解決方案簡報

使用 Fortinet OT 安全平台保護虛實整合系統

解決方案簡介

網路犯罪分子日益鎖定營運技術（OT）與關鍵基礎設施領域中的虛實整合系統（CPS）作為攻擊目標，導致業務損失、生產中斷，並對關鍵基礎設施的穩定性構成嚴重威脅。[1] 由於風險上升，OT 資安已被提升至企業層級管理，且有 60% 的組織計劃在未來十二個月內，將 OT 資安納入資安長（CISO）的管理範疇之下。[2]

Fortinet OT 安全平台是目前最全面的 OT 資安解決方案組合，專為保護 OT 環境而設計。該平台涵蓋安全網路架構、安全服務邊緣（SSE）、安全營運解決方案（OT SecOps）、專屬威脅情資服務，以及涵蓋廣泛的技術合作生態系。所有這些解決方案皆為高度整合設計，可支援供應商整併、集中化管理，以及 IT/OT 融合，進而簡化作業流程、提升網路安全，同時降低整體擁有成本。

OT

Fortinet OT 安全平台被 Westlands Advisory 評選為 2023 年 IT/OT 網路防護平台導航報告中的唯一領導者。[3]

OT 專屬解決方案的必要性

負責管理與保護 OT（營運技術）環境的資安長（CISO）、資訊長（CIO）及網路安全團隊，面臨多項獨特挑戰，包括需選擇並管理數量龐大且繁雜的 OT 安全供應商。在如此複雜的 OT 環境中建立安全防護，同時兼顧人員安全與生產穩定等營運優先事項，極具挑戰性。

然而，如今許多企業已採用整合式平台，以因應供應商整併、IT 與 OT 技術融合，以及有限資安人力資源的最佳化問題。為了解決這些挑戰，理想情況下，資安長應部署一套 OT 安全平台，提供一至性的網路、網路分段、SSE（安全服務邊緣）及 OT SecOps（營運技術安全營運）解決方案，並能與既有系統無縫整合。

Fortinet OT 安全平台是一套完整的網路與資安解決方案組合，專為 OT 而設計，涵蓋從基本的網路連接到進階 SSE 與 OT SecOps 解決方案的全面防護。

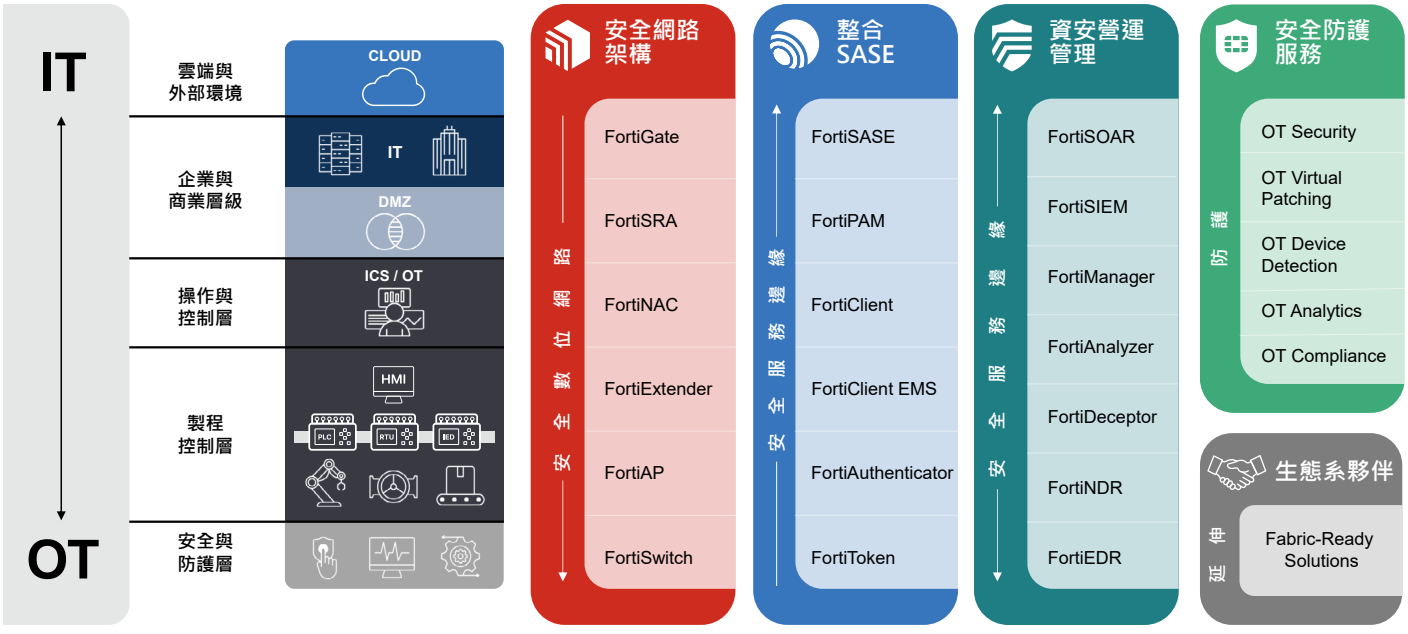

圖 1：Fortinet OT 安全平台

透過安全網路連接與防護 OT 環境

Fortinet OT 安全平台透過 FortiGate 次世代防火牆（NGFW）實現與虛實整合系統（CPS）的初始連接，並搭配 FortiSwitch 提供後續的網路分段。針對資源受限的 OT 網路與裝置，則由 FortiSRA 提供安全遠端存取解決方案。這些關鍵的連線與存取能力專為 OT 環境量身打造，包括強固耐用的硬體設計及進階 AI 驅動的 OT 資安服務。

OT 安全平台亦回應了資安團隊所面臨的其他共通挑戰。由於 OT 系統與裝置常因供應商不支援、缺乏更新或因產品定位因素衝突而未能及時修補漏洞，因此導入積極的預防性資安控制措施至關重要。該平台可針對 OT 應用與通訊協定提供網路分段與微分段控制，並透過漏洞管理引擎執行防護措施，例如虛擬補丁技術。該引擎內建逾 1,000 條虛擬補丁規則，能即時保護未修補易受攻擊的 OT 裝置。

為強化資產與網路可視性，OT 安全平台內建 FortiGuard OT 安全服務，提供來自主要工業控制系統（ICS）製造商的 OT 應用與協定漏洞防護功能。透過 FortiGate NGFW 搭配更新的特徵碼與漏洞資料庫，可即時偵測針對 OT 系統的攻擊行為。OT 安全服務涵蓋超過 80 項工業自動化與控制系統協定，採用由 FortiGate 入侵防禦引擎驅動的 1 套威脅引擎，內含超過 18,000 條漏洞特徵碼，其中逾 4,000 條專門針對 OT 安全防護所設計。

由於許多 OT 裝置與系統缺乏修補機制，透過虛擬補丁與漏洞遮蔽技術來阻止漏洞被利用與防禦時下攻擊顯得格外關鍵。Fortinet OT 安全平台提供下列功能：

- 利用 FortiGate NGFW 實現資安控制與政策強制執行
- 在網路層實現完整的使用者與裝置可視性與控制，支援是否搭配 FortiSwitch 的網路微分段
- 跨 IT 與 OT 使用 FortiAnalyzer 進行集中式監控、日誌記錄與報表分析
- 使用 FortiManager 對 FortiGate 設備執行集中式裝置管理與資安政策落實，涵蓋 IT 與 OT 環境
- 由 FortiGuard Labs 提供的即時、最新且可操作的威脅情資、修補建議與零時差漏洞防護

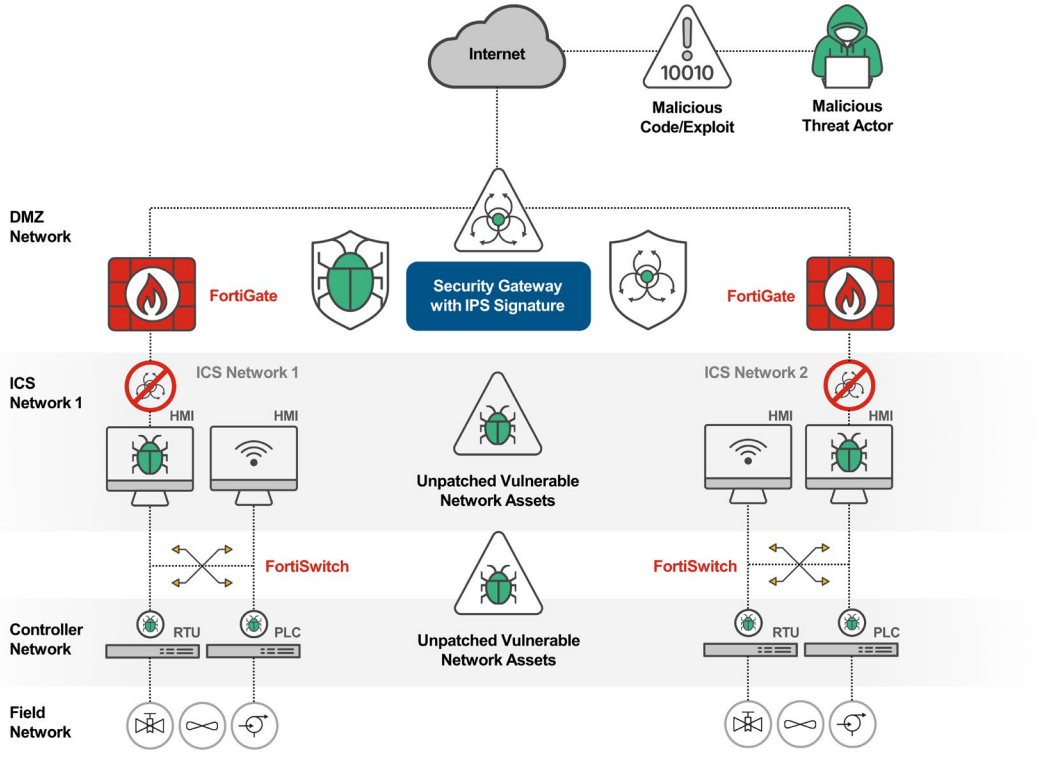

圖 2：ICS/OT 網路中的虛擬補丁機制

OT 的 SSE 方案

SSE（安全服務邊緣）策略延伸至 OT 網路可能面臨挑戰，原因包括營運時哪一件事需優先的衝突、關鍵 ICS 網路與裝置的敏感性，以及缺乏專為 OT 設計的零信任解決方案。Fortinet OT 安全平台內建特權存取管理（PAM）與網路存取控制（NAC），協助您克服這些挑戰。

這些解決方案雖然各自功能強大，但也可以協同工作，驗證連接到 OT 網路的使用者和設備，並根據設備或使用者的角色限制僅存取適當的資源，無論用戶位於何處或應用程式託管在何處，Fortinet SSE 解決方案都可以安全地將使用者連接到應用程式。

NAC 能選擇性地授權使用者存取應用，並識別與保護 IT、OT 與工業物聯網（IIoT）資產。資產擁有者與操作人員亦能全面掌握與控制所有連線至網路的元件。FortiSRA 提供安全的遠端存取能力，支援第三方廠商、稽核人員與內部員工連線 OT 系統，同時防禦來自遠端存取與不受信任網路的威脅。

FortiPAM、FortiAuthenticator 與 FortiToken 等身分與存取管理解決方案協同合作，限制僅授權使用者可存取。與此同時，FortiGate 的網路分段技術可根據業務需求進一步實現零信任存取，切分 IT/OT 網路。

Fortinet SSE 解決方案功能包括：

- FortiGate NGFW：提供資安控制與政策強制執行
- FortiNAC：對所有網路連線資產提供可視性、控管及自動化應對
- FortiSRA：為 OT 環境提供無代理的安全遠端存取功能
- FortiToken：支援一次性密碼（OTP）應用程式、推播通知或硬體型 OTP 裝置的雙因素認證
- FortiAuthenticator：支援單一登入與身分驗證，可識別使用者並從第三方系統查詢授權資訊，再傳送至 FortiGate NGFW 執行身分識別型資安政策
- FortiPAM：提供特權帳號與資產存取管理能力，實現零信任安全架構，包括對 OT 應用與系統的控制、監控與記錄使用者行為，並支援對關鍵資產的安全遠端存取

Gartner 表示：「整體對於 CPS（資通物理系統）安全，特別是 OT（營運技術）安全的關注，正持續升溫，這一趨勢不僅體現在 Gartner 的調查結果中，也反映於客戶諮詢的趨勢上。這背後的原因包括：威脅行為者（某些情況下甚至涉及國家級力量）愈加頻繁地針對關鍵基礎設施與工業系統發動攻擊；同時，隨著企業推動數位轉型，其攻擊面亦隨之擴大。
此外，法規遵循的要求也日益提升，例如歐盟即將施行的 NIS2 指令與《網路韌性法案》（Cyber Resilience Act），以及美國新版的 NIST 資安框架等。」[4]

透過 OT 專屬安全營運強化 OT 資安防護

使用專為 OT 設計的平台，可整合多個資料來源，加快威脅偵測時間，並實現資安應變的自動化。Fortinet 的 OT SecOps 解決方案專為整合網路與安全營運而設計，提供統一化的管理與監控平台，涵蓋 OT 網路與資安基礎架構。

其功能包括資產識別、網路通訊拓撲圖管理（對應 Purdue 企業參考架構）、MITRE ATT&CK ICS 矩陣、OT 應變手冊，以及風險與合規性報告等。

IT 與 OT 團隊亦須在資安防護與營運優先事項之間取得平衡。在風險緩解過程中，部分修復措施可能需延後執行，由 OT 資安或營運團隊處理，以確保生產與服務不中斷。最終目標是打造一個融合 IT/OT 的資安營運中心，充分運用威脅情報、分析、威脅偵測、誘捕（honeypots）、事件應變、威脅獵捕及治理與合規性機制，且不影響 OT 環境的正常運作。

為實現此目標，Fortinet OT SecOps 解決方案包括：

- FortiGate NGFW：提供資安控制與政策強制執行。
- FortiAnalyzer：整合日誌管理，並提供 OT 資安分析與報表功能，涵蓋 IT/OT 風險、IEC 62443 及 NERC CIP 合規性報告。
- FortiEDR：提供即時自動化端點威脅偵測與防護、事件處置協調，以及鑑識分析。
- FortiSIEM：可收集來自 IT 與 OT 系統的日誌數據，並分析橫跨兩者的威脅行為；同時支援 MITRE ATT&CK 架構下的威脅活動視覺化，適用於企業 IT 與 ICS 環境。
- FortiSOAR：可自訂的資安營運平台，提供自動化流程、事件分流，以及 OT 企業所需的即時修復機制，協助辨識、防禦並反制攻擊。
- FortiDeceptor：部署誘捕系統（OT 裝置誘餌與協定誘騙），用以誘導、揭露並排除內外部威脅，避免造成實質損害前即加以偵測。
- FortiNDR：結合 AI 與神經網路的網路偵測與應變解決方案，支援亞秒級調查能力，並透過深度學習技術自動化 SOC 分析師的回應作業，內建虛擬安全分析師以即時識別、分類與回應各類威脅。
- Security Operations Center-as-a-Service（SOCaaS）：雲端代管資安監控服務，分析由 FortiGate NGFW 與其他資安產品產生的事件，負責初步事件分類並升級確認的威脅警報。
- FortiRecon 數位風險防護：SaaS 型服務，整合三大模組：外部攻擊面管理、品牌防護與對手導向情報（Adversary-Centric Intelligence）。FortiRecon 提供對攻擊者行動與計畫的洞察，協助企業於偵查階段即介入干預，顯著降低後期風險、時間與緩解成本。

支援 OT 安全平台的整合與融合

在保護 CPS（虛實整合系統）時，企業常面臨技術上的挑戰，主因為營運優先事項的競合所致。確保 OT 環境安全需與整體企業網路有效連接，這往往是 OT 安全營運中心首次整合 IT 與 OT 的實踐。

同時，許多 OT 組織也希望透過供應商整併與 IT/OT 資源融合，來最佳化營運效率。Fortinet OT 安全平台透過其 OT 專屬的網路連線能力、安全服務邊緣（SSE）與安全營運（SecOps）解決方案，有效應對上述挑戰。該平台提供高度彈性與可擴充性，協助組織建構完善的 OT 資安防護體系。

[1] CISA, Critical Infrastructure Sectors, accessed August 1, 2024.

[2] Fortinet 2024 State of OT and Cybersecurity Report.

[3] Fortinet Named Sole Leader in 2023 IT/OT Network Protection Platforms Navigator™ Report, July 27, 2023.

[4] Gartner, Emerging Tech: Top Factors Driving Cyber-Physical Systems Security Growth, April 26, 2024.

May 11, 2025 9:34 AM / 2436831-A-0-EN