

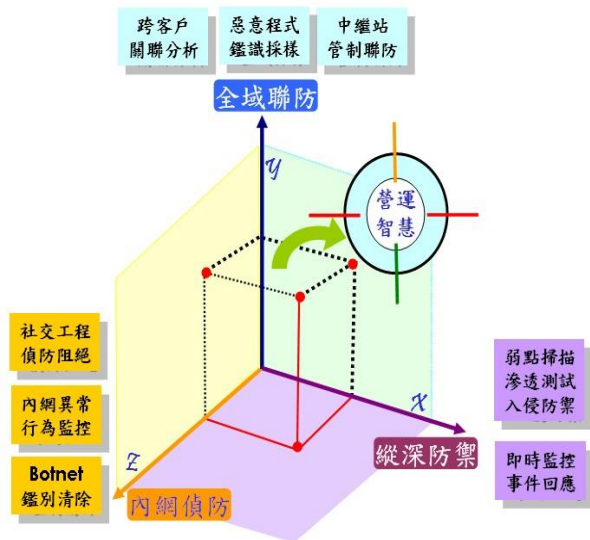
SafeCove AD/WAF/DAM 入侵偵防包(每年訂閱)

產品簡介

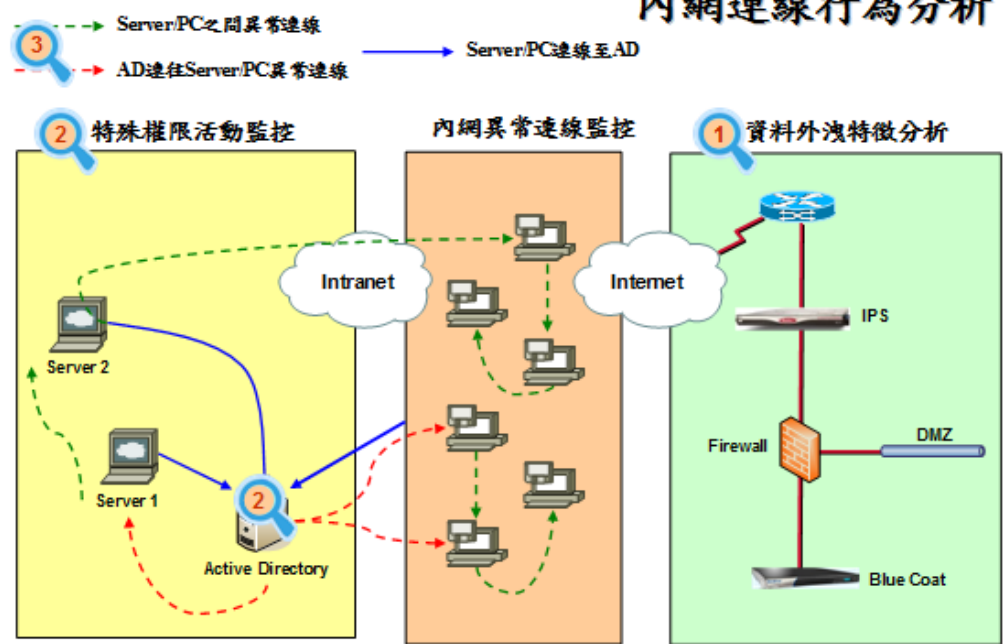
現今資安事件偵防已面臨極大之挑戰，多數惡意入侵行為皆採行混合多種社交工程攻擊之手法滲透至企業與機關內網，植入惡意程式進行埋伏，再伺機進行惡意攻擊與機敏資料的竊取，其多變的入侵行為與手法為現有防毒與防護系統皆難以防護之處，這也是此類攻擊行為可怕的地方。

SafeCove AD/WAF/DAM 入侵偵防包，以本公司雲端資安智能監控平台，搭配於

用戶端安裝的資安事件收集模組，可以針對 Microsoft AD、網頁防火牆（WAF）或資料庫稽核系統（DAM）之日誌記錄與事件進行主動分析，以系統化的方式進行相關存取日誌與事件收集、關連性分析後，對未知型態的入侵事件與社交工程攻擊行為進行



內網連線行為分析



事件預警，提供給政府機關作為因應個資安全與資訊安全的管理依據。

產品功能說明

項目	內容說明			
產品功能				
Microsoft AD 社交工程偵防功能	新型態的惡意入侵行為，入侵者在入侵內網後會潛伏一段時間，於內網進行刺探，伺機竊取 domain admins 帳號。本系統將主動對 Microsoft AD 使用者帳號登入與異常活動之行為進行記錄與分析，以主動發覺惡意入侵行為。			
	日誌與事件稽核項目			
	Event ID	Event 說明	Event ID	Event 說明
	528 / 4624	使用者成功登入電腦	6006	Event log 已停用
	529 / 4625	使用者名稱或密碼錯誤	601 / 4697	嘗試安裝服務
	530 / 4625	非法時間進行登入	602 / 4698	排程工作已被建立
	531 / 4625	已停用的帳戶試圖登入	624 / 4720	帳號建立
	532 / 4625	過期的帳戶試圖登入	630 / 4726	帳號刪除
	533 / 4625	系統不允許該使用者登入	636 / 4732	administrators 成員新增
	534 / 4625	不被允許的登入類型	684 / 4780	對 administrators 成員設定 ACL
	535 / 4625	帳戶密碼已經過期	517 / 1102	稽核紀錄被清除
	536 / 4625	沒有啟用 Net Logon 服務	680 / 4776	經由 XX 登入
	537 / 4625	因其他原因而登入失敗	576 / 4672	指派特殊權限到新的登入
	539 / 4625	試圖登入時被鎖定	540 / 4624	登入成功
WAF 入侵攻擊偵防	● 網頁應用程式或弱點攻擊行為偵測 ● 異常網頁存取行為或探測活動偵測 ● SQL Injection/cross site scripting 等攻擊行為偵測			
DAM 機敏個資存取與異常行為偵防	● 監測個資或特定敏感資料存取行為 ● 建立資料安全與稽核，資料存取紀錄與證據保存 ● 違反資料庫存取政策之行為偵測			

項目	內容說明
技術支援	
資安問題諮詢	● 5x8 線上（電話／電子郵件）資安問題諮詢 ● 客服電話：0800-286-009 ● 選購項目 - 遠端技術支援 ● 5x8 電話通知，隔日到場 ● 工作內容： - 資安事故設備隔離程序 - 找出並排除可疑惡意程式 - 找出可疑入侵手法或被駭途徑 - 系統回復 ● 每次啟動至少 4 小時（到府起算），不足 4 小時以 4 小時計

產品授權

產品名稱	授權數量
SafeCove AD/WAF/DAM 入侵偵防包(每年訂閱)	可支援監控 Microsoft AD/WAF/DAM 等設備，監控 1 台設備之資安事件監控

產品售價

- NT\$89 萬(未稅)

交付項目

- SafeCove AD/WAF/DAM 入侵偵防包使用授權(每年訂閱)
- 用戶端資安事件收集模組一年使用授權

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：4 GB 以上

- 硬碟空間： 500 GB 以上
- 作業系統： Microsoft Windows 2003 Server 標準版 或 Linux 以上

預期效益

- 獲得即時專業資安事件通報，強化資料防護政與管理依據
- 建立有效防護資料外洩之安全預警機制
- 資安事件發生時，可以儘快找出事件來源，以便有效防範事件擴散
- 獲取早期預警通知，有效防制新的資安威脅