



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

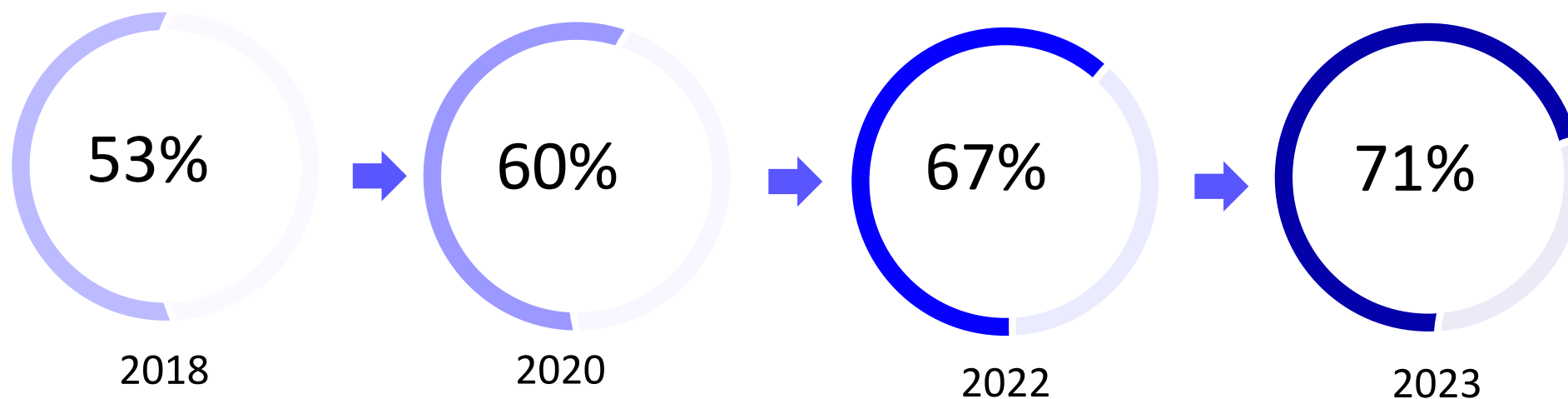
AI自然語言查詢，帶來管理變革

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

Insider導致的資料外洩趨勢連年成長

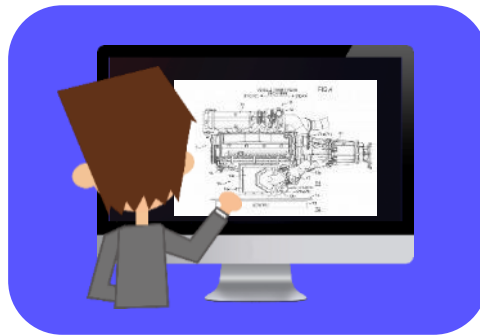
- Ponemon Institute 的《Cost of Insider Risk Global Report 2023》報告顯示：近年來，每年發生21至40起內部威脅事件的組織比例持續增加*



Insider風險：潛藏在員工的日常活動中



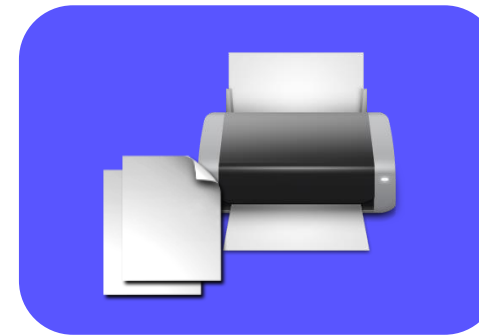
透過共用伺服器
取得檔案



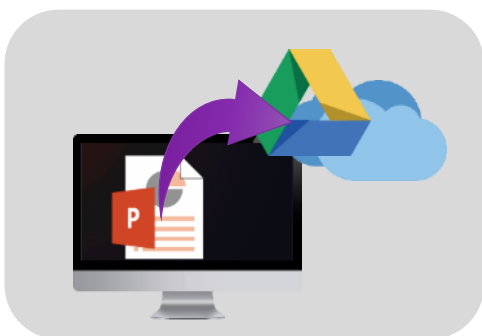
以專業軟體
開啟檔案



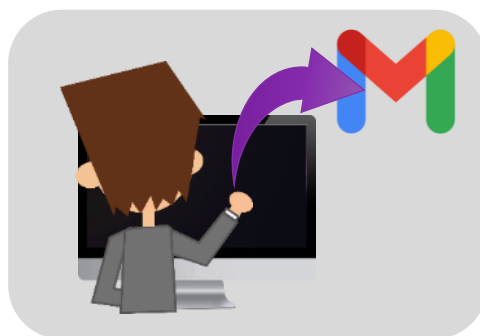
隨身碟方便
交換檔案



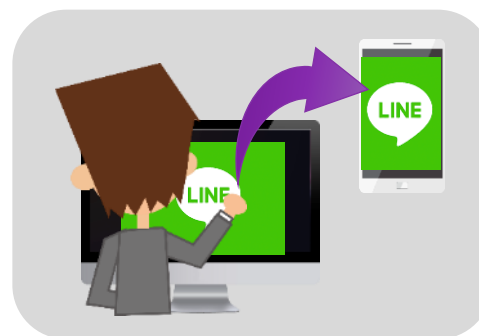
列印紙本資料



上傳檔案到雲端
方便存取



把資料寄到
Gmail私人信箱

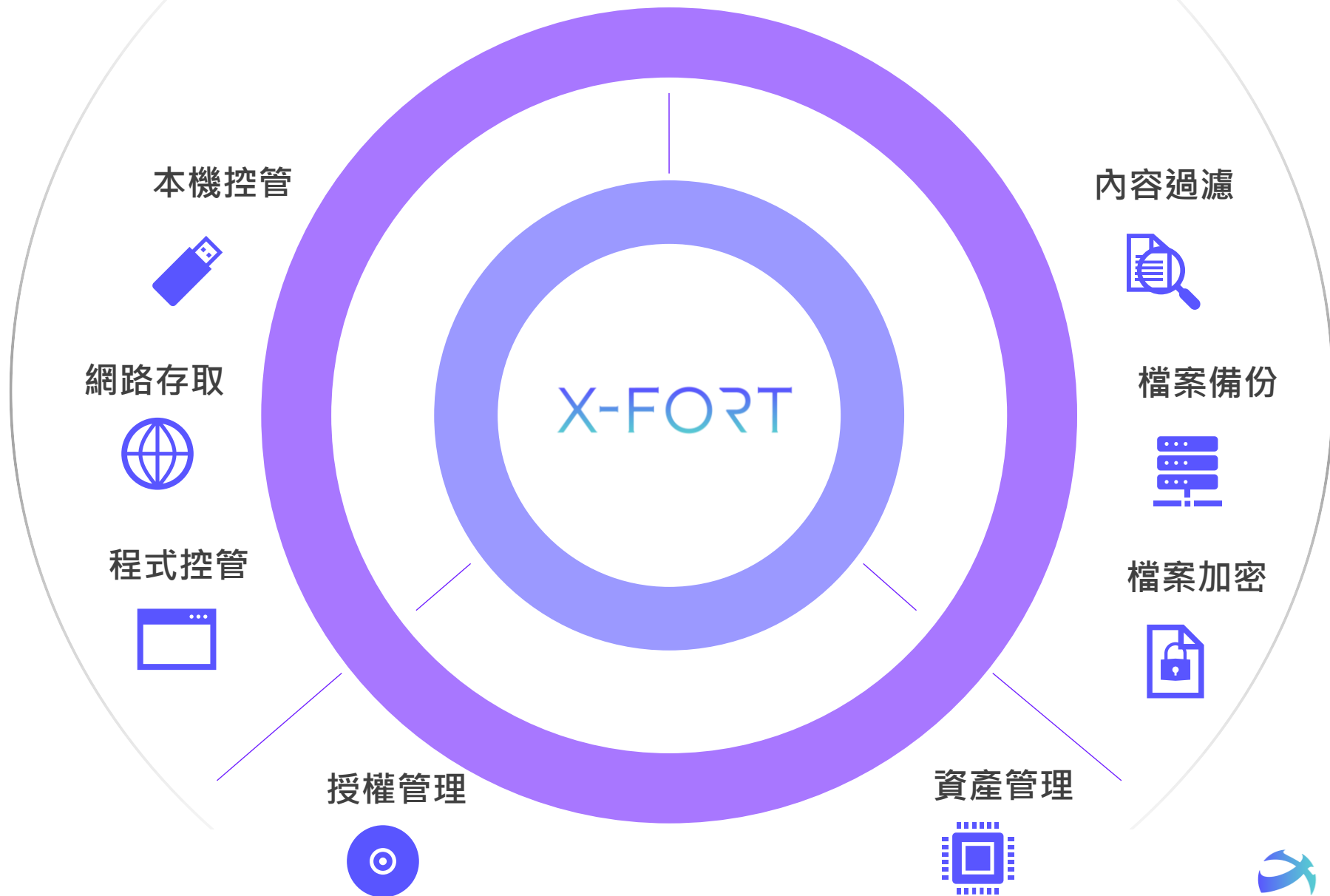


IM軟體方便
交換檔案

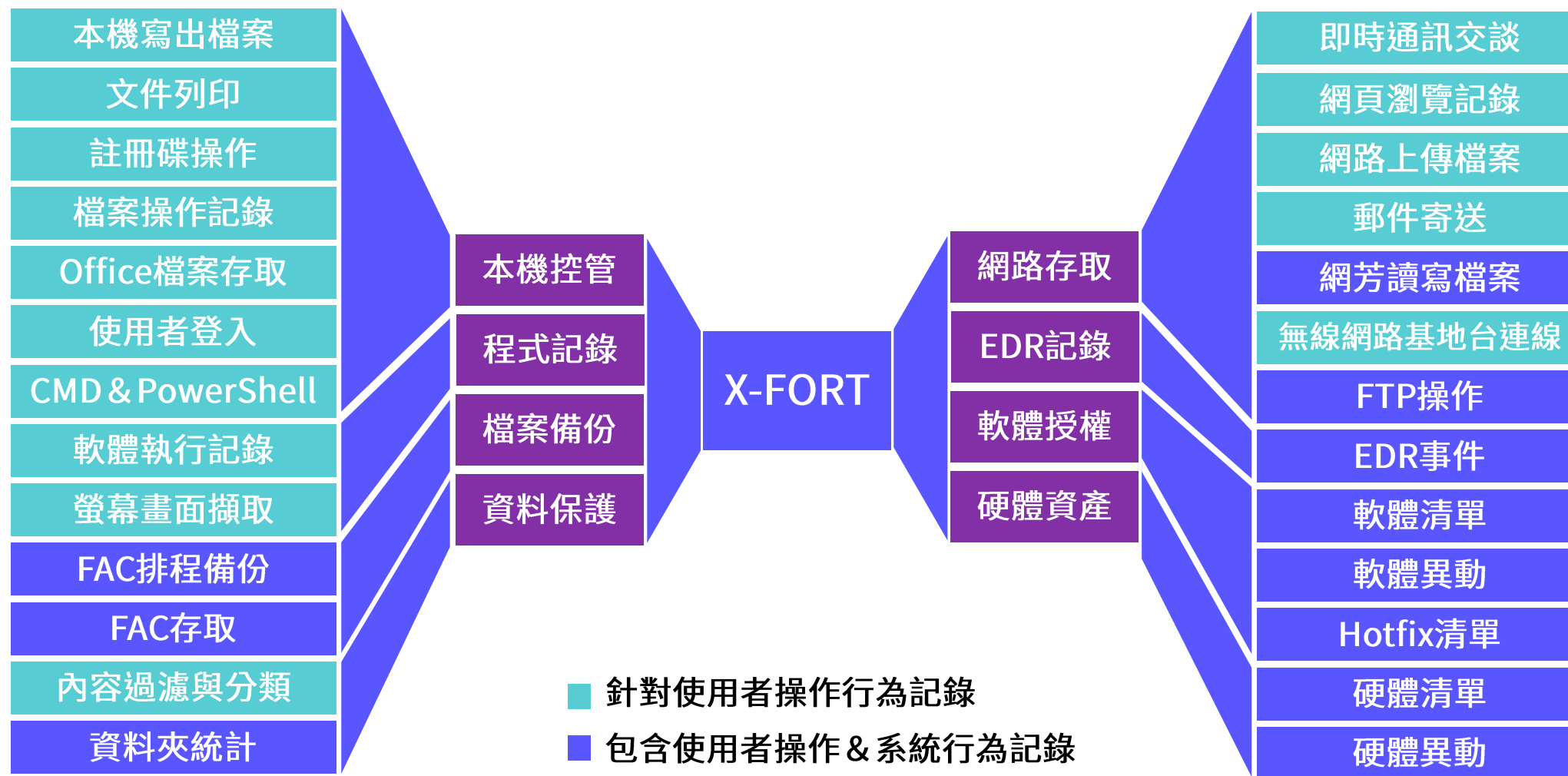


電腦帶回家工作

完整的軌跡記錄，是掌握內部風險的根基



X-FORT提供全方位的使用者與電腦操作記錄



IT、主管、稽核皆可製作屬於自己的儀表板



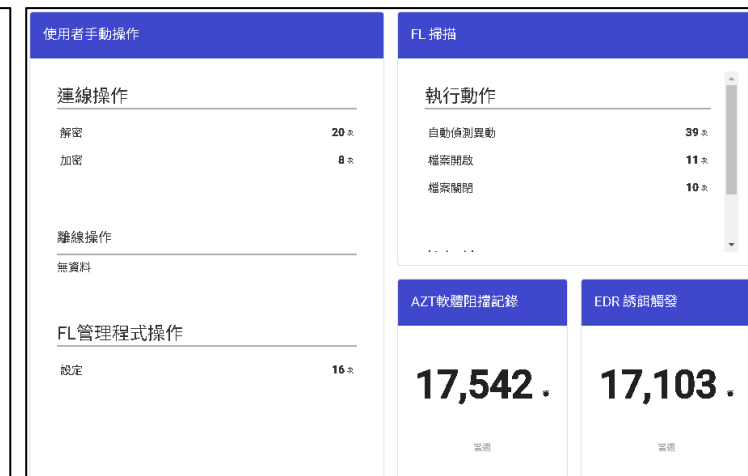
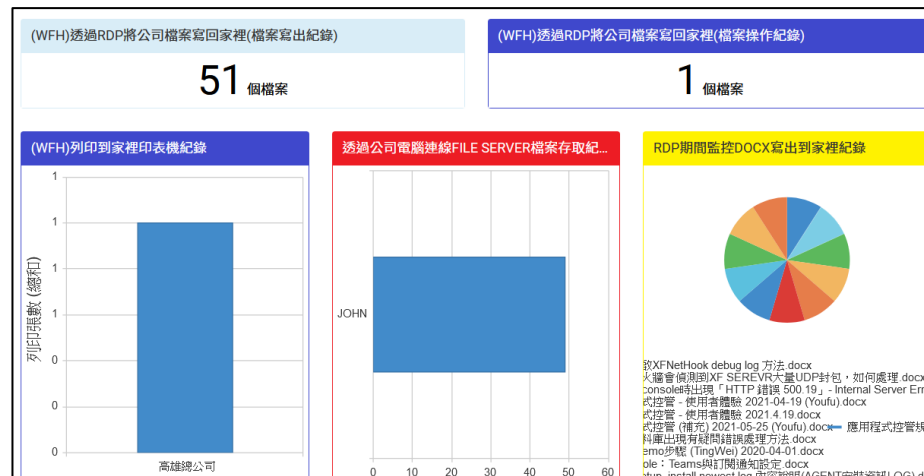
資安人員



部門主管



IT人員





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

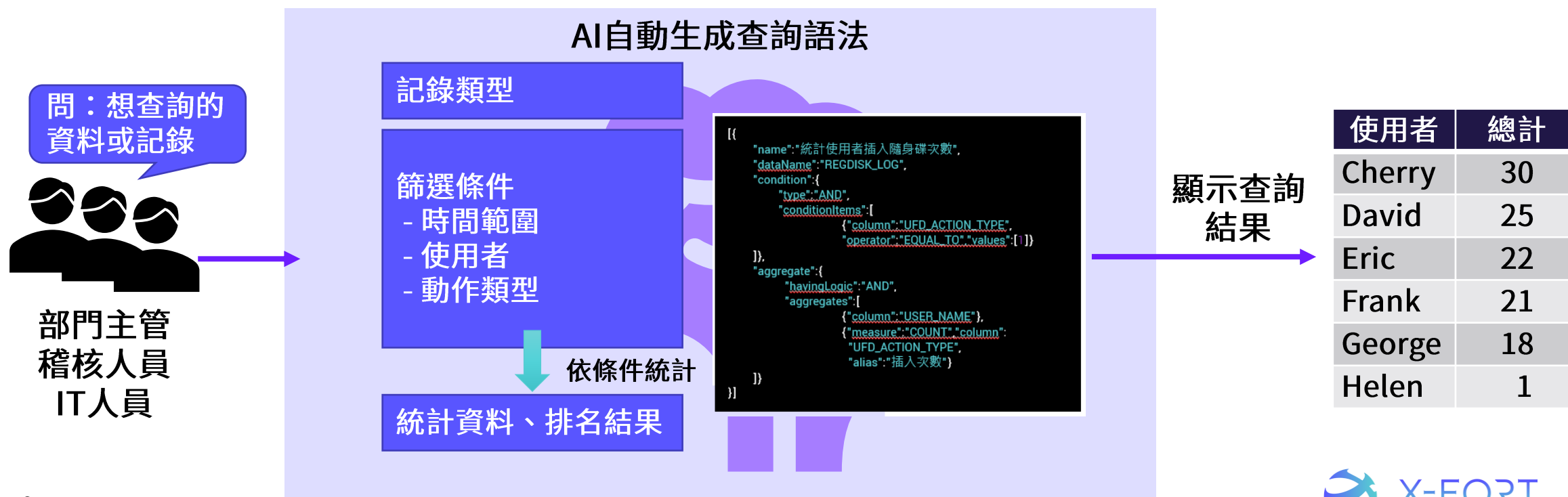
AI分析使用者記錄，偵測內部威脅

將生成式AI的使用，納入安全管理

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



查詢情境



IT觀點

- Shadow IT風險



主管觀點

- 離職員工的資料保護



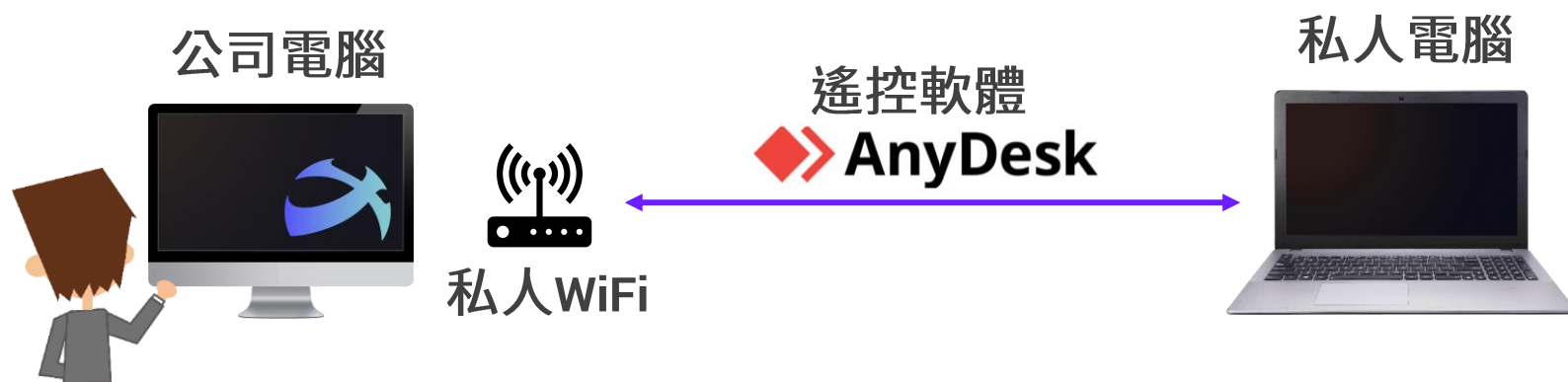
稽核觀點

- 資料保護的日常稽核

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



有誰使用AnyDesk遠端遙控軟體

執行AnyDesk軟體

AnyDesk 新建连接

输入目标地址以设置会话

此工作台

您的工作台可通过此地址连接。

1 162 265 285

通过邮件推荐AnyDesk...

为自主访问设置密码...

这使您无论身在何处都可以远程访问您的办公桌面。

AnyDesk 6.0 有哪些新功能？

查看此版本中最有趣的新功能。

了解更多

公司電腦可與外部連通
可能導致重大資料洩露



X-FORT

資料中心 > 自然語言查詢

自然語言查詢

最近6個月，Anydesk軟體的執行記錄

最近6個月Anydesk軟體執行記錄

拖曳列標題到此處按列組合顯示

記錄時間	延續時間 (秒)	網域名稱	部門名稱	使用者名稱	執行檔名稱
2024/3/22 10:10:22	19 分 45 秒	GoodDemo	研發中心	Cherry	anydesk.exe
2024/3/21 10:11:48	31 分 50 秒	GoodDemo	研發中心	Cherry	anydesk.exe
2024/2/3 10:40:19	2 時 51 分 33 秒	GoodDemo	業務部	SnowDin	anydesk.exe

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)

有誰使用私人WiFi基地台

用手机當WiFi熱點

Wi-Fi

FA-01

FA-01_5G

FA-03

FA-03_5G

Apple iPhone 14 Pro

更多 Wi-Fi 設定

!

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



資料中心

自然語言查詢

自然語言查詢

查詢無線網路基地台名稱不包含FA的連線記錄，且SSID由小到大排序

查詢無線網路基地台名稱不包含FA的連線記錄，SSID由小到大排序

拖曳列標題到此處按列組合顯示

記錄時間	網域名稱	部門名稱	使用者名稱	MAC	SSID
2024/3/25 18:20:50	GoodDemo	業務部	SnowDin	06-DF-2D-B0-1A-35	Apple iPhone 14 Pro
2024/3/31 10:00:00	GoodDemo	業務部	SnowDin	06-DF-2D-B0-1A-35	Apple iPhone 14 Pro
2024/1/3 13:27:58	GoodDemo	研發中心	JobsKai	18-31-BF-53-6B-20	Apple iPhone 14 Pro

X-FORT提供使用WiFi基地台控管，可禁止私人手機WiFi熱點

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

寄送檔案到私人Gmail信箱

將檔案寄到私人信箱

機密文件

訊息 插入 設定文字格式 繪圖 選項

↶ ↷ 📎 📎

Aptos 12

傳送

收件者

cherry@gmail.com

副本

機密文件

草稿

📎 (機密)7.0.2.6規格.docx 14 KB

▼

(機密)7.0.2.6規格說明書|

⚠️

可能導致資料外洩
或違反個資法



≡

X-FORT

🔍 資料中心 > 📄 自然語言查詢

TRIAL

自然語言查詢

過去3個月，用Outlook寄信給Gmail信箱，且有夾帶附檔

×

➔

Outlook發送至Gmail且夾帶附檔

拖曳列標題到此處按列組合顯示

郵件類型 ▼	寄件者 ▼	收件者 ▼	郵件主旨 ▼	郵件內文 ▼	附件檔案清單
Outlook	SparkTai	Lee@gmail.com	機密文件	(機密)7.0.2.6規格說明書	(機密)7.0.2.6規格.docx
Outlook	SnowDin	Cherry@gmail.com	Data	Data	NormalA.pdf;NormalB.docx

建議使用X-FORT內容過濾，檢查檔案內容並加註分類標籤

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

> 本機 > UFD (E:) > 文件 > 客戶需求

排序

檢視

名稱

智能健康追蹤手環有限公司_客戶需求.xlsx

智慧型家庭影院系統有限公司_客戶需求分析.xlsx

智慧城市交通管理系統有限公司_交通優化客戶需求分析.xlsx

智慧家庭能源監控系統有限公司_節能管理需求.xlsx

刪除數個項目

!

您確定要永久刪除這 4 個項目嗎?

是(Y)

!

重要資料永久遺失
影響業務運作和資料完整性



X-FORT

資料中心

自然語言查詢

自然語言查詢

最近1個月，業務部的KennyWen刪除檔案的記錄

業務部KennyWen刪除檔案記錄

拖曳列標題到此處按列組合顯示

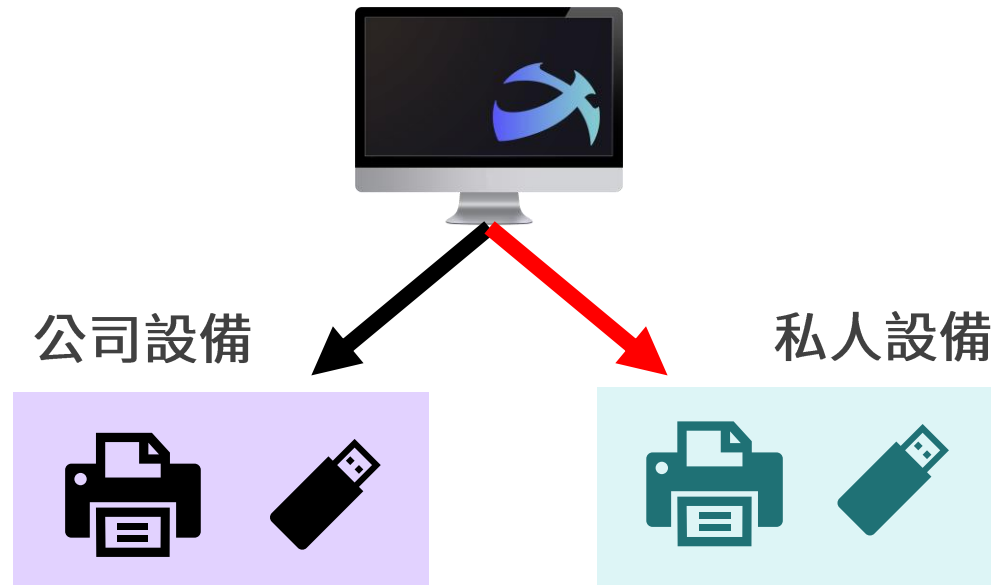
電腦名稱 (#)	IP	動作類型	來源檔案路徑
PC_KennyWen	11.1.1.210	刪除檔案	D:\合約\人工智慧諮詢_人工智慧策略規劃合約.docx
PC_KennyWen	11.1.1.210	刪除檔案	D:\合約\機器學習實驗室_機器學習技術開發合約.docx

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

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



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

自然語言查詢

最近3個月，依部門統計未註冊隨身碟次數

x



年/月/日

~ 年/月/日

最近3個月未註冊隨身碟次數統計

@BACKGROUND_PROCESS@

財務部

UNKNOWN

管理部

業務部

部門名稱

X-FORT提供隨身碟控管，只允許使用公司配發的隨身碟

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



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

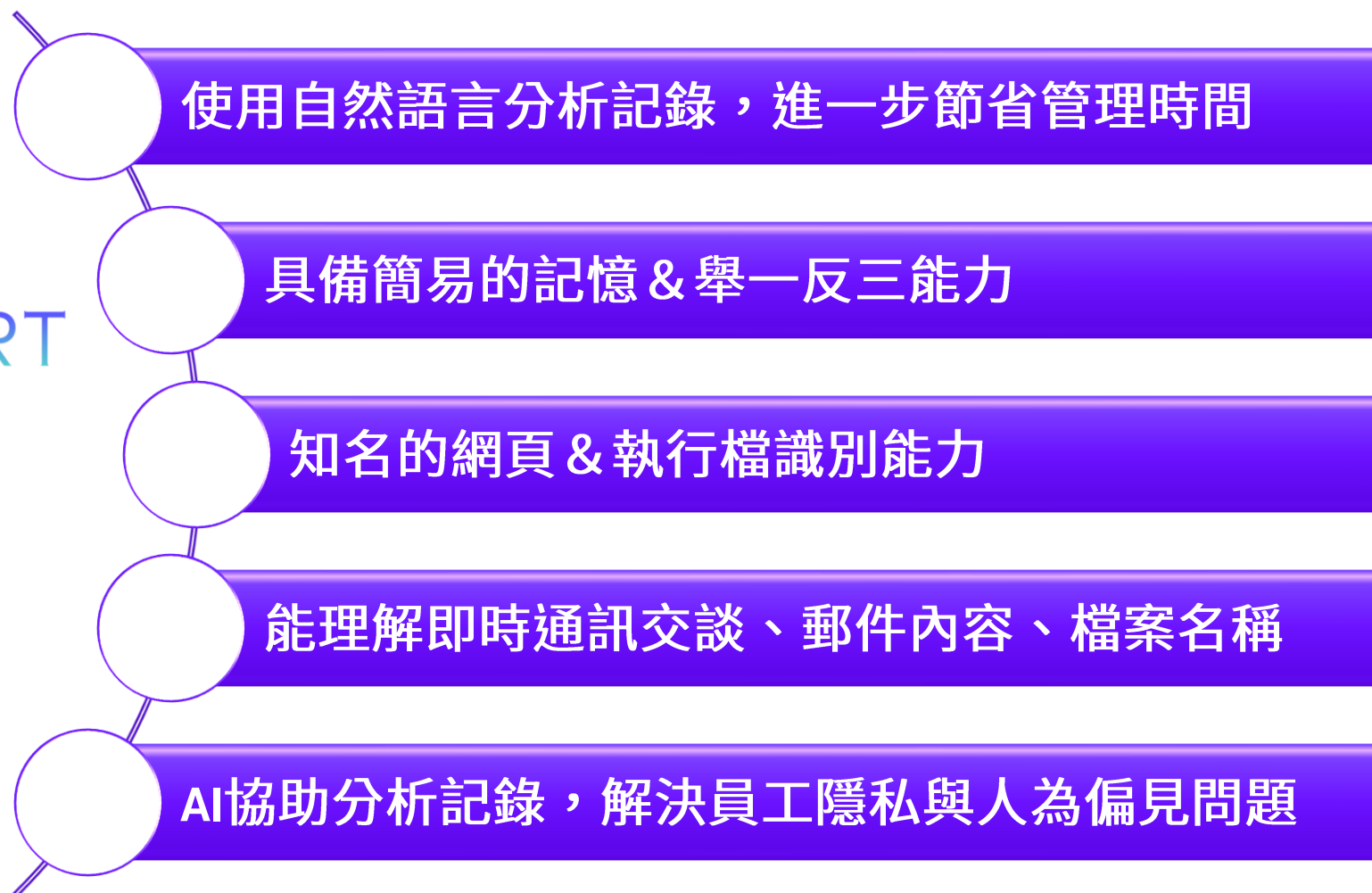
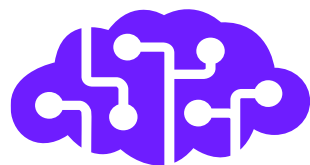
AI分析使用者記錄，偵測內部威脅

將生成式AI的使用，納入安全管理

用AI分析X-FORT記錄優點



+



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



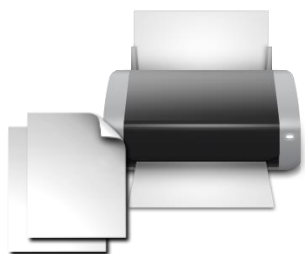
分析交談內容

- 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

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



分析X-FORT-console記錄 ▾



分析X-FORT-console記錄

作者：FaChatGPTOne 人

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

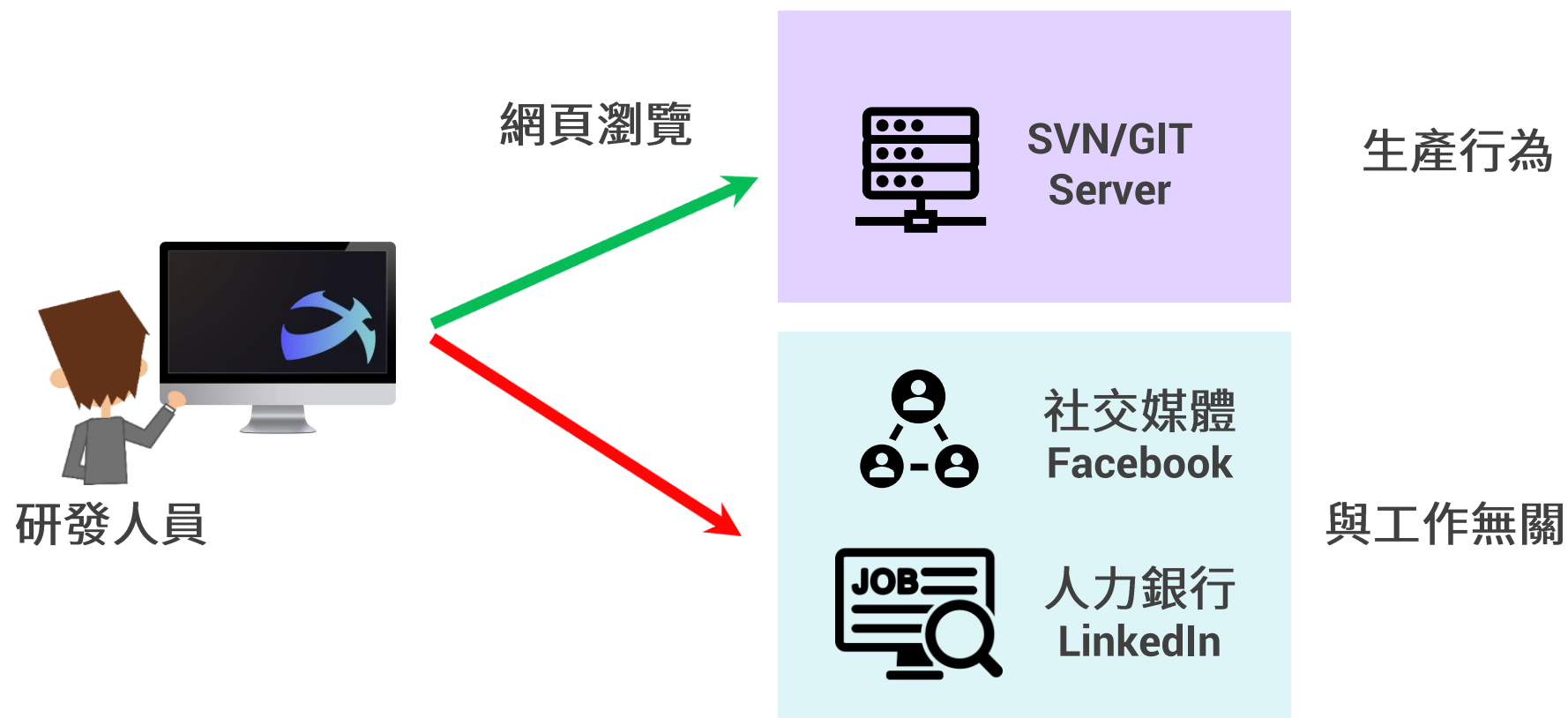
從郵件記錄分析資料外洩風險



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





分析X-FORT-console記錄

作者：FaChatGPTOne 人

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





分析X-FORT-console記錄 ▾



分析X-FORT-console記錄

作者：FaChatGPTOne 人

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

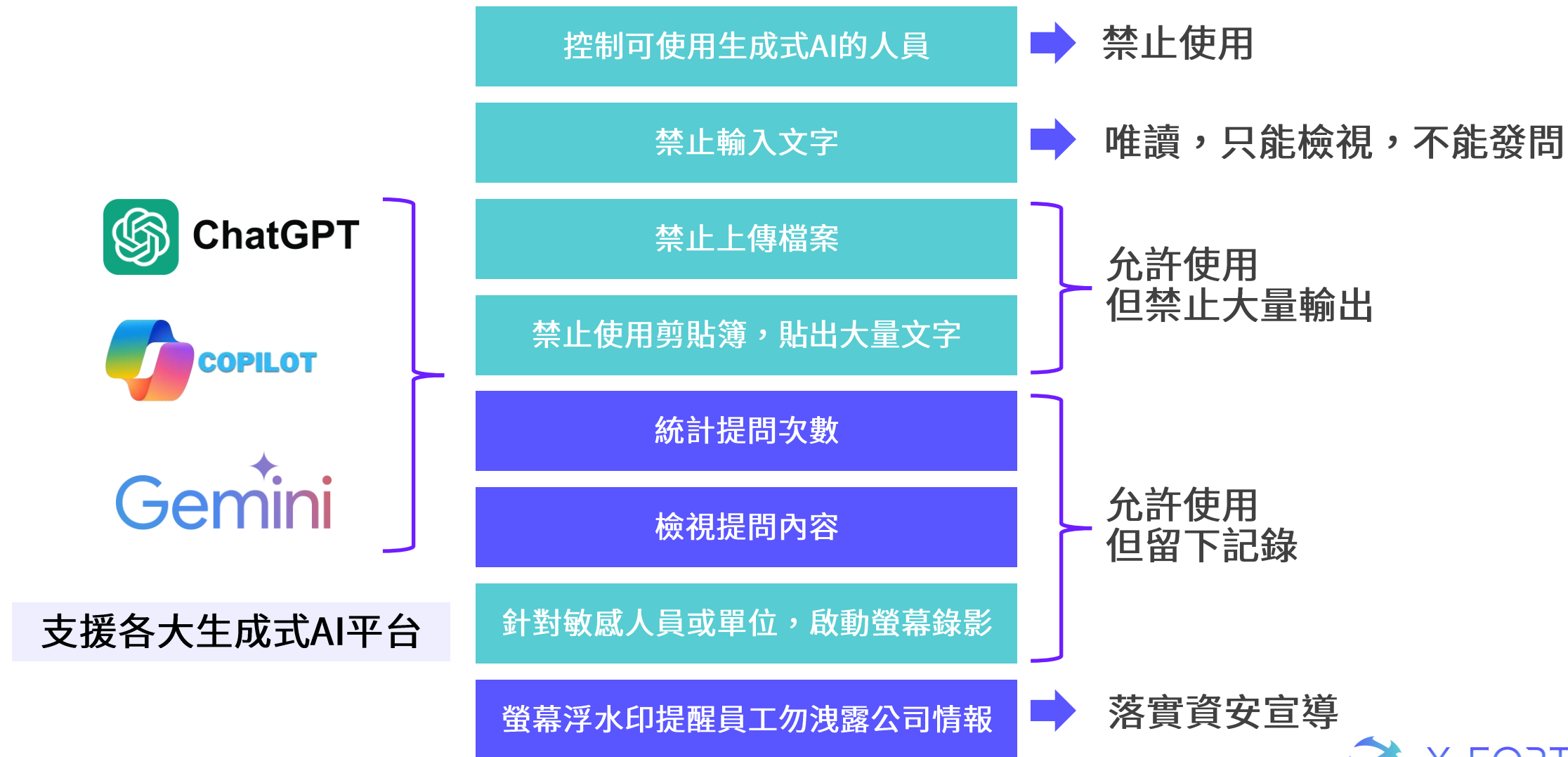
完整的軌跡記錄，是掌握內部風險的根基

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

生成式AI安全管理的管理對策



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+<<+\n"hello+world!\n";\n++++return+0;\n}"] }, "metadata": {}, "parent message id": "aaa1d61d-f4ef-43e2-bbd6-

針對敏感人員或單位，可啟動螢幕錄影

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



資安巡航 守護無垠
Ultimate Security for Business Longevity

FineArt