

QNAP

ADRA-NDR

主動式資安快篩機制

有效達成內網威脅偵測與分析



什麼是ADRA NDR?
它是台Firewall?
Switch? 還是其他的?

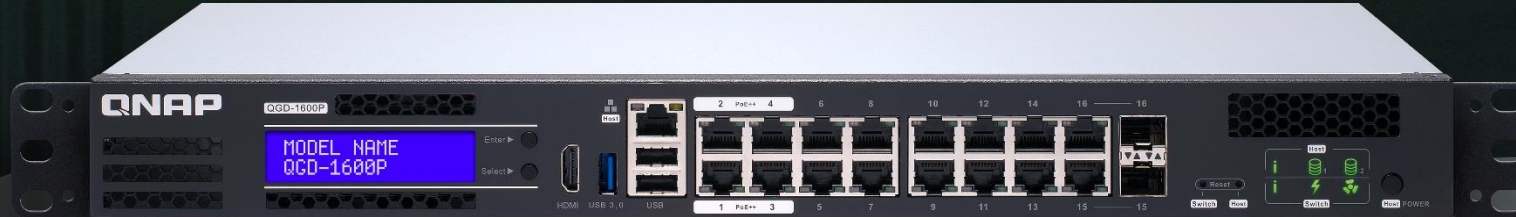


ADRA
NDR

ADRA NDR

內建資安快篩功能的智能交換機

ADRA NDR



威脅自動偵測

Threat Watch
Threat Trap

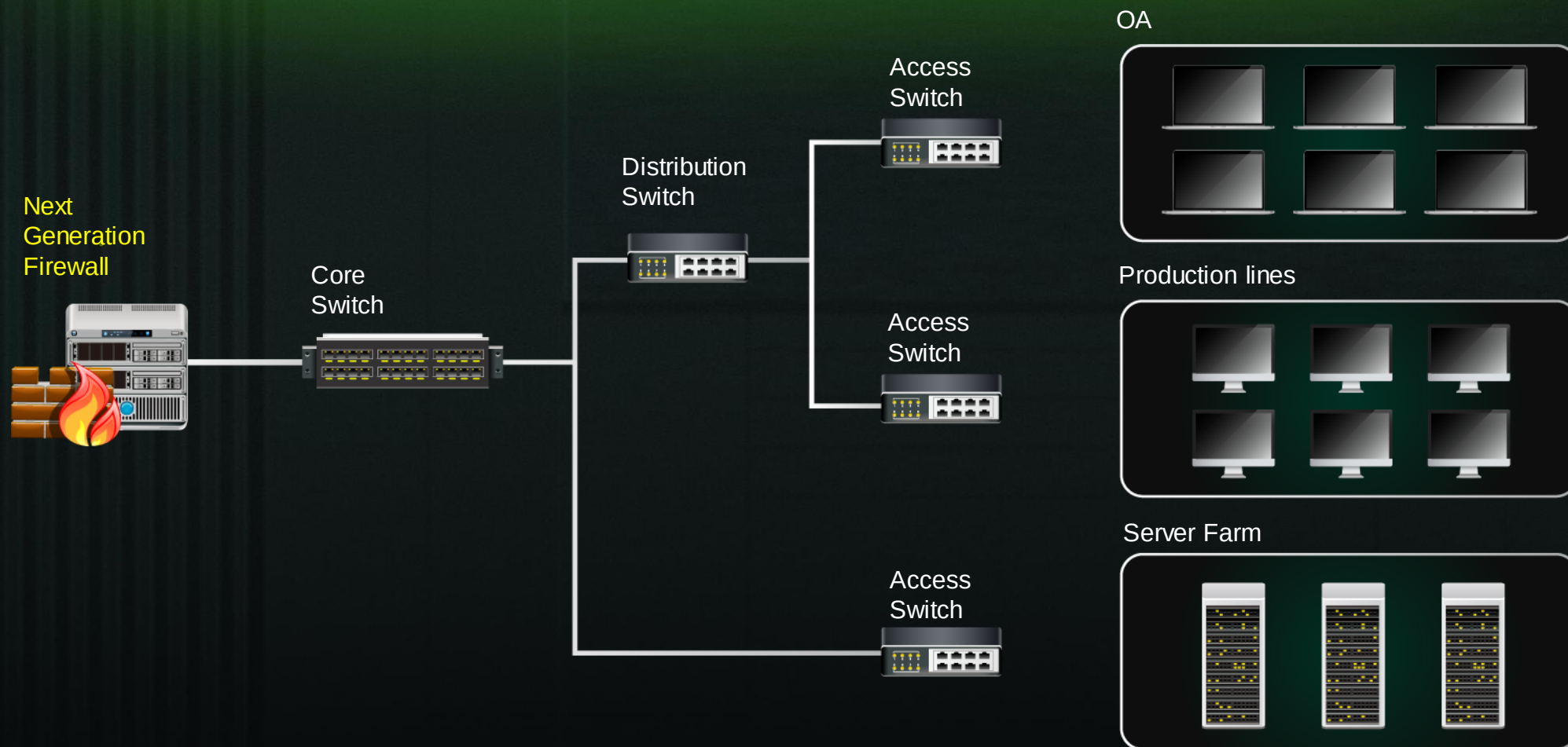
及時威脅分析

Correlation Analysis
Deep Threat Analysis

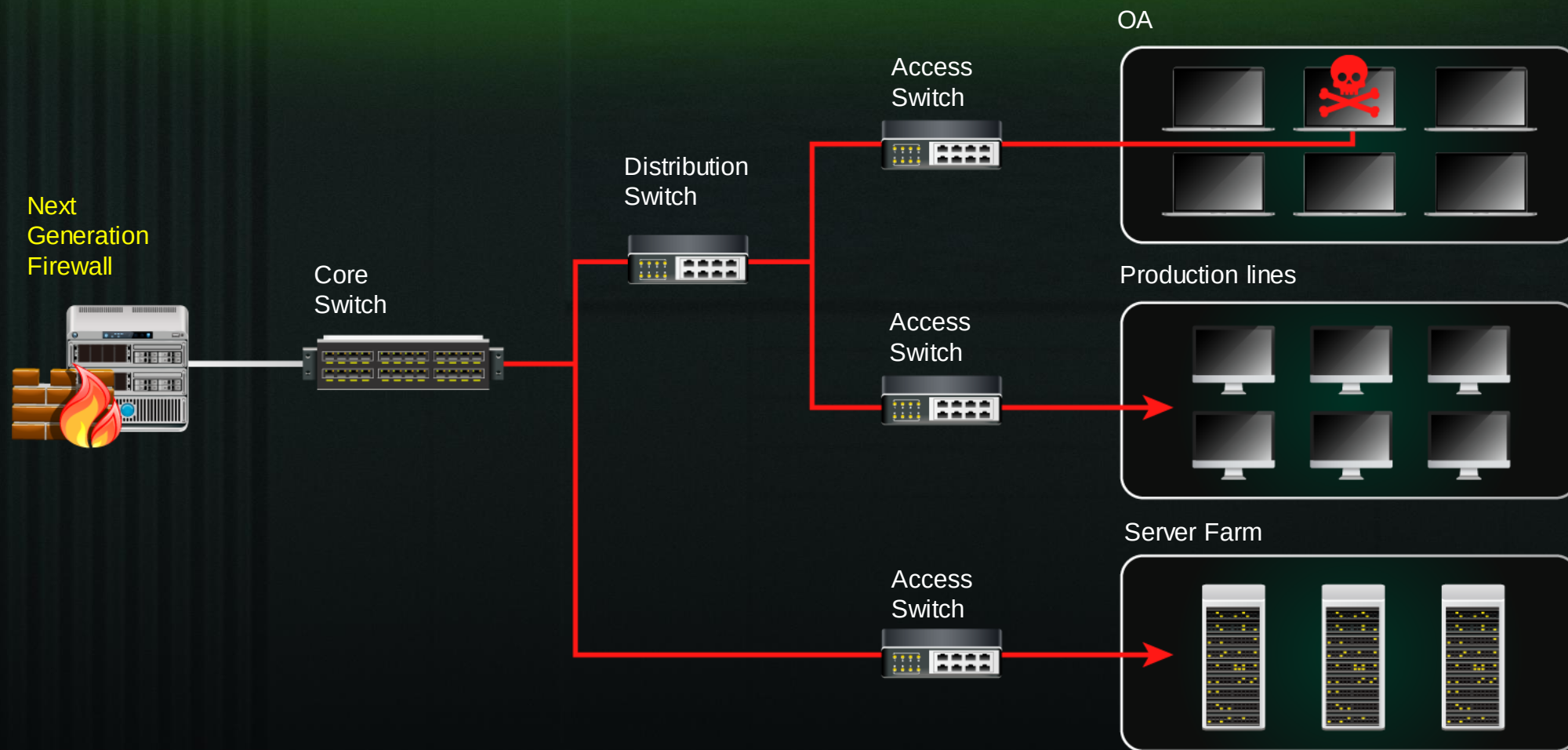
主動隔離威脅
來源

Access Switch
Isolate Victims/Zone
Risk Management

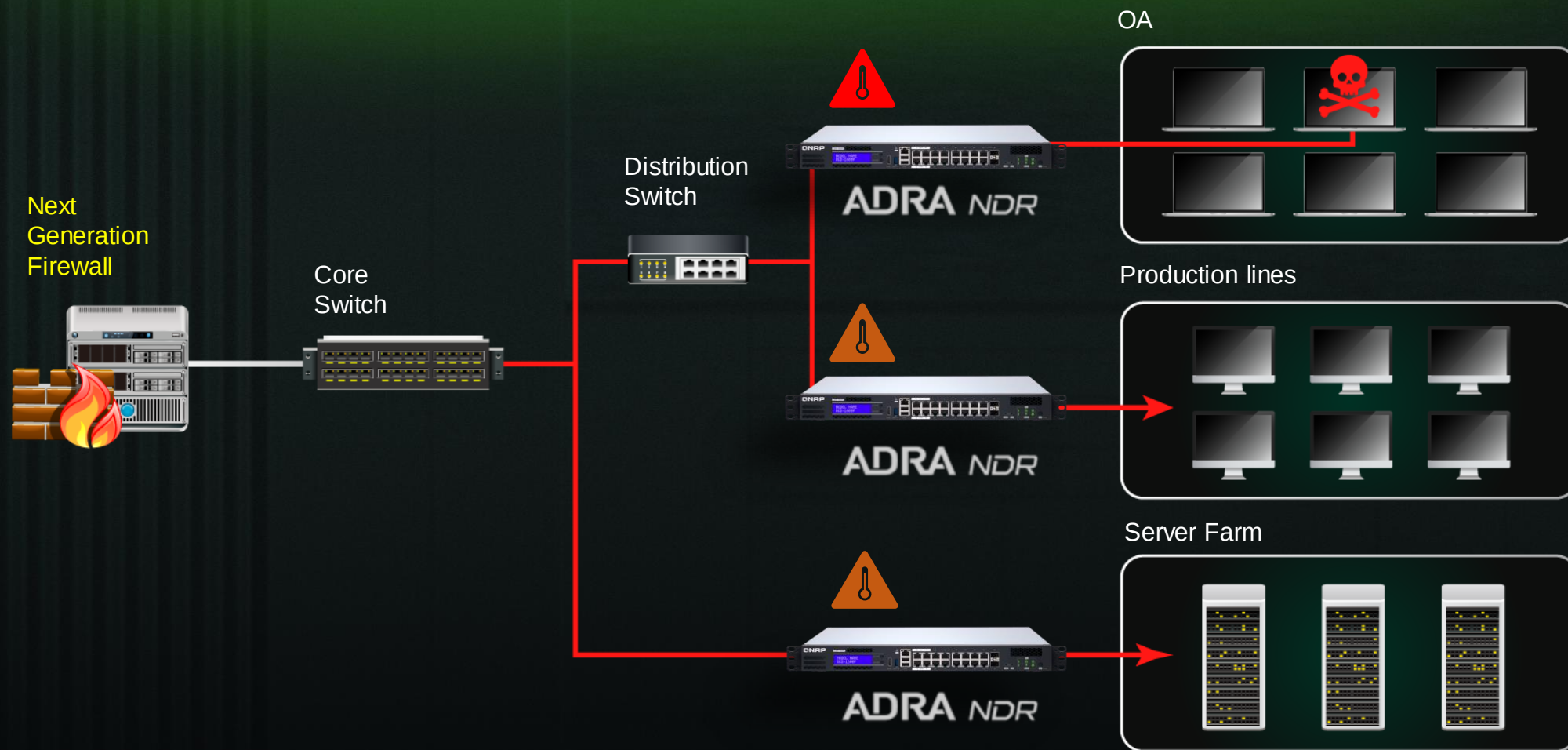
傳統的中小企業網路架構



傳統架構對內網威脅抵抗力較薄弱



ADRA NDR可彌補這一塊



目標市場及使用者的痛點



ADRA
NDR



目標市場

很多中小企業因為資安布建的不充足，
常常變成主要的攻擊目標

Enterprise

5.000+ devices

Mid Enterprise

1.000 – 5.000 devices

Medium business

250 – 1.000 devices

Small Business

10 – 250 devices

Consumer

為什麼中小企業需要ADRA NDR?

缺乏資源
預算考量，
資安分析/管理人員不足

傳統NAS使用者
實體儲存設備容易成為目標

很多舊款設備
舊設備存在著很多漏洞

容易跟威脅妥協
攻擊者容易得到贖金

產品型號

建議edge數量	10– 50 devices	30 – 80 devices	60 – 110 devices
Global Model name (multi-OS)	QGD-1600P	QGD-1602P-C3558-8G	QGD-1602P-C3758-16G
License (ADRA NDR)	Global: 1 year / 3 years	Global: 1 year / 3 years	Global: 1 year / 3 years
CPU/RAM	Intel Celeron 4C / 4GB	Intel Atom 4C / 8GB	Intel Atom 8C / 16G
Disk(manual added)	2 x 2.5" SATA Slot	2 x M.2 NVMe 2280 or 2 x 2.5" SATA slot	2 x M.2 NVMe 2280 or 2 x 2.5" SATA slot
Switch	14 x 1GbE RJ45 + 2 x Combo(RJ45&SFP)1GbE	8 x 2.5GbE RJ45 8 x 1GbE RJ45 2 x 10GbE SFP+	8 x 2.5GbE RJ45 8 x 1GbE RJ45 2 x 10GbE SFP+
PoE	Yes	Yes	Yes
Management Port	1 x 1GbE RJ45	2 x 5GbE 2 x 1GbE	2 x 5GbE 2 x 1GbE

不同情境下建議的終端設備數量

情境	一般網頁瀏覽	一般網頁瀏覽 (75%) + 高度網路 使用設備(25%)	高度網路設備	各機種建議的 Trap啟用數量
QGD-1600P	50	30	10	1-2
QGD-1602P-C3558-8G	80	60	30	3-6
QGD-1602P-C3758-8G	110	90	60	6-8

Note: 如有在ADRA上啟用Trap功能，請將每一台Trap都視為一個高網路流量使用設備

網路威脅 101



ADRA
NDR



網路攻擊時間軸

第一台被攻擊
拿下的設備

沒有適合的
內網防護網

整個內網被攻陷

1

Discover your intranet

Lateral movement for exploit

All

Day 0

Day 7 ~ 30

Day 30 ~ 180

Incident

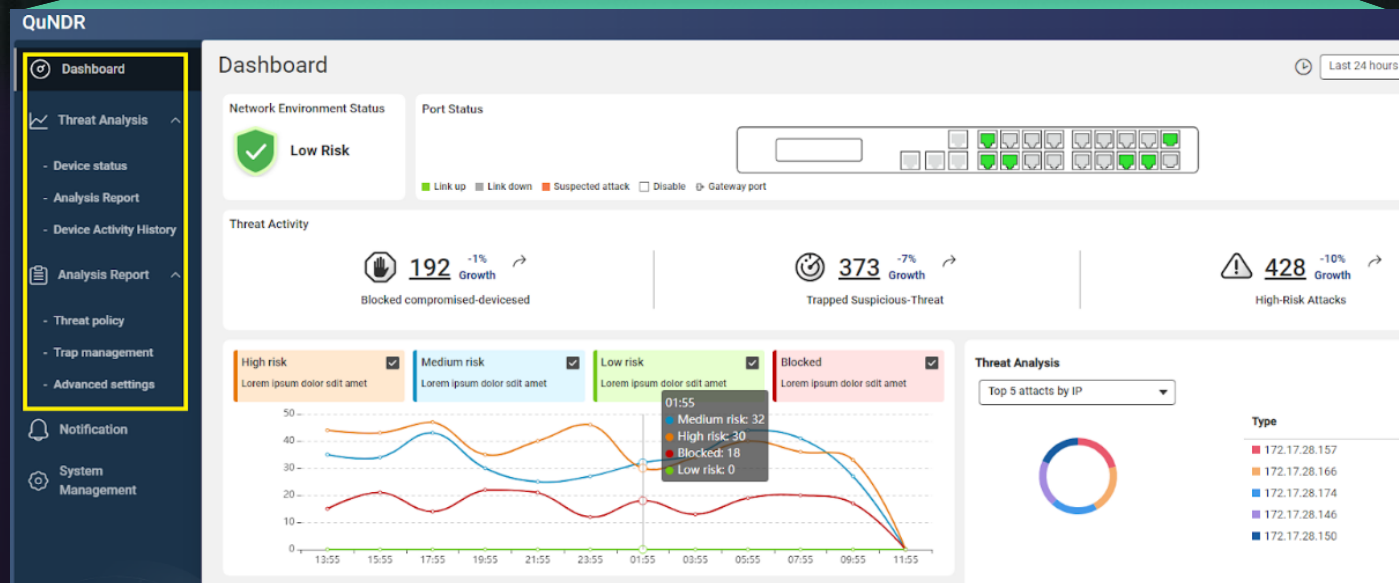
主要產品功能介紹



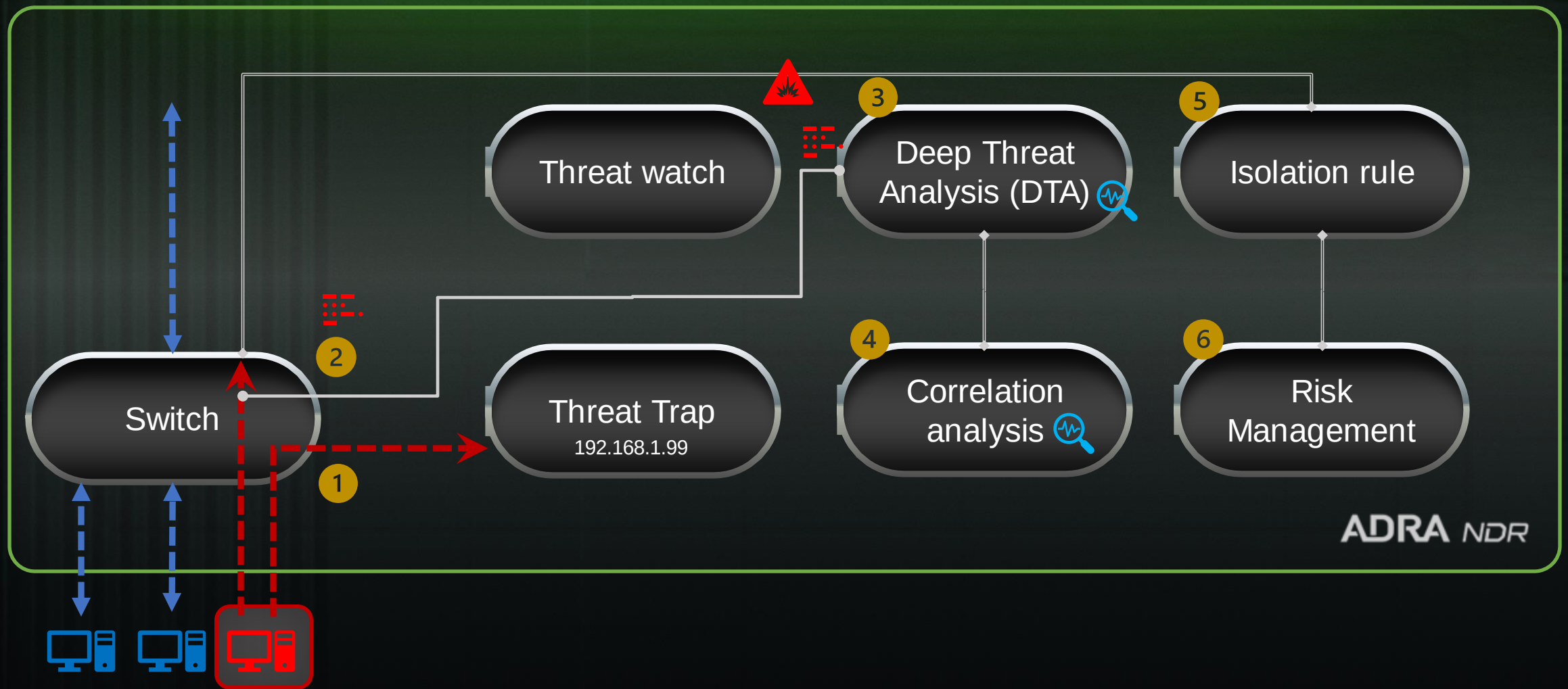
ADRA NDR



創新思考: Threat Trap (主動出擊)



偵測及分析流程



如何將QGD升級為ADRA



ADRA
NDR



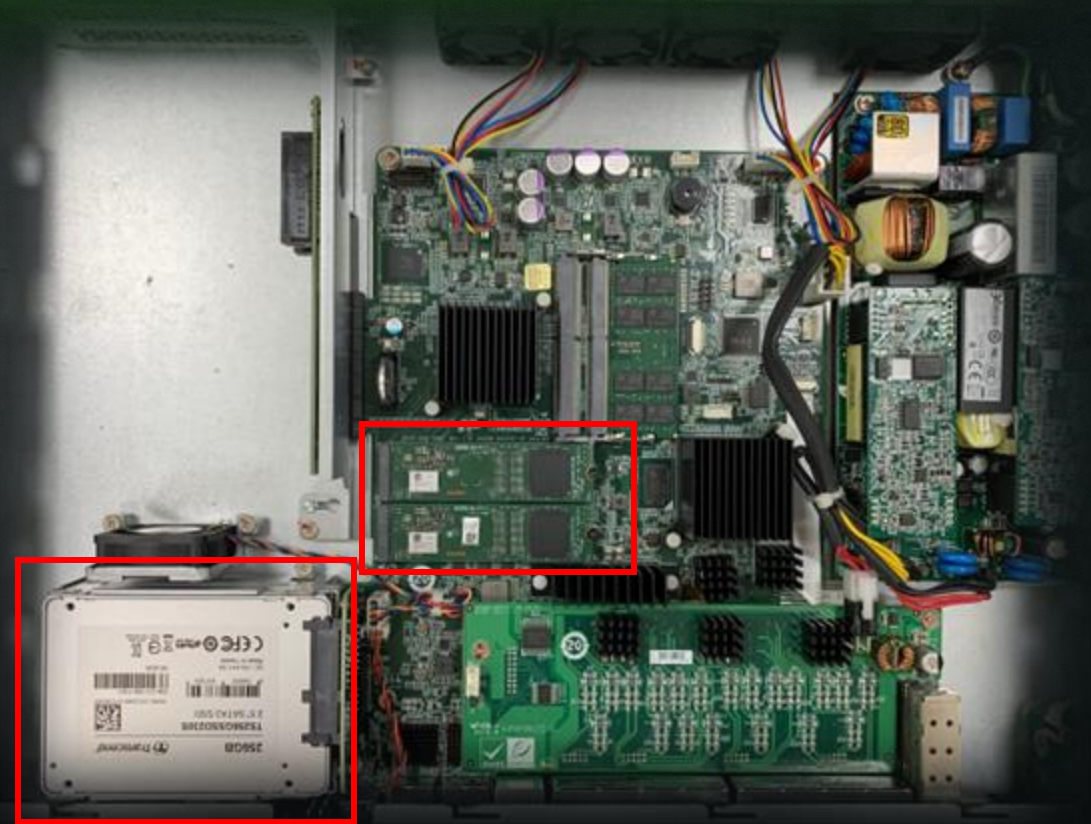
安裝 M.2及2.5" SSD

QGD-1600P系列

- Installed w/ 2.5" SSD (1-2 pcs)
- Minimum requirement is 256GB 2.5" SSD

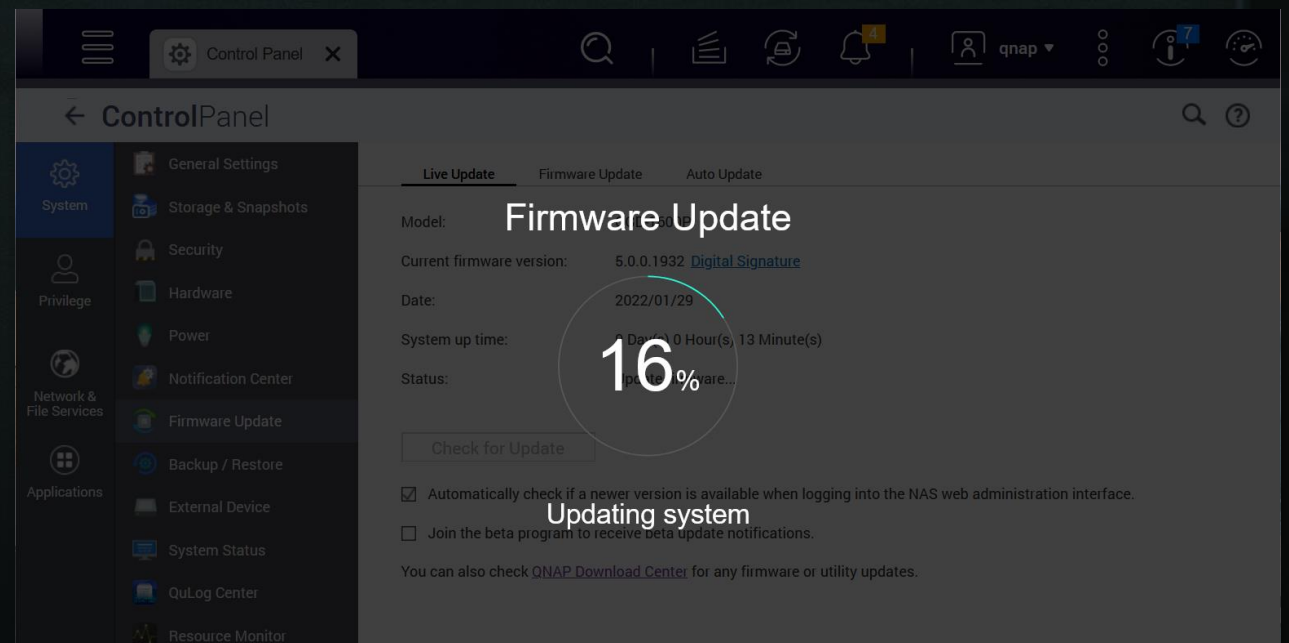
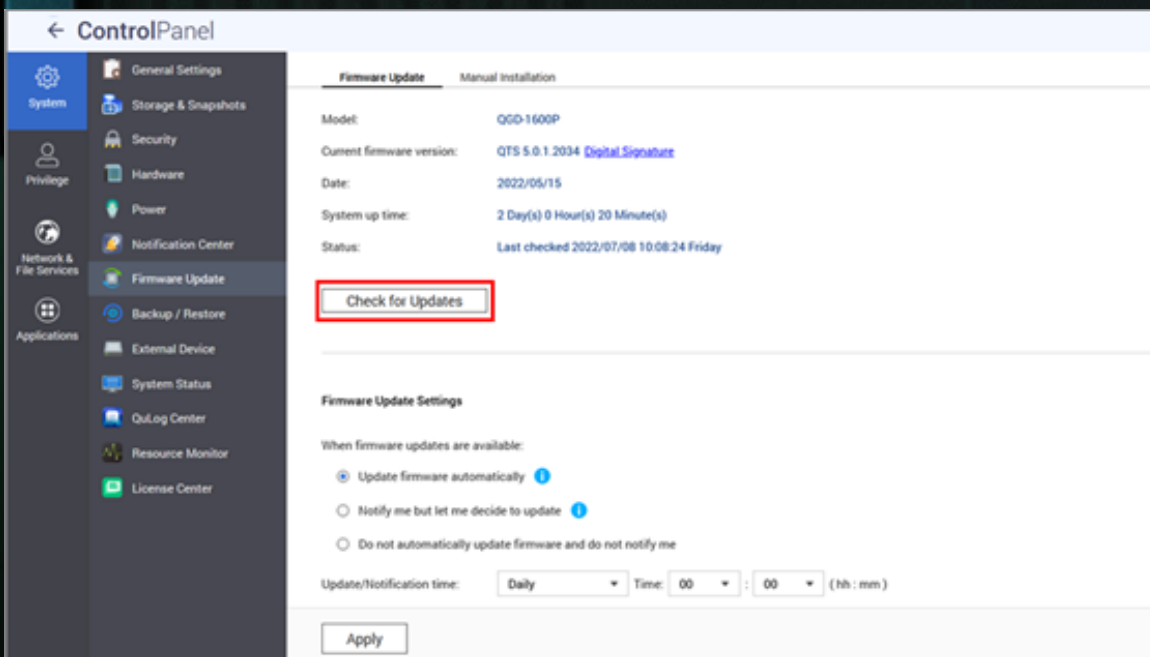
QGD-1602P 系列

- Installed w/ M.2 SSD (1-2 pcs) and 2.5" SSD(1-2 pcs)
- Minimum requirements are 128GB M.2 SSD and 256GB 2.5" SSD



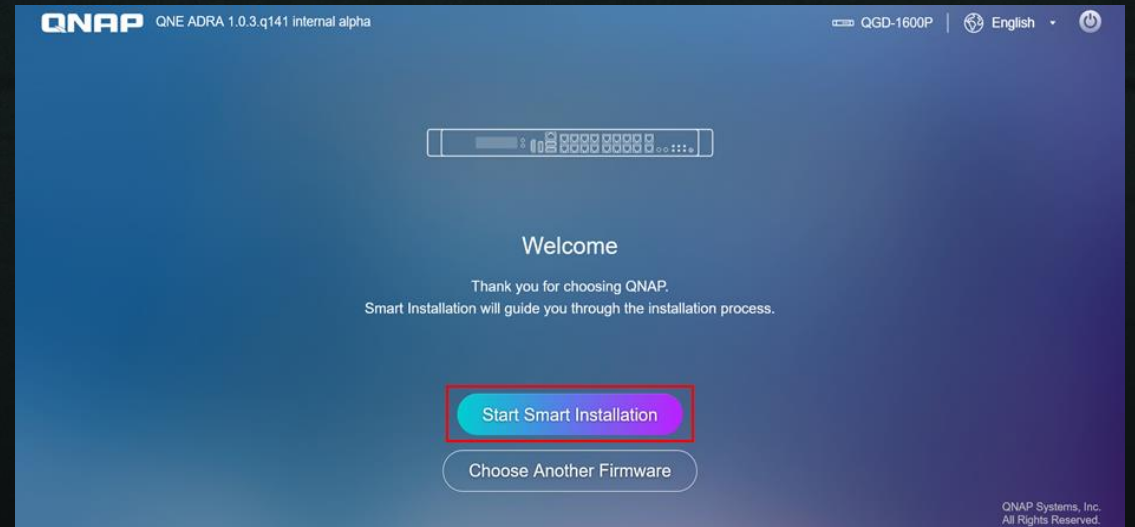
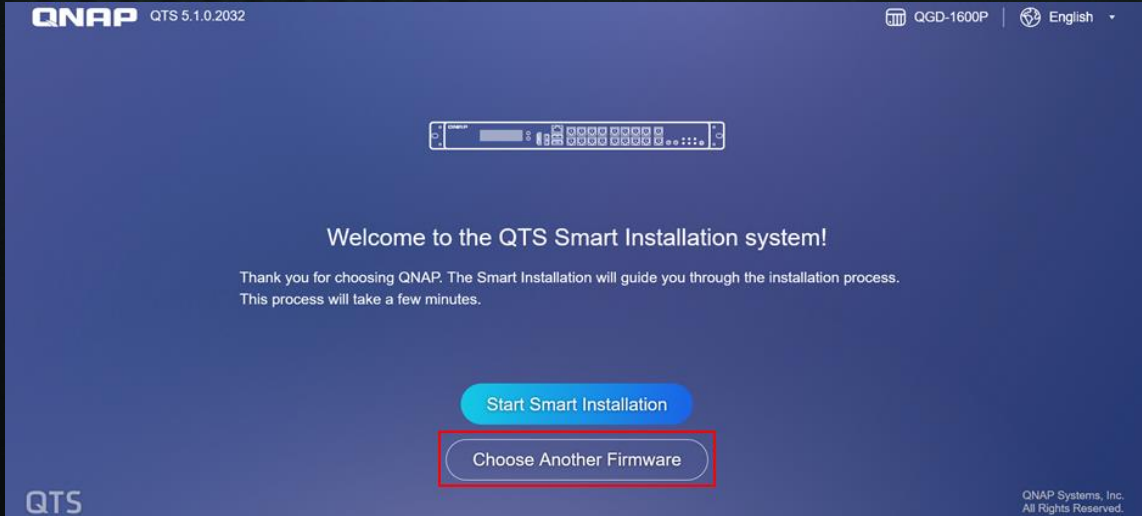
將 QTS 升級到雙系統版本

- 登入QGD
- 到 FW Live update 頁面
- 確定 QTS 更新到最新版



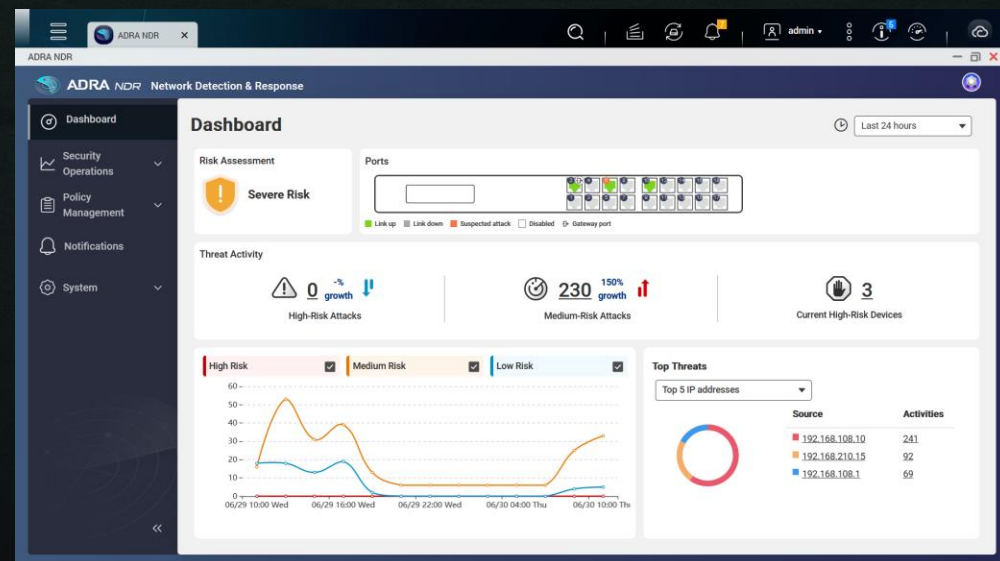
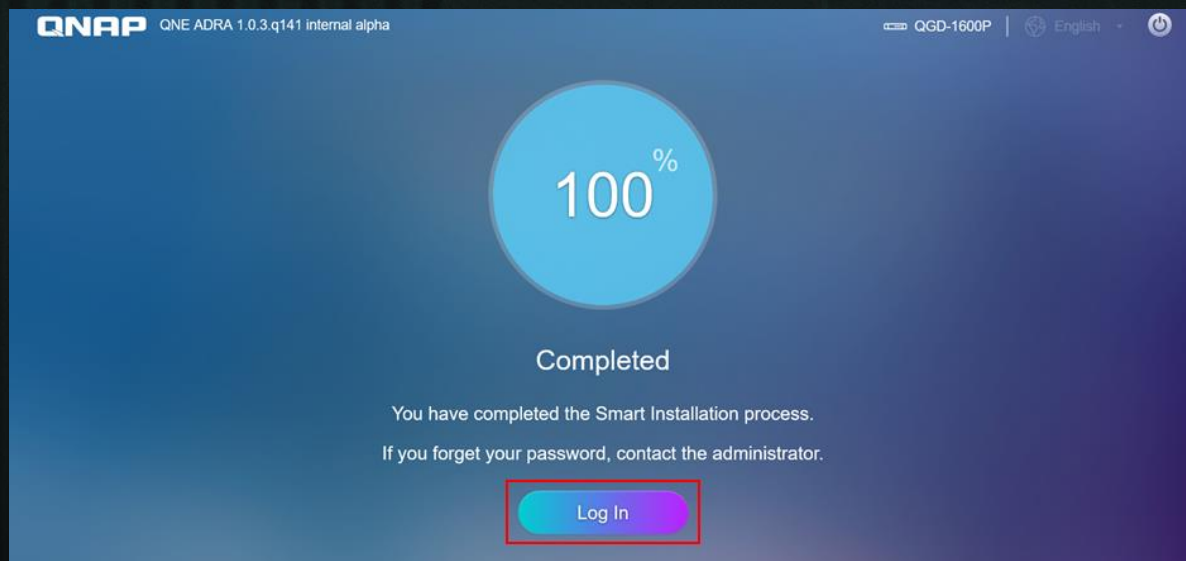
切換到 QNE ADRA 韌體

- 將 QGD 重新reset
- 重開機完成後，QGD 會跳出是否要選擇切換韌體的畫面
- 預設機器還是選擇 QTS for QGD, 如果要切換成ADRA請點選 “Choose Another Firmware”



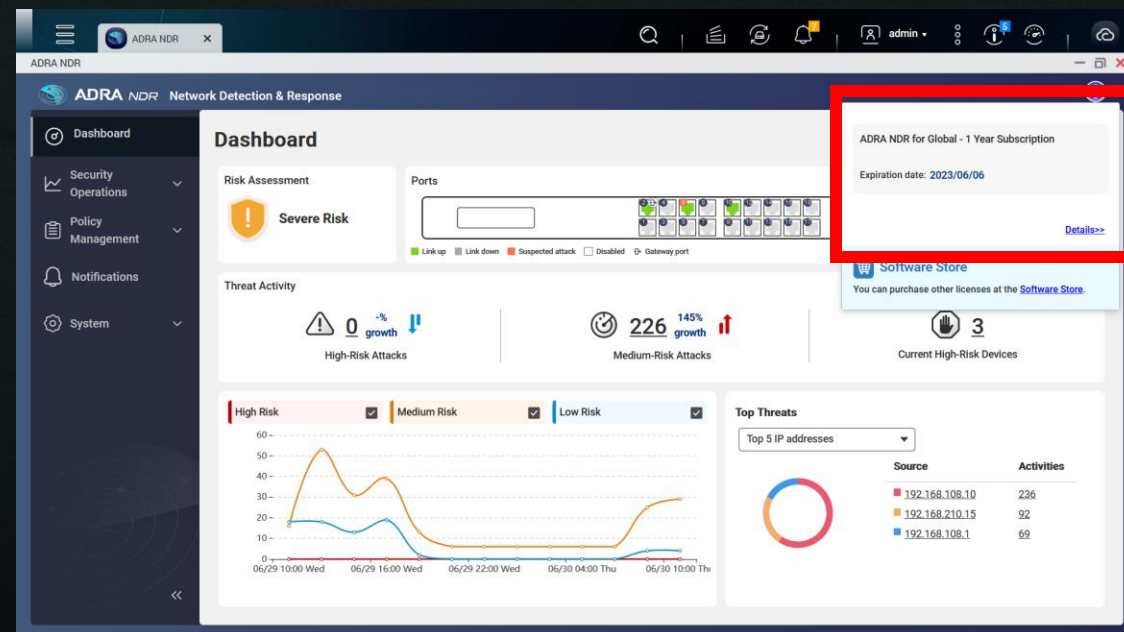
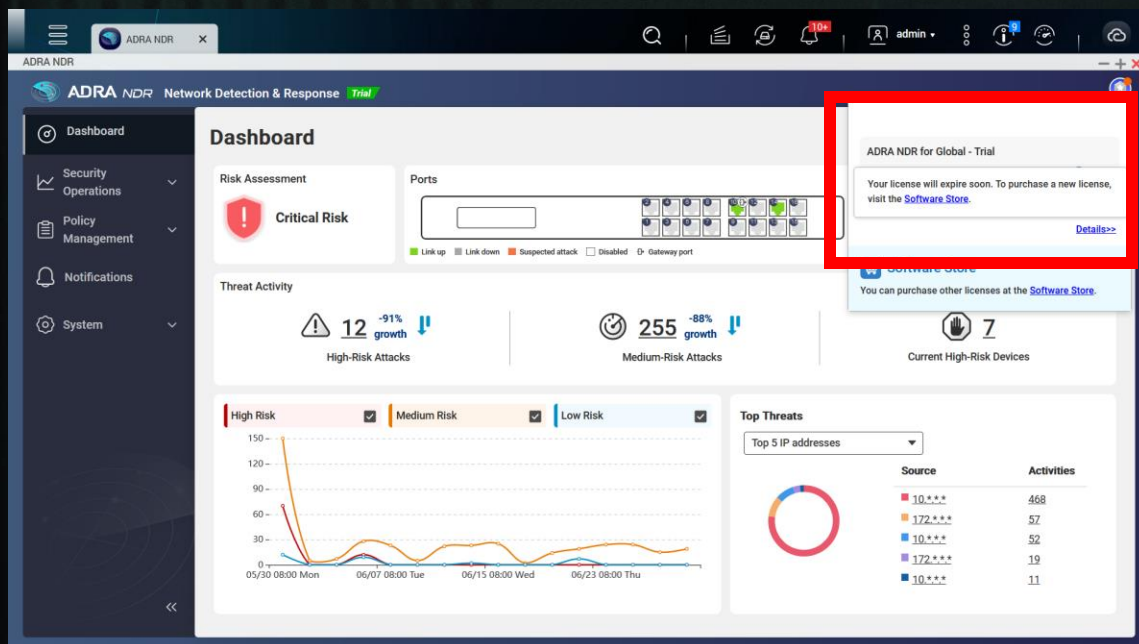
完成 FW 安裝流程進入 ADRA NDR

- 跑完安裝流程之後，就會跳出login畫面
- 登入後就可以開啟ADRA NDR功能



購買註冊License

ADRA NDR預設有30天試用，需購買啟用標準版License才能獲得完整ADRA NDR功能



試用跟標準版 License的差別



ADRA NDR



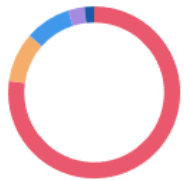
ADRA

只會顯示部分資訊給Trial License使用者

資料如Hostname, Source IP, Source MAC, Destination IP會被隱藏起來。

Top Threats

Top 5 IP addresses



Source

Activities

10.***	469
172.***	57
10.***	52
172.***	19
10.***	11

Risk Management

Total devices:58

Take Action

Delete

☐	Added ↓	Updated ↑	Source IP ↑	Source MAC ↑	Hostname	Risk	Status
☐	2022/06/28 11:01:29	2022/06/28 11:17:17	10.***			Medium	Normal Scan

Threat Analysis

Total entries:40



Specify keywords



No grouping

Time ↓	Trigger	Risk ↓	Hostname ↓	Source IP ↓	Source MAC ↓	Destination IP ↓	Details
2022/06/30 15:22:48	Security operation			10.***	-	-	10.*** placed under Normal Scan by the system.

有限的功能

部分功能如Risk Management, Threat Analysis and Rules是無法啟用的

Risk Management										
Total devices:58		Take Action		Delete		Specify keywords				
☐	Added ↓	Updated ↑	Source IP ↑	Source MAC ↑	Hostname	Risk	Status	Rule	Comment	Records
☐	2022/06/28 11:01:29	2022/06/28 11:17:17	10.*.*			Medium	Normal Scan			 
☐	2022/06/28 03:00:05	2022/06/28 03:15:07	8.*.*			Medium	Normal Scan	Default Policy		 

Threat Analysis

Last 24 hours

Total entries:40

i

Specify keywords

No grouping

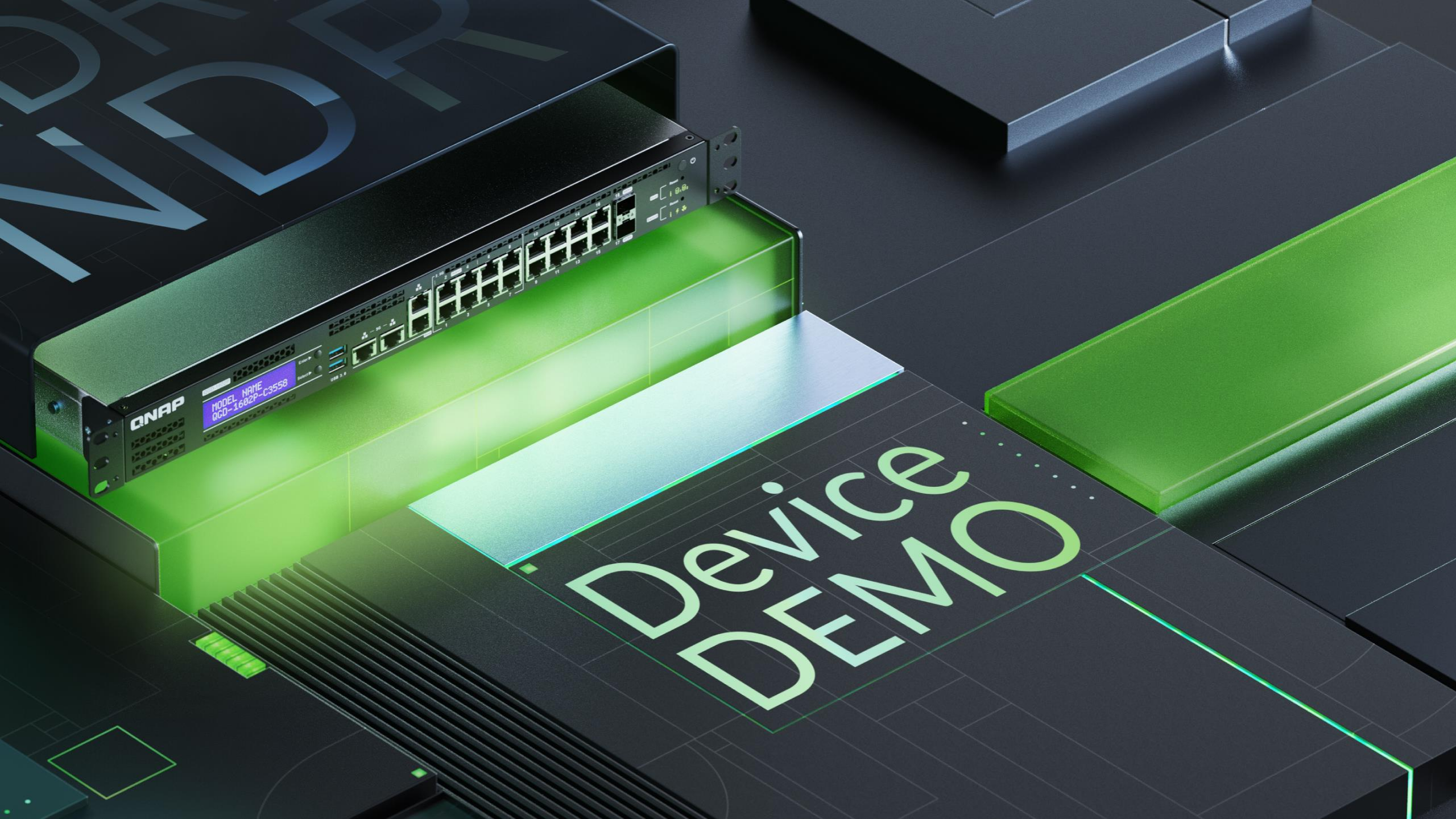
Time ↓	Trigger	Risk ↓	Hostname ↓	Source IP ↓	Source MAC ↓	Destination IP ↓	Details	Exclude
2022/06/30 15:22:48	Security operation			10.*.*	-	-	10.*.* placed under Normal Scan by the system.	

Rules

If all rules are disabled, a system-wide Risk Inform policy is adopted by default, which means you will only be informed of risk events in Analysis Report.

+ Add Rule

Priority	Name	Source	Protection Policy	On/Off	Action
⋮	test	All	Strict Protection Auto-quarantine all potential attacks.	☐	



The QNAP logo is displayed in the top left corner in a white, bold, sans-serif font. The background of the entire image is a dark, futuristic digital landscape with glowing green lines and various electronic components like circuit boards and connectors. A large, semi-transparent 'ADRA NDR' watermark is visible in the center-right area.

QNAP

QNAP Product

is your best choice

© 2022 著作權為威聯通科技股份有限公司所有。威聯通科技並保留所有權利。

威聯通科技股份有限公司所使用或註冊之商標或標章。檔案中所提及之產品及公司名稱可能為其他公司所有之商標。