X-FORT

縱深防禦，多層次保護混合工作模式

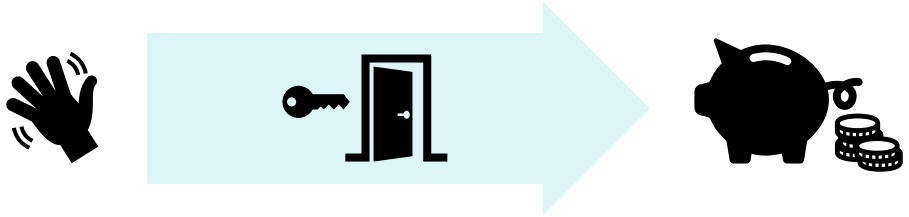
精品科技 技術總監 / 賴頌傑 Dean Lai

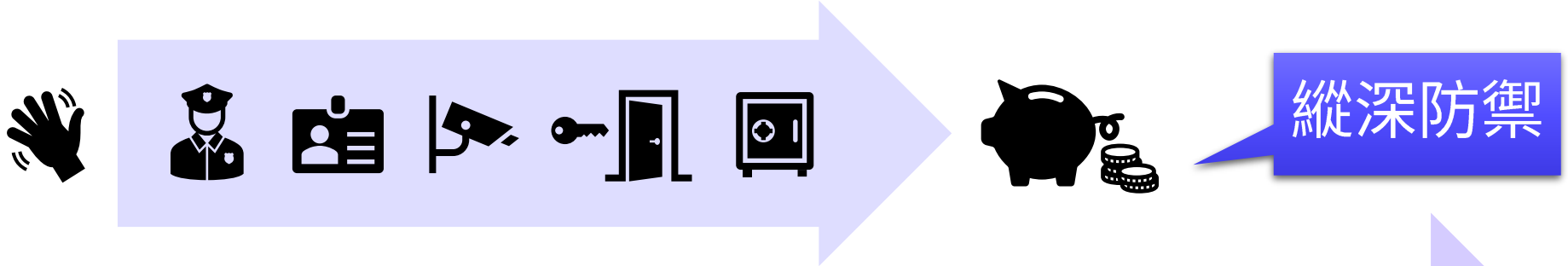
FineArt

縱深防禦

多面相控制建立內部縱深

縱深防禦的優勢





多層次控管

不同的控管方式

- 有效性：不容易造成突破
- 廣泛性：多種觀點的防護
- 調整性：自由調整控制的精細度

X-FORT

使用端點防護方案的必要性

脫離企業的保護環境

公事/私事可能混用

強制

- 最有利的政策落實點 (PEP, Policy Enforcement Point)
- 強制落實資安政策

持續

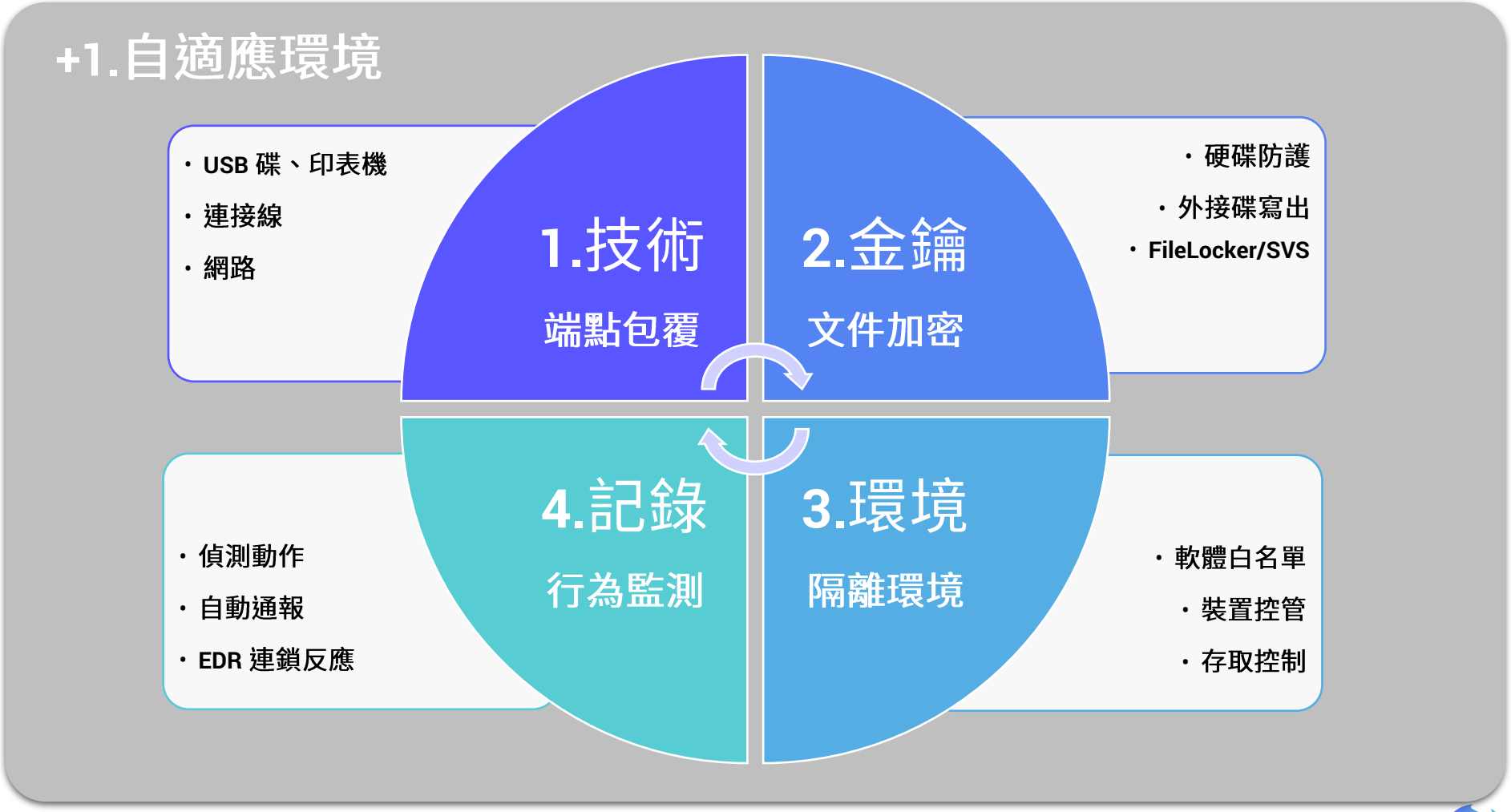
- 使用者活動監視
- 避免非信賴裝置混用網路
- 連接非信任周邊裝置

即時

- 實現即時控制
- 獨立判斷與反應

X-FORT

端點上的多層次保護：４＋１



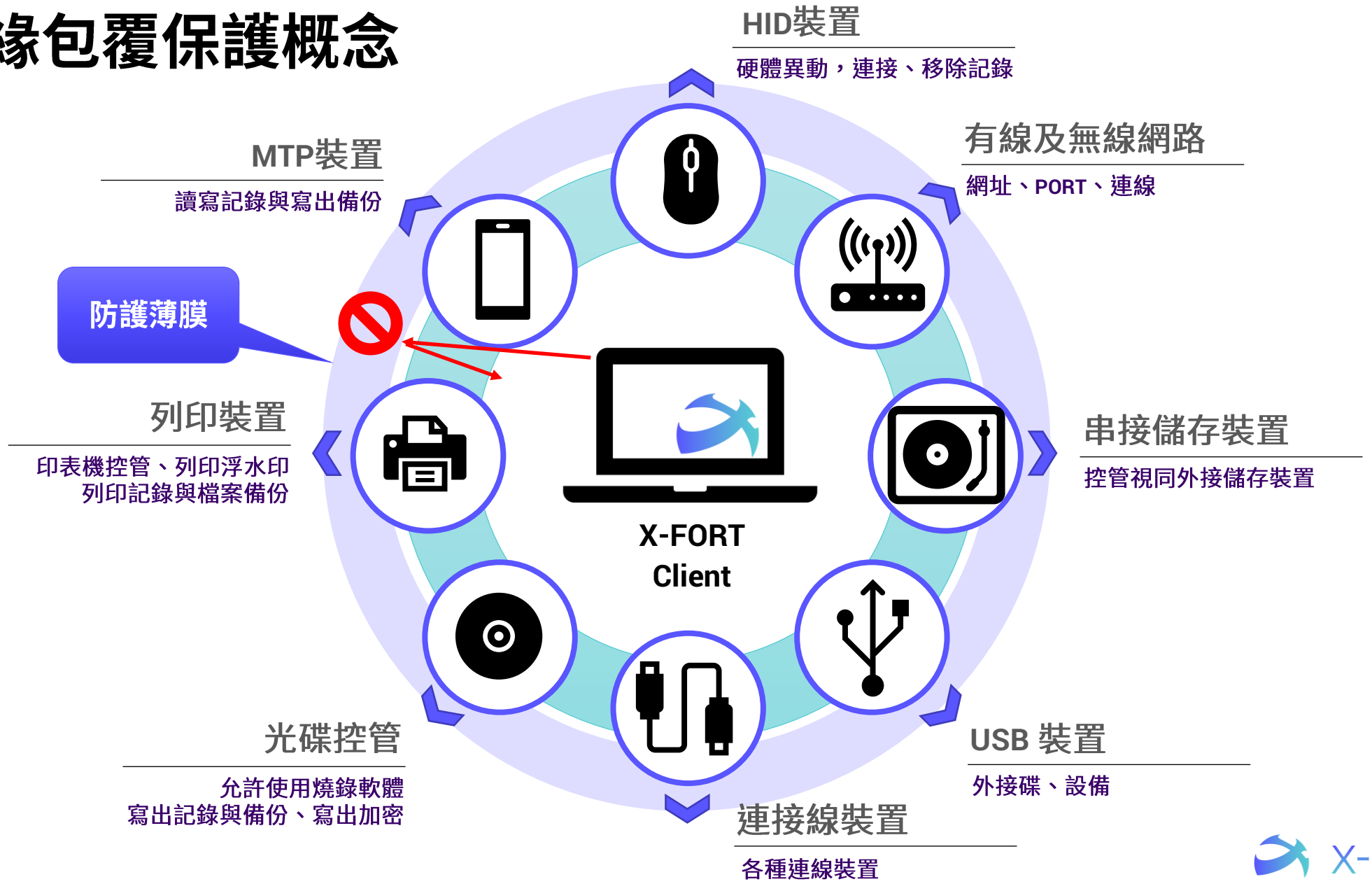
X-FORT

端點上的多層次控管 4 + 1

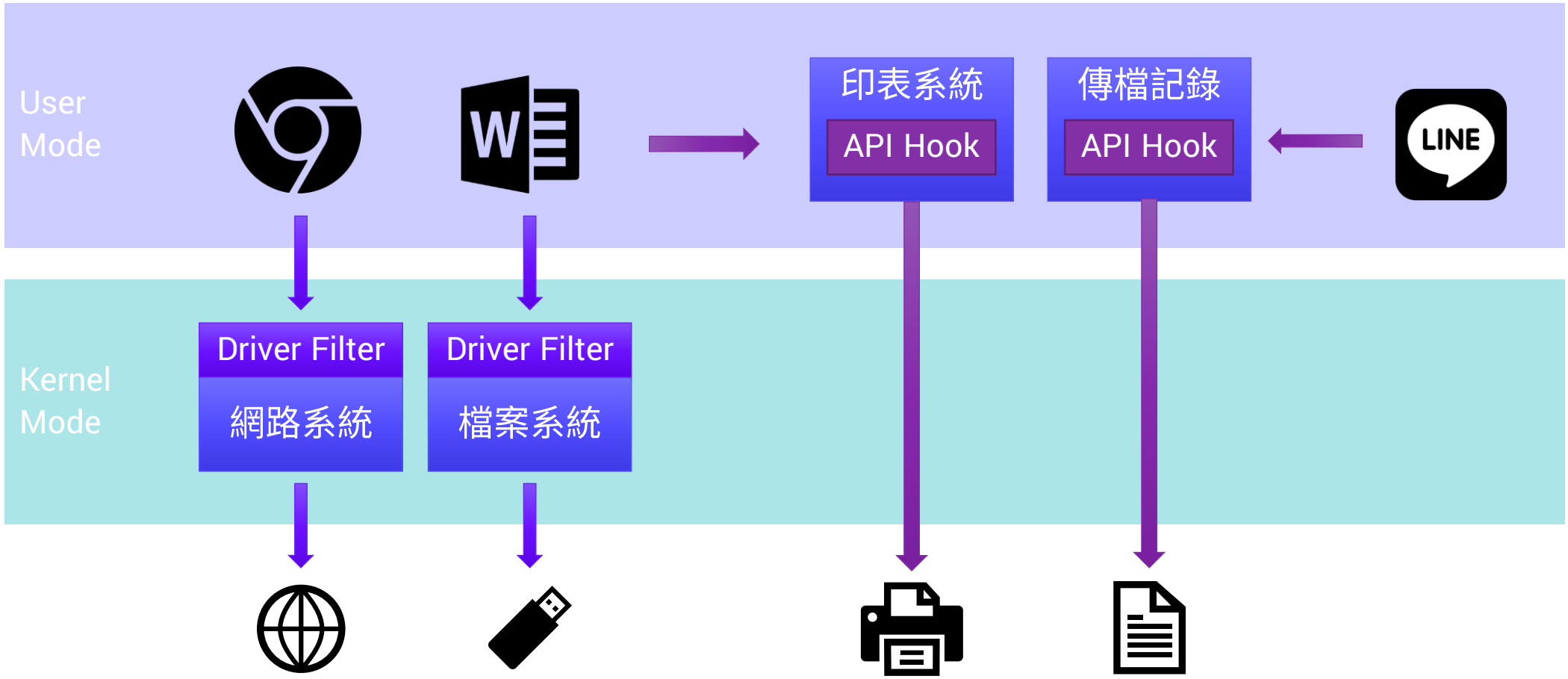
最有效的政策落實

1.端點邊緣包覆保護

邊緣包覆保護概念


HID裝置
硬體異動，連接、移除記錄
有線及無線網路
網址、PORT、連線
串接儲存裝置
控管視同外接儲存裝置
USB 裝置
外接碟、設備
連接線裝置
各種連線裝置
光碟控管
允許使用燒錄軟體
寫出記錄與備份、寫出加密
列印裝置
印表機控管、列印浮水印
列印記錄與檔案備份
MTP裝置
讀寫記錄與寫出備份
防護薄膜
X-FORT
Client

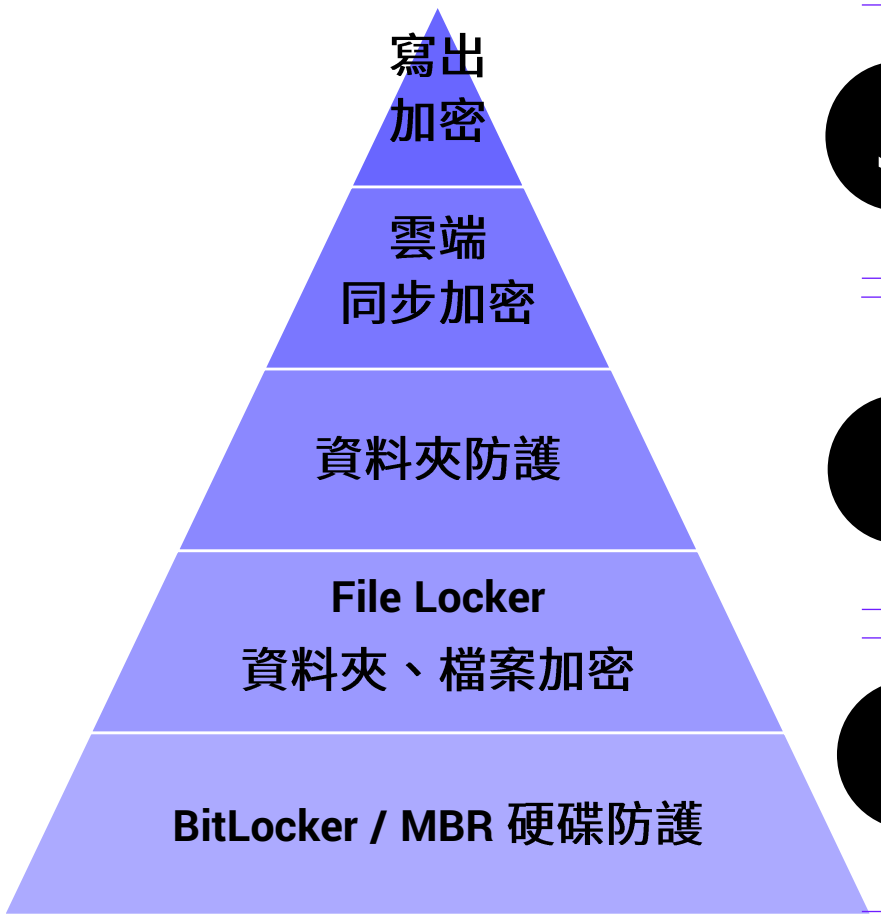
端點邊緣安全： Driver Filter / API Hook



X-FORT

2.文件加密保護

內容保護與加密



3

Data in transit

上傳檔案、寫出外接儲存裝置加密、IM/FTP傳輸控制

2

Data in use

使用中防護，授權的應用程式、資料夾存取

1

Data at rest

檔案系統、儲存媒體

X-FORT

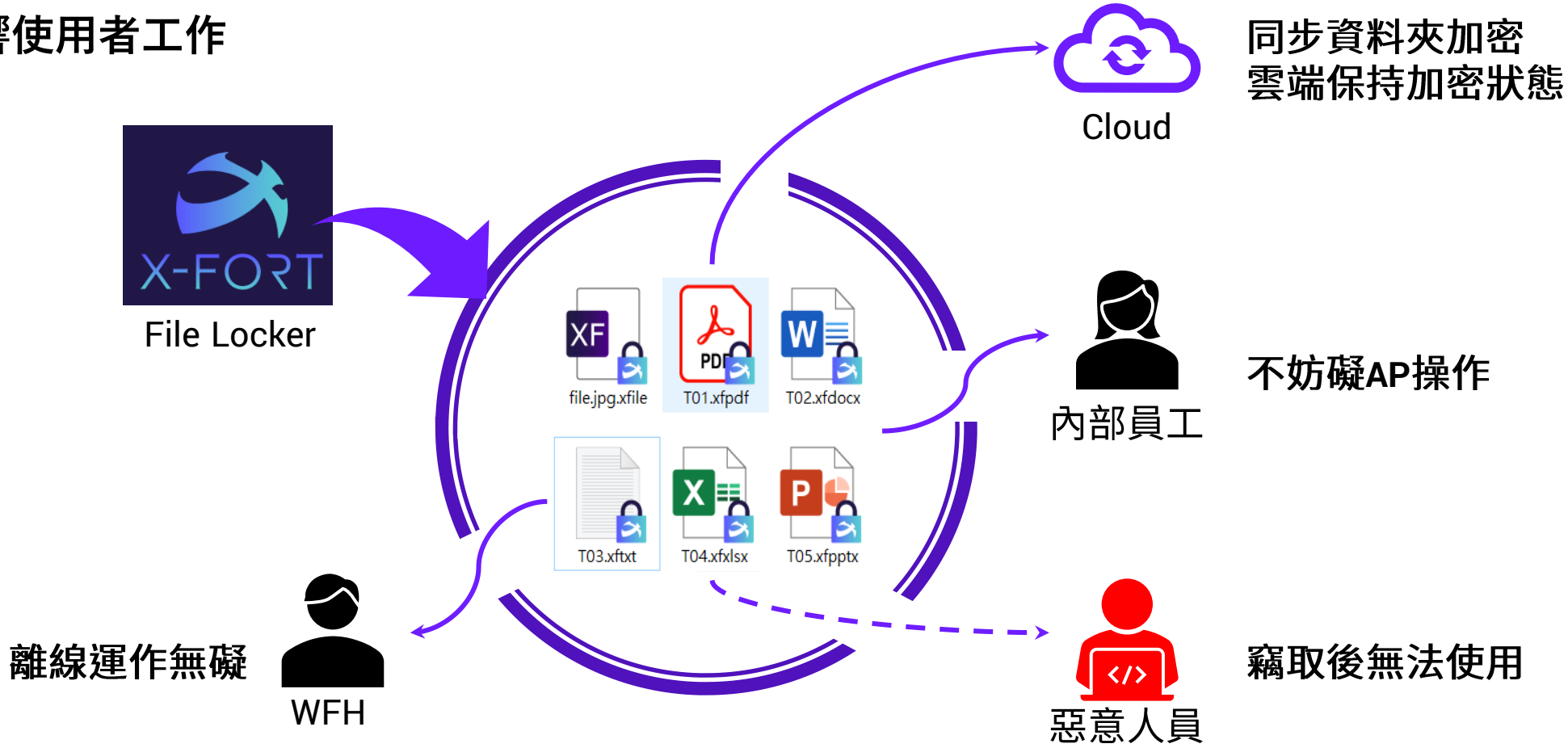
例１：硬碟防護 – MBR / BitLocker 硬碟防護

- 串接到其他電腦電腦， 無法正常讀取硬碟
  - MBR 硬碟: MBR 加密
  - UEFI / MBR 硬碟: BitLocker自動加密本機磁碟， 統一控管金鑰

X-FORT

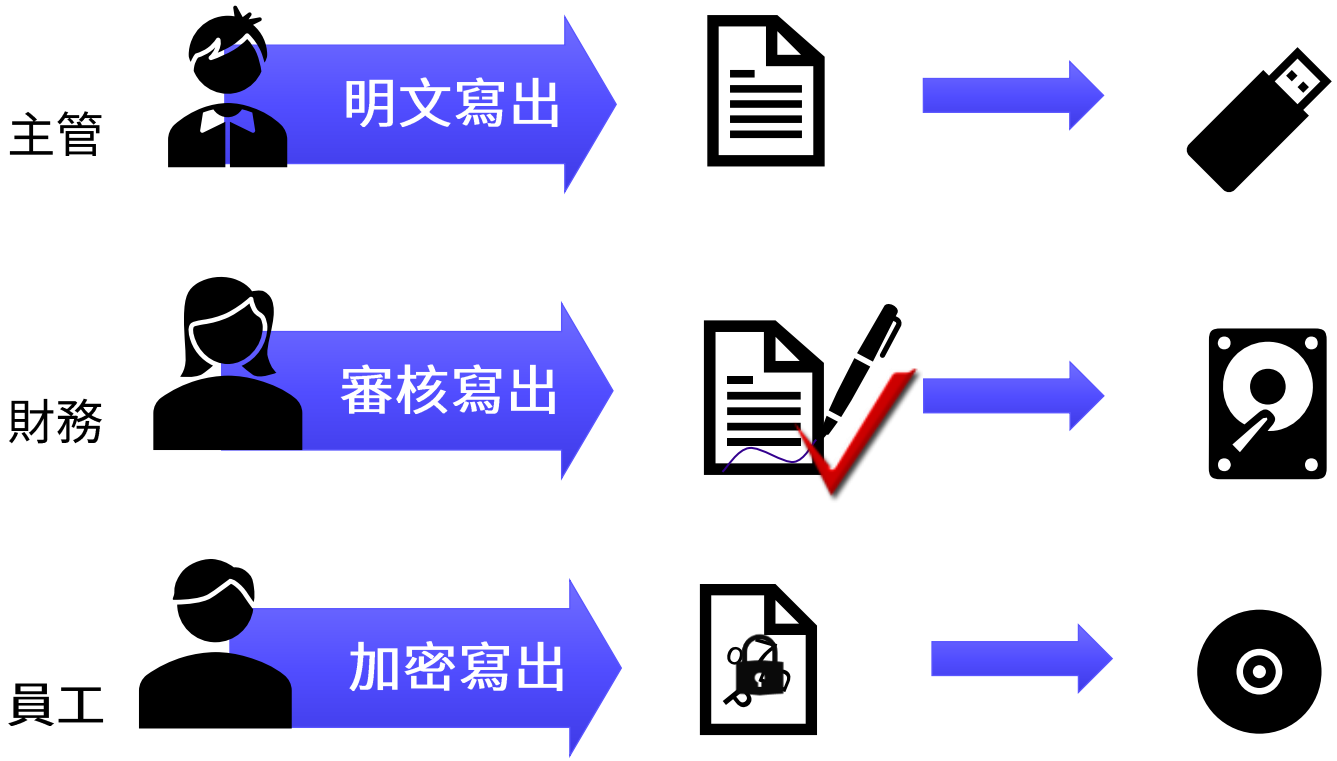
例２： File Locker / SVS 檔案加密 / FAC 資料夾防護

- 不限制AP行為
- 不影響使用者工作



例３：外接儲存媒體寫出

- 最能符合客戶多樣化需求，依人員角色設定
- 寫出加密：Agent電腦解密、指定電腦解密、密碼解密



X-FORT

3.環境隔離保護

有效防範未知威脅

軟體環境控管

1 應用程式白名單 AWL

- 建立信任清單
- 預設禁止執行
- 動態更新

2 程式執行控制

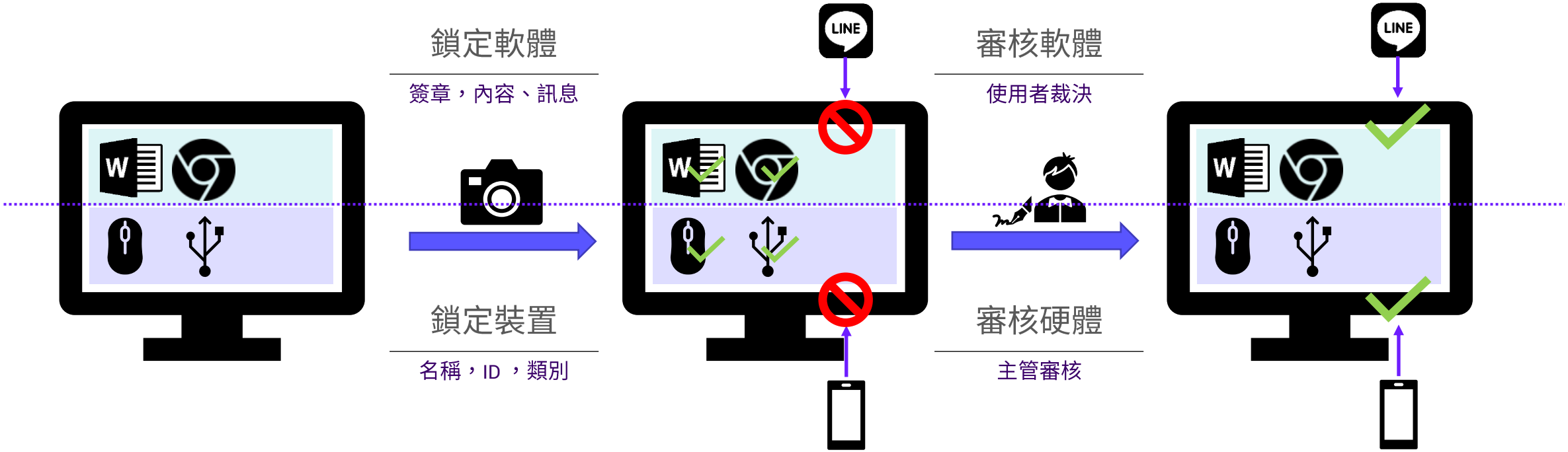
- 已知不良程式
- IT 授權管理疑慮
- 耗費資源

3 應用程式行為控制

- 通訊連線
- 截圖
- 網路存取
- 浮水印
- 另存新檔

X-FORT

軟體白名單 & 硬體裝置鎖定白名單



X-FORT

4.行為監測

偵測活動內容及時防止災害擴大

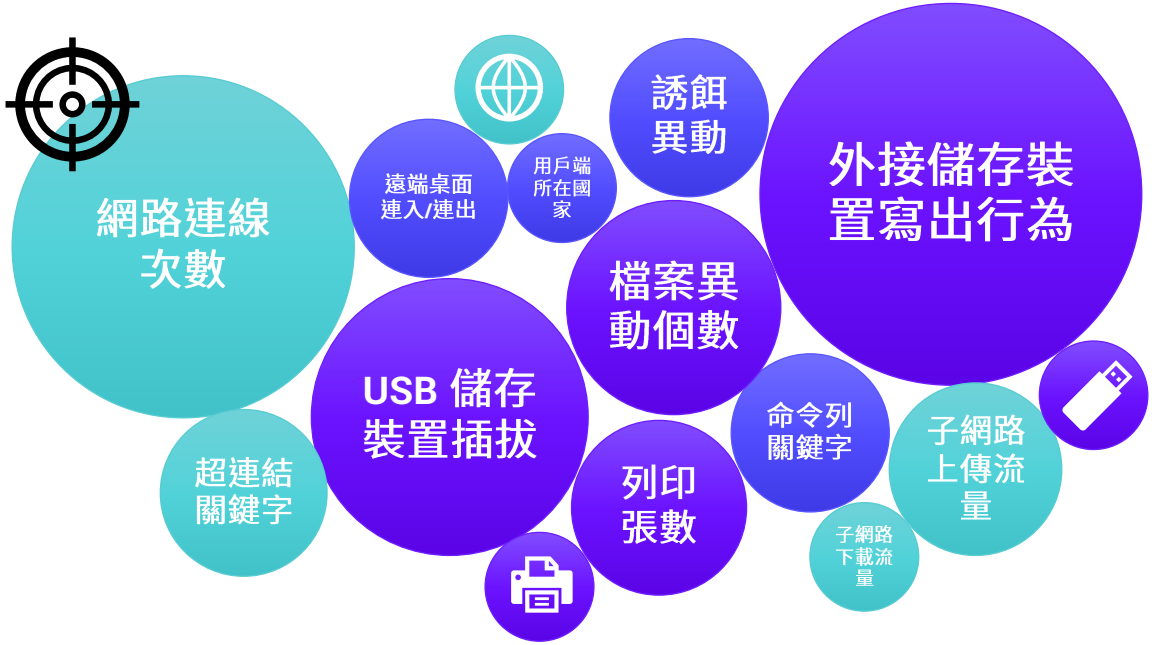
使用者行為監控

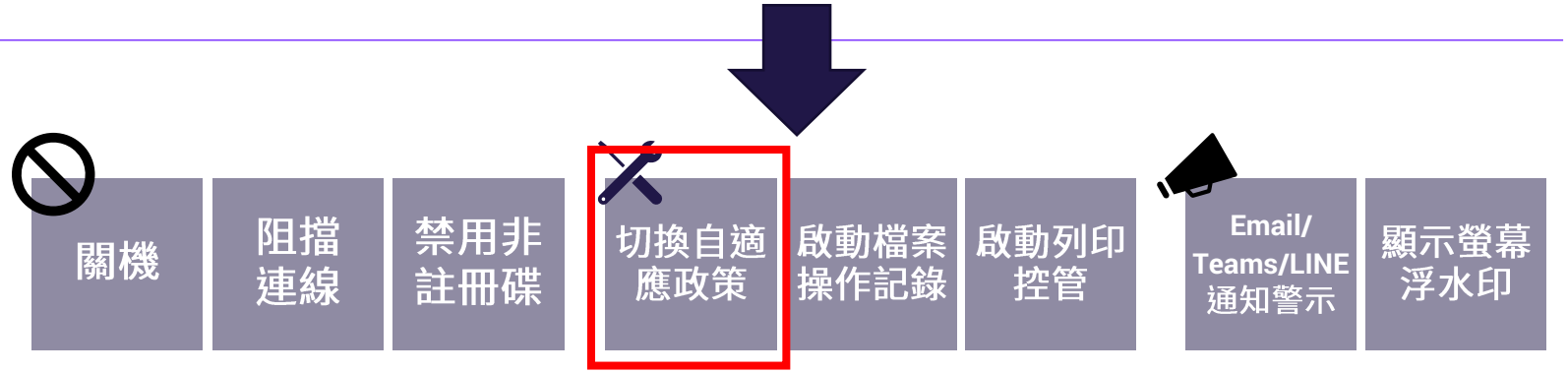
- 使用者檔案操作 / User File Operation
- 剪貼簿 / Clipboard
- 應用程式執行 / Application Activity
- 裝置存取 / Device Access
- 列印 / Printing
- 檔案傳輸 / File Transferring
- 網頁瀏覽 / Web Browsing
- 即時通訊 / Instant Messaging
- 郵件傳輸 / Mailing
- 系統檔案操作 / System File Operation

X-FORT

EDR事件偵測與反應

- 強化感知內部人員於端點活動
- 對象包含使用者及應用程式
- 偵測及反應模組範圍包括
  - 外接儲存裝置管理
  - 列印裝置控管
  - 操作記錄
  - 共用資料夾控管
  - 通訊控管
  - 網頁控管
  - 雲端控管





X-FORT

+1. 自適應環境

因地制宜彈性工作

遠距工作：控管隨身攜帶，政策自動切換

公司內	遠端VPN	分公司網段	離線	臨時需求	動態偵測
標準模式 工作政策	自動切換 遠端政策	自動切換 網段政策	自動切換 離線政策	審核提升 暫時權限	操作行為切換 EDR政策

X-FORT

結論

縱深防禦的優點

縱深防禦，多層次保護混合工作模式

方便

- 資安防護及操作方便性中取得平衡

深度

- 雞尾酒般組合不同的手段，來進行深度的防護，使得入侵竊取資料的途徑更加困難

彈性

- 在不同的環境下，能夠更有智慧的適應不同的環境

X-FORT

Work from Anywhere的資安挑戰與對策

1 基礎建設不足

- 以往的基礎建設針對機動工作，非大量遠端工作
- 工作者的所在地設施，無法滿足工作所需
- 用戶端IT環境幾乎沒有資安防護措施

2 非信任裝置 (Use Your Own device)

- 使用裝置可能員工自備，裝置上資料和私人檔案混用
- 缺乏安全保護，作業系統、應用程式、端點安全
- 混用公司專屬及私人連線

3 僵化的政策規則

- 沒有明顯的邊際，難以區分信任區、信任裝置
- 無法因地制宜
- 限制使用，妨礙業務彈性

補強端點防護

- 端點Agent防護如影隨形，控管、記錄不中斷
- 檔案加密、檔案存取控管、資料夾防護
- 限制網路連線、檔案傳輸控制與各式操作記錄

多層次零信任

- 裝置(硬體)鎖定、軟體白名單
- 寫出註冊外接媒體；寫出檔案加密保護
- 敵我識別，防止其他端點裝置存取

情境感知

- 自適應政策，因地制宜
- EDR 事件偵測與反應
- 申請審核開放使用

X-FORT

X-FORT

資安巡航 守護無垠

Ultimate Security for Business Longevity

FineArt