FortiSIEM Playbook

可將事件處理流程自動化，從調查到處置都能依照 SOP 執行。

FortiSIEM 自動化服務

從事件調查到回應處置，形成自動化閉環

豐富的自動化與協調能力

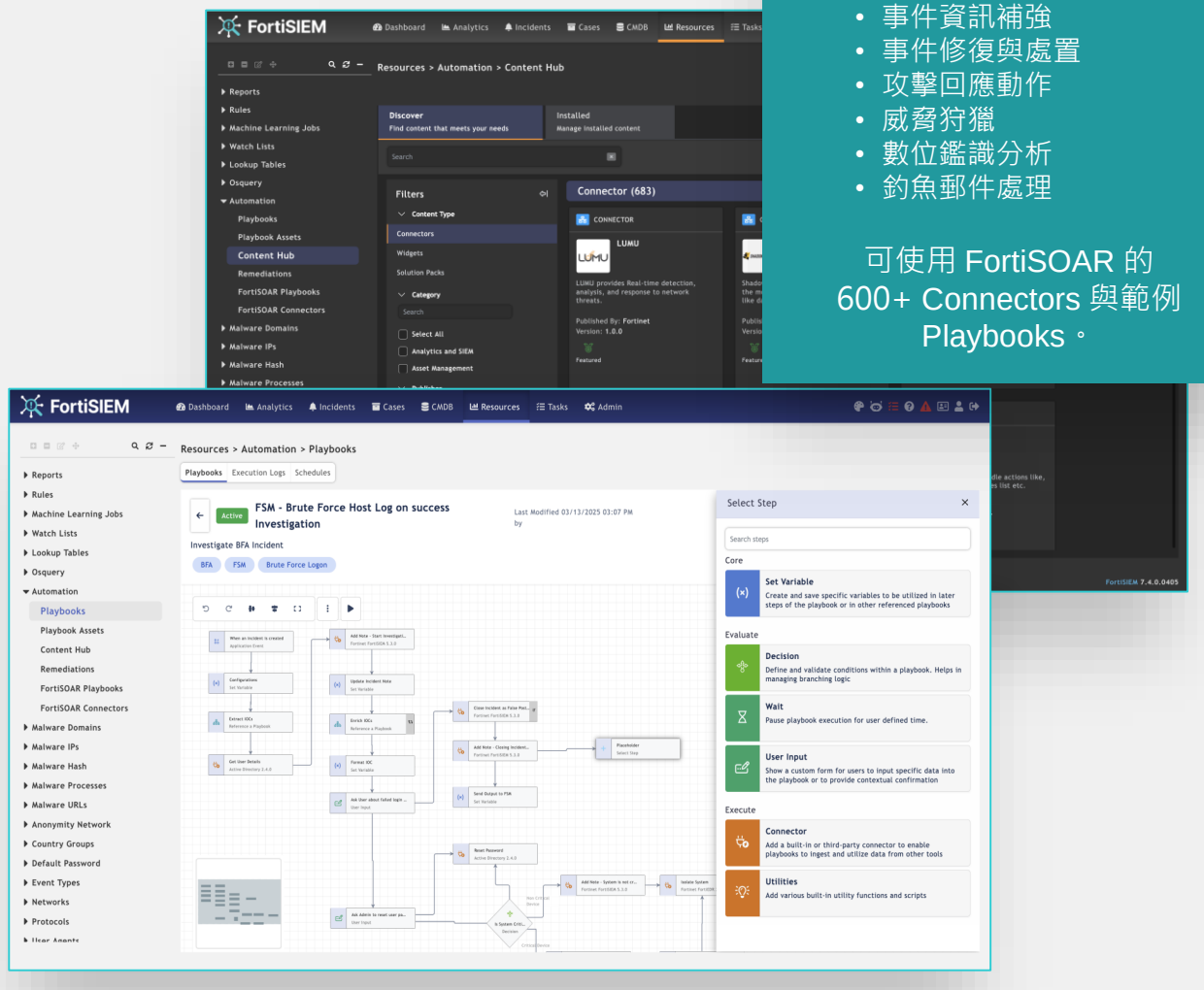
- 自動化功能可直接整合於 SIEM 工作流程中
- 提供預建 SIEM Playbook 函式庫與 Connectors
- 可存取 600+ Connectors 與範例 Playbooks
- 提供視覺化 Playbook 設計器
- 後端由 FortiSOAR Cloud Automation Service 提供自動化能力

透過自動化 SIEM 相關任務，提升 SOC 分析師效率，並將事件處理流程標準化。

FortiSIEM Playbooks 涵蓋範圍

- 事件調查
- 事件資訊補強
- 事件修復與處置
- 攻擊回應動作
- 威脅狩獵
- 數位鑑識分析
- 釣魚郵件處理

可使用 FortiSOAR 的 600+ Connectors 與範例 Playbooks。

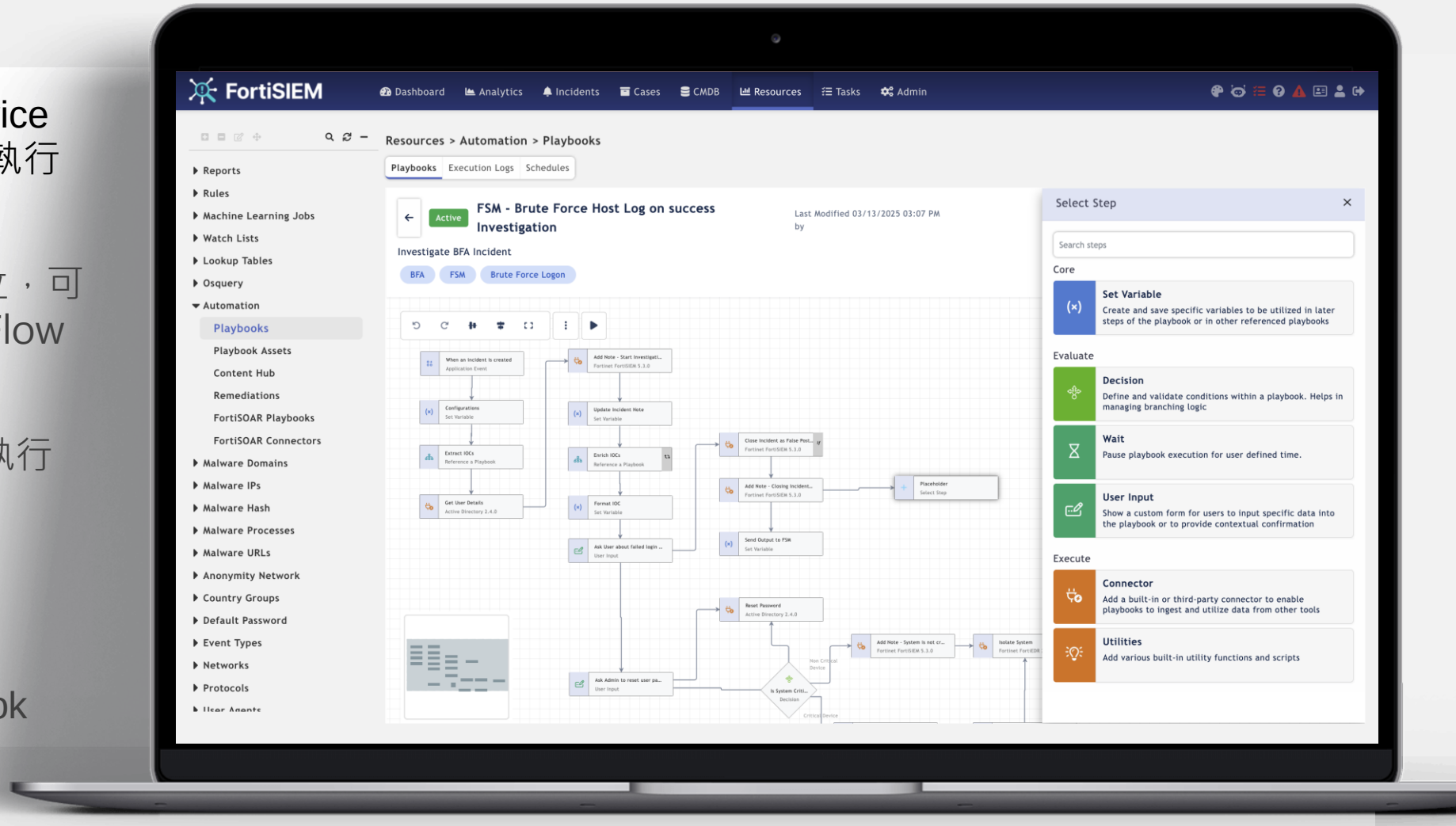


從偵測、調查到處置，形成完整閉環

透過原生 SOAR 實現自動化回應

FortiSIEM Automation Service 原生整合 Playbook 建立與執行能力，簡化事件回應流程。

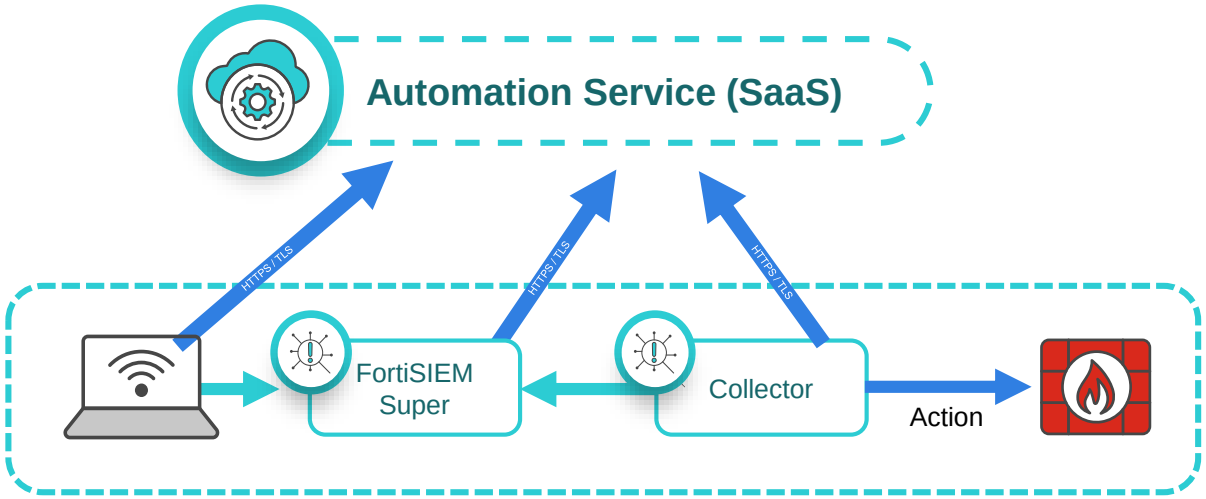
- 支援視覺化 Playbook 建立，可透過 Trigger、Action 與 Flow 串接調查與回應流程。
- 可在事件調查過程中手動執行 Playbook
- 可依據 Incident 自動觸發 Playbook
- 可依排程定期執行 Playbook

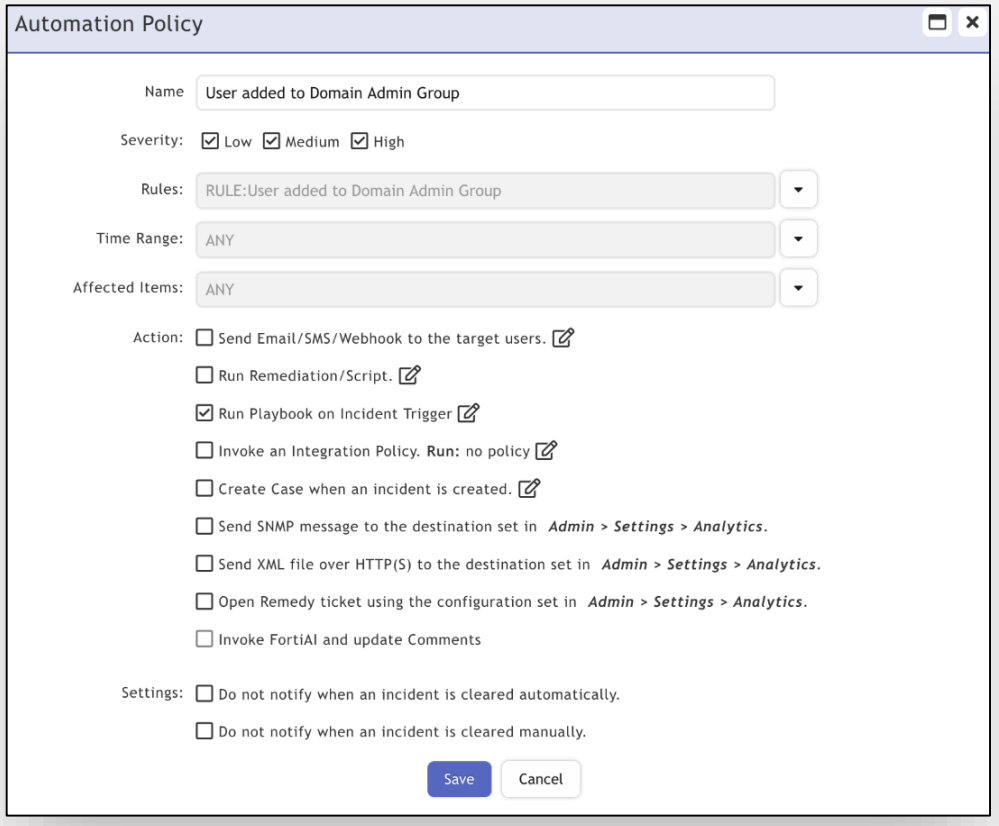


且看 FortiSIEM Automation 如何運作

Playbook 觸發與管控

- Playbook 的觸發與管理整合在 FortiSIEM 標準工作流程中
- Playbook 可依 Incident 類型自動觸發，也可手動執行或排程執行
- 授權價格依 Playbook 同時執行數量計算





- 所有與FortiSOAR Cloud通訊皆由 FortiSIEM 主動發起，採用 request / reply 方式進行
- Playbook 動作由本地端 FortiSIEM 元件負責執行

FortiDLP

讓數據安全更智能、更全面

情境：內部員工突發數據外洩行為

情境說明

某企業的財務部員工平時只會存取內部 ERP 系統中的財務報表，但某天突然大量下載敏感數據，並試圖透過雲端（如 Google Drive）或 WebMail 上傳

傳統 DLP 會怎麼做

依賴靜態規則，定義關鍵字或建立文件指紋，封鎖所有含「財務數據」的檔案傳出，但這樣的策略可能會影響正常業務流程，例如合法的財務報表發送，無論誤擋或漏擋，都只能被動的調整策略

無 AI 分析能力，無法偵測「正常 vs. 異常」行為，容易造成誤判

你想要的 DLP 應該怎麼做

自動學習該員工的日常行為模式，透過 AI 分析使用者歷史行為，建立基線，如正常存取頻率、檔案大小、傳輸管道等，當偵測到異常時，觸發更嚴格的 DLP 政策

保護數據需要全面且深入的情境能見度

外洩事件：SaaS 應用的可見性與控制

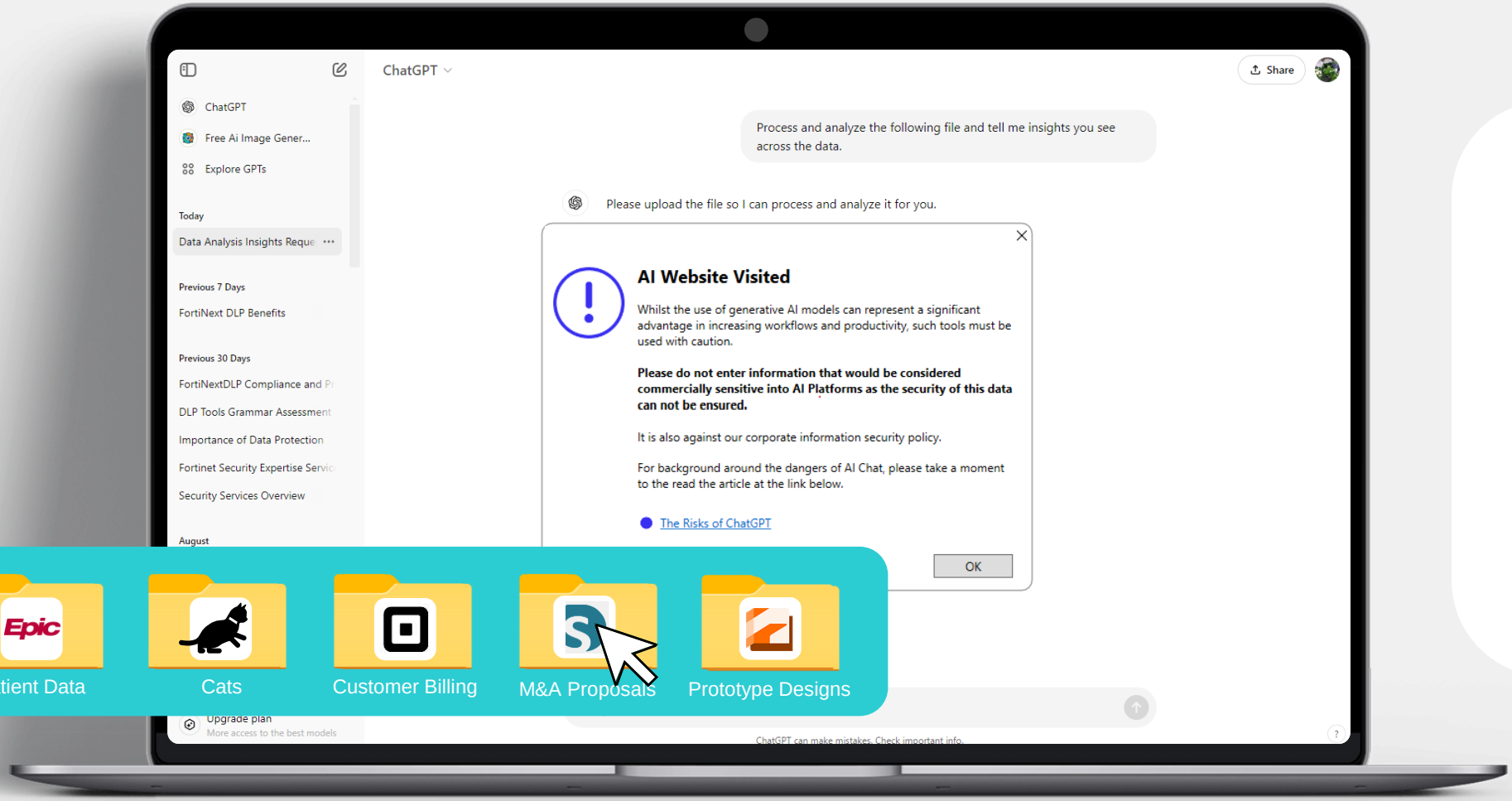
Timestamp	User	Device	Severity	Description
05/01/2024, 21:54	Joy Jones		Critical	Downloads **vacation-plan.csv** from **Acme Corp | OneDrive**
05/01/2024, 21:54	Joy Jones		Info	Login outside of usual working hours
05/01/2024, 21:43	Joy Jones		Low	Uploaded **vacation-plan.csv** to **Acme Corp | OneDrive**
05/01/2024, 21:35	Joy Jones		High	Renamed **sales-contacts.csv** to **vacation-plan.csv**
05/01/2024, 21:33	Joy Jones		High	Downloaded **sales-contacts.csv** from **Salesforce**
05/01/2024, 21:29	Joy Jones		Info	Login outside of usual working hours
05/01/2024, 21:28	Joy Jones		Info	Connected to **HOME_SWEET_JONES**

全面監控 SaaS 和裝置應用程式

高風險活動的防護策略

影子 AI：保護敏感資料在 AI 工具中的分享

當員工使用未經批准的、時下流行 GenAI 工具時，能保護企業資料的同時不影響生產力

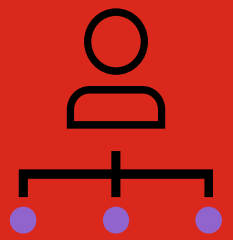


防止員工將敏感數據上傳到 GenAI 和其他 AI 工具

- 當員工/使用者的行為可能暴露敏感資料時，發送警報通知
- 宣導員工正確處理資料的責任

FortiPAM

Who、How、What、Safe，集中控管確保特權存取全程授權、監控與稽核。



FortiPAM - 用戶管理 (Who)

確認誰可以存取特權資源

用戶認證管理

- 本機帳戶
- 遠端帳戶:
  - RADIUS
  - AD/LDAP
  - SAML 驗證

彈性的多因子驗證機制

- 多因子驗證機制(MFA)
  - Email OTP
  - FortiToken
  - FortiToken Mobile
  - FIDO Key

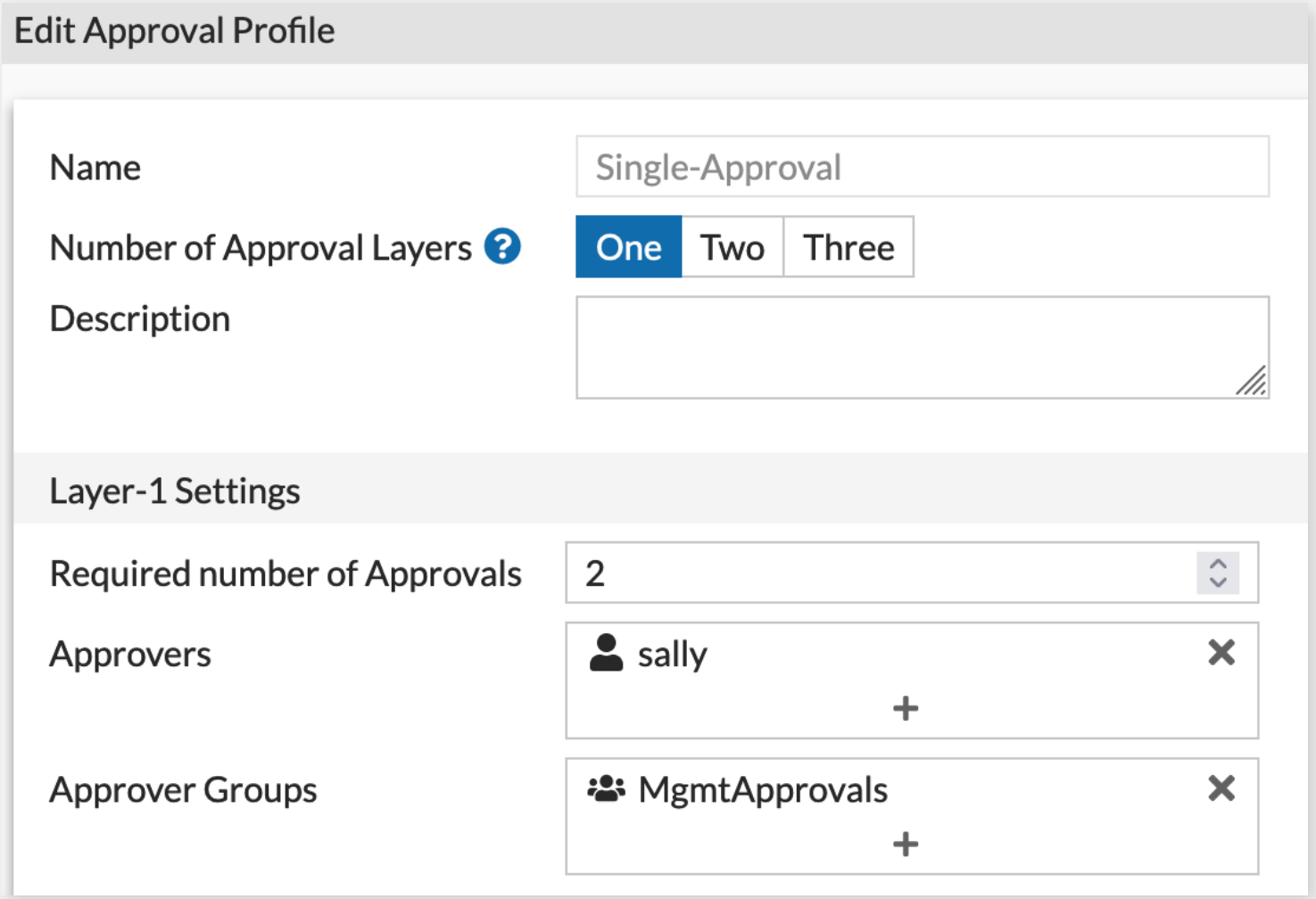
進階的安全強化機制

- 來源位址確認
- 連線標的防護
- 連線時間限制
- 零信任存取架構

FortiPAM - 用戶管理 (How)

存取憑證流程審核

- 依您組織核決流程設定核可流程。
- 啟用後，使用的用戶，**在獲得授權後**才能連線主機。
- **存取流程審核流程最多 3 層**。
- **每一層至少一位授權者**。
- 核決權限角色決定只有用戶在**正確的時間、正確的方式**，才能存取您的關鍵系統。



FortiPAM - 用戶管理 (What)

凡走過必留下足跡

會話錄影紀錄

- **支援全會話錄影 。**
- **會話使用期間滑鼠點擊、鍵盤活動紀錄。**
- **影像保留紀錄政策。**
  - 可自定義會話錄影保留政策。

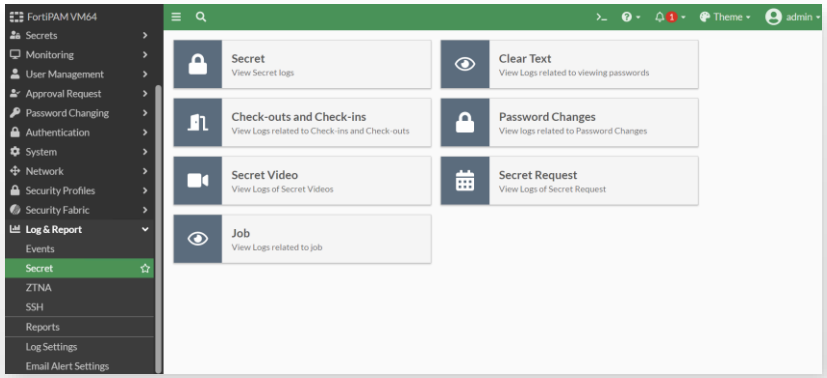
紀錄

Events

- 系統紀錄。
- 使用者活動紀錄。

Logs

- 存取紀錄。
- 簽出、簽入紀錄。
- 操作紀錄。



FortiPAM - 用戶管理 (Safe)

安全檔案傳輸、機密資料保護與監控

檔案安全傳遞

檔案交換惡意威脅偵測

- 可聯動 FortiSandbox、FortiNDR 偵測已知、未知 Zero-day 惡意程式。
- 支援 WebSCP、WebSMB。

系統資料安全保護

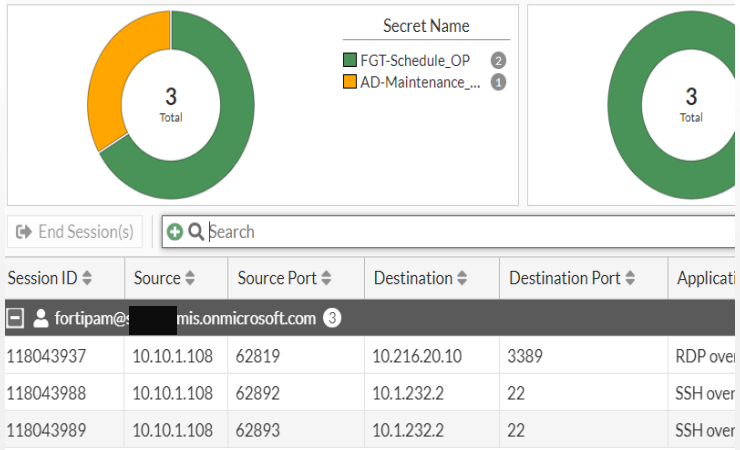
TPM 加密機制

- TPM in Hardware Models 。
- vTPM in Virtual Machine。

Trusted Platform Module

監督

- SSH 風險性指令控制。
- 使用者及連線監控。



Thank You