X-FORT

電子資料控管系統

控管·管理·監控·反應·稽核

www.fineart-tech.com

詳細內容

資料安全專家

X-FORT是完整的資料安全防護解決方案，包含DLP、DRM和ITAM。防止機密資訊洩漏遺失，並提供應用程式管理、電腦資產盤點及遠端遙控的管理系統。

DLP
Data Leak Prevention

DRM
Document Management

ITAM
IT Asset Management

X-FORT

DLP Data Leak Prevention

- 外接式儲存裝置控管
- MTP裝置
- 光碟裝置控管
- 列印裝置控管
- 一般裝置控管
- 共用資料夾控管
- 通訊控管
- 網頁控管
- 雲端控管
- 電子郵件控管
- 傳輸控管
- SVT伺服器安全通道

DRM Document Management

- 文件加密(SVS安全碟)
- Role-Based權限管理
- 應用程式存取文件控制

ITAM IT Asset Management

- 資產管理
- 軟體安控
- 遠端控管

UBA User Behavior Analytics

- 操作記錄
- 記錄分析/稽核

功能模組一覽

※ 規格功能可能因產品版本變更而有所調整，規格依照實際產品為主
※ 若因其他軟/硬體、作業環境異動影響功能完整度，精品將視情況提供調整建議

S:標準模組
O:選配模組

類別		功能模組	子功能	說明	選購
DLP	本機安控	基本外接式儲存裝置控管	儲存裝置	● 一般外接式儲存裝置防護，包含外接式硬碟、隨身碟、記憶卡、MP3播放器等 ● 多種控管模式：如禁用、唯讀、寫出明文/密文；密文檔案支援連線/離線解密 ● 儲存裝置註冊機制：硬體辨識、軟體辨識、序號辨識	S
			MTP裝置	● 可禁用、唯讀、開放使用MTP裝置；提供寫出、讀入、阻擋記錄，並備份寫出檔案	
			硬碟防護	● 防止使用者利用光碟、USB隨身碟開機、硬碟串接方式避開控管 ● MBR防護：保護硬碟MBR區域，不被其他系統讀取 ● BitLocker防護：中央控管方式管理Windows BitLocker	
		進階外接式儲存裝置控管		● 多種明密文寫出模式：群組解密、密碼自解檔、限期自解檔、電腦自解檔 ● 線上申請開放控管，寫出檔案需主管審核機制，主管線上審閱內容後核覆 ● 限制每日或單一檔案寫出至外接式儲存媒體的檔案大小	O
		光碟裝置控管		● 可禁用光碟機及燒錄軟體 ● X-BURN燒錄：燒錄明文/密文，完整的燒錄記錄及警示；提供主管審核機制，審核後燒錄光碟	O
		列印裝置控管		● 可控管本機、網路、分享及虛擬印表機，設定不同的列印政策 ● 不限應用程式或印表機，強制列印浮水印 ● 列印文件可控管張數、警示，備份列印內容或原始檔案，檔名含特定關鍵字發出警示 ● 提供主管審核機制，可申請暫時開放印表機或取消浮水印	O
		操作記錄*1	系統檔案	● 記錄系統檔案刪除及檔名異動 (含命令模式下操作)	O
			使用者日誌	● 記錄軟體執行活動 、網頁瀏覽活動 ● 記錄用戶端電腦的登入/登出事件 ● 記錄檔案操作行為，包含檔案建立、複製、搬移、更名與刪除	
		進階操作記錄		● Microsoft Office 檔案存取記錄：開檔、存檔、另存的操作記錄 ● 剪貼簿文字記錄：使用者複製、貼上剪貼簿的文字內容 ● CMD及PowerShell命令執行記錄，執行結果記錄和執行警示	O *1 Req.
		其他控管		● 通訊埠及工具防護：紅外線、藍牙、傳輸線軟體、PrtScr鍵、定位服務、行動裝置同步軟體、遠端遙控軟體、Ghost軟體、VMware軟體、P2P軟體、登錄編輯器、音效卡、無線網卡、USB連接的網卡 ● 一般裝置控管：可禁用Windows【裝置管理員】中的一般裝置	O
		X-DISK		● 個人化的加密虛擬碟，存放個人重要的機密檔案，不同人員共用電腦，也可各自保有私有的空間，並記錄使用者對X-DISK的操作行為	O
	網路安控	共用資料夾控管		● 使用者和外來電腦間的共用資料夾傳輸檔案，可加以禁止、記錄、備份 ● 監視共用資料夾的讀取流量、刪檔數目，達到上限時發出警示及e-mail	O
		通訊控管		● 內/外通訊埠防護；提供主管審核機制，允許申請暫時開放通訊埠 ● 應用程式連線控管：限制應用程式連結網段目的地、通訊埠，防止未經授權連線存取 ● 網段流量控管：限制可存取目的網段流量，分別控管上傳量與下載量	O
		網頁控管*2		● 禁止或允許瀏覽HTTP或HTTPS網址 ● 瀏覽記錄包含搜尋關鍵字、標示連結目的地國家 ● 網頁特殊控管功能：符合指定網址時，禁止瀏覽器的開啟舊檔、另存、列印、鍵盤、複製、貼上、拖曳出/入網頁等功能 ● WebPost控管：可記錄或禁止網頁的POST/PUT上傳行為 ● 網路流量監測：提供每日上傳/下載的資料流量上限警示 ● 提供主管審核機制，允許申請暫時開放網頁瀏覽	O
		網頁文字記錄		● 指定網址清單(含HTTPS)擷取文字內容作為記錄	O *2 Req.
		Webmail記錄		● 記錄Outlook.com, Yahoo! Mail, Gmail的Webmail郵件包含主旨、收件者、內容、附檔名稱	O *2 Req.
		雲端控管		● 控管應用程式使用SSL/TLS網路連線，包含雲端硬碟同步軟體 ● 依網址關鍵字阻擋連結雲端硬碟 ● 複製檔案至雲端同步資料夾即自動加密 ● 防止Office另存到雲端硬碟	O *2 Req.
		傳輸控管		● 即時通訊軟體可禁止執行、禁止傳檔、禁用截圖、禁用桌面分享；記錄傳訊內容、備份傳送檔案&截圖內容 (Line, Skype, Skype for Business, WhatsApp, Tencent QQ, WeChat, 阿里旺旺) ● 視訊會議軟體可禁止執行、禁止傳檔；記錄與備份傳送檔案 (Zoom, Webex Meetings, Webex Teams, 釘釘, BlueJeans, GoToMeeting, Slack, Chatwork, Microsoft Teams, Telegram, Viber) ● 可禁止或控管FTP/FTPS的上傳/下載行為，含記錄與備份 ● 可控管3G/4G網卡的撥接軟體 ● 禁用分享網路(行動熱點) ● 無線網路基地台控管與連接記錄	O
		電子郵件控管*3		● 限制可使用的外寄SMTP郵件伺服器寄送郵件 ● 記錄及備份使用者寄送的郵件 ● 支援Notes與Outlook控管	O
		Outlook 附檔加密		● 自動加密：依收件者自動判斷，將Outlook信件的附檔加密後寄出 ● 寄送審核：附檔加密的信件先寄給群組管理員，核覆後寄出密碼 ● 禁止寄送清單：指定禁止寄送的網域名稱或關鍵字，如任一收件者email符合，自動阻擋該信件 ● 防止誤寄郵件：按下傳送時，提示使用者再度確認，防止不慎將郵件寄給錯誤的收件者	O *3 Req.
		SVT 伺服器安全通道		● 安裝X-FORT Agent的電腦，才能存取受保護的伺服器 ● 指定的使用者或部門，透過身分驗證才能連結受保護的伺服器 ● 電腦與受保護伺服器之間的通訊加密，防止網路監聽、竊取機密資料 ● 保護對象不限服務類型，支援TCP通訊，不需額外設定或撰寫程式碼	O

類別		功能模組	子功能	說明	選購
ITAM	軟體安控	基本軟體安控	應用程式控管	● 清查電腦硬碟內的執行檔，建立白名單 ● 規則比對應用程式屬性，支援應用程式簽章的憑證、檔案雜湊、檔名、路徑，支援父行程關係定義 ● 動態白名單管理，支援觀察模式，執行記錄方便快速建立規則	O
			資料夾防護	● 限制特定資料夾中特定副檔名的檔案(如*.exe)，防止未經授權的使用者或程序，在該資料夾中新增、更名特定副檔名的檔案 ● 限制用戶端電腦中特定資料夾內的檔案，只能被指定的信任程式存取，確保資料夾內的資料，不被其他非授權程式存取，或加入檔案	
			軟體執行控管	● 記錄使用者禁止或非允許的軟體執行；依時段管理禁止或允許執行軟體 ● 提供主管審核機制，允許申請暫時開放使用軟體	
			安全備份	● 定時自動備份資料夾，並限制應用程式存取備份目的，確保備份安全 ● 搭配資料夾防護，確保備份目錄不被破壞	
		特殊軟體安控	● 軟體執行時，管制特定功能，禁止開啟舊檔、另存、列印、鍵盤、複製、貼上、拖曳出/入程式 ● 軟體執行時或永久啟動螢幕浮水印，文字可選擇漸層效果，不易被背景色屏蔽		
	資產管理	軟體資產*4	授權管理	● 管理軟體資產、軟體採購 ● 提供套裝軟體整合、軟體別名分類、軟體降級權管理 ● 自動/手動分配軟體授權及統計未授權軟體，可回收軟體授權再重新分配 ● 系統管理員依組織、部門劃分授權數量，由群組管理員分配授權數量	O
			軟資異動管理	● 軟體的安裝或移除異動，記錄及警示系統管理人員及群組管理員 ● 遠端移除軟體：遠端移除使用者已安裝的軟體 ● Hotfix資訊：蒐集並管理電腦的Hotfix資訊，可線上更新/移除指定Hotfix ● 機碼資訊：顯示用戶端電腦中指定的機碼	
		CPE軟體描述	● 軟體資產比對CPE字典，比對結果輸出Excel或JSON檔案，以供弱點資料庫查詢	O *4 Req.
		硬體資產	● 硬體資產管理：管理硬體資源、硬體採購、設備管理、設備盤點 ● 硬體異動警示：硬體裝置有異動時警示，及硬碟空間超過設定值時警示 ● 電腦採購與盤點：管理電腦設備的生命週期，比較與撥發時的差異	O
	遠端管理	遠端功能	● 線上管理用戶端的本機帳號新增、修改、刪除、啟用、停用、權限變更 ● 可對用戶端電腦送出喚醒、登出、重開機、關機命令或廣播訊息 ● 支援立即派送、排程派送、檔案續傳、傳輸頻寬管理、種子電腦派送功能 ● 提供線上服務功能，可遠端檢視或遙控使用者電腦，線上叫修後提供滿意度問卷調查 ● X-Monitor支援多螢幕(GridView)監控，部門主管可即時監看部屬的電腦畫面	O
		畫面擷取	● 單一畫面擷取，如視窗切換、使用剪貼簿、Microsoft Office操作時 ● 固定時間間隔連續擷取，如執行特定軟體、網頁清單 ● 可自訂影像品質、解析度、顏色及間隔時間條件 ● 矩陣瀏覽(GridView)畫面記錄；匯出單張畫面圖檔，或連續畫面影片檔	O
DRM	文件控管	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 ● 使用者可自行選擇文件加密類別，不同類別的文件，人員可各別設定存取權限 ● 控管螢幕擷圖、剪貼簿、另存雲端硬碟，限制檔案在安全碟內使用，防止檔案洩漏 ● 記錄安全碟的操作，如建立、掛載、卸載、匯出明文 ● 當使用者掛載SVS碟時，可依角色顯示螢幕浮水印 ● 提供主管審核機制，允許匯出明文	O
		DEC文件加密中心	● 將檔案伺服器指派為文件加密中心，文件放入共用的網芳資料夾，即會依資料夾指定的SVS類別，自動加密成SVS檔案	O
SYSTEM	基本系統管理	用戶端	● 多重連鎖自我防護，防止惡意移除 ● 支援作業系統安全模式下的控管與記錄 ● 當用戶端異常或出現不明電腦時，系統自動發出警示	S
		伺服器&控制台	● 單一伺服器可管理1,000台以上用戶端電腦 ● 採用PKI 1,024bits公開金鑰加/解密機制及AES 256bits加密演算法；支援HSM金鑰管理 ● 資料庫備份：支援完整備份、差異備份、排程備份；同時還原檢視多個資料庫 ● 多種管理者角色：系統管理員、系統稽核員、群組(部門)管理員及自定義角色	
		記錄分析	● 記錄查詢結果根據管轄範圍分權，不同管理者顯示不同結果，避免權限擴張 ● 依人員、日期範圍查詢記錄，以時間軸順序排列查詢記錄 ● 依關鍵字查詢多人(或全部)、各類別相關記錄 ● 搭配整合查詢記錄及寄送報表，設定排程自動寄送報表給管理員	
		儀表板	● 提供Web介面設定儀表板，組合多種記錄於同一頁面，一次掌握多種圖表狀況 ● 儀表板支援表格、橫條圖、直條圖、圓餅圖、折線圖、樞紐分析表、文字雲、地圖等	
	進階系統管理	進階伺服器(多重伺服器)	● 支援手動/自動調整負載平衡與備援機制；伺服器斷線，用戶端自動尋找備援伺服器 ● 依網段指派用戶端的管轄伺服器 ● 信任伺服器間，可交換加密金鑰，使用加密檔案 ● Relay Server機制，各自儲存備份檔案，只將記錄回傳至主伺服器	O
EDR	EDR事件反應	行為偵測與反應	● 監視及偵測違規行為，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、禁用隨身碟、禁用印表機等；管理者可遠端執行命令(如強制關機、遠端命令等)、復原用戶端發生之自動反應 ● 自適應政策：透過EDR組合偵測執行特定程式、電腦所在位置等組合為偵測條件，條件觸發自動切換控管政策 ● 記錄各種違規事件、反應動作與處置方式	O

本機安控

外接式儲存裝置控管

針對外接式儲存裝置控管，只有儲存媒體受到影響，其他裝置不受影響。如鍵盤內含記憶卡，僅記憶卡受到控管，不影響鍵盤使用。

在管控USB外接式儲存裝置中，X-FORT提供多種控管模式，包含完全禁止、唯讀（Read only）、寫出明文/密文、審核寫出...等，最多樣的控管方式，提供企業內不同工作性質與人員階層的彈性管理。

控管各種介面儲存媒體，範圍包含：

- 各式USB裝置的儲存媒體：USB隨身碟、手機、MP3播放器、記憶卡（CF, MS, MMC, Micro SD, SD, XD）、外接式硬碟、磁片、數位相機、PDA...等。
- 透過各種介面連接本機的儲存裝置，SATA、IDE等會產生磁碟機代號皆在控管範圍內。

支援最多種寫出模式

提供以下多種檔案寫出模式，並可將寫出檔案備份至X-FORT伺服器。

<table>
<tr><td>完全禁止</td><td colspan="3">對於任何連接本機的儲存媒體，都禁止讀取或寫出。</td></tr>
<tr><td>唯讀</td><td colspan="3">允許外接式儲存媒體內的資料讀入電腦，但不允許電腦內的資料寫出至外接式儲存媒體。</td></tr>
<tr><td rowspan="4">密文寫出</td><td>離線解密
(AES加解密)</td><td colspan="2">寫出的密文檔案，在安裝X-FORT Agent的電腦上均可解密，無需與X-FORT伺服器連線。</td></tr>
<tr><td>連線解密
(PKI機制加解密)</td><td colspan="2">應用於檔案在公司內部流通，寫出的檔案以密文方式寫出，將檔案拖回裝有X-FORT Agent的電腦，且電腦與X-FORT伺服器有連線時可自動解密。</td></tr>
<tr><td>群組解密*</td><td colspan="2">寫出的密文檔案可預設指定的群組人員可以解密，用於控管加密檔案在企業內流通時，指定的群組人員才能解密。</td></tr>
<tr><td>審核寫出*</td><td colspan="2">審核寫出密文需經主管審核批准，才可寫出密文檔案至外接式儲存裝置；搭配寫出記錄、寫出檔案實體備份和審核記錄，可事後稽核備查。</td></tr>
<tr><td rowspan="7">明文寫出</td><td>允許寫出明文時間</td><td colspan="2">設定特定允許的寫出時間，在時間範圍內，擁有寫出明文檔案的權限；超過允許的寫出時間，將自動恢復為原權限。</td></tr>
<tr><td rowspan="5">永久允許寫出明文</td><td colspan="2">與原本操作方式完全相同，可以寫出明文檔案，適用於高階主管或特定人員。並可設定在寫出資料時需輸入密碼驗證，再次驗證身分，避免有其他人借用其電腦時，將資料取走。以下自解檔使用AES技術加密，且解密後將不再受到X-FORT控管。</td></tr>
<tr><td>ZIP加密檔</td><td>將寫出的明文檔壓縮成為ZIP檔格式，之後使用一般的ZIP解壓縮程式並輸入密碼，即可解開此檔案。(可以多個寫出檔案自動壓縮成同一檔案)</td></tr>
<tr><td>密碼自解檔*</td><td>以密碼保護的自解檔。</td></tr>
<tr><td>限期自解檔*</td><td>檔案通過密碼驗證，並在規定時間內，才能解密為明文檔。</td></tr>
<tr><td>電腦自解檔*</td><td>檔案必須在指定的電腦中解密。</td></tr>
<tr><td>審核寫出*</td><td colspan="2">需經主管審核批准，才可將明文檔案寫至外接式儲存裝置；搭配寫出記錄、寫出檔案實體備份和審核記錄，可事後稽核備查。</td></tr>
</table>

線上申請開放控管*

提供主管審核機制，使用者可申請暫時開放外接式儲存裝置；審核許可後，在開放時間內允許讀取及寫出外接式儲存裝置。搭配寫出記錄、寫出檔案實體備份和審核記錄，可事後稽核備查。

* 需搭配進階外接式儲存裝置控管使用

檔案寫出記錄&備份

- 記錄各用戶端電腦檔案外接裝置寫出活動，包括寫出檔案日期、網域、使用者、部門、電腦名稱、寫出方式、寫出類型（明文或密文）、來源檔名、檔案大小、儲存檔案、寫出電腦和原因備註等資料欄位。
- 儲存寫出檔案，檢視記錄時可開啟檔案內容。

外接式儲存裝置註冊機制

可將隨身碟、指紋碟、市售的外接式儲存裝置(如外接硬碟)等在X-FORT伺服器上註冊，並且只允許註冊過的外接式裝置可被存取使用，其他未經註冊者，將無法使用。支援類型包含：

- 硬體辨識註冊：讀取裝置上的Hardware ID註冊，同批號的裝置只需註冊一次即可，較其他方式便利。
- 軟體辨識註冊：寫入特定識別資訊到外接儲存媒體上，若重新註冊資訊會有所不同。
- 序號辨識註冊：讀取裝置序號註冊，序號具唯一性，需逐一個別註冊。

MTP裝置

媒體傳輸協定MTP(包含PTP)讓行動裝置可以傳輸檔案，是Windows Media功能的一部份。隨著行動裝置的普及，MTP已經被廣泛應用，作為智慧型手機的預設傳輸模式，數位相機、MP3和MP4播放器都已支援MTP協定。除了原本的「裝置控管功能」可用來禁用MTP裝置外，還支援記錄、備份與警示功能。

- 使用模式

禁止使用	不能讀、寫MTP裝置裡的檔案
唯讀使用	可將行動裝置裡的檔案複製到電腦，反向則不行
可讀寫	不限制使用MTP裝置

- 記錄&備份：使用檔案總管在MTP裝置上讀入或寫出，記錄檔案名稱和備份檔案。
- 警示功能：使用者將檔案寫出至MTP裝置時，可發送警示訊息給群組管理者或系統管理者。

硬碟防護

X-FORT系統可啟動有效磁碟的「硬碟防護」功能，即便使用者以磁片/光碟片開機，或將受保護的硬碟串接至另一台電腦內，均無法存取到受保護硬碟內的資料。受保護的硬碟只在X-FORT Agent的電腦在正常開機時才能存取，如此一來，將可保障硬碟失竊或被有心人士任意取走時，硬碟內的資料不會外洩。

- MBR硬碟防護 (只適用2TB以下的MBR硬碟，不支援NVMe SSD)
  - 透過修改硬碟的MBR區域，使得必須要在有X-FORT Agent下，才可正常存取。
- BitLocker硬碟防護 (可支援MBR/GPT格式的大容量硬碟及SSD)
  - 以中央控管方式啟動BitLocker功能，開機後X-FORT Agent自動將磁碟解鎖。
  - 自動接管系統內的BitLocker功能，重新產生密碼並置換。電腦開機後，X-FORT Agent會自動帶入密碼解鎖，使用者不需自行輸入密碼。
  - 支援TPM晶片加密開機磁碟，開機時自動解鎖。(無TPM晶片需手動輸入密碼；Windows 7不支援TPM解鎖)
  - 提供救援機制，救援金鑰加密儲存在資料庫中，萬一發生問題時可取回解鎖或解密。

	MBR硬碟防護	BitLocker硬碟防護
保護對象	實體硬碟	分割磁碟
資料加密	無	有
救援金鑰	無	有
支援硬碟格式	MBR	MBR/GPT
支援OS	• 所有X-FORT支援的Windows OS	• Windows 7 企業版/旗艦版 • Windows 8/8.1 專業版/企業版 • Windows 10 專業版/企業版/教育版

光碟裝置控管

記錄 審核 備份

禁用光碟機、燒錄機

禁止使用任何光碟機或燒錄機。建議可用於不需使用光碟機或燒錄機的員工，即使私接光碟機或燒錄機也無法使用。

禁用燒錄軟體

可唯讀使用光碟機，但不允許燒錄，適用於配有燒錄機的電腦。

X-BURN

X-BURN為X-FORT獨有之內建燒錄工具，具有以下功能。

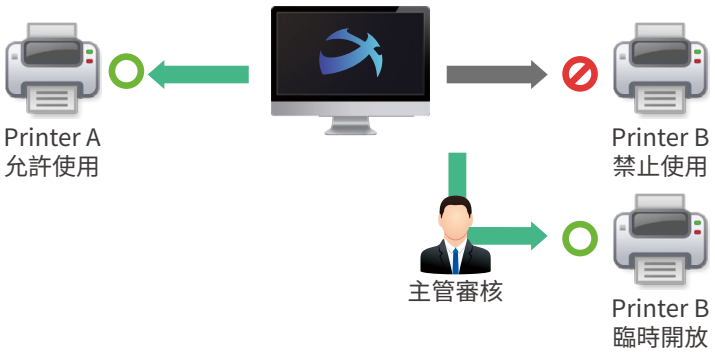
- 記錄&備份：燒錄時，可將燒錄檔案備份至X-FORT伺服器，供事後稽核。
- 燒錄檔案警示：燒錄檔案時，檔名含特定關鍵字，自動提出警示。
- 線上申請開放燒錄：提供主管審核機制，使用者可申請暫時開放燒錄，主管檢閱檔案後許可。使用者只可燒錄申請時的檔案，若原本燒錄檔案已被修改，需重新提出申請。
- 燒錄內容：
  - 視需求將檔案燒錄為明文或密文。
  - 燒錄明文時，可指定燒錄的檔案類型格式，包含純明文檔、自解檔、ZIP檔等6種類型。

列印裝置控管

包含禁止列印、強制浮水印、暫時開放印表機，並記錄列印內容，多項控管模式，讓管理更彈性，並具備事後追查的功能。支援實體印表機、網路印表機、分享印表機、虛擬印表機。

列印控管

- 限制用戶端使用未控管的印表機。
- 限制每日列印頁數上限。



線上申請開放列印

提供主管審核機制，用戶端可申請暫時開放列印的印表機，或允許暫時取消浮水印列印的權限。

浮水印功能

- 提供7種浮水印樣式可供挑選，支援空心/實心字、濃淡調整，不干擾列印內容。
- 支援巨集參數，可顯示部門、使用者、日期時間等。
- 支援特殊編碼，事後隱密反查原列印記錄及備份。

記錄&備份

- 列印記錄：記錄使用者所有文件列印事件，部門主管或IT人員可透過記錄評估是否啟動印表機控管。
- 備份列印內容：
  - 用戶端電腦在列印時，備份支援備份為列印圖檔，事後重新列印還原當時列印實際頁面。
  - 選擇備份列印的原始檔案，不論列印頁數，皆備份整個檔案。

警示

- 列印檔案警示：當用戶端所列印的文件或檔案符合檔案過濾表(檔名關鍵字)的設定條件時，發出警告通知。
- 列印張數警示：列印張數超過設定值時，發出警告通知。
- 檔案過濾表：IT人員可設定檔案過濾項目，當有符合過濾條件文件被列印時，X-FORT系統會自動發出警示通知。

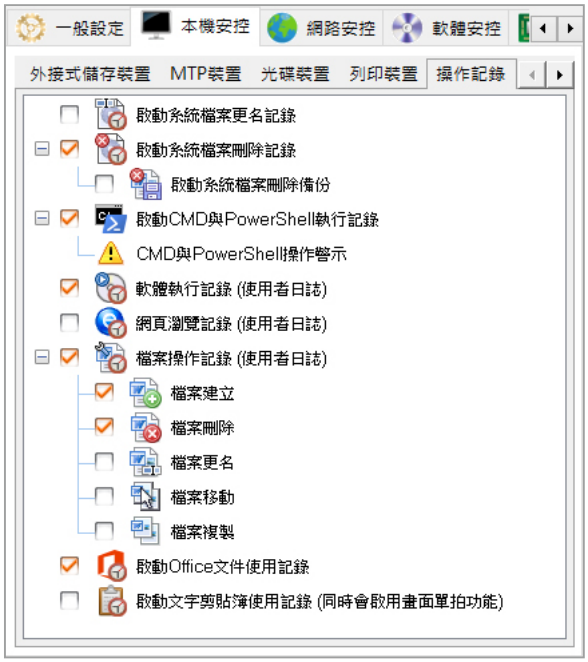
操作記錄

啟動系統檔案更名/刪除記錄

- 系統檔案名稱異動，記錄更名前後的相關資訊。
- 系統檔案被刪除，可記錄與備份被刪除的檔案。

使用者日誌

- 軟體執行記錄：使用者執行軟體時，或執行軟體視窗標題名稱有所變動時，都會記錄下來。
- 網頁瀏覽記錄：當瀏覽器Chrome, Edge, IE, FireFox視窗標題變動時，會記錄視窗標題與網址。
- 檔案操作記錄：記錄透過檔案總管對檔案的操作細節。應用範圍包含本機、網路芳鄰、外接式儲存裝置等。對於建立、刪除、更名、移動、複製檔案，均會留下詳細的記錄。



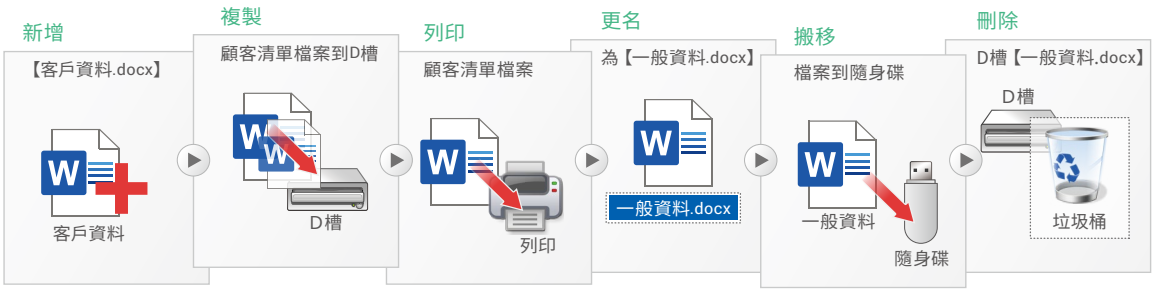
進階操作記錄

Microsoft Office檔案存取記錄

使用Microsoft Word, Excel, PowerPoint, Visio應用軟體執行開檔、存檔、另存新檔時，操作的日期、時間、使用者、電腦資訊，以及檔案的來源與目的檔名都完整的記錄。

剪貼簿文字記錄

記錄使用者複製/貼上剪貼簿的文字內容。



CMD及PowerShell記錄

CMD與PowerShell是作業系統預設功能，利用執行指令可以啟動提權、複製/合併檔案操作、螢幕截圖、上傳檔案等，演變成隱性資安漏洞。

- 蒐集CMD及PowerShell執行指令與輸出文字記錄，供事後調查、追溯。
- 設定警示指令表，使用者執行符合的指令時，發送mail給群組管理者或系統管理者。

其他控管

特定裝置控管

可針對特殊項目做控管，禁用對象包含：

- 紅外線 (IrDA)
- 螢幕擷取鍵 (PrtScr)
- 遠端遙控軟體
- SHARE軟體
- 禁用USB連接的網卡
- 傳輸線軟體
- PrtScr按鍵使用記錄
- Ghost軟體
- 登錄編輯器
- 禁用光碟機
- 藍牙(Bluetooth)裝置
- 定位服務
- VMware軟體
- 音效卡
- 藍牙(Bluetooth)傳檔
- 行動裝置同步軟體
- P2P軟體
- 無線網卡

一般裝置控管

面對日新月異的周邊裝置，為強化裝置控管功能，針對Windows「裝置管理員」中一般裝置開放或禁用；管理者也可自行新增或遠端匯入欲控管的裝置項目。

X-DISK

記錄

X-DISK為一套虛擬磁碟產生工具，具本機管理員權限的使用者 (Local Administrators)，即可新增與掛載虛擬磁碟。藉由X-DISK所提供的功能，即使不同人員共用電腦，也可以各自保有私有的空間。由於X-DISK虛擬磁碟本身已加密保護，即使虛擬磁碟被複製，或硬碟被串接到其他裝置，也不用擔心機密檔案外流。為保護公司資產，部門主管可掛載閱覽所屬人員的X-DISK。

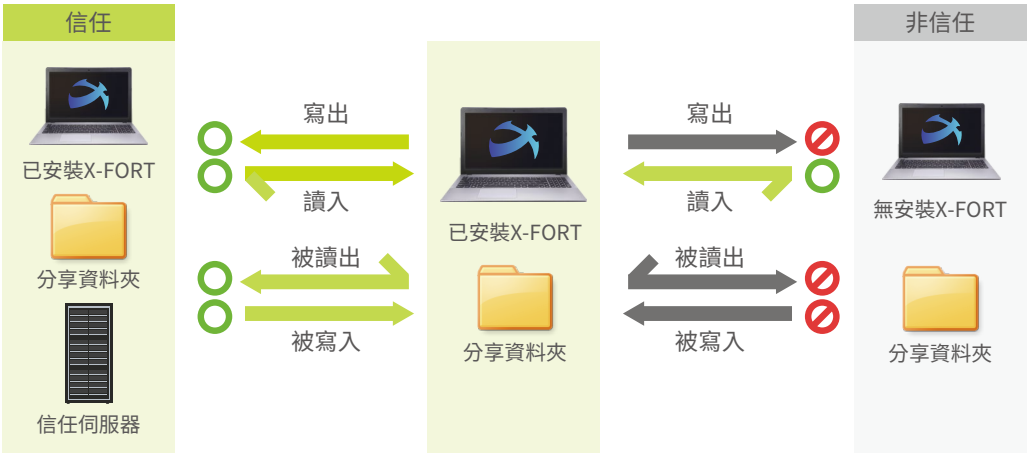
	共用電腦虛擬碟掛載前		共用電腦虛擬碟掛載後	
	C 槽	D 槽	由C槽劃分出X虛擬碟 (擁有者為員工A)	由D槽劃分出Y虛擬碟 (擁有者為員工B)
員工A	可讀寫	可讀寫	可讀寫	不可讀寫
員工B	可讀寫	可讀寫	不可讀寫	可讀寫
部門主管	可讀寫	可讀寫	可讀寫	可讀寫

網路安控

共用資料夾控管

共用資料夾存取機制

- 控管寫出：使用者電腦無法透過共用資料夾，將檔案寫出至無安裝X-FORT Agent的電腦或非信任電腦。
- 控管讀入：使用者電腦可由其他無安裝X-FORT Agent的電腦或非信任電腦，透過共用資料夾讀入檔案到本機。
- 寫出/寫入檔案名稱符合過濾條件時，顯示警告視窗給使用者、群組管理者，或發送mail給系統管理者。
- 阻止無安裝X-FORT Agent的電腦，透過共用資料夾存取（包含寫出或寫入）已安裝X-FORT Agent的電腦。



記錄 & 備份

- 共用資料夾寫出/寫入都有詳實記錄，也可選擇將寫出/寫入檔案備份到X-FORT伺服器備查。
- 信任電腦可排除不記錄；或只記錄關注電腦，其他電腦不記錄。

刪檔與流量監測警示

- 監測指定的共用資料夾讀取流量與刪檔數目，達到上限時發出警示及mail給群組管理者或系統管理者。

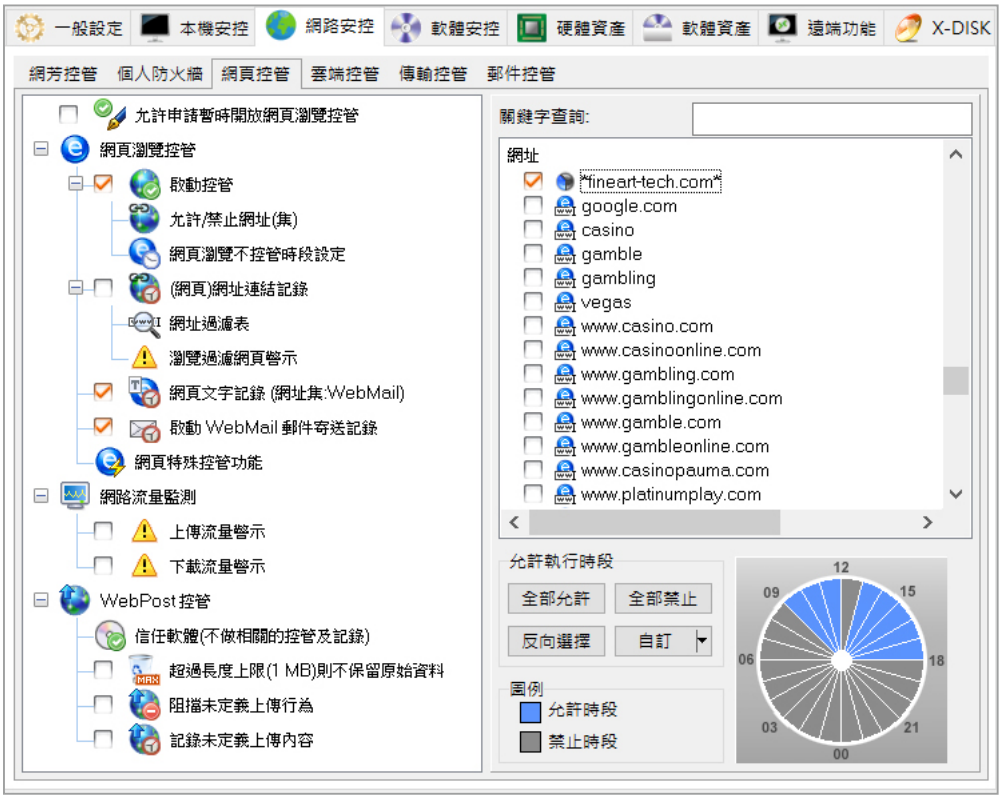
通訊控管

- 可以管制每一台電腦的TCP/IP通訊埠。系統已內建RFC（Request For Comments）規範的所有標準通訊埠，必要時可以新增自訂的通訊埠列表。可設定允許/禁止使用的通訊埠，或設定此通訊埠可使用時段（例如：午休時間）。並提供主管審核機制，用戶端可線上申請暫時開放通訊埠控管。
- 應用程式連線控管：限制應用程式連結網段目的地、通訊埠，防止未經授權連線存取。不論連線成功、失敗皆可留記錄。
- 網段流量控管：限制可存取目的網段流量，分別控管上傳量與下載量。分別上傳與下載事件，超過限制量發出示警、暫停使用網路。

網頁控管

控管用戶端的網頁瀏覽行為，功能包括：

- 允許或禁止瀏覽的HTTP/HTTPS網址，並記錄阻擋的行為。
- 支援Chrome, Edge, IE, FireFox, Opera, SlimBrowser, Maxthon, Yandex, Brave, WaterFox, QQ等瀏覽器的網址連結記錄。瀏覽記錄包含搜尋關鍵字、標示連結目的地國家。(瀏覽器大多基於知名引擎開發，行為相近，不在上述瀏覽器，也可能留下連結記錄)
- 特殊控管：在使用瀏覽指定網址時，可控管功能如禁止瀏覽器的開啟舊檔、另存、列印、鍵盤、複製、貼上、拖曳出/入網頁等功能，以阻絕潛在的外洩風險。
- 網路流量監測：使用者每日所需上傳/下載總流量為監測值，當超過流量時，發出警示通知群組管理者或系統管理者。
- WebPost控管機制：可記錄或禁止網頁的POST/PUT上傳行為。
- 線上申請網頁瀏覽：用戶端可申請暫時開放網頁瀏覽，主管審核後放行。



網頁文字記錄 (必須搭配網頁控管模組使用)

- 指定網址清單，擷取網頁文字作為記錄內容。(包含HTTPS的網頁)
- 使用者在瀏覽網頁時，記錄網址、標題與網頁文字，做為查詢關鍵字的依據，例如：OneDrive, Facebook…等。

Webmail記錄 (必須搭配網頁控管模組使用)

常用的Outlook.com, Yahoo! Mail, Gmail的Webmail，以mail的型式記錄，包含主旨、收件者、副本(Cc)、密件副本(Bcc)、附件名稱及信件內容，讓管理者一目了然。

雲端控管 (必須搭配網頁控管模組使用)

控管雲端硬碟服務，提供「阻擋/開放個別雲端硬碟的使用」；針對Google Drive, OneDrive, Dropbox雲端硬碟同步資料夾提供「自動檔案加密」，其他雲端服務可利用HTTPS連線彈性管理。

- 控管連線軟體：分別控管可使用的連線軟體，包含雲端硬碟同步軟體。
- 控管SSL/TLS網路連線：將軟體設為放行或禁止SSL/TLS連線；連線行為均保存詳細記錄，提供資安稽核用。
- 限制瀏覽：使用瀏覽器時，當瀏覽的網址符合禁用的關鍵字時，會被阻擋。
- 控管Office：可以阻擋Microsoft Office直接將檔案存到OneDrive雲端硬碟。
- 自動檔案加密：使用者將檔案複製到「雲端硬碟同步資料夾」時，可將檔案自動加密後，同步至雲端。同時需搭配關閉瀏覽器上傳功能，以阻擋明文檔案透過瀏覽器上傳。

傳輸控管

即時通訊與視訊會議軟體控管

- 即時通訊軟體可禁止執行、禁止傳檔、禁用截圖、禁用桌面分享；記錄傳訊內容、備份傳送檔案 & 截圖內容。
- 視訊會議軟體可禁止執行、禁止傳檔；記錄與備份傳送檔案。
- 其他軟體可透過軟體安控模組禁用，或禁止透過檔案總管開啟或拖拉之檔案傳輸行為。

FTP控管

- 限制連線的FTP/FTPS站台，控管上傳/下載行為，允許的傳輸行為可記錄、備份檔案。

撥接軟體&無線基地台控管

- 禁用3G/4G網卡的撥接軟體，避免脫離內部網路管制。
- 禁用分享網路(行動熱點)。
- 連接無線網路時，中斷其他網路連線，避免跨網連線傳輸。
- 依SSID & MAC設定合法的無線AP，確保電腦無法連上私接或偽裝的無線AP。

軟體		禁用	記錄傳訊	檔案傳輸			禁用分享桌面	截圖		版本鎖定
				禁用	記錄	備份		禁用	記錄	
即時通訊	LINE	O	O	O	O	O	O	O	O	O
	Skype / Skype for Business									
	Tencent QQ									
	WeChat									
	阿里旺旺									
	WhatsApp						N/A			
視訊會議	Zoom	O	X	O	O	O	X	X	X	X
	Webex Meetings / Webex Teams									
	釘釘									
	BlueJeans									
	GoToMeeting									
	Slack									
	Chatwork									
	Microsoft Teams									
	Telegram									
	Viber									
其他		O	X	O	X	X	X	X	X	X

O：支援 / X：未支援 / N/A：無此功能

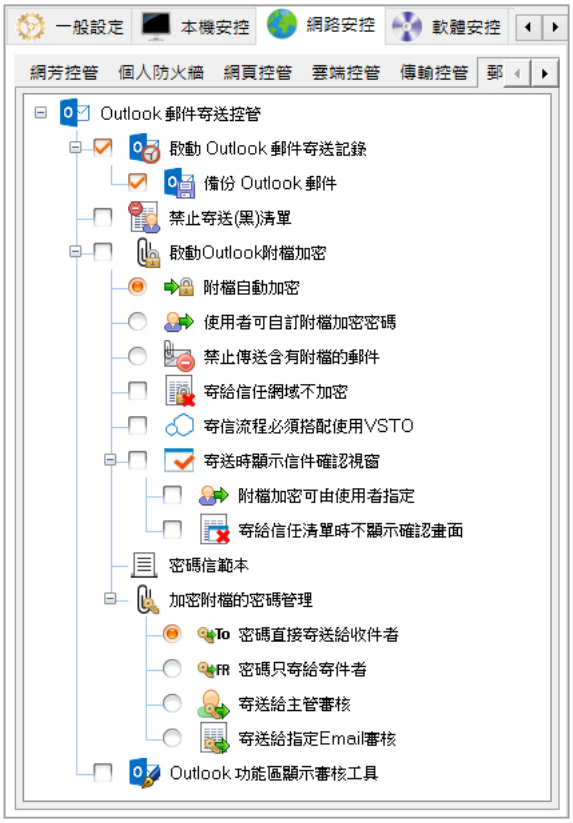
電子郵件控管

防止員工利用非公司認可的郵件伺服器發信，造成控管或防護上的漏洞，X-FORT限制用戶端只能使用公司認可的外寄郵件伺服器。記錄透過SMTP協定、Lotus Notes與Outlook傳送的電子郵件，並可備份這些郵件備查。

Outlook 附檔加密

(必須搭配電子郵件控管模組使用)

整合Outlook，提供簡單人性化的精靈，引導使用者寄出附檔加密的信件。搭配實際操作需求，可選擇自動寄出密碼給寄件者或收件者。



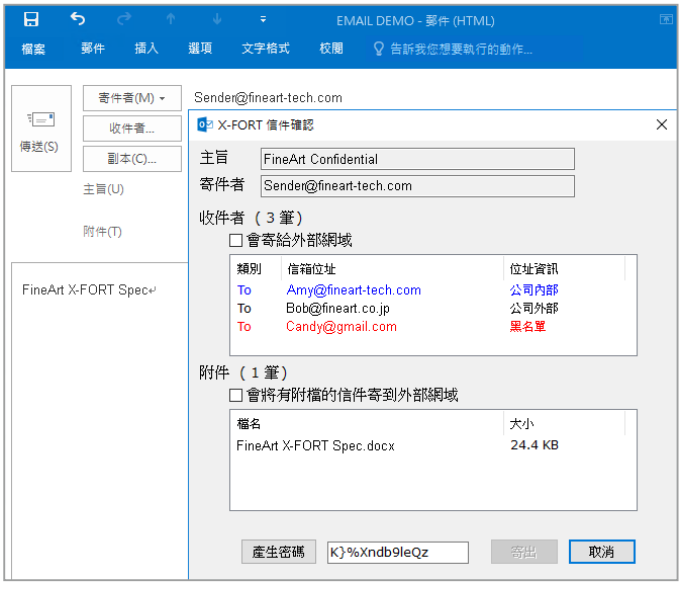
收件者管理

依寄送對象可分為白名單(如：內部名單、允許放行名單)或黑名單，其中黑名單可指定網域名稱(如gmail.com)或關鍵字。當使用者使用Outlook按下寄送時，若收件者包含黑名單，則信件無法送出，阻擋的事件也會產生相關記錄。

白名單	全部收件者為白名單，可設定不加密附件寄送
灰名單	收件者中包含任一未定義的收件者，即啟動附檔控管機制
黑名單	任一收件者為黑名單，且信件含有附件則無法寄送

主管審核

使用者在寄送附件時，無法確定是否可以提供給客戶，可將檔案寄送給群組管理者，或指定審核人員放行後，才寄出給外部；密碼由系統產生自動寄送給寄件者，再由寄件者寄送給收件者。



密碼複雜度

由系統產生或使用者自訂的密碼，須符合系統密碼複雜度原則。

防止誤寄郵件

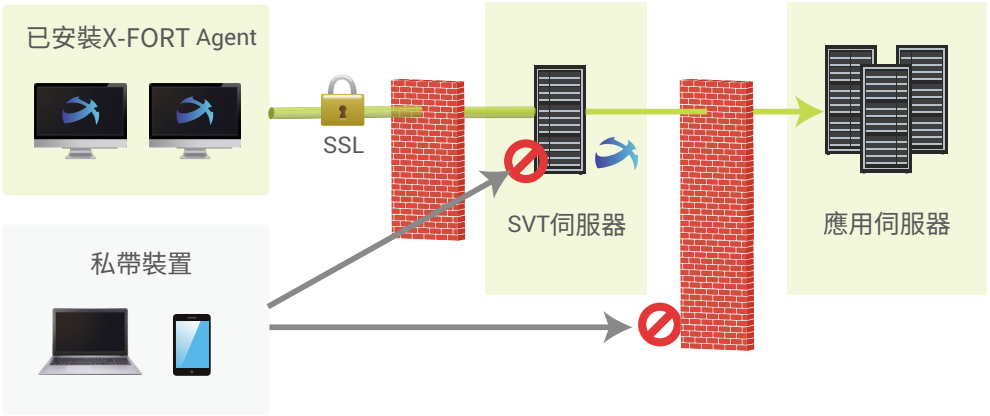
用Outlook傳送郵件按下「傳送」時，提示收件人身分會顯示視窗，提醒使用者再度確認。

SVT 伺服器安全通道

SVT(Secure Virtual Tunnel)伺服器安全通道可保護內部伺服器，避免未經授權的個人、電腦或其他裝置存取資料。

裝置敵我識別 & 身分驗證

- 安裝X-FORT Agent的電腦，透過SVT伺服器驗證後，才能存取受保護的伺服器。
- 只有指定的使用者、裝置和程式，才能連結受保護的伺服器。
- 避免有權限者私帶裝置，利用本身的權限存取資料伺服器。



通訊加密

- 裝置與SVT伺服器之間的通訊使用TLS加密，防止網路監聽、竊取機密資料。
- 與SVS搭配加密保護資料，限制人員、應用程式存取被保護伺服器時，下載的檔案強制存入SVS安全碟保護。

系統整合

- 搭配防火牆使用，SVT伺服器控管用戶端存取受保護的伺服器。
- 過濾並控制來源，防止未具X-FORT Agent的設備(如：私帶電腦、裝置)存取受保護的伺服器。
- 指定的應用程式，只可透過SVT伺服器，存取指定的伺服器。
- 保護對象支援TCP通訊協定，不需撰寫程式碼(如：API)。

範例說明

只有被授權的使用者，使用指定的程式，才能透過SVT伺服器連線到受保護的伺服器。

【研發人員】

指定的程式TortoiseSVN可連線到SVN Server，其餘人員無法連線

	使用程式	SVN	其他未保護(如KM)
研發人員	TortoiseSVN*	O	X
	其他程式	X	O

* 被指定的程式

【業務人員】

指定的程式Chrome可連接使用CRM系統；而IE不屬於被指定程式，故不允許連入CRM

	使用程式	CRM	其它未保護(如KM)
業務人員	Chrome*	O	O
	IE	X	O
	其他程式	X	O

* 被指定的程式

軟體安控

基本軟體安控

應用程式控管

- 支援管理者遠端掃描，及使用者手動掃描端點應用程式。
- 支援白名單機制及黑名單機制。
- 規則比對應用程式屬性，支援應用程式簽章的憑證、檔案雜湊、檔名、路徑，支援父行程關係定義。
- 掃描用戶端白名單：指定執行檔延伸檔名，自動掃描電腦硬碟內的執行檔，建立白名單。

【動態白名單管理】

- 支援觀察模式，產生執行記錄方便快速建立規則。
- 預設放行作業系統工作路徑，不影響更新維護運作。
- 允許白名單執行檔所執行的子行程。
- 憑證名稱字串支援部份比對。
- 未定義應用程式，授權使用者自行決策。
- 中央集中管理，啟動應用程式控制模式、檔案掃描排程。

安全備份

- 定時自動備份資料夾，並限制應用程式存取備份目的，確保備份安全。
- 搭配資料夾防護，確保備份目錄不被破壞。

資料夾防護

- 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。
- 信任應用程式：可限制用戶端電腦中特定資料夾內的檔案只能被「指定程式」存取，確保資料夾內的資料，不被其他非允許的程式存取，或其他未允許的檔案加入。如此可以有效保護用戶端的資料，不被惡意程式存取或竄改，確保資料的正確性。
- 例外處理名單：在限制異動副檔名清單及信任應用程式名單中，設定排除控管的例外名單。

軟體執行控管

- 提供軟體禁用功能外，可設定軟體使用的時段，控管軟體只能在規定的時段內被使用，其他時間禁止使用。
- 被禁用的軟體，使用者無法自行安裝。使用者嘗試執行被禁止或非允許的軟體，也會留存記錄。

線上申請軟體使用

提供主管審核機制，用戶端可申請暫時開放軟體使用。

特殊軟體安控

針對特定軟體的特殊控管功能，項目包含：

控管功能	說明
禁止列印	操作特定軟體時，可停用特定軟體中的列印功能
禁止複製到剪貼簿	操作特定軟體時，防止將內容複製到剪貼簿
禁用鍵盤	當特定軟體為前景視窗時，無法透過鍵盤輸入任何文字
禁用另存新檔	操作特定軟體時，無法另存新檔到其他路徑
禁用滑鼠拖曳資料	執行特定軟體時，無法拖曳內容或檔案到特定軟體中；禁止拖曳資料到其他程式
啟用螢幕浮水印	執行特定軟體時，啟用螢幕浮水印； 啟用永久螢幕浮水印，如設定方式為「精品科技 機密 - %user% %Date%」，電腦開機後立即顯示「精品科技 機密 - Andy Liu 2019/9/9」

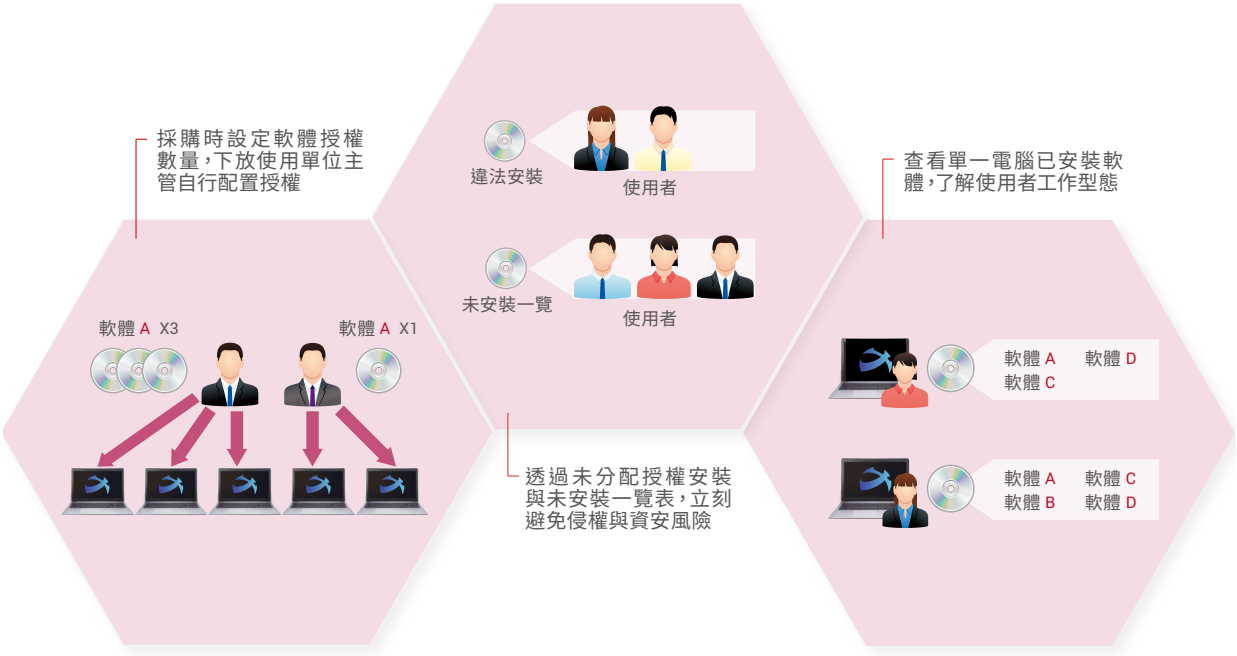
資產管理

軟體資產 記錄

軟體資產管理 & 軟體授權管理

可全盤掌控公司內的電腦安裝軟體，有效的管理軟體的授權分配與合規性。亦可輸入軟體採購的其他資訊，包含採購日期、採購金額等同步管理。適用各種授權類型，包含一般(大量授權/彩盒包)、訂閱、隨機版、試用版、升級、試用授權等，亦可自訂授權。依授權規則可自動或手動分配授權給人員或裝置。

- 套裝軟體整合管理：同一軟體授權安裝時包含多個軟體，可整合管理。如1套「Adobe Creative Suite」授權包含「Photoshop、Illustrator、InDesign、Acrobat Pro、Dreamweaver」等軟體。
- 軟體別名分類管理：相同軟體但顯示名稱不同，仍視為同一軟體統一管理與分配授權。多語系顯示不同，如「Windows 10 專業版、Windows 10 Professional」，歸類後自動識別為同一軟體。
- 軟體相容性 (降級權)：購買的授權可安裝較舊版本的授權。如「Windows 10 專業版」可向下相容「Windows 8.1/8 專業版、Windows 7 專業版」。（相同軟體因購買授權方式不同，有可能不支援向下相容）
- 分權管理：系統管理員依組織、部門劃分授權數量，由群組管理員分配授權數量。



軟資異動管理

- 軟硬體資產定期掃描，定期更新資產狀態。
- Hotfix資訊：管理每台電腦Windows Hotfix安裝及未安裝的現況，並執行用戶端的Hotfix安裝/移除。
- 遠端移除軟體：清查電腦內所有安裝的軟體，若發現不合宜的軟體，強制遠端移除(該軟體需要符合特定條件)。
- 機碼管理：清查每台電腦上所登錄的Windows機碼（Registry）資訊，以掌握電腦作業系統環境的現況。

CPE軟體描述 (必須搭配軟體資產模組使用)

將端點回報的應用程式名稱資訊與 CPE (Common Platform Enumeration)官方字典或自訂CPE 字典上登記的名稱進行比對。X-FORT蒐集端點軟體資訊，自動比對CPE字典輸出作業系統、軟體應用程式的準確資訊。

- 支援匯入CPE v2.3 版本任一日期的 CPE 字典檔，更新比對規則。
- 可調整軟體名稱相似度，提高相容性；亦可調整演算法不適合的比對結果。
- 蒐集用戶端軟體資產，比對軟體名稱與CPE規則，輸出比對符合結果為JSON、EXCEL格式。
- 支援銜接弱點比對系統，以供弱點資料庫(CVE)查詢。

硬體資產

硬體資產管理

X-FORT Agent會自動回報硬體資訊。無法用程式回報的設備，管理者也可以匯入統一管理，包含硬體零件（硬體採購）、設備資產（如桌椅、一般設備）；這些設備也可以搭配Barcode進行盤點。

硬體異動警示

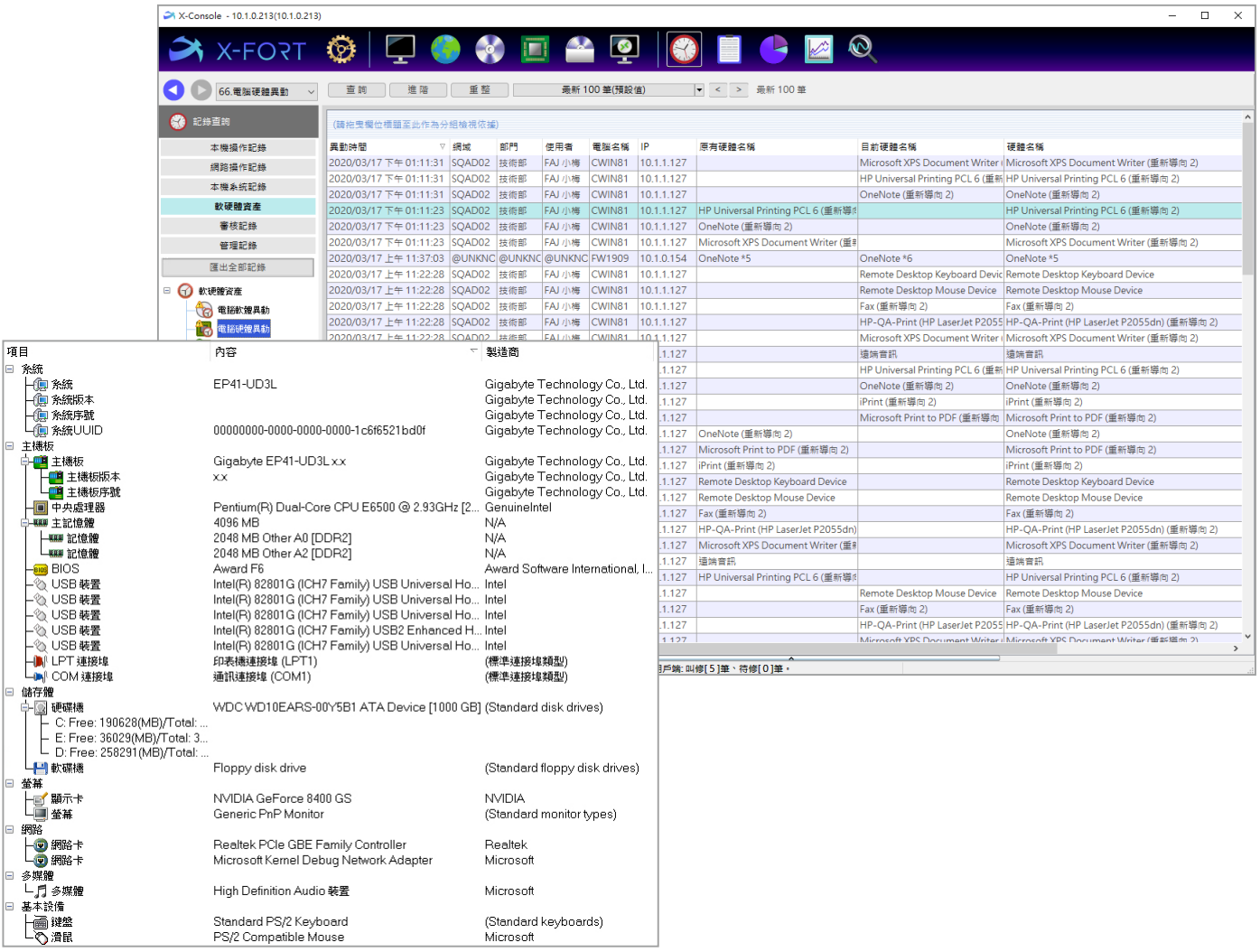
管理者可設定「硬體裝置異動警示」及「硬碟使用率警示」功能，當用戶端硬體裝置異動時，即時通知管理者。若使用者的硬碟空間不足時，也會通知管理者。

電腦採購

可將採購相關資訊，如電腦型號、財產編號、保管人、所在位置、採購日期、採購金額等輸入系統同步管理；亦可依採購金額、日期、保固期限，計算出電腦的殘餘價值。可調整資產現況，包含庫存、撥發、轉移、備用、歸還、送修、報廢、租賃等生命週期的狀況。

自動化設備盤點

可透過設備盤點功能清查電腦設備，比較撥發時與現狀配備的差異，列出異動的配備清單。



遠端管理

遠端功能 記錄

本機帳號管理

線上對用戶端的本機帳號管理，可新增、修改、刪除本機帳號，亦可啟用或停用本機帳號。

線上服務與遠端遙控

使用者線上叫修電腦，管理者可透過遠端遙控處理電腦問題，亦可詳細記錄所有相關處理過程。如管理者、使用者帳號、處理狀況、問題類型、連線時間等資訊。

檔案派送

- 提供立即派送與排程派送兩種檔案派送方式，並且可指定檔案派送至目標電腦後是否執行。支援多種檔案格式派送，包含單個執行檔、MSI安裝包、批次檔案等。
- 具檔案續傳、可管理傳輸頻寬及階層派送功能。
- 可選定種子的電腦，提供區域檔案派送來源。

開關機命令

對用戶端電腦送出下列功能：「喚醒」、「登出」、「重開機」及「關機」命令，其中喚醒功能是透過網路執行遠端喚醒命令給未開機電腦的網路卡，讓電腦自動開機。電腦必須支援WOL(Walk On LAN)，並在BIOS中啟用。

傳送訊息

可由系統管理者，將重要的訊息立即對用戶端電腦送出廣播訊息。

X-Monitor

提供給部門主管使用的遠端監視工具，可藉此觀察工作狀態。部門主管只能監視所屬部門之員工，其他非管轄之員工無法進行監視。

畫面擷取 記錄

畫面單拍

畫面擷取時機包含：

- 切換焦點視窗或應用程式時。
- 開啟或切換網頁時。
- 使用剪貼簿複製、剪下和貼上的操作行為。
- 操作Microsoft Word, Excel, PowerPoint, Visio應用軟體另存新檔的動作時。
- Outlook按下寄信按鈕時。

畫面連拍

- 固定畫面連拍：開啟固定連拍功能，並設定「畫面連拍間隔」的秒數，即啟動間隔的秒數，就會進行擷取畫面的記錄。
- 網頁清單：設定畫面連拍的【網址集】清單，當用戶操作網頁瀏覽且與【網址集】內的網址關鍵資訊符合時，會依所設定的間隔時間進行連拍畫面。
- 軟體執行：設定畫面連拍的【程式集】清單，針對於【程式集】清單內的特定軟體執行或使用時，會依所設定的間隔時間進行連拍畫面。
- 色彩管理：依管理人員需求，可選擇以16色、256色或全彩的圖片品質，作為畫面的儲存格式。

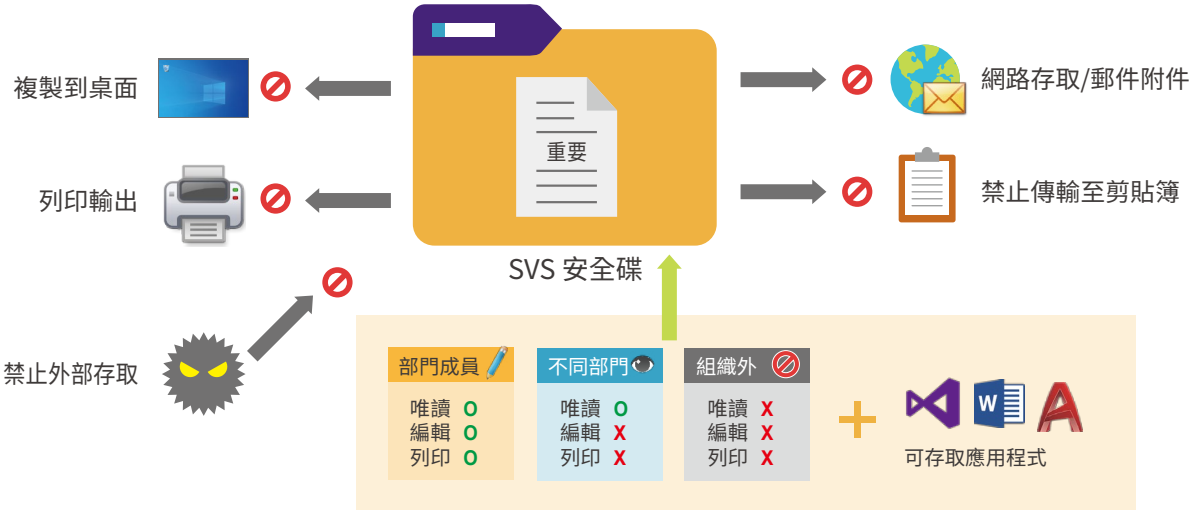
畫面記錄瀏覽

- 多樣式的檢視畫面記錄
  - 以矩陣型式的縮圖列表，顯示螢幕畫面記錄，同時瀏覽多筆連續畫面顯示。
  - 展開每張畫面的關聯文字記錄資訊，具有文字與畫面對照的瀏覽效果。
  - 畫面記錄撥放功能，可放大照片後，快速跳至上一張或下一張。產出的影片可直接在瀏覽器上撥放。
- 匯出圖片或影片
  針對特定使用者的螢幕操作畫面，加以日期、應用程式、標題作為條件進行篩選，並匯出
  - 單張圖片檔
  - 畫面串接的影片檔

文件控管

SVS安全碟 / DEC文件加密中心

SVS安全碟提供強大的文件保護機制，利用掛載虛擬磁碟方式，將文件存放在受保護的安全碟內，以確保安全性。提供完整的權限控管功能，可對每個安全碟設定不同的使用者存取權限，包含閱覽、編輯、列印、匯出明文...等。



加密機制

- 強制加密：指定的應用程式(如Word, AutoCAD)強制將檔案存入SVS安全碟中，達到保護的效果。
- 手動加密：使用者可自行挑選SVS類別，依所選的類別建立SVS檔案。
- DEC文件加密中心：將檔案伺服器指派為文件加密中心，文件放入共用的網芳資料夾，即會依資料夾指定的SVS類別，自動加密成SVS檔案。

SVS管理角色

- 系統管理員：定義系統設定與操作權限。
- 文件管理員：設定組織成員SVS安全碟的存取權限。
- 群組管理員：審核組織成員文件權限變更申請，檢視成員文件操作記錄。

文件與角色權限

- 分權閱覽：有權限的使用者可掛載安全碟，可閱覽、列印或編輯檔案。
- 角色與類別：使用者可擁有多個角色，依照角色賦予安全碟的使用類別組成權限；角色與類別越多，權限組合越多。
- 自訂授權：SVS安全碟的建立者，可授權該碟的使用對象、權限和期限。
- 寫出控管：SVS安全碟只進不出，只有被賦予權限的使用者才可匯出明文檔案到一般磁碟。

編輯控制

- 交互防護：控管螢幕擷圖、剪貼簿，防止被保護文件內容複製到其他未受保護文件。
- 限制存取：檔案限制在安全碟內使用，防止檔案複製到一般硬碟或雲端硬碟。
- 暫時權限：依工作需要開放暫時權限，期限過後恢復原本權限。
- 離線使用：未與X-FORT伺服器連線時，依所設定的離線天數使用。
- 保留軌跡：記錄安全碟的「建立、掛載、卸載、匯出明文」等操作以備查詢。
- 螢幕浮水印：依照角色可設定螢幕浮水印樣式，當使用者符合角色並掛載SVS碟時，將顯示螢幕浮水印。
- 審核解密：使用者可向主管申請，將SVS檔案解密為明文。

系統管理

基本系統管理

部署快速

- 遠端部署：透過X-Console，具備本機管理者權限帳號(如：網域管理者)，遠端部署X-FORT Agent。
- Logon Script安裝：設定網域的Logon Script，當使用者登入網域時自動安裝。
- MSI封裝檔：電腦開機套用本機群組原則即進行安裝。
- 手動安裝：與X-FORT伺服器連線時，使用者端手動安裝X-FORT Agent。
- 離線安裝：連同既有政策，打包X-FORT Agent，手動安裝於非連線電腦。

自動與Active Directory同步

可排程設定自動與Active Directory (AD) 進行同步，無需手動或使用其他工具進行同步，可降低IT管理者的負擔，並具有以下效益：

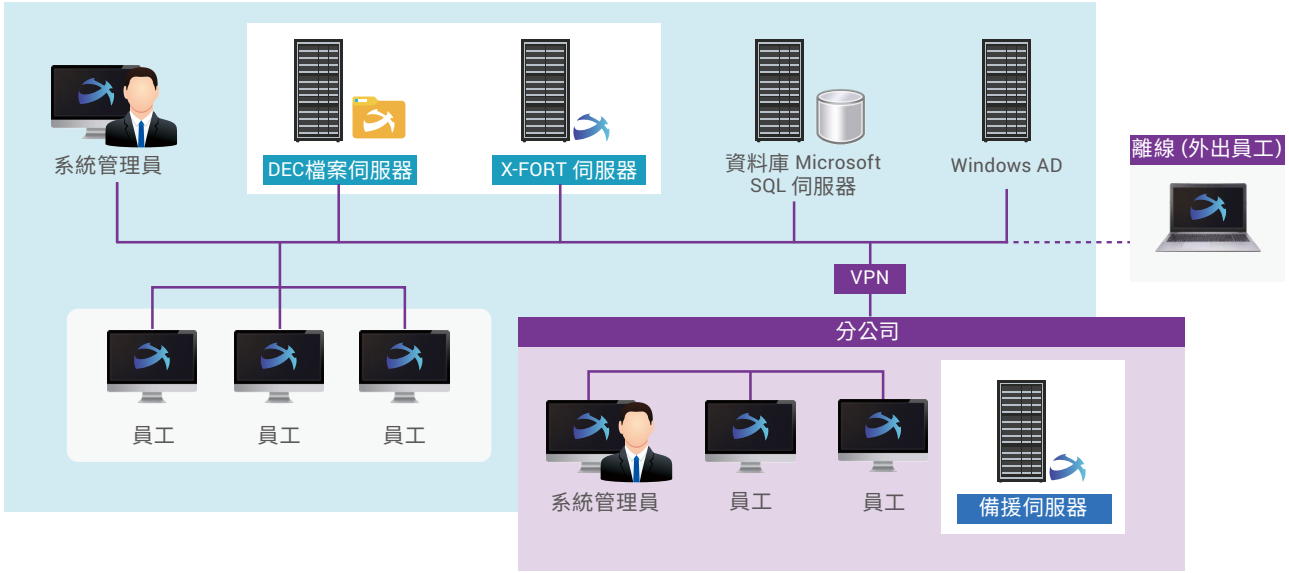
- 集中管理使用者帳號：直接與AD的帳號管理整合，管理者無需另外新建一套帳號管理使用者，透過AD單一登入(Single sign-on)的應用，可直接認證每位用戶端使用者。
- 網域組織同步管理：直接同步AD所建立的組織、OU、群組架構，管理者無需花時間在建立與維護另一套用戶帳號管理系統。

政策設定

- 一般政策
  - 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。
  - 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。
  - 使用者政策(預設)：分別依群組、OU、使用者指定政策，依登入使用者帳號套用權限。

  (優先度：網段政策 > 電腦政策 > 使用者政策)
- 特殊政策：於特殊情境下自動生效與恢復，不需管理者介入。
  - EDR自適應政策：透過EDR組合偵測執行特定程式、電腦所在位置等組合為偵測條件，條件觸發自動切換控管政策。(須搭配EDR事件反應模組使用)
  - 離線政策：當電腦無法與X-FORT伺服器連線時，套用此政策。
  - 暫時政策：在指定期間內生效的政策；如調廠區工作需要使用隨身碟，只於調派期間開放使用。

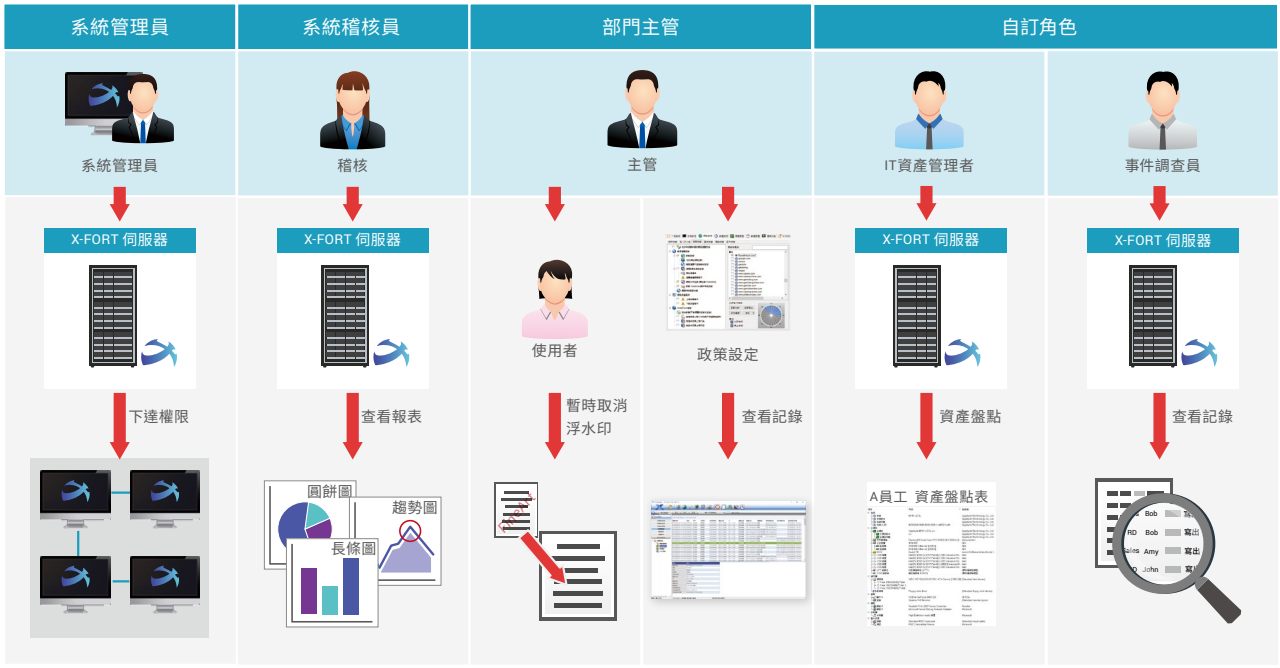
  (優先度：EDR自適應政策 > 離線政策 > 暫時政策)



管理角色

利用管理角色，依職務執行需要，設計管理任務，達成權責分離的目的。系統建置部署與資訊安全管理權責分離，符合商業營運管理邏輯。

- 系統管理員：X-FORT系統最大權限管理者，可賦予其他管理者角色與權限，規範管理範圍與政策。
- 系統稽核員：查詢記錄及審視權限內容，但不能變更任何記錄與設定。
- 部門主管：檢視管轄範圍內的記錄；審核組織成員的線上申請。
- 自訂角色：
  - 依功能模組指定管理項目，例如盤點人員，僅授予軟硬體資產模組實施盤點，而不涉及其他安全政策的設定。
  - 可自訂管轄範圍、記錄類型、組織人員，如：事件調查員，限定只能調閱某特定人員的外接式儲存裝置寫出記錄。
- 使用者：登入使用者可檢視本身的各種操作記錄。



定期排程

- 依所設定的網段IP及子網路遮罩，掃描範圍內所有連線電腦，及偵測區域網路中的已安裝/未安裝X-FORT Agent的電腦狀態。
- 加密金鑰對定期更新，避免遭到有心人士暴力破解。
- 定期將系統記錄、報表mail給管理者與主管，有效掌握人員操作狀況。

記錄與資料整合分析

- 記錄查詢結果根據分權與管轄範圍，依登入的管理者身份，只可檢視管轄範圍內人員或電腦的記錄；不同管理者顯示不同結果。針對人員、日期等組合篩選條件，可指定欄位(如：記錄時間)順序排列，檢視多種類記錄或資料。
- 檢視記錄與資料

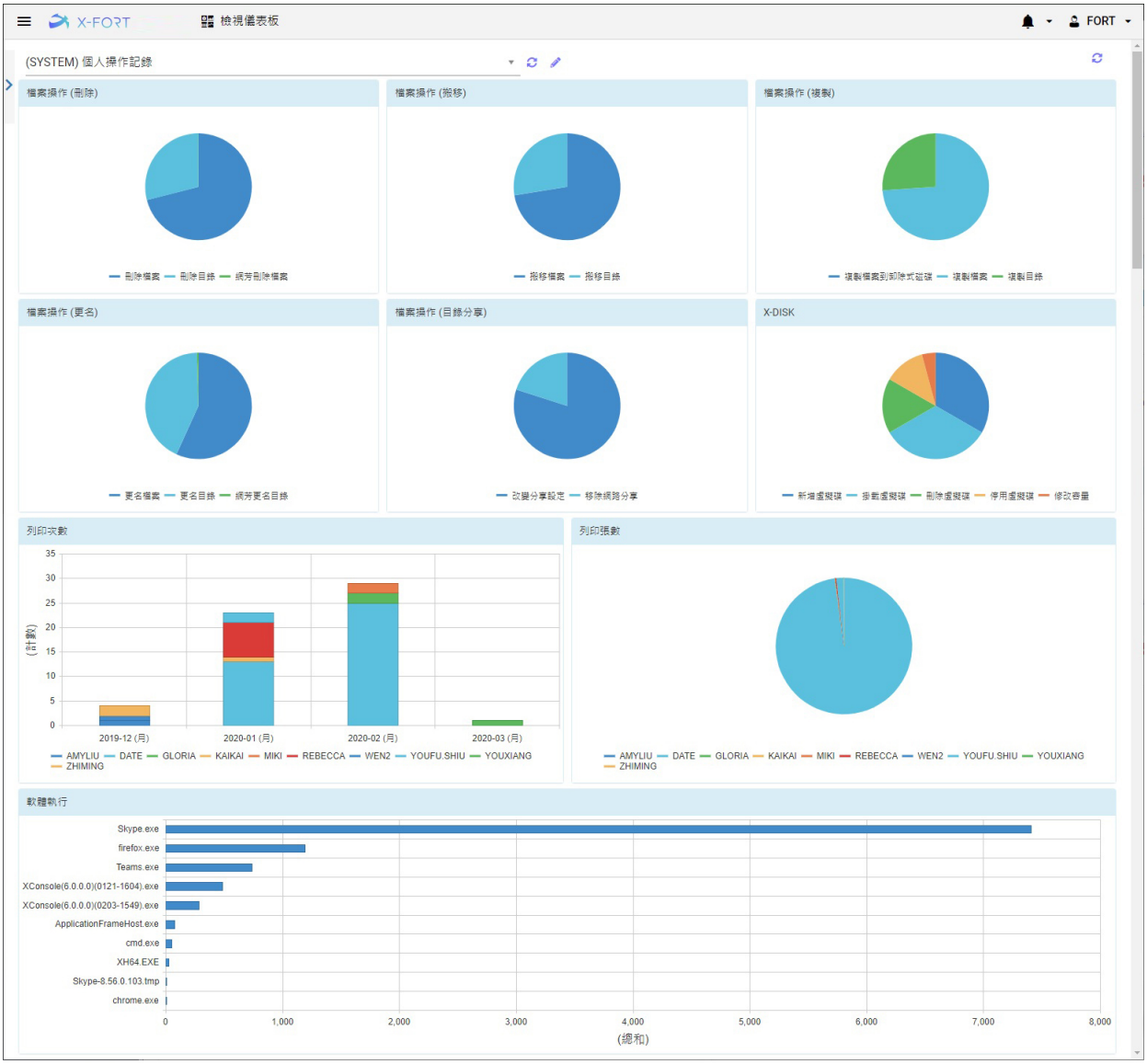
自訂篩選條件	• 使用預設的篩選條件，或使用進階條件顯示資料；此檢視可用於製作報表或儀表板的篩選條件 • 自訂顯示欄位，或啟動彙總計數、加總、平均、計數/加總總和百分比，快速統計資料的結果 • 選擇排序的欄位，進行資料降冪、升冪排列

儀表板

- 可自行組合多個小工具(Widget)在同一頁面，一次查看各種相關結果，即時掌握資安狀況。
- 小工具類型包含直條圖、圓餅圖、折線圖、樞紐分析表、表格、卡片、矩形樹狀圖等，以不同面向來檢視資料。
- 管理者登入系統主頁，依管理角色的管轄範圍篩選結果，呈現特定儀表板。

匯出報表

- 內建多種報表範例列表，可將篩選條件中選擇的欄位與條件查詢出的內容，匯出PPT、 HTML、 Word、 Excel檔案。
- 自訂報表
  - 由儀表板快速建立報表範本，指定對應篩條件匯出報表。
  - 提供報表編輯器，可自行製作範本；範本可作為附件整合至訂閱通知。
- X-Report利用Excel製作範本，可內含公式、圖表、樞紐分析表、交叉分析篩選器等。
- W-Console可立即產生報表，或透過排程管理定期寄送報表。



事件警示&訂閱通知

- 當X-FORT伺服器或用戶端服務發生異常時，會自動發出警示mail給所屬的群組管理者或系統管理者。警示包含發現異常電腦、發現未安裝電腦、IP/MAC異動、惡意破壞BitLocker、AD同步失敗...等。
- 可訂閱LINE Notify、Microsoft Teams、Email、瀏覽器通知，當事件觸發時，即時通知管理者與使用者。

資料庫管理

- 可定期備份，亦可選擇差異備份，或還原資料庫，查詢涵蓋目前主資料庫與備份資料庫中的記錄。
- 系統可自動建立還原資料庫資訊，或利用手動操作方式，建立還原資料庫資訊。
- 可針對還原資料庫「新增」、「移除」、「修改」，及設定「關聯」、「取消關聯」等操作。
- 可跨多個備份資料庫進行查詢：記錄、報表、統計、趨勢中心等。
- 在報表、統計與趨勢中心，將自動參照記錄的原始資料，加以關聯呈現結果。
- 監測資料庫伺服器效能，可透過X-Console隨時確認資料庫的CPU使用率與磁碟空間。

資料庫採用Microsoft SQL Server

- 支援取得與導入方便：相容性佳，具有文字介面和圖形介面，並提供Wizard，易於安裝和管理。
- 安全性佳：提供資料加密、稽核、災害復原、容錯、備份等功能，使企業資料得到更安全的保護。
- 擴充性好：提供資料倉儲、資料採礦...等資源。

進階系統管理

進階伺服器

X-FORT單一伺服器可處理1,000台以上用戶端（實際經驗單一伺服器最多可支援3,000台以上用戶端）

- 負載平衡：為了減輕單一伺服器的負擔，可設定多台伺服器，平均分擔伺服器的負載量。
- 備援伺服器：為確保服務不中斷，支援伺服器備援機制，多台伺服器之間可以互為備援，即使一台伺服器發生故障，用戶端仍可以連線至他台伺服器，以維持系統正常運作。
- 中繼伺服器：
  - 分擔備援伺服器與主伺服器的流量；用戶端將記錄上傳回中繼伺服器後，集中回傳主伺服器。
  - 儲存實體備份檔(如備份寫出檔案、列印、刪除檔案、燒錄、即時通訊傳輸檔案...等)，不需回傳主伺服器。

EDR行為偵測與反應

EDR為端點安全檢測與反應處置，監視和記錄端點上的活動，檢測可疑行為、評量安全風險，及回應內部潛在威脅。使用EDR方案來追蹤、監視和分析端點的人員操作、應用程式活動記錄，以便適時主動或手動回應即時威脅。

- 偵測可能外洩活動，寫出USB、列印、傳送檔案、網路連線、網路流量等，予以攔截、阻擋。
- 用戶端自動反應包含螢幕浮水印、警示、限制網路傳輸、禁用隨身碟、禁用印表機等；管理者可遠端執行命令、復原用戶端發生之自動反應動作。
- 自適應政策：透過EDR組合偵測條件，觸發後自動切換控管政策。
- 結合X-FORT各式記錄、EDR反應記錄，方便稽核事件處理。

偵測 (Detect)		反應 (Action)	
USB 儲存裝置插拔	子網路上傳流量	禁用非註冊碟	啟動螢幕浮水印反應時截圖
使用者檔案異動個數	子網路下載流量	啟動檔案操作記錄	Email、Teams、LINE通知警示
外接儲存裝置寫出行為	超連結關鍵字	啟動列印控管	切換自適應政策
命令列關鍵字	遠端桌面連線連入/連出	阻擋連線	關機
列印張數	用戶端所在國家	阻擋特定通訊協定連線	
網路連線次數	誘餌異動	顯示螢幕浮水印	

系統規格建議

硬體

X-FORT Server 主機硬體規格

控管裝置	100台(註1)	300台	1,000+台
CPU	Intel i5/4核心以上	Intel i5/4核心以上	Intel i7/4核心以上
RAM	8GB以上	8GB以上	12GB以上
硬碟	500GB以上	750GB以上SAS	1TB以上SAS
網路	100Mbps	1,000Mbps	1,000Mbps

註：1.X-FORT Server和Database Server共用同一台主機，RAM需為X-FORT Server與Database Server總和
2.使用者規模超過1,000台電腦，或長時間蒐集大量記錄時，依照實際需求增加硬體資源
3.若考慮備援或負載平衡，請加購系統進階模組
4.以上硬體規格含IIS Server

Database Server 主機硬體規格

控管裝置	100台	300台	1,000+台
CPU	Intel i5/4核心以上	Intel i5/4核心以上	Intel i7/4核心以上
RAM	8GB以上	8GB以上	16GB以上
硬碟	500GB以上	1TB以上SAS	2TB以上SAS
網路	100Mbps	1,000Mbps	1,000Mbps

註：長時間蒐集大量記錄，依照實際需求增加儲存空間

X-FORT Client 主機硬體規格

CPU	Core 2 Duo 以上等級
RAM	2GB以上
硬碟空間	安裝時可用空間至少400MB以上空間，安裝後系統碟建議保留20%以上容量空間

軟體

X-FORT Server 主機軟體規格

Windows平台	Windows Server 2019 Windows Server 2008 R2	Windows Server 2016	Windows Server 2012/R2
Java VM	Amazon Corretto OpenJDK 11以上		
IIS	8.0以上		
.Net Framework	4.8以上 (W-Console需Windows Server 2012以上)		
目錄服務(非必要)	Microsoft Windows Active Directory		

Database Server 主機軟體規格

Windows平台	Windows Server 2019 Windows Server 2008 R2	Windows Server 2016	Windows Server 2012/R2
Database版本	Microsoft SQL Server 2019 Microsoft SQL Server 2014	Microsoft SQL Server 2017 Microsoft SQL Server 2012	Microsoft SQL Server 2016 Microsoft SQL Server 2008 R2

X-FORT Client 主機軟體規格

Windows平台	Windows 10（不支援手機、平板用的Windows Phone及Windows RT系統） Windows 8.1, 8 Update（不支援手機、平板用的Windows Phone及Windows RT系統） Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate SP1 Windows Server 2019, 2016, 2012/R2, 2008/R2（部份功能不支援）
VDI平台	Citrix XenDesktop 7.17~8.2, VMware Horizon 7.1 所發佈之Desktop & App Windows 10, 8.1, 7・Windows Server 2016, 2012 R2, 2008 R2

註：VDI代表Virtual Desktop Infrastructure

※上述支援作業系統平台可能因產品版本更新而有所變動，實際支援作業系統平台以產品實際規格為準

資安巡航 守護無垠

Ultimate Security for Business Longevity

FineArt

E sales@fineart-tech.com T +886-3-5772211 A 新竹市埔頂路18號8樓