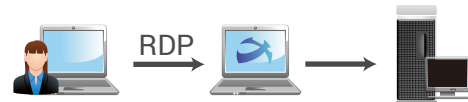


遠距工作

許多企業改變了工作型態，居家辦公、行動辦公也都成為主流，但也帶來新的資安危機。由於遠距辦公時，使用的網路環境及電腦設備，已非平常組織所建置安全保護網之下，甚至使用非公司的制式配備。端點安全是組織能夠使用的最佳安全模型之一，端點控管不論裝置在何處，都能夠實現最強固的資安政策落實。

調整控管建議

- 多層存取：導入跳板機制，外部遠端連線僅限連入組織的中繼主機，並強化身份認證
- 網路監控機制：啟動連線存取記錄、連線活動記錄、辦公區操作記錄、上網行為記錄
- 限制存取連結裝置：限制遠端連線分享本機資源、防止外流到遠端存取設備（如：RDP 分享本機磁碟）



Case 1 使用安裝 X-FORT 設備遠距工作

- 使用 VPN：直接存取公司內部環境與服務，如同在公司內工作。連入時依網段不同，套用 X-FORT 專屬政策。
- 未連 VPN：X-FORT 自動切換成離線政策，如通訊埠控管，只允許連結 VPN 通訊埠。

Case 2 使用私人電腦，連結安裝 X-FORT 設備

- 使用 RDP 連線：限制使用 RDP 遠端桌面工具存取內部資源。中繼電腦須安裝 X-FORT，政策與平時工作相同。
- 使用 VDI：X-FORT 自動啟動使用者工作階段防護，政策與平時工作相同。

X-FORT 擁有多項活動監視及存取控管手段，適用遠距工作架構變化，不論內外一起保護。

| 模組 | 說明 | Case 1 | | | | Case 2 | | | |
|---------|---|--------|----|----|----|--------|----|----|----|
| | | 禁止 | 控管 | 記錄 | 備份 | 禁止 | 控管 | 記錄 | 備份 |
| 儲存裝置控管 | ● 控管外接式儲存裝置，包含禁用、唯讀、寫出加密、寫出明文等 | V | V | V | V | V | | | |
| 裝置控管 | ● 禁用燒錄器、紅外線、藍牙、無線網卡、USB 網卡 | V | | | | V | | | |
| 列印裝置控管 | ● 控管本機、網路、分享及虛擬印表機 | V | V | | | V | | | |
| 操作記錄 | ● 軟體執行記錄 | | | V | | | | V | |
| | ● 網頁瀏覽記錄 | | | V | | | | V | |
| | ● 檔案操作記錄 | | | V | | | | V | |
| 進階操作記錄 | ● 記錄使用者複製 / 貼上剪貼簿的文字內容 | | | V | | | | V | |
| 共用資料夾控管 | ● 詳實記錄 / 備份網路芳鄰寫出 / 寫入檔案 | V | V | V | V | V | | | |
| 通訊控管 | ● 允許 / 禁止使用的通訊埠，限定使用 VPN 通訊埠 | | V | V | | V | V | V | |
| 傳輸控管 | ● 即時通訊軟體禁止執行、禁止傳檔；記錄傳訊內容、備份傳送檔案 | | | V | V | | | V | V |
| | ● 視訊會議軟體禁止執行、禁止傳檔；備份傳送檔案 | | | V | V | | | V | V |
| 軟體安控 | ● 禁用遠端連線軟體 | V | | | | V | | | |
| 特殊軟體安控 | ● 管制應用程式功能，包含列印 / 複製到剪貼簿 / 鍵盤 / 另存新檔 / 滑鼠拖曳上傳檔案 | | V | | | | V | | |
| | ● 執行特定軟體時，啟用螢幕浮水印 | | | | | | V | | |
| 畫面擷取 | ● 單一畫面擷取，如視窗切換、使用剪貼簿、Microsoft Office 另存 | | | V | V | | | V | V |
| | ● 固定間隔連續擷取，如執行特定軟體、網頁清單 | | | V | V | | | V | V |