X-FORT

動態切換政策與回應

隨著遠距辦公、行動辦公的普及，使得端點電腦處於非 IT 管理的場所;基礎建設環境差異，需要因地制宜的資安政策。依照業務內容所需的保護程度不同，彈性調整資安政策，並搭配自動切換，讓工作更為方便有效率。

一般控管政策

政策類型	說明	情境
網段政策	• 判斷電腦所在網段，自動切換套用當地網段指定政策	• 常調派於不同場區間，因兩廠區工作性質不同，依照網段切換不同資安政策
電腦政策	• 以裝置為政策套用對象，不區分登入使用者，均套用相同政策	• 多用於公用電腦，給予嚴格的控管政策
使用者政策（預設）	• 分別依群組、OU、使用者 身分指定政策，依登入使用者帳號套用權限	• 相同電腦登入不同使用者，分別套用政策，確保使用者操作記錄的可歸責性
未驗證身分政策	• 使用者未通過身分驗證，以零信任概念，套用最嚴格的管控	• 使用者用本機帳號登入，為取得有效記錄，在未驗證身分前，給予嚴格控管

（優先度為 網段政策 > 電腦政策 > 使用者政策 > 未驗證身分政策）

條件式政策

政策類型	說明	情境
動態回應 (EDR) 政策	• 偵測執行特定程式、電腦位置、使用者活動等組合條件，觸發自動切換政策或執行反應	• 偵測有異常(如：大量寫出檔案至隨身碟)，立即啟動螢幕浮水印警告，並切換嚴格政策
主管審核政策	• 由主管審核決定暫時開放控管，如外接式儲存裝置、網頁瀏覽、取消列印浮水印	• 繳交主管機關之文件需取消列印浮水印，由主管審核後開放
離線政策	• 當裝置無法與X-FORT伺服器連線時生效	• 行動辦公時，脫離公司管控環境，啟動較嚴格控管，如：關閉網芳、印表機
RDP 政策	• 被RDP連入時，限制遠端連線分享本機資源 (如：RDP分享本機磁碟)	• 在家上班使用私人電腦連入公司電腦，防止資料外流到遠端存取設備
暫時政策	• 在指定期間內生效的政策，到期自動切回原指定政策	• 出差至海外，需暫時開放

（優先度為 動態回應 (EDR) > 主管審核 > 離線政策 > RDP 政策 > 暫時政策）

動態回應偵測與反應

傳統固定規則管理，沒辦法對有權限的使用者，進一步有效預防外洩行為。EDR 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，提供主動事件偵測與反應。

EDR 對應模組	偵測 (Detect)	反應 (Action)
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
列印裝置控管	• 列印張數	• 啟動列印控管
共用資料夾控管 / 通訊控管 / 傳輸控管 / 網頁控管	• 網路連線次數 • 子網路上傳/下載流量 • 超連結關鍵字	• 阻擋連線 (HTTP/SMTP/FTP) • 阻擋特定通訊協定連線
EDR	• 遠端桌面連線連入/連出 • 用戶端所在國家 • 誘餌異動	• 顯示螢幕浮水印，並截圖 • Email、Teams、LINE通知警示 • 切換控管政策或關機