X-FORT

深入剖析使用者行為，利用 AI 偵測內部威脅

X-FORT 電子資料控管系統

精品科技 資安顧問 許祐福

FineArt

Agenda

完整的軌跡記錄，是掌握內部風險的根基

AI自然語言查詢，帶來管理變革

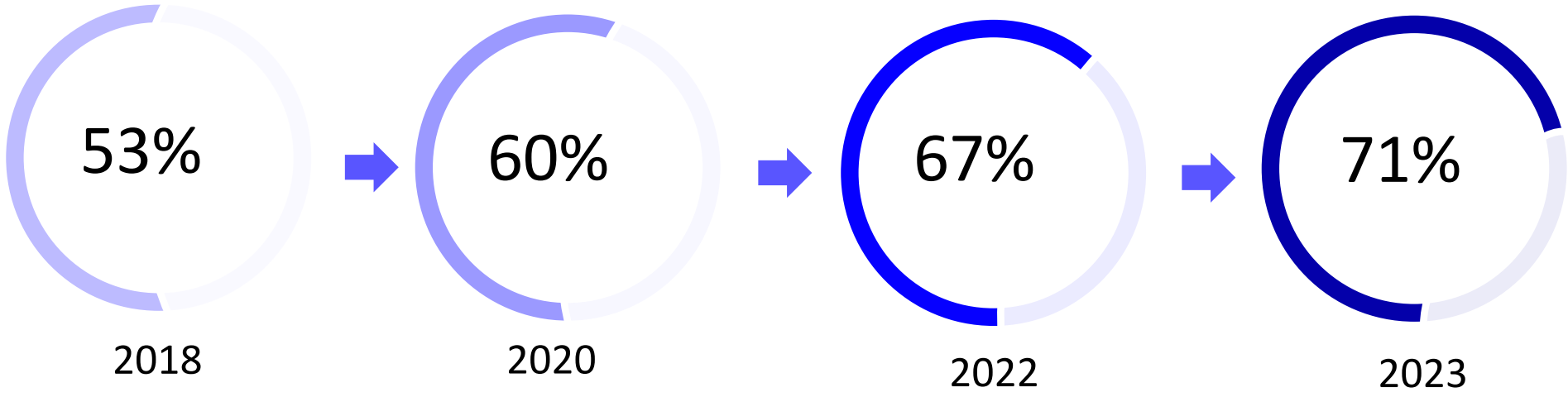
AI分析使用者記錄，偵測內部威脅

將生成式AI的使用，納入安全管理

X-FORT

Insider導致的資料外洩趨勢連年成長

- Ponemon Institute 的《Cost of Insider Risk Global Report 2023》報告顯示：近年來，每年發生21至40 起內部威脅事件的組織比例持續增加*

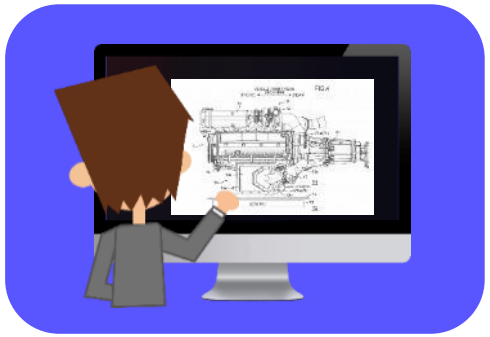


* Ponemon Institute: Cost of Insider Risk Global Report 2023

X-FORT

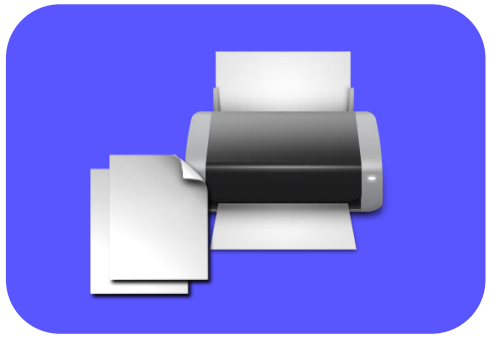
Insider風險：潛藏在員工的日常活動中

透過共用伺服器
取得檔案

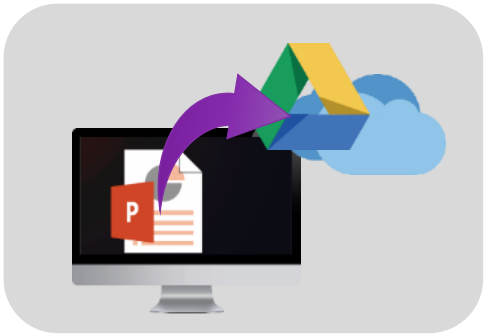


以專業軟體
開啟檔案

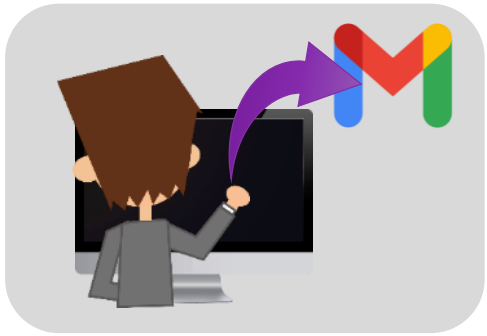
隨身碟方便
交換檔案



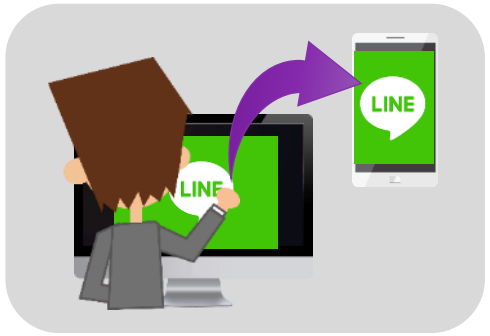
列印紙本資料



上傳檔案到雲端
方便存取



把資料寄到
Gmail私人信箱

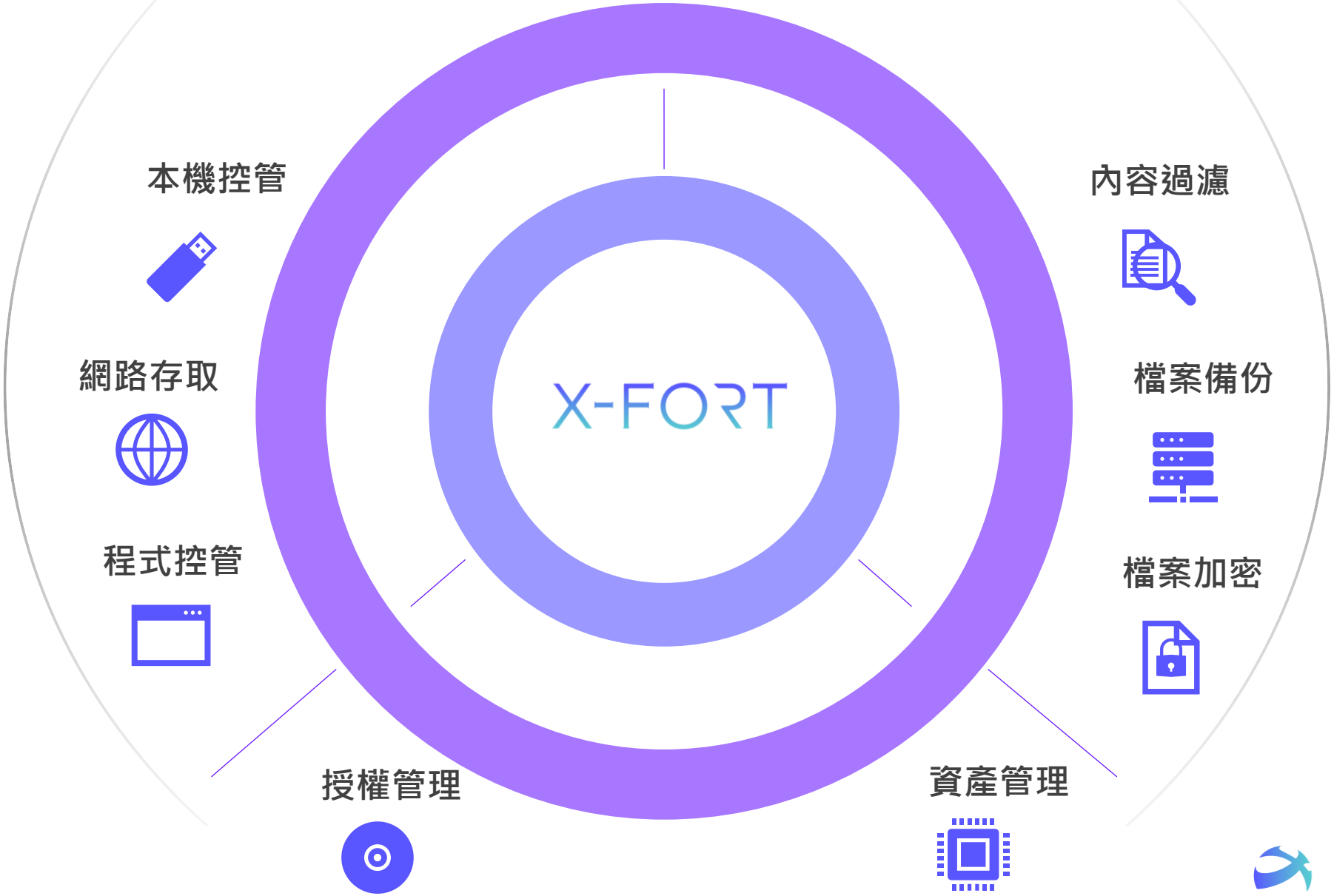


IM軟體方便
交換檔案

電腦帶回家工作

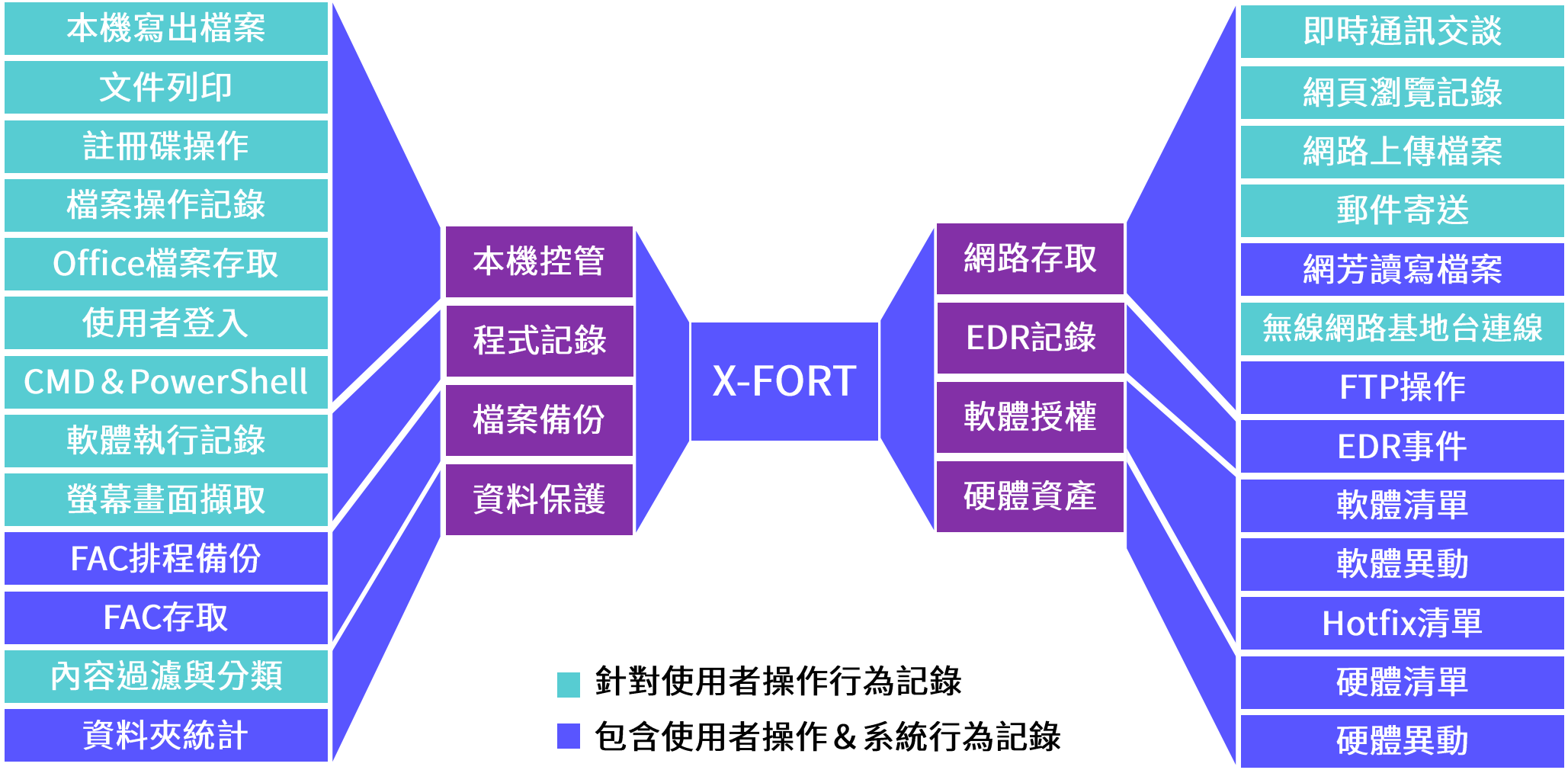
X-FORT

完整的軌跡記錄，是掌握內部風險的根基



X-FORT

X-FORT提供全方位的使用者與電腦操作記錄



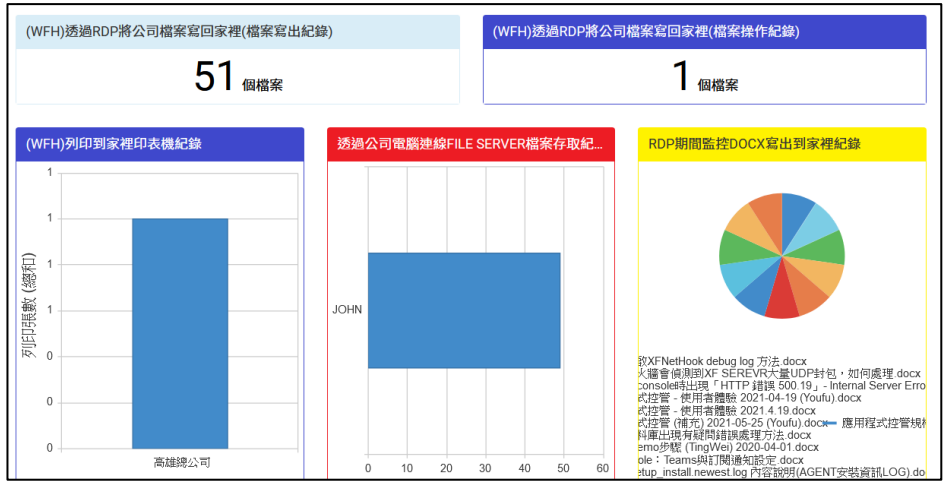
*僅列舉代表性記錄, 未涵蓋X-FORT所有記錄/資料類型

X-FORT

IT、主管、稽核皆可製作屬於自己的儀表板

資安人員

部門主管



IT人員

X-FORT

Agenda

完整的軌跡記錄，是掌握內部風險的根基

AI自然語言查詢，帶來管理變革

AI分析使用者記錄，偵測內部威脅

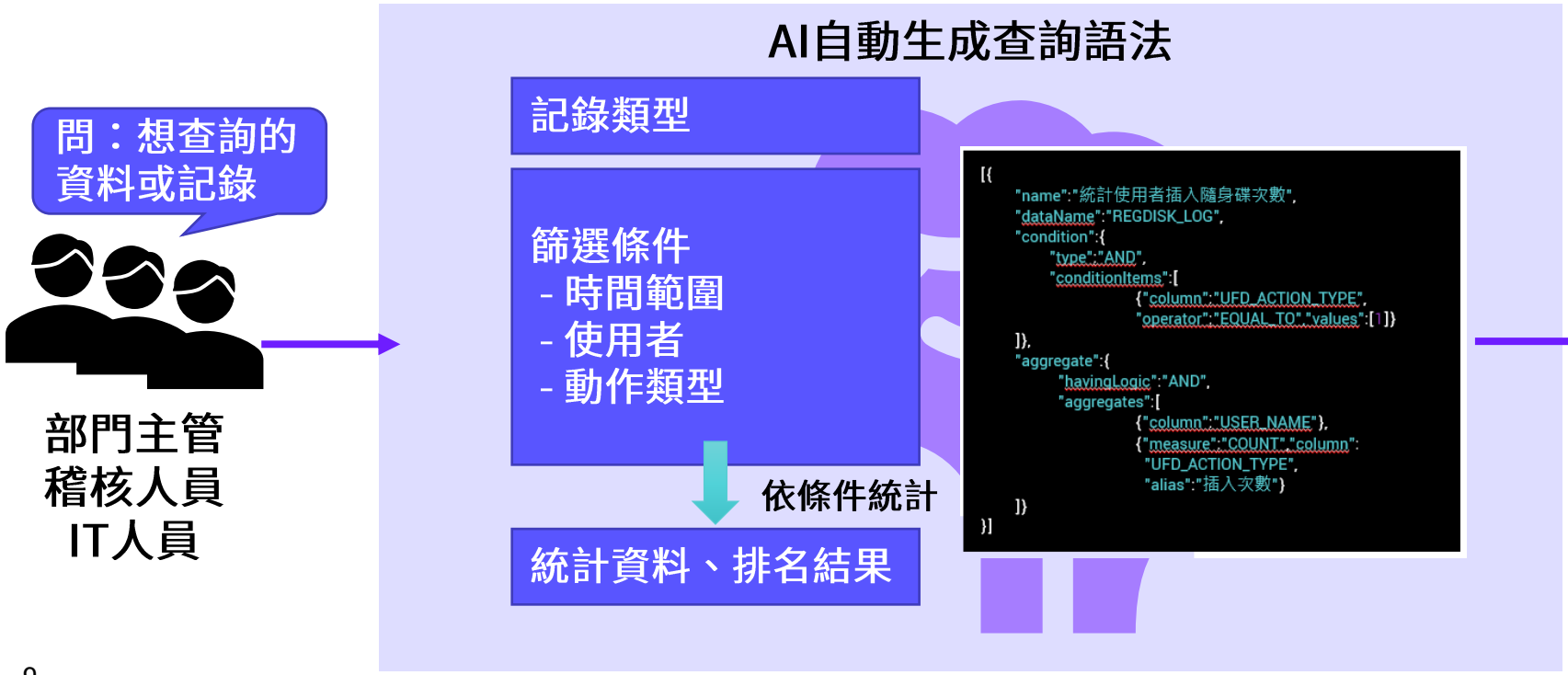
將生成式AI的使用，納入安全管理

X-FORT

AI使查詢操作更加簡便，提高資安監控效率

自然語言查詢運作原理與優點

- 不須確切清楚記錄名稱、條件、資料內容
- 省去設定查詢條件，例如：使用者 = Cherry；時間範圍 = 3個月



使用者	總計
Cherry	30
David	25
Eric	22
Frank	21
George	18
Helen	1

X-FORT

查詢情境

IT觀點

- Shadow IT風險

主管觀點

- 離職員工的資料保護

稽核觀點

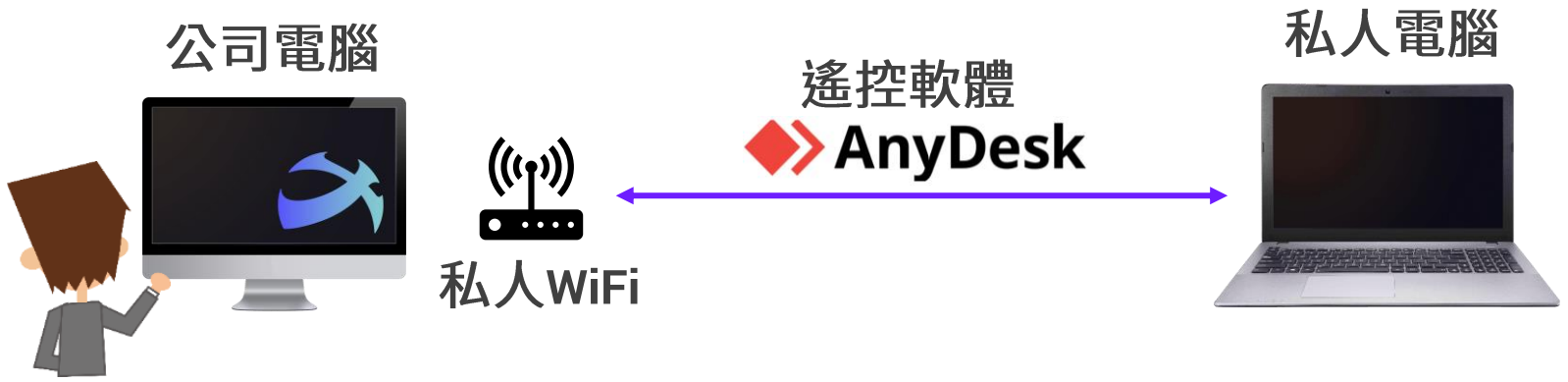
- 資料保護的日常稽核

X-FORT

IT觀點：Shadow IT風險

未經IT部門批准，員工私自使用的軟硬體或服務，可能帶來安全風險，例如

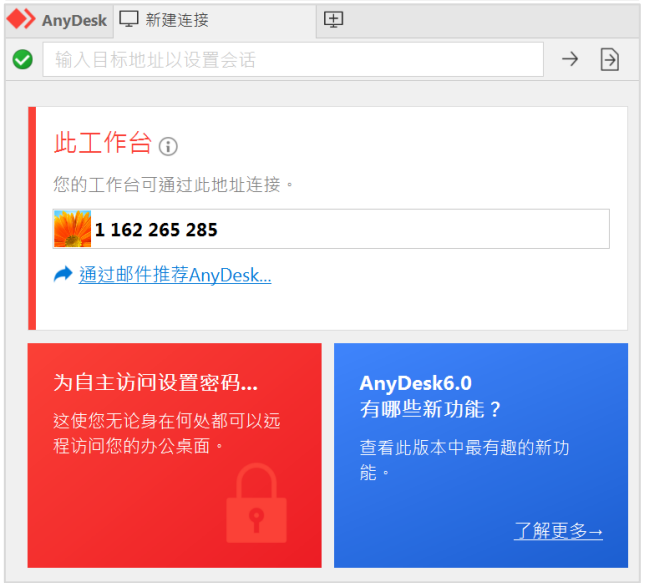
- 有誰使用AnyDesk遠端遙控軟體
- 有誰使用私人WiFi基地台



X-FORT

有誰使用AnyDesk遠端遙控軟體

執行AnyDesk軟體



公司電腦可與外部連通
可能導致重大資料洩露

X-FORT提供軟體控管，可禁止違反公司資安政策的程式 (含免安裝版)

X-FORT

有誰使用私人WiFi基地台

用手機當WiFi熱點

脫離公司網路保護
可能違反資安政策
並增加被攻擊的風險

X-FORT提供使用WiFi基地台控管，可禁止私人手機WiFi熱點

X-FORT

主管關注風險：員工離職前管理

即將離職員工，可能破壞資料的機密性和完整性，例如

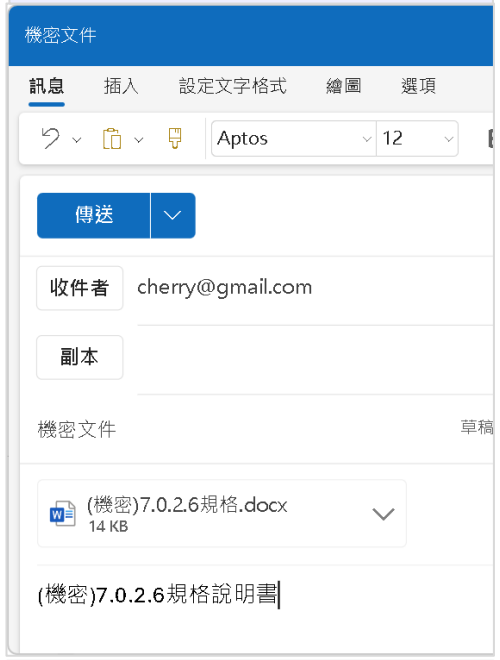
- 離職前，將公司檔案寄送到自己的Gmail私人信箱
- 離職前，刪除不想交接的檔案

59%自願或非自願離開組織的員工，承認在離職時會帶走機敏資料

2016 Deloitte Debriefs “Insider threats: What every government agency should know and do

寄送檔案到私人Gmail信箱

將檔案寄到私人信箱



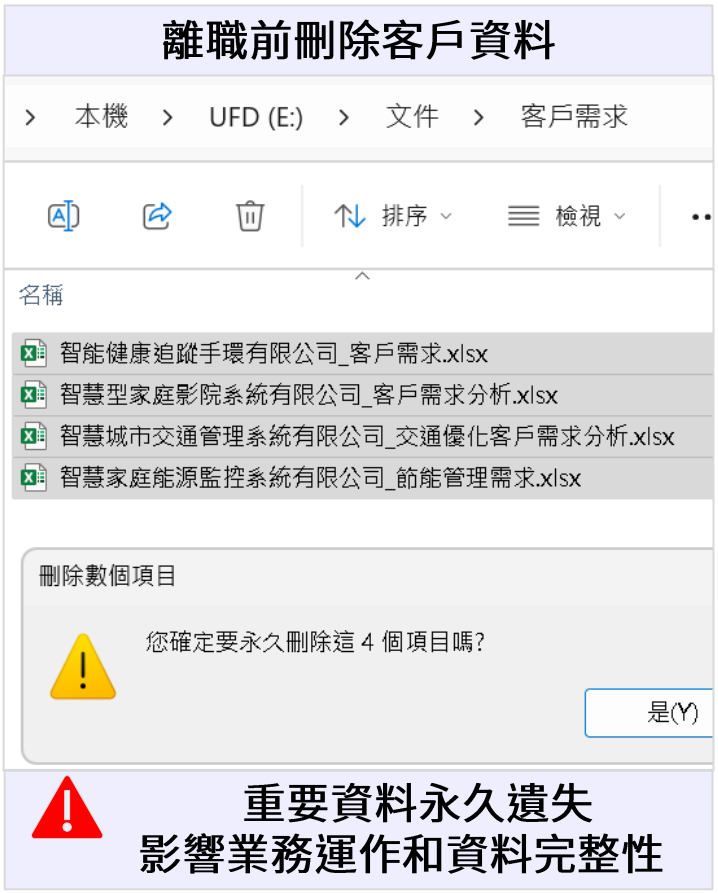
可能導致資料外洩或違反個資法

建議使用X-FORT內容過濾，檢查檔案內容並加註分類標籤

X-FORT

即將離職員工，最近1個月刪除檔案記錄

離職前刪除客戶資料



重要資料永久遺失
影響業務運作和資料完整性

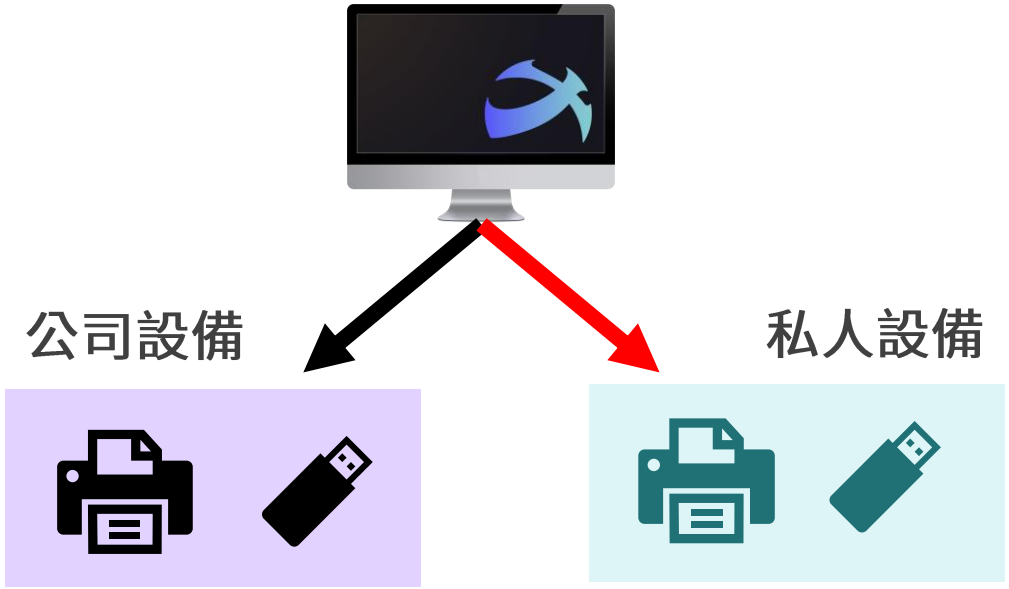
X-FORT提供安全備份，可定時備份使用者電腦＆檔案伺服器重要檔案

X-FORT

資安人員關注：資料保護的日常稽核

稽核重點，例如私人設備

- 有哪些部門使用私人隨身碟
- 有誰使用家中印表機列印文件

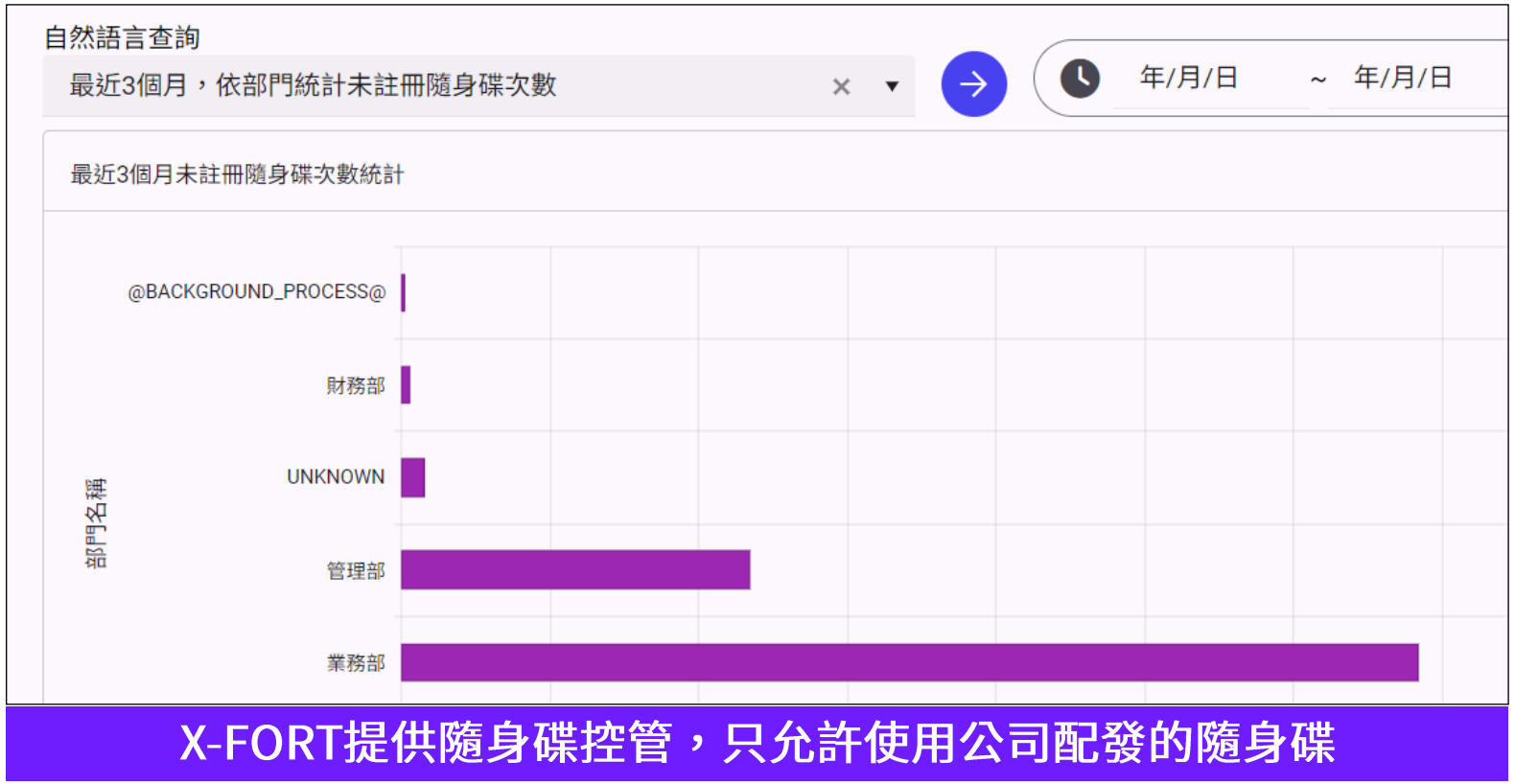


X-FORT

有哪些部門使用私人隨身碟

使用非公司的私人隨身碟

可能導致資料外洩
傳播病毒、駭客入侵



X-FORT提供隨身碟控管，只允許使用公司配發的隨身碟

X-FORT

用家中印表機列印文件

家中印表機列印公司文件

可能導致資安事件
違反公司資安政策

自然語言查詢

查詢使用印表機名稱不等於HP LaserJet Pro M404n 或Canon PIXMA TR8520的列印記錄

查詢特定印表機名稱外的列印記錄

拖曳列標題到此處按列組合顯示

電腦名稱 (#)	IP	列印張數	列印份數	檔案路徑
PC_MiniHuang	11.1.1.38	10	1	E:\會議\行政部門會議記錄_2024年.xlsx
PC_JANELIN	11.1.1.38	36	1	E:\機密文件\新一代產品原型設計_2024_機密.docx

X-FORT提供列印控管功能，可禁止使用未知印表機

X-FORT

Agenda

完整的軌跡記錄，是掌握內部風險的根基

AI自然語言查詢，帶來管理變革

AI分析使用者記錄，偵測內部威脅

將生成式AI的使用，納入安全管理

X-FORT

用AI分析X-FORT記錄優點

X-FORT

+

- 使用自然語言分析記錄，進一步節省管理時間
- 具備簡易的記憶＆舉一反三能力
- 知名的網頁＆執行檔識別能力
- 能理解即時通訊交談、郵件內容、檔案名稱
- AI協助分析記錄，解決員工隱私與人為偏見問題

分析情境

分析列印行為

- 使用公司印表機印私人文件
- 使用私人印表機印公司文件

分類網頁瀏覽

- 分析與工作無關的網頁瀏覽行為

分析交談內容

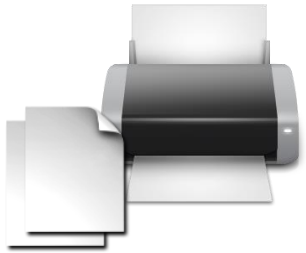
- 分析郵件、即時通訊交談記錄
- 從交談內容偵查資料外洩風險

X-FORT

分析用公司印表機印私人文件，或私人印表機印公司文件

分析列印記錄

- 可記憶公司配置的印表機型號
- 用列印文件名稱，判斷與工作內容是否相關
- 查詢使用公司印表機，列印私人文件
- 查詢使用私人印表機，列印公司文件



DEMO

X-FORT

分析X-FORT-console記錄

作者：FaChatGPTOne

機密文件的列印記錄

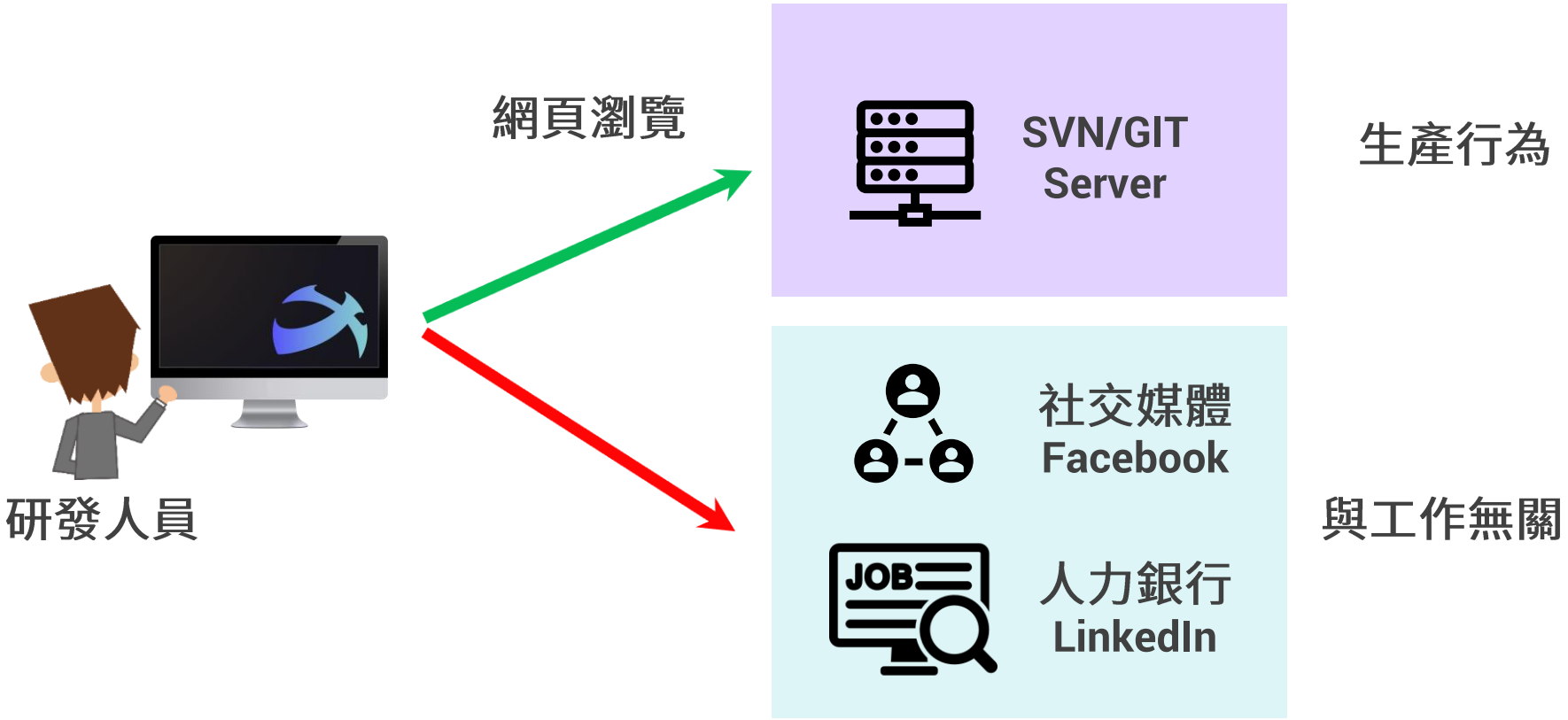
從即時通訊交談記錄分析資料外洩風險

分析與工作無關的網頁瀏覽記錄

從郵件記錄分析資料外洩風險

傳訊息給 分析X-FORT-console記錄.....

分析與工作無關的網頁瀏覽行為



X-FORT

分析X-FORT-console記錄

分析X-FORT-console記錄

作者：FaChatGPTOne

機密文件的列印記錄

從即時通訊交談記錄分析資料外洩風險

分析與工作無關的網頁瀏覽記錄

從郵件記錄分析資料外洩風險

傳訊息給 分析X-FORT-console記錄.....

從郵件＆即時通訊交談內容分析資料外洩風險

分析Outlook郵件記錄、Webmail郵件記錄、即時通訊交談記錄

- 寄送到外部的郵件內容，是否有資料外洩風險
- 分析即時通訊交談內容

DEMO

X-FORT

分析X-FORT-console記錄

分析X-FORT-console記錄

作者：FaChatGPTOne

機密文件的列印記錄

從即時通訊交談記錄分析資料外洩風險

分析與工作無關的網頁瀏覽記錄

從郵件記錄分析資料外洩風險

傳訊息給 分析X-FORT-console記錄.....

Agenda

完整的軌跡記錄，是掌握內部風險的根基

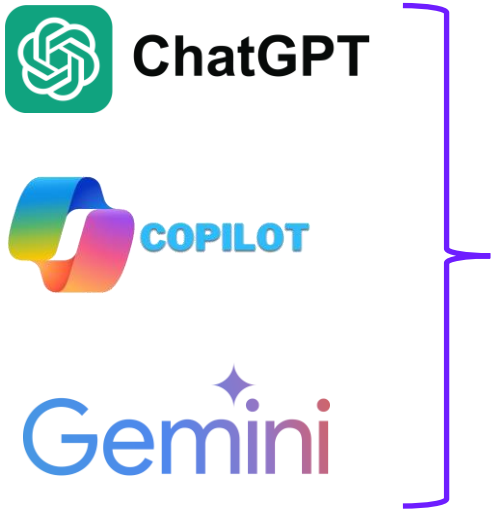
AI自然語言查詢，帶來管理變革

AI分析使用者記錄，偵測內部威脅

將生成式AI的使用，納入安全管理

X-FORT

生成式AI安全管理的管理對策



支援各大生成式AI平台

控制可使用生成式AI的人員 → 禁止使用

禁止輸入文字 → 唯讀，只能檢視，不能發問

禁止上傳檔案

禁止使用剪貼簿，貼出大量文字

→ 允許使用 但禁止大量輸出

統計提問次數

檢視提問內容

針對敏感人員或單位，啟動螢幕錄影

→ 允許使用 但留下記錄

螢幕浮水印提醒員工勿洩露公司情報 → 落實資安宣導

X-FORT

生成式AI安全管理 – 可以這樣做

螢幕浮水印：提醒不可洩露公司資訊

統計ChatGPT使用次數、記錄提問內容

上傳網址	主機名稱	資料型態	Log類型
https://chatgpt.com/backend-api/conversation	chatgpt.com	application/json	記錄上傳網址
https://chatgpt.com/backend-api/conversation	chatgpt.com	application/json	記錄上傳網址
https://chatgpt.com/backend-api/conversation	chatgpt.com	application/json	記錄上傳網址
https://chatgpt.com/backend-api/conversation	chatgpt.com	application/json	記錄上傳網址
https://chatgpt.com/backend-api/conversation	chatgpt.com	application/json	記錄上傳網址

*Dump.txt - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明

"text","parts":["分析以下程式碼，如何重構、優化!\nint+main()+
++std::cout+<<+\"hello+world!\";\n++++return+0;\n}"]},"metada
{}}],"parent_message_id":"aaa1d61d-f4ef-43e2-bbd6-

針對敏感人員或單位，可啟動螢幕錄影

X-FORT

結論：善用AI可大幅縮減識別資料外洩的反應時間

自然語言查詢
X-FORT記錄

查詢

幫助主管/稽核
發現異常

分析

X-FORT
提供控管措施

對策

落實資安政策

落實

X-FORT

X-FORT

資安巡航 守護無垠

Ultimate Security for Business Longevity

FineArt