# ADRA NDR
# 快篩資安進階防護方案

資深產品經理 Daniel Hsieh

# 目標式勒索軟體

- 套用APT複雜攻擊手法
- 攻擊用供應鏈 RaaS雲服務
- 攻擊速度(爆發)加快，平均2周
- 超過2/3的攻擊針對:

  製造業 (18%), 政府機構 (14%), 教育 (13%), 科技 (10%), 醫療 (9%)

# 客戶災情的背後意義

**當勒索病毒攻擊到NAS**

NAS或備份伺服器處於最內層的網路，這代表為時已晚(準備爆發) 會導致嚴重災情

**NAS需要高速 2.5/10G傳輸速度**

內網服務經過交換器(Switch)需要高速也就是Line Rate。傳統資安方案無法滿足。

**內網擴散的根本問題**

內網處於中空區無人看管、企業中太多舊系統無法更新、太多未知攻擊訊號無法分析

# 為何目標式勒索病毒越來越猖獗?

## 內網擴散
## 為何這麼容易?

### 突破城牆防禦無人看管

1%的受感染電腦，卻成了野火燎原

### 內網架構與效能

以往的資安設備屬於全掃描，一旦掃描效能降低，但內網架構需要高速(Line rate)。

## 很難查到
## 可疑內網擴散?

### 需要龐大資安團隊

內網擴散的隱匿技巧

大數據的log/封包與資安團隊

### 被忽略的擴散攻擊

網路列印傳真伺服器，常駐式虛擬機(VDI/RDP)，供應商上傳伺服器或雲端服務，都是內網!

## 查到蛛絲馬跡
## 卻仍爆災情

### 時間太晚

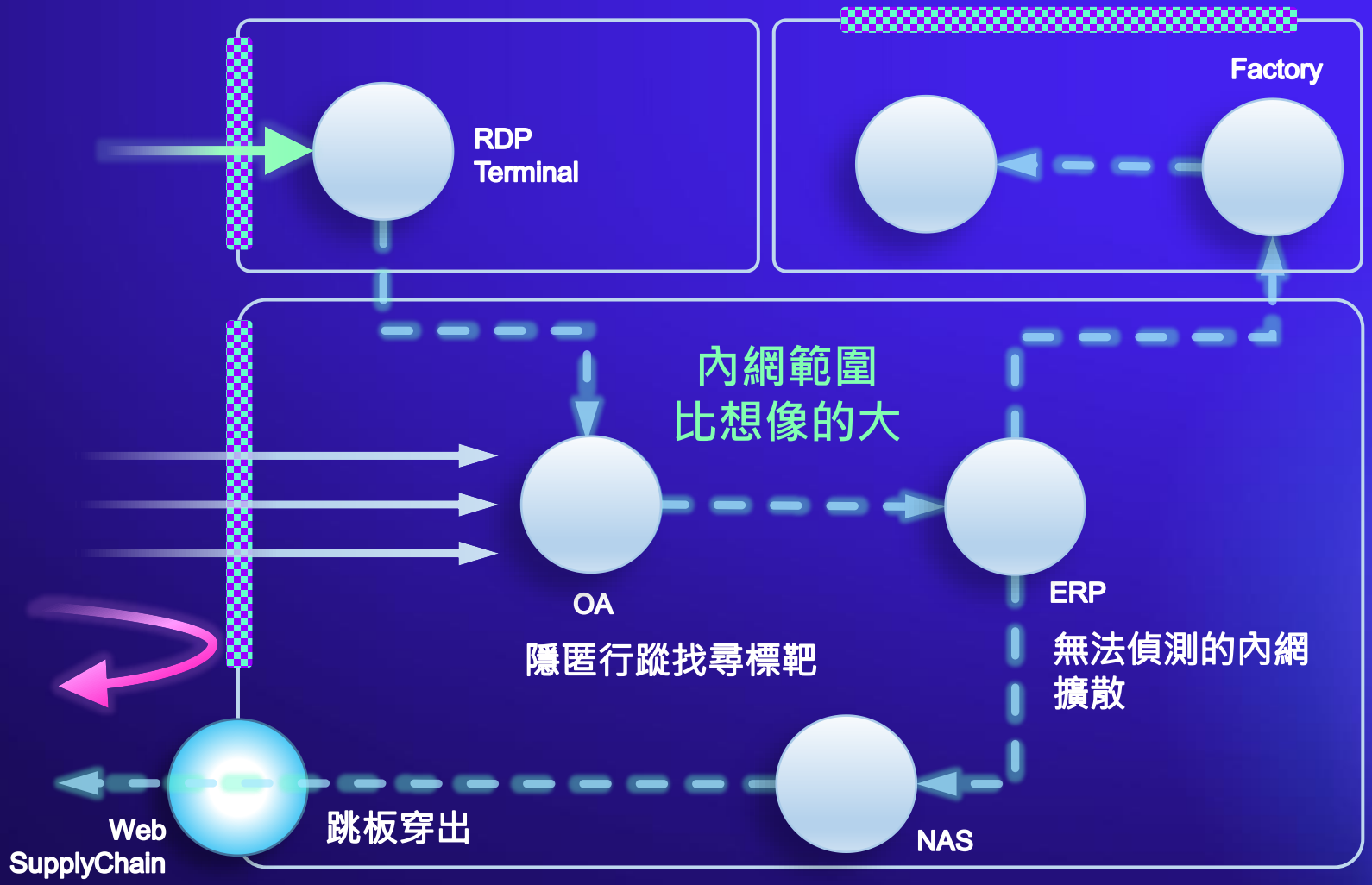
已經接近足以執行勒索的階段

### 感染範圍太大

防火牆或EPP介入

僅阻擋了某幾台電腦的C&C，反而加速勒索病毒的執行

# 內網擴散手法


RDP
Terminal
Factory
內網範圍
比想像的大
OA
隱匿行蹤找尋標靶
ERP
無法偵測的內網
擴散
Web
SupplyChain
跳板穿出
NAS

# ADRA NDR


## 快篩式威脅偵測
Threat Watch

Threat Trap

## 關聯與深度防禦分析
Correlation Analysis

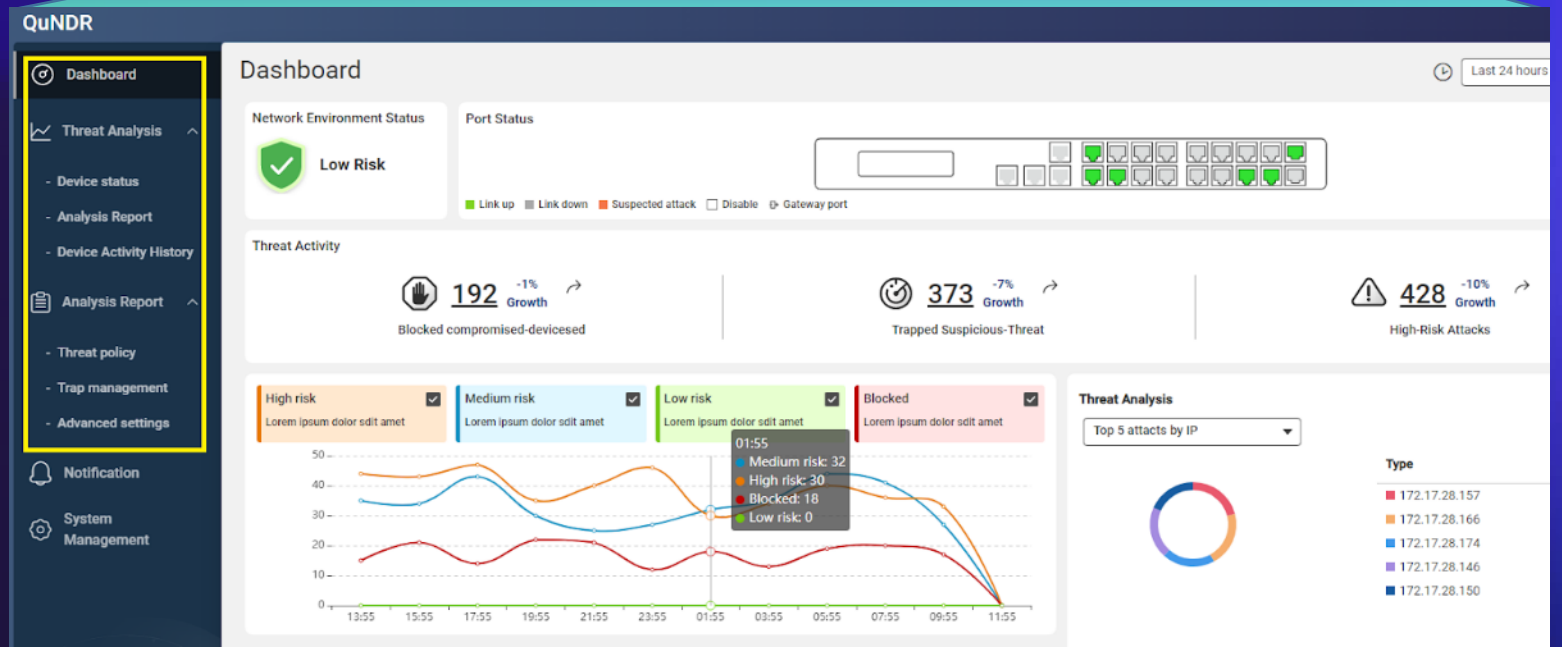
Deep Threat Analysis

## 早期隔離快速回應
Access Switch

Isolate Victims/Zone

Risk Management

# ADRA NDR
# 快篩內網攻擊網路防護設備

# ADRA NDR – 偵測技術

**Threat Watch**

## 威脅監視

檢測ADRA NDR網路交換器特殊封包，察覺內網擴散初期的攻擊探勘行為 (Kill Chain - Discovery)

**Threat Traps**

## 威脅誘捕

模擬多種常用服務(SSH, SAMBA, QNAP服務等)之誘餌系統，察覺攻擊擴散(Kill Chain – Discovery/Lateral movement)

# ADRA NDR – 分析技術

**Deep Threat Analysis**

## 深度威脅檢測

當設備被Watch/Trap偵測捕捉後，立即對網路封包流量的深度威脅檢測分析 (超過2~5萬*個偵測規則)

**Threat Correlation Analysis**

## 自動化關聯分析

找出不同時序和發生的風險事件關聯 (Correlation)，自動提高風險的判斷

# ADRA NDR – 隔離技術

**Isolate the initial infected zone**

## 小區隔離

獨立(無須外部Firewall)運作的隔離規則(Policy)，自動隔離高風險熱點 (受感染電腦)，立即鎖定擴散在最少數量，最小範圍的設備。

**Risk Management**

## 風險維運

IT可以依據風險等級，主動處理。例如，針對營運用的電腦可以暫時放行，清理完畢後再回復到受保護狀態。

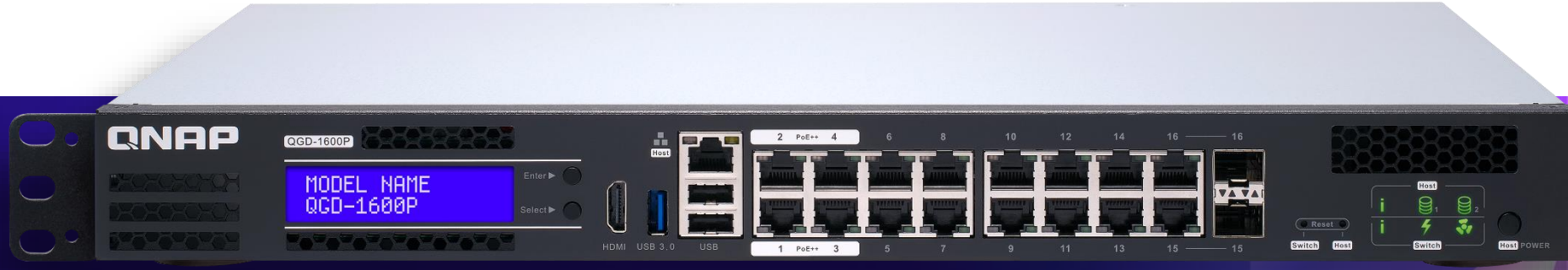
# 關鍵特色

- **不傷網路架構**，快速安裝
- **保持高效**，不因偵測而拉低傳輸效能
  可建置於伺服器或VM Farm之前
- **透明掃描**，攻擊者無法察覺
- **快篩偵測**，佈署位置與偵測技術
- **即刻阻止**，可以隔離電腦併即刻還原

# QNAP ADRA NDR
# 免費借測 - 線上登記

## 立即掃描 QRcode 完成登記

完成登記後將由專人與您聯繫後續借測事宜



# QNAP針對目標式勒索軟體的全面對策

QNAP

高階儲存
風險控管

資料防護
快速還原

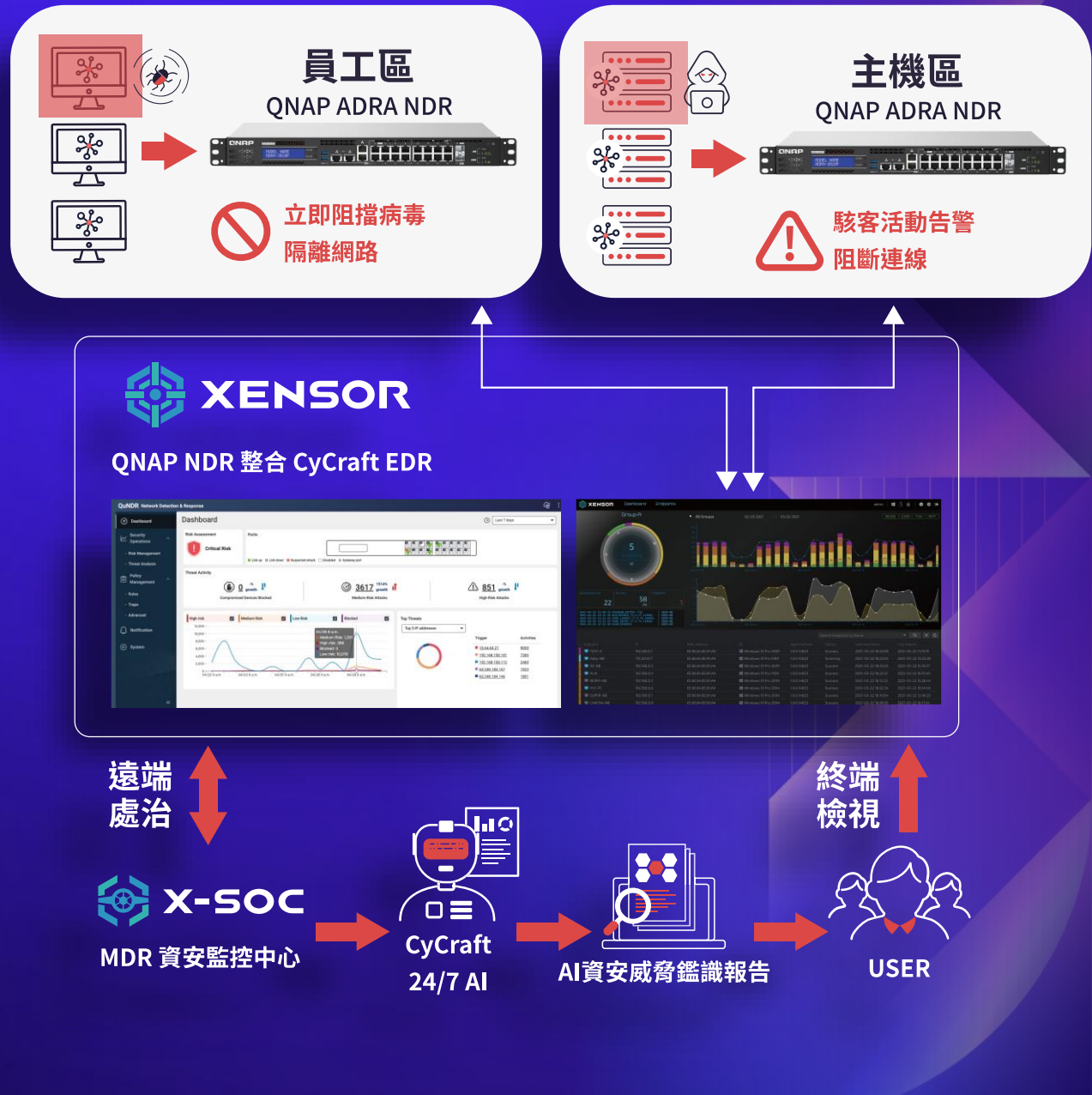
內網快篩
資安防護

**PSIRT**　解決數百萬個客戶遭遇目標式攻擊的內網防禦、資料安全的完整方案

# 威聯通與奧義智慧攜手合作

# AI XDR
# 企業內網安全解決方案

1. **支援網路端威脅偵測及過濾**
   - 威脅情資快篩、封包過濾及內網行為分析。
   - 自動更新全球威脅情資。
2. **支援端點鑑識調查**
   - 派送鑑識掃描任務，遠端進行鑑識調查。
   - AI自動產製威脅通報。
3. **MDR遠端緊急應變與威脅清除計畫**
   - 終端惡意程式即時阻擋、隔離與清理。
   - 支援內網擴散主機網路隔離功能。



QNAP

# 是您最好的選擇！