端點威脅偵測：內部風險的識別與主動回應

精品科技 資安顧問 Alden Chen

alden@fineart-tech.com

FineArt

傳統內部威脅

資料竊取 **Data Theft**	員工竊取公司機密，如客戶資料、財務報告、研發技術文件等。 • 透過 USB 隨身碟、Email、雲端存儲（Google Drive、Dropbox） 傳輸。 • 離職前大量存取機密文件，打算跳槽到競爭對手。
系統破壞 **Sabotage**	IT 員工惡意刪除關鍵系統數據或破壞生產環境。 • 安裝惡意程式（Malware）、後門（Backdoor），讓駭客能入侵企業系統。 • 內部人員啟動DDoS 攻擊癱瘓內部系統。
內部欺詐 **Insider Fraud**	竄改數據、偽造數據，進行內部欺詐。 • IT 人員操控系統權限，讓自己或同夥能繞過內部稽核。

X-FORT

AI 時代的外洩威脅

傳統	現代	
資料竊取 Data Theft	AI模型的資料保存與使用	• 部分GenAI服務保存輸入資料，用於後續模型訓練改進 • 未適當保護而被未授權的第三方存取，導致資料洩漏 • 上傳內部資料後，轉換摘要形式(如簡報、筆記)
系統破壞 Sabotage	模型提煉攻擊 Training Your AI on Desktop	• 硬體進步與精煉技術實現本地訓練與fine-tune • 內部人員利用機密數據訓練私人 AI 模型
內部欺詐 Insider Fraud	敏感信息提示 Prompt	• 將機密信息輸入公共 AI 平台尋求分析 • 提交的內容成為公開查詢資訊
	繞過傳統檢測	• 利用 AI 生成內容 • 轉換訊息形式 • 難以被傳統系統識別的變種數據

X-FORT

引用MITRE 外洩技能

- 拍照或錄製螢幕
- 列印紙本
- 串接HDMI錄影(實體錄影)

實體操作

- 郵件儲存於未寄送信箱
- (檔案或文字)以附件寄送

郵件

- 傳送到外接(可卸除式)儲存媒體
- 以藍牙傳輸檔案

外接裝置

- Corporate email account
- Third-party corporate email account
- Burner email account
- 私人郵件信箱

- SD card
- USB device (e.g., “thumb” drive)

工作管道

- 協作會議軟體傳送訊息(e.g., Microsoft Teams, Slack)
- 傳送到公司所擁有，但網際可存取的伺服器

網路上傳

- SFTP, FTP, Streamlined File Sharing
- 遠端伺服器；裝置 (shared via SMB, FTP)
- Code repository (e.g., Bitbucket, GitHub)
- 雲端儲存空間

- 核准使用檔案傳輸服
- 未奉核檔案傳輸服務

- 雲端檔案儲存s (Dropbox)
- 照片同步 (Google Photos)
- AWS Server

X-FORT

外洩技術與其偵測指標

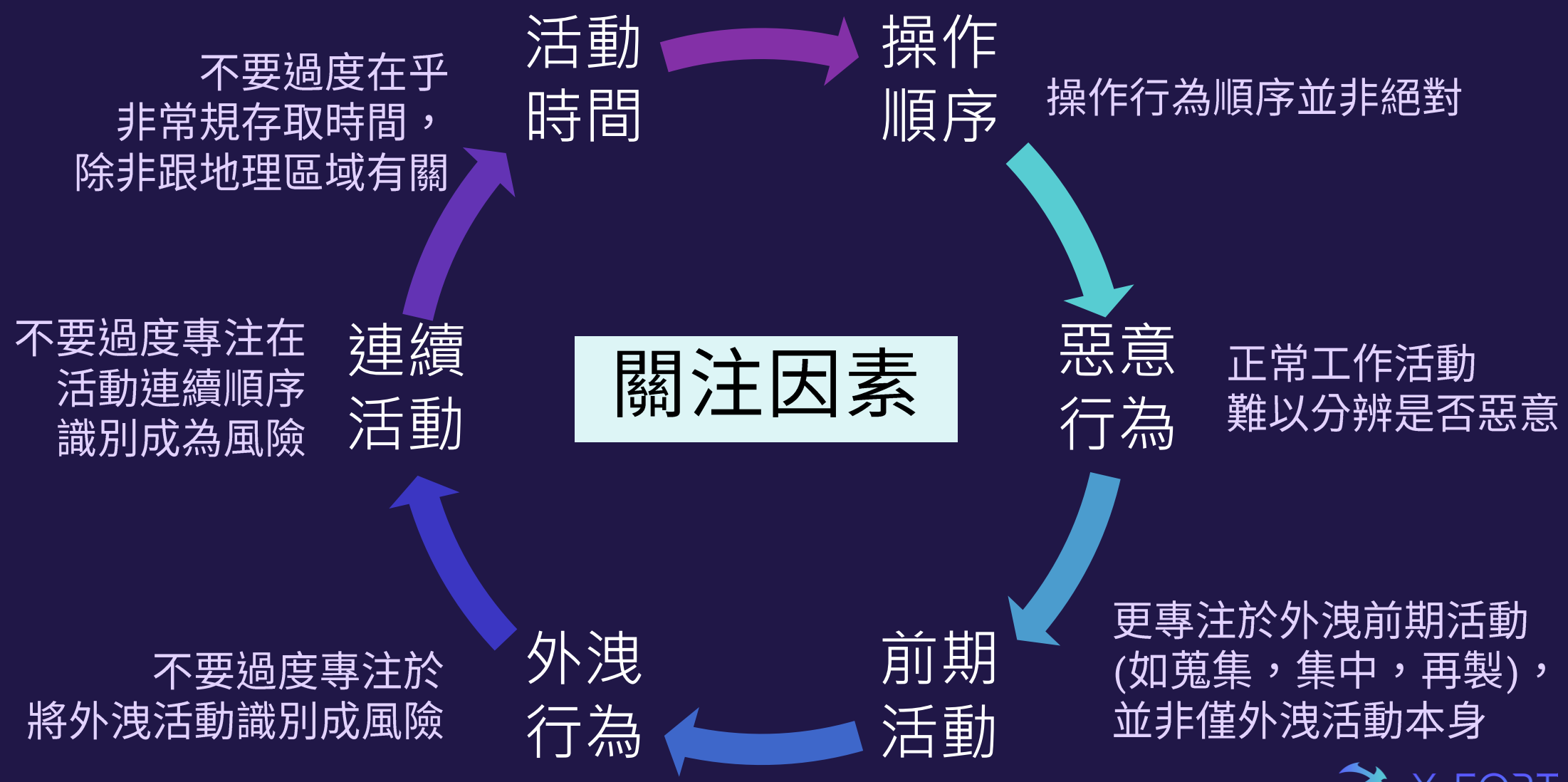
	使用截圖錄影工具	即時訊息通信管道	列印機敏文件
Indicator	截圖工具使用活動	傳送訊息 傳送檔案(LINE, Skype)	列印檔案至印表機 使用非授權印表裝置 列印數量
Detection	應用程式活動 快捷鍵	即時訊息APP活動 訊息內容 檔案上傳活動	列印記錄 浮水印 列印數量監控與警示 列印裝置控管

X-FORT

外洩技術與其偵測指標

	可卸除儲存媒體	外部電子郵件	雲端儲存空間與檔案分享服務
Indicator	傳送檔案至可卸除式媒體 藍牙傳輸檔案	寄送郵件至外部網域 (Gmail, Yahoo) 本文及附件	上傳檔案至雲端硬碟 (Google Drive, Dropbox) 上傳至GitHub SMB檔案分享, FTP
Detection	檔案操作 外接儲存裝置活動記錄	Email 本文及附件 keyword過濾 限制MTA 網頁郵件控管 非信任網域	檔案操作活動 檔案傳輸活動

顛覆傳統觀念



X-FORT

早期預警(EWS)與Pre-Ex Indicators

Harvesting

搜尋關鍵字
內部網站下載
內文摘取(Content Scraping)
檔案分享存取
(瀏覽器)直接列印至PDF

Re-production

放入容器(Zip, Rar, Embed)
更名/另存
再製成另一種檔案
其他隱藏技巧

Transferring

外部/可卸除式儲存媒體
應用程式執行程序
網頁/雲端儲存服務
檔案分享服務
郵件及附件

X-FORT

Insider Threats 的 Endpoint DLP 對策

端點外洩防護

01

離線(Standalone)仍可運作

02

中央管制政策

03

用戶不能自行脫離控管

04

用戶端事件記錄即時回傳

05

用戶端即時應變

X-FORT

裝置與周邊零信任

操作行為控管 (Control)

使用權 (Permission)

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

串接儲存裝置
控管視同外接儲存裝置

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

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

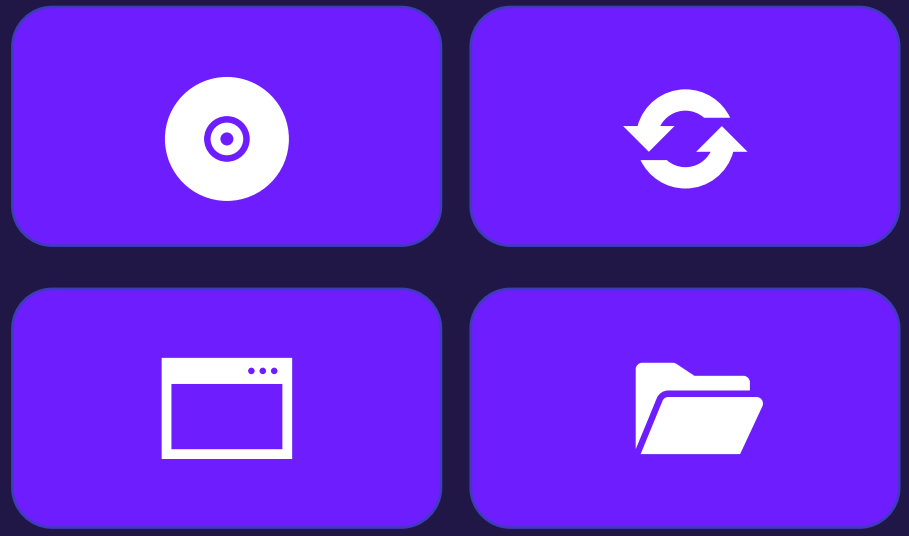
MTP裝置
讀寫記錄與寫出備份

X-FORT

應用程式零信任

限制新增、安裝應用程式

防止未來未知未授權程式存取、執行



自動更新管理

限制資料夾與檔案存取風險分數

X-FORT

網路存取控制

Untrusted device
Peer-to-Peer access
Ad hoc access

4G/5G Adapter

Shared Hot Spot

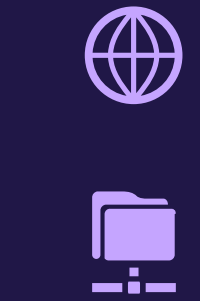
WiFi AP

SIM Card

Cloud Drive
Web Storage

FTP /IM
File transferring

Webmail



Web access
/Upload

Unmanaged Share

Application Access

X-FORT

使用者活動監視User Activity Monitoring（UAM）

檔案操作

- 建立、更名、刪除、移動、複製
- 信任應用程式資料夾存取控制，
- 複製到剪貼簿、記錄文字
- Office 開啟檔案、存檔

網路活動

- 瀏覽網站
- 網芳存取與檔案分享
- 限制網路連線

應用程式活動

- 程序執行
- 網路連線
- 檔案存取

資料傳輸

- 雲端服務
  - 上傳檔案至雲端
  - 瀏覽器複製到雲端(遠端)儲存空間
- FTP/IM/Meeting/檔案分享
- 外部/可卸除式媒體

列印

- 列印裝置
- 浮水印
- 列印頁面與檔案備份

Desktop session recording 擷圖、錄影

- 應用程式
- Instance Message / Net meeting
- Unconditional

X-FORT

資料檔案傳輸控制

檔案傳輸管道

- 網頁式電子郵件
- 即時通訊/線上會議
- 傳輸至外接/可卸除儲存裝置
- 網頁上傳檔案
- 剪貼簿活動

回應處置

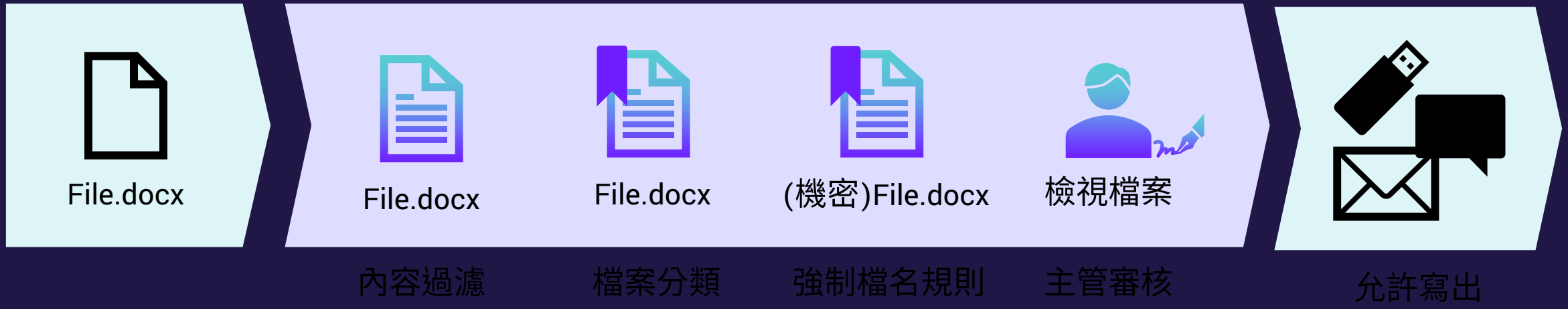
- 內容過濾
- 郵件附件
- 阻擋
- 標示標籤及保留記錄
- 保留證據檔案

X-FORT

數據探索與文件檔案分類

內建正規表示式(RegEx)、關鍵字過濾檔案傳輸內容

- 電子郵件寄出，寫出外接裝置，IM檔案傳輸
- 即時過濾(Just-In-Time)檔案內容，依比對規則阻擋、放行；
- 備份之附加檔案，加註標籤至記錄
- Webmail 過濾郵件內容與備份附加檔案，加註標籤至記錄
- 強制檔案命名規則



X-FORT

軌跡記錄及分類標籤

- 記錄顯示偵測到的InfoType、Match count 匹配摘要
- 依據過濾規則進行分類標籤，例如內容含有電子郵件、身分證號、手機號碼者，標籤為“個資”。

記錄時間	使用者名稱	符合模式數	已符合資訊類型	檔案名稱	已符合分類標籤
2025/03/11 19:16:28	ALDEN	1	Email Address(1)	Data Security Plus (no PII).pptx	TAIWAN PII (Class)
2025/03/11 19:16:28	ALDEN	24	Taiwan PII <tag>(5),Taiwan ID Number <InfoType Tag>(5),Mobile Phone <InfoType T...	Malaysia IC and Taiwan ROC PII in Contra...	Malaysia PII (Class)
2025/03/11 19:16:28	ALDEN	67	Taiwan ID Number <InfoType Tag>(12),Mobile Phone <InfoType Tag>(12),Email Add...	Malaysia IC and Taiwan ROC PII.xlsx	Malaysia PII (Class)
2025/03/11 19:16:28	ALDEN	23	Taiwan PII <tag>(5),Taiwan ID Number <InfoType Tag>(5),Mobile Phone <InfoType T...	Taiwan ROC PII in Contract.docx	TAIWAN PII (Class)
2025/03/11 19:16:28	ALDEN	66	Taiwan ID Number <InfoType Tag>(12),Mobile Phone <InfoType Tag>(12),Email Add...	Taiwan ROC PII.xlsx	TAIWAN PII (Class)
2025/02/26 18:09:53	ALDEN	24	Taiwan PII <tag>(5),Taiwan ID Number <InfoType Tag>(5),Mobile Phone <InfoType T...	Malaysia IC and Taiwan ROC PII in Contra...	Malaysia PII (Class)
2025/02/26 18:09:53	ALDEN	67	Taiwan ID Number <InfoType Tag>(12),Mobile Phone <InfoType Tag>(12),Email Add...	Malaysia IC and Taiwan ROC PII.xlsx	Malaysia PII (Class)
2025/02/26 18:09:53	ALDEN	23	Taiwan PII <tag>(5),Taiwan ID Number <InfoType Tag>(5),Mobile Phone <InfoType T...	Taiwan ROC PII in Contract.docx	TAIWAN PII (Class)
2025/02/26 18:09:53	ALDEN	66	Taiwan ID Number <InfoType Tag>(12),Mobile Phone <InfoType Tag>(12),Email Add...	Taiwan ROC PII.xlsx	TAIWAN PII (Class)

X-FORT

端點防護控管範圍

X-FORT Endpoint Protection Platform

X-FORT

最後的拼圖

Windows原生記錄難以提供足夠的事件視角

主動事件回應

使用者的活動偵測條件

- 使用者的活動偵測條件
  - 連接外接裝置
  - 使用者活動
    - 檔案操作
    - 網站存取瀏覽
    - 列印/列印至PDF
  - 網路檔案分享
  - 開啟通訊埠
  - 遠端桌面連線

應變與行動

- 應變與行動
  - Blocking 阻擋
    - Shutdown 關機
    - Disable network connection 停用網路連線
    - Disable USB external storage 關閉外接裝置
  - 動態調整政策
    - 置換更新使用者政策
    - 啟用檔案操作記錄
    - 啟動列印控管與記錄
  - 提示與告警
    - 用戶端螢幕浮水印
    - 電子郵件通知管理人員、主管、稽核

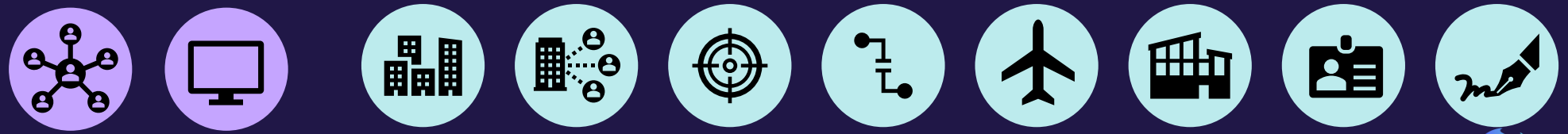
動態適應安全政策調整

端點安全政策

- 以角色為基準部署
  - 使用者角色User / OU / Group
  - 本機電腦角色/ Group (Unconditional)
- 動態政策部署(Conditional)
  - 條件變更自動調整
  - 依網路區段
  - 應對事件回應Incident responsed
  - 臨時政策Temporary
  - Out-of-Box Baseline,　同中求異
  - 未驗證身分的對象

Practice

- 最有效的政策落實點
- Best (PEP, Policy Enforcement Point)



X-FORT

Ultimate Security for Business Longevity

www.fineart-tech.com

FineArt