白皮書

隆重介紹 FortiOS 7.6

強化 Fortinet 的
即時網路安全作業系統

整合式安全的需求

過去數十年來，網路安全情勢一直都是以各自獨立的做法為主，在整個網路中部署個別產品，而網路連結與資安則是各自為政。這種分散策略留下了重大漏洞，迫使組織胡亂拼湊不同的單點解決方案，造成了複雜性也阻礙了可視性。然而，Fortinet 始終倡導不同的願景：網路連結與資安的融合。基於整合式安全的原則，我們認識到真正的網路保護需要全面性的平台做法。

我們長期致力於開發並提供一個統一平台，而 FortiOS 7.6 的發布，我們領先業界的作業系統的最新更新，進一步鞏固了這點。這項更新為 Fortinet 安全織網，當今市場上最成熟、最全面的網路安全平台，帶來了新的功能與服務。與剛加入平台趨勢的競爭對手不同，我們多年來一直在努力建構並完善安全織網，從而獲得了最廣泛的產品覆蓋範圍。這些最新的安全織網強化功能包括：在我們的三大支柱中加入新的生成式 AI 功能；為我們的防火牆、SASE 和 SOC 營運加入新的託管服務；為我們的統一代理程式帶來新的整合；以及新的資料保護。

「FortiOS 是世界上最強大的即時網路安全作業系統，能夠簡化內容、應用、用戶、裝置、資料以及位置的管理。」

謝青
Fortinet 創辦人
董事長
兼執行長

這種統一平台方法的力量在於其獨特的核心：

- **單一作業系統（FortiOS）：**我們致力於提供基於單一作業系統的整合式網路與安全平台，這體現在我們於多項 Gartner 魔力象限類別中領先業界的地位，包括防火牆、LAN 邊緣、SD-WAN 和安全存取服務邊緣（SASE）──這一切都由相同的 FortiOS 提供支援。這種整合方法消除了管理不同系統的複雜性，並確保整個網路中安全策略與實施的一致性。
- **單一統一代理程式（FortiClient）：**Fortinet 代理程式為資訊科技團隊提供無與倫比的遙測、可視性與掌控。它無縫整合端點保護平台（EPP）和零信任網路存取（ZTNA）功能，再加上即將推出的端點偵測與回應（EDR），為你的端點提供全面性的安全態勢，還可以與其餘的網路安全框架和 SOC 環境無縫整合。
- **單一管理工具（FortiManager）：**我們的統一管理工具可以對整個混合式環境進行集中控制，從你的園區和資料中心到你的分支辦公室，從遠端用戶到你的多雲環境。FortiManager 簡化本地、雲端以及雲端交付安全解決方案的管理，提供單一管理平台以實現全面性的網路可視性與控管。
- **單一資料湖（FortiAnalyzer）：**我們新發表的資料湖可以當作安全營運中心（SOC）分析的中央儲存器。這項統一的資料平台簡化了威脅偵測、調查和回應，讓你的安全團隊有能力做出更快速、更有根據的決策。

透過利用單一的作業系統、代理程式、管理工具和資料湖，Fortinet 安全織網打破了各自獨立的安全解決方案限制。這種內化的統一性促進了卓越的整合、簡化管理，並為你的安全團隊提供無與倫比的可視性與掌控。

雖然其他公司可能會利用平台來造成供應商綁定，我們致力於維護和擴展業界最廣泛、開放的合作夥伴生態系統。這種方法確保 Fortinet 安全織網仍然是一個多供應商平台解決方案，無縫整合你現有的安全基礎設施，保護資安投資，並在選擇資安供應商時提供靈活性。

FortiOS 7.6 的強化功能

Fortinet 安全織網平台瞄準各種關鍵應用案利，為網路的每個角落提供廣泛的整合式安全與網路功能。FOS 7.6 的最新強化功能在以下領域提供全新或更豐富的功能：

安全網路

Fortinet 安全織網的安全網路組件結合關鍵的網路連結、連通性與安全功能，包括 OT、IOT 以及邊緣安全。

FOS 7.6 強化功能包括：

- **用於管理、配置、文件與支援的 FortiAI：** FortiAI 現在包含 FortiManager 內的生成式 AI，以協助平台管理、新產品和功能部署、網路監控以及存取文件和支援資產。FortiAI 有助於更快做出決策，協助快速偵測並緩解事件，以及確保組織可以輕易採用他們所需的技術。

- **託管型 FortiGate 服務：**這項新的服務可以透過部署、配置、監控和管理 FortiGate 部署來減輕 NOC 團隊的負擔。這項服務由 Fortinet 專業人員組成，利用雲端工具成為 NOC 團隊的延伸。客戶和合作夥伴可以利用這些服務，好讓他們的網路安全專家可以專心從事更有價值的活動。

- **資料外洩防護：**DLP 強化功能提高偵測可信度和精準比對能力，以確保敏感資訊無論位於混合式網路內的什麼地方都能保持安全。

- **FortiLink NAC：**我們內建的 NAC 功能是我們專有的 FortiLink 協定的一部分，其功能的強化使 FortiGate 裝置能夠直接管理 FortiSwitch 和 FortiAP 產品。FortiLink NAC 使 Fortinet 交換器和無線基地台能夠識別 IoT 裝置並將其正確載入到適當的網段，不需要額外的授權。

- **Wi-Fi 7 控制器：**我們的無線控制器現在可以管理我們最近發表的 Wi-Fi 7 無線基地台。

- **新的 AIOps 服務：**改善 SD-WAN 的監控與管理，以及 DEM 共享資訊的能力，進而帶來更好的可視性與更好的使用者體驗。

- **新的 FortiGuard 服務：**FortiGuard 服務為組織提供主動且聰明的網路安全做法，使他們能夠自信地應對不斷變化的威脅情勢。我們現有的 AI 驅動服務套件包含以下強化功能：

  - **增強 FortiGate NGFW 內嵌式保護功能：** AI 驅動的即時內嵌式偵測與預防功能可以識別並阻止最複雜和新穎的威脅。

    - AI 驅動內嵌式惡意軟體預防服務的重大升級，包括即時反網路釣魚和加速 AI 預先過濾器等新功能
    - 更快地做出判斷的能力
    - 零號受害者的關鍵預防
    - URL 和網頁過濾的 AI 強化，提升預防惡意攻擊的能力

Unified SASE

隨著組織整合更多基於雲端的資源並支持混合工作模式，雲端交付和基於雲端的安全解決方案變得越來越重要。保護遠端用戶的安全，同時維持可靠的連結，對採用混合工作模式策略的組織來說至關重要。FortiOS 7.6 的強化功能包括：

- **統一代理程式（FortiClient）：**FortiClient 將許多解決方案整合到單一代理程式中，包括 ZTNA、VPN、EPP、持續漏洞評估、智能沙箱、遙測和 DEM，以及 PAM 和 NAC 的代理功能。FortiOS 7.6 為 FortiClient 增加了完整的 EDR 功能，為具備可視性、控制和遠端存取功能的主機增加勒索軟體防護、基於行為的偵測以及自動化回應。

- **SASE (SSE + SD-WAN)：**

  - 託管 SASE / ZTNA：與託管 FortiClient 服務類似，FortiSASE 營運團隊可以協助 SASE 客戶登入並配置他們的 SASE 入口。這項遠端服務及其託管服務工程師將會配置 FortiSASE，減輕本地 NOC 或 SOC 團隊管理這項網路安全元件的負擔。

  - 用於遷移、規劃與部署的 FortiAI：新的生成式 AI 可以協助過渡到公有雲端的過程，並在特定雲端平台內引導應用程式和服務的規劃和部署。這項服務將包含在雲端供應商產品中，例如 AWS 的 FortiAI 和 Azure 的 FortiAI。

  - 資料保護：DLP 強化功能為 SASE 用戶提高偵測可信度和精準比對能力，以確保敏感資訊無論位於混合式網路內的什麼地方都能保持安全。

  - 交換器 / AP / 5G 支援：FortiSASE 對輕量型邊緣應用案利的全新支援可以實現遠端 AP、交換器和 FortiExtender 部署。

  -SD-WAN：FortiOS 7.6 提供 20 多種新的 SD-WAN 功能，以簡化操作並改善使用者體驗。上層的強化協作功能簡化並自動化橫跨多雲的連通性，使操作更有效率。底層頻寬和品質監控服務的改進提供全面性的連結、路徑和應用服務效能監控，以優化使用者體驗並簡化操作。

  - 遠端瀏覽器隔離：組織現在可以輕易將 RBI（遠端瀏覽器隔離）新增至他們的 SASE 用戶群，以進一步將用戶和網路威脅隔離開來。

  - 端到端數位體驗監控（DEM）：DEM 代理程式現在已經新增至 FortiClient，提供端到端 DEM 給 FortiSASE 用戶，帶來更好的可視性與故障排除。

  - 第三方 SSE 支援（IPSec）：FortiSASE IPsec 服務連接讓潛在客戶可以使用 IPsec 通道將第三方 SD-WAN 分支和一般路由器連接到 FortiSASE 平台。這在選擇和管理供應商以及轉換供應商時提供更大的靈活性。

  - 統一政策：利用部署在本地和虛擬防火牆以及 SASE POP 的通用 FortiOS，用戶可以在所有的防火牆建置點建立統一政策。

AI 驅動的 SOC 營運

偵測、預防和緩解威脅和攻擊仍然是許多 SOC 團隊面臨的關鍵挑戰。這就是為什麼我們為 SOC 環境開發了先進的 AI 功能以強化威脅識別，包括引導 SOC 團隊進行威脅調查與回應的生成式 AI。

FortiAnalyzer 7.6 是 Fortinet 安全織網的中央資料湖，它統一配置、事件和告警，並提供先進的威脅視覺化圖表。它還引進了安全自動化訂閱服務，提供高級報告、事件處理和事件回應劇本等強大的功能。這些強化功能提升 SecOps 團隊的能力並簡化操作，改善了對安全事件的偵測、調查與回應。新的 FortiOS 7.6 強化功能包括：

- **強化的 SOC 即服務（SOCaaS）：**將 SOCaaS 與 SASE、鑑識和託管型 FortiGate 服務整合在一起，再加上整合爆發型威脅的偵測能力，大幅強化了我們的託管 SOC 產品。

- **FortiAI 整合：**將 FortiAI 整合到 FortiAnalyzer 中可以強化系統分析和回應安全威脅的能力。透過利用 FortiOS 遙測資料，FortiAI 提供諮詢支援，有助於更快做出決策並採取有效的行動，例如特定報告查詢或事件處理。

- **SIEM Lite：**為 FortiAnalyzer 增加輕量型 SIEM 功能有助於集中安全織網中的資料，透過合併配置、事件和告警來得到更好的可視性與分析。其威脅視覺化圖表（包括互動式拓撲）為安全威脅和模式提供直觀的圖像表述。

- **SOAR Lite：**為 FortiAnalyzer 增加輕量型 SOAR 功能（可透過安全自動化訂閱服務取得），提供精心挑選的內容包，其中包含開箱即用的高級報告、事件處理、進階關聯規則、第三方日誌解譯器、自動化連接器、資料加值和事件回應劇本。這些內容包提供顯著的優勢，因為它們將會持續更新，獨立於未來的 FortiAnalyzer 版本，確保 SecOps 團隊隨時掌握最當前的工具和資料。

- **治理、風險及合規（GRC）：**FortiAnalyzer 7.6 解決了遵循、維持和持續改善合規性與風險管理的複雜性，同時透過新的 GRC 報告滿足安全基礎設施的動態特性。其針對攻擊面與合規性管理的服務可以主動評估網路漏洞，並協助引導安全態勢中的針對性改善。這些工具簡化合規性流程，自動生成關於產業特定風險與不合規配置的報告，針對 IT 和 OT 環境的安全態勢提供寶貴的見解。

- **用於事件回應的 FortiAI：**生成式 AI 輔助可以分析 FortiSIEM 中的告警事件，並為 FortiSIEM 和 FortiSOAR 中的後續行動提供指示。

- **EDR 與 FortiClient 的整合：**將 EDR 加入 FortiClient 中可以為我們的統一代理程式帶來完整的端點偵測與應變功能，包括在單一代理程式中結合勒索軟體防護和 ZTNA 功能。

Fortinet 的優勢

Fortinet 提供業界最完整且強健的網路安全平台。自二十多年前成立以來，我們一直專注在有機創新與產品開發上，輔以針對特定技術或功能的戰略收購，以創造業界最全面的整合式網路安全與網路連結解決方案策略。

這種對整合式安全織網的不懈追求，使我們能夠提供基於單一作業系統、單一統一代理程式、單一管理控制台和單一資料湖的單一平台。研究顯示這種平台方法能夠帶來更好的安全結果、更有效率的營運、更好的使用者體驗以及更強大的 ROI。

FortiOS 7.6 建立在我們先前廣泛的開發基礎上，再加上最新的生成式 AI、託管服務和進階功能，以進一步加快並簡化當今日益複雜的 NOC 和 SOC 營運。

March 29, 2024 1:19 PM
2641038-0-0-EN