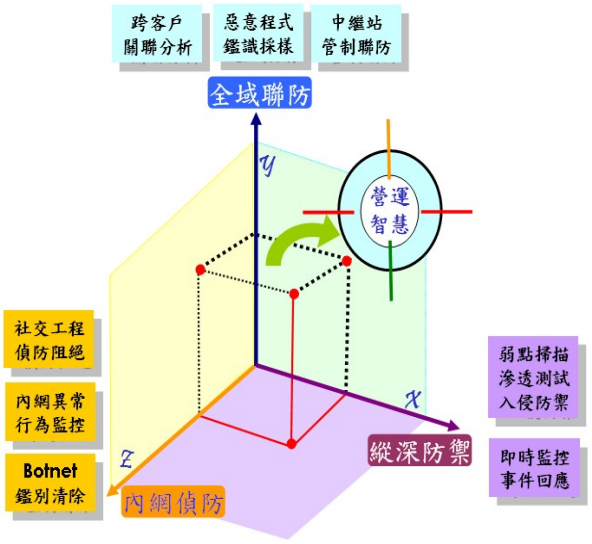
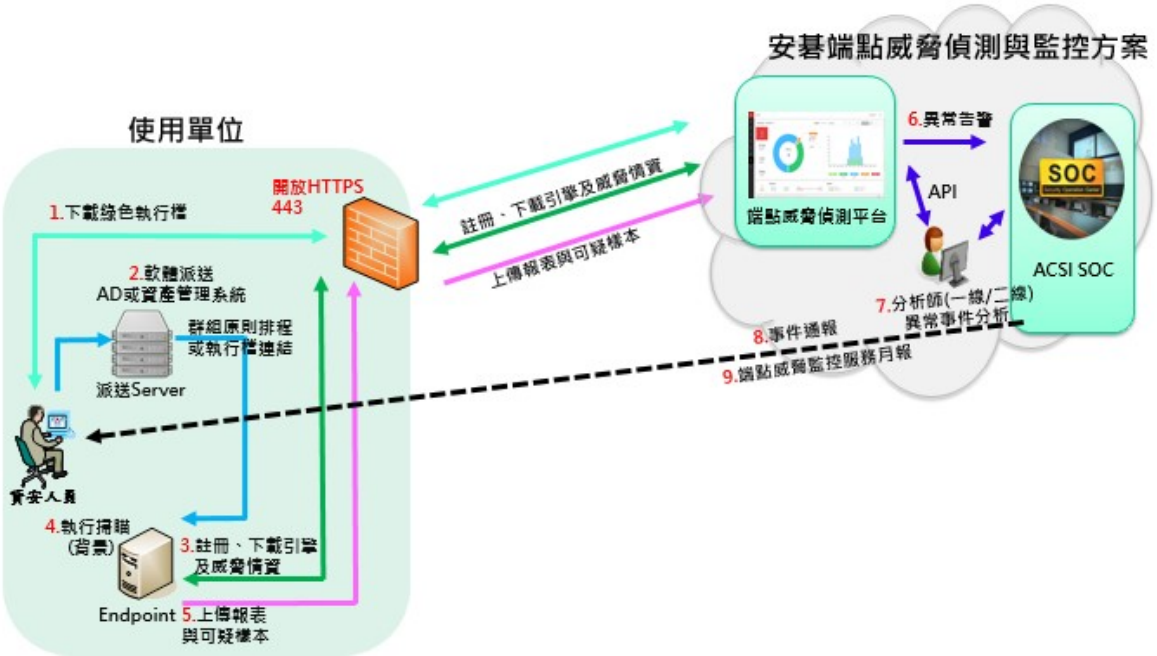
SafeCove 端點威脅偵測與監控包(每年訂閱)

產品簡介

近年來頻繁的針對式資安攻擊事件，對於企業與機關的資安防護形成的巨大衝擊與影響，企業與機關用戶迫切尋求先進的資安防護服務來強化主機與端點防護能力，以抵禦先進攻擊的資安威脅。進階威脅的攻擊手法，能輕易避開防毒軟體、入侵防禦設備的偵測，僅依靠特徵碼與制式偵測規則，並無法發覺此類未知的攻擊手法。因此，具備先進資安威脅偵測、監控與回應機制的專業資安防護方案開始受到用戶關注，以應付日益嚴峻的資安防護威脅與挑戰。



SafeCove 端點威脅偵測與監控包，基於安碁資訊多年來的資安監控經驗，可整合先進的端點威脅偵測平台，提供機關與企業用戶端點資安防護維運與資安防護監控機制。此方案可整合端點威脅偵測、威脅狩獵、資安事件監控與回應能力，強化企業與



政府機關全天候進階資安攻擊威脅偵測與防護能力，早期發現惡意入侵。

產品功能說明

項目	內容說明
產品功能	
API 整合端點威脅偵測與回應平台，提供整合資安事件監控與自動通報機制	● 透過 API 整合端點威脅偵測平台，擷取端點惡意威脅軌跡特徵資訊，彙整於資安監控系統進行跨設備關聯分析、監控與自動化事件通報。 ● 提供端點威脅與異常行為偵測。 ● 提供端點威脅偵測季報。 ● 支援 TeamT5 Threat Sonar 等平台。
整合資安威脅偵測、狩獵與回應機制維運	● 自動化偵測高風險惡意程式與惡意攻擊行為。
技術支援	

產品授權

產品名稱	授權數量
SafeCove 端點威脅偵測與監控包(每年訂閱)	提供 1 台使用者端點作業系統或伺服主機作業系統威脅偵測與監控授權

產品售價

- NT$ 35,000 (含稅)

交付項目

- SafeCove 端點威脅偵測與監控包使用授權(每年訂閱)
  - 含資安事件收集模組

資安事件收集模組硬體需求

- CPU ： Intel 4 核心 2.0 GHz 以上
- 記 憶 體： 16 GB 以上
- 硬碟空間： 500 GB 以上
- 作業系統： Microsoft Windows 2008 Server 標準版 或 Linux 以上

預期效益

- 提供端點威脅偵測與回應機制維運、異常事件分析、資安事件回應的整合機制，確保資安防護的有效性。
- 整合事件關聯分析，提升事件分析與告警的準確性。