EDR 事件反應

EDR 代表端點事件偵測和反應，搭配 X-FORT 強力控管，特別針對組織內部成員在端點上的不當活動進行偵測、記錄並自動反應，減低災損與預防擴散。不論內外威脅、人為或程式，提供主動有效事件偵測與反應。傳統固定規則管理裝置可用性、可得性；卻沒辦法進一步對有權使用的用戶，有效預防外洩行為。EDR 在不犧牲業務彈性的前提下，也確保充分的安全性。

選擇模組與功能

模組	具備 EDR 模組	偵測 (Detect)	反應 (Action)
EDR 事件反應	基本外接式儲存裝置控管	• USB 儲存裝置插拔	• 禁用非註冊碟
	操作記錄	• 使用者檔案異動個數 • 外接儲存裝置寫出行為	• 啟動檔案操作記錄
	進階操作記錄	• 命令列關鍵字	
	列印裝置控管	• 列印張數	• 啟動列印控管
	共享資料夾控管	• 網路連線次數 • 子網路上傳流量 • 子網路下載流量 • 超連結關鍵字	• 阻擋連線 • 阻擋特定通訊協定連線
	通訊控管		
	傳輸控管		
	網頁控管		
	遠端功能 & 畫面擷取	• 遠端桌面連線連入/連出	
	EDR 模組	• 用戶端所在國家 • 誘餌異動	• 顯示螢幕浮水印 • 啟動螢幕浮水印反應時截圖 • Email、Teams、LINE通知警示 • 切換自適應政策 • 關機

組合偵測方法與運作方式

控管模組各自提供了偵測來源以及可選擇的反應行動，例如網路模組提供了偵測網路連線次數，可選擇的反應為阻擋連線等三項。如果具備 EDR 全部模組，偵測條件和反應可以任意組合。

實際應用說明

想像一個場景，同一天內當用戶端匯出客戶資料，用 Gmail 寄出夾帶附檔的信件，並且開始大量刪除工作檔案時；採取反應措施： 系統立即阻擋上網，並將擷取當下的螢幕畫面 ，發 LINE 通知主管。

獨立運作，有效控管

由於 Agent 安裝於受保護的端點裝置，不論與伺服器連線與否，都可獨立運作。電腦脫離公司環境，也依舊能持續偵測與自動反應，滿足遠距工作所需的安全保障。