X-FORT

阻斷勒索！端點控管讓 EDR 反應更直覺快速

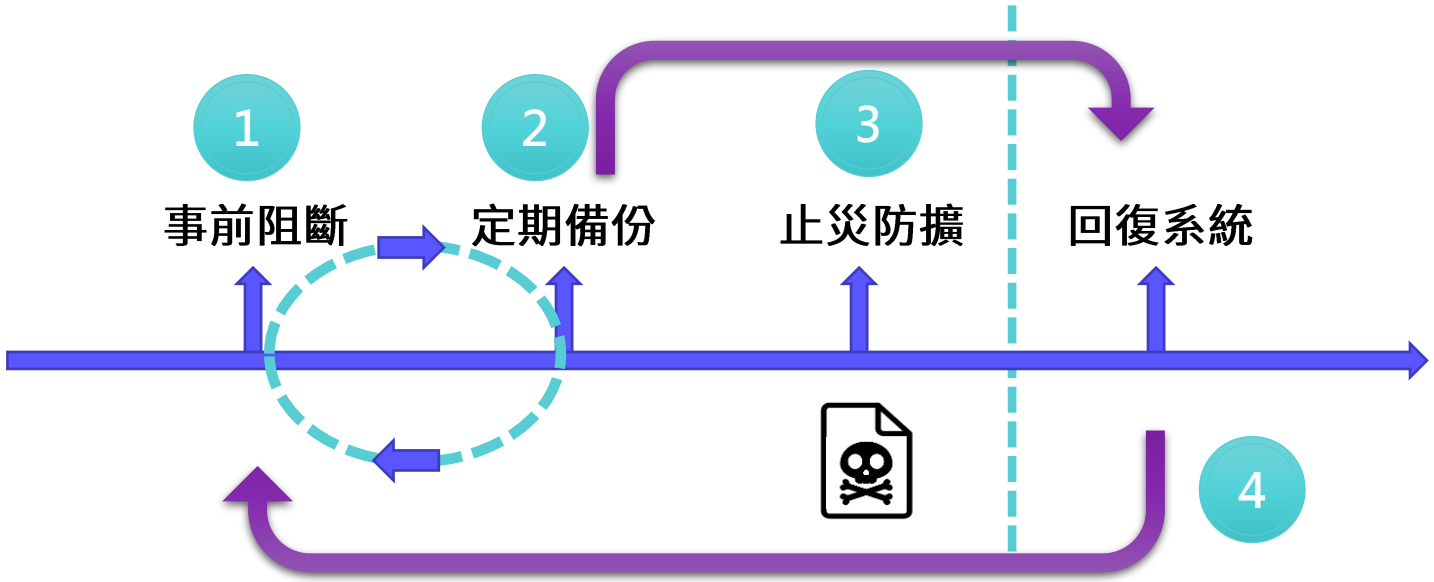
精品科技 技術總監 賴頌傑

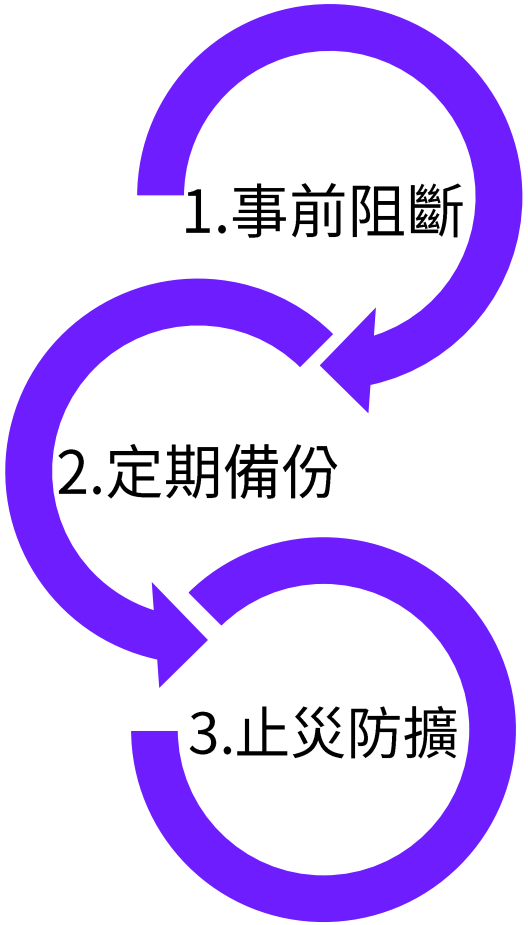
dean@fineart-tech.com

FineArt

阻斷勒索軟體的三大重點

- 事前阻斷
  運用應用程式白名單機制，足以切斷大部份的駭客攻擊
- 定期備份
  完整保護下的防駭備份，讓備份資料受到第二層保護
- 止災防擴
  EDR 方案，讓問題發生時，端點主動防堵，避免災害擴大



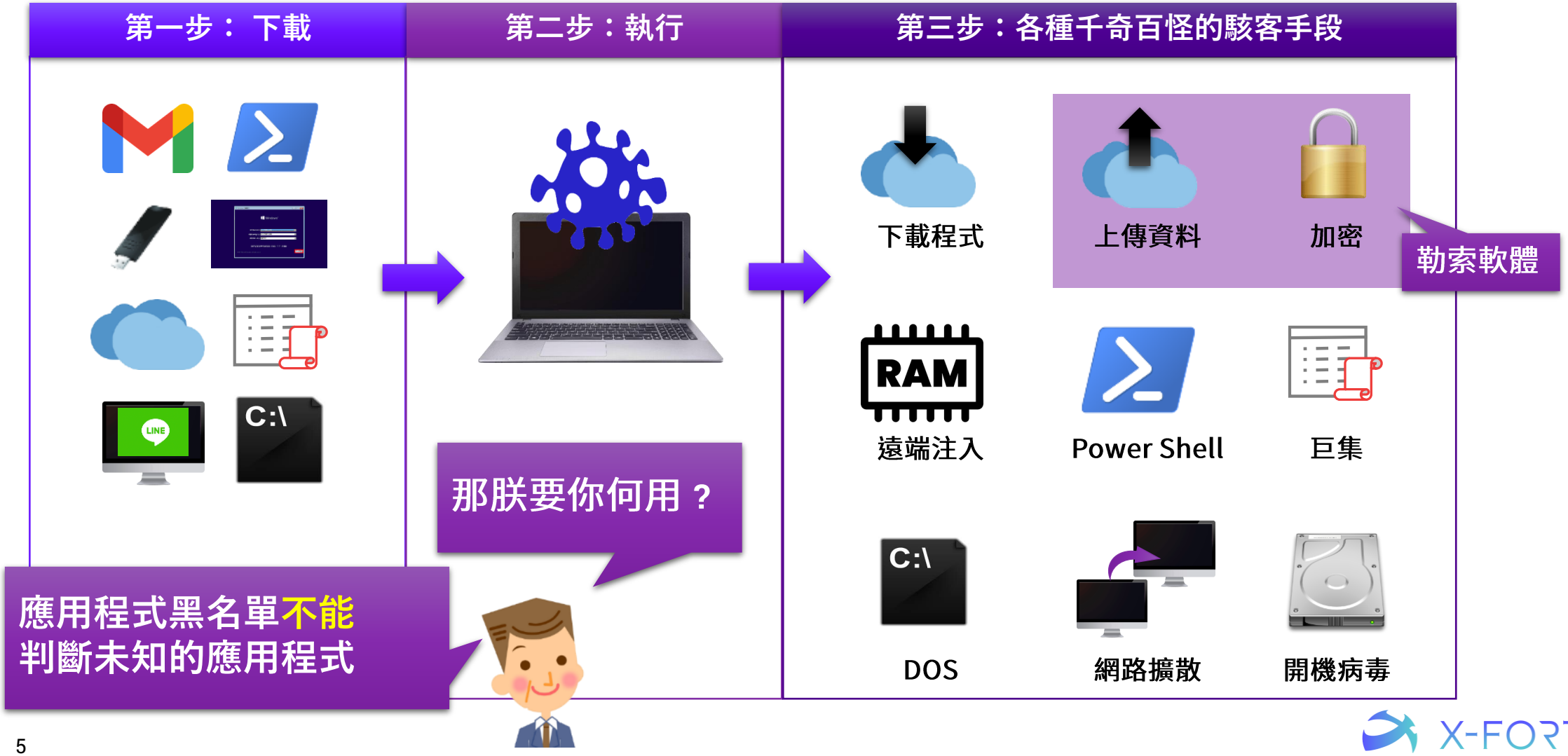


X-FORT

事前阻斷

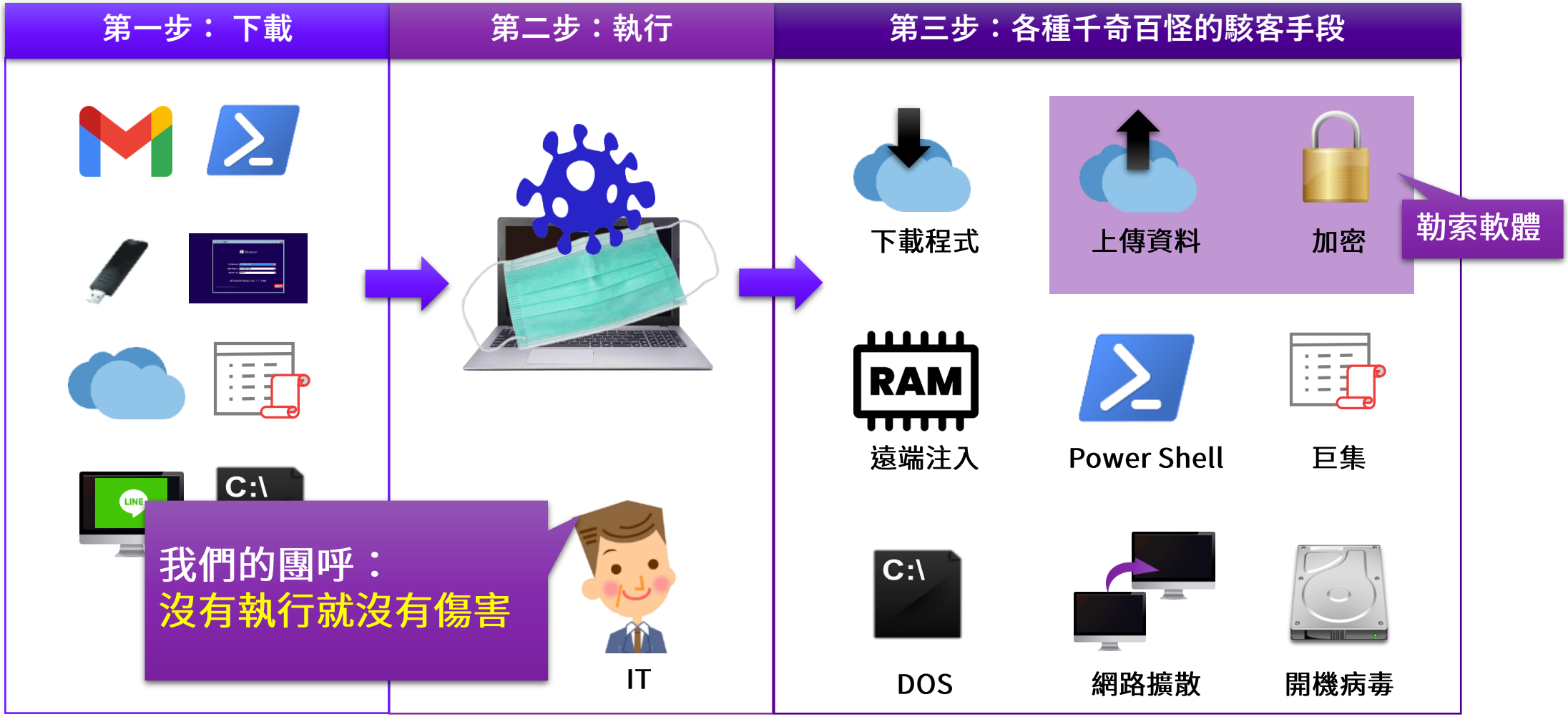
運用應用程式白名單機制，足以阻斷大部份的駭客攻擊

事前阻斷 ➔ 推薦使用應用程式控管



X-FORT

防堵攻擊的正確態勢 ➔ 在第二步執行時控管



X-FORT

應用程式控管是什麼？➔ 使用白名單技術

傳統黑名單技術

IT 列舉黑名單

採用應用程式白名單控管技術

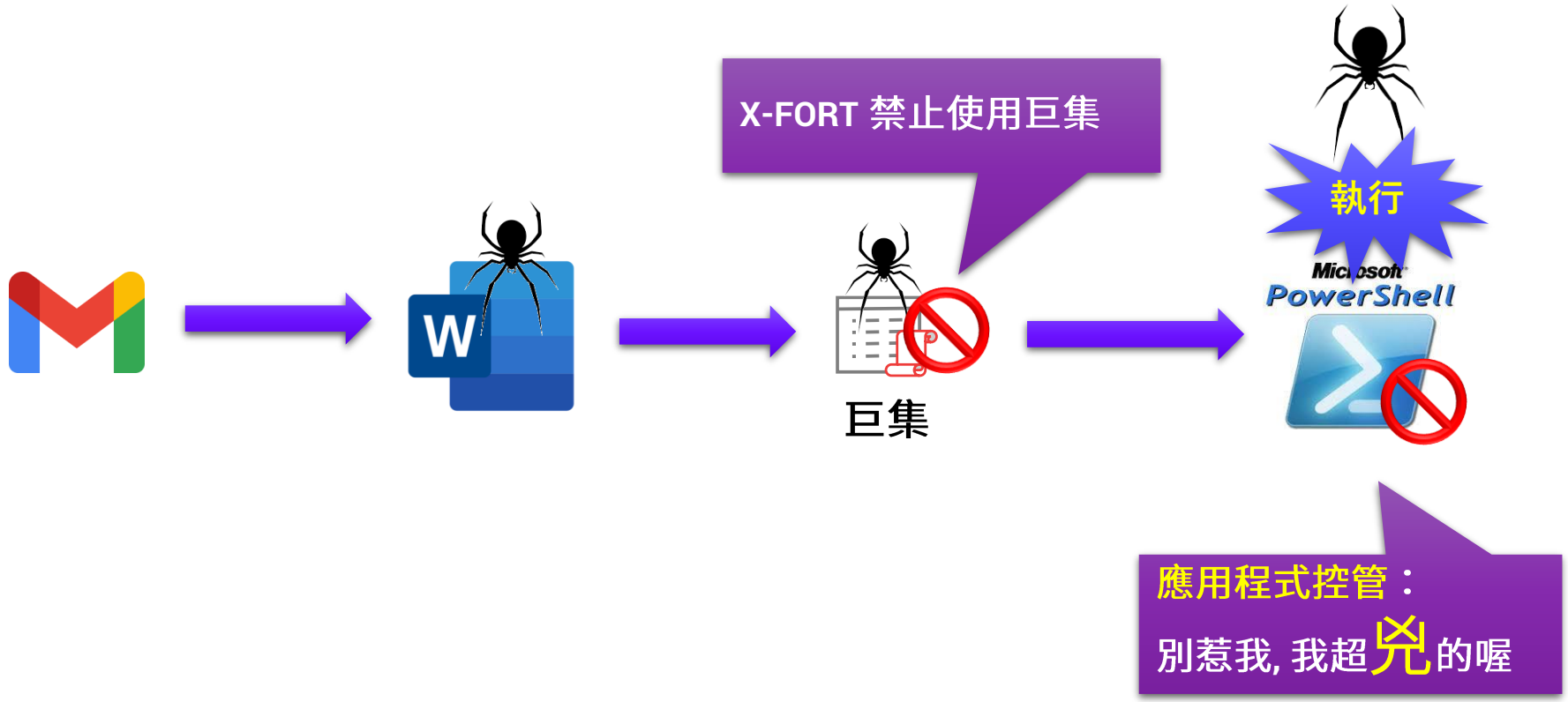
IT 建立白名單

取得應用程式資訊

完整白名單

例子 1: 蜘蛛勒索軟體

- 入侵流程 及 阻擋點 🚫

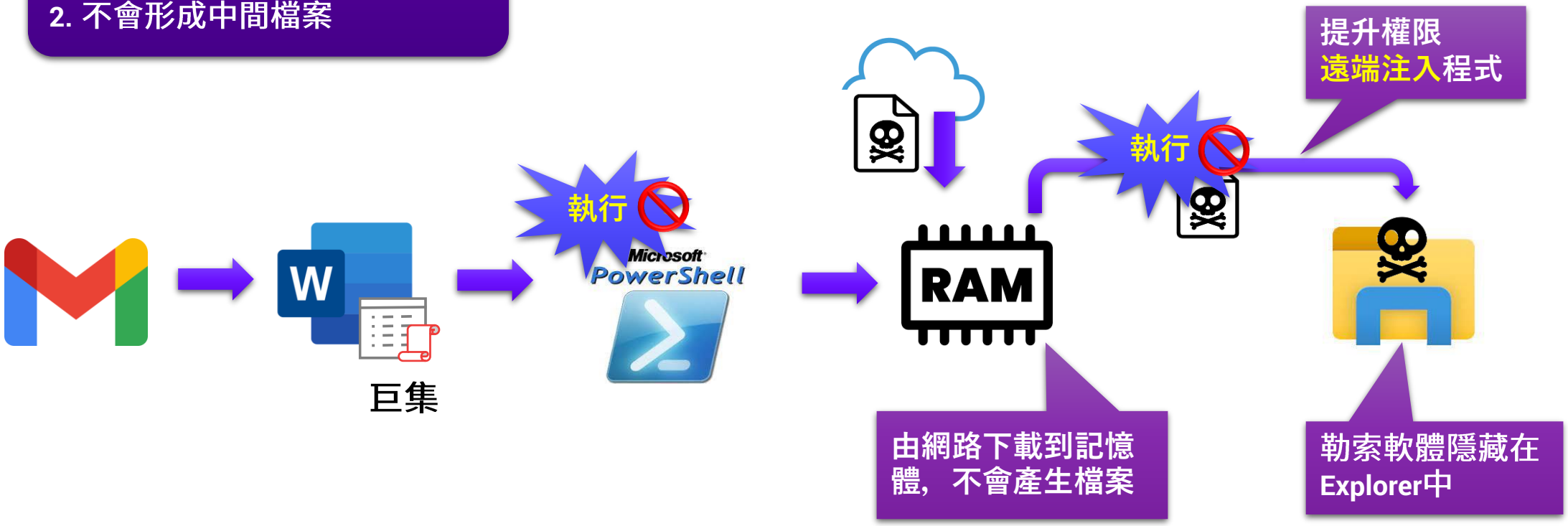


X-FORT

例子 2: 勒索軟體 NetWalker

- 入侵流程 及 阻擋點 🚫

NetWalker 特色:
1. 使用 Windows 內建程式
2. 不會形成中間檔案



X-FORT

應用程式白名單的彈性管理

清查

由使用者或管理者發動
取得應用程式白名單

使用者自決

自行決定新增白名單
可關閉應用程式控管

父行程

防止使用合法的應用程式做為攻擊工具；使用 LOLBAS 工具 Bash.exe

記錄

完整的記錄，可重新滙成白名單

觀察模式

蒐集使用者日常執行的程式並列管

繼承

動態加入信任的應用程式所帶起的子程式

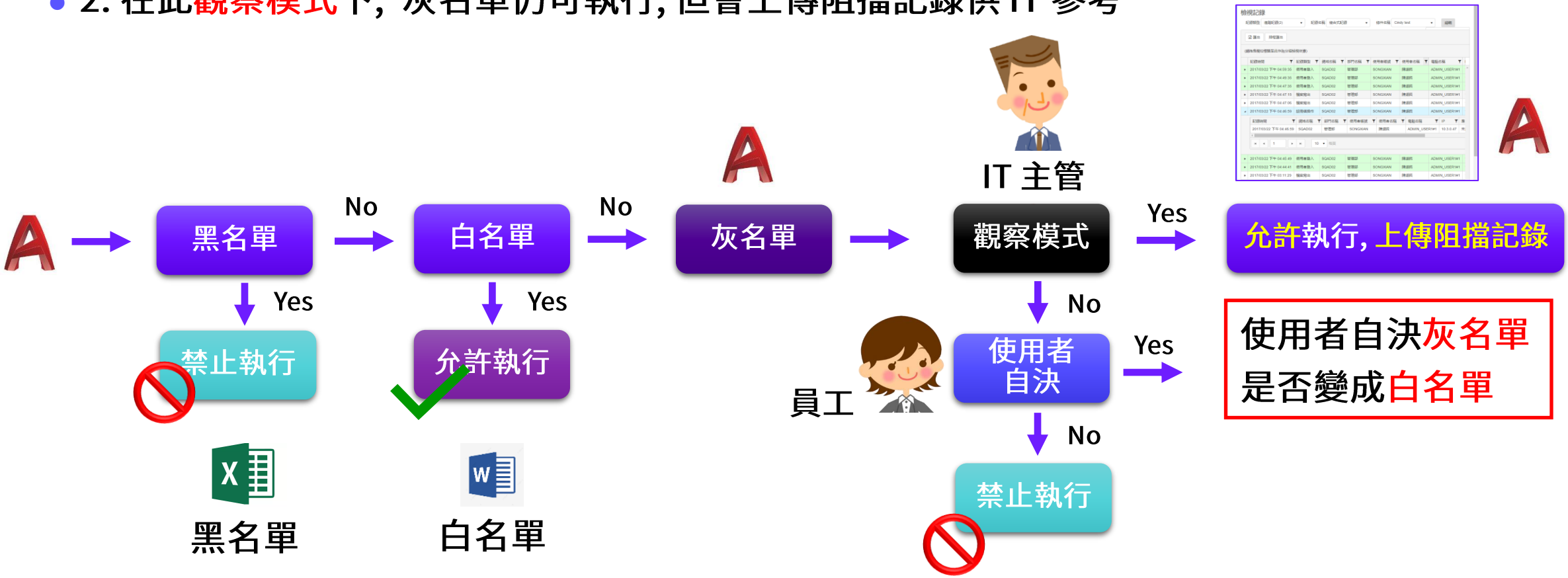
自適性

符合部份簽章字串即可為白名單；如：使用 *Microsoft*

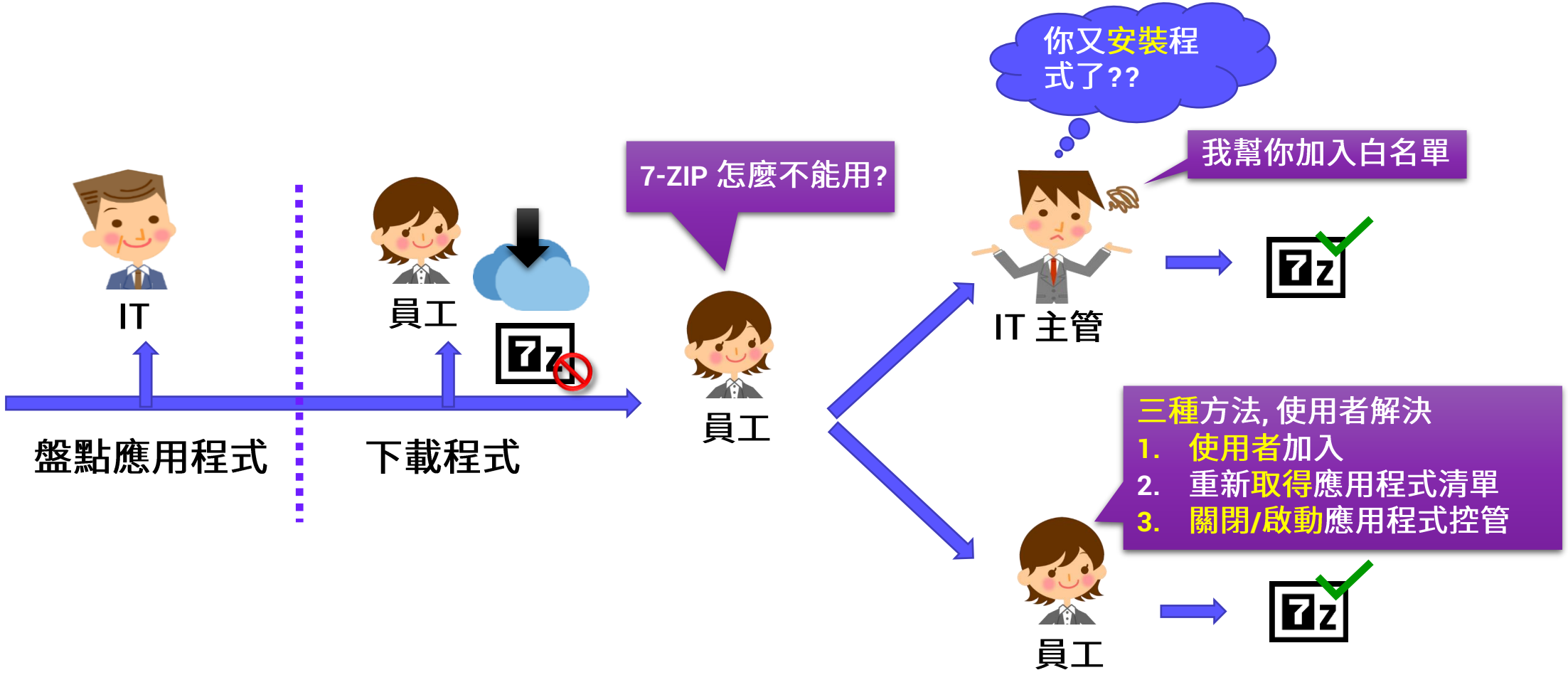
X-FORT

觀察模式: 在不打擾使用者情況下, 觀察漏網之漁

- 1. 在剛剛部署應用程式控管功能, 建議開啟觀察模式
- 2. 在此觀察模式下, 灰名單仍可執行, 但會上傳阻擋記錄供 IT 參考

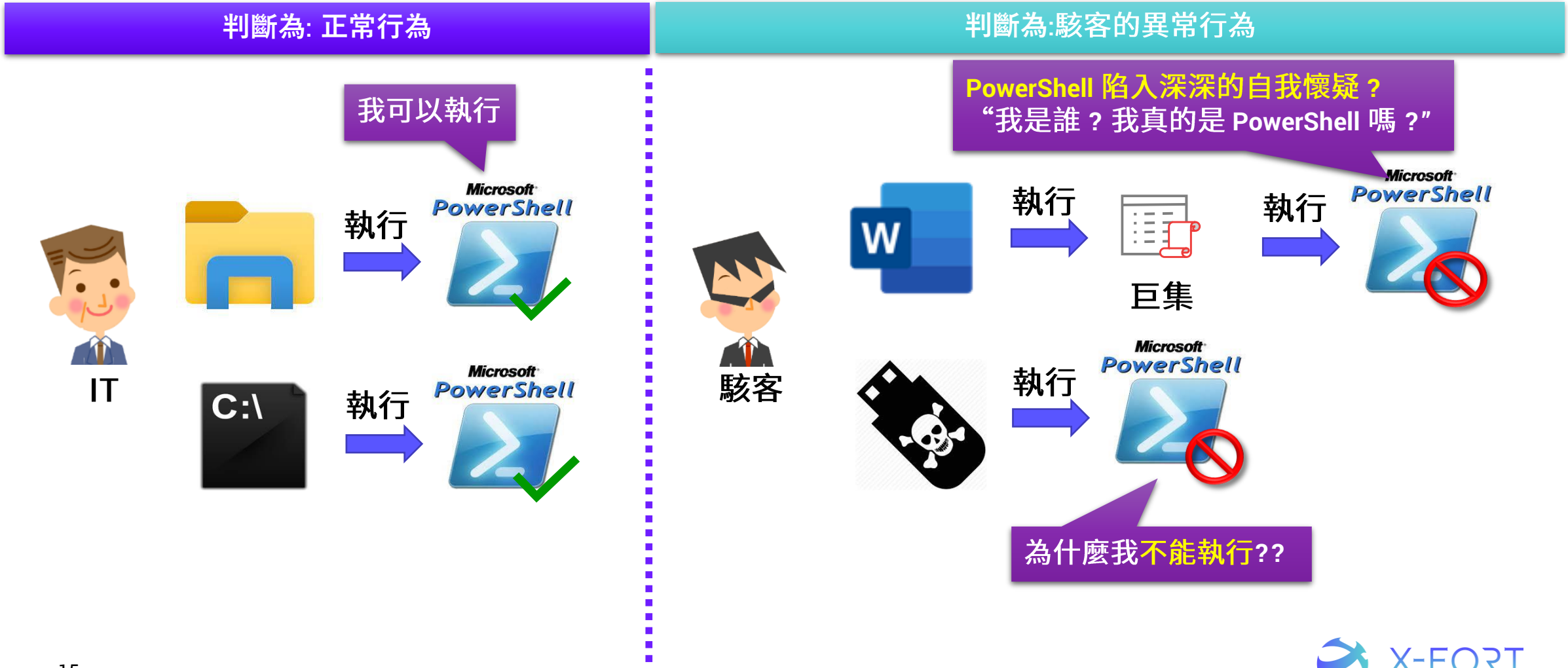


使用者自決


IT
盤點應用程式
員工
下載程式
7-ZIP 怎麼不能用?
員工
你又安裝程式了??
我幫你加入白名單
IT 主管
三種方法, 使用者解決
1. 使用者加入
2. 重新取得應用程式清單
3. 關閉/啟動應用程式控管
員工

X-FORT

控管父行程：防止使用合法的應用程式做為攻擊工具



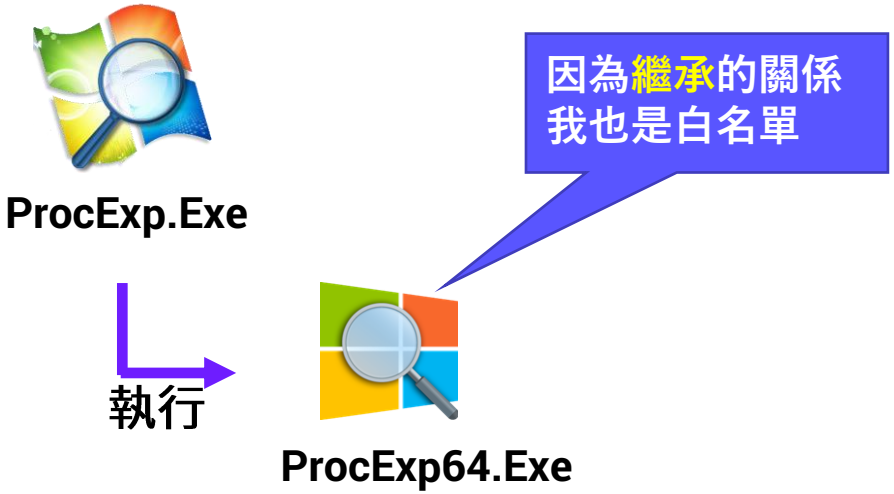
X-FORT

繼承：白名單的子程式繼承為白名單

例 1:

ProcExp.Exe 會在執行時, 解出另一子程式 ProcExp64.Exe

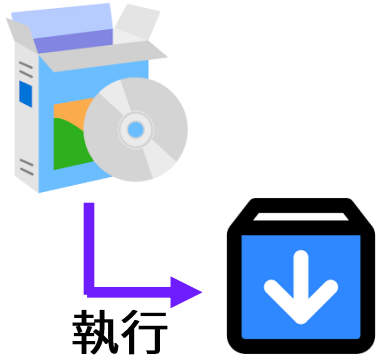
在 Win64 下, 會執行 ProcExp64.Exe 取代原 ProcExp.Exe



例 2:

安裝程式, 會執行安裝子程式；

子程式也會被信任

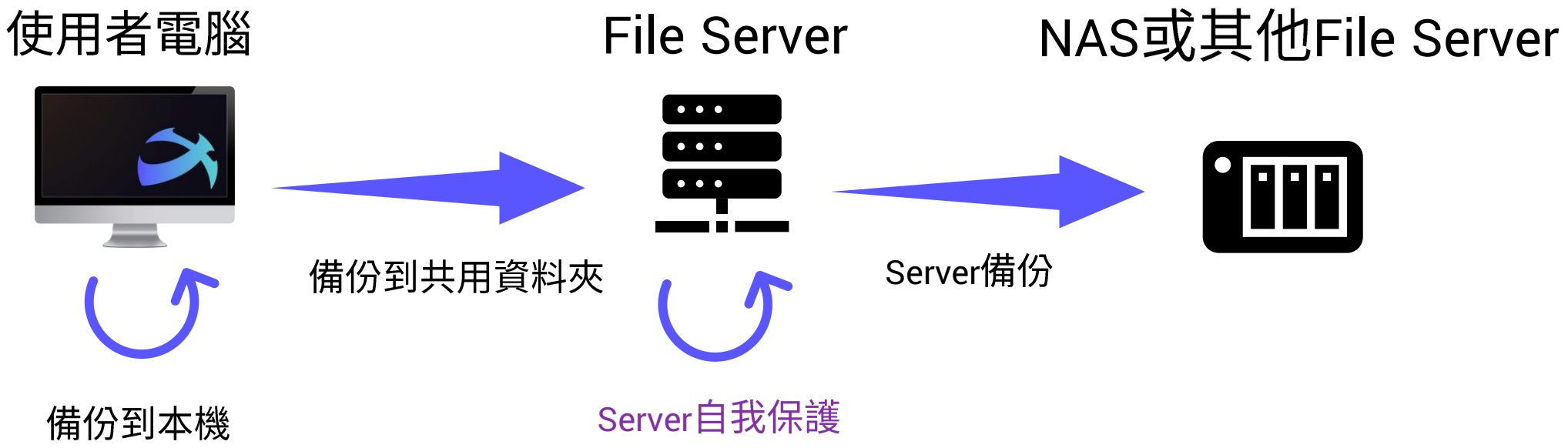


X-FORT

3. 定期備份

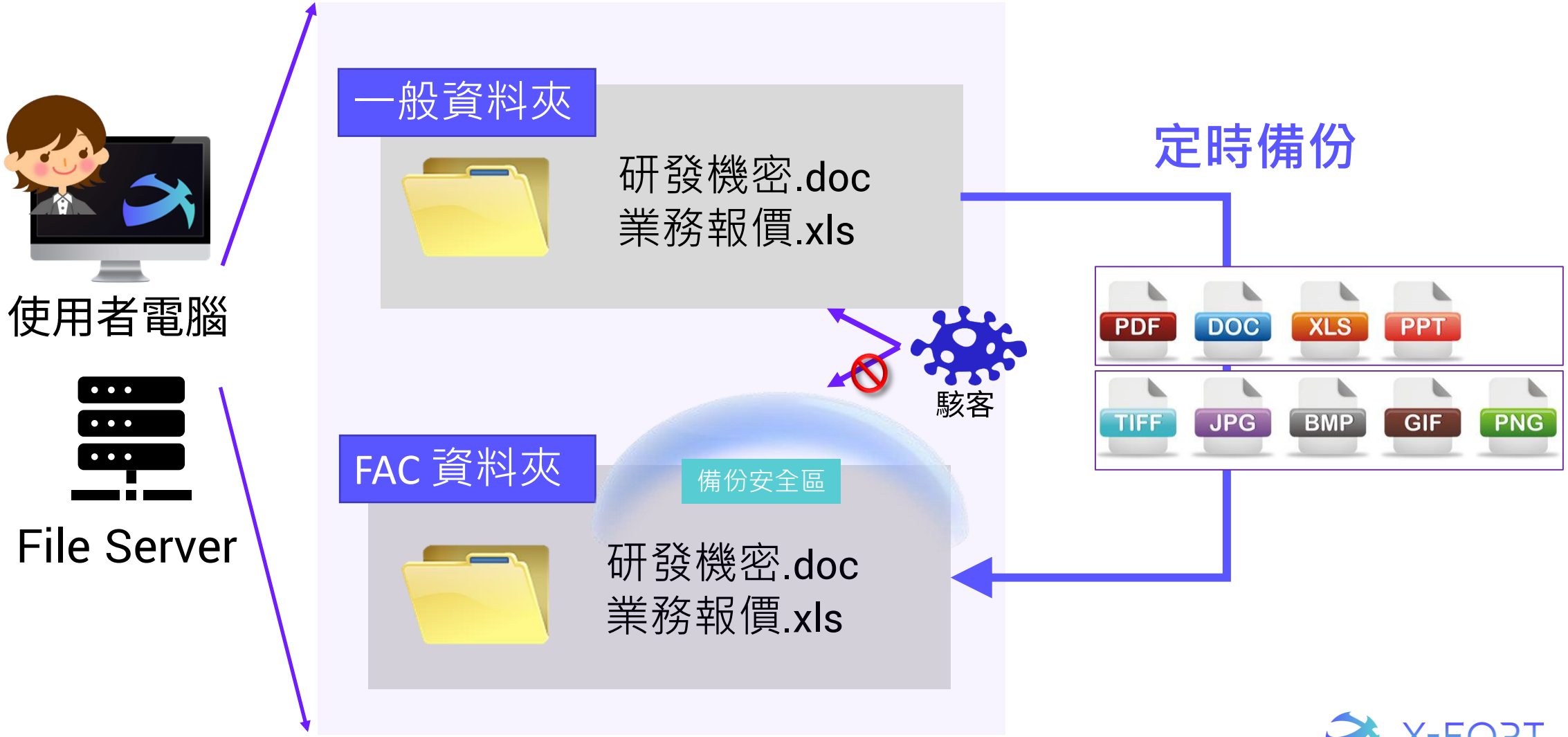
完整保護下的防駭備份，讓備份資料受到第二層保護

面對勒索軟體 – 備份仍是必要的減災方案



X-FORT

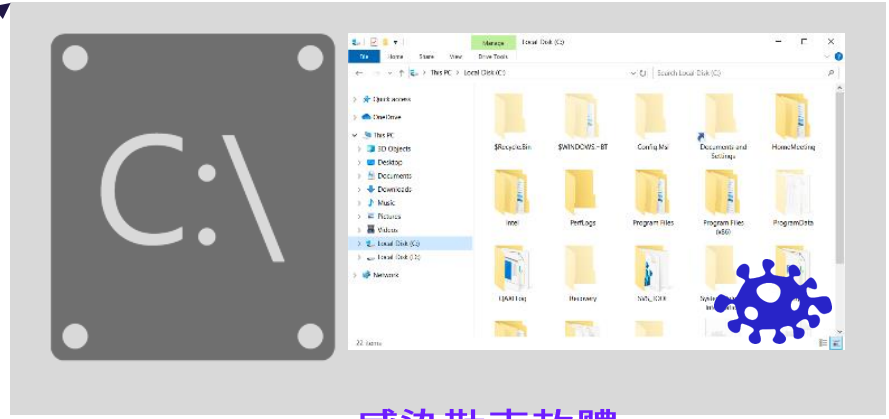
FAC 的應用一: 保護備份目錄 (安全備份)



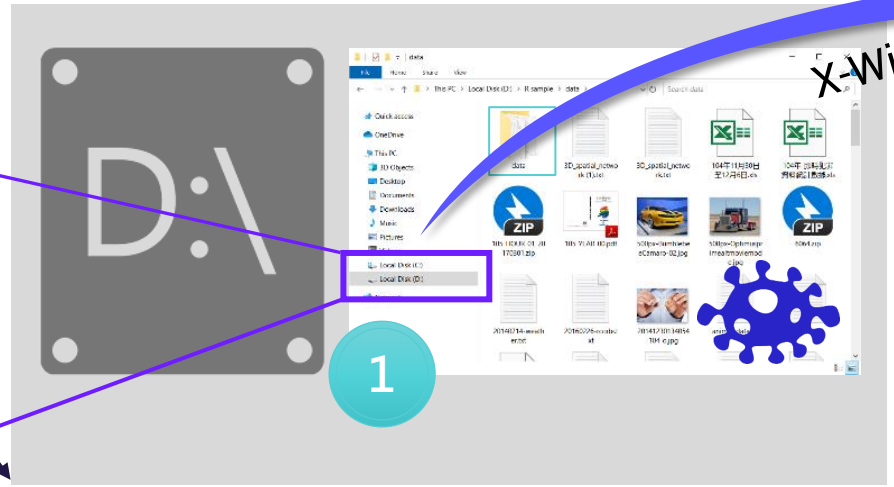
X-FORT

FAC 的應用二: 保護工作目錄 (安全工作區)

- 檔案鎖定列表
- 限制可存取的檔案的應用程式



感染勒索軟體



X-Wizard

安全工作區

透過X-Wizard可把安全區的檔案從受感染的電腦中存到外接碟

外接碟

IT 主管

- 重要檔案存放在安全區
- 特定軟體才能讀寫安全區檔案

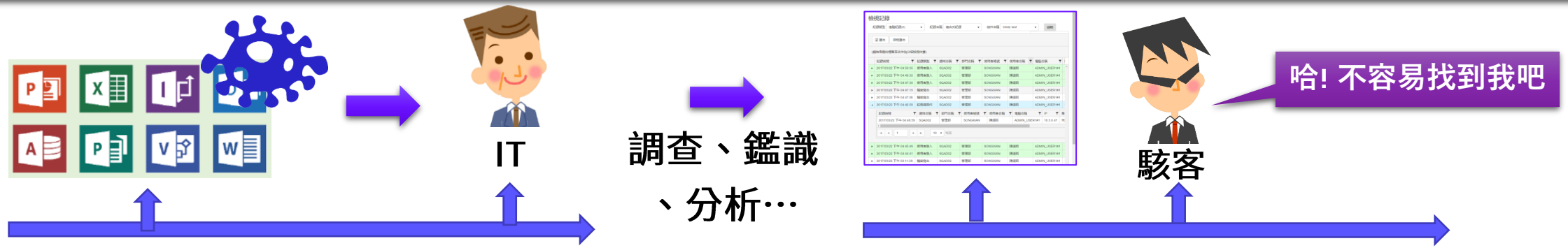
X-FORT

4. 止災防擴

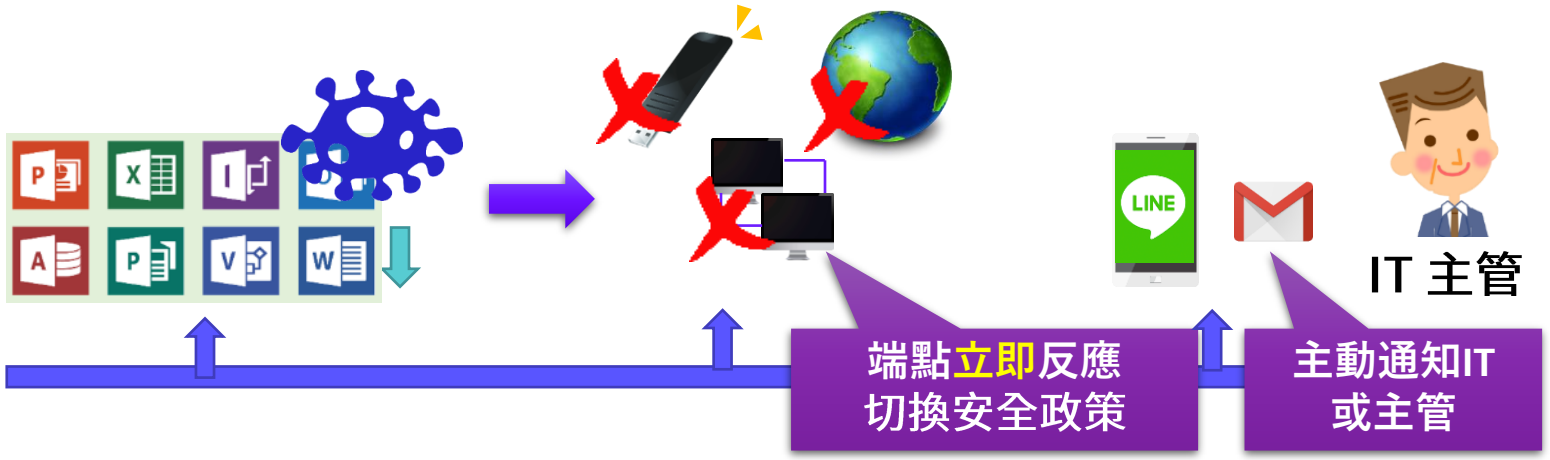
EDR (Endpoint Detection and Response) 方案，讓問題發生時，可以由端點主動防堵，避免災害擴大

為何要使用 EDR？

傳統方案: 發生問題後， 需 IT介入調查找出問題， 採取應變



EDR 方案: 發生問題後，自動反應處理



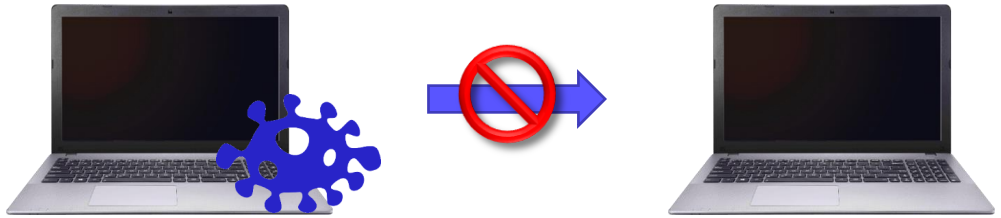
X-FORT

EDR 應用

例 1: 插入 USB ➔通知主管, 開始錄影

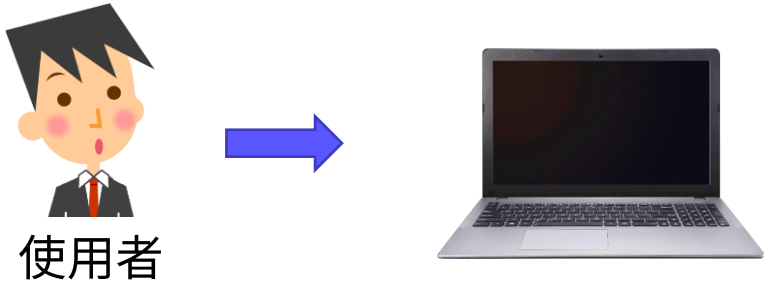
自動反應, 不須 IT 人員介入

例 3: 中勒索軟體 ➔ 斷網， 防止擴散



例 2: 在家遠端 RDP 登入

➔ 啟動使用者操作記錄, 禁用 USB



例 4: 出差到不同國家➔ 動態調整資安政策

X-FORT

EDR 事件和反應全部串連起來

DETECTION

1. 流量異常
2. 連線數量過多
3. 連線國家
4. 連線特定IP
5. 通訊Port
6. 列印張數
7. 檔案操作
8. USB插拔 / 寫出行為
9. VPN 連入／連出
10. 電腦位置
11. 關鍵字事件
12. 誘餌異動事件

RESPONSE

1. 螢幕浮水印
2. 斷網
3. 阻擋 Port / Protocol
4. 阻擋目的地 IP
5. 啟動檔案操作記錄
6. 禁用 / 啟動列印記錄
7. 警示
8. 切換自適性政策

任何的偵測事件發生時，都可以多重疊加不同的反應
例如：斷網
＋啟動浮水印
＋ 通知主管 ...

- 應用程式控管
- FAC
- SVS
- 上百種控管

X-FORT

EDR 應用情境範例 1/2

偵測事件	訴求	活用情境	對外	對內
USB裝置插拔	隨身碟使用頻率	插入已註冊/非註冊碟 & 次數		V
使用者檔案異動個數	大量寫出	寫出到已註冊碟/非註冊碟 & 檔案數		V
	大量刪除	一定時間內，刪除大量的本機檔案		V
列印張數	大量列印	列印張數過高		V
網路連結次數	弱點攻擊 / 暴力破解	頻繁探索多台電腦的 SMB 共用資料夾	V	V
	弱點攻擊 / 暴力破解	頻繁嘗試遠端桌面（RDP）登入遠端電腦	V	V
	弱點攻擊	頻繁存取Web伺服器，且非標準通訊協定(如80、443)的服務Port	V	
	微量異常	對內部不同網段(跨部門)的互通	V	V
	私架伺服器	連向本機（127.0.0.1）或 User 網段的 FTP、Web、SMB 服務	V	V
	異常國家 / 地區連線	異常國家 & 特殊 port & 連線次數過多 例子: 頻繁連到俄羅斯，且非網頁(80、443)的連線	V	

X-FORT

EDR 應用情境範例 2/2

偵測事件	訴求	活用情境	對外	對內
網路上傳 / 下載流量	大量上傳	對內部網段 (同部門 or 不同部門) 的大量上傳	V	V
	大量上傳	對外部網路的大量上傳	V	V
	大量下載	從敏感伺服器下載大量檔案	V	V
超連結(網址)關鍵字	異常使用	敏感伺服器不必要的連線對象 (例子: 業務連JIRA、研發連 CRM / ERP)		V
	頻繁匯出	頻繁連結到特定網址 (例子: CRM、ERP 匯出介面)		V
	非生產力行為	上網搜尋某些關鍵字 (例子: 破解、翻牆)		V
	弱點攻擊 / 暴力破解	頻繁連結內網 Web 伺服器的登入頁面 (1天連 JIRA 登入頁面超過 100次)	V	V

X-FORT

X-FORT

資安巡航 守護無垠

Ultimate Security for Business Longevity

FineArt