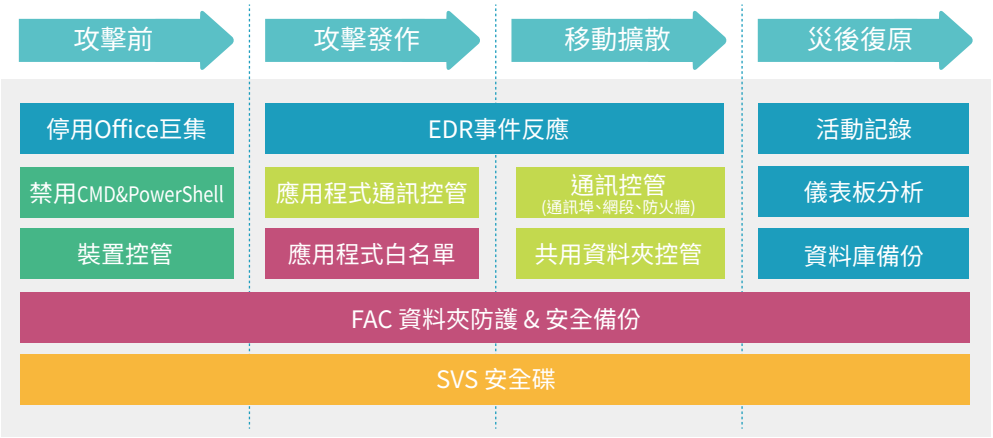
X-FORT

勒索軟體對應方案

Targeted Ransomware 透過滲透受害者內部網路，取得權限、執行特定命令，修改群組原則等方法，下載勒索病毒，並在網域內的電腦上擴散與執行。
X-FORT 端點防護不同於沙箱、特徵比對、或郵件過濾技術，透過限縮不必要的物件活動，將風險控制到最小。例如：將不使用的 AP 禁用或限制存取，進而阻絕勒索軟體的發作、擴散。
亦可搭配存取控管、檔案加密、備份機制，確保資料保護的最後一道防線；即使資料外洩或被加密，也不擔心資料被公開或毀損遺失。



應用功能一覽

攻擊階段	對應模組	功能
攻擊前	其他控管	● 硬體白名單，僅允許使用已列管的裝置
攻擊前	基本外接儲存裝置控管	● 控管外接儲存媒體，僅允許使用已註冊的裝置
攻擊前	基本系統管理	● 禁用Office巨集，避免使用者點開郵件附件，直接執行巨集
攻擊前	基本軟體安控	● 禁用各式指令軟體，如CMD、PowerShell ● 禁用各式系統工具，如WMIC
攻擊發作	進階檔案操作	● 記錄CMD及PowerShell輸入命令與執行結果
攻擊發作	通訊控管	● 應用程式通訊控管：限制應用程式連結網段目的地，防止未經授權連線存取。如限制PowerShell僅可存取內部網段，阻斷所有外部連線
移動擴散	共用資料夾控管	● 防止裝置利用網芳存取受保護的裝置
攻擊發作 移動擴散	基本軟體安控	● 資料夾防護：限定用戶端電腦的特定資料夾內的檔案，僅能被特定的軟體存取，不被惡意程式存取或竄改 – 信任應用程式：限定白名單中應用程式存取，禁止其他程式變更檔案 – 限制異動副檔名：指定附檔名類型(如 *.exe)，防止未經授權的使用者或程序，在資料夾中新增或更名該類型檔案
災後復原	基本軟體安控	● 自動備份指定資料夾檔案 (可備份資料庫檔案)
全階段	SVS安全碟	● 強制應用程式(如Word, AutoCAD)將檔案存入受保護的SVS安全碟，萬一檔案遭竊取仍為加密狀態，防止資料外洩
移動擴散 災後復原	EDR事件反應 遠端功能	● 監視及偵測檔案操作(如刪除、更名次數)、網路流量、網址關鍵字等，主動反應控制風險 ● 用戶端自動反應包含螢幕浮水印、警示、限制網路傳輸等；管理者處置包含強制關機、遠端命令等

FineArt 精品科技股份有限公司 M sales@fineart-tech.com T +886-3-5772211 A 新竹市埔頂路18號8樓