

XENSOR



端點 APT 進階持續性 威脅攻擊防禦系統

結合機器學習演算法和獨特 FTA 鑑識技術，提供企業高效的自動資安風險盤點 (Threat Triage)，並對全單位進行遠端事件調查與內部入侵行為分析 (Threat Hunting) 等。有別於傳統資安產品，Xensor 整合了多維度威脅情報，包含使用者帳號行為調查、程式記憶體鑑識、端點電腦鑑識與網路活動分析，不需額外病毒碼與特徵規則，能主動快速反應，降低資安應變成本。

- ✓ 可選擇 Agent 即時威脅獵捕與 Agentless 鑑識模組
- ✓ 支援惡意程式即時阻擋與遠端清理
- ✓ 支援 SYSLOG 通報，可客製化的 API 介面，快速導入 MSSP/SOC 流程
- ✓ 配合 IT 管理架構，可支援高承載堆疊架構



輕量彈性 容易部署

超低系統資源使用，提供自建或雲端建置方案，端點部署也可選擇常駐型即時威脅獵捕或免安裝型鑑識模組掃描器



強化鑑識 主動獵捕

支援 Windows、Linux 與 MacOS 作業系統平台，主動找出潛伏威脅和駭客行為軌跡，協助企業達到鑑識級調查能力



立即轉換為 合理投資報酬

提升資安團隊運作效率，快速應變並極小化駭侵損失，強健公司商業營運



VANS 資安弱點 通報機制模組 (*加購項目)

掌握場域風險情勢，進行資產與弱點管理，並落實資通安全管理法之資產盤點與風險評估應辦事項



GCB 政府組態 基準模組 (*加購項目)

規範資通訊設備的一致性安全設定，以避免成為駭客入侵管道，進而減低引發資安威脅事件之風險

* 註：此項目為加購模組，須至少購買或具有「資通安全健診系統」、「Xensor 端點 APT 進階持續性威脅攻擊防禦系統」、「AIR (AI-bot Response) 端點偵測及應變機制 (EDR/MDR)」等產品其中一項，才可加購此項目。