X-FORT

零信任周邊裝置、應用程式、端點、網路存取全部鎖定
Zero Trust on Endpoint

資安顧問 / 陳育徽 Alden Chen

FineArt

為何要保護端點？

Cyber security trends for 2022 and beyond

工作方式改變

- Work From Home
- Telework
- Remote Work

端點安全成為主角

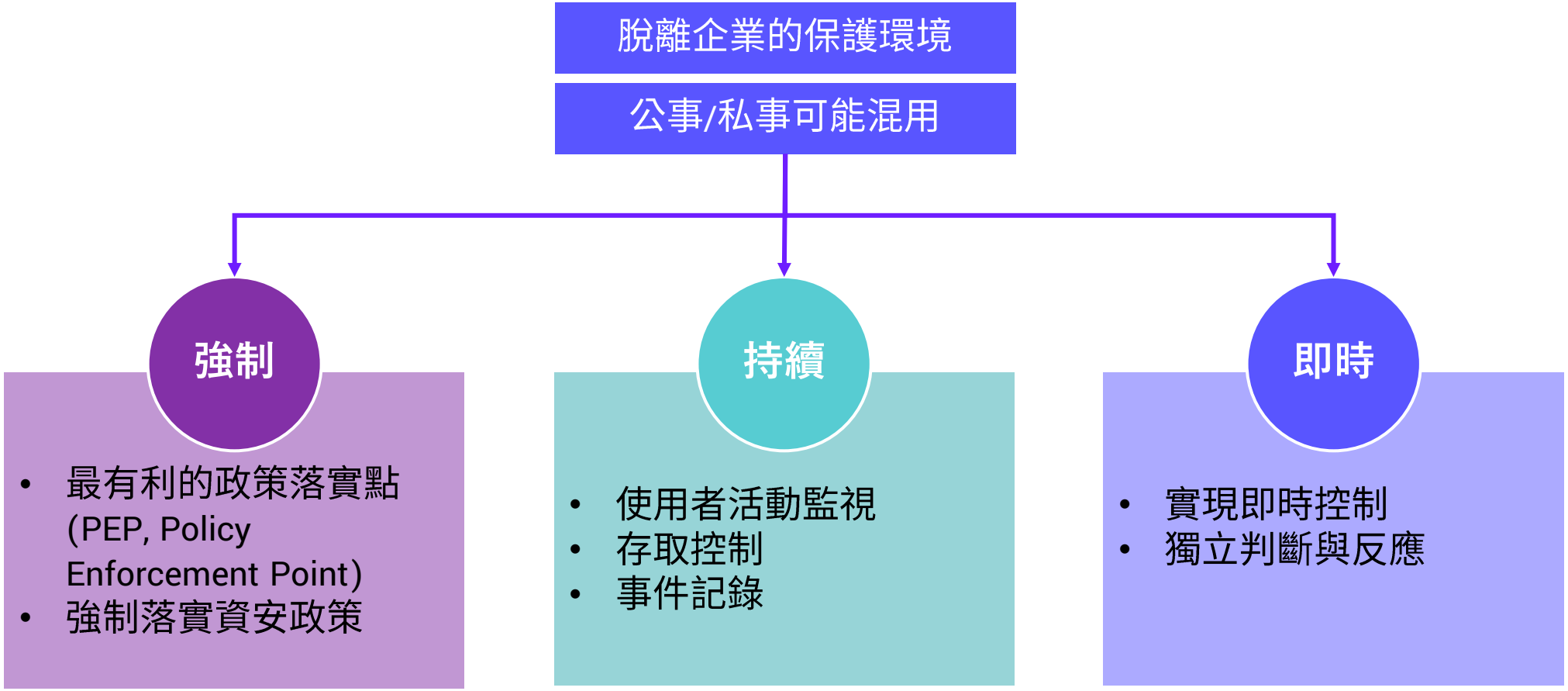
- SASE
- 資料存取去中心化
- 安全邊境消失

勒索持續威脅

- 資料毀損外洩
- 勒贖或報復

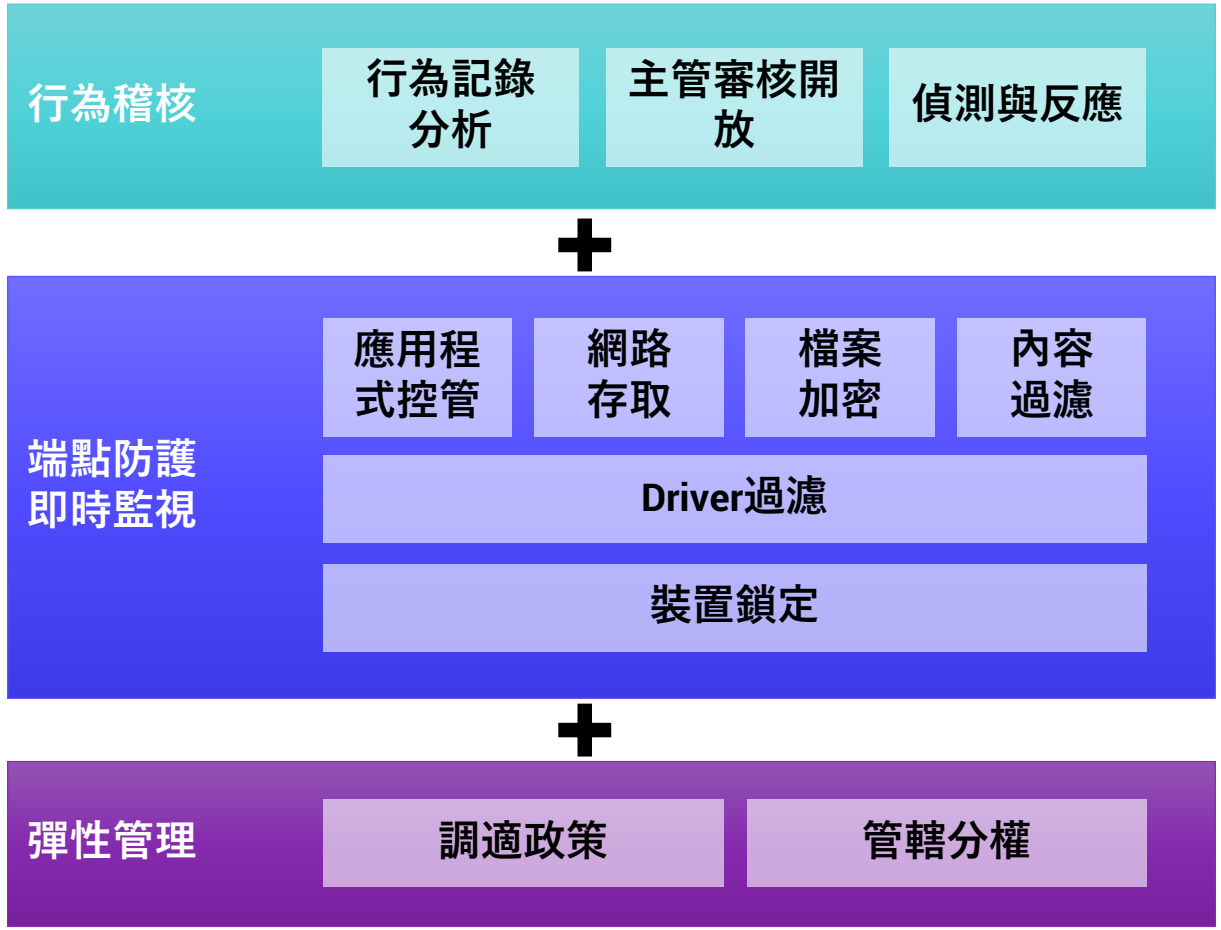
X-FORT

使用端點防護方案的必要性



X-FORT

端點上多層次控管 (管理面)



- 多向量攻擊需要分層端點保護
  - 不依賴基礎建設
  - 不依靠邊境過濾
  - 真實活動記錄
  - 自我協助

X-FORT

X-FORT 端點零信任架構

端點上的零信任

應用程式

Zero Trust Execution
- 應用程式白名單
- FAC 檔案存取控制
- 應用程式活動

端點

Zero Trust Endpoint
- 信任端點存取
- 阻擋非信任端點
- 持續活動監視

裝置

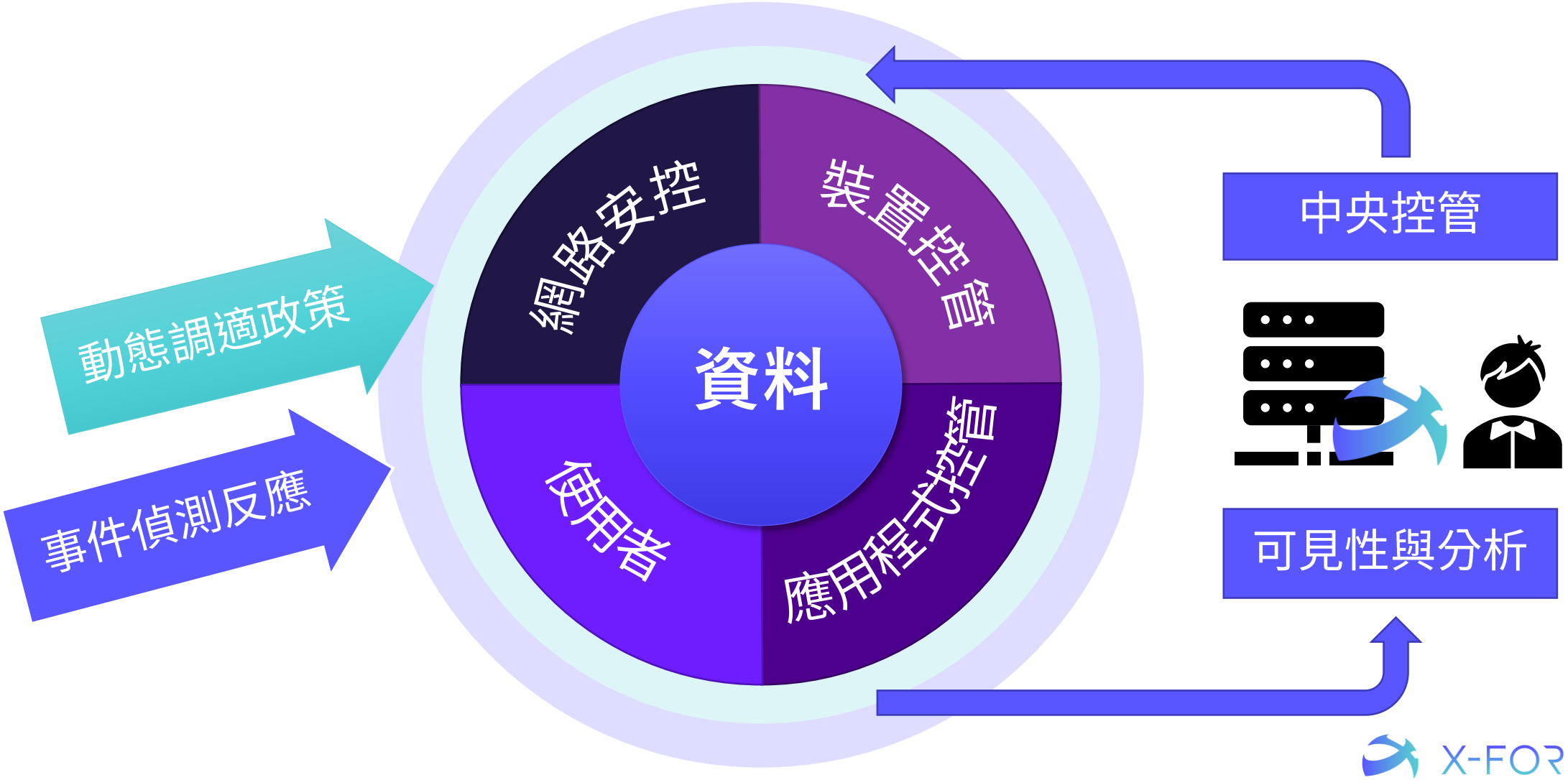
Zero Trust Device
- 註冊信任儲存裝置
- 防止其他裝置連接
- 存取控制

網路存取

Zero Trust Network Access
- 網路存取控制
- 網芳分享控制
- 雲端及檔案傳送

X-FORT

以資料為中心的零信任控管



X-FORT

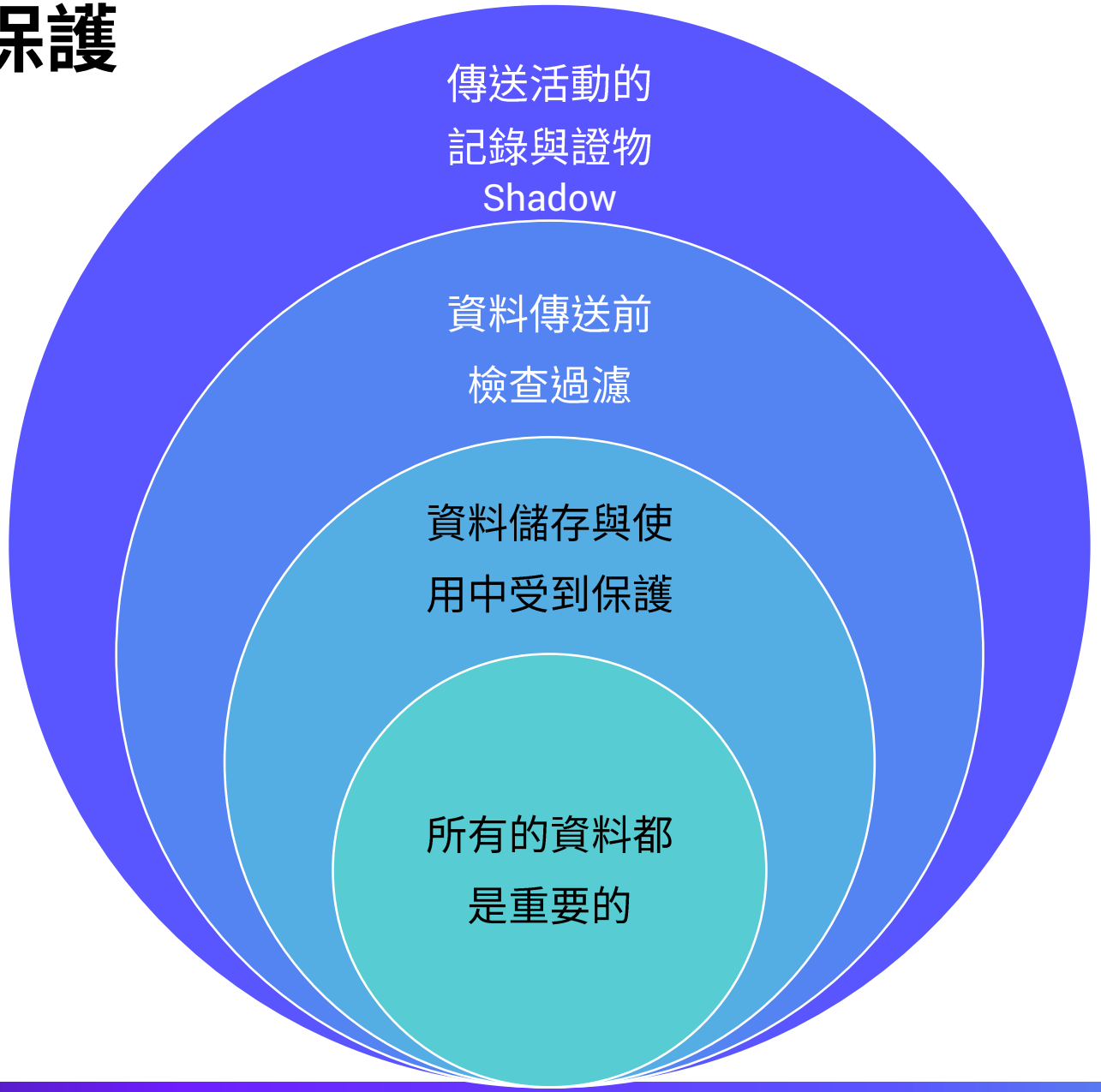
零信任架構


身分驗證
裝置控管
• 裝置鎖定
網路/APP控管
• 應用程式存取
• AWL
• 網路存取
權限控管
• 強制政策
• Role-Based Access Control
加密
• 檔案傳輸
• 電子郵件
• 寫出外接媒體
資料Data
• 研發資料
• 營業秘密
• 個資

X-FORT

資料保護

零信任資料保護



X-FORT

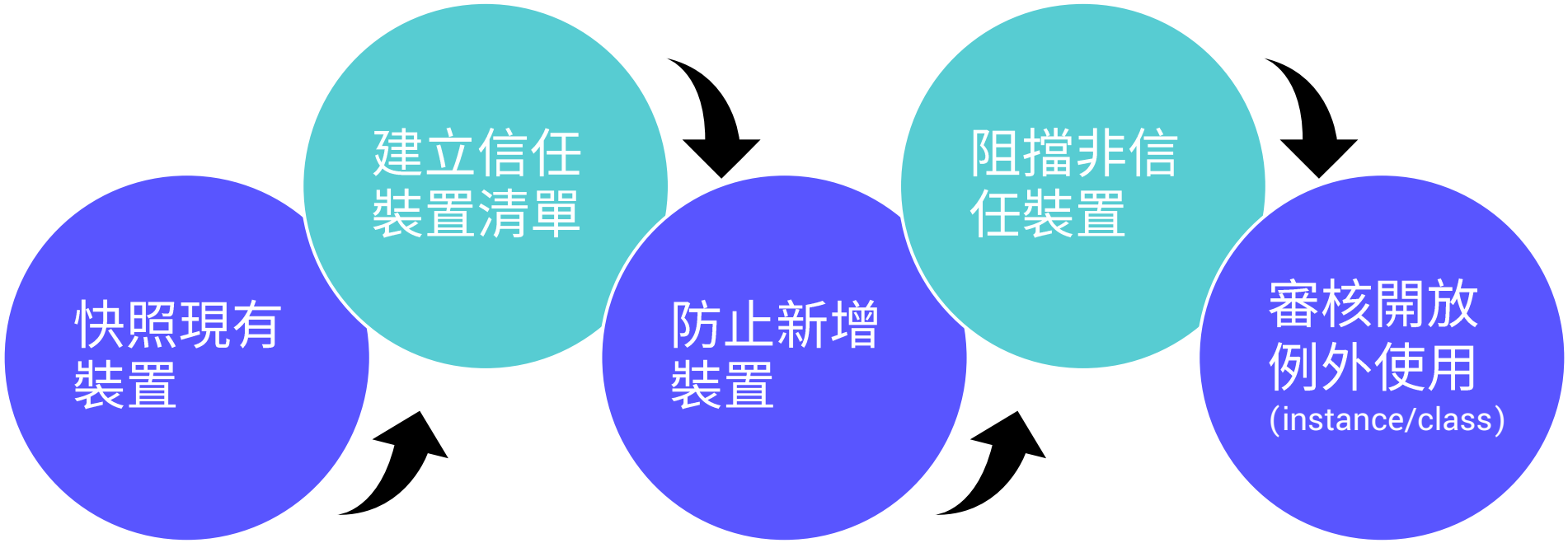
涵蓋資料生命週期

資料夾防護	信任程序存取	防止其他程序存取	防止未授權變更
存取權限	預設內部流通	指定對象	
檔案系統	File Locker 檔案加密	資料夾自動加密	寫出外接碟檔案加密
全碟加密	BitLocker 硬碟加密	MBR 硬碟保護	

X-FORT

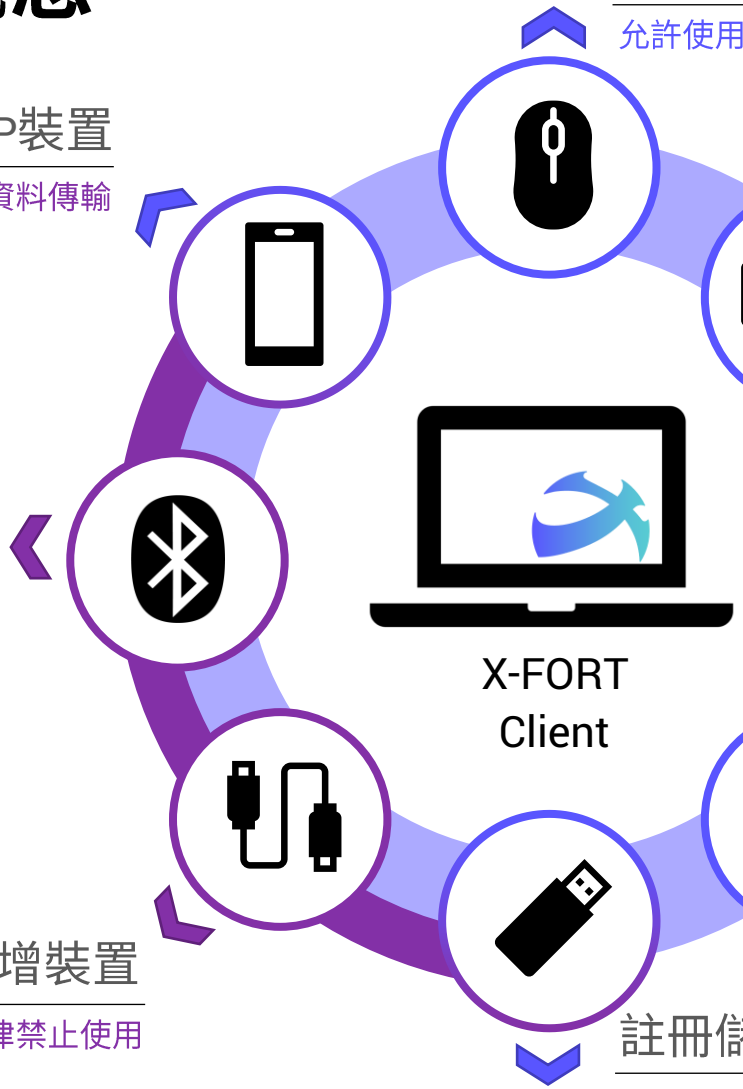
零信任裝置存取

Device Lockdown 裝置鎖定



X-FORT

裝置控管概念



HID裝置
允許使用裝置類型

複合式裝置
允許使用HID

串接儲存裝置
依裝置類型阻擋

串接儲存裝置
依裝置類型阻擋

相機裝置
允許使用裝置

開放指定裝置
依裝置(instance)特徵允許使用

註冊儲存裝置
允許指定外接儲存裝置
開放唯讀，不可寫出

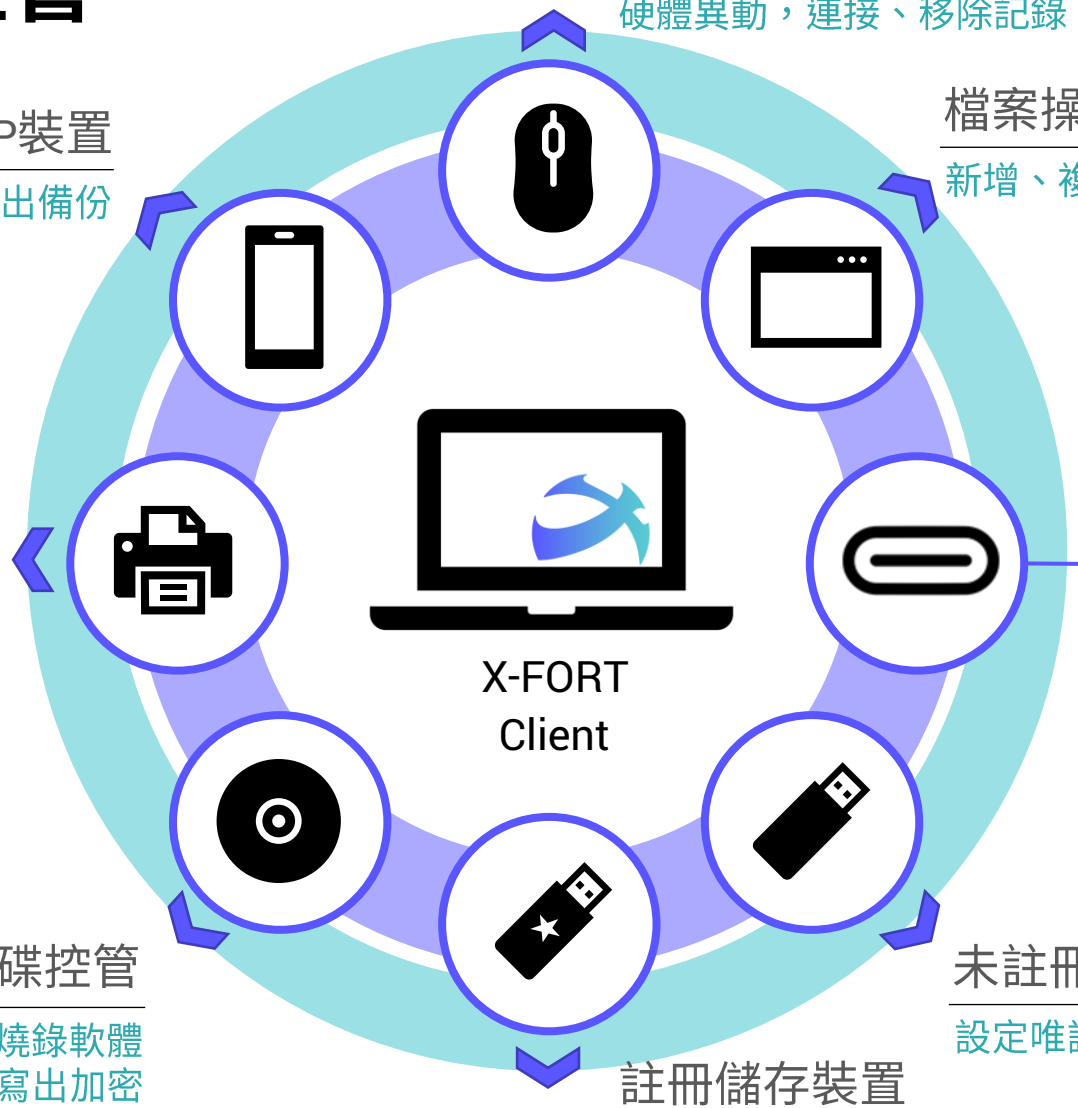
新增裝置
一律禁止使用

其他裝置
一律禁止使用

MTP裝置
開放充電功能/控制資料傳輸

X-FORT

操作行為控管



HID裝置

硬體異動，連接、移除記錄

檔案操作記錄

新增、複製、更名、刪除

MTP裝置

讀寫記錄與寫出備份

列印裝置

印表機控管、列印浮水印
列印記錄與檔案備份

串接儲存裝置

控管視同外接儲存裝置

光碟控管

允許使用燒錄軟體
寫出記錄與備份、寫出加密

未註冊儲存裝置

設定唯讀 (與註冊裝置區別功能)

註冊儲存裝置

限制使用註冊裝置

X-FORT

零信任應用程式

應用程式控管

應用程式白名單

- 建立信任清單
- 預設禁止執行
- 防止安裝程式
- 動態更新

程式執行控制

- 已知不良程式
- 軟體授權管理疑慮
- 浪費運算資源

存取控制

- 通訊連線
- 截圖/剪貼簿
- 網路存取
- 浮水印
- 另存新檔

應用程式白名單機制(AWL)

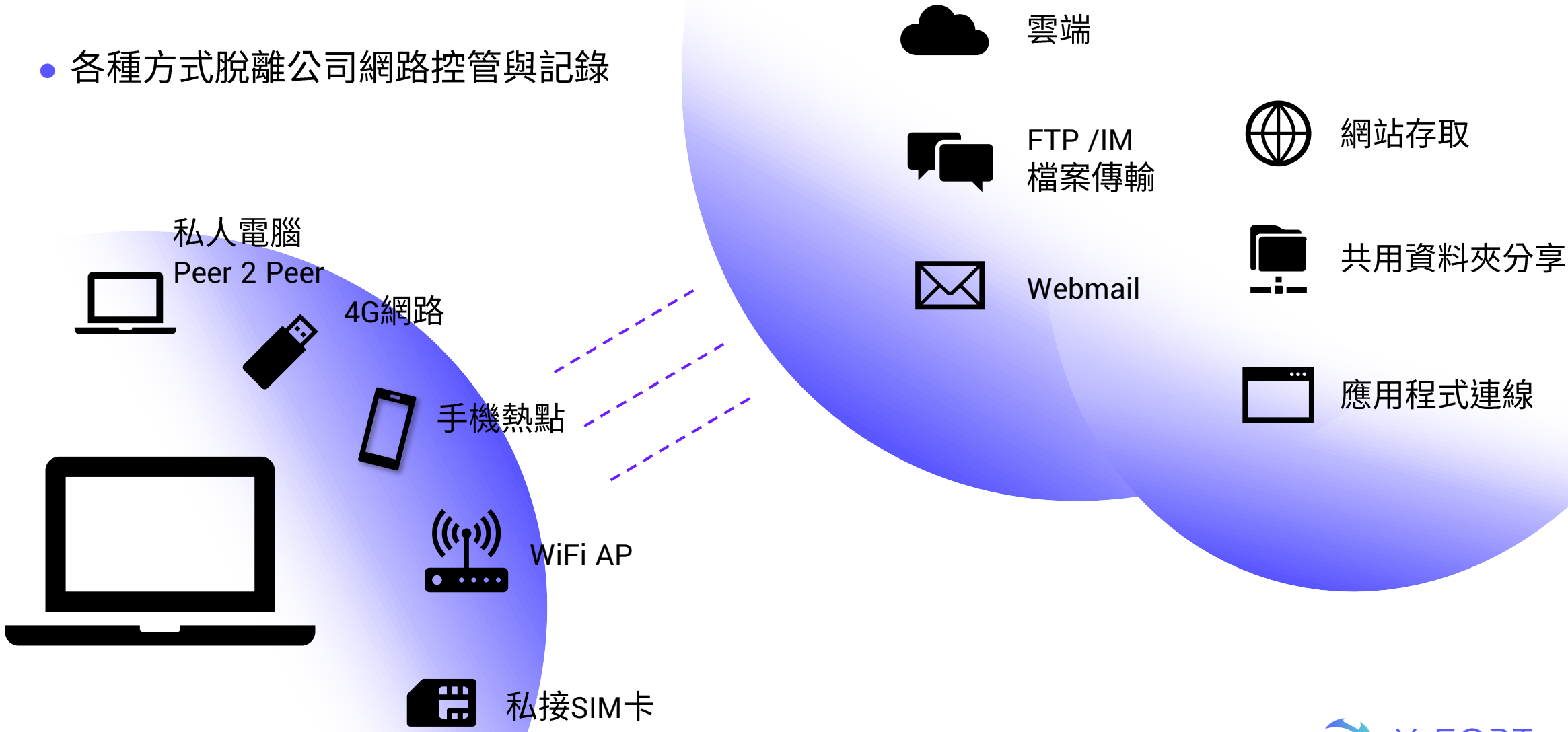
- 白名單決定應用程式執行
- 搭配既有的程式控管
- 防止未經授權的程式安裝
- 預設阻擋未定義的程式執行
- 規則為基礎的機制，不依賴更新特徵
- 在更新修補的空窗之前，就能提供保護力

X-FORT

零信任網路

端點上的網路存取控管

- 各種方式脫離公司網路控管與記錄



X-FORT

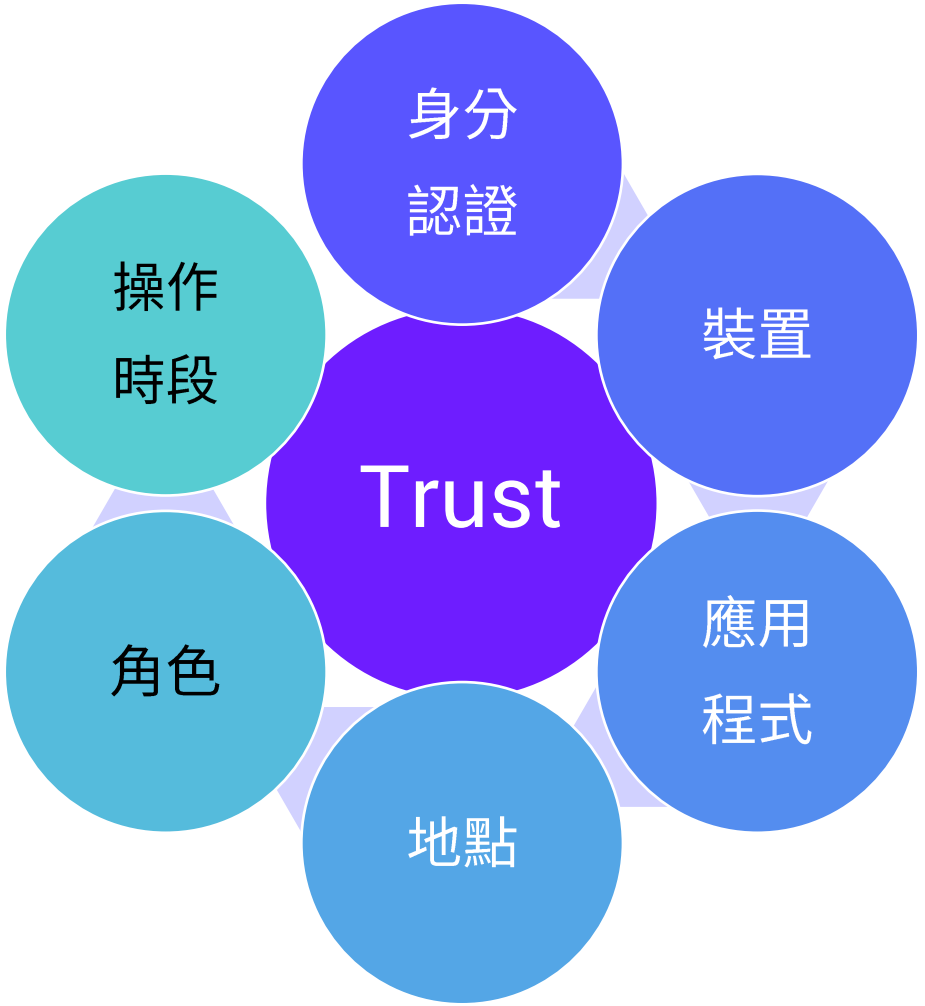
動態政策調整 與 主動偵測&反應

動態評估存取政策

主動追蹤已偵測事件，主動反應，預防災害擴大

為何需要動態切換政策?

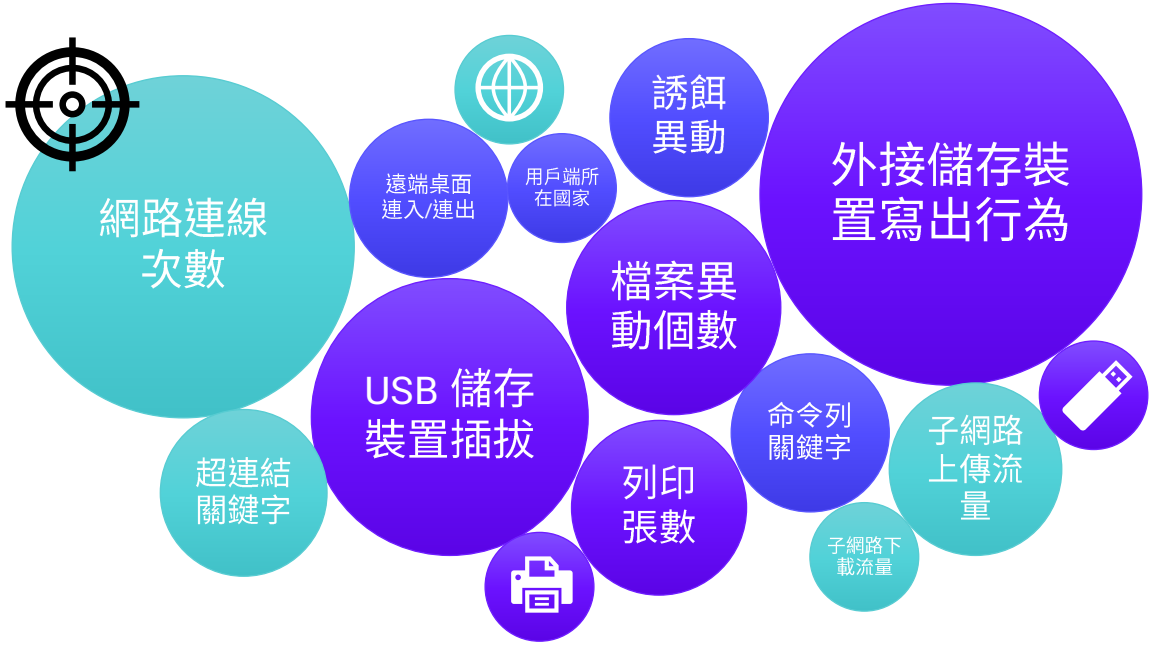
- 傳統靜態政策
  - 沒有彈性，影響生產力
  - 工作不方便，員工反彈
  - 工作開放，形成控管漏洞
  - 被動反應，效果差
- 調適情境變化
  - 非工作時間
  - 檔案操作行為
  - 存取多台伺服器
  - 遠端連線政策

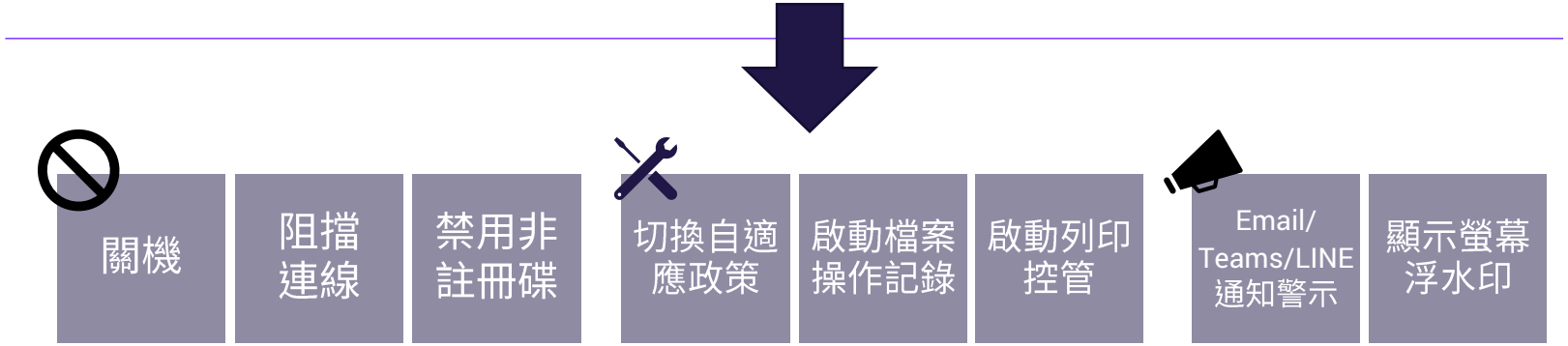


X-FORT

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

資安巡航 守護無垠

Ultimate Security for Business Longevity

FineArt