

ADRA NDR 軟體功能

- 風險等級
- 風險控管
- 威脅分析
- 自訂風險管控規則
- 網路誘捕器
- 例外設定&自訂監控網路埠
- 網路行為通知
- 外部儲存記錄檔

硬體規格及建議監控數量

HW models (multi-OS)	QGD-1600P	QGD-1602P-C3558-8G	QGD-1602P-C3758-16G
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
建議終端設備監控數量	10 – 50台	30 – 80 台	60 – 110 台

服務授權

SKU	LS-ADRANDR-GL-1Y	LS-ADRANDR-GL-3Y
使用期間	1 年	3 年



ADRA NDR

主動快篩 & 內網威脅偵測的資安設備

ADRA NDR 是基於QGD-1600P /QGD-1602P 智能交換機開發出來的內網快篩設備，讓企業網路在交換機端，也有一台可進行資安快篩功能的設備，並在網路威脅前期就進行隔離，進而做到風險控管。

ADRA NDR的三大核心功能

1 主動威脅偵測

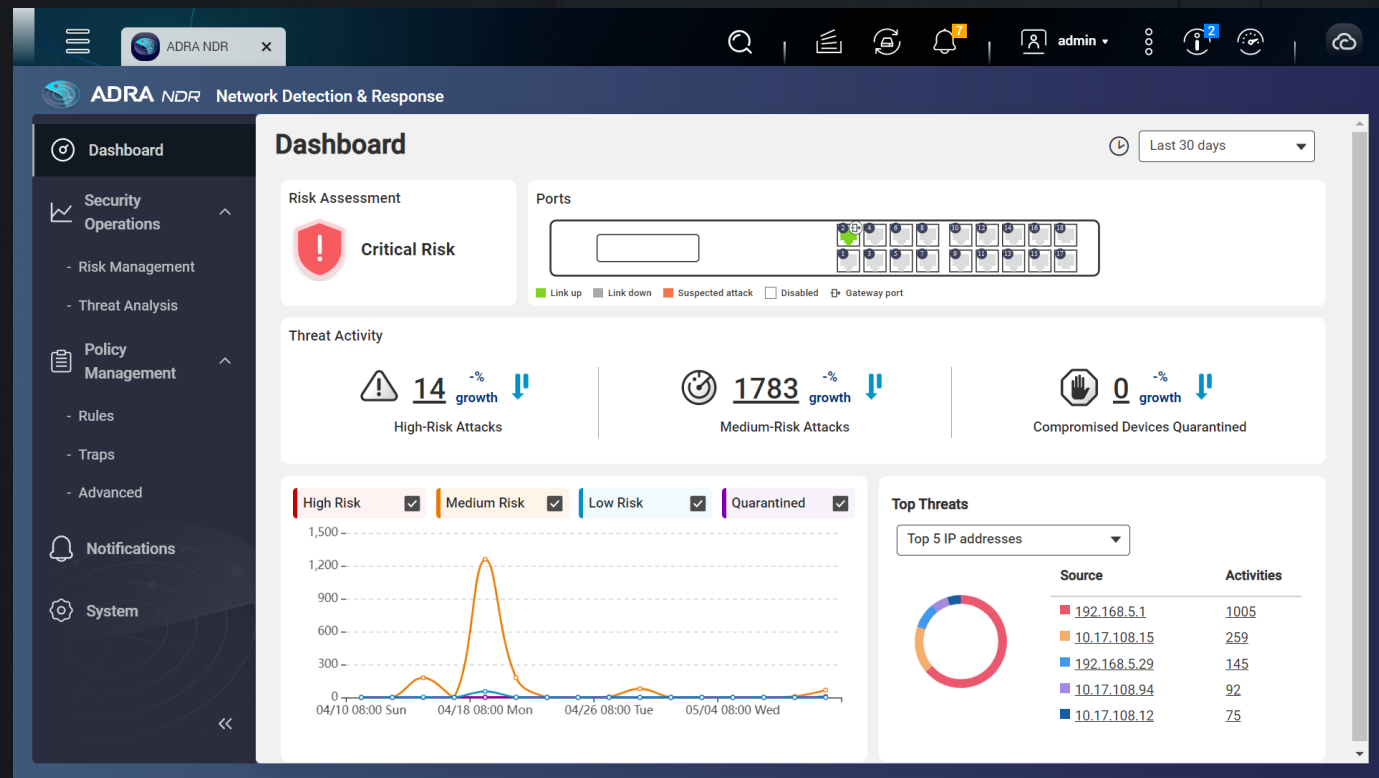
主動出擊，著重在網路威脅前期，越早發現可疑行為可以更早進行管控。

2 及時行為分析

透過行為交叉比對，加上核對網路行為，確保能及時發現網路威脅。

3 對威脅進行隔離

將已被感染的來源進行網路隔離，避免內網其他設備曝露在再被感染的風險之下。



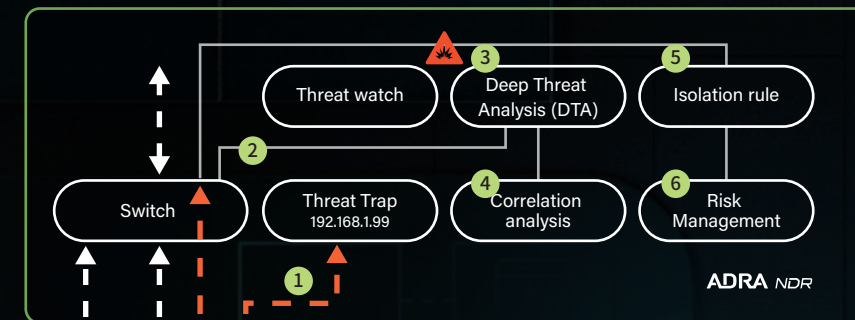
及時狀況顯示

圖型化且及時性的介面顯示，讓管理者清楚知道內網的狀態，及可能造成威脅的目標在那邊。



威脅誘補

傳統網路架構都需實體架設蜜糖罐(Honeypot)來進行誘補，ADRA NDR可直接增加多台誘補器增加誘補成功率。



維持高效傳輸

特別設計的封包檢查機制，讓ADRA NDR在進行網路威脅快篩時，仍保有交換機的高速傳輸效能。