CHIEF | 是方電訊
是方電訊股份有限公司
070-1018-6688 | 02-2657-6688
台北市 114 內湖區瑞光路 68 號 2 樓



經銷商

CHIEF APP CLOUD

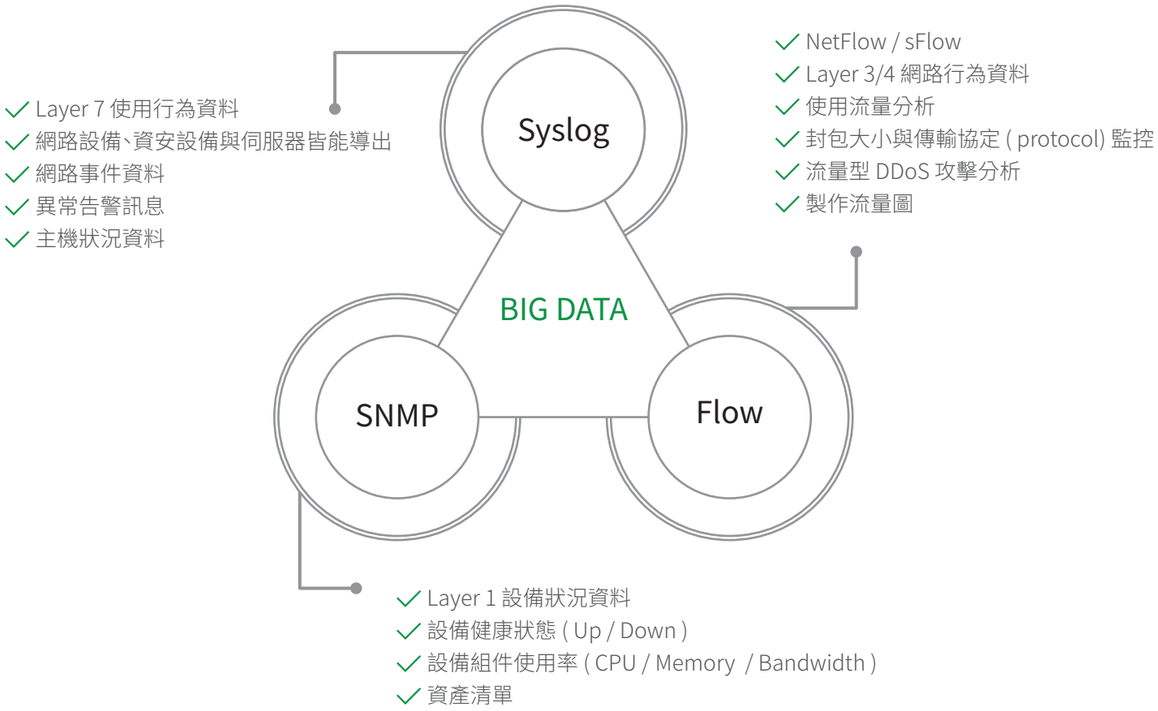
# 日誌分析管理 LogAnalysis

## 不僅提供儲存與查詢，內建人工分析智慧更能有效協助IT維運

無論您是因為法規規範必須將日誌儲存起來以方便隨時查詢、產生日常統計報表，或是希望透過日誌的分析提升資安能力與IT系統營運績效，日誌分析管理系統將是您的最佳選擇。

再也無須每年花費大把經費採購日誌收集與儲存軟硬體，透過網路將伺服器日誌、網路設備日誌、資安事件日誌以及流量數據(NetFlow/sFlow)等資料上傳至LogAnalysis日誌分析管理服務，就可以完成日誌保存與管理要求。您將擁有一個專屬的網站(Portal)，能夠輕鬆查詢日誌以及製作所需的統計報表。

LogAnalysis日誌分析管理服務內建的人工智慧會根據收集到的日誌與流量數據加以分析，如果有異常暴增的資安事件或是流量，系統會自動發出告警以及顯示在Dashboard上，協助您即時掌握需要緊急處置的事件，輕鬆完成日常管理與維運工作。



## 功能特色

- 清楚而專業的資安事件分析以及統計報表。
- 自訂報表功能，可彈性製作豐富多樣的即時線上圖型。
- 24小時無間斷執行異常行為分析，自動化告警。
- 日誌歷史資料儲存與查詢，符合法規要求，協助日常維運管理工作。
- 人工智慧可主動發覺帳密猜測攻擊。
- 關聯功能可讓日誌管理發揮最大效益。

## 功能說明

### Syslog Data 儲存 / 查詢 / 分析

- 支援多種設備/伺服器的Syslog日誌搜集。
- 人工智慧分析日誌。
- 採用雲架構，可快速搜尋日誌，擴充儲存空間。

### 分析功能

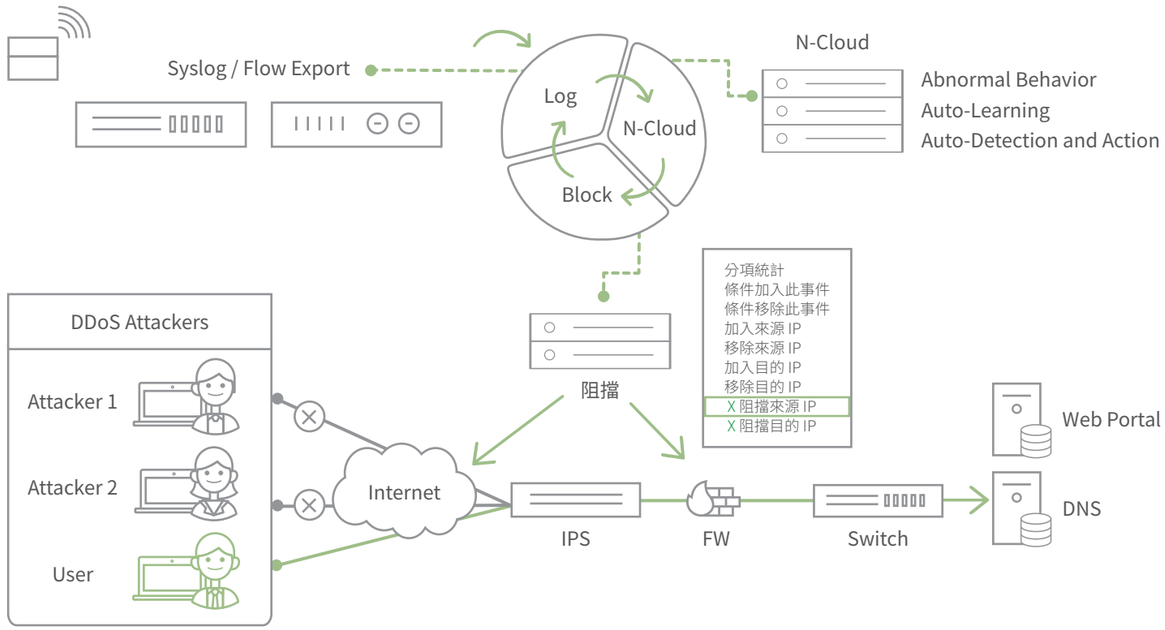
- 使用智能分析與TOP N排序。
- 針對個別組織進行流量監控與用量分析。
- 支援Threshold設定，用量超標時會發出告警。

### 異常行為即時分析

- 學習歷史行為，自動建立合理 Base Line。
- 即時告警 Syslog 事件、Flow 用量異常突增之行為。
- 聯防，結合 FW、IPS、Switch、Wireless 阻擋異常突增來源。

### 報表功能

- 每個Domain管理者都可以定義專屬報表。
- 自動產生與寄送Off-line報表。
- 支援AD名稱解析對應，更容易瞭解IP真實身分。



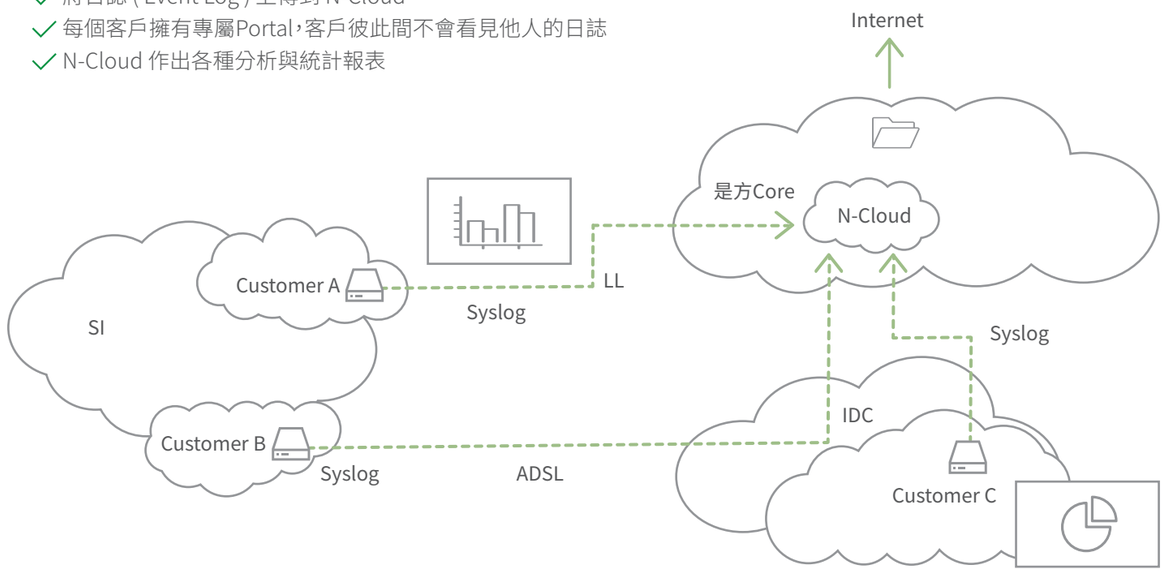

## 應用範圍

- 有日誌儲存與分析統計需求者。
- 需要透過流量分析以協助網路維運與各種用量統計需求者。
- 必須符合法規要求者。
- 有日誌儲存備份需求者。
- 希望達成上述需求但預算不足以自建系統者。

## 平台架構

### 用戶端的設備 ( 如: FW, Router / Switch, Server, Security Device )-

- 將日誌 ( Event Log ) 上傳到 N-Cloud
- 每個客戶擁有專屬Portal，客戶彼此間不會看見他人的日誌
- N-Cloud 作出各種分析與統計報表




## 應用效益

- 相較於自建日誌儲存軟體與硬碟空間，日誌分析管理服務可提供高穩定度且更為經濟的服務。
- 提供每個用戶獨立且專屬的Portal，具備高隱密性。
- 專屬Portal提供全中文化的操作介面，無論是查詢、建立統計報表都能夠輕易上手。
- 可統一收集來自各種品牌資安設備的事件日誌、各種伺服器日誌、網路設備NetFlow、sFlow資料。
- 加解密演算法(AES & SHS)通過美國NIST CAVP驗證，確保資料的安全性與不可否認性。
- 內建人工智慧演算法則，以大數據分析技術學習歷史數據後為每一個日誌建立動態合理閥值，主動告警發生異常突增的事件，以減輕人員管理與分析日誌的負擔。
- 符合法規規範要求。
- 可以依據需求創建Dashboard，將最關心的內容投影在監控螢幕上，即時呈現最新狀態，一目了然。
- 提供是方專有的DDoS攻擊分析服務。
- 100%台灣製軟體與服務。