EDR 端點威脅防禦應變

台灣近年嚴重的資安事件發生時間，根據統計都是下班或是假期時間，加上長時間的潛伏期，令企業難以防範。同時，資安事件發生的當下，需要經驗豐富的專家針對資安系統發出的警報進行分析，甚至對當下的資安威脅調查與處理，這都是企業亟欲達成但是迫於現實考量無法達到的目標。

國際知名的資訊顧問的公司 GARTNER 建議 ：
“企業應使用 MDR 服務，增加 24*7 威脅偵測與事件調查與反應資安的能量，利用 MDR 服務來彌補現有資安操作的空隙，例如弱點掃瞄與日誌監控管理下的時間差 “。

EDR 端點威脅防禦應變簡介

EDR 端點威脅防禦應變，利用高靈敏度的端點偵測與應變解決方案，全時保護企業組織內重要 PC 與 Server 伺服器等端點主機，並結合了巨量的國際與本土資安情資，即時的情資驅動威脅偵測與主動獵捕可疑威脅，既使是進階長期潛伏或最新零日的可疑威脅，也能有效感知，自動協助採取應變動作，當下中止駭客惡意活動，徹底根除組織內潛伏的惡意行為，確保真正的企業組織資訊安全。

服務支援的託管端點系統

-Windows Server 2008 R2 - 2019 &Windows 10-8 (64&32bit)

Mac OS 10.9 above(64Bit only)

Linux RHEL & CentOS 7 (above)

知名 EDR 方案與巨量情資高效偵測威脅

採用國際知名的 EDR(Endpoint Detection and Response) 解決方案，同時結合 EPP 端點 Antivirus 防毒引擎在同一個端點應用程式，同時可以防衛、偵測並採取應變處理於已知的惡意程式與未知的可疑威脅，有效防堵最新不斷改變攻擊手法的資安威脅。偵測能力的關鍵核心，是結合國際即時情資來源與國內發生最新的本土情資，自動驅動偵測檢查在受託端點內詳細的系統資訊與運作程序等多樣的入侵指標，清