

RDsecurer

重新定義網路傳輸秩序

Traffic Delivery Platform 模組

Flow Defender

威脅聯合防禦閘道



Flow Defender

提供低網路延遲與高防護效能，快速識別和過濾出威脅情資，同時支援多樣性的情資整合處理和網路防護相結合，可以實現即時威脅防禦，並保障網路通訊品質。

威脅防禦系統在數位轉型中的重要性與挑戰

巨量處理能力與全方位威脅清單管理機制

提供雙向 200 Gbps 網路通訊頻寬處理能力，有效減低傳統資安閘道效能負載。

具備最高100萬筆 IPv4/IPv6 惡意清單即時防禦能力，輕鬆管理多元資安情資。

具備超低延遲網路加速引擎，提供高品質網路通訊環境。

提供政策式存取控制機制，依據 L2~L4 作為流量複製過濾條件，建立單獨存取控制政策與例外清單。

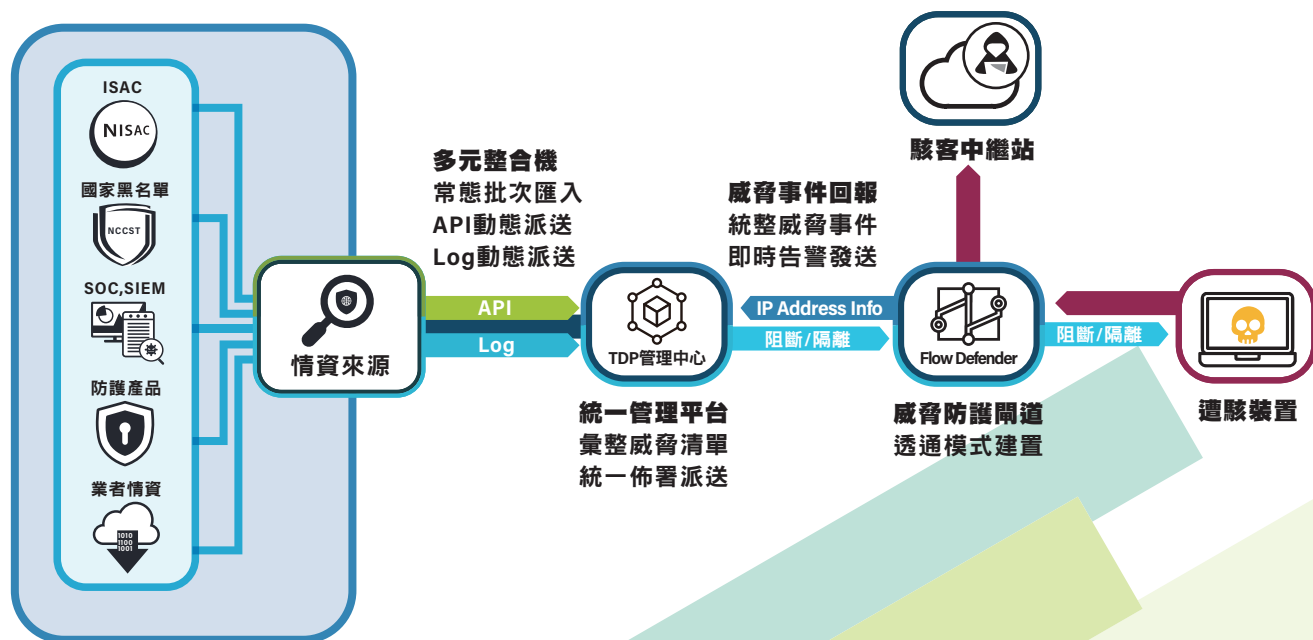
多元聯合防禦機制

常態型清單提供常見之 GUI 圖形化批次匯入，與雲端儲存空間檔案匯入方式

動態型清單除了提供 API 動態派送機制外，亦可整合現有資安產品之 Syslog 事件紀錄，作為識別特定行為之流量應處方式。

制定動態防禦清單之處理時限，可定義動態每筆處理清單有效防禦時間為48小時，逾時即解除阻斷防護。

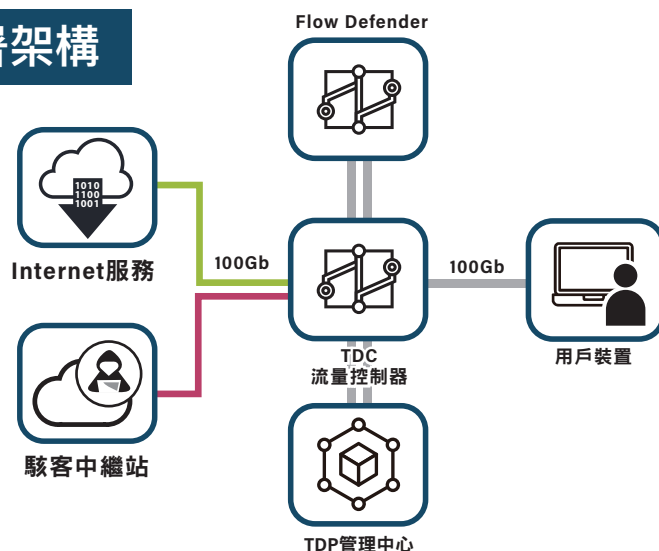
將動態防禦清單轉至常態防禦清單內，滿足資安防禦的長期防禦政策需求。



Flow Defender 聯合防禦閘道佈署架構

Flow Defender 聯合防禦閘道佈署於網路出口閘道，提供 SSL 加密圖形化管理介面制定管理政策；亦可採用 TDP 管理中心，以單一平台統一管理單位內各 Flow Defender。

此外，另可搭配 Flow Chain 智慧導流系統，強制導流內網通訊流量至 Flow Defender 執行威脅過濾，除可強化網路通訊安全外，以可有效降低網路通訊沿線穿越資安產品無謂的效能耗損，進而達成最佳化防護投資。



技術規格 | Traffic Delivery Platform

功能模組名稱	功能	說明
Flow Defender 系統功能	Negatives / Permits List 拒絕清單 / 允許清單	有害或惡意 IP 阻斷機制，過濾條件支援 IP list、IP subnet 或 IP range 或通訊協定 (protocol)。 系統最高支援 100萬筆 (含) 以上過濾能力
	拒絕清單匯入機制	提供 CSV 文件格式檔案匯入機制，清單物件化管理機制，可依據不同清單提供來源建立拒絕清單物件。 提供 Web 自動下載匯入機制，指定清單更新週期自動完成清單匯入。 提供 API 主動式匯入機制，方便整合如：SIEM等第三方即時情資，清單物件化管理機制，可依據不同清單提供來源建立拒絕清單物件。
	威脅儀表板與報表	攻擊來源/受害位址/使用者帳號 Top10 資訊。 常態性/動態威脅防禦清單總數統計。 週期性威脅統計報表。
	加密圖形化管理介面	具備 TLS V1.3 之 SSL 圖形化加密網頁管理介面
	網路流量統計顯示	即時顯示已納管之 TDC 網路控制器流量資訊，可依據其獨立通訊埠流量得知實體或虛擬化資訊系統之網路通訊流量現況，並可依據查詢結果會出相關資訊
	集中化網路管理能力	可於單一管理介面納管大量 TDC 網路控制器，設定並派送服務鏈導流政策至 TDC 網路控制器
	多租戶管理分權架構	具備多租戶階層式存取控制管理架構，系統管理員可依據不同服務或區域配置獨立管理介面，各分權管理介面可獨立設定存取控制及網路配置等相關設定
	分權管理機制	具備多種帳號分權管理群組，系統管理者可依據不同的管理帳號及群組對象套用特定管理權限
	管理稽核記錄	提供管理帳號登入管理稽核事件記錄、查詢及匯出功能
	設定檔管理	具備管理設定檔備份及還原等管理功能
Flow Defender 硬體功能	告警發送	具備 E-Mail, Syslog 等多種類型告警發送機制
	Defender-25	提供 2x25GbE SFP28 連接埠，最高支援雙向50 Gbps 即時流量處理能力。
	Defender-100	提供 2x100GbE SFP28 連接埠，最高支援雙向200 Gbps 即時流量處理能力。

