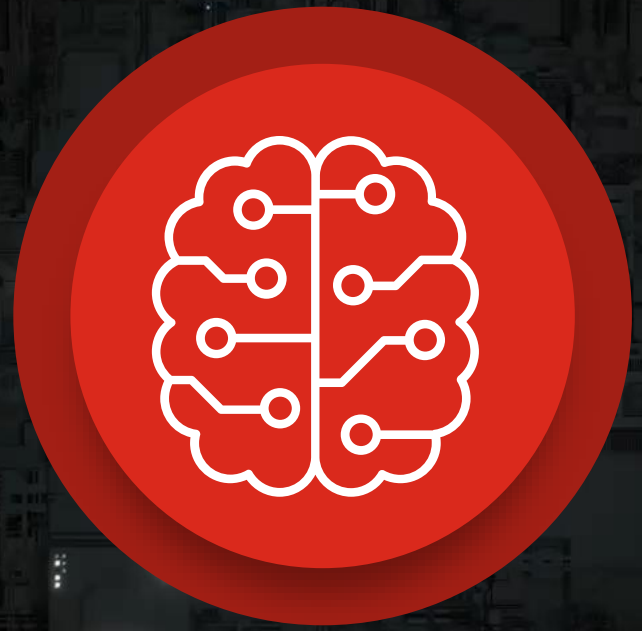
AI 驅動的安全運營

Why work harder when you can work smarter



李鵬 Paul Li

Fortinet 技術顧問

AI 人工智能 應用在網維營運 (NoC) 與資安營運中心 (SoC)

新一代生成式 AI 的安全助理

使用自然語言 (natural language) 和生成式 AI 來引導管理者，與管理者互動應答，啟動自動化作業流程，大幅簡化網維與分析師日常維運負載。

降低人為判斷失誤，決策有 AI 幫忙

借助 FortiAI，資安團隊可以做出更明智的判斷與決策，快速應對威脅，並在複雜任務上節省時間，提高了運營效率，提升了 IT 團隊的技能水平。

FortiAI 大型語言模型 LLM 安全架構

FortiAI 大語言模型 (LLM)，強化安全訓練，透過「內容過濾」「監控稽核」「存取控制」「提示固化」「機密確保」建構 LLM 安全架構，個資檢測，資料屏蔽，機敏資訊不外露。

AI 驅動的安全營運中心 Fortinet SecOps

FortiAI 已無縫整合到 FortiManager、FortiAnalyzer、FortiSIEM 和 FortiSOAR 的管理者日常維運中，協助優化分析師資安威脅調查並快速響應，即時緩解，SIEM 事件互動確認、SOAR 自動化流程劇本創建 ... 等。

✓ Security-First AI　✓ Platform Approach　✓ Use Case-Focused　✓ Automation-Driven

FortiAI 能為我們做些甚麼？

提升洞察力

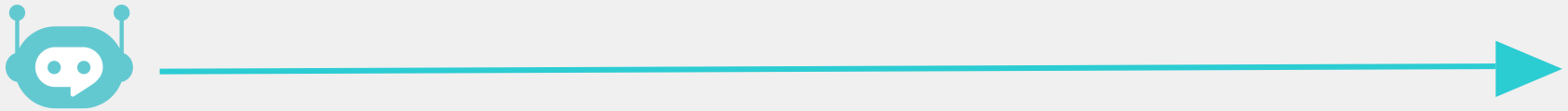
建構整個維運環境的知識庫，從網路、用戶、傳輸數據的應用以及資安態勢

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依最佳實踐執行

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建議行動



FortiAI for FortiAnalyzer

CONFIDENTIAL

Access Limited to Authorized Personnel

帶您認識全新的 SOC AI 安全助理

FortiAI 新一代生成式 AI 安全助理，為主動型安全運維而生

高效減輕工作負擔

- 大幅降低安全運維團隊的工作壓力

直觀簡化平台操作

- 透過自然語言互動應答，輕鬆上手

智能解析、評估與建議

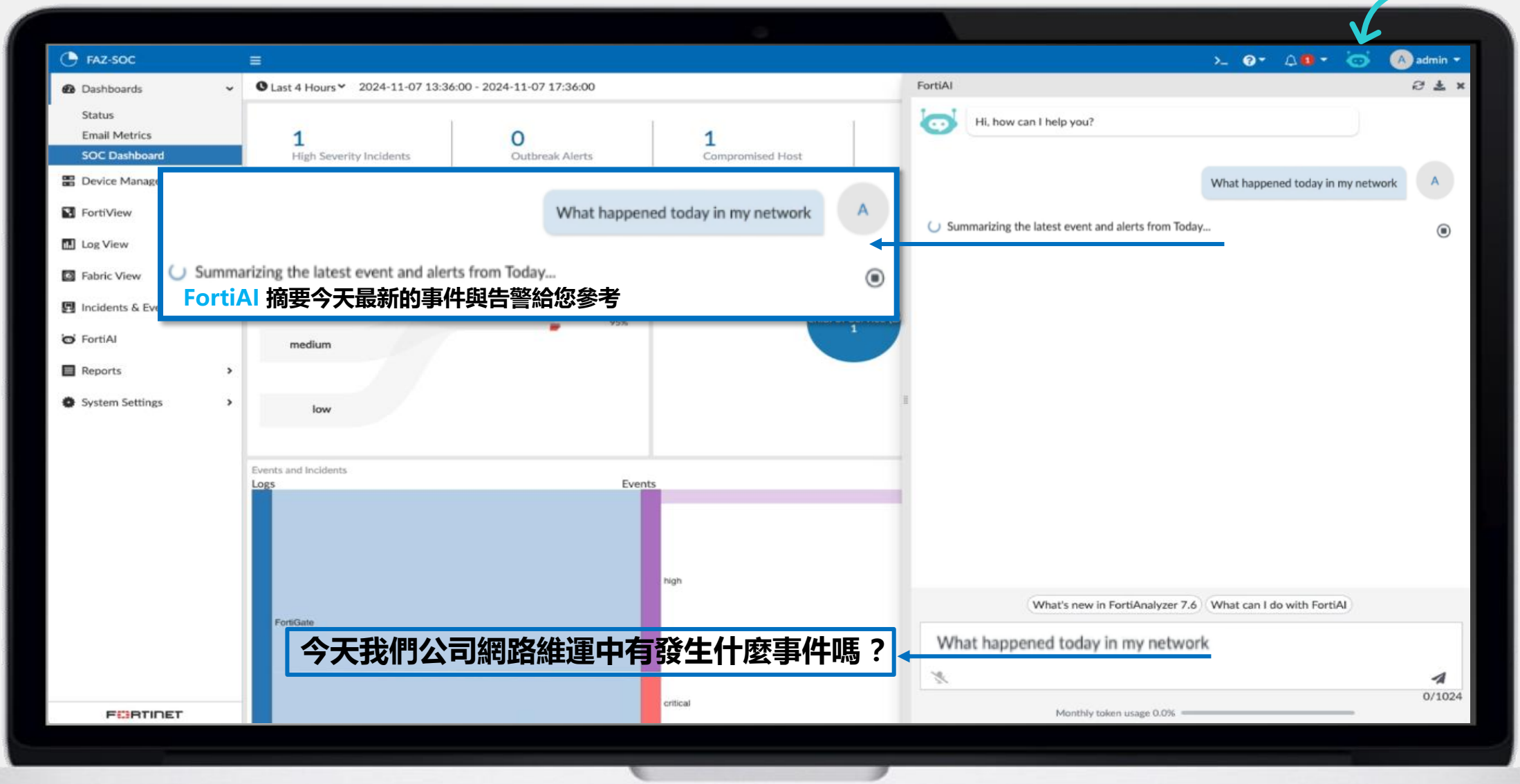
- 即時解析資安事件
- 自動生成事件摘要
- 精準評估潛在風險
- 提供專業修復建議

輕鬆創建化繁為簡

- 事件查詢
- 報表產出
- SIEM 偵測規則
- 自動化腳本
- 安全織網設備聯防

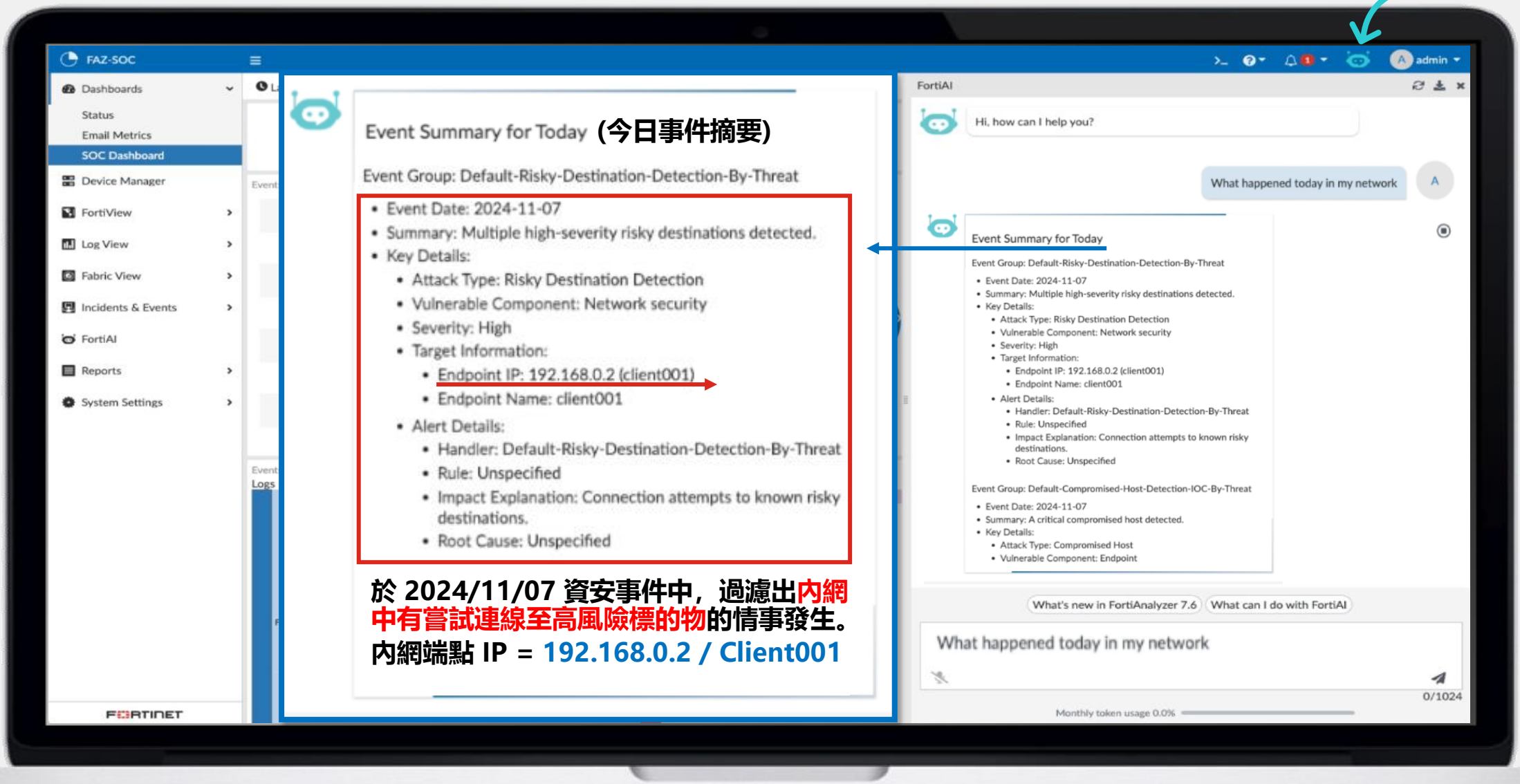
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



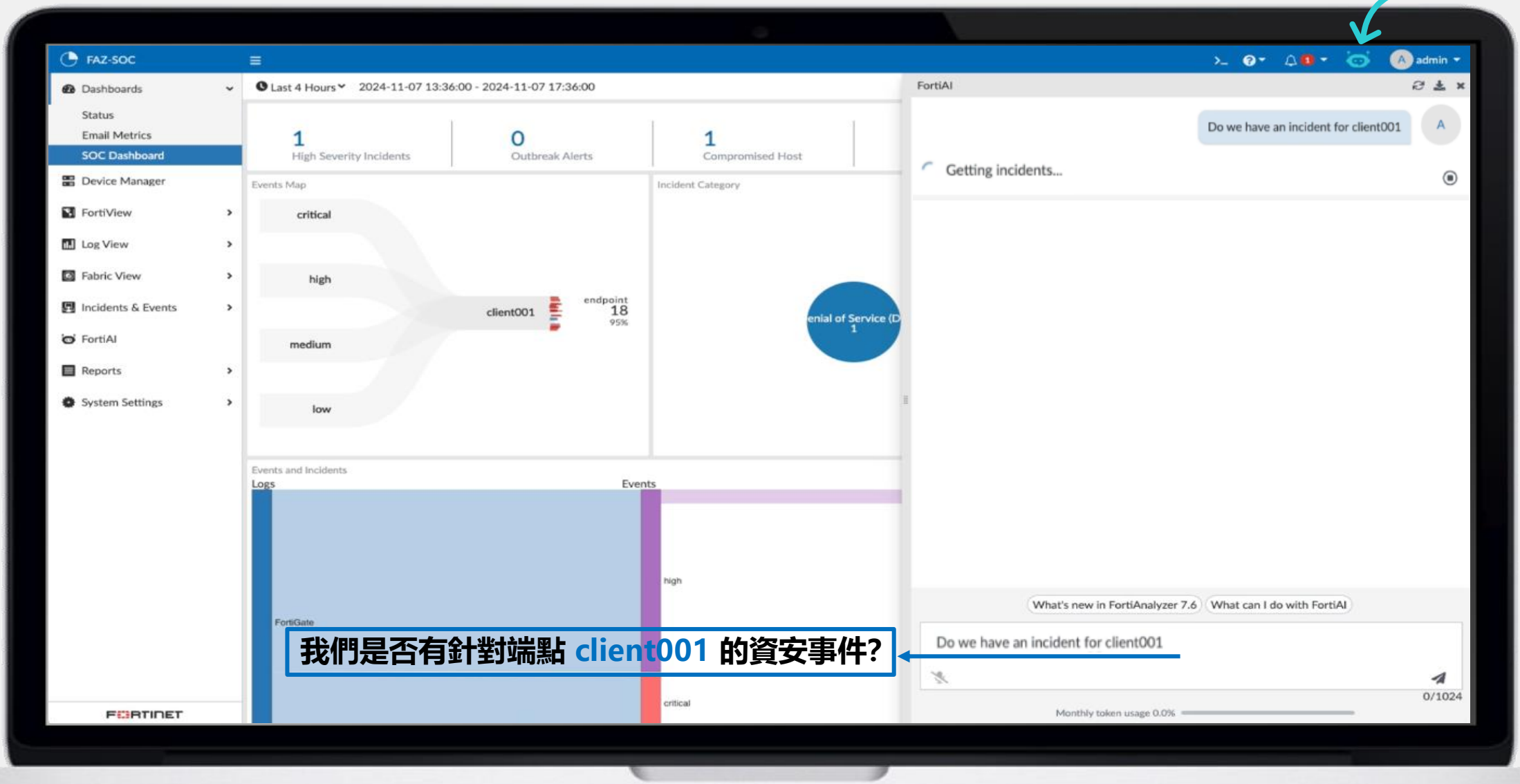
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



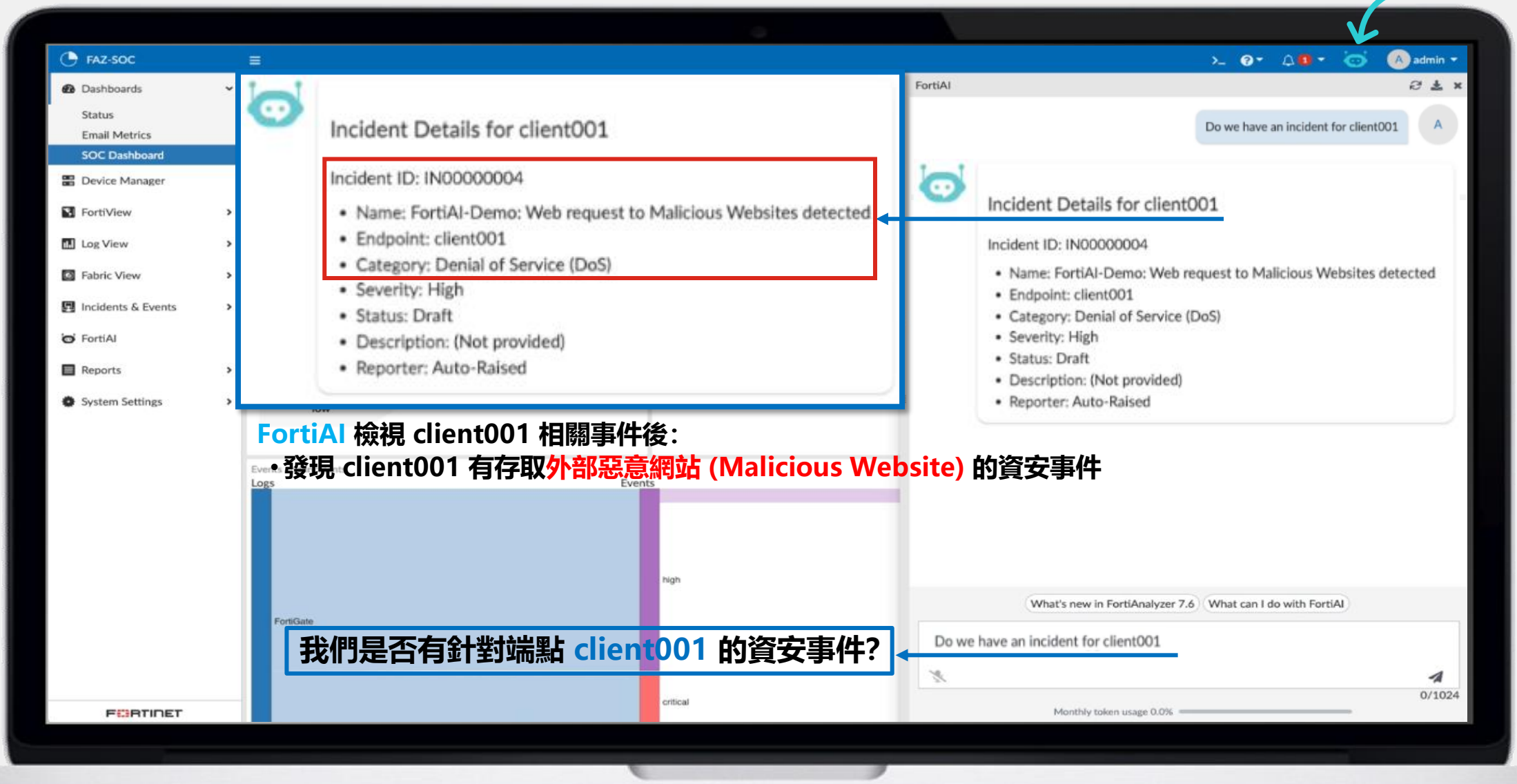
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



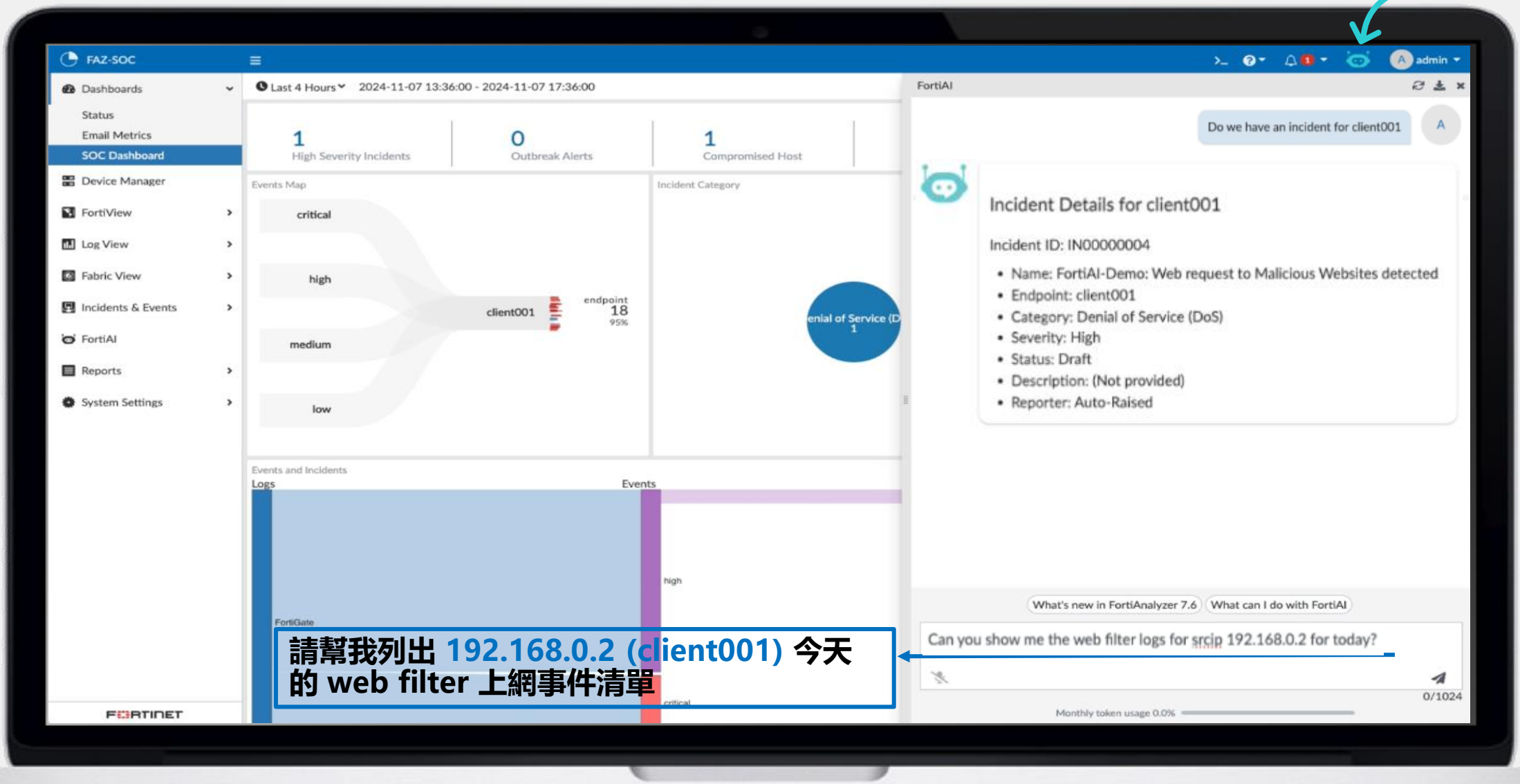
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



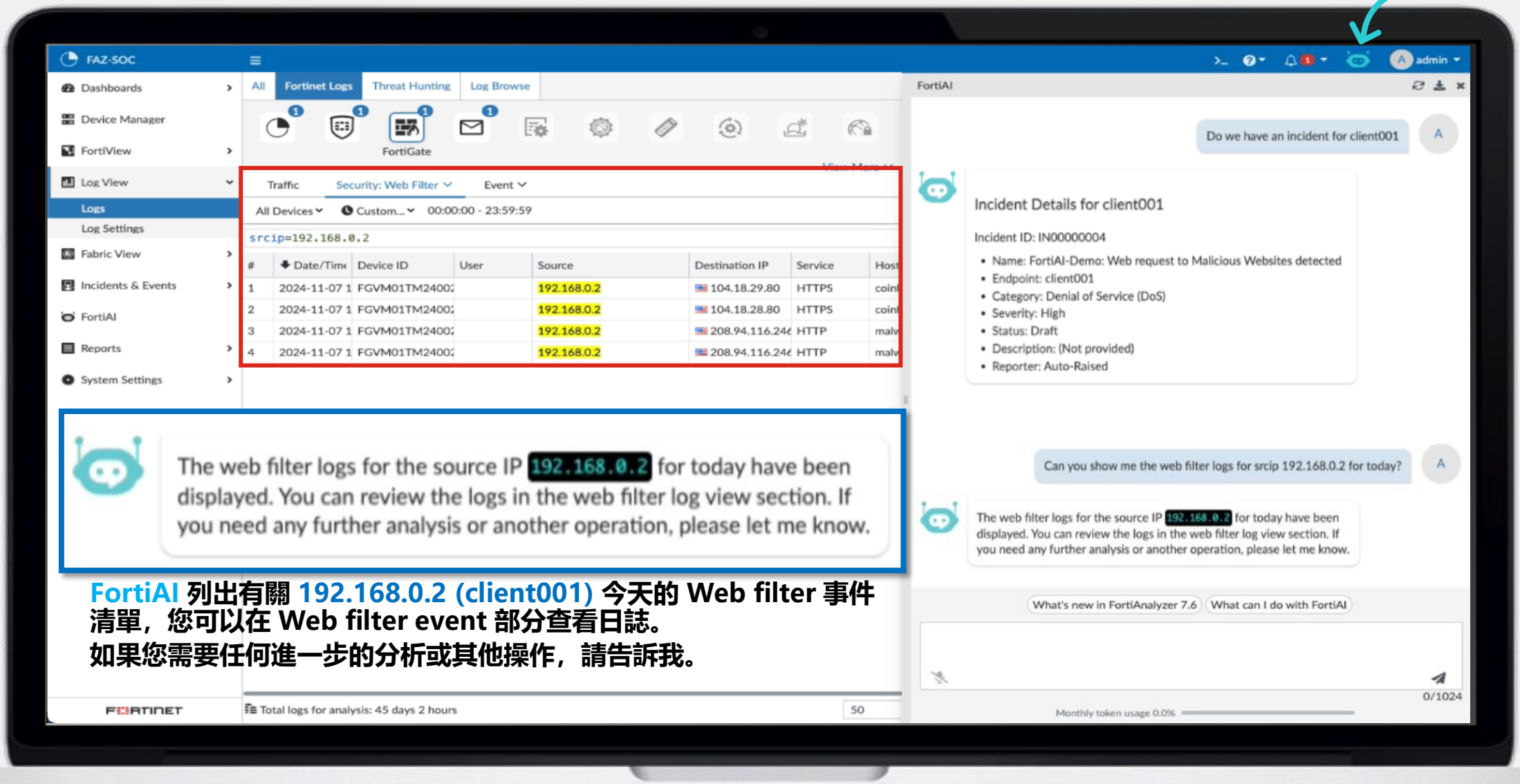
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件

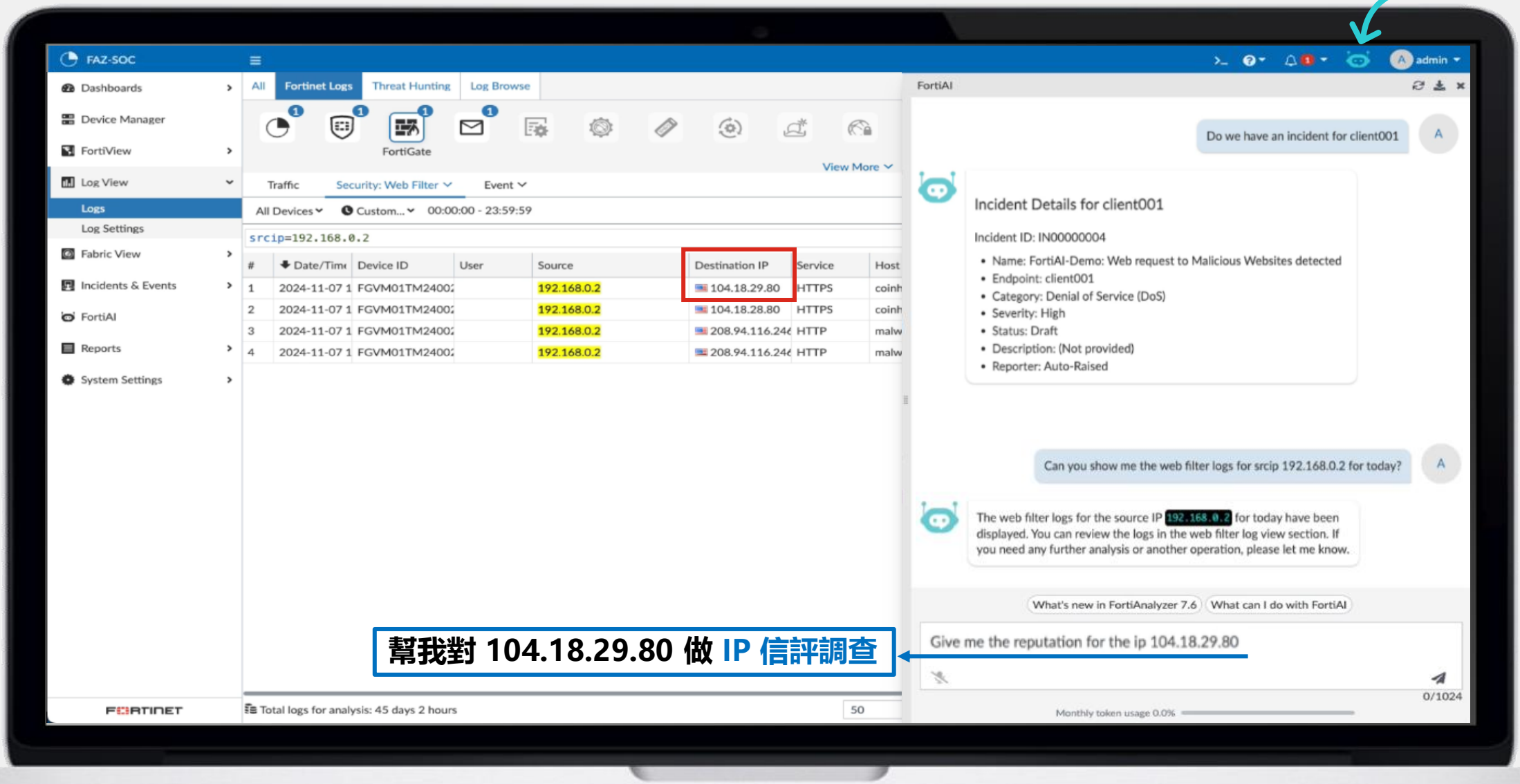


FortiAI 列出有關 192.168.0.2 (client001) 今天的 Web filter 事件清單，您可以在 Web filter event 部分查看日誌。

如果您需要任何進一步的分析或其他操作，請告訴我。

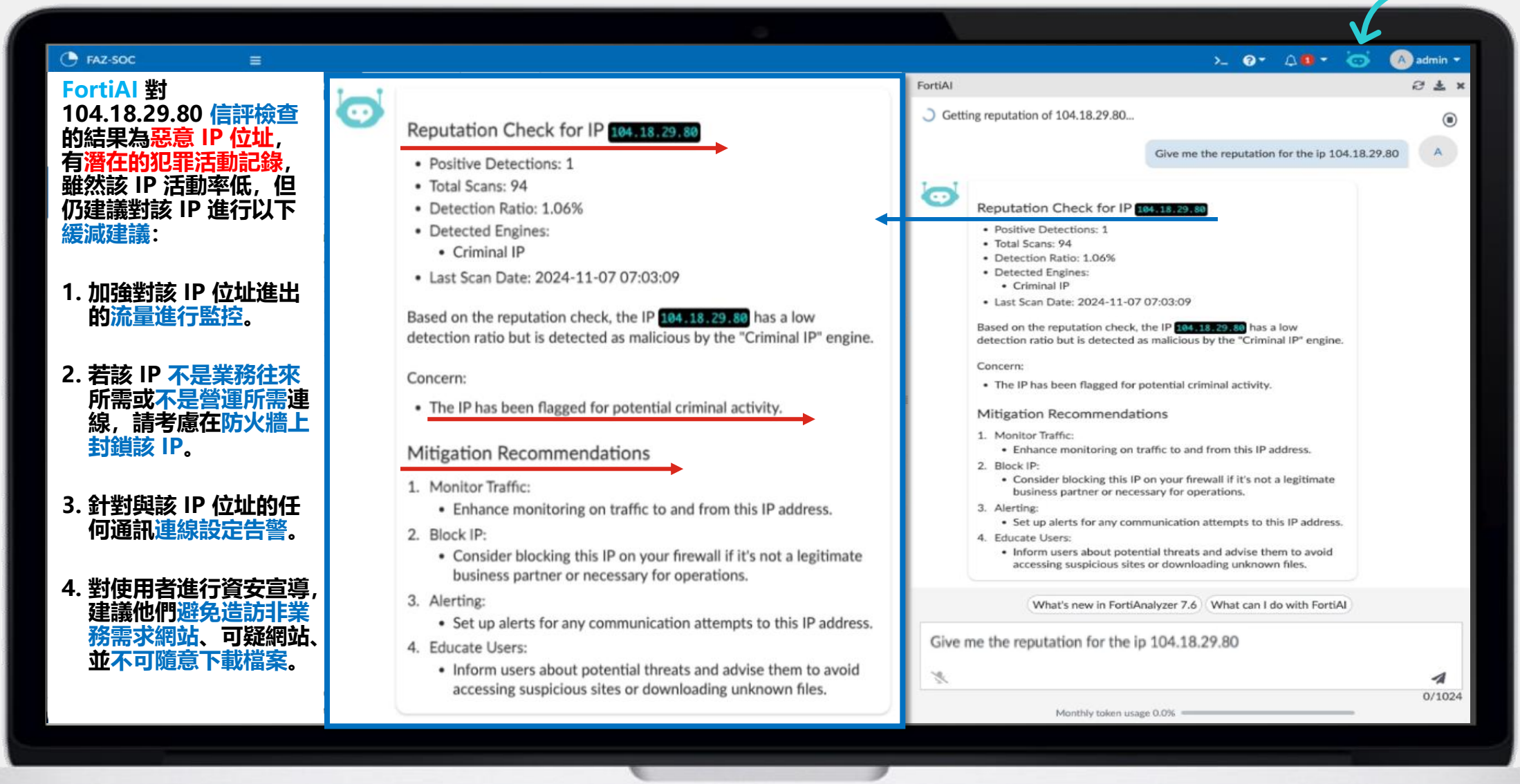
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，精準評估潛在風險



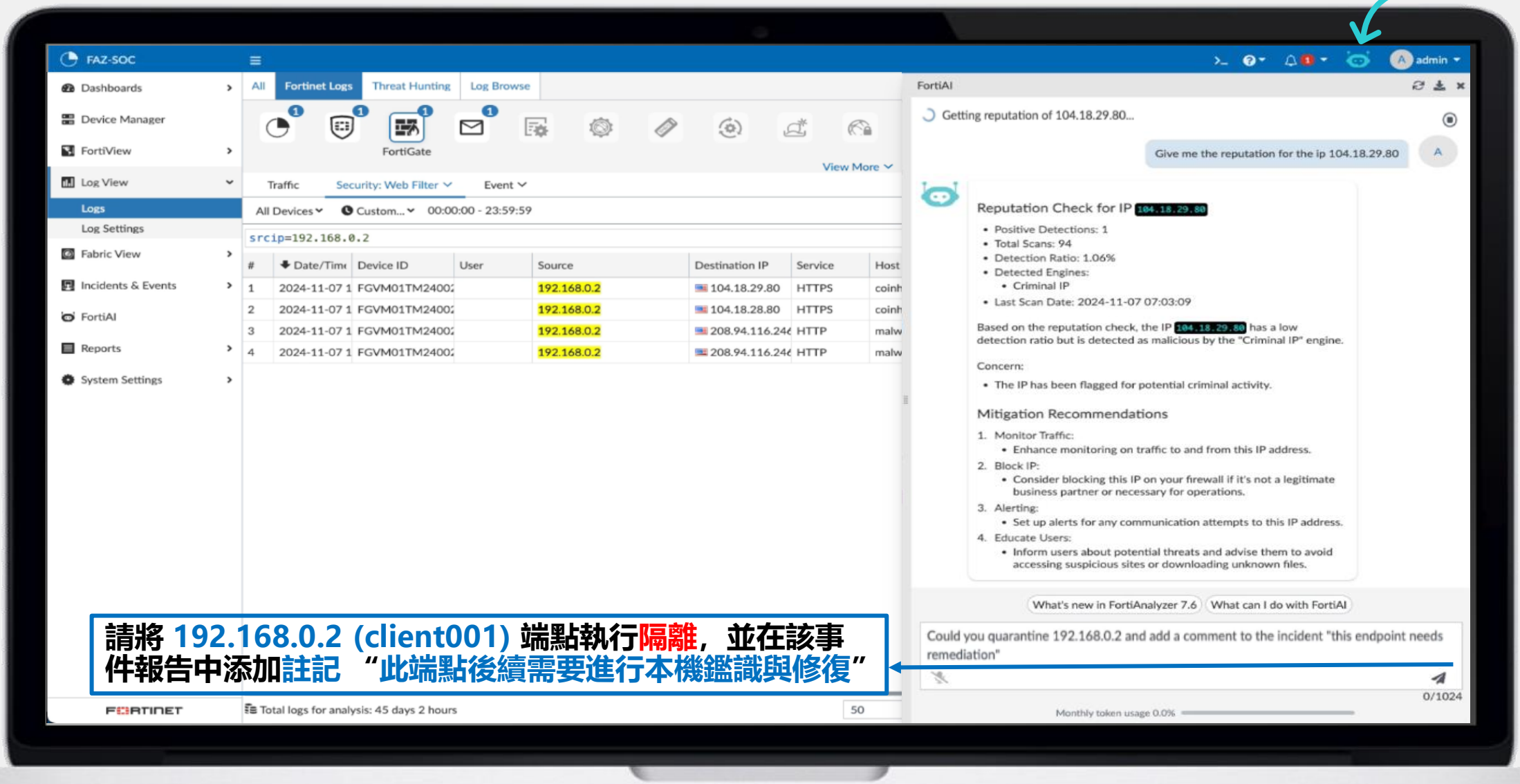
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，精準評估潛在風險



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，與端點防護自動聯防

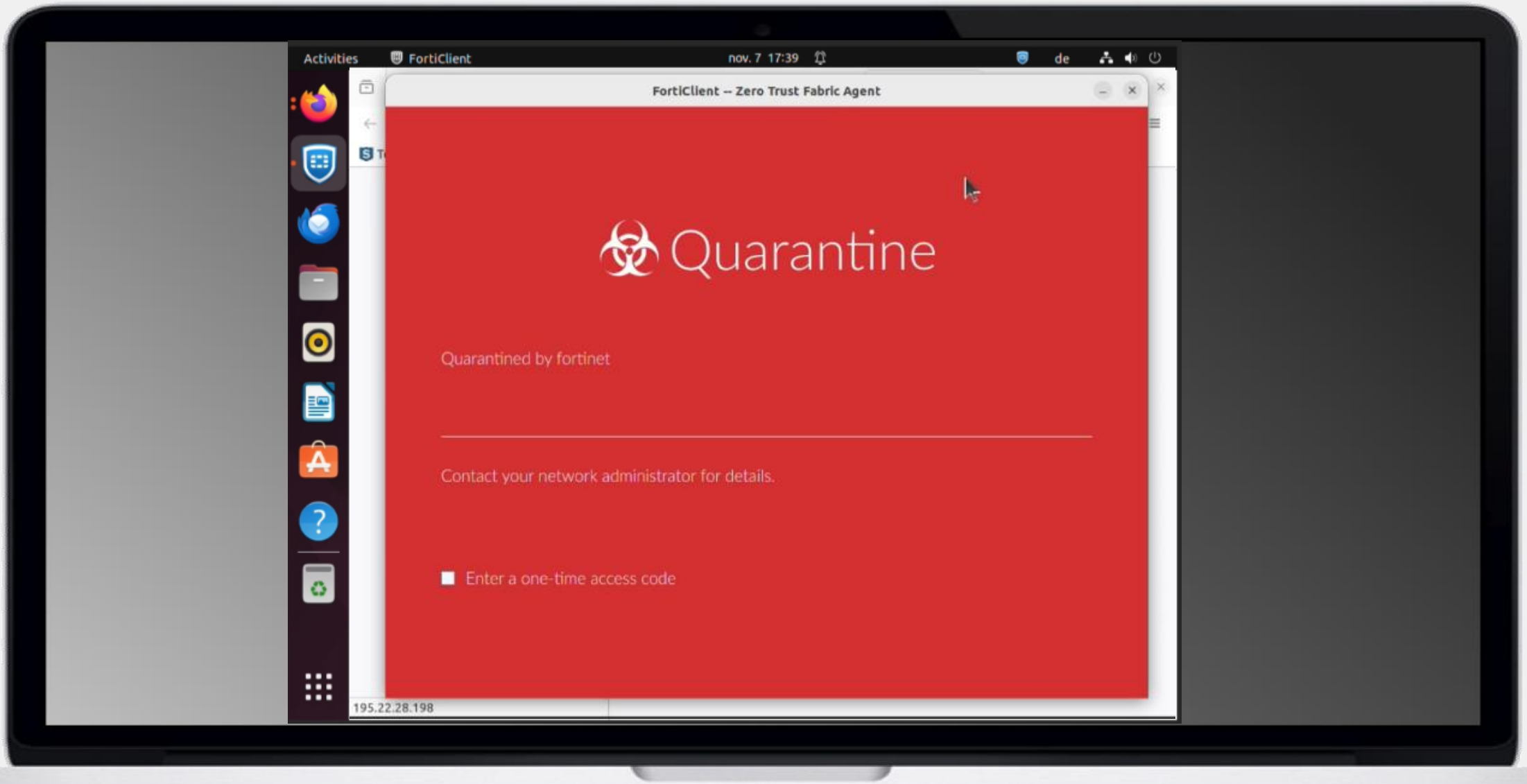


FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，與端點防護自動聯防

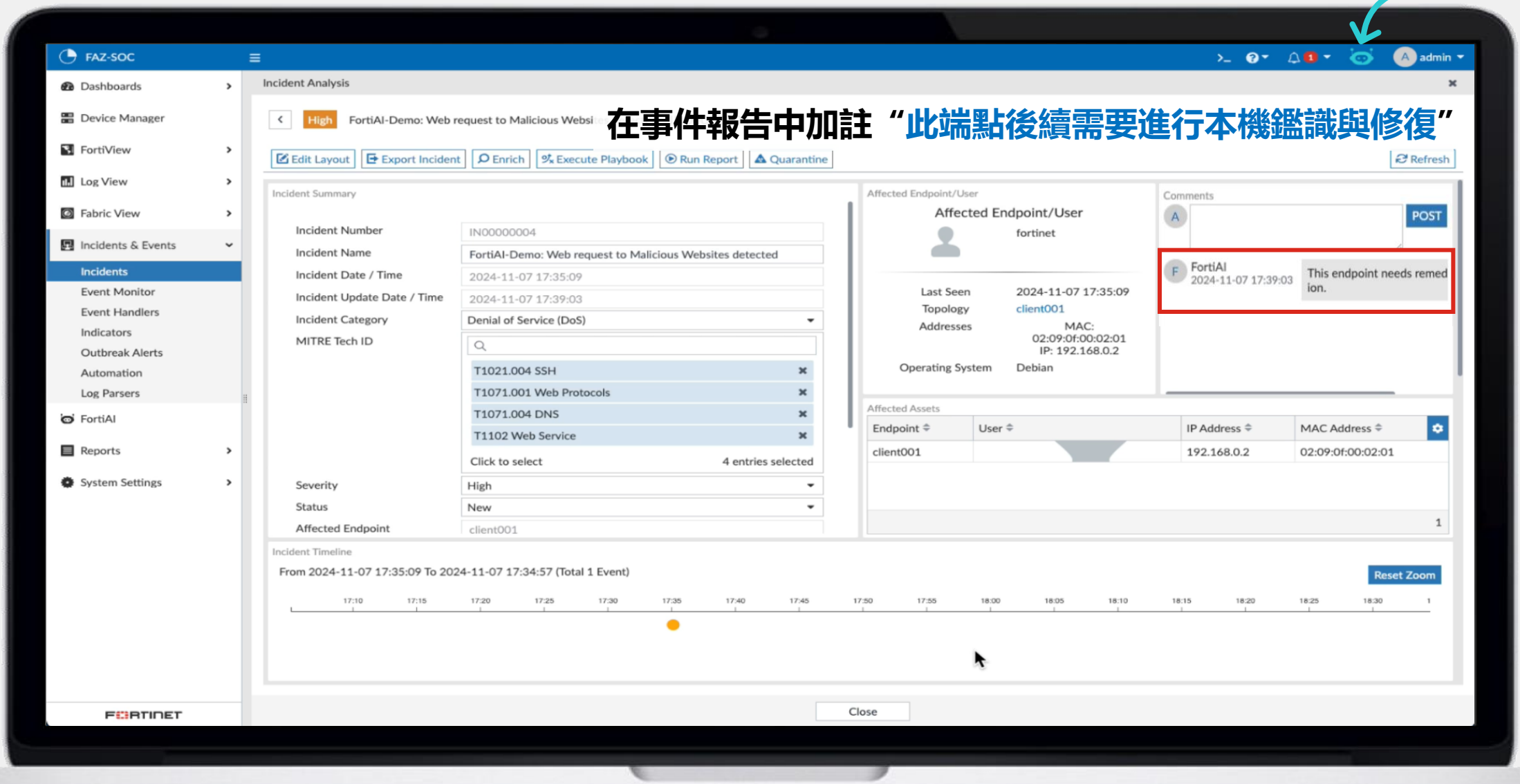
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，與端點防護自動聯防



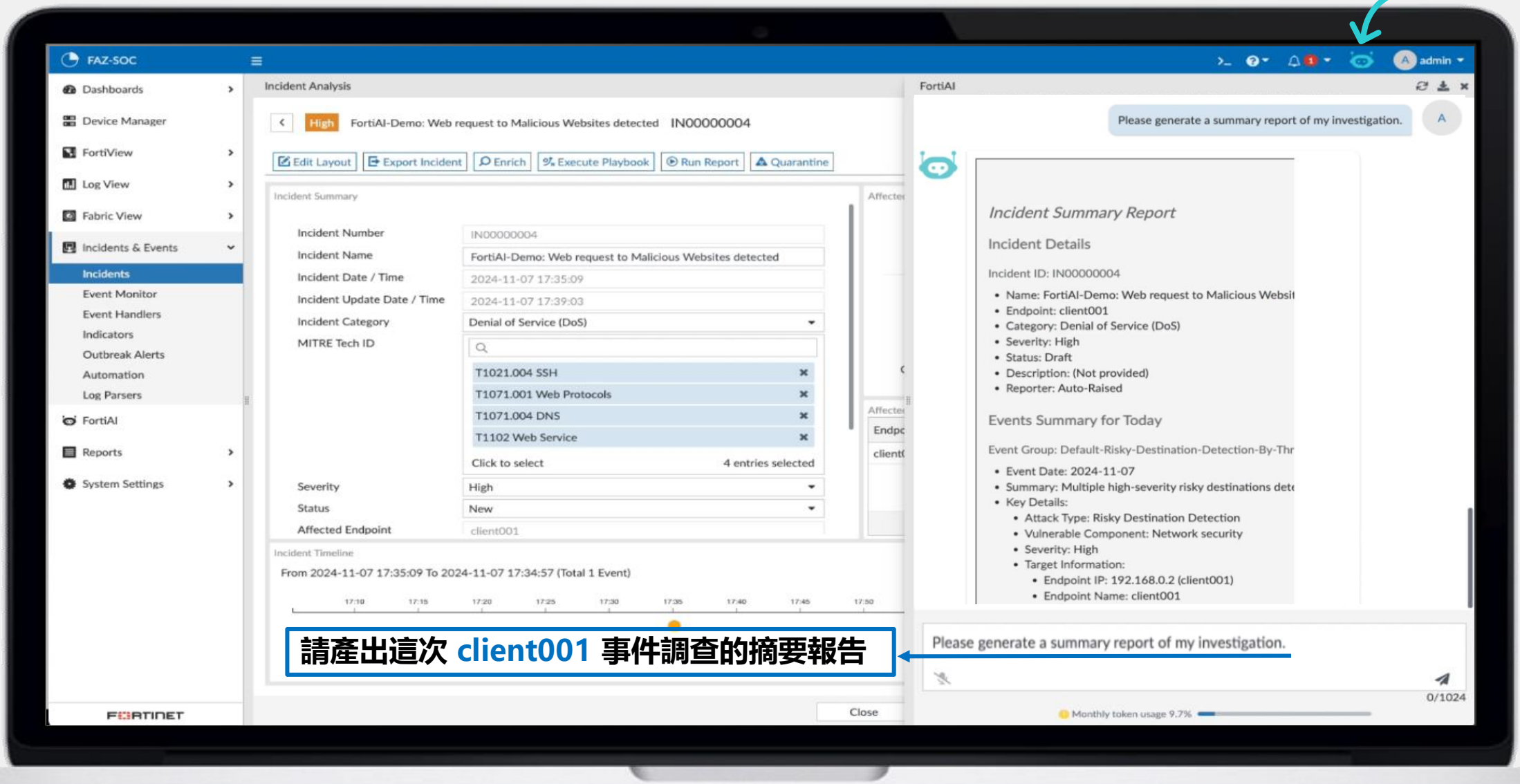
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，自動生成事件摘要



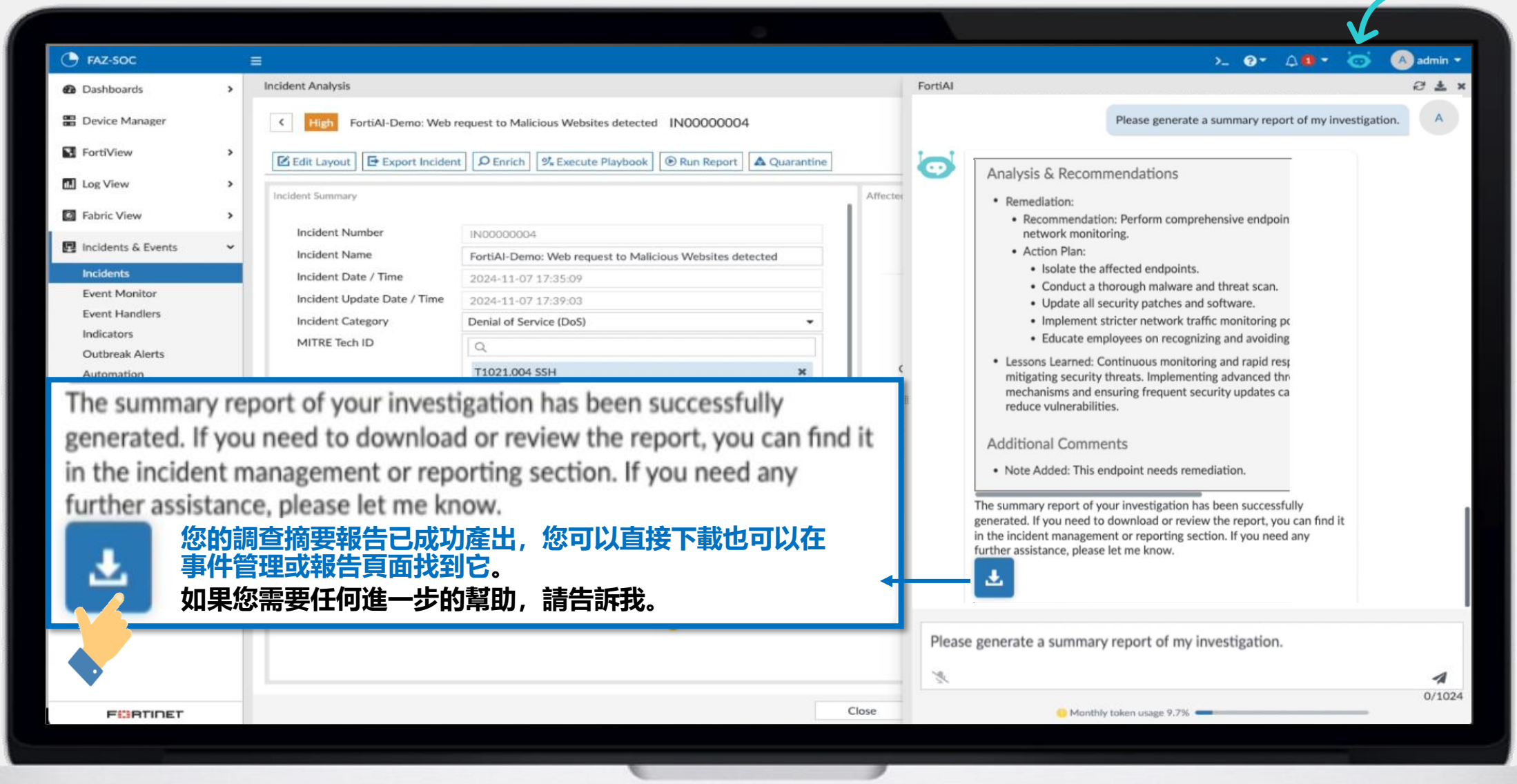
FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，自動生成事件摘要

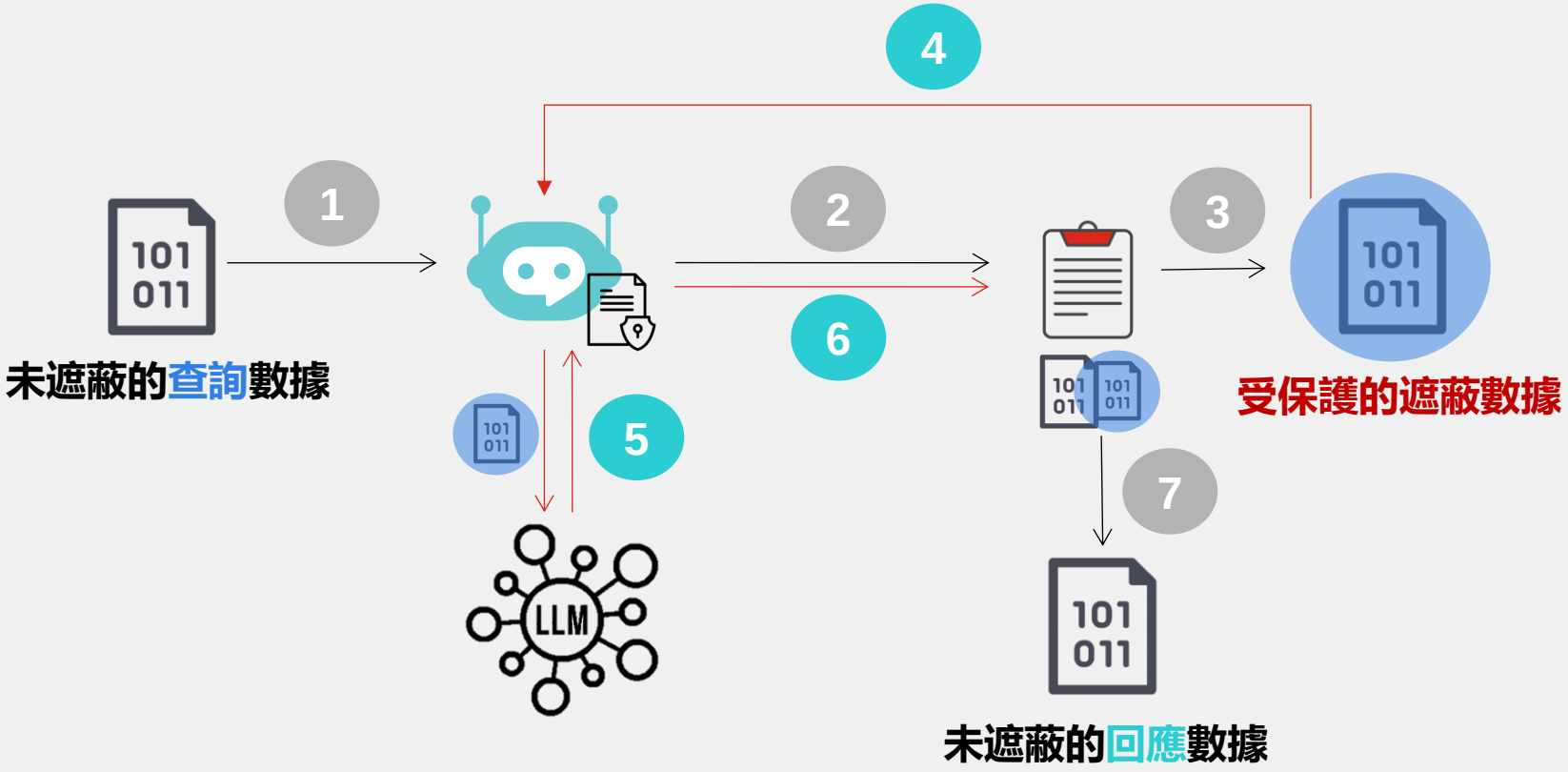


FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，自動生成事件摘要



FortiAI 保護客戶數據隱私安全 (Data Privacy)



受保護的數據列表

- ✓ IoT devices
  - MAC, vendors and hostnames
- ✓ FortiGate device name
- ✓ The "root" keyword
- ✓ VDOM names
- ✓ IPv4 and IPv6 addresses
- ✓ MAC addresses

FortiAI for FortiManager

CONFIDENTIAL

Access Limited to Authorized Personnel

FortiManager 被忽略的能量

設定即忘

- FortiManager 功能很強大，但常常忘了要在哪裡配置設定。
- 客戶有時會習慣直接在 FortiGate 配置設定。

大材小用

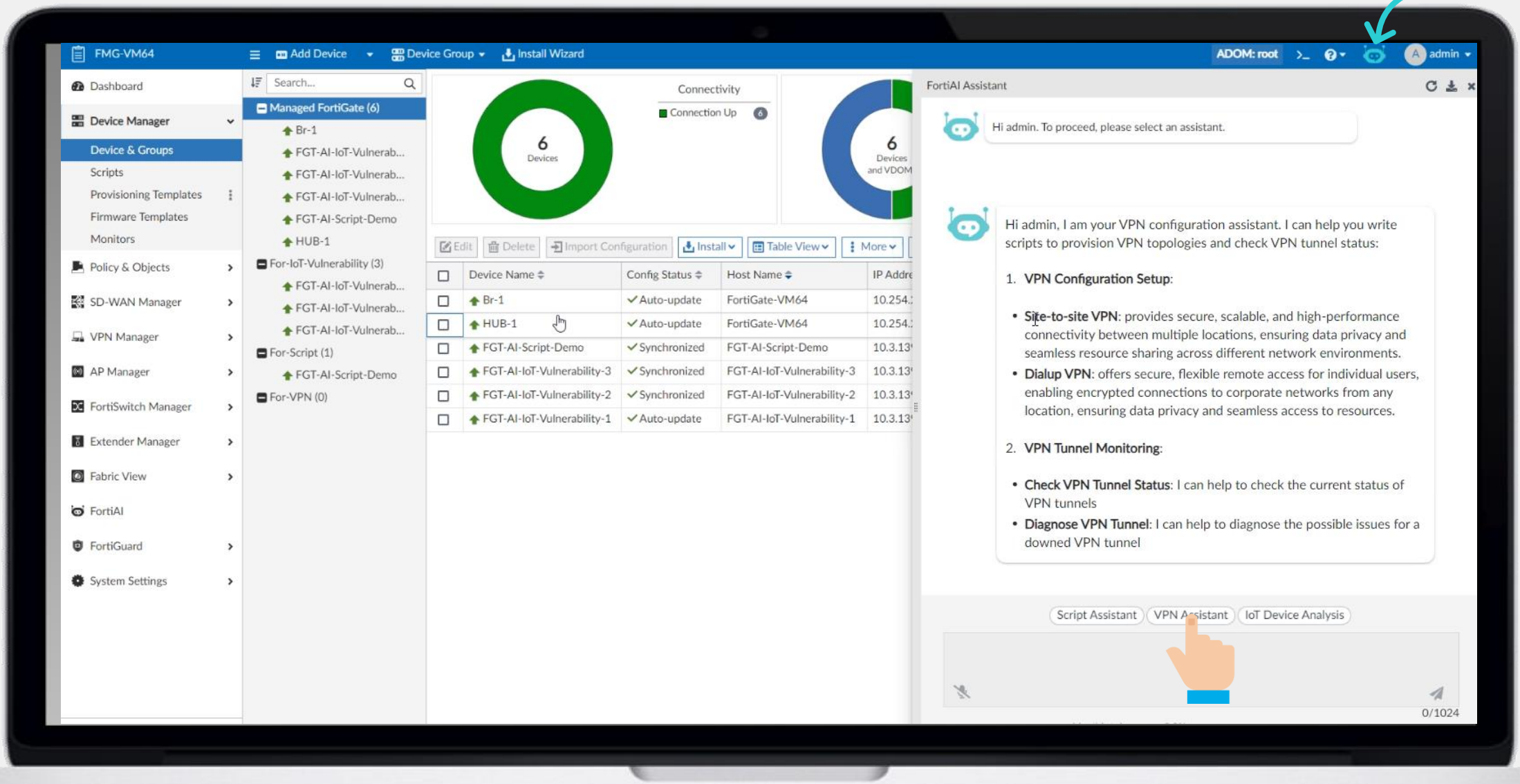
- FortiManager 功能很強大，但許多客戶並未充分利用它。
- 他們經常僅僅用於政策配置，大多數客戶只使用了 20% 功能。

獨立使用

- 大部分獨立運作，錯過了將 FortiManager 與其他 Fortinet 解決方案整合。
- 儘管擁有強大的管理平台，許多客戶仍未能實現高水平的整合。

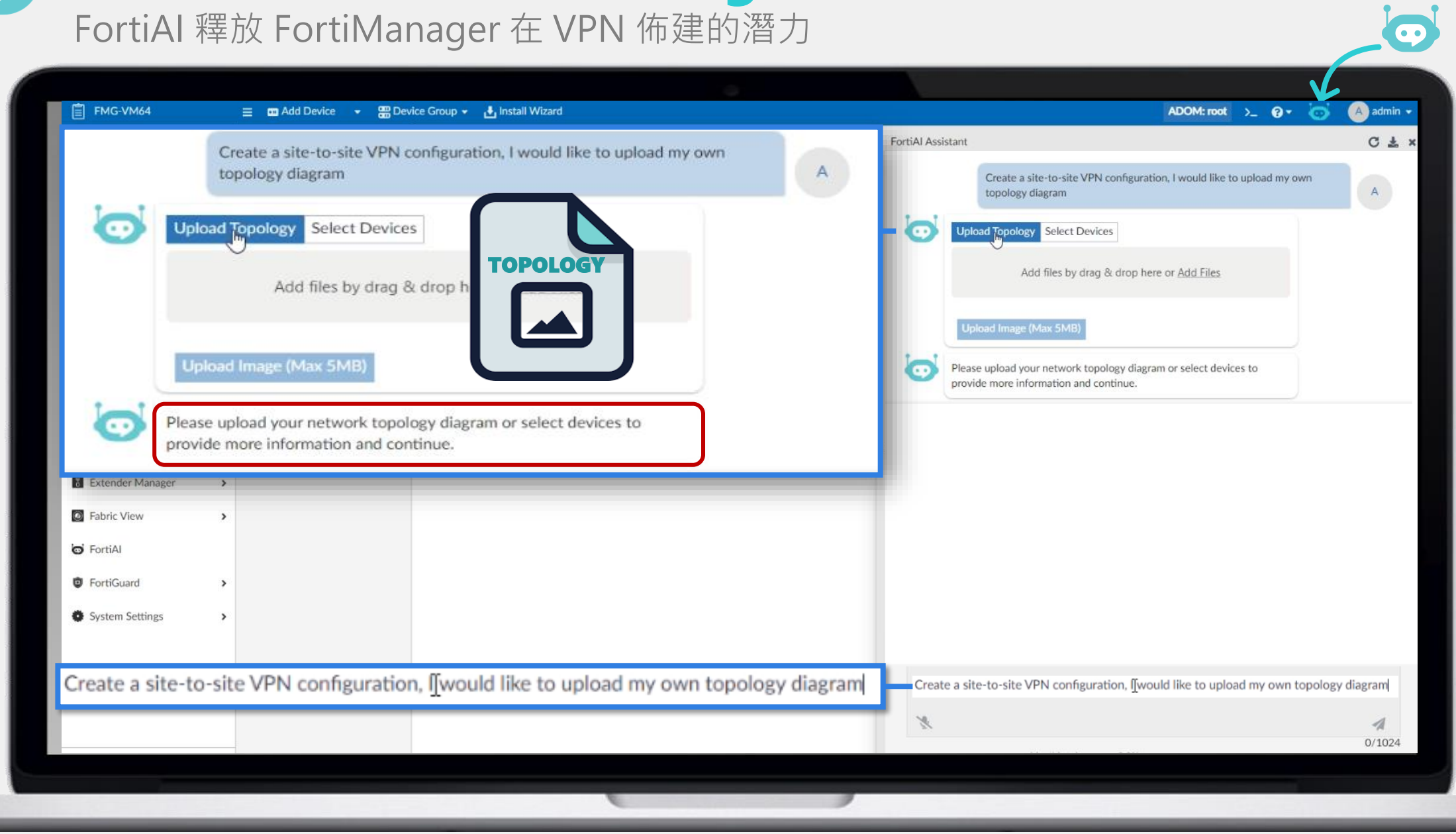
FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



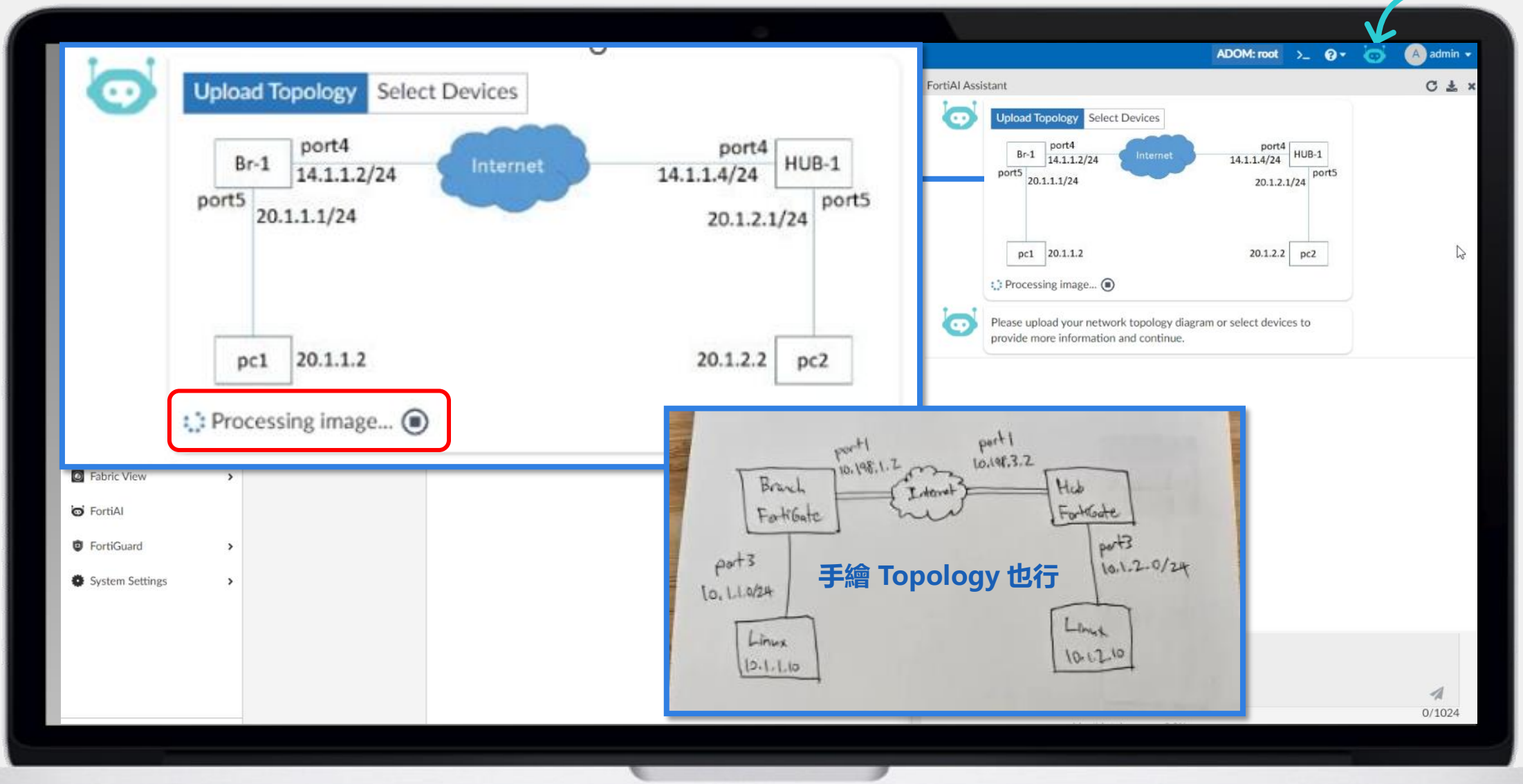
FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



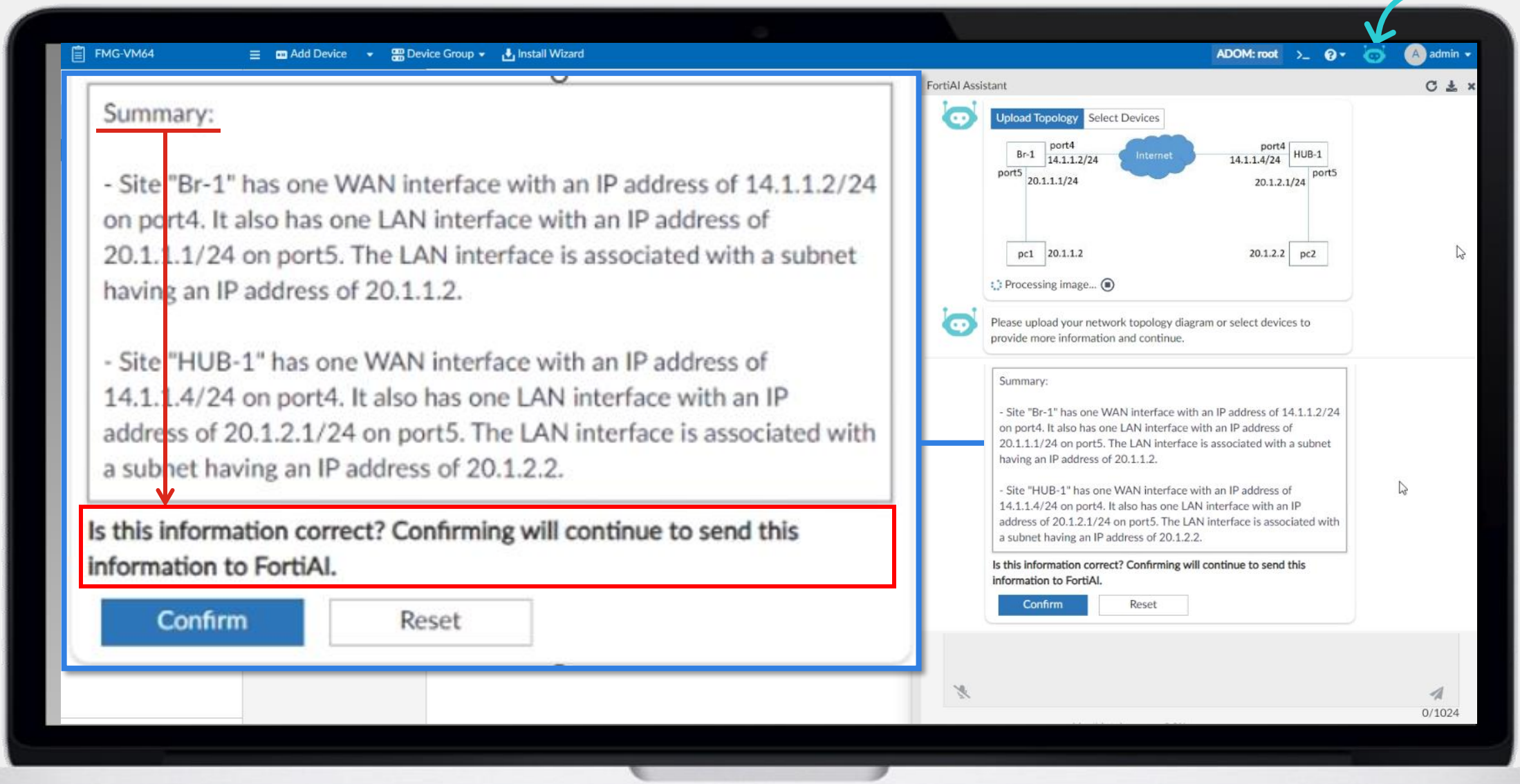
FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



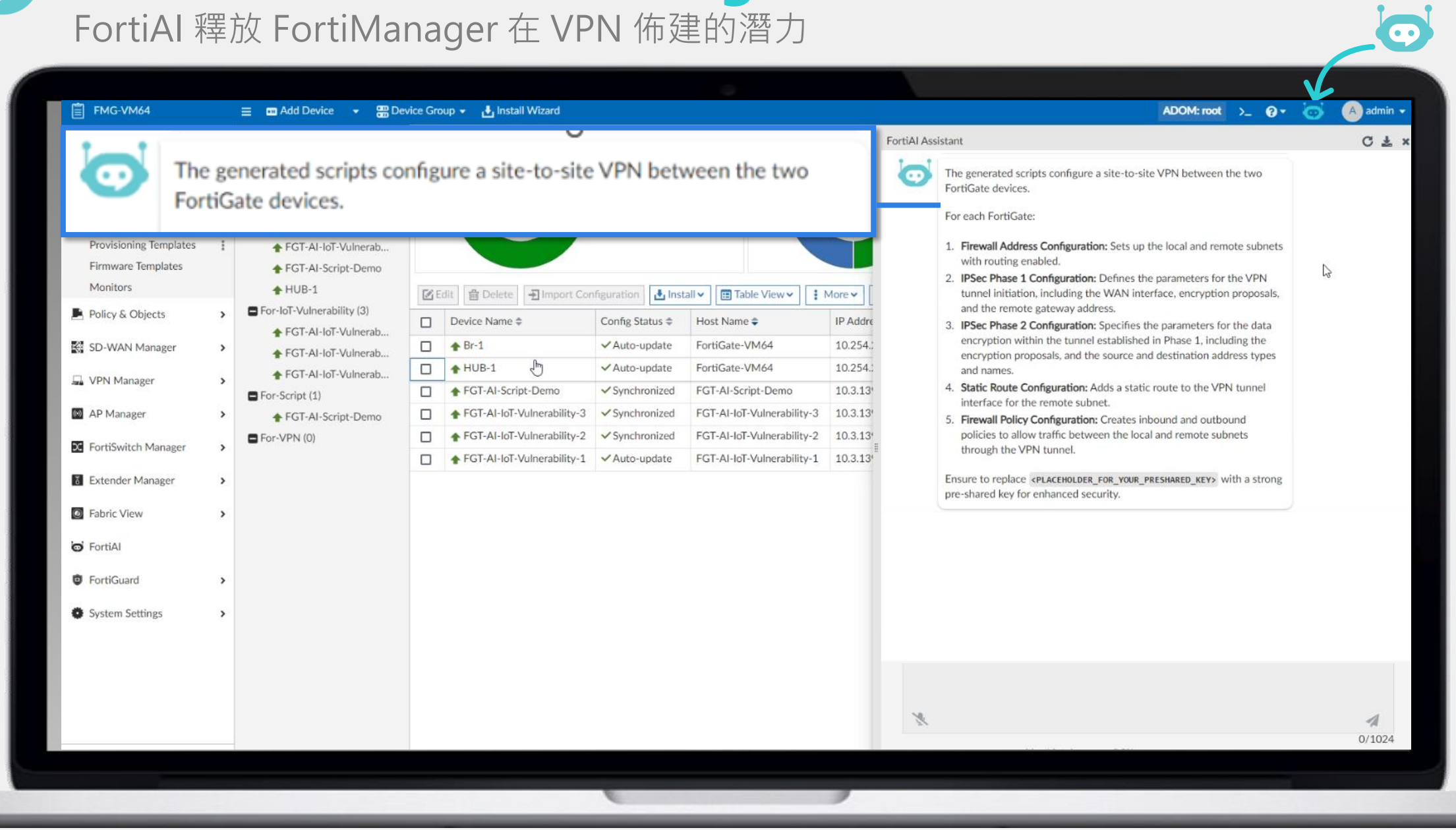
FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



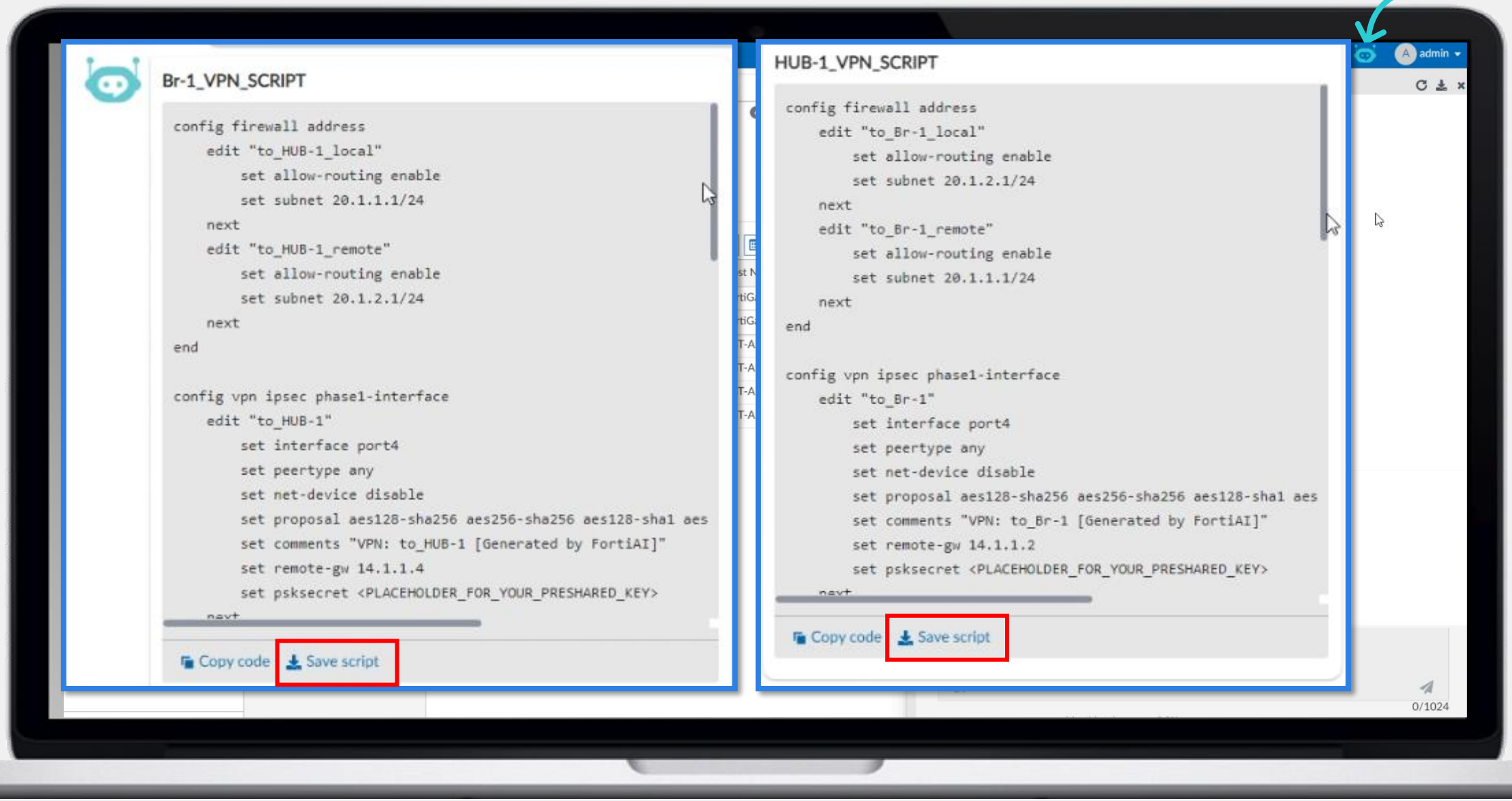
FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



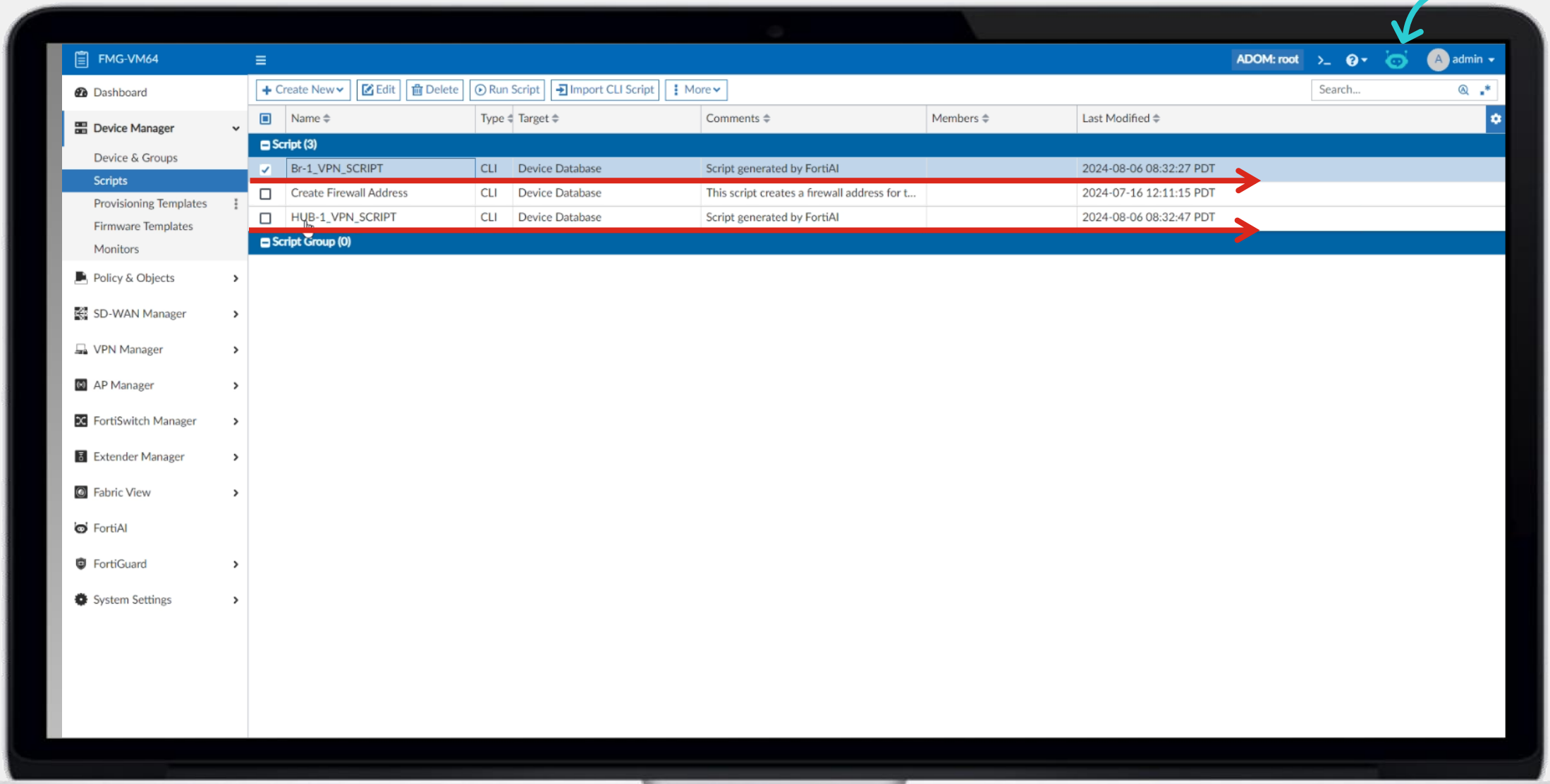
FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



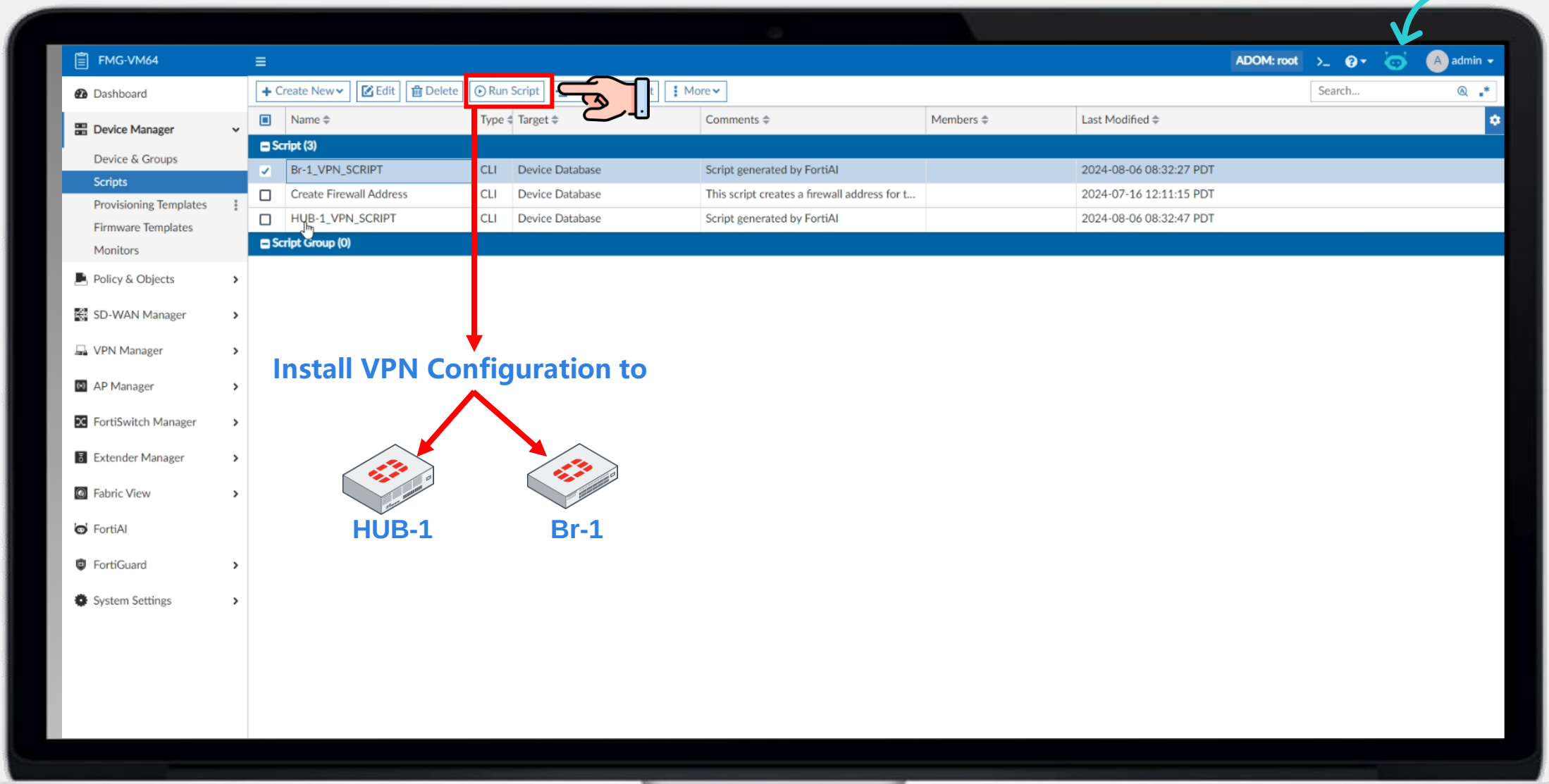
FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



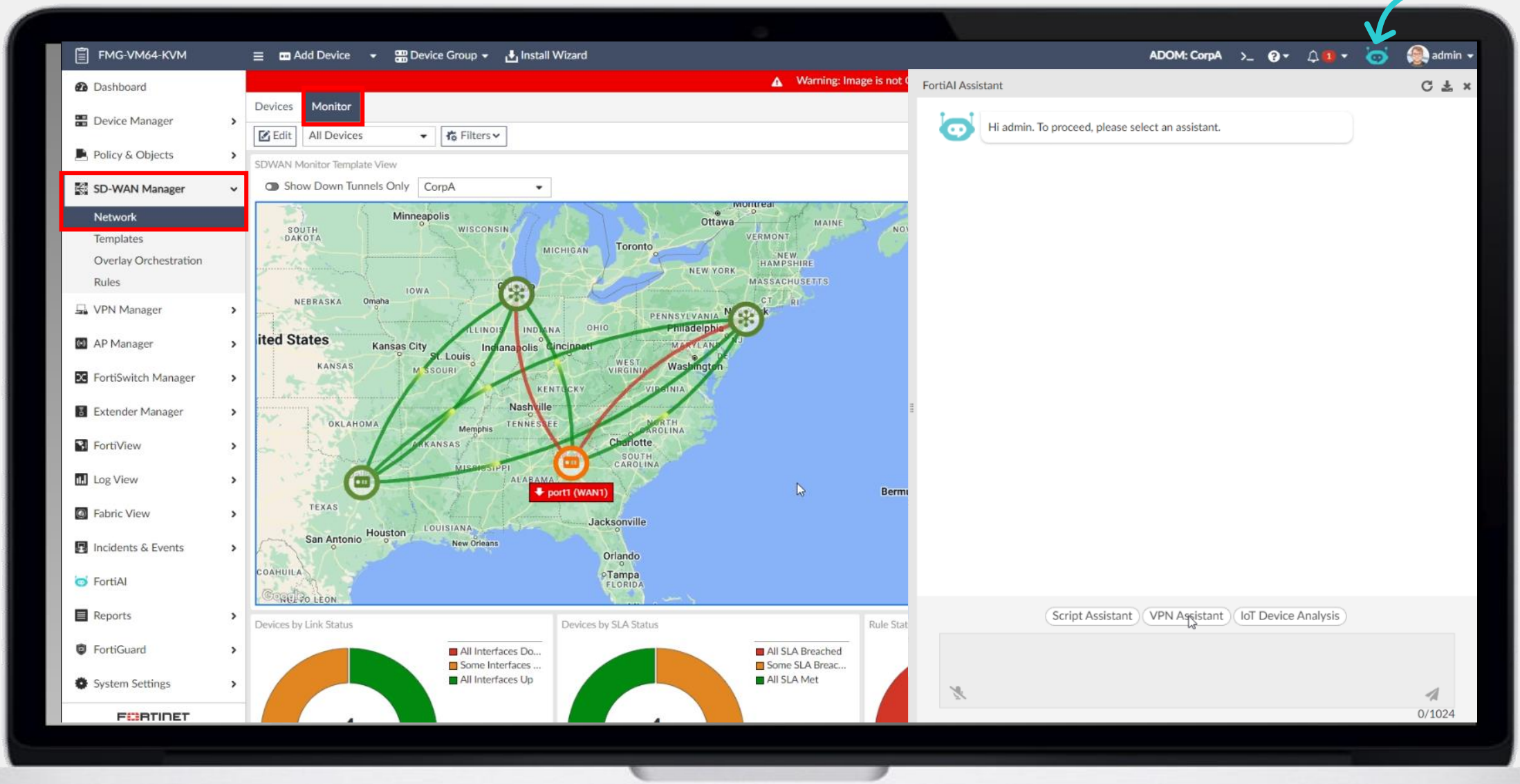
FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



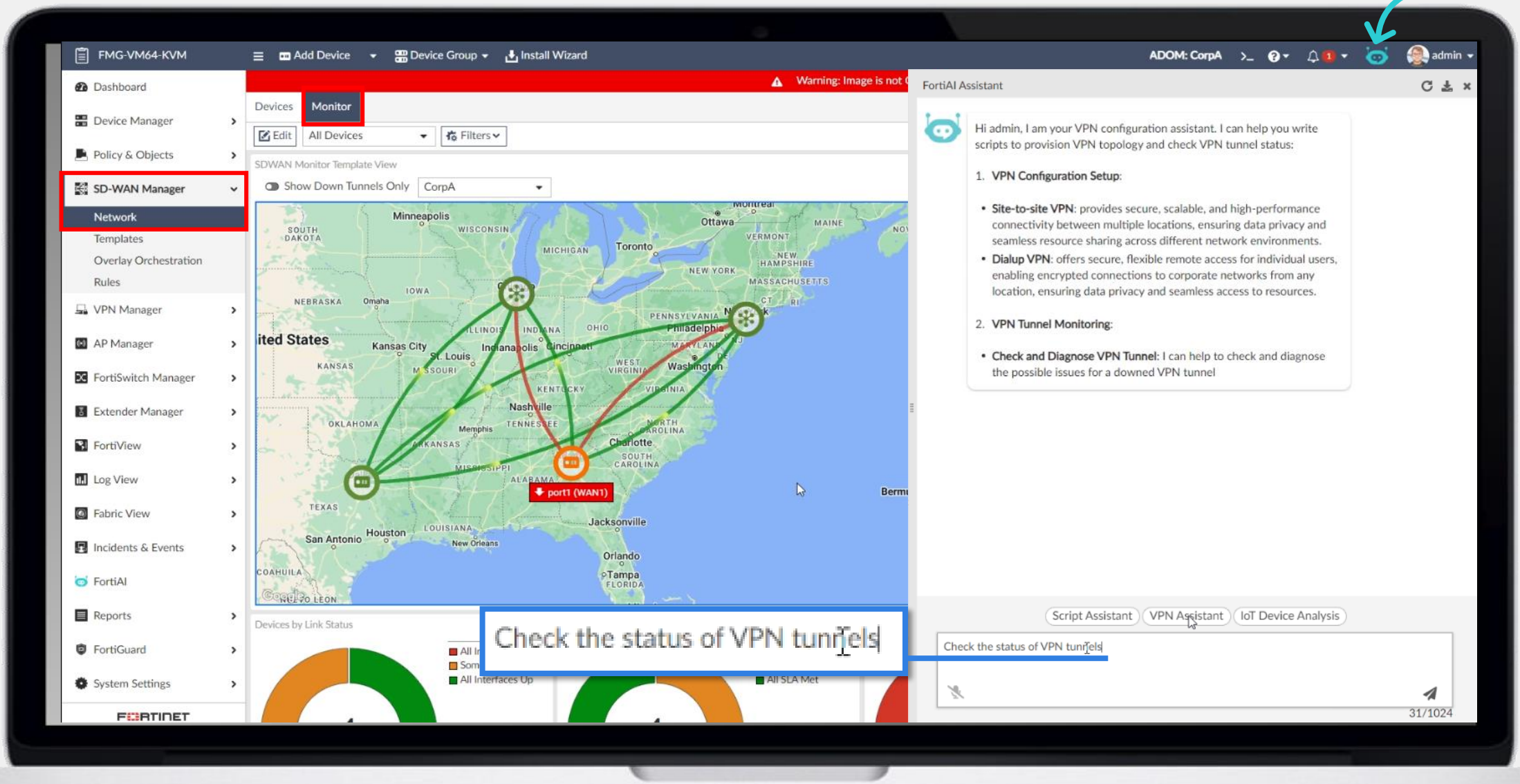
FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



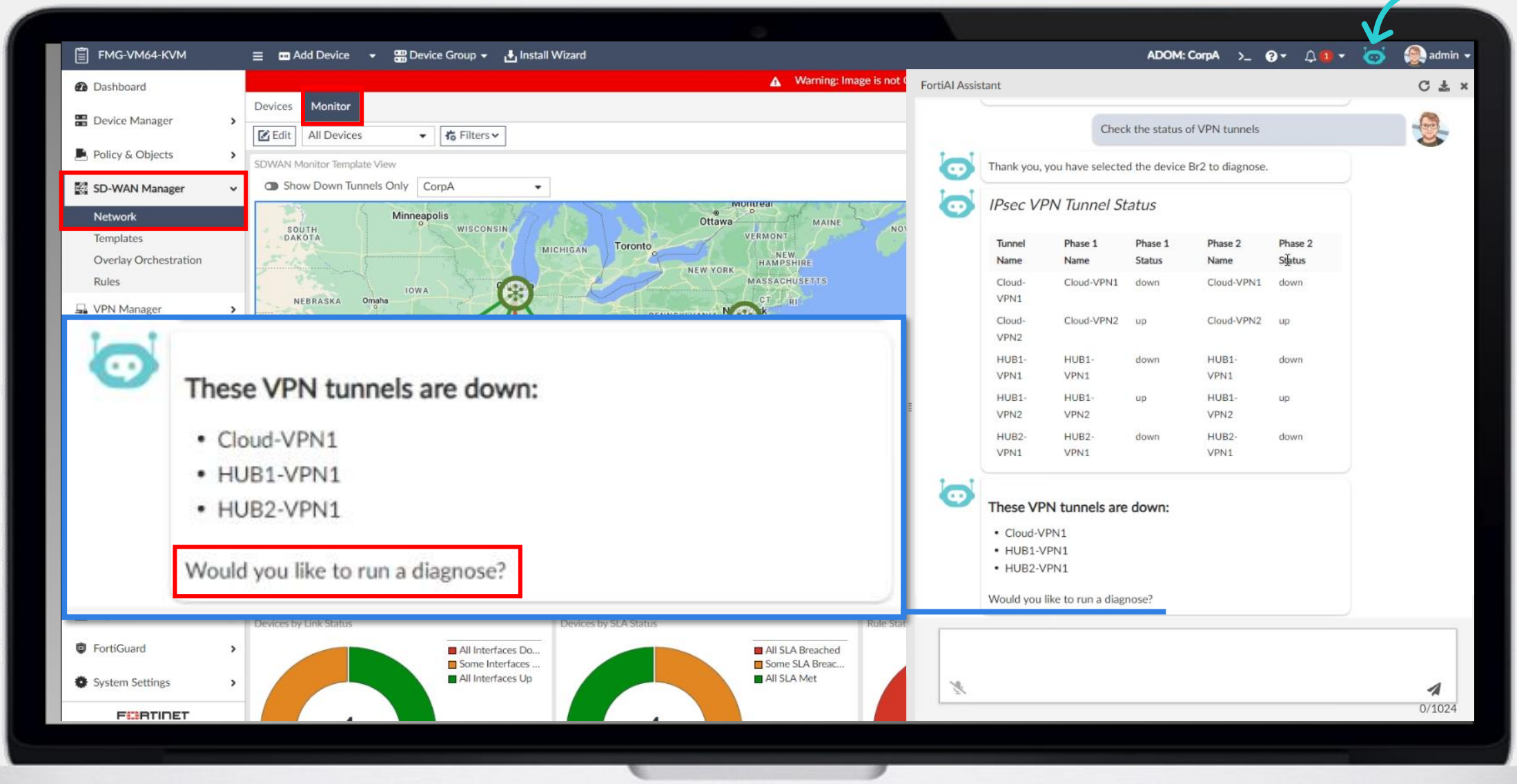
FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力

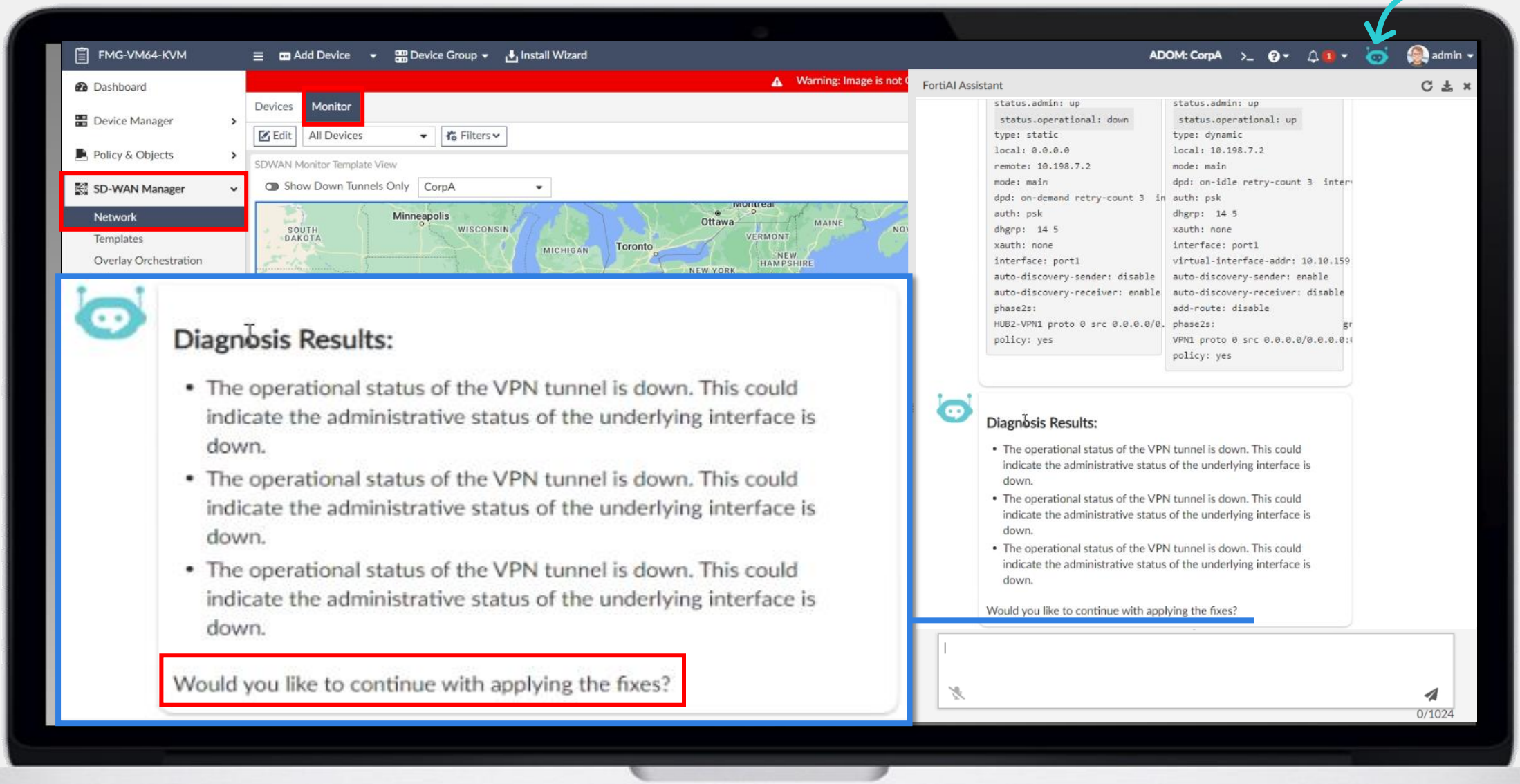


FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力

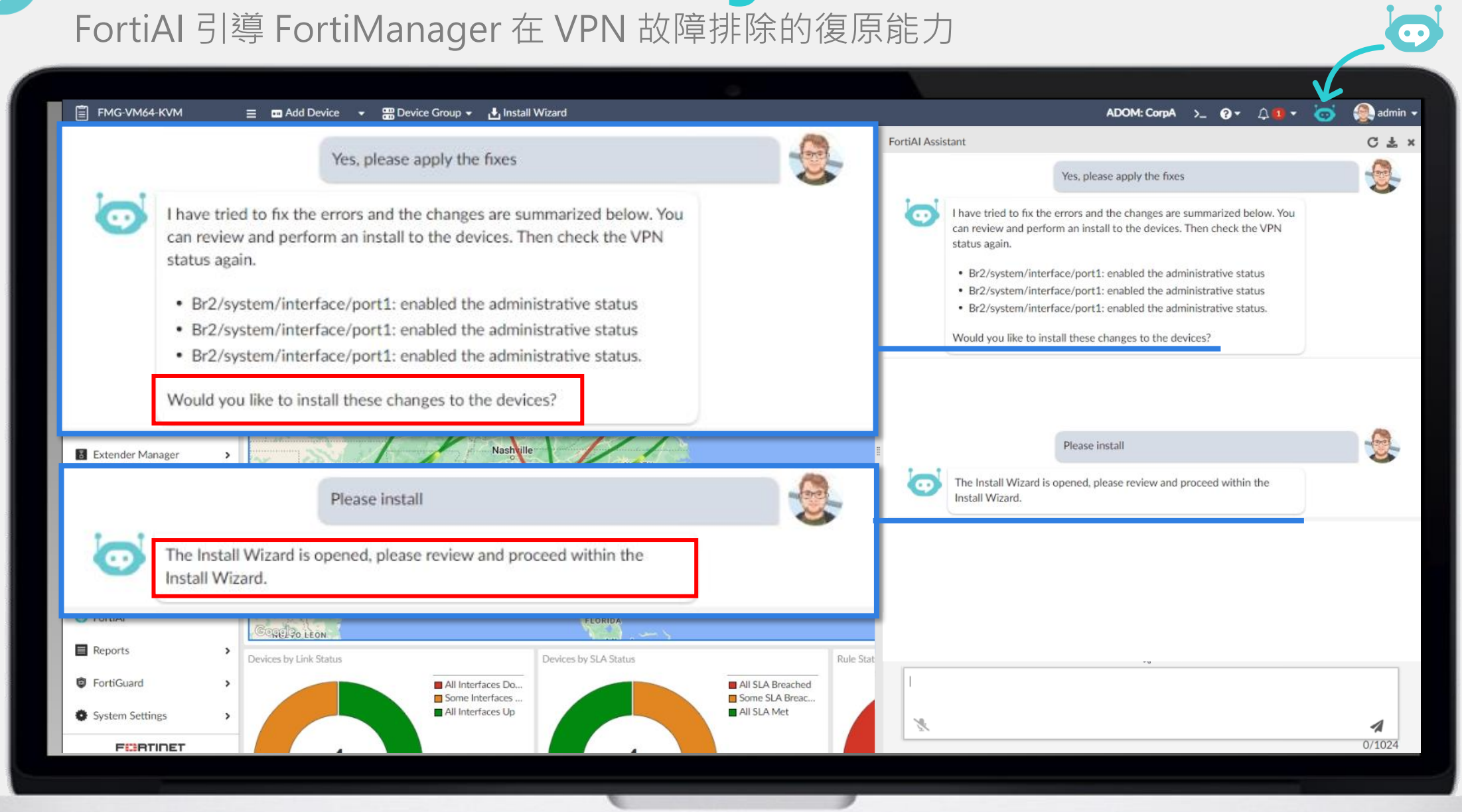
FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



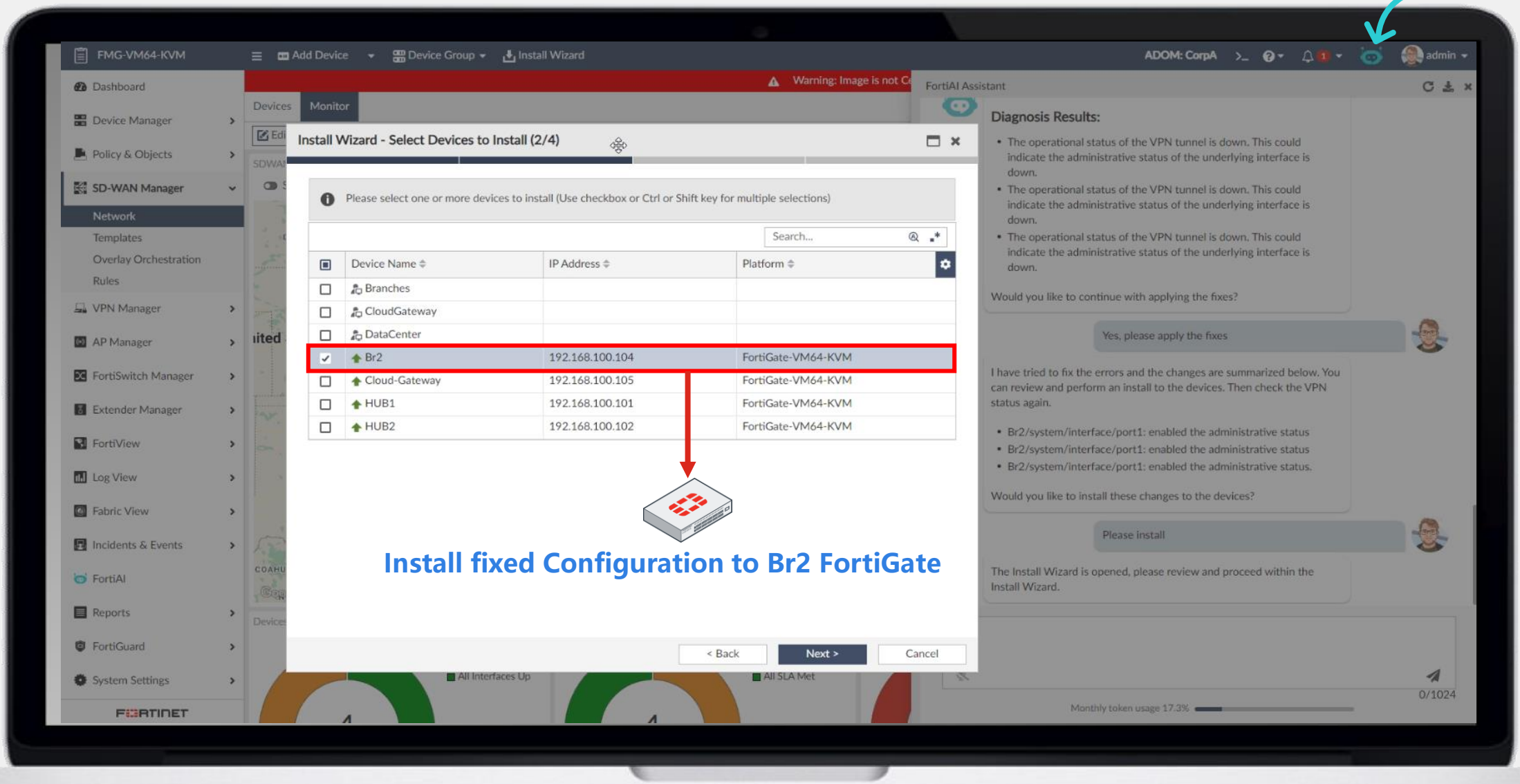
FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



FortiAI with FortiManager Demo

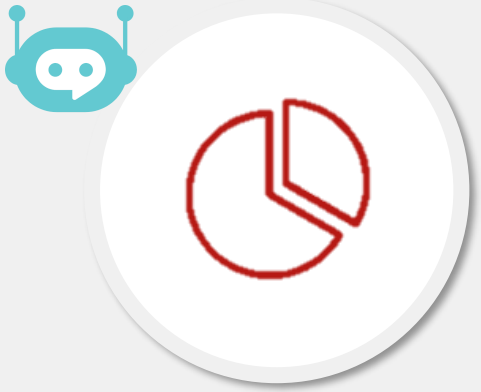
FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



FortiAI 釋放 FortiManager 的潛力

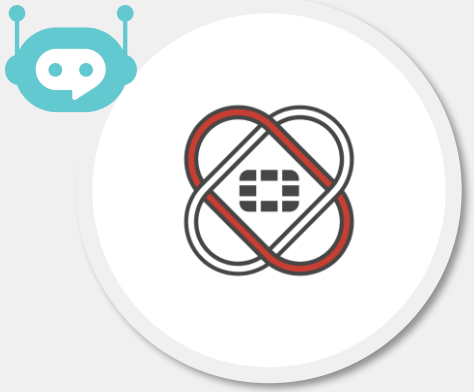
設定即忘

- 管理者與 FortiAI 有高度互動性和對話性。
- 人們將會更頻繁地使用它。



大材小用

- 成為工作中不可或缺的一部分。
- FortiAI 可以利用更多功能和能力來解決客戶的問題。



獨立使用

- 解決了方案之間的獨立使用問題。
- 借助 FortiAI，這些解決方案可以在幕後進行整合和自動化。

現今 SOC 與 NOC 面臨的維運挑戰

不僅需要佈署防護型資安解決方案，還需要建立自動化預警生態系統

太多供應商資訊難統整

大量日誌告警關聯分析困難

複合式新形態攻擊威脅

缺乏有經驗的資安人員

手動回應緩慢費工耗時易出錯

現今 SOC 與 NOC 迫切的需求

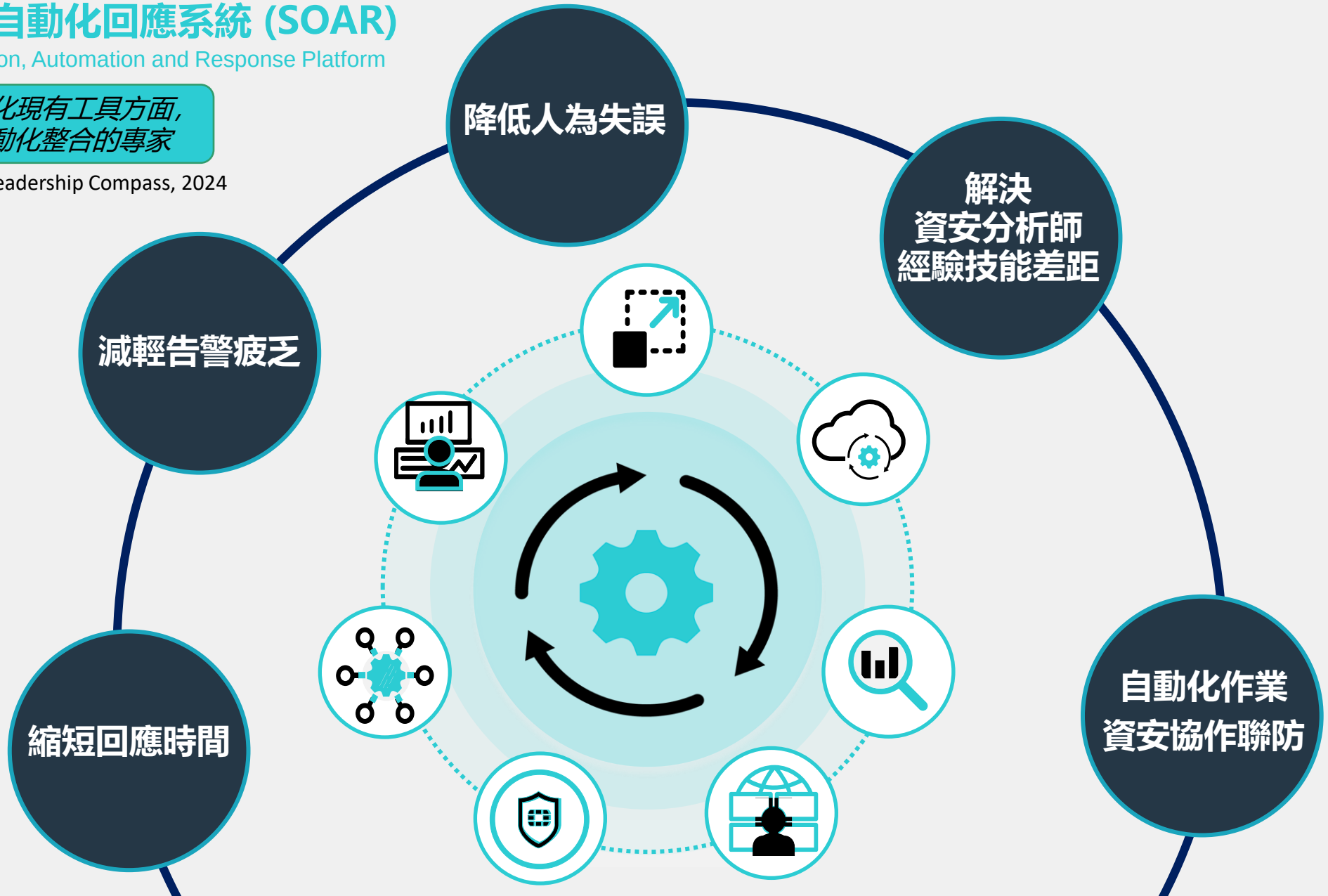
現今 SOC 與 NOC 迫切的需求：SOAR

安全協調，自動化回應系統 (SOAR)

Security Orchestration, Automation and Response Platform

在自動化和最大化現有工具方面，SOAR 堪稱自動化整合的專家

- KuppingerCole SOAR Leadership Compass, 2024



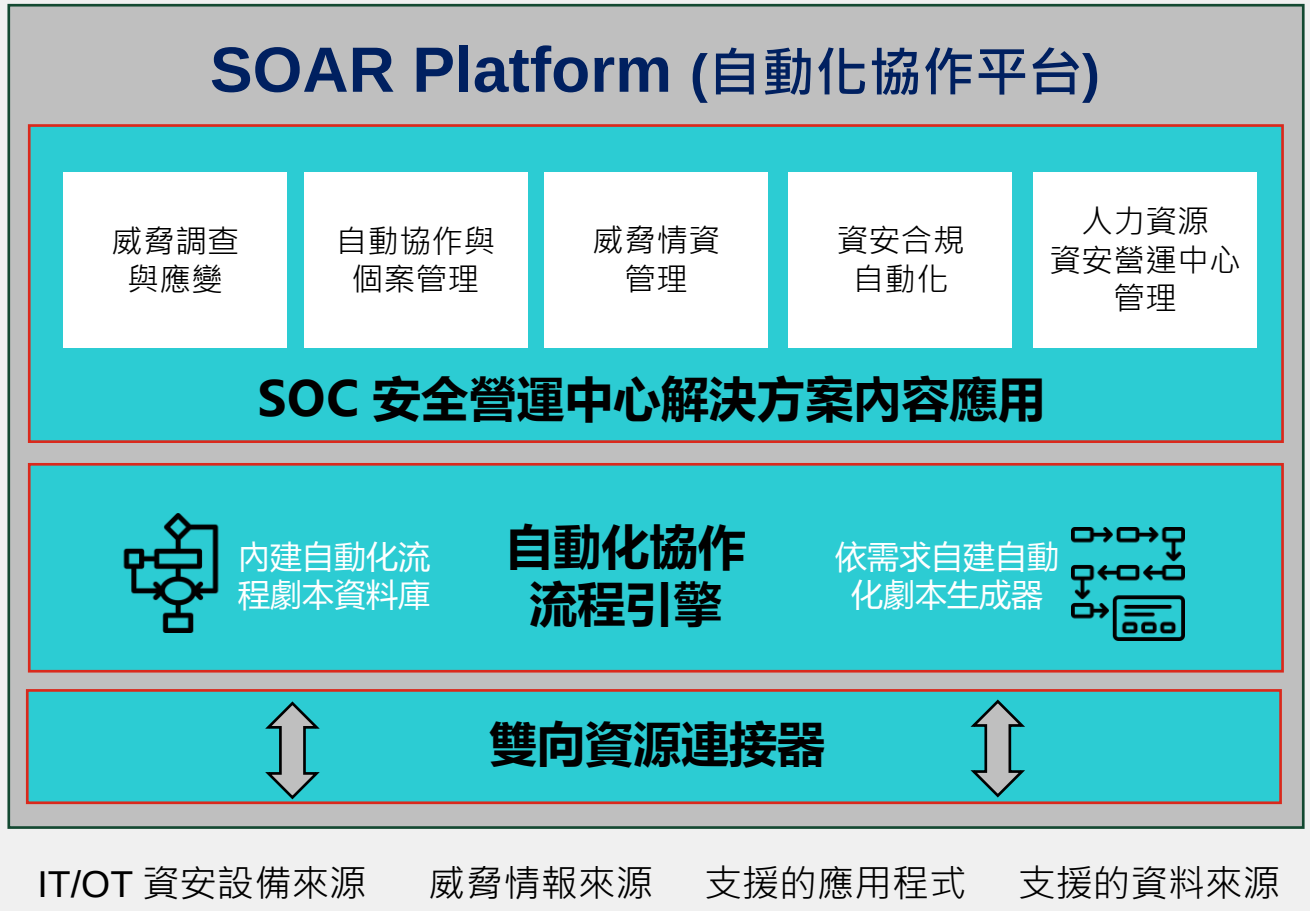
What is FortiSOAR

Security Orchestration, Automation & Response
安全協調，自動化回應系統 (SOAR)

A leader in the KuppingerCole 2024
& 2023 SOAR Leadership Compass

SOAR 自動化協作平台，能夠做到：

- **Connects (連結)**
  - 連接至外部任何應用程式、系統或數據來源
- **Executes (執行)**
  - 透過預設或自訂的自動化流程劇本(playbook)執行各種自動化作業流程
- **Supports (支援)**
  - 支援安全運營 (SecOps) 解決方案內容應用
- **Extends (擴展)**
  - 可將自動化作業流程擴展至網路運營中心(NOC)或任何其他功能的系統



SOAR 自動化協作平台普遍面臨的挑戰 (知易行難)

How to Investigating ?

資安事件調查該從何著手？

Response Plans ?

事件回應計畫如何制訂？
自動化劇本內容如何解讀？

Playbook Generation ?

自動化流程劇本如何建立？

導入生成式 AI 自動化流程建立與執行的好幫手

資安事件調查該從何著手？

- 提供告警的詳細資訊及最佳應對措施。
- 分析相關惡意軟體及其攻擊者的背景。
- 探討惡意軟體的作動機制、傳播方式及攻擊者慣用手法。
- 檢視對應該威脅攻擊者常用的 MITRE ATT&CK 戰術與技術。

讓我來幫忙

FortiAI 協助威脅事件調查

事件回應計畫如何制訂？
自動化劇本內容如何解讀？

- 提供勒索軟體告警應變計畫步驟 。
(如隔離受感染主機、通報資安團隊 ...等)
- 解讀 HTML 語法中的輸入字串語意。
- 解讀想了解的特定 Jinja 模板語法用途與運作邏輯。

讓我來幫忙

FortiAI 協助擬定應變計畫

自動化流程 Playbook 生成？

- 建立自動化流程聯動防火牆封鎖惡意 IP/Domain，並發送 Line 通知管理者。
- 針對觸發重大告警的資產啟動 Qualys 弱點掃描，並將掃描結果與該資產關聯分析後產出報告。
- 一旦發現弱點，自動在 ServiceNow 建立派工單 (Tickets)，進入 IR 事件處理流程。

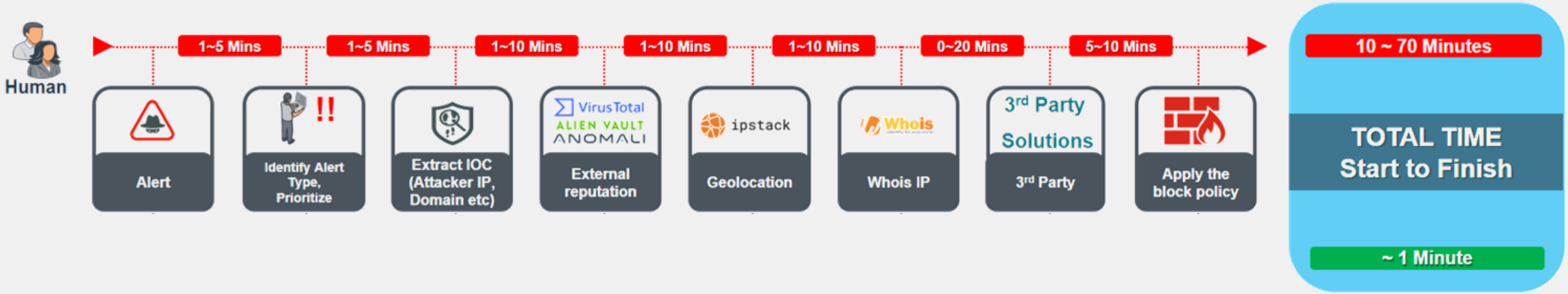
讓我來幫忙

FortiAI 協助自動化劇本生成

應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – 自動化協作系統作業流程圖示

SOC 資安事件協作處理流程：異常行為與 IOC 威脅與攻擊分析

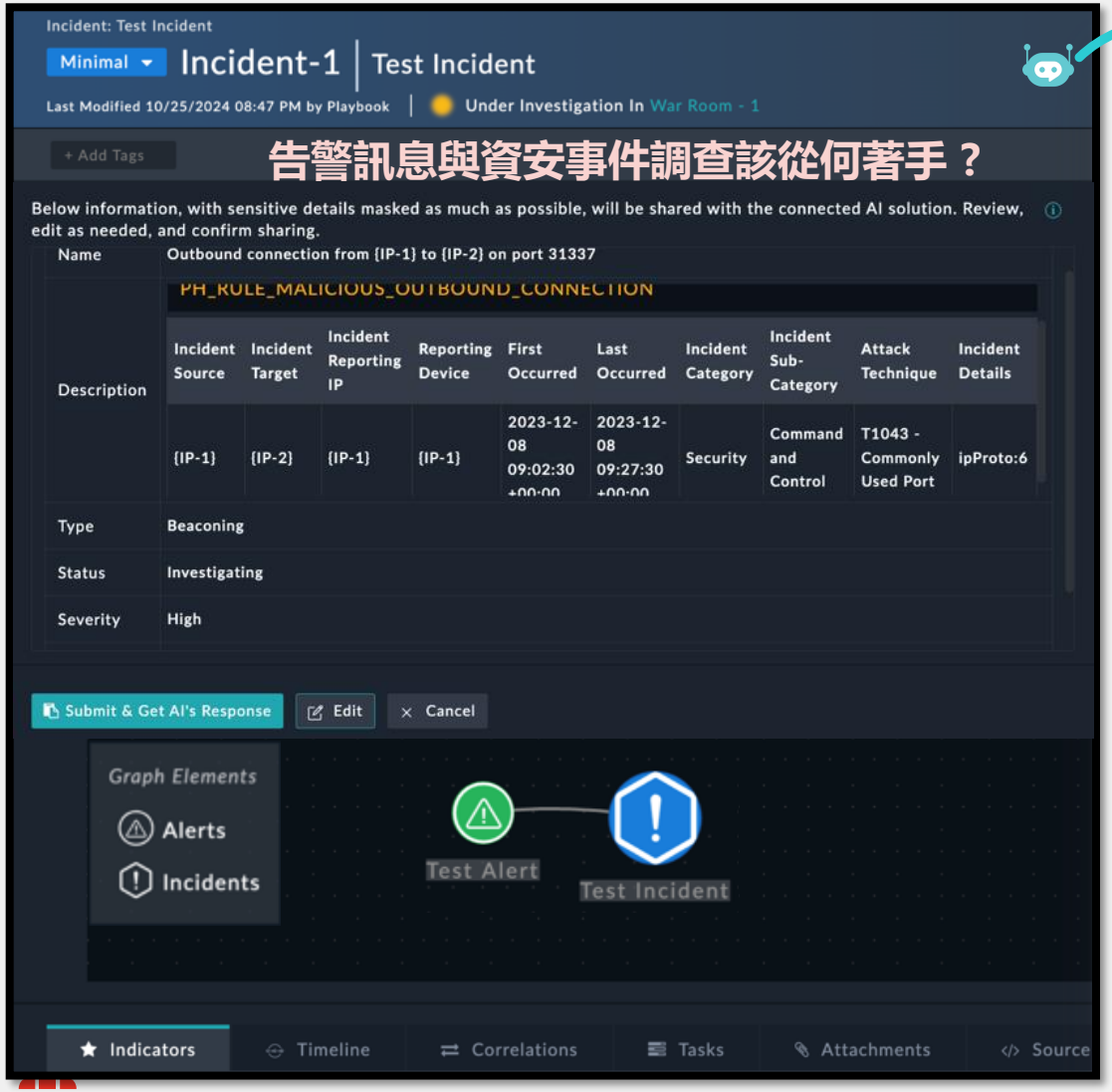


MTTR(Mean Time To Response) 資安事件平均回應處理時間

導入 FortiSOAR 自動化協作系統，大幅提升 SOC 營運效率並降低人為作業失誤

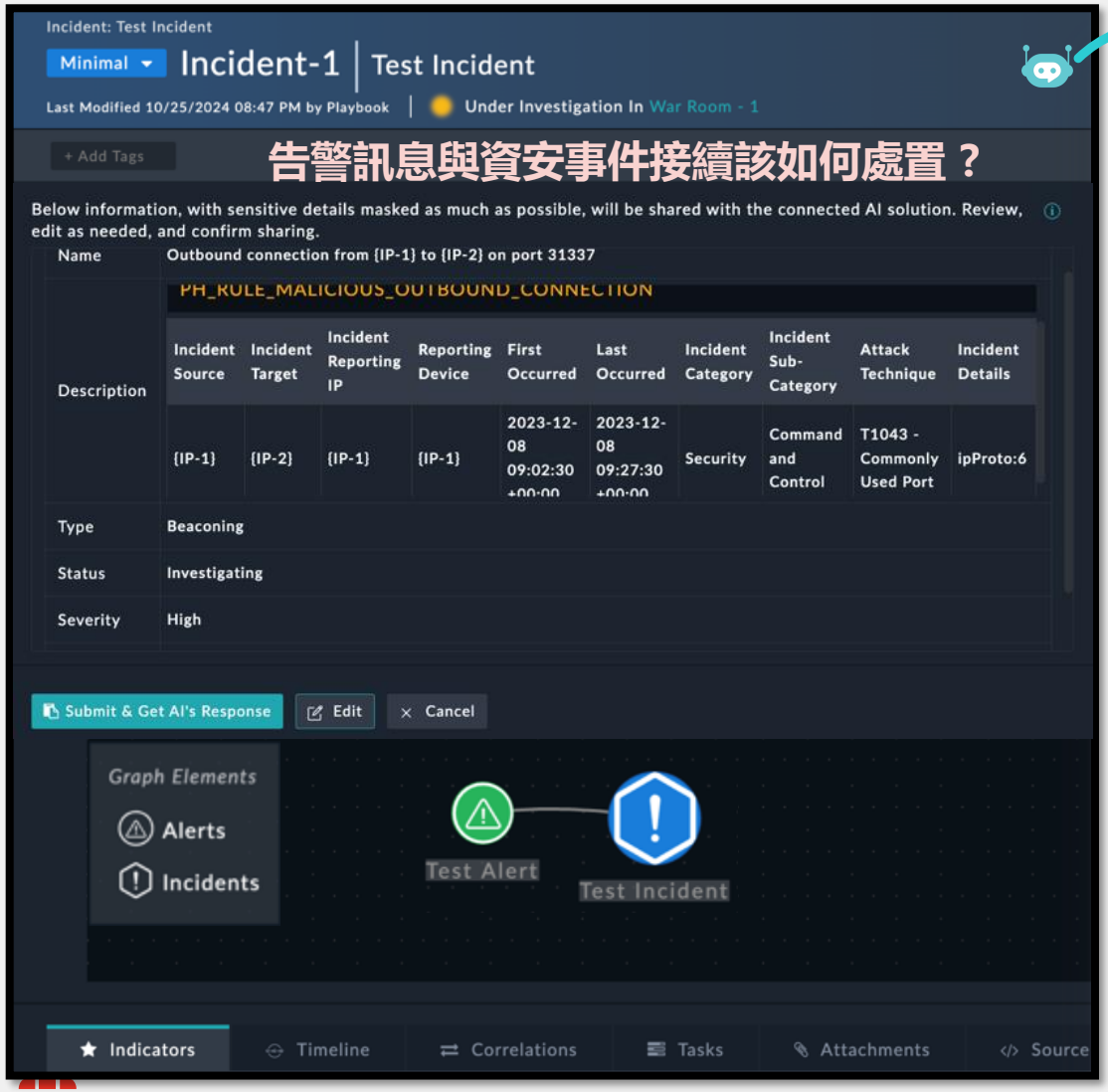
應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – FortiAI 解讀資安事件，並將事件摘要彙報予管理者



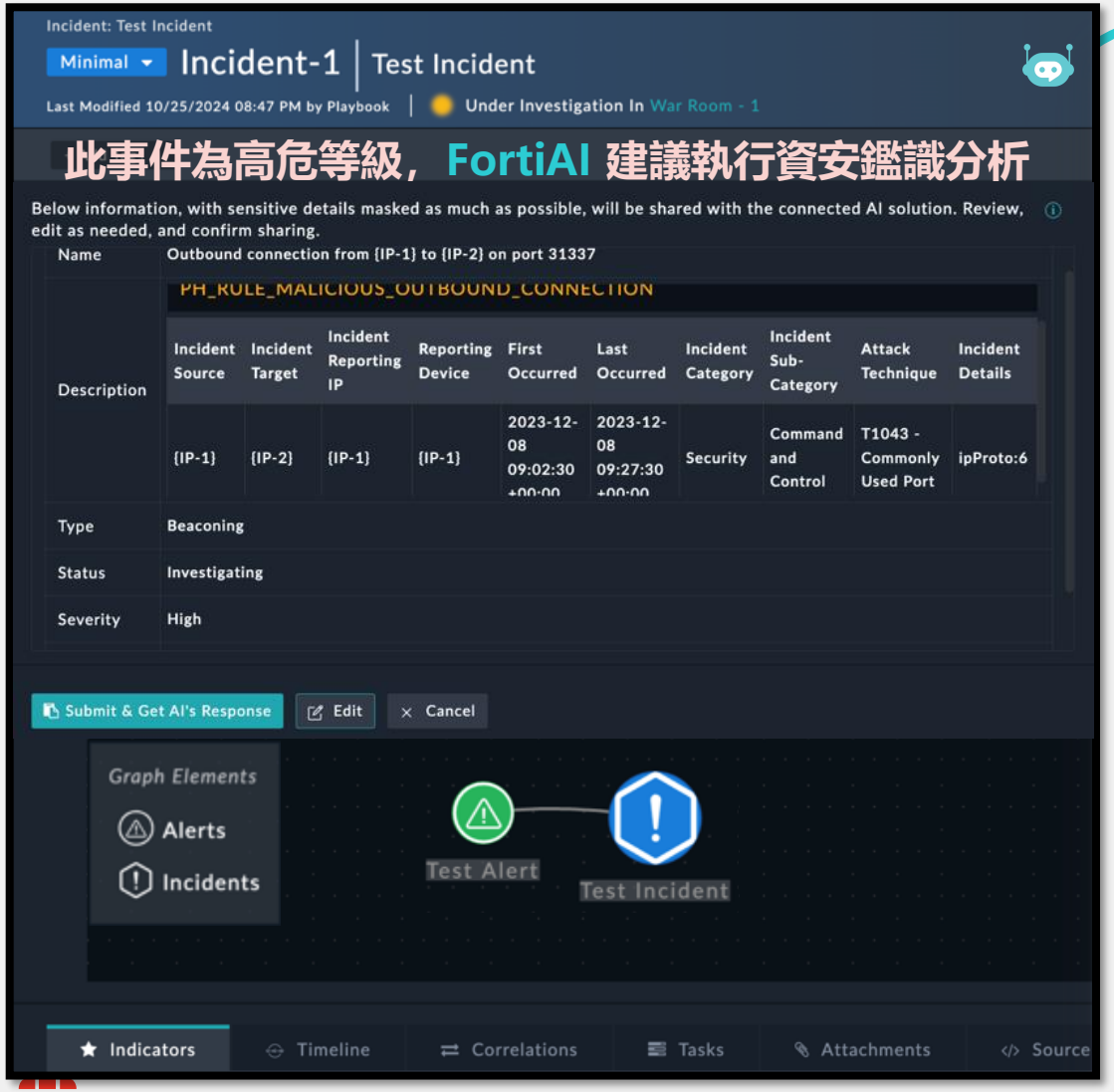
應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – FortiAI 解讀資安事件，並給予適當的處置建議彙報予管理者



應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – 透過 FortiAI 將事件升等至戰情室與資安分析師群共同會勘鑑識

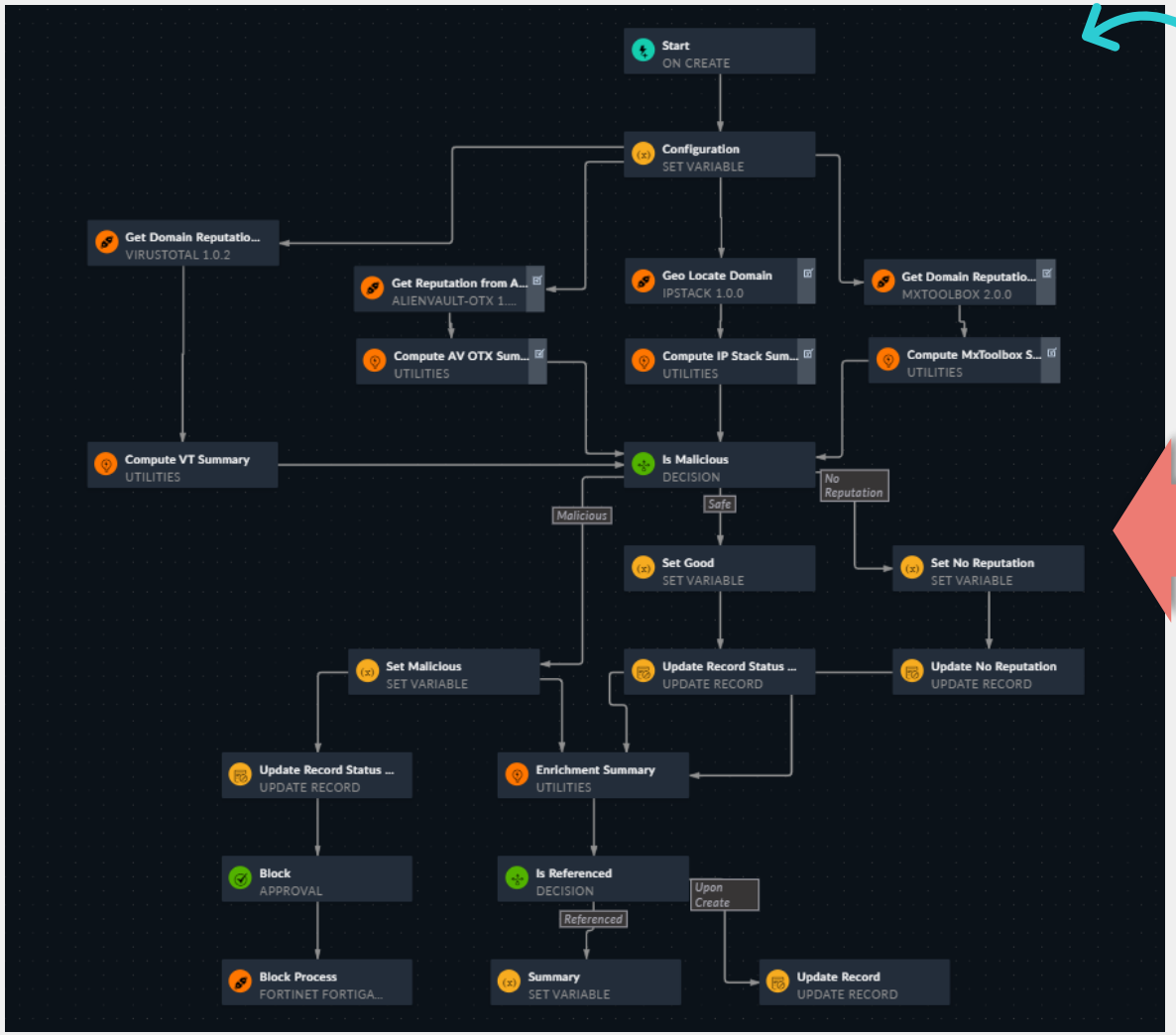


應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – 透過 FortiAI 將事件升等至戰情室與資安分析師群共同會勘鑑識

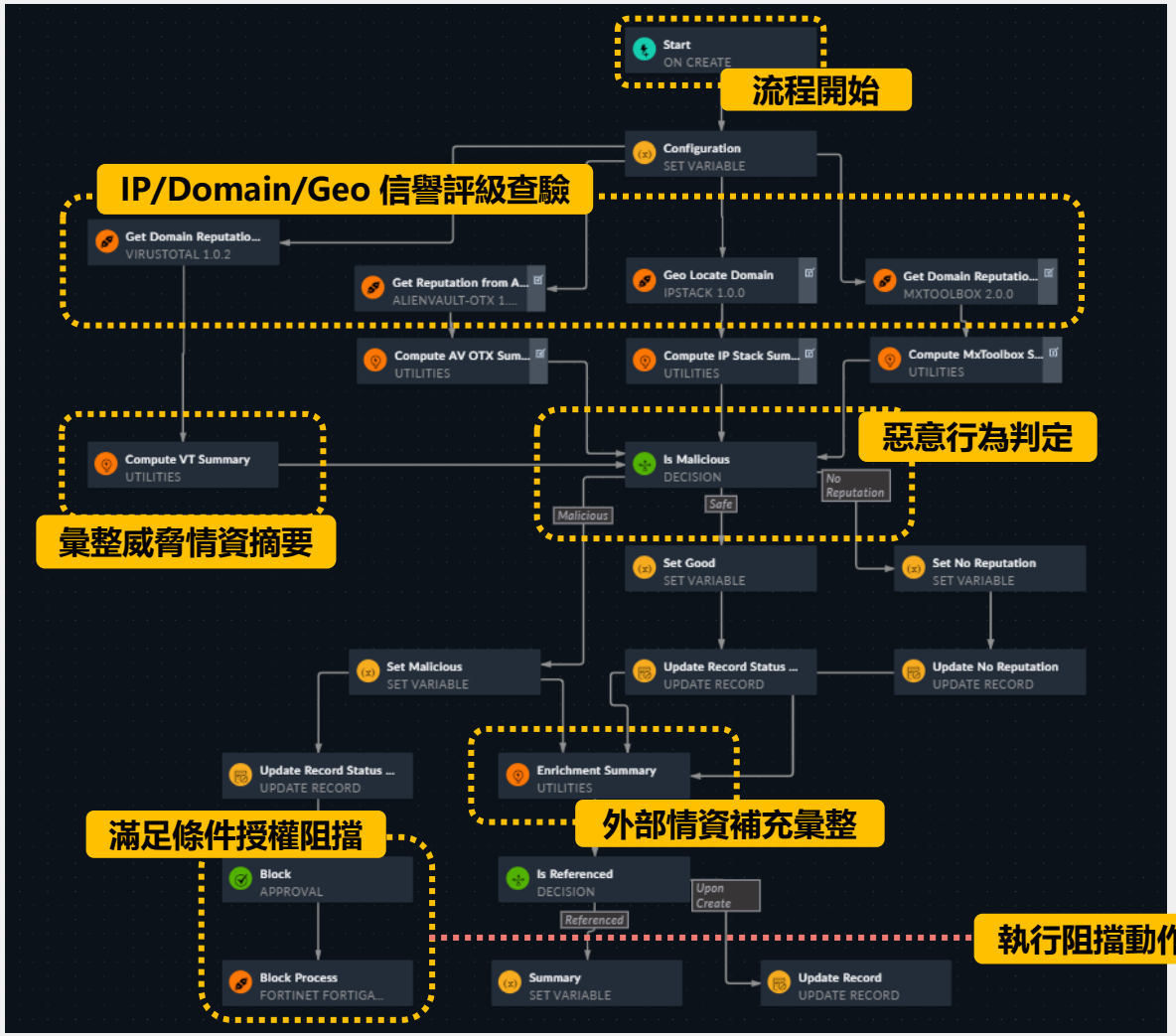
應用範例 – 安全威脅分析自動化作業流程

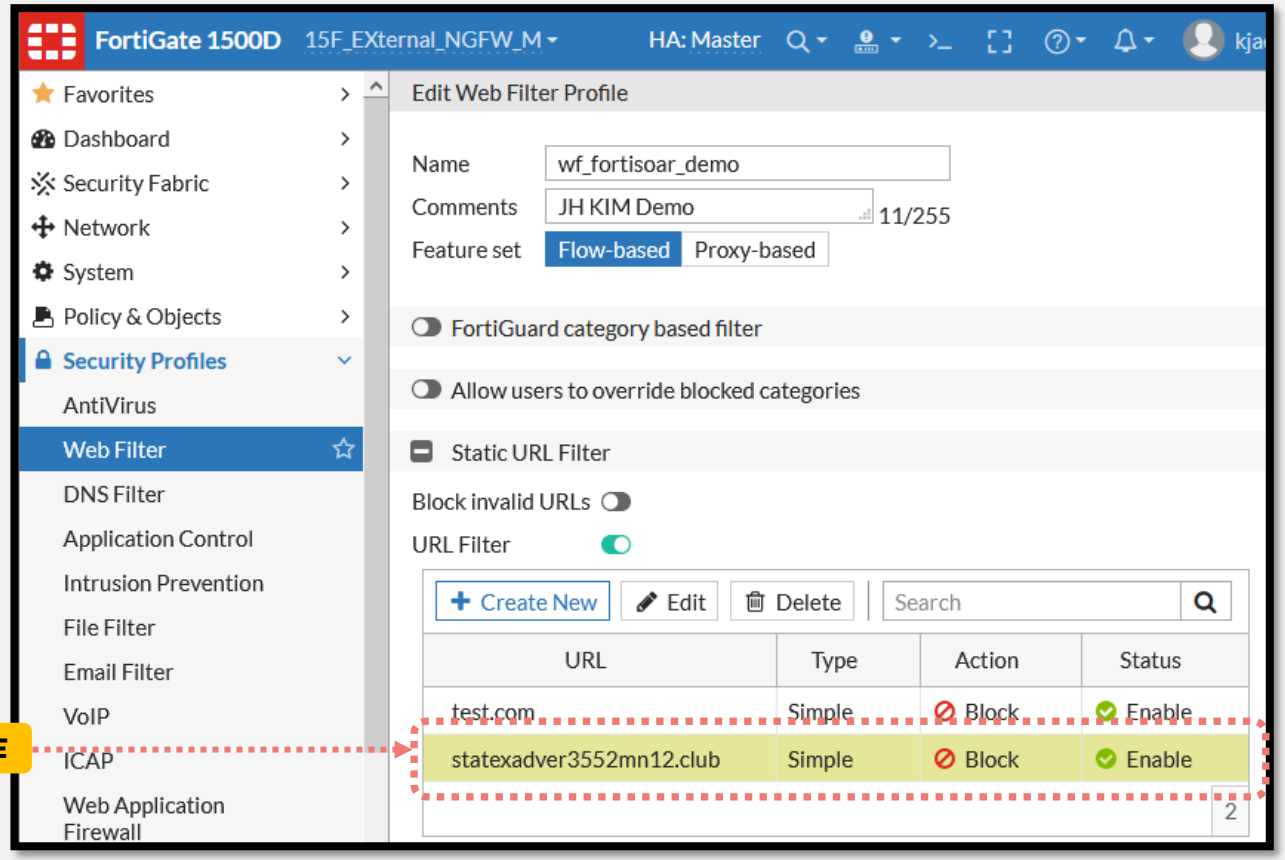
AI 智能 SOC 平台 (FortiSOAR) – 透過 FortiAI 生成 IOC 威脅攻擊自動化授權阻擋作業流程



應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – 透過 FortiAI 生成 IOC 威脅攻擊自動化授權阻擋作業流程






FORTINET