

【 資料保護及權限稽查案例研究 】

netwrix 如何協助半導體產業巨頭 防止高風險資料外洩

Softnnext 中華數位科技

引人注目的事件

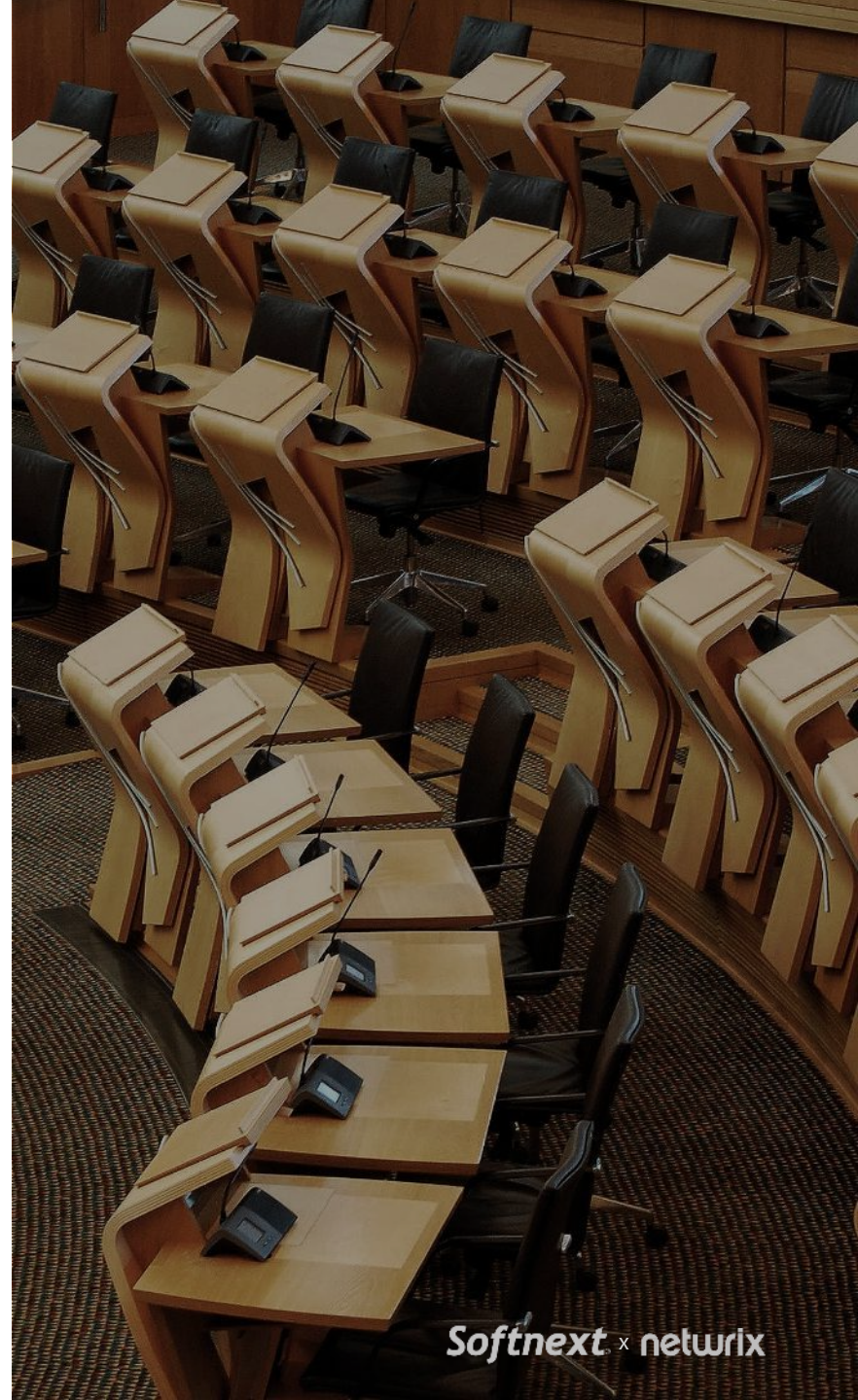
事件概述

事發企業簡稱 ABC 企業

- 數名員工涉嫌非法取得機密文件，經證實這些文件與 ABC 企業即將推出的2奈米製程技術（目前最先進的技術）有關。2025.8
- 該公司的內部監控系統在例行檢查中檢測到異常文件存取，並立即展開調查並迅速回應。
- 涉事人員包括現任和前任員工。其中三人已被高等檢察院智慧財產權部門依據《國家安全法》拘留。他們已被 ABC 企業解僱，並面臨法律訴訟。
- ABC 企業已正式宣布啟動法律訴訟程序，強調其對侵犯商業機密行為的零容忍政策。公司正在全力配合司法部門，並迅速採取行動以降低任何相關風險。

法律和刑事責任風險

- 據國家科學技術委員會 (NSTC) 稱，本案涉及的技術，具體而言，即14奈米以下製程節點，已被列為「國家核心關鍵技術」。
- 根據相關法律，涉及此類技術的違法行為最高可判處12年有期徒刑，並處以1億新台幣以下罰金。台灣高等檢察院智慧財產部門已依據《國家安全法》展開調查，這是台灣司法系統首次針對此類高度敏感技術盜用事件採取嚴肅的司法應對措施。
- 多年來，ABC 企業面臨多起商業秘密爭議，包括2000年針對中芯國際 (SMIC) 的技術侵權訴訟，以及因前任高管跳槽後涉嫌將專有技術帶給競爭對手而引發的問題。



關鍵因素

細目	概述
時間戳	調查於2025年7月啟動，相關資訊於8月5日公開
技術範圍	涉及2奈米製程技術核心機密
涉案人員狀況	至少有三名涉案人員已被還押候審，探視權被剝奪，並已被公司解僱
法律行動	調查根據《國家安全法》進行，涉案人員可能面臨最高 12 年的監禁和罰款
公司職位	法律措施迅速落實，彰顯了零容忍立場和完善的內部控制體系
商業影響	專家認為，這起事故對營運的影響仍在可控範圍，但對公司形象造成不利影響

關鍵性分析



不可否認性

能證明特定使用者對文件或系統上執行的操作負責，確保其行為不可否認



取證完整

記錄完整且不可篡改
可作為法律或內部稽核的有效證據，並支持後續的取證調查

Netwrix 為何能提供協助？

已實施的解決方案：

Netwrix可提供兩類方案

Agent mode

Netwrix Access Analyzer

Agentless

Netwrix Auditor

適用目標資料：

File Server

NetApp Storage

SharePoint

對客戶的關鍵支援

- **存取活動日誌**：記錄誰在何時、從哪個設備存取哪些文件，包括開啟、修改、複製或刪除文件等操作
- **詳細的變更日誌**：全面追蹤目錄和權限變更（例如，誰授予了誰的存取權限）
- **警報通知機制**：針對異常活動（例如大量文件下載）即時發出警報
- **防止日誌被刪除或修改**：利用防篡改儲存結構（可與 SIEM 和不可變日誌整合）

Netwrix 為何能提供協助？

已實施的解決方案：

Agent mode **Netwrix Access Analyzer**

適用目標資料：

File Server

NetApp Storage

SharePoint

對客戶的關鍵支援

- **機密資料發現與分類**：包含可自訂的類別，例如技術文件、專利設計等
- **存取分析**：識別誰可以存取關鍵數據，偵測權限過高的帳戶，並刪除休眠（幽靈）帳戶
- **風險報告與控制建議**：提供切實可行的洞察，以降低資料外洩風險
- **支援定期存取審查**：允許資料所有者定期進行權限審查（資料所有者審查）

部署於案例企業的資料保護環境

文件洩漏前

文件洩漏中

文件洩漏後

情境

誰有權限存取
2nm 技術文件？

是否存在權限過高
或存取不受控制的情況？

可設定異常行為警報嗎？

已部署功能

Netwrix Defend
可產生具有存取權限的
使用者列表，幫助主動移除
不必要的權限

Netwrix Defend
可分析是否有機密資料
被過度分享

Netwrix File Audit
針對異常活動提供即時警報
如深夜大量存取設計檔案

部署於案例企業的資料保護環境

文件洩漏前

文件洩漏中

文件洩漏後

情境

工程師們正在
大量複製設計文件

帳號登入異常

異常行為識別

已部署功能

Netwrix 方案可記錄所有
複製/下載活動並提供即時警報

與 AD 監看模組整合，可以識別前
員工在異常時間的登入活動

支援基於行為的分析，並對異常模
式觸發警報

部署於案例企業的資料保護環境

文件洩漏前

文件洩漏中

文件洩漏後

情境

證明某人在特定時間存取
特定文件或執行操作

內部調查必須提供
支持性證據

日誌是否有任何
修改或刪除？

已部署功能

完整的原始日誌確保不可
否認性，從而實現精確的
可追溯性

提供圖形報告和稽核日誌
(可匯出為 PDF 格式，並支援
SIEM 整合)

支援與不可變日誌
(Immutable Logs)整合
並將日誌匯出到第三方安全
平台，如 Splunk

Netwrix 符合不可否認性和取證真實性要求



不可否認性

✓ 是

Netwrix 記錄完整
與使用者帳戶綁定，可與 AD 身份
驗證和日誌保護機制整合



取證完整

✓ 是

Netwrix 支援日誌保護
與不可變日誌 (Immutable Logs) 整
合，允許與第三方 SIEM 共享資料
以供審查

適用於案例企業的資料保護環境

跳板機及關鍵系統存取監看：

全程活動側錄

Netwrix Auditor for Windows 側錄模組

適用目標設備：

Windows-based跳板機及關鍵系統

對客戶的關鍵支援

- **側錄影檔輕量無負擔：**當操作鍵盤或滑鼠時才進行側錄，檔案小有利儲存，可設定若一段時間無操作活動，暫時中斷側錄
- **靈活設定：**依據人員帳號或軟體名稱、視窗標題來指定或排外觸發側錄。可設定側錄解析度，即使灰階畫面的文字依舊清晰易讀
- **操作歷程日誌：**提供每個錄影 Session 的紀錄內容，檢閱操作歷程更方便
- **違規登入存取警示：**可設定人員在異常時間登入或存取特定系統而發送警示通知

國產NAS檔案伺服器 存取稽核策略 (補充)

建議方案：

中華數位科技自主研發

CRA for NAS 檔案存取及權限稽核系統

適用目標資料：

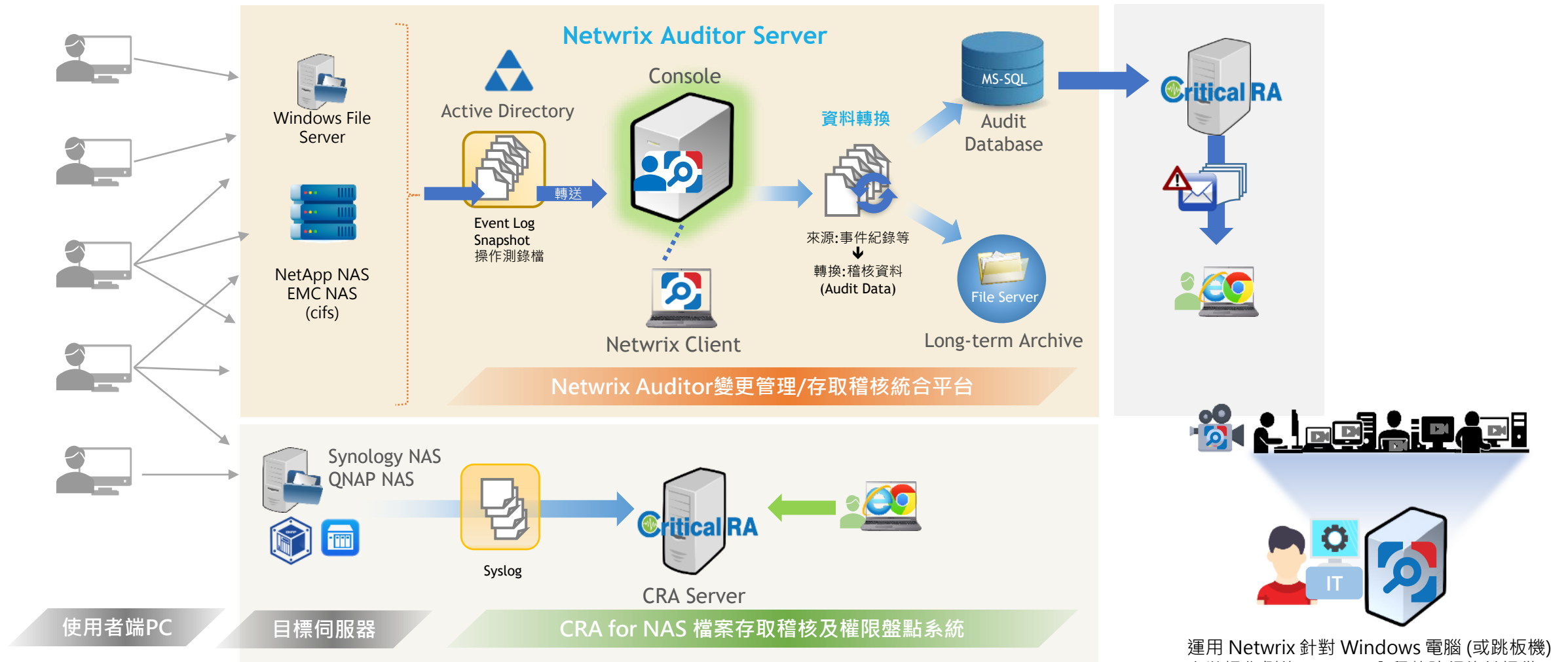
Synology

QNAP

對客戶的關鍵支援

- **存取活動日誌**：記錄誰在何時、以及從哪個設備存取了哪些文件，包括開啟、修改、複製或刪除文件等操作
- **詳細的變更日誌**：全面追蹤目錄和權限變更（例如，誰授予了誰的存取權限）
- **檔案資料夾權限盤點**：可稽查人員被賦予哪些分享檔案資料夾的權限資訊，防範不當授權而衍伸資料存取風險
- **警報通知機制**：針對異常活動（例如大量文件下載）即時發出警報

Netwrix & CRA 變動稽核系統架構



運用 Netwrix 監看檔案伺服器、資料庫，用CRA 監看 Synology、QNAP 檔案伺服器來防範不當使用活動及存取權限稽查

運用 Netwrix 針對 Windows 電腦 (或跳板機) 安裝操作側錄 Agent，全程軌跡紀錄並提供輕量錄影檔

智慧財產權(IP)保護策略

- 可建立完整的存取日誌，防止抵賴
- 提供鑑識級稽核證據，支持法律訴訟
- 分析並修復權限風險，防止內部資料外洩
- 即時發送異常行為警報，縮短回應時間

企業監控範圍





THANK YOU