

# N-Partner

Company Profile & Sales Kit

企業產品手冊與銷售指南



Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting



# Content

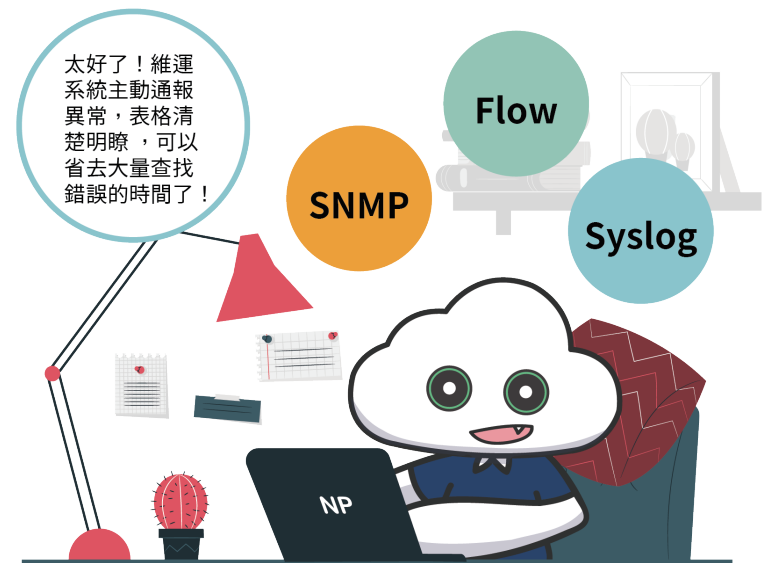
傳統管理 VS 智慧維運 -----	02
N-Partner 產品總覽 -----	04
N-Partner 核心技術說明 -----	06
執行數位足跡分析輔助神器 N-Probe -----	10
網路延遲與網頁服務瀏覽效能監測 -----	11
Dashboard 建構您隨選的戰情中心 -----	12
N-Partner 的防駭祕笈 -----	14
IP 軌跡動態關聯圖 -----	18
市場上最佳 CP 值的日誌收集系統 -----	20
預測硬體效能與網路服務品質的未來走勢 ---	22

## 您是多工多勞 IT 人嗎？



IT 維運人員接收到網路異常通報時，必須逐一登入諸多設備觀察狀態、查找日誌紀錄，靠著經驗與時間賽跑著，試圖找出障礙根源。如果沒有良好的維運工具單憑人力，**往往事倍功半...**

## 試試高效率的智慧管理吧！



新一代內建人工智慧的 IT 維運系統  
無論日常維運或網路異常都能高效解決

## N-Partner 產品總覽



納管全域設備以及系統，收集SNMP、Flow、Syslog三種維運數據進行關聯比對分析。內建智慧學習技術能根據所在環境條件建立動態基準值，**主動發覺異常並即時發送告警或是聯防協作抑制災害擴大**，讓IT維運變得更簡單。是網管、流量分析、日誌三合一系統。



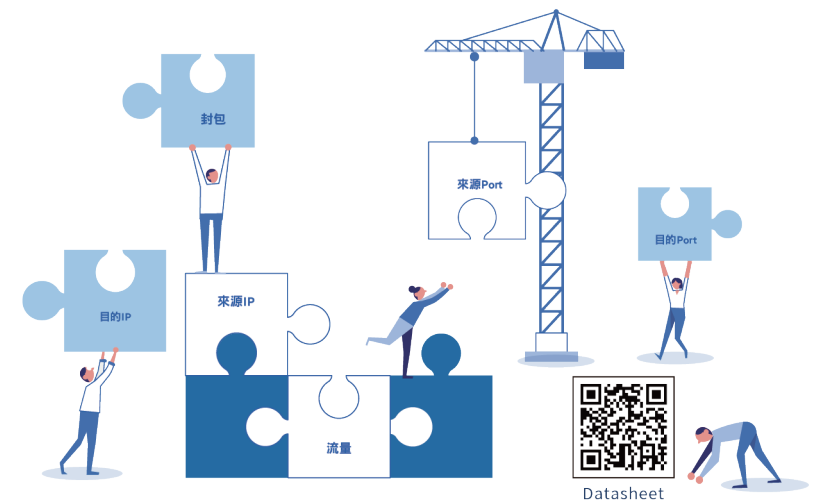
N-Reporter的擴容版本，運用雲架構與NoSQL儲存技術提供高達百萬EPS以上的資料處理效能。**支援多租戶設定，可根據權限制分不同管理範圍**，適合大型企業、金融、政府與教育網建置集中化的維運中心以及電信服務商作為SaaS服務之用。



接收Mirror流量轉換成1:1 NetFlow資料後送到外部流量分析系統，支援1G、10G、40G介面，**解決交換器/路由器不吐Flow或啟動Flow輸出時的效能問題**。可從Mirror流量裡擷取DNS相關訊息轉換成DNS日誌。可作為Web服務品質量測工具。



獨創的智慧維運助手工具，運用人工智慧技術對各種數據進行學習，最大特點在於**能夠根據每個不同的網路環境調整分析的策略與重點、記憶使用者的操作喜好**，透過自動推播將值得注意的網路與資安訊息告知管理者，做到更進階的維運協助。

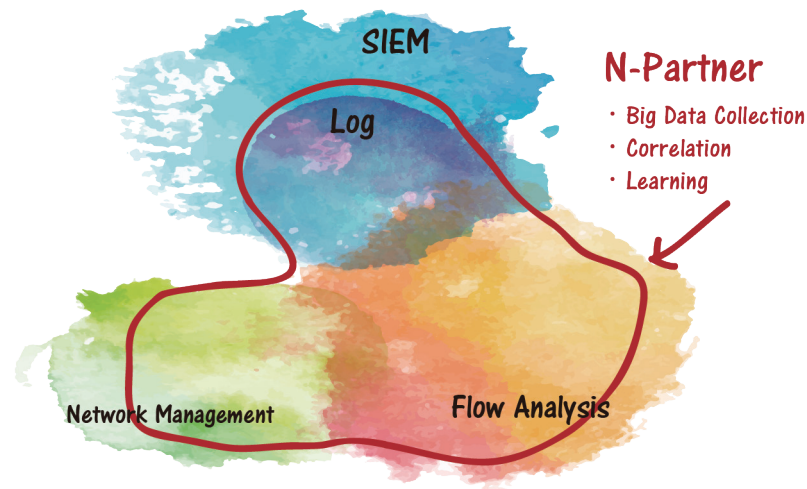


## 取代傳統 IT 管理模式，N-Partner 的核心技術說明

提供您單一平台即整合「網管、流量、日誌」的智慧維運方案

以往為了日常維運需求，須花費高額預算分別採購網管、流量分析與日誌工具，然而工具間各司其職缺乏整合讓維運工作效率無法隨著投資而提高。

N-Partner 智慧 IT 維運平台：N-Reporter / N-Cloud，整合了 SNMP、Flow 與 Syslog 三種主流網管和資安事件分析技術，可進行三種異質資料間的關聯分析，**只須建立一個平台即可完整採集單位內全域的設備資訊，即時掌握所有狀況，確保 IT 系統運作品質，並且大幅降低 IT 人員的工作負荷與時間壓力。**



# N-PARTNER

## 新一代智慧 IT 維運系統



### 真正智慧化的流量即時分析，強化資安最經濟也最有效的方式

- ◆ 迅速察覺異常流量，透過自動化聯防阻擋擴散型病毒
- ◆ 人工智慧學習，無須人工設定閾值
- ◆ 掌握人員的網路使用行為

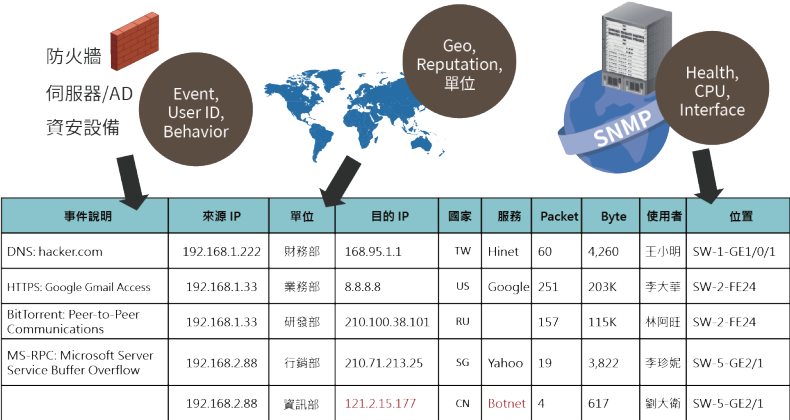
### 快速定位障礙根源，節省維運除錯時間

- ◆ 專業 SOC/NOC 等級即時監控畫面
- ◆ Drill-Down 進階查詢詳細資料內容
- ◆ 彈性自訂 Dashboard，整合資安 / 設備狀態 / 流量訊息於一個畫面中
- ◆ 支援跨廠牌設備 Syslog 資料的收集與分析，管理者再也不需跨設備查找

## 可在單一管理畫面全面掌握內網使用行為

將三大網路維運領域 (SNMP/Flow/Syslog) 加以整合是建構新一代維運體系框架的必要做法。N-Reporter/N-Cloud 產品將來自不同系統的異質資料主動關聯起來，省去人工比對查找所耗的時間。

### N-Reporter/N-Cloud 的管理畫面 ▼



## 內建機器學習演算法

過往採用人工逐一設定監控門檻值的辛勞情況將不復見。

首先，N-Reporter/N-Cloud 產品可以定義多種型態分析標的，諸如每個伺服器群、某個部門單位、某個連續或是不連續的 IP 範圍等，將收集到的數據分別根據每個設定標的進行獨立的學習運算，推算出合理使用基準區間，用來比對即時狀態，出現異常使用情況時立即發送告警，幫助 IT 人員**確切掌握網路情況、快速定位異常根源與修復**。

Robin，您昨天瀏覽過的[Internet出口流量服務分佈]報表，現在發生紅色警戒，請問您要點擊查閱細節嗎？YES / NO

NO.	Mail From	Mail To	Hit Count	Bytes	Flow Chart
2	mai@...com	sarav@...com	72	185.05M	<a href="#">View</a>
3	mo@...com	TEST@...com	40	164.08K	<a href="#">View</a>
4	liuli@...y.com	liu@...1.com	16	28.22K	<a href="#">View</a>
5	gac@...com	g@...com	16	39.13K	<a href="#">View</a>
6	halt@...com	A@...com	12	182.01M	<a href="#">View</a>
7	fc.d@...com	jc@...com	10	93.83K	<a href="#">View</a>
8	sely@...com	se@...com	10	2.35M	<a href="#">View</a>
9	johr@...com	mus@...com	8	1.88M	<a href="#">View</a>
10	ps_c@...com	trij@...com	8	8.33M	<a href="#">View</a>

**Warning!**  
Best check yo self, you're not looking too good.

智慧維運助手工具，能主動告警  
即時提醒管理者異常根源

## 執行數位足跡分析 輔助神器 N-Probe

- ◆ 支援 1 Gbps、10Gbps 和 40Gbps 之介面 Mirror Traffic
- ◆ 解決交換器 / 路由器不吐 Flow 或啟動 Flow 輸出時的效能問題

功能一 將實際流量轉換成 1:1 NetFlow Data 送到外部流量分析系統

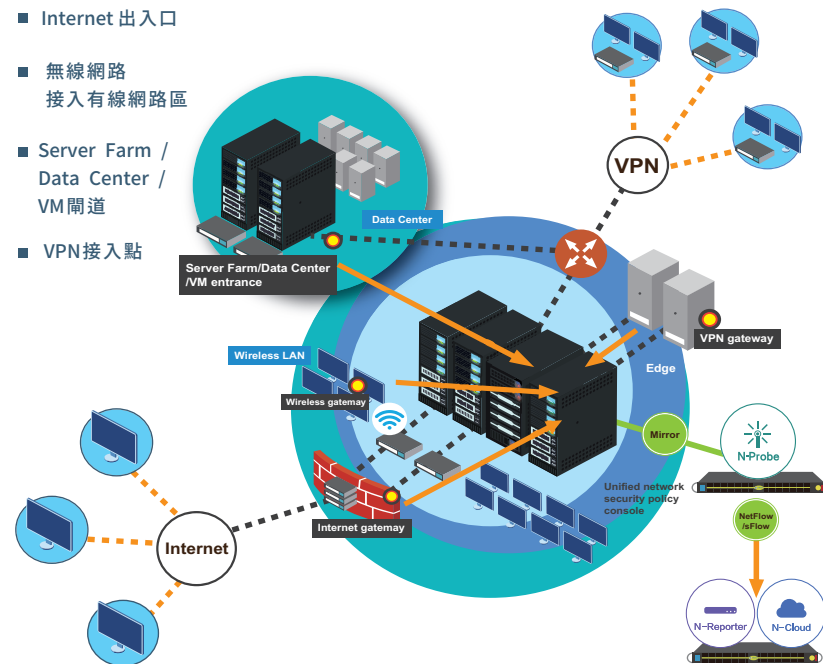
功能二 擷取實際流量裡的 DNS 封包，產出 DNS Log 送到外部日誌分析系統

功能三 能針對多個監測目標發出 ICMP，量測延遲時間 RTT

功能四 能針對多個網頁目標定時發出瀏覽請求，量測回應時間 RTT

### 建議需要 Mirror 流量的網路重要節點

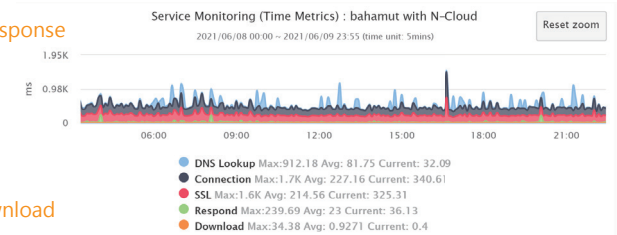
- Internet 出入口
- 無線網路  
接入有線網路區
- Server Farm /  
Data Center /  
VM 閘道
- VPN 接入點



## 網路延遲與網頁服務瀏覽效能監測 (Performance Monitoring, PM)

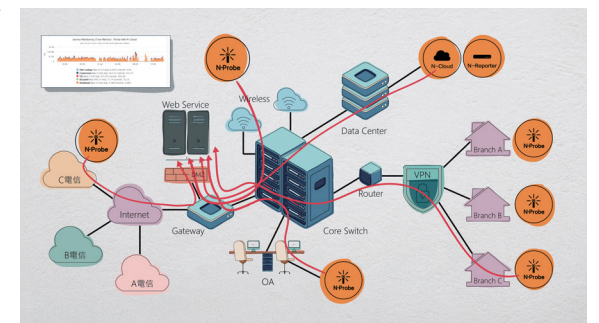
N-Partner 現階段提出兩種監控延遲的方式：一是用 ICMP 持續發出測試 Ping 封包用以收集各網路節點的延遲數據 (Round Trip Time, RTT)；另一個則是針對被監控的網頁服務 (Web Service) 定時地模擬人們瀏覽該網頁，將反應時間記錄下來進行分析。監控網頁服務 (Web Service) 效能其過程共分成五個階段：

1. DNS Query and Response
2. TCP Connection
3. SSL
4. Response
5. The First Page Download



N-Reporter/N-Cloud 持續接收 RTT 與 Web 服務的量測數值繪製圖形同時進行分析運算。告警的方式可以是事先預設閾值，超過後發出告警，或是透過 N-Reporter/N-Cloud 的智慧學習機制所建立的動態閾值比對，針對異常突升的延遲進行告警。

N-Reporter/N-Cloud 可以從管理 IP (Management IP) 發出 ICMP Ping 量測網路延遲 RTT；以及發出網頁服務瀏覽請求記錄不同階段的延遲數值。為了可以更貼近使用者感受，可以在不同的網路位置佈署 N-Probe，例如：在 OA 網段裡、外點辦公室、無線網路區、Internet 的 ISP 電信機房等等，藉由不同角度的模擬瀏覽監控，網站營運管理者將更能即時掌握服務的品質狀態。



# Dashboard 構建您隨選的戰情中心

連線到威脅情資  
列管域名的排名統計

連線到威脅情資  
列管域名的國家排名

連線到威脅情資  
列管域名的外國排名

威脅情資列管域名的  
國家分布

正常DNS查詢  
來源IP排名

正常DNS查詢  
來源國家排名

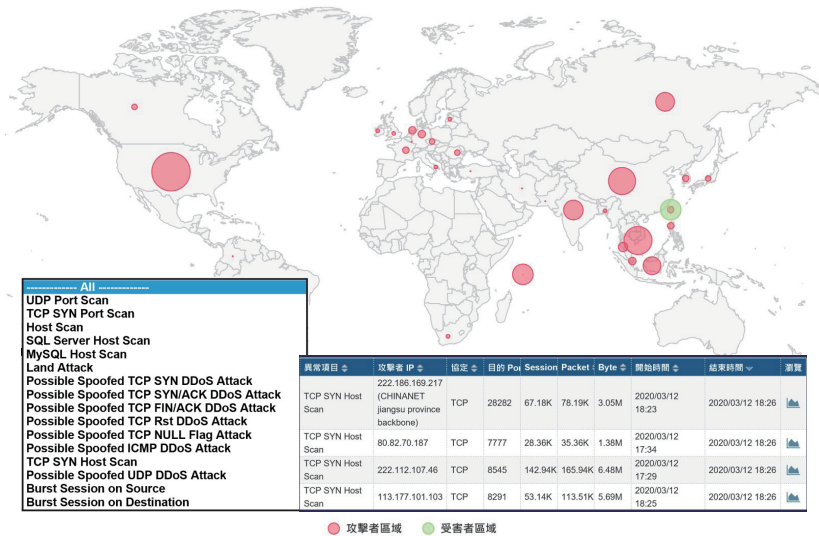
DNS查詢  
國家排行



## N-Partner 的防駭秘笈

### DDoS 與異常流量消弭

N-Reporter/N-Cloud 內建多種異常流量偵測機制，無須人工事先定義閾值，針對持續收集到的流量數據 (NetFlow/sFlow) 執行即時分析，讓異常流量行為無所遁形。此外，亦能結合威脅情資資料庫比對來往的流量，**結合交換器或是防火牆進行聯防阻擋**，避免災情擴大！



內建多種異常流量偵測演算法  
分析 NetFlow/sFlow 資料即時發現 DDoS 攻擊

## N-Partner 的防駭秘笈

### 惡意行為來源的即時定位與聯防

可透過 N-Reporter/N-Cloud 管理平台，直接下指令給 FW/Switch 設備，達到聯防之效。

#### Step 1

Syslog/Flow設備持續將發現的事件與流量資料輸出到N-Reporter/N-Cloud

#### Step 2

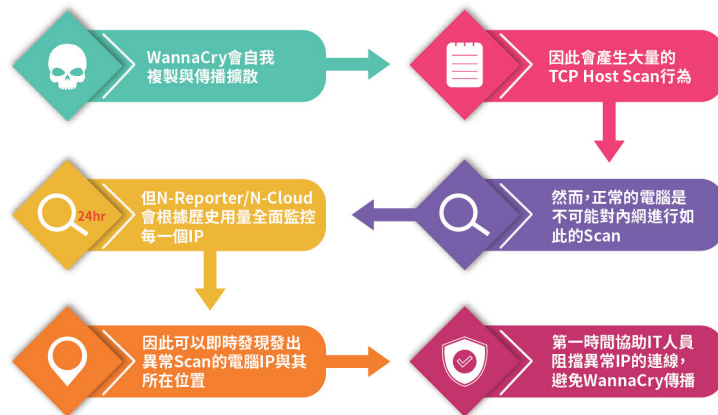
N-Reporter/N-Cloud根據收集到的Syslog / Flow Data建立歷史用量圖，發現任何異常突增即時告警



## N-Partner 的防駭秘笈

### 阻止勒索病毒擴散

在許多 N-Partner 用戶的實際案例裡，惡名昭彰的 Wannacry 病毒，爆發的瞬間就已經被 N-Reporter/N-Cloud 主動偵測發現，運用的方法正是**真正智慧化的流量分析技術**。遂行擴散式勒索軟體的終端設備其發送封包與連線的行徑與正常人員所使用電腦大不相同，如同發燒的病患會有特殊的症狀。擁有在電腦數眾多環境裡找出惡意 IP 位置這樣的技術，N-Reporter/N-Cloud 成為防止勒索病毒擴散的好方案。

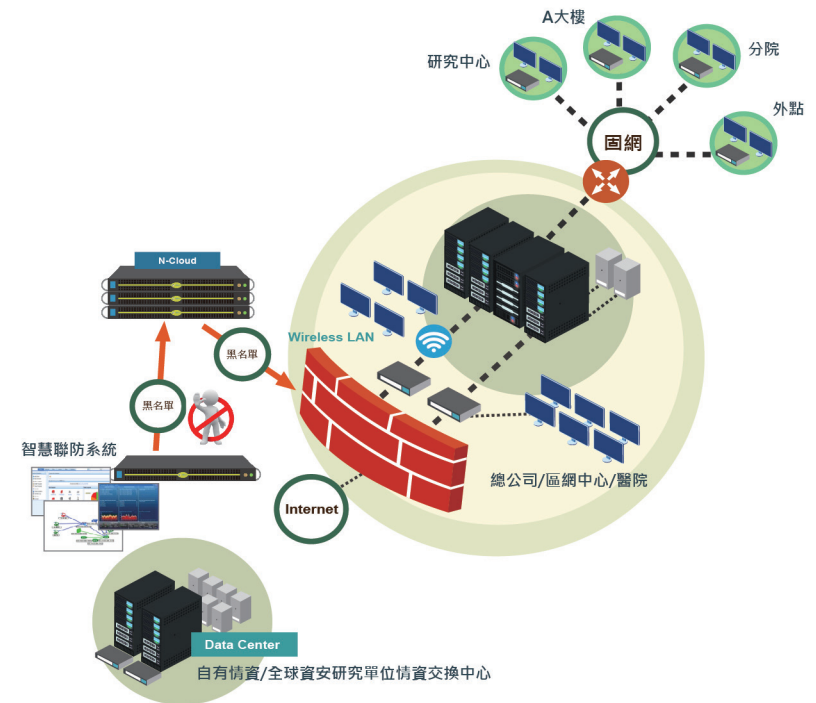


善用流量數據分析技術幫助資安防禦的最佳案例

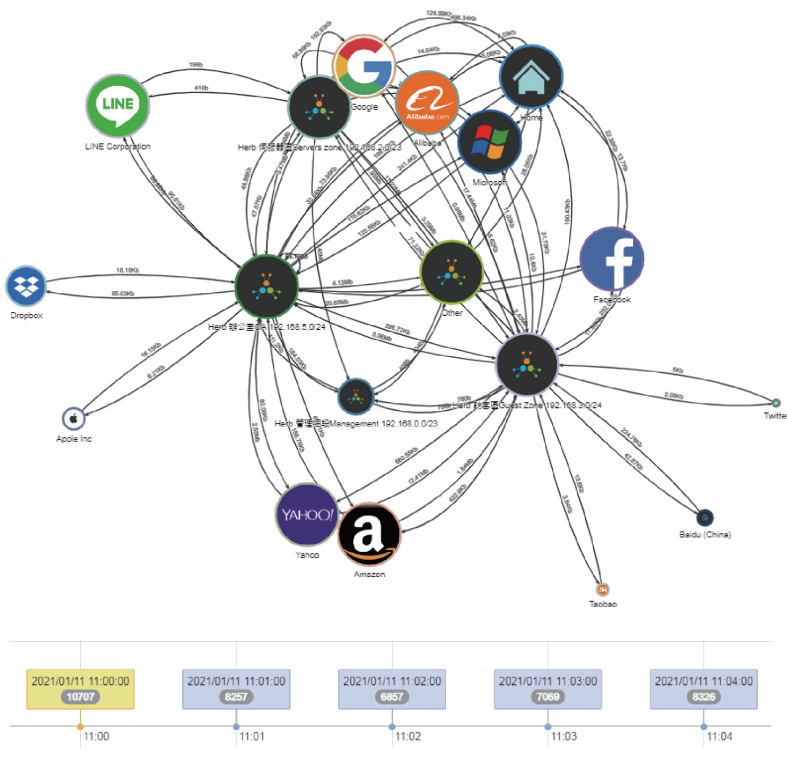
## N-Partner 的防駭秘笈

### 威脅情資聯防

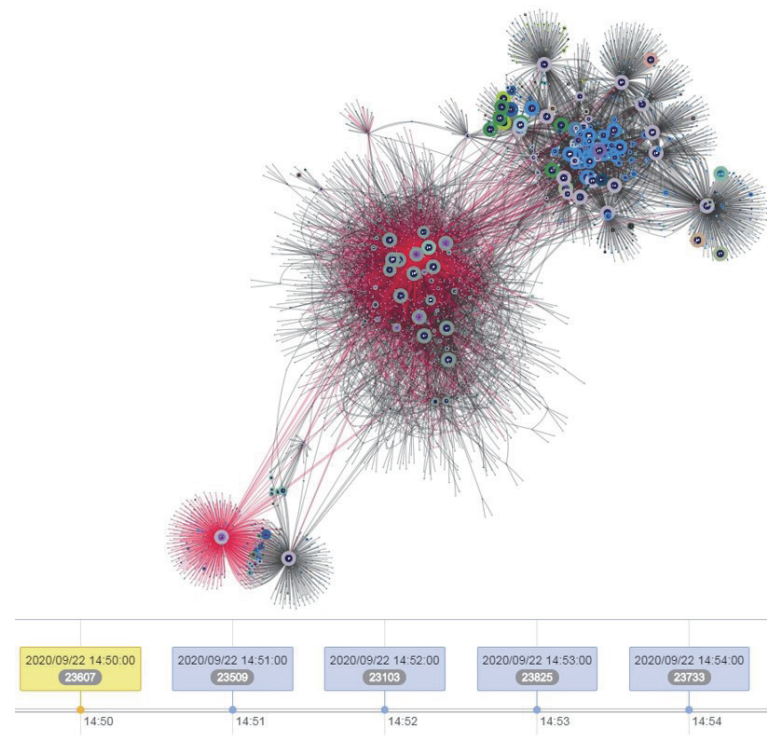
- ◆ N-Cloud 負責接收防禦黑名單後，下指令到防禦設備
- ◆ 統計防禦成果
- ◆ N-Cloud 亦提供 API，可分享資訊做其他客製開發



【IP 軌跡】動態關聯圖 - 網路知名服務使用行為分析



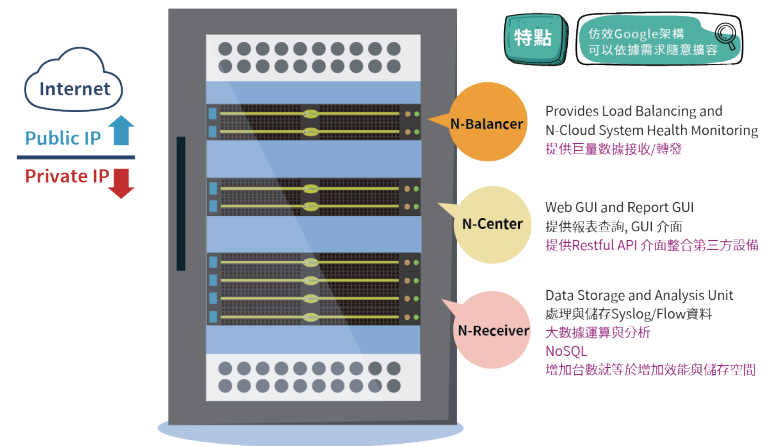
【IP 軌跡】動態追蹤，圖示化更易辨識異常連線



## 再巨量的日誌量也不用怕

### 兼具效能、高 CP 值計價與無限擴容的優勢

- ◆ 採用 NoSQL 架構對數據進行標籤分類，方便日後的快速查詢
- ◆ Full HA 高可用性架構，硬體更換與軟體更新都不停機
- ◆ 維持在同一平台架構上持續彈性擴容，能夠接收處理數十甚至百萬 EPS 的日誌數據，無懼日誌暴漲
- ◆ 平均 EPS 價格低廉，擁有最佳 CP 值



## N-Reporter/N-Cloud 產品，採用優於多數日誌產品的彈性計價方式

### 市面上大部分的日誌產品

- ◆ 大多以EPS量或是日均儲存量計價，費用就越高。
- ◆ 當遇到異常情況如DDoS攻擊時，日誌數量產出暴增，日誌軟體接收量授權不敷使用，恐遭丟棄，無法達成日誌需被完整儲存的預設目標。

### 彈性擴充N-Cloud規模

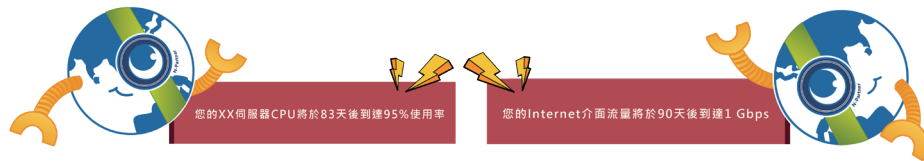
- ◆ 計價方式1：  
依據接收的設備總數計價，常應用在少數設備就會產生大量日誌的環境。
- ◆ 計價方式2：  
提供10,000EPS起跳的方案適用於有很多設備，但個別日誌量不多的環境。

不論採用哪種計價模式，隨著日誌量逐漸增加，也可以**維持在同一平台架構上持續彈性擴容幾乎無上限**。因此能**隨時因應組織的各種日誌蒐集需求**，在合理預算內同時滿足**高效能以及巨量收集需求**。

**PAY AS YOU GROW**

## 預測硬體效能與網頁服務品質的未來走勢 建立早期預警機制

趨勢預測 (Prediction) 是藉由演算法則將收集到的歷史數據建立未來走勢模型。現階段所推出的預測功能分成短期趨勢 (Short-term Prediction) 以及長期趨勢 (Long-term Prediction)，皆已內建在最新版本 of N-Reporter 與 N-Cloud 產品裡，在保固期內的产品皆可透過韌體更新方式取得。在短期趨勢裡使用者可以看見未來數小時到數天裡的走勢變化；而長期趨勢則呈現數月後的線形可視圖。搭配事先定義的合理閾值，N-Reporter 與 N-Cloud 智慧維運系統將提前預警資源不足風險。



▲ 圖：您的 XX 伺服器 CPU 將於 83 天後到達 95% 使用率      ▲ 圖：您的 Internet 介面流量將於 90 天後到達 1 Gbps

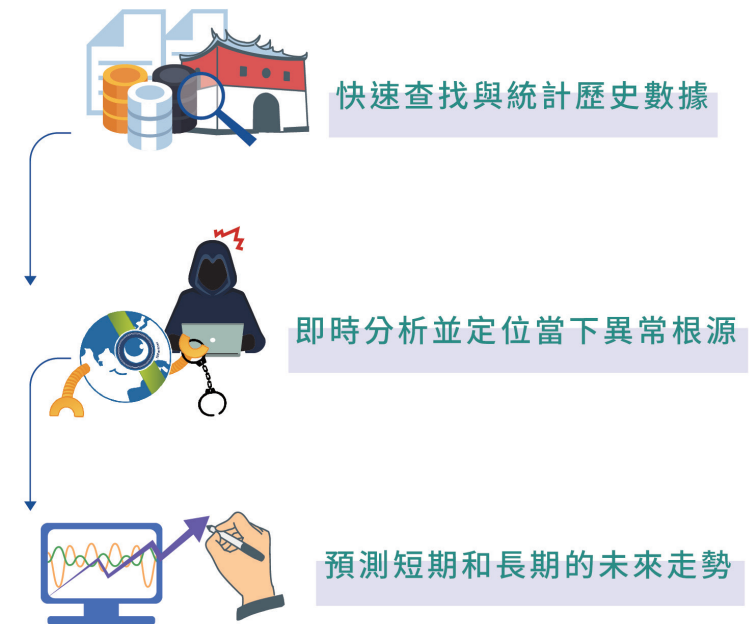
### N-Reporter 與 N-Cloud 產品內建趨勢預測的項目：

- ◆ 針對系統硬體資源的趨勢預測：CPU/Memory/Disk Utilization、Interface Throughput



- ◆ 針對網路延遲的趨勢預測：ICMP Ping Round Trip Time (RTT)
- ◆ 針對網頁服務的趨勢預測，包含瀏覽網頁的五個階段：DNS Query and Response → TCP Connection → SSL → Response → The First Page Download

## 從過去到未來，完全掌握網路動態 All in N-Partner





## N-Partner 新夥伴科技，IT 人新世代的絕佳夥伴

新夥伴科技股份有限公司 (N-Partner Technology Ltd. Co.) 成立於 2011 年，總部位於台中市，為台灣專注大數據收集、高效能處理以及智慧分析的軟體研發團隊。

研發團隊核心成員均擁有超過 15 年的電信等級網路維運以及軟體開發經驗，並集合網路、資安、作業系統與 Kernel、電腦硬體與虛擬機、C 語言、PHP/Java、資料庫、大數據處理與雲架構...等領域專才，以及籌組新型創意行銷美術設計團隊，提供給 IT 管理者更清楚且有效率的威脅預警與網路障礙除錯依據，更快、更精準禁止災害擴大！至今已榮獲國內多數政府機關、教育網、多家金融集團、跨國企業、醫療院所與電信公司採用，商業版圖方面也正與國內其他資安技術領域研發商共組台灣國家隊逐步拓展至東南亞，展望成為全球 IT 人的最佳管理方案選項。



官方FB專頁



官方Line帳號



官方影音頻道

 **N-Partner** 新夥伴科技股份有限公司

Tel : 04-23752860      Fax : 04-23757458

403 台灣台中市西區忠明南路497號13樓

Sales Information : [sales@npartnertech.com](mailto:sales@npartnertech.com)

Technical Support : [support@npartnertech.com](mailto:support@npartnertech.com)

