以安全驅動網路

# 幫助智慧製造安全實現靈活轉型

製造業解決方案手冊

www.fortinet.com/tw

# 目錄


**數位轉型的多維度資訊安全風險分析** 02

1. IT 與 OT 融合的風險 02
2. 隔離與互聯並存的風險 03
3. 合規性考量 03

**Fortinet 護航製造業數位轉型的優勢** 04

1. 可涵蓋整個攻擊平面的全方位解決方案 04
2. OT 專有應用辨識與威脅特徵資料庫 04
3. 與第三方工控安全及工控系統的緊密整合 05

**數位轉型中新增必選題 - OT 安全的風險防範與實踐** 06

1. 網路攻擊路徑與攻擊平面概覽 06
2. 使企業安全與 Purdue 模型保持一致 06
3. Fortinet Security Fabric 工控安全整體解決方案的 8 個落地階段 08
   - 階段 1. 可視化 08
   - 階段 2. 集中管理 08
   - 階段 3. 安全區域劃分 09
   - 階段 4. 網路存取控制 09
   - 階段 5. 抵禦已知與未知威脅 09
   - 階段 6. 智能分析與偵測 10
   - 階段 7. OT 資安態勢感知與回應 10
   - 階段 8. 信任評估 10
4. Fortinet Security Fabric 工控安全整體解決方案安全元件 11

**數位化企業微分段隔離措施的必要性討論** 21

1. 更加精細化的網路安全管理 21
2. 更少的漏洞，更少的交叉感染 21
3. 更低的部署與管理成本 21
4. 更智慧型的風險管理關聯機制 21

**Fortinet 護航大型製造業企業案例分享** 22

1. 微分段隔離解決方案案例 22
2. 進階威脅及勒索軟體防禦案例 23
3.Fortinet 與 Nozomi 整合工業安全案例 24

# 數位轉型的多維度資訊安全風險分析

在雲端計算、大數據、物聯網、人工智慧的創新技術浪潮中，數位轉型已經成為大量政府與企業組織推動業務創新、重構組織 IT 的重要方式。但是數位轉型同時也會引入多維度的資訊安全風險，威脅著組織關鍵的數位資產，甚至影響業務的正常營運。

## 01 IT 與 OT 融合的風險

工業 4.0 時代，營運技術（OT）與資訊技術（IT）成為重要的驅動力， 並且由於企業營運具有互聯互通的特性，智慧型裝置之間的互聯性不斷加強，網路攻擊的影響也比以往任何時候都更加廣泛。

製造業的數位轉型讓 IT 部門與生產部門從簡單關聯轉變成複雜關聯，這些新變化使得企業在發展與創新中得到大量機會，同時也導致企業需要應對轉型過程中的特有風險。IT 部門的職能範疇已經滲透到企業營運的各個方面，連繫著技術與產品，以及企業與員工、客戶與合作夥伴，沒有哪個部門能脫離 IT 技術，這意味著 IT 部門必將承擔起更大的責任。

得益於開放的系統架構與創新的軟體應用，過去十年來，OT 與 IT 系統之間的資料流不斷增加，但是從工業網際網路中的專有通訊與硬體升級到整個企業的開放式連線之後，讓網路安全威脅更加難以檢測、調查與修復。之前，工業控制系統（ICS）與其他 OT 裝置都是孤立部署的，缺乏安全保障措施。 IT 人員沒有必要擔心安全問題，因為工業技術已經從傳統的 IT 網路中隔離出來。現在，隨著 OT 與 IT 網路的融合，工業裝置啟用 IP 成為網路生態系統的一部分，傳感器與其他控制器現在成為 IT / OT 融合網路上的工業物聯網（IIoT）端點，這些以前透過隔離部署來提供保護的安全邊界正在坍塌。

### IT 與 OT 融合

**以前完全隔離與各自專屬的兩者現在緊密的連線在了一起**

| 從前，OT 是 ... | | 現在，OT 是 ... |
|---|---|---|
| 與 IT 隔離 | → | 與公司 IT 網路互聯 |
| 運作專有控制協定 | → | 採用通用 TCP/IP 協定 |
| 運作在專有硬體上 | → | 運作在由 IT 發端的通用硬體上 |
| 運作在專有的嵌入式作業系統上 | → | 運作在主流 IT 作業系統上 |
| 由銅纜或者雙絞線連線 | → | 越來越多的透過標準 WiFi 協定連線 |

IT 與 OT 之間日益緊密的聯繫導致了一種觀點，即 OT 是 IT 的一種擴充，但事實並非如此。在針對機密性、完整性與可用性的訴求上，IT 將機密性放在首位，慣於使用最新的硬體與軟體，部署最新的安全技術與更新補丁檔案，而此類活動更有可能在 OT 中出現意想不到的結果。在生產環境中，不允許頻繁重新啟動裝置，發起掃描、更換驗證與審計憑證，這將會影響 OT 場景中最核心的可用性指標，導致更加糟糕的後果。

## 02 隔離與互聯並存的風險

大量工控系統漏洞、攻擊方法可以透過多種公開、半公開管道獲取，許多技術分析報告給出了網路攻擊步驟、攻擊代碼甚至攻擊工具等詳細資訊，極易被駭客等不法分子利用。在互連環境下，絕大多數工業控制系統在沒有防護措施的情況下，透過辦公網路暴露於網際網路，且因有系統漏洞，能夠輕易被遠端操控，面臨巨大安全風險；在相對隔離的環境下，工廠網路內部同樣會遭到行動存儲裝置、 第三方合作夥伴網路等管道遭遇惡意代碼攻擊。

## 03 合規性考量

根據市場調查，2024 年全球將有 390 億個聯網終端，產生 57.3ZB 的資料，而多數資料將落在監控、工業、及醫療等應用服務。在物聯網、大數據與 AI 等技術的潮流下，智慧製造、智慧醫療已成臺灣政府積極推動的政策，然而，所面對的營運科技（OT）資安威脅也持續受到關注。針對資安威脅，台灣政府設立了資安法予以管制，從國家法令要求驅動聯網安全維護，而在產業標準上， IEC 62443 等亦為工控領域立下標準。因此，工業控制系統需要依據不同等級的安全措施，還應評估“建構縱深的安全防禦體系”、“採取互補的安全措施”、“保證一致的安全強度”、“建立統一的支撐平台”、“進行集中的安全管理”等五方面總體性要求， 保證其整體安全保護能力。

# Fortinet 護航製造業數位轉型的優勢

## 01 可涵蓋整個攻擊平面的全方位解決方案

Fortinet 具備同時保護 OT 與 IT 環境的能力，具備完整的 IT 網路的網路安全防護方案，同時為 OT 環境提供：

**01** 與 IT 網路安全隔離（LEVEL 4 與 LEVEL 3 隔離）

**02** ICS 安全解決方案

**03** 操作 DMZ 區與工業環境隔離（LEVEL 3 與 LEVEL 2 隔離）

**04** 工業網際網路內異常行為與安全威脅監控

## 02 OT 專有應用辨識與威脅特徵資料庫

Fortinet 的工業應用防火牆 FortiGate 支援所有主流協定與應用，能夠辨別超過 1800 個工業應用以及防護面向於工業控制系統的攻擊。是業界最全面的特徵資料庫之一。

### 應用可視化

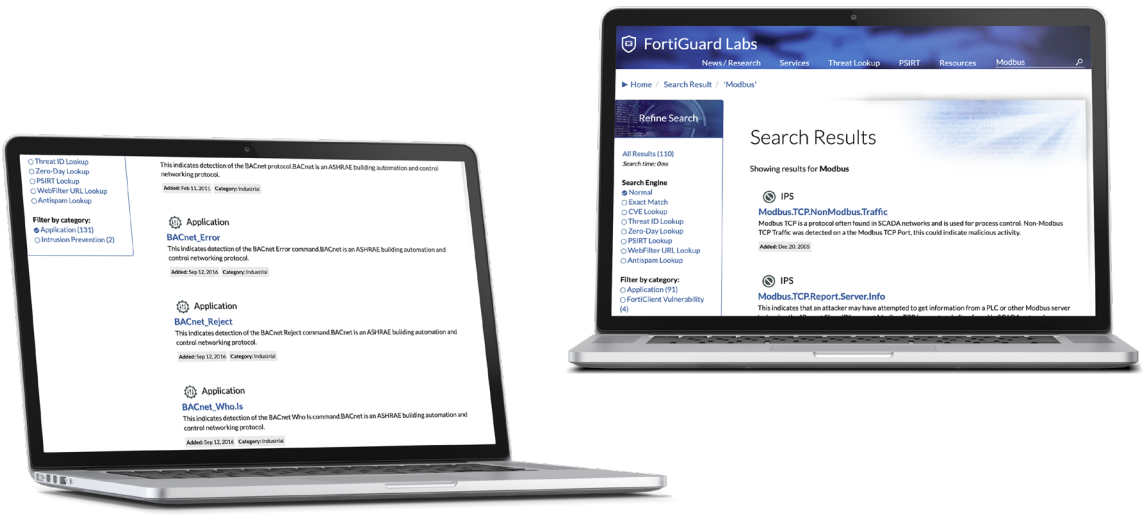
#### 支援的協定

- BACnet
- DNP3
- Elcom
- EtherCAT
- EtherNet/IP
- HART
- IEc60870-6 (TASE 2)/ICCP
- IEc608705-104
- IEc61850
- LONTalk
- MMS
- Modbus
- OPC
- Profinet
- S7
- SafetyNET
- Synchrophasor

#### 支援的應用與廠商

- 7 Technologies/ Schneider Electric
- ABB
- Advantech
- Broadwin
- CitectSCADA
- CoDeSys
- Cogent
- DATAC
- Eaton
- GE
- IConics
- InduSoft
- IntelliCom
- Measuresoft
- Microsys
- MoXA
- PcVue
- Progra
- QNX
- RealFlex
- Rockwell Automation
- RSLogix
- Siemens
- Sunway
- TeeChart
- VxWorks
- WellinTech
- Yokogawa

深度包檢測（DPI）應用控制
Modbus,IEC 60870-6(ICCP) 與 IEC.60870-5.104
內容記錄到 FortiAnalyzer，FortiSIEM 與 Syslog




## 與第三方工控安全及工控系統的緊密整合

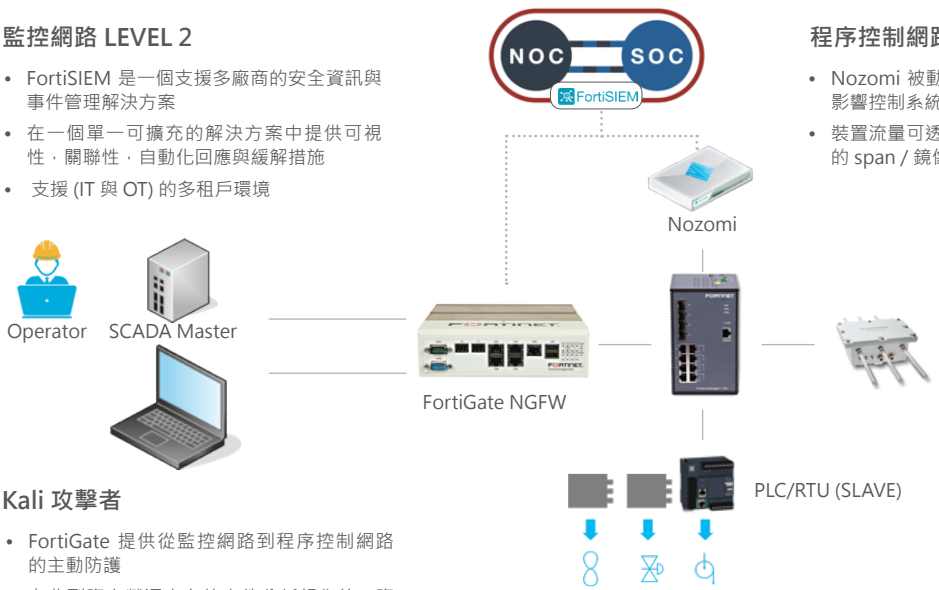
Fortinet 的工業安全解決方案可以與工業控制系統的第三方廠商組合成為一個整體的解決方案，對工業網際網路中的異常行為進行自動檢測與自動回應。以 Nozomi 為例，FortiGate 可以進行關聯，有效的監測到異常，並根據預先制定好的規則進行回應。

### 監控網路 LEVEL 2

- FortiSIEM 是一個支援多廠商的安全資訊與事件管理解決方案
- 在一個單一可擴充的解決方案中提供可視性，關聯性，自動化回應與緩解措施
- 支援 (IT 與 OT) 的多租戶環境

### 程序控制網路 LEVEL 1/0

- Nozomi 被動監控網路，不會影響控制系統的效能
- 裝置流量可透過網路交換器上的 span / 鏡像埠進行監看




### Kali 攻擊者

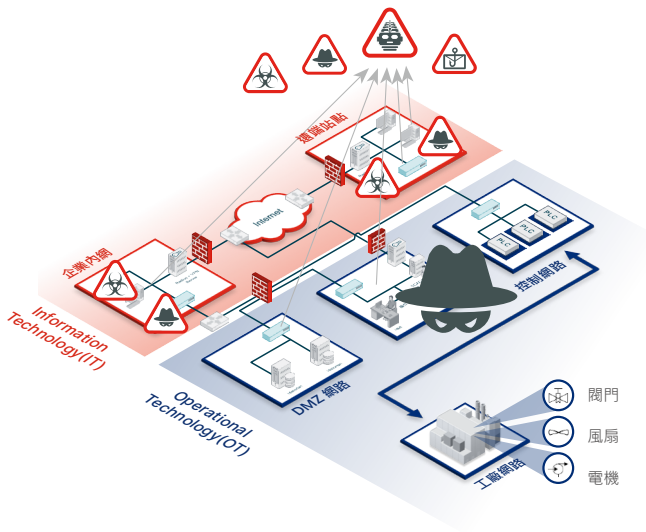
- FortiGate 提供從監控網路到程序控制網路的主動防護
- 在收到資安營運中心的事件分析報告後，資安團隊可以“BAN”攻擊者 IP。

# 數位轉型中新增必選題 - OT 安全的風險防範與實踐

結合不法分子攻擊路徑與攻擊平面分析，參考應用於工業控制 Purdue 模型架構，Fortinet Security Fabric 工控安全整體解決方案提供了基於 SCADA（資料採集與監視控制系統）安全的主動安全防禦能力， 使企業安全與 Purdue 模型保持一致，能夠在儀表匯流排網路、程序控制區域網路、區域總控網路、生產區域、企業環境等不同層面建構全方位、立體化、多層次、多維度的安全控制能力與階段性、涵蓋生產週期的安全保護。

## 01 網路攻擊路徑與攻擊平面概覽

Fortinet 的解決方案可以針對網路攻擊路徑與攻擊面進行全面的檢測與防護，目標是運用可視化技術，對網路攻擊指標與破壞程度進行綜合評估、對業務存取路徑與主機的弱點進行風險評估，並提供最優成本的安全防護方案，對安全威脅實施快速回應，對複雜的進階持續性威脅（APT）攻擊與未知威脅提前感應。




**步驟一**

**攻擊與滲透 IT 系統**

IT 系統複雜而脆弱，設計不合理， 代碼漏洞，設定錯誤，未進行合理的身份認證等問題；

**步驟二**

**內網橫向行動感染更多主機**

內網安全區域未有效劃分與隔離，無法阻擋內網橫向行動；

**步驟三**

**外聯駭客並準備破壞**

缺乏對從內而外的非法存取行為的檢測；

**步驟四**

**開始竊取並破壞**

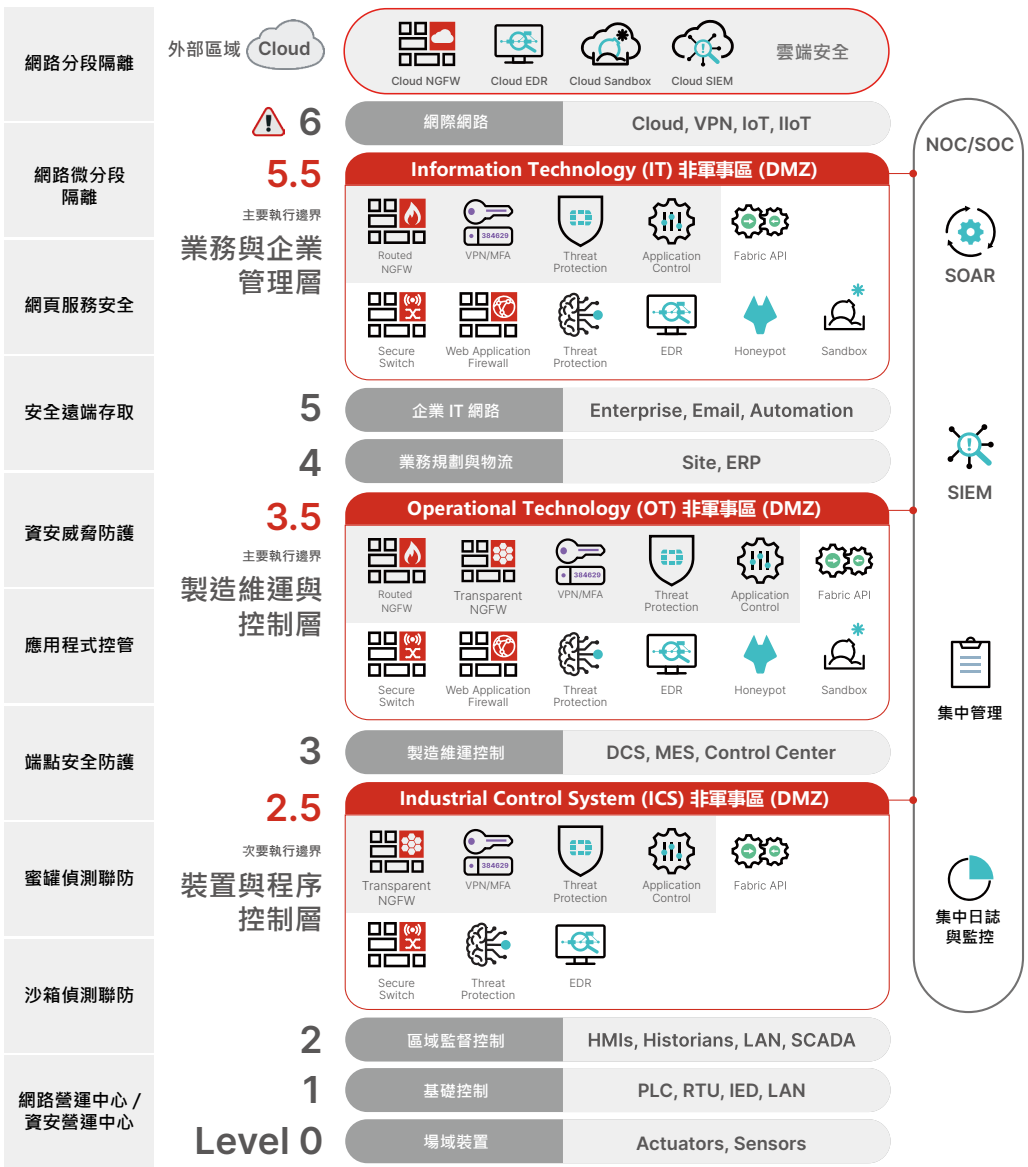
缺乏對整個網路的異常檢測與阻擋功能。

## 02 使企業安全與 Purdue 模型保持一致

Purdue 模型是工業自動化與控制系統（包括網路與安全要求）的指南。該模型還推動了 ISA-95 的製定，它是國際自動化協會的國際標準，定義了企業與控制系統之間的介面。金字塔形式的模型，定義了資訊從機台間向上流入企業高層級系統的路徑。該模型將企業與營運劃分為不同區域，並在兩者之間建立了工業化的 DMZ 或隔離區，防止從第 0 層到第 5 層之間的安全洩露。

| | | |
|---|---|---|
| Enterprise Zone | 5 | 企業 IT 網路 |
| | 4 | 業務規劃與物流 |
| DMZ | | 非戰區 |
| Operations and Control | 3 | 製造維運控制 |
| Control Area Zone(s) | 2 | 區域監督控制 |
| | 1 | 基礎控制 |
| | Layers 0 | 場域裝置 |

企業級防火牆 | 身份驗證與存取管理 | 惡意行為偵測與回應 | 資產探索，可視化與概要分析 | 終端防護 | 諮詢，整合與管理服務



## Fortinet Security Fabric 工控安全整體解決方案的 8 個落地階段


### 階段 1 可視化

實現了從監控網路到程序控制網路的可視化，達到透過辨別攻擊平面、安全防禦已知威脅，並為快速回應提供操作指南。為此，Fortinet 提供了 FortiGate 防火牆（包括 Rugged 系列工控系列）、FortiSwitch 安全網路交換器、FortiAP 無線基地台、 FortiGuard 威脅情資服務與專有 OT 協定及漏洞防護等元件。

### 階段 2 集中管理

針對 Purdue 模型中辨別攻擊平面、安全防禦已知威脅、快速回應的需求，Fortinet 提供了 FortiManager 與 FortiAnalyzer。其中，FortiManager 集中式的管理控制台，讓您輕鬆控制數千個支援 FortiOS 的裝置的安全政策、FortiGuard 威脅特徵資料庫版本更新、軟體版本與相關設定的部署。集中管理可以讓企業的安全管理節省大量的時間，如裝置自動探索，組態管理，全域資安原則，審計功能以及管理複雜 VPN 環境的能力。

FortiAnalyzer 透過匯聚 Fortinet 裝置日誌或告警資訊，為客戶提供了一個簡化、統一的安全管理分析平台。透過定制化的報告，使用者可以過濾與查看記錄，包括流量，事件，病毒，攻擊，網頁內容與電子郵件資料。透過對安全資料的挖掘，使用者可以確定系統的安全性與合規性。

## 階段 3 安全區域劃分

針對攻擊平面與資安事故回應的需要，避免惡意操作在系統間橫向運動，不僅需要檢測與預防橫向行動，更需要提前設定安全區域。因此，Fortinet 在設計動態安全架構模型時採用特定工作負載與應用服務流量模式的微分段隔離技術。企業需要能夠將物聯網裝置與通訊分為原則驅動的群組，並授予特定物聯網風險適合的基準權限。 Fortinet 的內網分段防火牆與網路交換器支援企業對其網路與裝置進行微分段，使 IT 系統能夠根據特定裝置類型與網路存取需求，採用分層、分區的安全政策。

## 階段 4 網路存取控制

工業網際網路涉及的工業控制裝置、無線接入裝置、邊緣終端裝置、重要網路裝置等存在大量安全漏洞，一但被攻擊者利用，將對裝置的可靠運作與網路品質造成嚴重影響。故此，Fortinet 提供了使用者認證（多因子認證）、裝置認證與網路存取控制（NAC）、端點安全防禦與異常行為分析檢測（UEBA）為一體的網路注入控制技術。架構支援透過使用者登入、多因子輸入或憑證等方式進一步驗證使用者身份，然後將其綁定到基於角色的存取控制（RBAC），進而將經過身份驗證的使用者與特定存取權限與服務進行比對。此外，FortiNAC 還可以準確地發現並辨別連線網路或正在尋求存取網路的每台裝置，對其進行掃描，以確定它未受感染，然後分析裝置，以確定其角色與功能 - 是否為最終使用者的手機或筆記型電腦、網路伺服器、印表機或無界面物聯網裝置（例如 HVAC 控制器或者安全識別證讀卡機）。 UEBA 可辨別跨多個使用者，實體或 IP 的安全事件，發現內部威脅與未知威脅，形成以行為分析為中心的零信任安全體系，提升企業整體安全營運能力。

## 階段 5 抵禦已知與未知威脅

在此階段，提供了 FortiGuard 威脅情資服務，以及針對 OT 網路的智慧型蜜罐系統 FortiDeceptor、FortiSandbox 智能沙箱、FortiGate 新世代防火牆與 FortiClient

終端安全軟體等元件，實現了從監控網路到程序控制網路的主動防護，透過使用整合度高、自動化、細緻與深度的檢測、安全防禦與回應系統，替代了傳統需要消耗大量時間的檢測與手動回應機制，讓使用者避免成為被攻陷的目標，能夠有效抵禦未知威脅，讓組織減少損失。

## 階段 6 智能分析與偵測

如何更快速以及更有效的分析與檢測已知與未知的威脅，發現零日攻擊，是資安防護持續關注的重點。Fortinet 的 FortiNDR 是一個利用深度神經網路 (DNN) 技術且提供本地部署的網路安全分析產品，能夠快速分析與檢測新型態的威脅，為使用者帶來次秒級的進階威脅檢測與事件分析溯源能力。

FortiNDR 內建的 Virtual Security Analyst ( 虛擬安全分析師 )，可以在無監督模式下運行，可在最短的時間內研究發掘出新的威脅。由於 DNN 具有天生的自我學習能力，它可以不斷適應快速變化的網路威脅格局，包括由駭客與攻擊者透過人工智能或機器學習所發動的網路攻擊。

## 階段 7 OT 資安態勢感應與回應

Fortinet 的 FortiSIEM 安全資訊與事件管理解決方案可以在單一可擴充的解決方案中提供可視性、關聯性、自動化回應與執行緩解調控措施，FortiGate 則可以提供從監控網路到控制網路的主動防護，並與 Nozomi Networks 等第三方 OT DPI 檢測工具協作，對於異常行為進行及時回應。

## 階段 8 信任評估

針對辨別攻擊平面、安全防禦已知威脅、快速回應、信任評估需求，SIEM 可以說是網路安全專業人員必不可少的支撐工具。它可以作為所有資料收集與分析活動的集中點，可對系統日誌與網路資訊提供智慧型分析。一但 SIEM 設定正確，它便可以搜尋惡意行為與系統活動，在安全事件惡化成為有影響的資料洩露事件之前提醒企業的資安事故反應團隊。為此，Fortinet 提供了 FortiSIEM，從 IoT 到雲端，統整收集分析跨廠商各種設備與應用服務的日誌與資訊，與自動化事件回應多方面進行整合。此外，FortiSIEM 資源庫還提供了預設的資安事故緩解調控腳本，可以與來自各種廠商的裝置與系統來進行手動或自動化連動，達成快速有效的協作聯防。

04

# Fortinet Security Fabric 工控安全整體解決方案安全元件

**階段 1 可視化與階段 3 安全區域劃分** —— 解決方案及元件

安全區域劃分提供了工業級防火牆、交換器及無線產品

- FortiGate Rugged 系列工業級防火牆
- FortiSwitch 安全網路交換器
- FortiAP（戶外 / 工廠層級）無線基地台

## FortiGate 符合的工業標準與合規性

IEC 61850

ICE-61850 描述了用於電子的統一通訊系統設計。 IEC-61850-3 提供了在這種苛刻環境中部署的裝置的硬體要求指導。

### EMI

未受保護的裝置在暴露於高水平的電磁干擾時可能會發生故障或被破壞

- 需要強大的電磁相容性（EMC）設計

### 溫度

在惡劣的環境（-20 至 +75° C）溫度中可以正常運作。

- 需要高效的散熱系統與自我加熱適應系統

### 抗震

- 裝置必須能夠承受從機櫃機架上掉落下來
- 可以對抗 50G 衝擊與 5-500Mhz 抗振動要求
- 保護裝置用於緩衝

## 完整的安全解決方案

IEC 61850

COMPLIANCE ENGINEERING

FortiGate Rugged 30D

FortiGate Rugged 35D

FortiGate Rugged 60D

FortiGate Rugged 90D

FortiGate Rugged 系列工業級防火牆

FortiSwitch 工業級安全網路交換器與 FortiAP 無線基地台

## 工業級防火牆

Fortinet FrotiGate 新世代防火牆（NGFW）可透過消除單點產品並整合的安全功能，例如 SSL 深層檢測（包括最新 TLS1.3）、網頁過濾、入侵安全防禦系統（IPS），提供全面的可視性並保護任何邊緣，進而幫助降低成本與復雜性。FortiGate NGFW 能夠滿足超大規模與混合 IT 架構的獨特效能需求，支援組織提供最佳使用者體驗，並高效管理安全風險，進而提高業務連續性。

FortiGate NGFW 能夠對進出網路的流量進行超大規模檢查。檢查速度、 規模及效能無與倫比，可確定僅放行合法流量，同時不會影響使用者體驗或造成成本高昂的停機。

作為 Fortinet Security Fabric 的重要組成部分，FortiGate NGFW 能夠與廣泛的 Fortinet 安全產品以及多廠商環境中的第三方安全解決方案進行溝通。FortiGate NGFW 可透過與人工智慧 (AI) 驅動的 FortiGuard 與 FortiSandbox 服務無縫整合，有效防範已知與零日威脅，並透過與 Fabric 管理中心相整合，大幅提高營運效率。

傳統安全解決方案主要面向辦公室與企業環境，而 FortiGate Rugged 系列則是經過工業加強的多合一安全裝置，可提供專門的威脅防護，切實保護關鍵工業與控制網路免遭惡意攻擊。

## FortiGate NGFW 使用案例

FortiGate NGFW 可透過為任何邊緣與任何規模的應用提供有效保護，幫助組織實現數位轉型。它可幫助組織提高營運效率、實現工作流程自動化，並為組織提供一流的威脅防護來改善安全態勢。 FortiGate NGFW 擁有業界最高的安全計算評選以及下列優勢：

**管理外部安全風險**

隨著 HTTPS 流量的日益成長，如果不應用 TLS 進行解密，組織將無法檢測到近 90% 的加密 HTTPS 流量。這無疑會將組織置於針對性惡意軟體攻擊與資料丟失的風險之中。 FortiGate NGFW 可幫助建構安全驅動型網路，實現應用、威脅與網路的全面可視化。其經產業驗證的一流安全防護能力可延伸到任何邊緣，進而確保組織持續正常營運，實現業務連續性。

**管理內部安全風險**

扁平式的網路不提供任何進階安全檢查，一但遭到攻擊便會陷入癱瘓。FortiGate NGFW 可透過基於網路的分段設計來縮小攻擊面並抑制攻擊在網路中橫向傳播的能力，並透過自動化工作流程、自調適的信任管理與高效能威脅防護保護所有的分段（基於微觀、宏觀、連線埠或應用），進而實現深度安全防禦、合規性與可信任的應用存取。

**管理漏洞**

大多數惡意軟體都透過已知漏洞進行傳播，是攻擊事件的罪魁禍首。 FortiGate NGFW 提供綜合性 IPS，能夠以毫無妥協的效能提供虛擬補丁能力與防範已知與零日攻擊，同時降低成本與復雜性。

**提供超大規模安全性**

傳統防火牆無法超高速處理大量的使用者流量，嚴重影響了使用者體驗。無視安全性只會給攻擊者破壞服務提供可乘之機。 Fortinet NGFW 提供了無與倫比的獨特安全性，可確定業務網站始終可用的存取性、迅速回應，並提供卓越的使用者體驗。

**安全連網入雲**

組織希望透過雲端實現靈活性、彈性與按需擴充。為了保持良好的使用者體驗與合規性，組織需要以網路的速度安全地從雲端傳入傳出資料。傳統防火牆不支援快速的巨量傳輸流，導致拖慢業務速度。 Fortinet 新世代防火牆提支援大象流（Elephant Flow），提供大型快速傳輸功能。該功能可支援高達 100Gbps 的巨量傳輸，並且能夠以相同的傳輸量等級使用 IPsec 進行加密。

**安全型分支機構解決方案**

在製造企業的數位轉型的過程中，企業往往聚焦工業軟體、工業控制系統、生產裝置等領域，而忽視了網路基層 —— IT 網路的建設。傳統製造企業中保守的網路結構、填補式的網路元件，不利於新技術的落地，也很難實現業務的開放與交互協作能力，且同時還面臨著不斷擴大的資訊安全風險。

透過在製造企業打造一個堅實健壯的底層網路，能夠更好地支撐上層業務的連通與擴充。作為安全與 SD-WAN 領域領導者，以及在三個 SD-Branch 相關領域（WAN 邊界、安全、WLAN&LAN）的唯一 Gartner 象限入榜廠商，Fortinet 推出了安全型分支機構解決方案 （Secure SD-Branch），可以在效能與網路擴充、安全、網路簡化方面滿足製造業的網路數位轉型需求。

Fortinet Secure SD-Branch 使用先進的硬體與軟體設計架構，為企業數位化網路提供至臻的網路效能與系統功能。 FortiGate 防火牆架構採取自主硬體研發的 ASIC 晶片加速，提供超高的網路吞吐效能。 Fortinet 還提供 FortiGate 完成 SD WAN 組網的技術方案，企業可透過高速的網際網路完成 SD-WAN 。

Fortinet Secure SD-Branch 架構中，集中控制器 FortiManager 支援集中化控制所有裝置，模板化製定安全政策，零接觸部署，集中 SD-WAN 監控等功能；此外透過 FortiLink 技術，FortiSwitch 網路交換器與 FortiAP 無線基地台可以被防火牆直接管理，簡化系統架構，降低管理操作複雜度。

該解決方案使用 FortiOS 作業系統，對多項進階安全功能進行整合與精細調試。此外，透過 FortiLink 技術，FortiSwitch 網路交換器與 FortiAP 無線基地台的流量可以透過通道模式進入防火牆進行安全政策控管，實現東西向隔離。

**產品優勢： 工業級**防火牆裝置、專有 OT 協定支援

| | FGR-30D | FGR-35D | FGR-60F | FGR-60F-3G4G |
|---|---|---|---|---|
| 防火牆效能 (1518 UDP) | 900 Mbps | 550 Mbps | 6 Gbps | 6 Gbps |
| 同時連線會談數 | 750,000 | 750,000 | 600,000 | 6000,000 |
| 新建連線會談數 / 秒 | 5,000 | 5,000 | 19,000 | 19,000 |
| IP Sec VPN 效能 | 45 Mbps | 45 Mbps | 3.5 Mbps | 3.5 Gbps |
| IPS 效能 (Ent.Mix) | 180 Mbps | 210 Mbps | 950 Mbps | 950 Mbps |
| NGFW 效能 (Ent.Mix) | 45 Mbps | 65 Mbps | 550 Mbps | 550 Mbps |
| Threat Protection 效能 (Ent.Mix) | 16 Mbps | 16 Mbps | 5000 Mbps | 500 Mbps |
| 介面 | 4 個 GE RJ45 埠<br>2 個 GE SFP 插槽 | 3 個 GE RJ45 埠 | 4 個 GE RJ45 埠<br>1 對 GE RJ45 bypass 埠<br>2 個 RJ45/SFP 分享埠 | 4 個 GE RJ45 埠<br>1 對 GE RJ45 bypass 埠<br>2 個 RJ45/SFP 分享埠<br>3G/4G LTE |
| 存儲 | - | - | - | - |
| 其他 | IP20 | IP67 | IP20 | IP20 |

## 安全乙太網路交換器

### 安全乙太網路交換器摘要

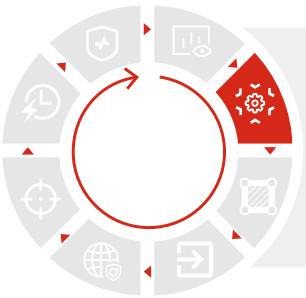
傳統乙太網路 LAN 面臨諸多挑戰，包括裝置與應用數量的指數級成長、來自無線網路的更高傳輸量需求以及復雜的安全部署。但 Fortinet 並未將目光僅鎖定在保護傳統乙太網路 LAN 上，而是採用了一種安全驅動型網路方法，透過 FortiSwitch 與 FortiLink 將乙太網路作為安全基礎架構的擴充來提供。此外，最新版 FortiOS 6.4 提供 NAC 網路存取基礎功能，且無需額外授權。 FortiSwitch 提供了廣泛的乙太網路交換器組合，它們安全、簡單且可擴充，非常適合從辦公環境到資料中心以及安全型 SD-Branch 與各種應用。

### 安全乙太網路交換器產品詳情

Fortinet 乙太網路交換器可獨立管理，也可透過 FortiLink 協定直接整合到 Fortinet Security Fabric 中。 FortiLink 是 FortiSwitch 的關鍵支援技術，其連線埠可充當 FortiGate 安全裝置的擴充連線埠。透過 FortiLink 連線時，FortiSwitch 的安全性可以對應 FortiGate 安全政策，進而為防火牆介面與交換器連線埠提供相同的安全性。 FortiGate 集中管理功能可透過零接觸自動探索、一鍵式 VLAN 與安全政策配置，簡化 FortiSwitch 部署與設定。借助整合存取層，FortiGate 可提供統一的視覺化圖形顯示與報告，進而簡化管理與故障排除。最後，FortiLink 可支援每個 FortiGate 最多堆疊 300 個交換器（具體取決於型號）。上述所有功能均免費提供，無需支付授權費用。

## 集中管理平台

**階段 2 集中管理** —— 解決方案及元件



Fortinet 管理與分析平台為本地、雲端與混合環境提供強大而簡化的網路配置、自動化與回應功能。 Fortinet 管理與分析技術業經十多年考驗，已獲得全球客戶的認可，廣泛部署於各種行業。

隨著企業網路在數位轉型中的演變，過去所依賴的工具已經變得陳舊過時。但仍有不少舊工具與新技術堆棧部署在一起，這就造成了無法互操作的複雜環境。企業部署的各種廠商的各式解決方案平均多達 75 種，並且這些解決方案之間無法共享威脅情資，這阻礙了網路安全防護，專業網路安全管理人員的欠缺更是進一步加劇了該問題。

簡化的網路配置、自動化與回應有助於整合複雜且各自為政的單點產品，並能夠與 Fortinet 解決方案以及所有 Security Fabric 合作夥伴整合相容。

FortiManager 與 FortiAnalyzer 等 Fortinet 產品可簡化網路配置、自動化與回應。

### FortiAnalyzer 日誌與報告分析產品型號：

| | FAZ-150G | FAZ-300G | FAZ-800G | FAZ-1000F | FAZ-3000G | FAZ-3500G | FAZ-3700G |
|---|---|---|---|---|---|---|---|
| GB/ 天 | 25 | 100 | 200 | 660 | 3,000 | 5,000 | 8,300 |
| 連續日誌處理速率 ( 日誌數 / 秒 ) | 500 | 2,000 | 4,000 | 20,000 | 42,000 | 60,000 | 100,000 |
| 連續日誌處理速率 ( 日誌數 / 秒 ) | 750 | 3,000 | 6,000 | 30,000 | 60,000 | 90,000 | 150,000 |
| 最大裝置數 / VDOM | 50 | 180 | 800 | 2,000 | 4,000 | 10,000 | 10,000 |
| 最大天數分析 | 90 | 50 | 50 | 34 | 30 | 38 | 60 |
| 介面總數 | 2 個 GE RJ45 | 4 個 GE RJ45 | 4 個 GE RJ45<br>2 個 GE SFP | 2 個 10 GE RJ45<br>2 個 10 GE SFP+ | 2 個 GE RJ45<br>2 個 25GE SFP28 | 2 個 GE RJ45<br>2 個 25GE SFP28 | 2 個 10 GE RJ45<br>2 個 25GE SFP28 |
| 存儲容量 | 2x 2 TB | 2x 4 TB | 4x 4 TB | 8x 4 TB | 16x 4 TB | 24x 4 TB | 60x 4 TB |
| RAID 支援 | (0/1) | (0/1) | ( 0/1, 1s/5, 5s/10 ) | ( 0/1, 1s/5, 5s/6, 6s/10/50/60 ) | ( 0/1, 1s/5, 5s/6, 6s/10/50/60 ) | ( 0/1, 1s/5, 5s/6, 6s/10/50/60 ) | ( 0/1, 1s/5, 5s/6, 6s/10/50/60 ) |

### FortiManger 集中管理平台產品型號：

| | FMG-200G | FMG-400G | FMG-1000F | FMG-3000G | FMG-3700G |
|---|---|---|---|---|---|
| 最大裝置數 /VDOM | 30 | 150 | 1,000 | 8,000 | 100,000 |
| 連續日誌處理速率 ( 日誌數 / 秒 ) | 50 | 50 | 50 | 150 | 150 |
| GB / 天 | 2 | 2 | 2 | 10 | 10 |
| 介面 | 4 個 GE RJ45 | 4 個 GE RJ45<br>2 個 GE SFP | 2 個 10GE RJ45<br>2 個 10GE SFP+ | 2 個 GE RJ45<br>2 個 25 GE SFP28 | 2 個 10GE RJ45<br>2 個 25GE SFP28 |
| 存儲容量 | 2x 4 TB | 8x4 TB | 8x4 TB | 16x4 TB | 60x4 TB |

## 進階威脅安全防禦

**階段 5 抵禦已知與未知威脅 / 階段 7 OT 資安態勢感知與回應 / 階段 8 信任評估**
—— 解決方案及元件

### 01 FortiSandbox — 零日威脅保護

**什麼是惡意軟體沙箱？**

上一代病毒數量少且複雜程度低，殺毒工具完全可以透過其特徵碼資料庫提供合理的保護。

但如今，病毒的數量與復雜程度不可同日而語，現代惡意軟體普遍採用漏洞利用等新型技術。合法應用中的漏洞一但被利用就會導致異常行為，攻擊者正是利用這種異常行為來破壞電腦系統。利用未知軟體漏洞發起的攻擊被稱為零日攻擊，也就是零時差攻擊，沙箱技術是目前最有效的零日攻擊防禦手段。

在電腦安全環境中，惡意軟體沙箱是一個將應用操作（例如打開 Word 文檔）限制在隔離環境中的系統。在這個安全的環境中，沙箱會分析對象的動態行為及其在偽裝的使用者環境中的各種應用交互，並檢測任何惡意意圖。因此，如果發生意外攻擊，只有沙箱會受到影響，網路上的其他電腦與裝置將安然無恙。與此同時， 沙箱會捕捉所有惡意意圖，發出警報並生成相關威脅情資，進而有效攔截零日攻擊。

惡意軟體沙箱的典型特質：

1. 檢測引擎由靜態與動態分析組成，可擷取惡意軟體屬性與技術。
2. 模擬各種裝置作業系統，包括 Windows、macOS、Linux 與 SCADA/ICS，以及相關應用與協定。
3. 支援多種資料來源，包括網路資料封包、文件共享、按需送出與 NGFW、SEG、EPP/EDR 與 WAF 的自動送出，以及其他整合安全控制 。
4. 報告與自動共享威脅情資 。
5. 靈活的部署模式，例如裝置、虛擬裝置、SaaS 與公有雲，可適應各種本地環境與雲端環境。

**Fortinet 智能沙箱解決方案**

- 業內首例基於機器學習（ML）的靜態與動態分析解決方案（專利申請中）。

- 基於 MITRE ATT & CK 標準的報告。
- 與 Fortinet 與非 Fortinet 解決方案相整合，自動安全防禦零日攻擊。

**Fortinet 智能沙箱解決方案特性及優勢如下：**

| 獲得獨立機構最高評選 | 提高效率與效能 | 加快威脅調查 |
|---|---|---|
| NSS Labs “推薦”用於基於沙箱的漏洞檢測與漏洞預防；透過了 ICSA Labs 進階威脅安全防禦認證。 | 利用兩個機器學習模型，提高了對零日威脅的靜態與動態惡意軟體分析能力。 | 內建 MITRE ATT & CK 矩陣可辨別各種惡意軟體技術。 |
| **廣泛整合** | **自動漏洞防護** | **統一 IT-OT 零日威脅防護** |
| 將零日威脅檢測擴充到新世代防火牆、網頁應用防火牆、安全電子郵件閘道器與端點保護平台。 | 透過共享即時更新，從源頭上攔截威脅，然後在整個組織內實施安全防護，進而加快安全防禦速度。 | 保護 IT 與 OT 環境以及資產免遭惡意軟體破壞。 |

## 02 FortiDeceptor – SCADA 商用智慧型蜜罐系統

FortiDeceptor 基於欺敵技術，與組織現有的漏洞防護政策相得益彰，它能夠欺騙、暴露與消除來自外部或內部的攻擊，進而避免實際損害的發生。

FortiDeceptor 身為 Fortinet Security Fabric 平台中的安全元件，可支援組織透過智慧型設定與自動部署，實現與現有 IT/OT 基礎架構無縫整合的誘餌，快速建立虛假欺敵網路，進而誘使攻擊者上鉤。

**切實可用的可視性**

GUI 威脅地圖可快速發現針對組織的威脅活動。

**自動保護**

能夠和 Security Fabric 與 FortiGate 相整合，可基於嚴重性即時攔截攻擊活動，進而避免實際損害的發生。

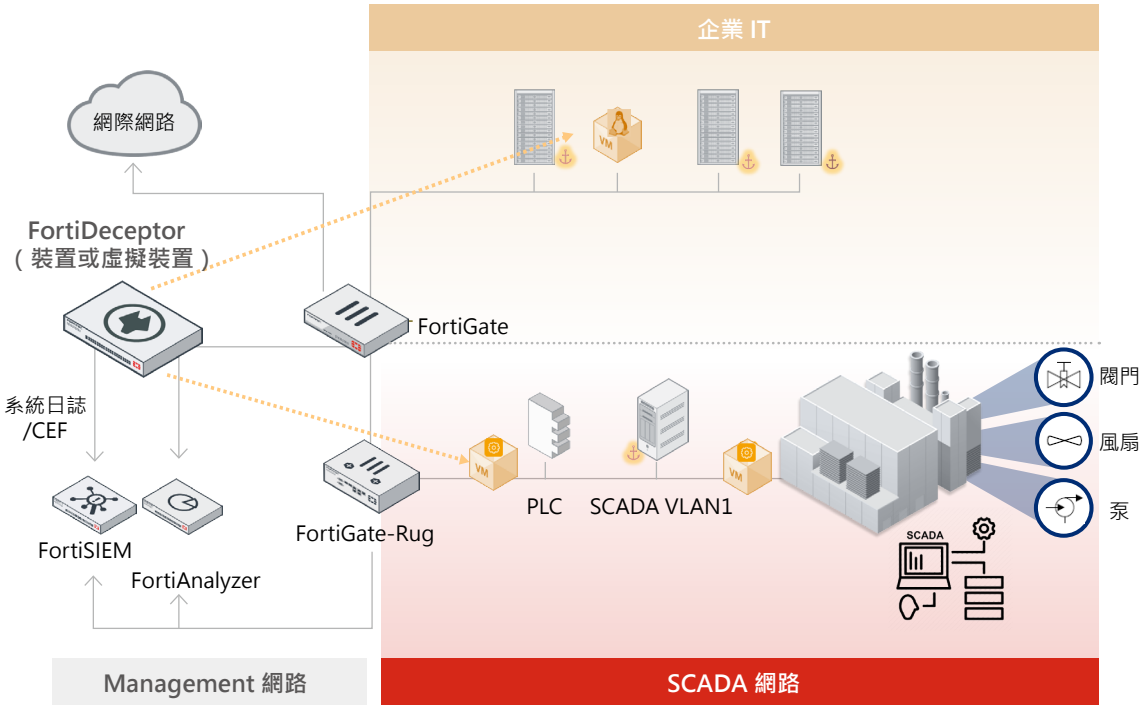
**輕鬆部署**

集中管理預建構或自定義誘餌的部署，並實現其自動化。

**統一的 IT-OT 漏洞防護**

透過被動足跡監看提供網路可視性和漏洞檢測。針對無法自行辨識威脅的資產，例如物聯網、SCADA 和醫療設備提供防護。

## FortiDeceptor — SCADA 商用智慧型蜜罐




### 支援的協定

- HTTP
- FTP
- TFTP
- MODBUS
- S7COMM
- BACNET
- IPMI
- TRIXONEX
- GUARDIAN-AST
- IEC 60870-5-104

### 關聯功能

- 告警
- 隔離

| | FDC-1000G | FDC-VM |
|---|---|---|
| 虛擬裝置執行個體支援（最大值）* | 20 | 20 |
| Vlan 支援（最大） | 128 | 128 |
| 介面 | 4 個 GE RJ45，4 個 GE SFP | 6 個虛擬 |
| 存儲容量 | 2TB（2 塊 1 TB HDD） | 200GB 至 16 TB |

## 03 FortiSIEM

### SIEM 摘要

隨著數位轉型席捲各個產業，攻擊面（不斷）急劇擴大，安全管理變得愈發困難。資安團隊在各種安全裝置產生的大量告警及其他資訊面前應接不暇。網路安全技能差距進一步加大了安全管理的難度。

基礎架構、應用與端點（包括物聯網裝置）都必須得到安全保護。這就需要獲得對所有裝置與所有基礎架構的即時可視性。組織還需要清楚哪些裝置存在威脅隱患以及威脅的藏身之地。

### FortiSIEM 提供新一代 SIEM 功能

FortiSIEM 將可視性、相關性、自動回應與修復功能整合到單個可擴充解決方案中。它能夠降低管理網路與安全營運的複雜性，有效地釋放人力資源、改善漏洞檢測水準，甚至能夠防止漏洞的發生。

而且，我們的架構能夠從各種資訊來源（包括日誌、效能指標、安全告警與組態異動）進行統一的資料收集與分析。 FortiSIEM 將安全營運中心（SOC）與網路營運中心（NOC）中常見的孤立分析技術相整合，能夠更全面地了解業務的安全性與可用性。

此外，FortiSIEM UEBA 利用機器學習與統計方法來界定正常行為與營運基準線，辨別有關業務關鍵型資料的異常使用者行為。借助從端點傳感器、 網路裝置流量記錄、伺服器與應用日誌以及雲端 API 提取的遙測資料，可提供端到端（從端點到本地伺服器與網路活動，再到雲端應用）活動的全面可視性。

針對進階持續性威脅或勒索病毒的攻擊，導入 AI / ML 智能分析，對應 MITRE 資安新框架，提供先期預警能力。

內建派工管理系統，可連動跨廠商的設備，滿足自動化協作聯防的需要。

## 04 FortiNAC

**階段 4 網路存取控制 / 階段 8 信任評估** —— 解決方案及元件

**FortiNAC：網路存取安全解決方案**

FortiNAC 是 Fortinet 網路存取控制解決方案。它可透過對所有連網內容進行監控、控制與自動化回應來加強整體 Fortinet Security Fabric。它可提供針對物聯網威脅的防護，將控制擴充到第三方裝置，並協調對各種網路事件的自動化回應。

**FortiNAC 支援保護物聯網裝置的三項關鍵功能：**

- 網路可視性，可查看接入網路的每個裝置與使用者
- 網路控制，可限制裝置在網路上的位置
- 自動回應，可將事件回應時間從數天縮短至數秒

FortiNAC 解決方案可透過集中式架構保護無線與有線網路，集中式架構可透過自動化回應支援分佈式部署。

**FortiNAC 始終是一款理想的解決方案，無論您的安全政策處於何種階段或成熟度等級。借助 FortiNAC，組織可以：**

- 提供 Agent 與無 Agent 網路掃描，以對裝置進行檢測與分類
- 為所有聯網裝置建立清單，並評估每個連網端點的風險
- 使用集中式架構來簡化部署與管理
- 利用對第三方網路裝置的廣泛支援來確定整體有效性
- 實施動態存取控制
- 為事件回應做好準備，並將回應時間從數天或數週縮短至幾秒鐘
- 整合 SIEM 解決方案以提供詳細的環境資料並縮短調查時間
- 面向大量端點裝置、使用者與訪客實現接入與授權流程自動化

| | FNC-CA-500C | FNC-CA-600C | FNC-CA-700C | FNC-M-550C |
|---|---|---|---|---|
| 類型 | 控制與應用伺服器 | 高效能控制與應用伺服器 | 超高效能控制與應用伺服器 | 集中管理平台 |
| 目標環境 | 小型環境 | 中型環境 | 具有少量持久型 Agent 的大型環境 | 適用於多站點環境 |
| 容量 | 管理網路中最多 2,000 個連線埠 * | 管理網路中最多 15,000 個連線埠 * | 管理網路中最多 25,000 個連線埠 * | 無限制 |

# 數位化企業微分段隔離措施的必要性討論

微分段隔離技術有助於讓物聯網環境受控，是緩解物聯網安全風險的可行方案之一。微分段隔離技術可以實現：扁平網路的設計；安全可視化；控制橫向攻擊面，減小安全漏洞造成損害大面積傳播；提高所有被攻擊對象的安全性。

**與傳統隔離技術的差別：**

**更加細緻的網路安全管理**

新世代防火牆、虛擬區域網路（VLAN）與存取控制列表（ACL）等其他解決方案在一定程度上也進行了網路分段。而採用微分段技術，安全與存取政策被應用於每個工作負載，能更好地防止攻擊，與 VLAN 等技術相比，這些工具能夠對資料流進行更精細的分段設計。

**更少的漏洞，更少的交叉感染**

正確地實現微分段隔離，就可以在物聯網裝置與其他敏感資料來源之間增加一層安全防護，避免漏洞的暴露與惡意行為的擴散。在具體過程中，使用者可以把資料中心、辦公、生產、研發等場景劃分為不同的存取區塊，採用在 IT 與 OT 之間採用多重的安全隔離技術，減少 OT 系統的漏洞暴露，減少辦公網路惡意代碼進入生產環境。

**更低的部署與管理成本**

企業可以按照業務、安全導向的設計理念來靈活地構築安全邊界，在高風險區域部署智慧型蜜罐系統、智能沙箱等更進階的防護方案，在安全防禦等級相同的一般區域，部署採購成本較為低廉的網路安全裝置，並利用整合式軟體定義網路技術替代傳統疊床架屋的安全防護設備，配合統一的可視性圖形管理介面來降低整體的營運管理成本。

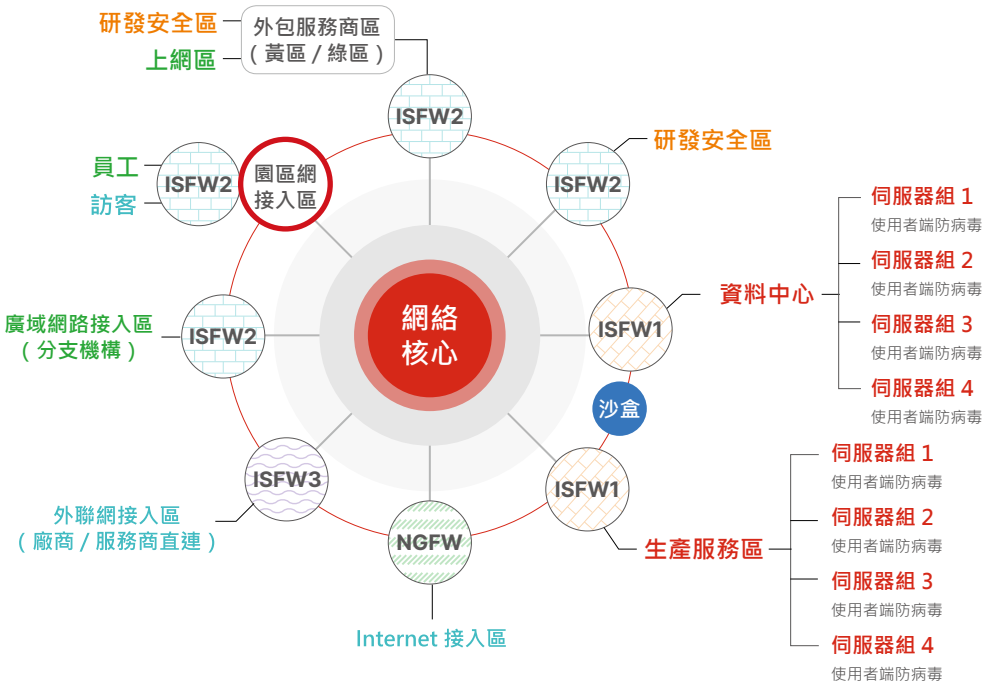
**更智慧型的風險管理關聯機制**

自動發現風險，自動評估風險，自動回應，並採取措施是未來的 OT 安全發展的方向。利用 OT 安全多樣化資訊之間的互相關聯，管理員可以建立一個高度自動化的系統，不僅在安全系統內進行關聯，還可以與 OT 操作系統進行深入的交互，達成智慧型的風險應對。

# Fortinet 護航大型製造業企業案例分享

## 01 微分段隔離解決方案案例

使用者採用基於零信任的精細安全區域劃分與設計，從邊界開始並擴充到內部網路分段，更好地控制資料流，保護網路免受進階威脅。在方案中，不同顏色的區域代表著不同的安全防護等級，並將物聯網裝置與通訊分為政策驅動的群組，授予特定了的適合工業網際網路的基準權限。同時採用高、中、低等級的存取安全政策， 部署與之對應的安全管理產品，所有的流量都透過防火牆、沙箱關聯，進而使企業能夠更好地控制裝置之間不斷增加的橫向通信量。

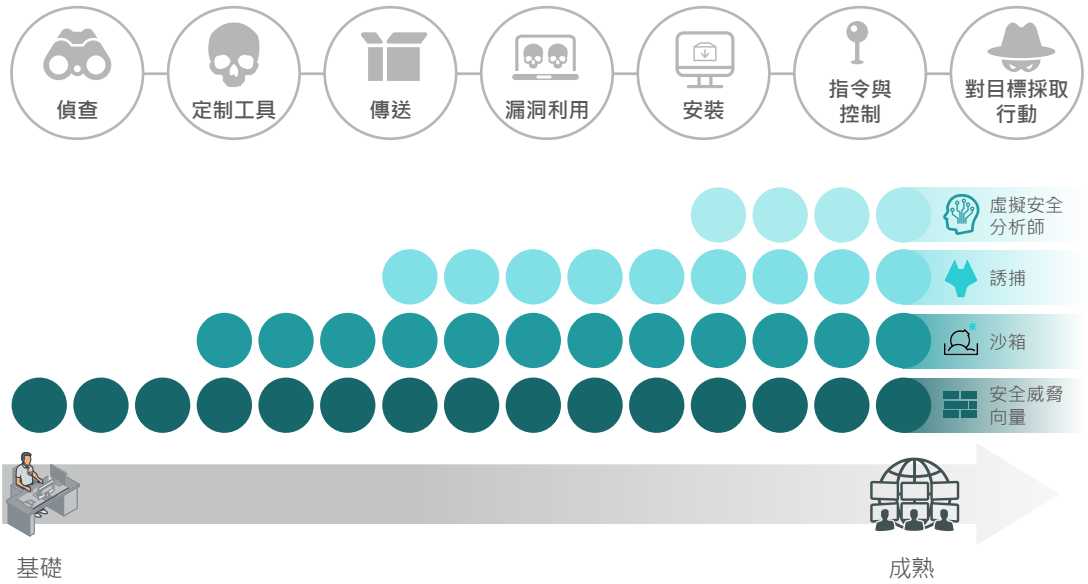



| ISFW1 | ISFW2 | ISFW3 | NGFW | 使用者端防病毒 | 沙箱 |
|---|---|---|---|---|---|
| 防火牆，IPS，防病毒，身份認證，網路存取控制，沙箱關聯 | 防火牆，IPS，身份認證 | 防火牆，IPS | 防火牆，IPS，防病毒，應用服務控制，URL 控制，殭屍網路，IP 信譽， 流量控制 | 不同作業系統，支援沙箱關聯 | 自動關聯，自動掃描共享文件夾 |

02

# 進階威脅及勒索軟體防禦案例

最近我們看到越來越多的工業網路遭到了進階持續性威脅（APT）的攻擊， 以及勒索軟體的侵入，生產安全與資訊安全遭到了重大打擊。因此，各個工業製造的客戶都在積極尋求解決方案。 Fortinet 在汽車製造，晶片製造，家電製造等各個領域的工業網際網路中，驗證與部署了專門針對 APT 與勒索軟體的防護體系。




透過 FortiSandbox、FortiNDR、FortiDeceptor、FortiNAC、FortiSIEM 等產品與技術，有機的構成了一個整體的進階威脅檢測體系，對於資安攻擊鏈的各個環節都能有效的檢測、發現與阻擋。最大程度的保護工業網際網路免於進階持續性的威脅。

**FortiGate**
Fabric 共享威脅資訊

**FortiAP**
無線接入與自動隔離

**FortiSwitch**
有線接入與自動隔離

**FortiSandbox**
“引爆” 可疑的對象

**FortiNDR**
採用 AI 技術的未知威脅檢測與防護

**FortiDeceptor**
工業網際網路智慧型蜜罐系統

**FortiNAC**
實現網路存取控制

**FortiSIEM**
日誌與記錄統整、關聯分析與回應

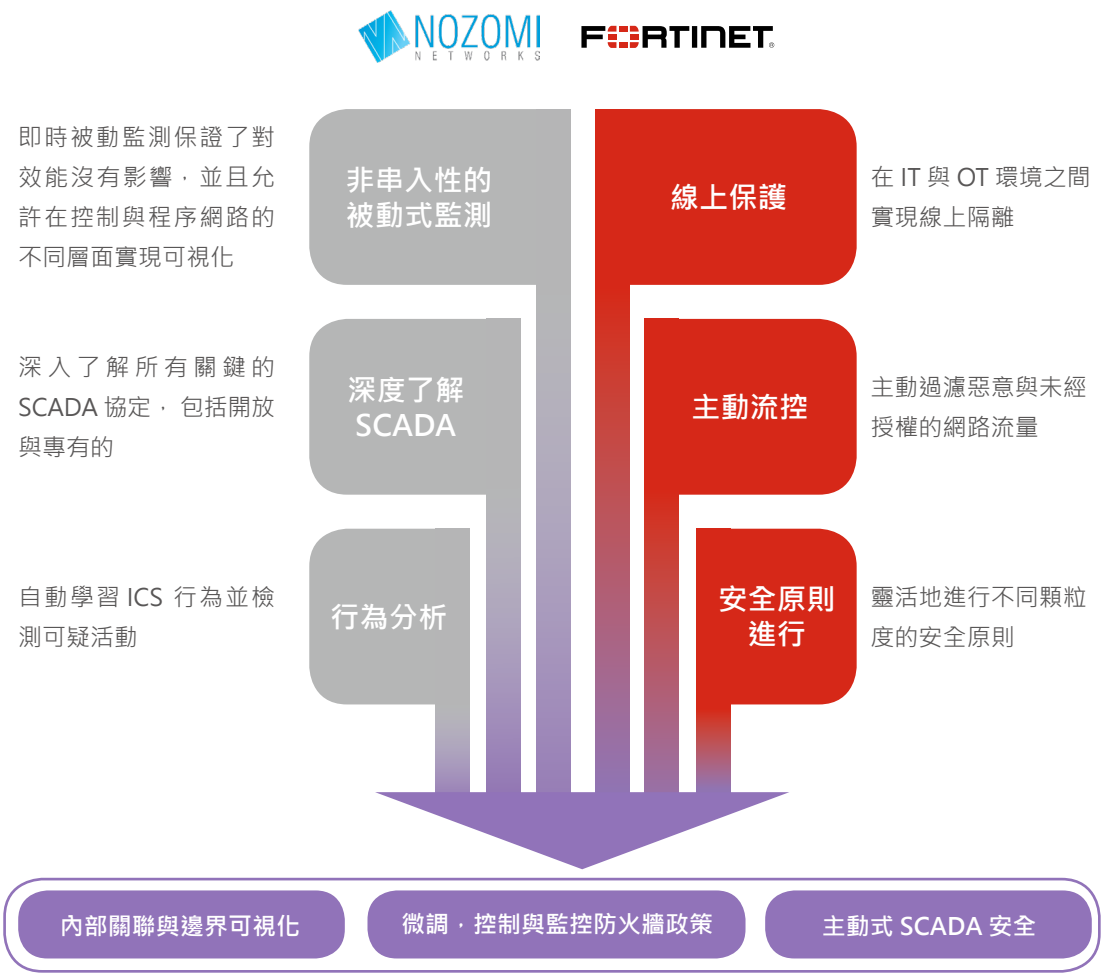
**FortiSOAR**
擴充的工作流自動化

**第三方工單系統**
建立個案，傳遞個案資訊

**第三方安全產品**
利用 Restful API 整合

# 03 Fortinet 與 Nozomi 整合工業安全案例

FortiGate 防火牆與 SCADAguardian 的整合是我們應對工業安全的有效解決方案。



台灣分公司
官方網站：https://www.fortinet.com/tw
免付費技術服務電話：0809-089-210