FORTINET

解決方案簡報

IT/OT 融合
帶來營運流程精簡化的新契機

解決方案簡介

當適當的資安措施到位時，資訊技術（IT）與營運技術（OT）融合所帶來的效益將遠大於其風險。其中一項經常被忽略的優勢，是能夠在整合的資安營運中心（SOC）中，同時簡化 IT 與 OT 環境中的安全作業。

IT/OT 融合不僅提供橫跨兩邊裝置的集中化管理機會，還能藉由整合雙方的資料輸入來進行威脅獵捕，並有效管理端點資源與部署欺敵誘捕技術，其潛力極具吸引力。

注意事項

在整合型資安營運中心（SOC）中導入 OT 意識與專業資源極為重要。IT 領域的最佳實務若直接套用於 OT 環境，往往不僅不適用，甚至可能造成更大的損害。這些潛在風險包括：

- 導致可程式邏輯控制器（PLC）無法運作
- 在未顧及監控控制與資料擷取系統（SCADA）與工業控制系統（ICS）流程安全與持續運行的情況下進行修補，導致生產流程受損
- 在 IT 與 OT 系統間過度統一使用者與帳號管理機制，導致過度整合與管理風險

此外，為了降低流程與安全中斷的風險，營運人員與代管服務供應商應聘用並培訓 OT 專家，並在配置 SOC 人力時充分運用其專業知識。

融合所伴隨的風險

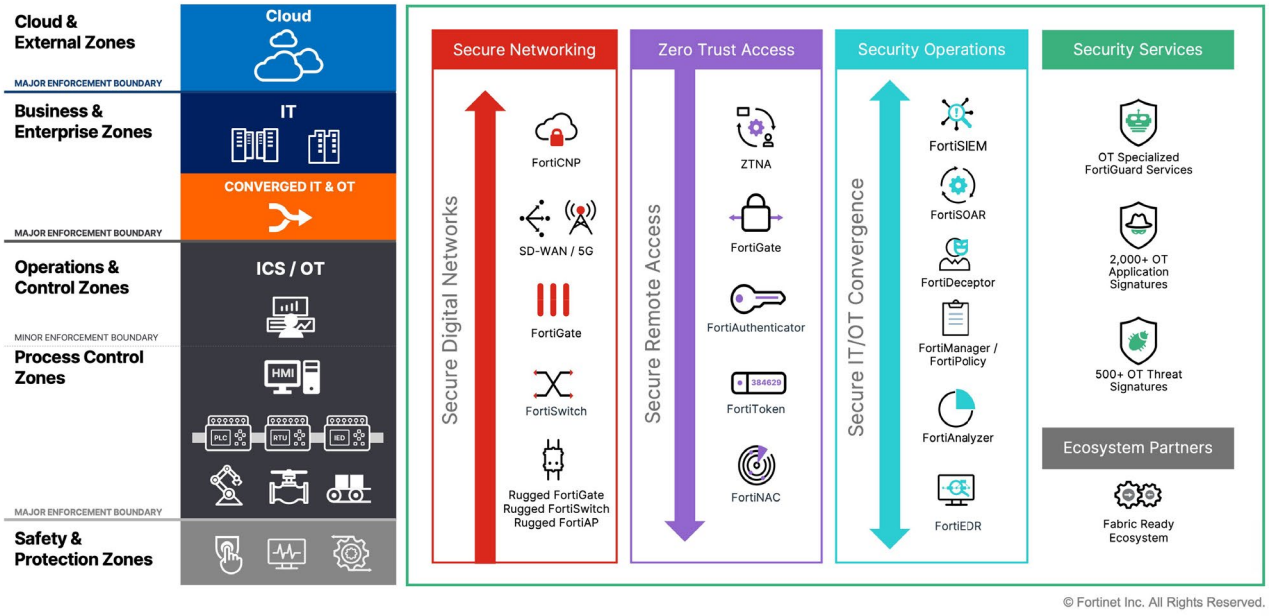
網宇與實體系統的融合 (Cyber-physical convergence) 可能會增加暴露於威脅中的裝置數量，並為攻擊者提供可用於其攻擊鏈的混合式生態系。進階威脅可有效滲透組織網路的各個層面，包括工業、製造業與關鍵基礎設施環境中的 OT 系統。

若在 IT/OT 融合後未實施適當的網路分段保護，任何成功突破 IT 系統的威脅，都有機會橫向滲透至 OT 領域中脆弱且具價值的目標。引入如工業物聯網（IIoT）與 5G 等新技術，更進一步擴大了攻擊面，使工業系統面臨更高的風險。

「傳統上彼此隔離的 OT 環境，如今已不再完全獨立。它們現在已與企業營運、原始設備製造商（OEMs）及其他第三方建立了直接連線。」[1]

安全織網（Security Fabric）– 營運技術（OT）

常見部署解決方案



融合式安全營運

Fortinet 提供多項解決方案，協助資產擁有者在 IT 與 OT 融合過程中維持穩健的資安防禦態勢。

研究顯示，將資安網路營運融合於單一 NOC/SOC（網路營運中心 / 安全營運中心）的資產擁有者，其資安事件發生率最低，且整體成效最佳。受訪的 OT 業者中，遭遇入侵次數較少的業者，超過 32% 會讓 SOC 監看和追蹤 OT 安全。。

一個能同時支援 IT 與 OT 的融合式 SOC，其核心組成包括：

- 安全資訊與事件管理（SIEM）
- 安全協作、自動化與回應（SOAR）
- 基於欺敵誘捕 (Deception) 技術的入侵防護
- 集中式政策管理
- 集中式日誌記錄與報表
- 端點偵測與回應（EDR）

集中式可視性

FortiSIEM 提供集中式可視性，協助資安營運團隊更有效地管理瞬息萬變的安全性、效能與合規性需求。透過跨網路營運中心（NOC）與資安營運中心（SOC）的即時關聯分析，提供業界領先且具專利的威脅偵測技術，FortiSIEM 協助資安團隊更全面理解其擴展環境的整體情境。FortiSIEM 也原生支援多租戶架構，能夠對不同網路區段、虛擬與邏輯環境提供獨立報表分析。

為防禦進階威脅，OT 環境需部署整合式資安營運平台，能夠即時掌握融合資產的狀態；並偵測已知與未知的攻擊戰術與技術，進一步建構快速且完整的事件應變計畫。從基本的日誌關聯分析，到運用人工智慧（AI）與機器學習（ML）

的進階異常行為分析，FortiSIEM 提供多項專為保護 OT 與 IT 系統設計的資安解決方案。

FortiSIEM 能揭示惡意攻擊者在工業控制系統（ICS）中所使用的戰術、技術與程序（TTPs），並透過 MITRE ATT&CK 框架進行分析。同時，FortiSIEM 也支援針對 IT 環境的 MITRE ATT&CK 模型，顯示資料如何依循 Purdue 模型進行流動與變化。

僅有 13% 的資安營運團隊認為他們對 OT 活動具備 100% 的可視性，此數據自 2020 年的 23% 明顯下降。[3]

統整人員、流程與技術

FortiSOAR 作為 Fortinet Security Fabric 架構的一部分，亦可作為不依賴特定廠商的獨立方案，屬於進階的 SOAR 產品，旨在統整人員、流程與技術。FortiSOAR 協助資安團隊加速事件調查、回應與修復流程，全面提升組織資安體系的營運效能。

由於事件回應程序冗長，分析人員愈來愈難以應對大量湧入的告警訊息。FortiSOAR 可集中整合這些告警，並加入更多關聯性上下文，以提升處理效率。FortiSOAR 可簡化諸如告警擷取、依嚴重性分類與任務指派等工作流程，也可自動化更複雜的端對端（E2E）任務，例如初步分流、資訊豐富化、深入調查與緩解措施，透過自動化將整個安全堆疊中的告警關聯到單一事件，從而統一集中安全流程。

FortiSOAR 全方位與可調整的功能，能有效彌補多供應商系統與流程間的落差，並為組織內各團隊提供集中式指揮平台，以便進行溝通、協調、整合與協作。

分散式欺敵誘捕平台

OT 環境多樣，涵蓋大量異質、多供應商設備與系統，且通常未內建資安機制。由於可用性、成本與修補限制等原因，透過代理程式或安全修補來強化資安往往不可行，因此組織應採取「預設遭入侵」的策略，搭配網內偵測技術以強化防禦。

FortiDeceptor 是一套分散式欺敵誘捕欺敵誘捕平台（DDP），提供非侵入式、無代理的 IT/OT 欺敵誘捕欺敵誘捕網路，可精確偵測網路中正在進行的攻擊。誘餌可產生高準確性、具可行性的告警訊息，並觸發自動化事件應變流程，以協助阻止零時差攻擊。

FortiDeceptor 可模擬多種 OT、ICS 和 IoT 類型的誘餌裝置，例如 SCADA PLC、HMI、醫療 IoT（如 PACS、輸液幫浦、印表機、IP 攝影機、路由器、數據機、UPS），以及 SAP 等關鍵應用與 ERP 系統。藉由內建的隔離功能，FortiDeceptor 可啟用自動化回應，防止攻擊進一步擴散。此產品可部署為實體設備、虛擬設備或雲端實例，並可與企業 IT 架構整合，作為 Fortinet Security Fabric 的重要組成部分。

集中式政策管理與日誌分析

FortiManager 是管理 FortiGate 設備的統一平台，可跨越 IT 與 OT 的界線，並適用於 Purdue 模型中的多個層級，協助整合網路與資安解決方案。此舉可降低組織的攻擊面，支援數位創新，同時簡化網管團隊的操作流程。

作為 Fortinet Security Fabric 的一部分，FortiManager 提供零接觸佈署、集中管理、一致性政策與自動化網路擴展，並支援開放的生態系統。FortiManager 可部署於本地（on-premises）網聯架構中，適用於無法上網的企業；同時也可部署於雲端，以支援採用雲原生架構的客戶。

FortiManager 搭配 FortiAnalyzer 可強化分析功能並改善合規性報告，從而大幅降低因配置錯誤而導致的資安風險暴露與網路中斷機率。FortiAnalyzer 是 FortiGate 的核心日誌記錄、報表與進階分析平台，提供易於設定的威脅監控與偵測功能，可識別網路異常與安全政策違規情況，並整合內建事件處理器、威脅分類機制以及開箱即用可對應多項 IT 與 OT 安全合規框架的報表。

基於行為模式的端點防護

EDR（端點偵測與回應）解決方案旨在透過行為分析提供端點層級的安全性，具備即時可視性、威脅分析與緩解能力。這些解決方能夠主動縮小攻擊面，不論是否連網皆能預防惡意程式入侵，並可即時偵測與解除潛在威脅，同時透過可自訂的劇本自動化應對與緩解程序。

FortiEDR 可與 Fortinet Security Fabric 原生整合，支援數百種第三方解決方案，並具備透過 REST API 架構建置自訂連接器的能力。

FortiEDR 為 OT 環境量身打造，具備兩大關鍵特性：首先，它持續支援終止支援的作業系統，如 Windows XP 與 Windows Server 2003；其次，FortiEDR 可部署於混合式架構中，透過客戶端資料中心或其他代理基礎設施進行代理轉發來支持雲端更新。

此外，FortiEDR 可封鎖來自 FortiGate 的惡意 IP 位址，或結合 FortiNAC 自動將受感染裝置導向緩解 VLAN，亦可與 FortiAnalyzer 或 FortiSIEM 整合，以關聯告警、日誌與其他資訊。

結論

就如同清理一個雜亂的車庫好讓第二輛車能夠停進去一樣，IT 與 OT 網路的融合為 IT 團隊提供了一個絕佳機會，可用來簡化 NOC/SOC 的運作。成功的 IT/OT SOC 建構關鍵，在於能夠納入 OT 專業人員的知識與組織能力，他們具備深厚的培訓與實務經驗。

一個設計良好的 IT/OT SOC 應具備以下能力：

- 從 IT 與 OT 雙方擷取資料，並提供具可行性的情資
- 跨 IT 與 OT 環境統一管理防火牆與交換器政策
- 同時於兩個環境中部署欺敵誘捕技術
- 管理適用於 IT/OT 的 EDR 系統
- 融合 IT 與 OT 網路可協助企業簡化營運流程，整合管理設備、獵捕威脅，並透過單一 SOC 平台保護關鍵端點資產。

[1] Gartner, Reduce Risk to Human Life by Implementing This OT Security Control Framework, June 17, 2021

[2] Fortinet, 2022 State of Operational Technology and Cybersecurity Report, July 21, 2022

[3] Ibid

FORTINET

www.fortinet.com

May 12, 2025 9:34 AM
1791726-0-0-EN