

QNAP

# 選擇 QNAP 建立 IT/OT 資安防線

從儲存到嚴密防護，營運安心不中斷





# IT/OT 資安分段做好、穩健做對

在現代企業營運中，IT 系統與 OT 現場早已密不可分，資安威脅也正從辦公網路蔓延至營運現場。對多數企業來說，實踐 OT 資安往往不是資源問題，而是落地方法與執行路徑的問題。

QNAP 深知企業導入資安防護時所面對的實務挑戰，因此我們不主張一次到位，而是從儲存到防護，逐步建立起可視、可控、可防禦的資安基礎，讓中小企業也能穩健踏出 IT/OT 資安的每一步。

80%

製造業企業在 2024 年經歷了  
更多資安事件或入侵<sup>1</sup>

45%

認為自身具備足夠能力應對這些威脅<sup>1</sup>

60%

坦言 OT 資安的複雜度是當前  
最大挑戰<sup>2</sup>

Data source

<https://www.telstrainternational.com/en/news-research/research/secure-manufacturing-the-challenges-of-IT-OT-convergence>

<https://www.paloaltonetworks.com/blog/network-security/state-of-ot-security-2024/>





# QNAP 將儲存技術 轉化為安全戰力， 守護企業 IT/OT 安全戰線

QNAP 擁有橫跨儲存、網通、安全偵測、備份隔離與遠端存取等多元產品組合，為不同規模與產業的 IT/OT 環境提供穩健支援。

同時，也可靈活對應 NIST CSF、IEC 62443 等主流 OT 資安標準架構，滿足關鍵基礎設施對資安分層防護的高度需求，協助企業打造「可視化、可防禦、可復原」的資安防線。







# 用對藍圖，資安更有方向

## 從 NIST CSF 2.0 開始，穩步建構 IT/OT 防線

- NIST Cybersecurity Framework（資安框架）已廣泛被企業、製造業與關鍵基礎設施採用，而 2024 年更新的 NIST CSF 2.0 更進一步強化了 OT 環境的實務應用
- 六大核心功能（Identify、Protect、Detect、Respond、Recover、Govern）為企業提供清晰的資安建設藍圖。
- 框架重視分層防護、資產可視性、事件應變與復原能力，與 QNAP 架構高度契合。
- 對中小型組織而言，NIST CSF 不僅是標準，更是可以逐步實施的實踐計畫。
- QNAP 以 NIST CSF 2.0 為主軸，整合 NAS、網路設備與安全應用，協助企業在現有 IT/OT 架構中導入可行的資安防線。



# 從標準到實踐

## QNAP 解決方案全面對應 NIST CSF 2.0 核心功能

- 全產品線標準內建功能
- 僅特定產品系列支援
- 不支援

功能分類	痛點	解決方案	NAS	QHora 路由器	ADRA 交換器	QSW 網管交換器
Identify 識別	IT/OT 環境設備多樣且缺乏統一資產清單	集中裝置管理	●	●	●	●
		可視化清單	●	●	●	●
		雲端監控	●	●	—	●
Protect 防護	老舊控制系統無法應對現代攻擊手法	資料加密	●	●	—	—
		多層存取控管	●	●	—	●
		網段隔離	●	●	●	●
Detect 偵測	缺乏對 IT 環境異常行為的即時監控能力	裝置異常偵測	●	●	●	●
		登入異常偵測	●	●	●	●
		網路異常偵測	●	●	●	●
Respond 回應	資安事件發生時無法即時通報與阻斷	即時通知	●	●	●	●
		遠端存取	●	●	●	●
		雲端管理	●	●	—	●
Recover 回復	系統復原缺乏自動化與備援，容易造成生產停擺	備援機制	●	●	—	●
		資料完整性	●	—	—	—
		災難復原	●	—	—	—





# 從儲存到網路，QNAP 強化 IT/OT 資安防護







# NAS

## 為 IT/OT 環境打造的關鍵資料儲存、備份與應用整合平台

- ・ 支援 AI 分析、虛擬化、QuFirewall 與 AMIZcloud 管理
- ・ 部分機型具工規設計 (寬溫、機架式 / 壁掛、雙電力)，適用嚴苛場域

### 企業級 QuTS hero NAS：

- ・ 高可靠度資料儲存與備份 (快照、不可變備份、WORM)
- ・ 高可用性 (HA) 架構降低中斷風險





# QHora 路由器

## 實現跨場域 IT/OT 網路安全互連與遠端維運防護

- Policy-based/ 靜態路由、L3 - L7 防火牆，提供 DPI 深度封包檢測與 IPS 入侵防護，實現微網段隔離 (Microsegmentation)
- 支援 Qbelt (DTLS + AES-256)、WireGuard、OpenVPN，確保安全遠端傳輸
- WPA/WPA2/WPA3 及 OWE，避免無線傳輸外洩
- Airgap+ 隔離備份，有效預防勒索病毒

### QuWAN SD-WAN：

- 多場域網路互聯及雲端集中管理
- 支援 WAN 優化與自動容錯，確保異地穩定連線





# ADRA NDR 交換器

## 即時防護 IT/OT 網路，抵禦惡意流量與異常行為

- 支援 OT 協議辨識與主動威脅陷阱，偵測上百台終端設備，及早識別內網橫向攻擊
- 透過 DPI 深度檢測揭露設備版本與漏洞，並結合行為與關聯分析，精準判斷可疑活動
- 針對中高風險事件，自動執行最小範圍阻隔，隔離受感染裝置，確保其他設備不中斷
- SOC/SIEM 協同，防護 NAS、電腦、印表機、高瓦數 PoE 攝影機，打造端到端資安防線



A black QNAP QSW network switch is shown from a top-down perspective, resting on a blue surface. The switch features a front panel with a QNAP logo, a management port, and 16 RJ45 ports. The first 8 ports are labeled 1 through 8, and the next 8 ports are labeled 9 through 16. The switch is illuminated with a blue light.

# QSW 網管型交換器

## 提供 IT/OT 系統長距離、高頻寬與穩定骨幹連線

- 2.5GbE/10GbE/25GbE/100GbE 與光纖長距離傳輸，適合大型 OT 廠區骨幹網路
- VLAN 與 QoS 管理，有效分流並優化不同 OT 應用的流量優先級
- 支援 AMIZcloud 雲端集中管理，簡化跨場域設備維運
- 部分機型具寬溫、機架式與 PoE，適用嚴苛環境

### 企業級 L3 交換器：

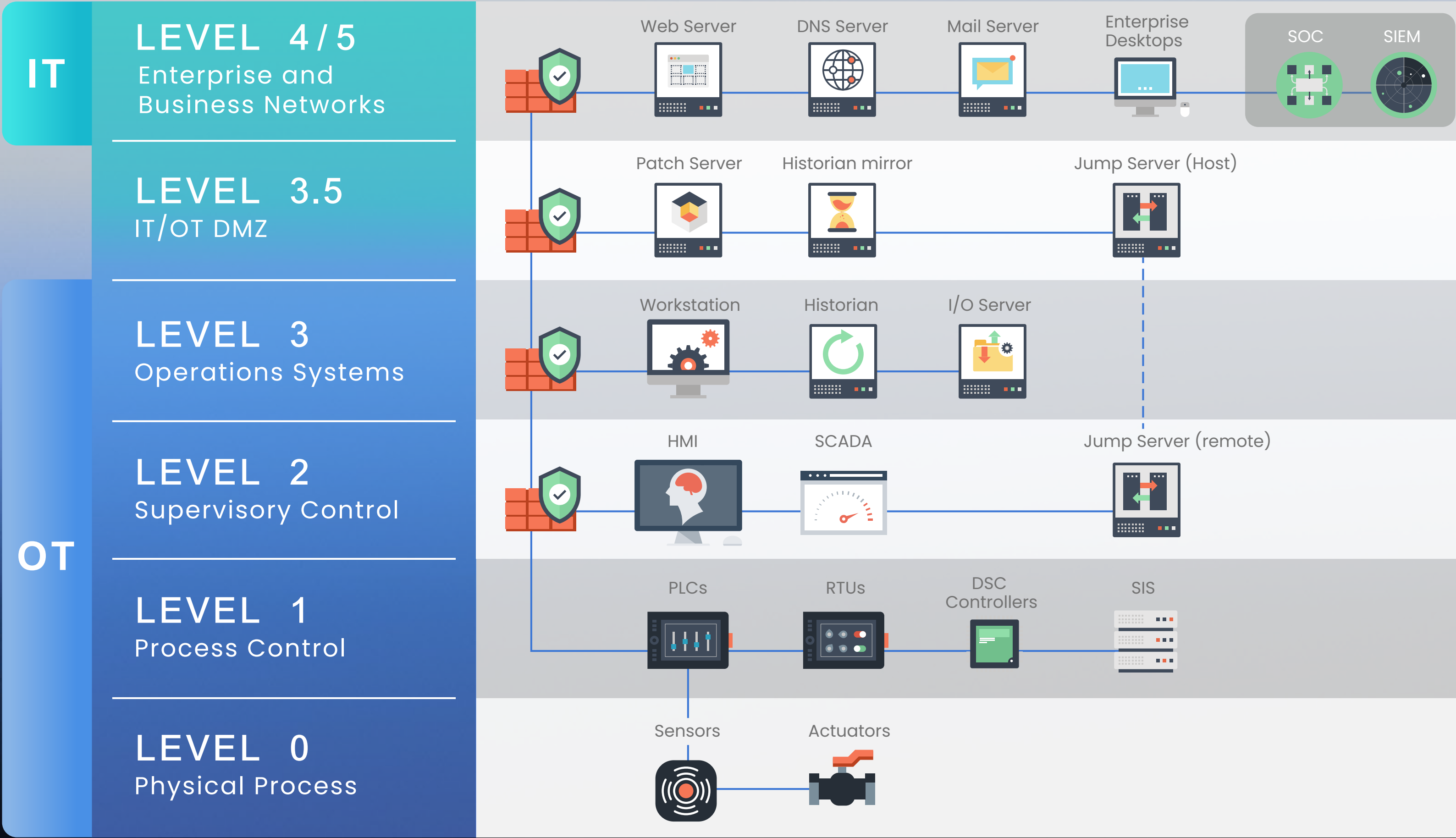
- 高可靠度 MC-LAG HA 功能，確保 24/7 工控環境不中斷運作
- PTP 符合 ITU-T G.8273.3 Class A，提供 <100ns 時間同步，確保 OT/ 工控通訊精準



# 以普渡模型為基礎，全面守護 IT/OT 營運

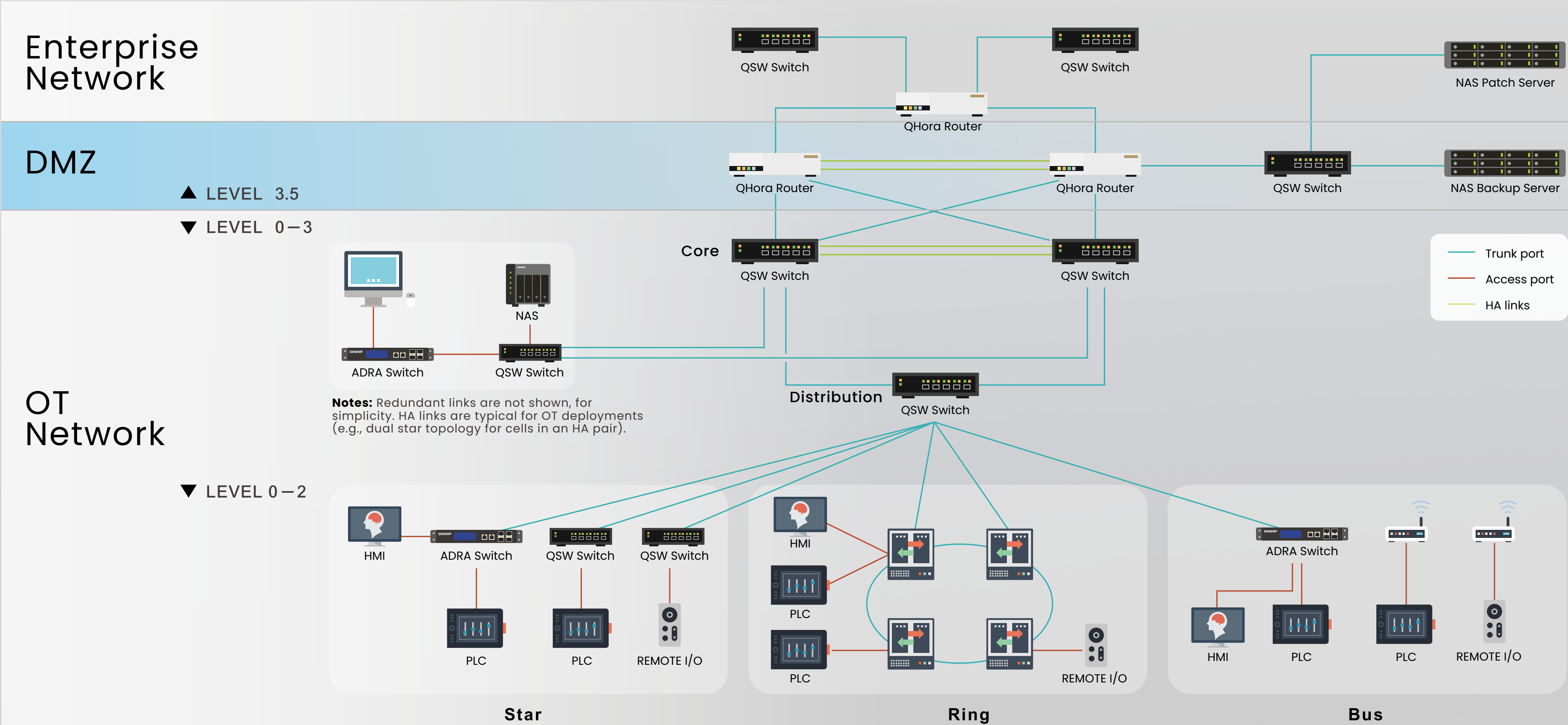
企業可採用符合國際標準的普渡模型 (Purdue Model) 作為工控網路分層架構，透過明確界定 IT 與 OT 的角色與邊界，進而為建構完善的資安防線與推動跨域協作奠定堅實基礎。

註：普渡模型為工控網路分層的通用架構，已廣泛應用於 ISA/IEC 62443 與 NIST 800-82 標準。





# QNAP 為您把關 IT/OT 交界層的資安防護





# 逐一拆解 NIST CSF 2.0 五大核心 打造可實踐的 IT/OT 資安防線





# Identify | 識別

## 從資產到身分的可視化，打好 IT/OT 資安基礎

資安防護的第一步是「知道自己擁有什麼」。但實務上，多數企業面臨資產無法統整、帳號分散、接線複雜等挑戰。QNAP 協助企業從人員、設備、網路、資料四個層面進行資產識別與權限管理，建立有效風險掌控基礎。

### 集中化資產盤點與設備管理：

- **QuWAN Orchestrator**：SD-WAN 雲端中控系統可自動辨識與集中管理企業網段中的 QNAP 設備，包含 IP 位址、型號與裝置狀態。
- **ADRA NDR 交換器 Device Inventory**：透過網路封包解析以自動識別區網內所有連接裝置的資訊，包括 MAC 位址、IP 位址、主機名稱等。

### 帳號整合與角色授權：

NAS 整合 AD/LDAP 與 Organization Center，建構角色型存取控制（RBAC），精準控管誰能存取什麼裝置與資料。

### 網路層級資產識別與監控：

QNAP 交換器支援靈活 VLAN 與 Port-based 管理，掌握設備分布與連線架構，補足 OT 現場難以掌控的「接線資產」盲區。





# Protect | 防護

## 多層防禦機制，全面守護系統、資料與網路

在 OT 環境中，僅依靠單一防護手段已不足以抵禦現代化攻擊。QNAP 提供多層防護機制，從系統到資料、從內部網路到網路管理，全方位提升基礎架構的韌性，確保生產與營運不中斷。

### NAS 系統防護：

支援多重要素驗證 (MFA) 與內建防火牆，防止未授權登入與惡意操作，確保 NAS 系統穩定可用。

### 資料安全與不可變儲存：

透過 AES-256 加密與不可變儲存 (WORM、Object Lock)，確保資料完整性並抵禦勒索軟體。搭配 Airgap+ 隔離備份，防止備份設備長期暴露於網路風險。

### 內網威脅隔離：

ADRA NDR 快篩網路偵測及應變設備針對 OT 網路流量進行過濾，並偵測惡意軟體的橫向移動與擴散，有效阻止攻擊者竊取或加密關鍵資料。

### 網路分段管理：

QNAP 交換器透過 VLAN 與 ACL 劃分生產、監控與管理網段，降低跨區域干擾並強化安全存取。





# Detect | 偵測

## 部署能理解網路流量與人機行為的監測系統

缺乏對 OT 內網流量與異常行為的即時監控，將使威脅長時間潛伏並擴大影響。QNAP 能從系統、網路到流量行為全方位即時察覺異常，縮短威脅偵測與應變時間，確保生產與營運安全。

### 系統與運行狀態監控：

NAS 可即時與持續監控系統狀態、檔案活動與存取紀錄，快速識別未授權存取、登入異常及可疑操作，並透過 AMIZcloud 雲端管理平台與 QuWAN 一元化管理與檢測所有 QNAP 裝置的運行狀態與資安風險。

### 惡意軟體偵測與移除：

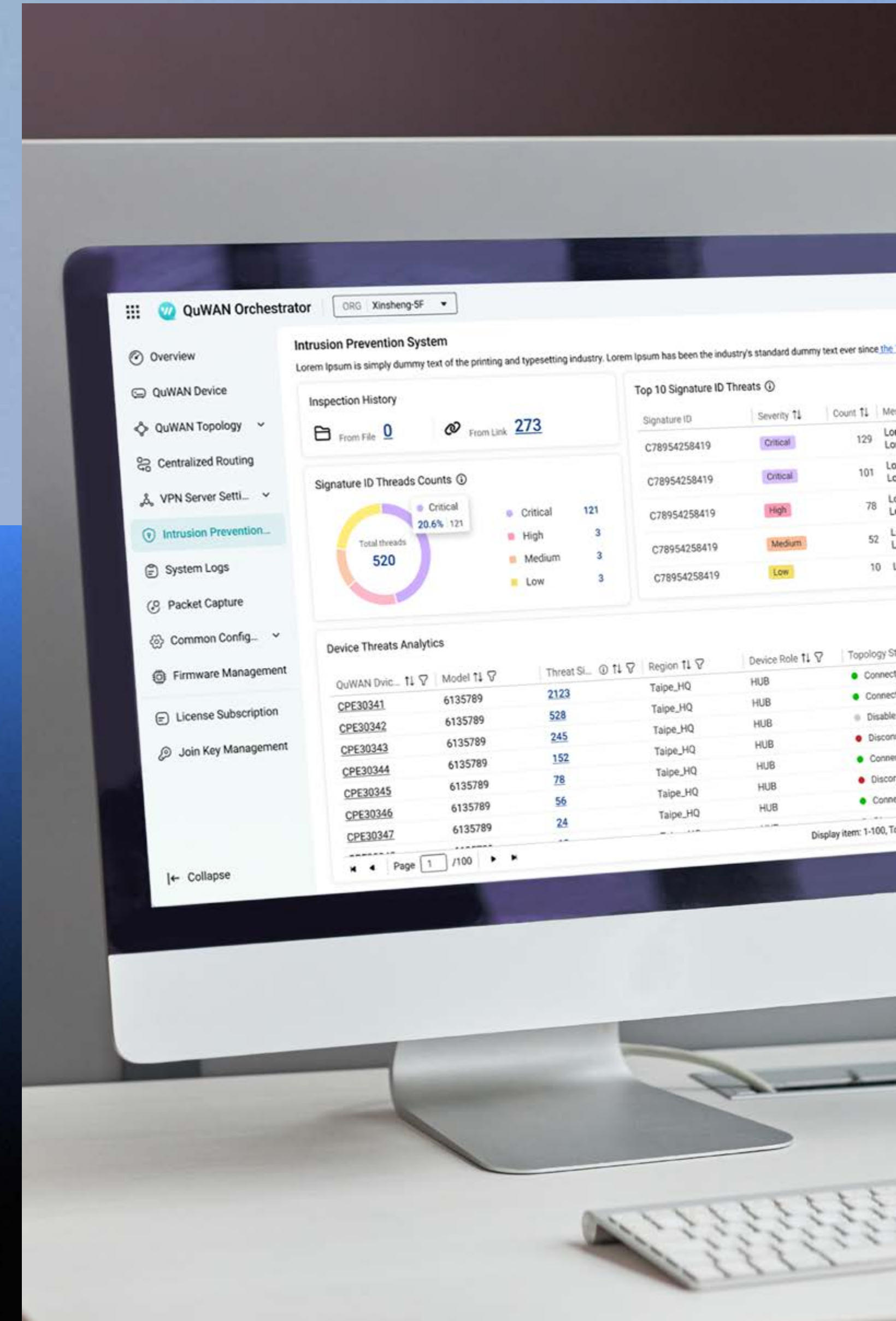
定期掃描 NAS 以偵測並移除惡意軟體，並由 QNAP 持續更新病毒定義檔，確保能即時防範最新、最危險的惡意威脅。除此之外，ADRA NDR 的 Trap 功能，可以提早發現惡意程式，並提早通知 IT 成員進行防護。

### 邊界網路威脅偵測：

QHora 路由器可設定入侵防禦 (IPS) 與即時封包檢測功能，可辨識並阻擋惡意流量，全面強化 OT 與 IT 網路邊界的安全性。

### 內網行為流量分析：

ADRA NDR 深入解析 OT 網路與內網行為，持續監控並依規則自動通報與記錄可疑事件，防止威脅擴散。





# Respond | 回應

## 即時通報、封鎖與遠端更新系統，有效遏止擴散

在 OT 環境中，任何資安事件的延誤處理都可能導致生產線停擺或安全事故。QNAP 提供即時通報與快速阻斷，確保威脅在擴散前被抑制。

### 即時事件通報：

結合 Notification Center，將異常事件同步推送至 Email、SMS、Syslog、Webhook 等多種管道，讓資安團隊與現場人員第一時間掌握狀況。

### 快速威脅阻斷：

在資安事件發生的第一時間，ADRA NDR 交換器可在確認威脅來源後立即隔離局部受影響設備，迅速切斷威脅的傳播路徑以防惡意流量進一步擴散，同時確保其他 OT 關鍵系統持續運作，衝擊降至最低。

### 遠端更新裝置系統：

利用 AMIZcloud 與 QuWAN SD-WAN，遠端集中控制多地 QNAP 設備，執行關機、重啟、更新系統等操作，作為復原前置作業，迅速部署安全修補程式與韌體更新，在第一時間封堵漏洞，防止威脅進一步擴散，並降低人工介入延誤的風險。

### 惡意程式移除：

定期移除惡意程式，立即阻斷感染源，防止對系統與資料造成進一步破壞。





# Recover | 復原

## 導入具備災難復原與資料完整性的備援架構

OT 環境的核心目標是「不中斷的生產」。QNAP 聚焦於災難後快速恢復與資料完整性，確保營運能在最短時間內恢復正常。

### 高可用性備援架構 ( 伺服器與內網 ) :

透過 NAS HA 高可用性 (Active/Passive HA) 與交換器 MC-LAG，在發生故障時，系統可自動由備援設備接手運作，業務系統能自動接手，避免 OT 控制系統中斷。

### 高可用性備援架構 ( 多分點 ) :

QHora 路由器透過 QuWAN 在 OT 環境中建構多節點 WAN 備援，跨站異常時自動切換至其他節點與路徑；內建 Dual-WAN，本地斷線時即時切換，確保遠端與雲端服務不中斷。

### 災難復原能力 :

藉由 Snapshot (快照) 可快速回復系統至正常狀態，縮短復原時間，降低因人為操作或惡意攻擊造成的影響。

### 全方位資料備份復原方案 :

QNAP 全方位備份方案涵蓋 Windows PC / 伺服器、SaaS 雲端資料、虛擬機 (VM) 資料備份，最小化營運資料完全遺失的機率。





# 資安不用一步到位， 但一定要開始。

從設備到權限，全面掌握企業資產與使用行為

從部署到擴充，有效整合資安防護與營運效率

從預防到復原，全面維護營運穩定性





# 深入瞭解

QNAP 協助您從現有設備出發，穩健邁出 IT/OT 資安的第一步。

想了解您的環境適合哪些方案？

想取得導入建議與技術諮詢？

## 請與我們聯絡

### QNAP Systems, Inc.

New Taipei City  
Email: [sales@qnap.com](mailto:sales@qnap.com)  
Tel: +886 2 2641 2000

### QNAP Inc. (USA)

Pomona CA  
Email: [usasales@qnap.com](mailto:usasales@qnap.com)  
Tel: +1-909-595-2782

### QNAP Inc. (Canada)

Markham, Ontario  
Email: [canadasales@qnap.com](mailto:canadasales@qnap.com)  
Tel: +1-905-947-1000

### QNAP GmbH (Germany)

Willich  
Email: [desales@qnap.com](mailto:desales@qnap.com)  
Tel: +49-2154-88428-0

### QNAP SRL (Italy)

Roma  
Email: [eusales@qnap.com](mailto:eusales@qnap.com)  
Tel: +39-(0)687-738456

### QNAP UK Limited

Swindon  
Email: [uksales@qnap.com](mailto:uksales@qnap.com)  
Tel: +44-(0)333-344-2522

### QNAP Japan

Tokyo  
Email: [jpsales@qnap.com](mailto:jpsales@qnap.com)  
Tel: +81-3-5901-9735

### QNAP Korea

Seoul  
Email: [krsales@qnap.com](mailto:krsales@qnap.com)

