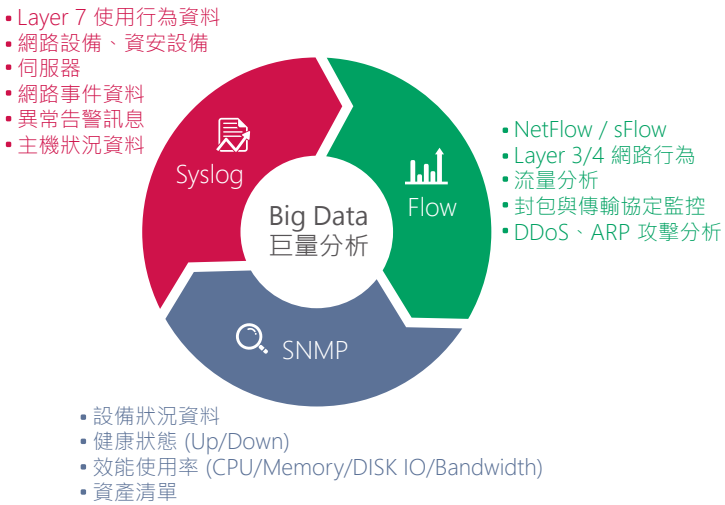
正邦 NETVISION

關注細節
防禦威脅

LOGinsight 巨量資料日誌安全管理解決方案

LOGinsight 巨量資料日誌安全管理解決方案，以獨特的大數據分析技術作為核心，針對不同的 IT 設備或裝置所產生的日誌紀錄統一蒐集、風險識別、分析報告，簡化管理人員作業時間以及資料正確性可視性，關聯式與行為分析包括 SNMP、Syslog 以及 Flow。

IT 管理人員藉由 LOGinsight 巨量資料日誌安全管理解決方案，可更快速找出所有網路設備與裝置、資訊安全設備、伺服器系統、應用系統、VMware 及防毒系統等潛在問題、威脅活動、攻擊模式、異常狀況、機密資料存取以及內部威脅等情報資訊，進一步調查並解析各種威脅來源與目的，輕鬆分析所有記錄，進而長期偵測與追蹤可疑的惡意活動，找出其他安全性解決方案所遺漏的隱性威脅，並依據事件風險等級產生所需稽核報表，符合企業日誌管理成本效益解決方案。



關鍵特點

- **巨量資料運算比傳統方式更快速**
  透過巨量資料運算及資料挖掘技術，將跨平台、設備裝置日誌統一蒐集、儲存、管理、搜尋分析，偵測網路安全攻擊和網路漏洞，及早扼止威脅以免造成危害，協助管理者防範 IT 營運風險。

- **基於 ISO27001 的 IT 設備風險分析平台**
  即時掌控所有 IT 設備及網路系統資料營運狀態，並可與 SIEM、NOC 及 SOC 整合成緊密聯合防禦平台，提高資產可用性與可靠型並降低整體維護成本。

- **支援 IT 營運管理分析整合資訊安全的全面防護**
  廣泛支援超過 500 種以上日誌產生來源收集任何資料，不限裝置和格式日誌資料蒐集，支援來自於任何 Syslog 或檔案型日誌來源的原始記錄，簡化資安鑑識調查。

- **鑑識分析簡化稽核管理作業**
  蒐集的安全訊息與事件日誌，提供稽核追蹤途徑，用來偵測網路攻擊行為與執行詳細的鑑識分析，包括依資料來源、時間、關鍵字、嚴重等級、組織網段、設備 IP 位址及 MAC 等過濾搜尋。

正邦 NETVISION 正邦資訊科技股份有限公司
台北市南港區南港路三段 225 號 12 樓之 1 TEL:(02) 2782-0798 FAX:(02) 2782-0782
www.netvision.com.tw

全方位的設備裝置支援

支援各種網路設備、安全性裝置及異質性平台的不同日誌記錄來源管理，包括：路由器 / 交換器、無線網路、防火牆、虛擬私有網路 (VPN)、入侵偵測/防護系統 (IDS/IPS)、防毒應用程式、主機與伺服器、資料庫、郵件及網頁應用程式、自訂裝置及專屬應用程式等，簡化跨不同安全性及整體網路裝置的搜尋、資料關聯與分析報告，並可整合其他網路資安設備進行聯合防禦，提供手動及自動阻擋機制迅速隔離資安問題，協助 IT 營運安全管理。

保護 IT 基礎架構提升風險管理價值

自動化的記錄蒐集、儲存及風險管理，監控網路裝置、設備配置與資訊，例如網路資產資訊、配置、身份行為、端點存取、設備存活、阻斷控制以及資料流程等。自動化原則引擎，可以評估實際或潛在網路流量，標示異常的攻擊路徑，藉此視覺化惡意探索的風險，讓事件資料與網路拓蹼及連線資料產生關聯一目了然，解決漏洞問題達到合規要求，提升 IT 風險管理價值與能見度。

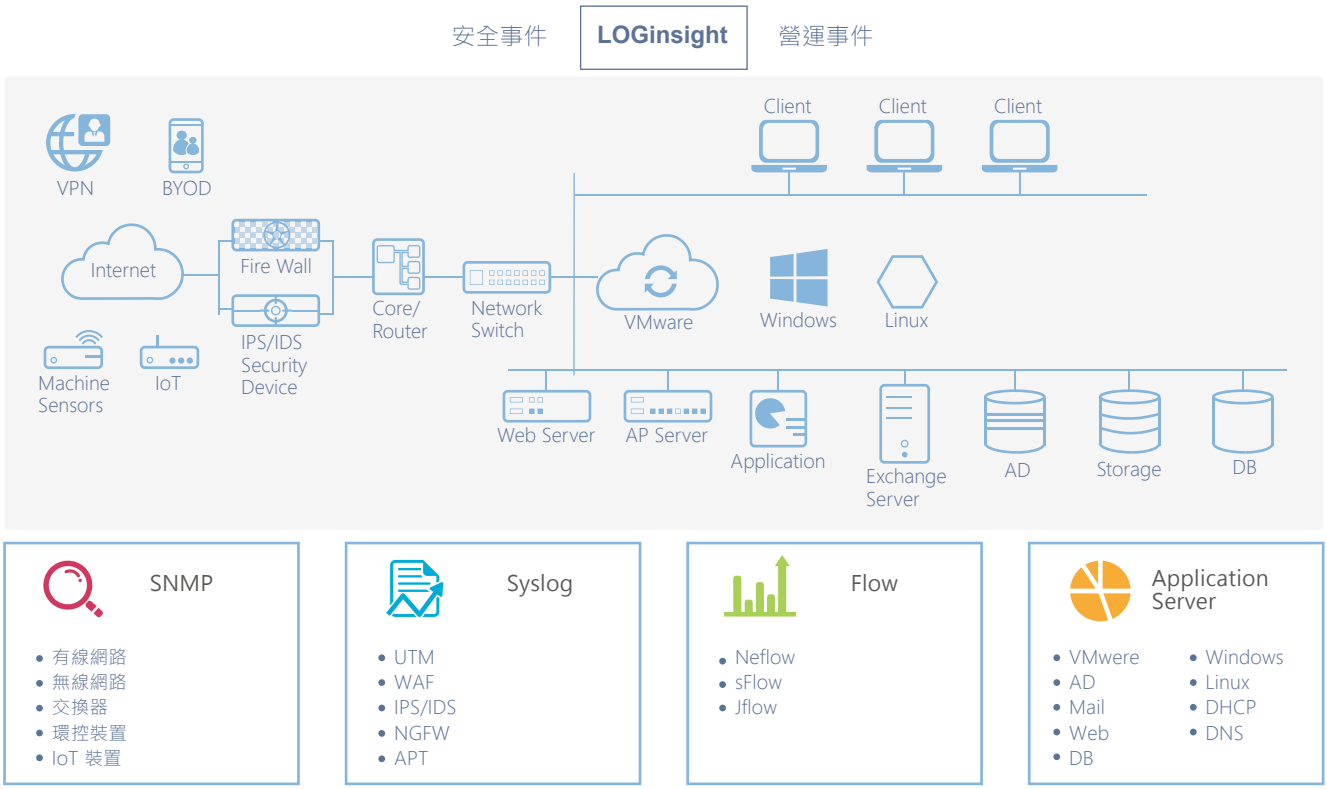
安全性資訊和事件關聯管理

可處理所有的事件，偵測可疑威脅行為，原始日誌資料均已加密不可更改，支援 Syslog 原始的 Raw Data 備份，管理人員可根據資安事件等級簡化後的分析，即時發視問題立即執行安全管理措施，並可依據管理模式定義監控特定活動並檢視資料長期趨勢，同時，直覺式使用者介面快速搜尋將需要注意的事件樣本轉換為重要的即時告警資訊，聚焦在監控威脅及內部攻擊防範以及持續性漏洞威脅發生，讓整體網路使用和安全管理作業不再有落差。

實現符合成本效益的法規遵循

採用單一整合式解決方案，自動蒐集分類、聚合、正規化、關聯分析、歸檔保存、稽核報表，符合法規要求如：PCI DSS 3.0 以及 HIPAA、HITECH、NIST 日誌管理標準，確保日誌資料保存的完整性 (Log file integrity checking) 以及不可竄改性，符合個人資料保護法應用，執行數位證據鑑識的工作，輕鬆完成 ISO 27001 ISMS 管理作業，減少人力作業時間成本，符合安全管理與成本效益。

SHA-1 雜湊演算法及公私鑰產生 Signature，每小時可產生數位簽章結合 Timestamp based 的方式，提供下載簽章檔 (PKCS7 方式封裝)。



Order Information

- LOGinsight 巨量日誌管理系統效能 1,000 EPS，分為Basic版、Enterprise版、Center版。可橫向擴展擴充及可自備 VM 或硬體主機 (請參考 ISOinsight 硬體平台)。
- ISOinsight IT 資源監控暨風險管理平台，進階全功能版本。