netwrix
#1 for change auditing

Netwrix Auditor

IT變動管理、存取稽核的領先方案

Netwrix Auditor是系統設定變更暨存取記錄稽核的全球領先品牌，可監看Windows 重要伺服器 (如AD 網域伺服器及Windows 檔案伺服器...等)及其他支援主機、設備的設定變更及存取稽核。人員異動的檔案存取權限調整、特權帳號變動稽核、異常大量檔案存取、密碼暴力攻擊、資料庫可疑異動、疑似勒索軟體感染、網路設備登入失敗 ...等資安管理關鍵，Netwrix 提供報表及即時警示通知，偵測異常預防風險。

Netwrix 稽核記錄支持長期歸檔保存，提供多款法規遵循報表集，可流暢地進行**合規性稽核**、**強化安全**、發生問題時能**簡化根本原因分析**，有助於迅速找出肇因並解決問題。

報表範本多達250款以上(內建法規遵循套版),
依需求自訂更多報表(輸出多種格式)

監看特權使用者的操作行為：即使被監看設備無產生任何日誌記錄(logs)，可針對特權使用者登入或指定使用系統/應用程式時來側錄操作歷程影片，精準鎖定操作變動，精簡控制影片大小，有助於資料儲放，及後續追蹤、搜尋並播放操作活動影片。

知名客戶

MITSUBISHI · CISCO · IBM · NASA · Allianz · AT&T

內建國際法規 稽核報表

GLBA · SOX · ISO/IEC 27001 · FISMA · PCI · HIPAA · GDPR · CJIS · NERC

Netwrix提供產品的適法性說明指南及內建多款國際法規遵循的稽核報表集，如ISO 27001, PCI, SOX, HIPPA, GDPR, FISMA, GLBA, CJIS...等其他法規標準，開箱即用的稽核工具

Updated:201901_NW9.7

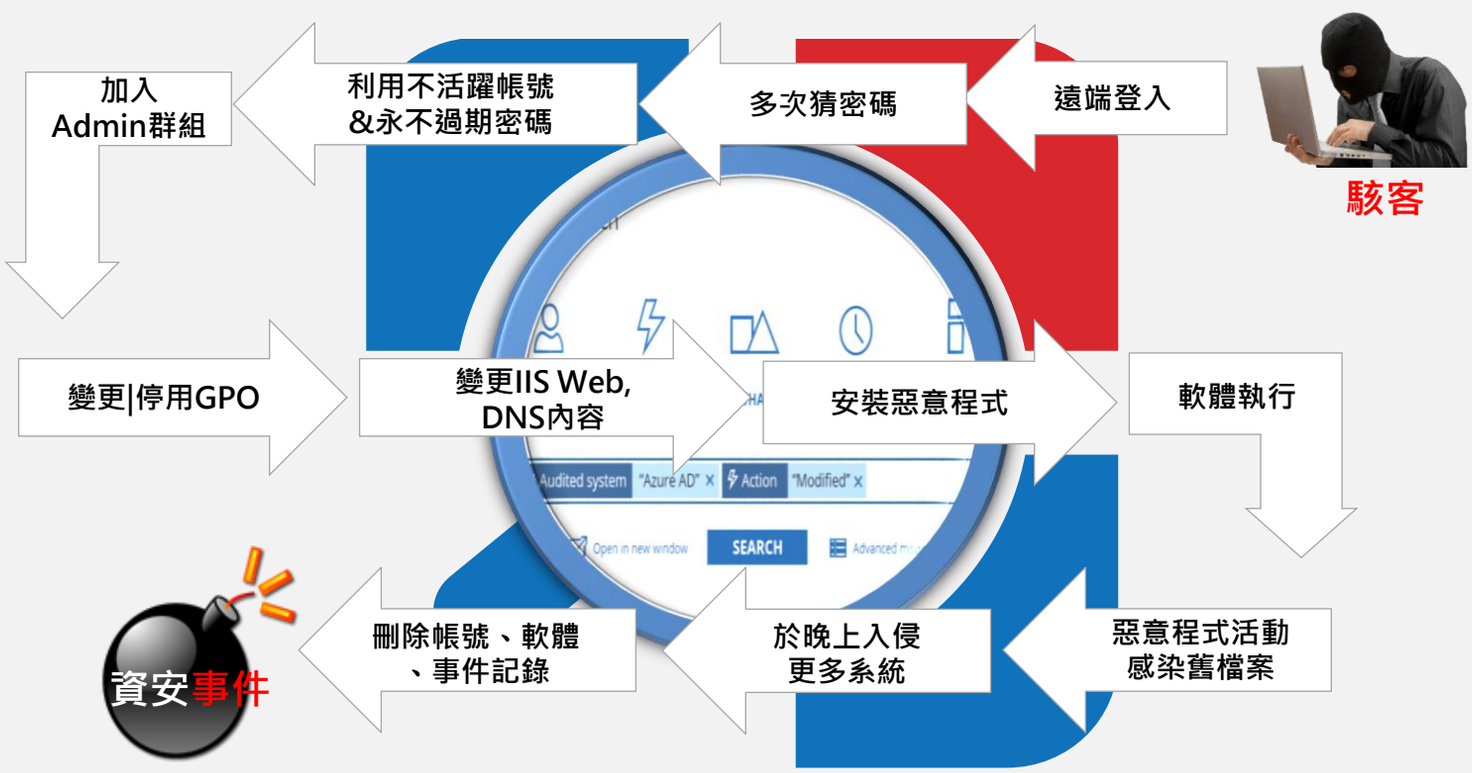
Application

追查資料外洩發生前
異常或違規的使用者行為

Netwrix Auditor提供安全性分析，幫助您找出”誰在搞鬼”！追查IT環境中重要系統（如Windows AD、File server..等) 發生哪些惡意或不當的活動軌跡，有助於迅速反應是否有內部威脅或外部網路攻擊。其中“使用者行為及盲點分析” 報表類別，可深入分析使用者存取活動的變化趨勢，透過歷史活動記錄及變化趨勢分析，找出使用活動的異常時點。這些安全性分析功能有助於你揭露IT環境中潛在威脅，保護企業機構的重要數位資產。

- 深入瞭解每次異常存取的使用者活動，找出更詳細的行為資訊。
- 關注異常的資料存取或異常登入等行為，找出潛在威脅的徵兆。
- 即早識別出受害的帳戶，以免災情擴大。
- 深入稽核特權帳戶以識別非法|不當的操作活動。
- 全盤掌握IT環境內的所有使用者活動，消除安全性盲點。
- 注意關鍵性變化、可疑的登錄及不尋常的失敗活動，利於快速回應資安事件。

運用 Netwrix 抓住 Hacker的入侵軌跡



運用 Netwrix找出可疑的使用者異常存取活動

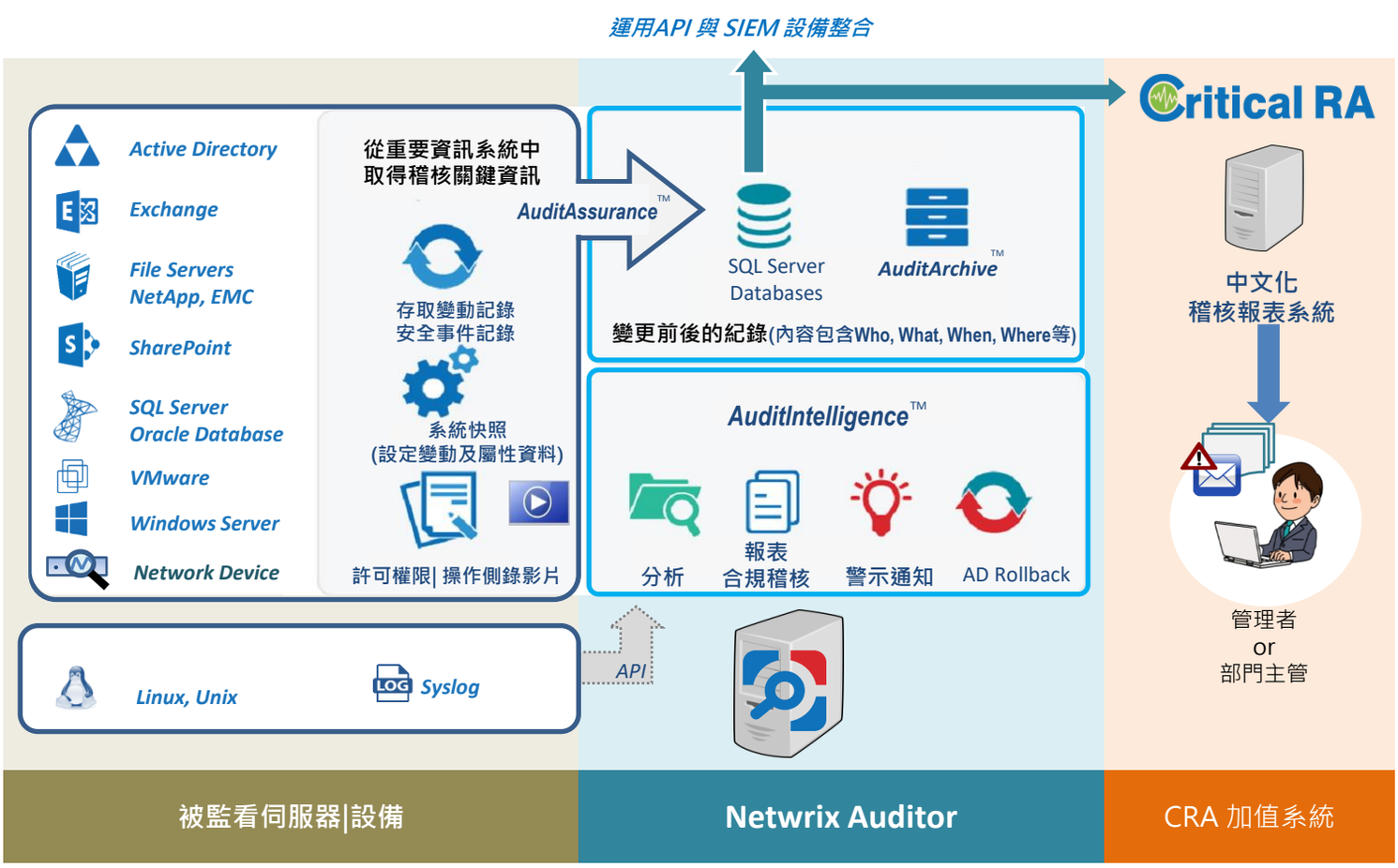
運用多種關鍵性報表與組合條件式查詢進行調查，就像使用Google搜尋一般容易，讓你抽絲撥繭、找出潛在安全威脅事件，如不尋常的使用者登錄及存取活動(可能肇因於帳戶身份被盜用或臨時帳戶、心懷不軌的特權帳戶或挾怨報復的人員)。

檔案存取活動及權限稽核

- 稽核檔案伺服器存取活動
- 權限設定變動輔助覆核
- 違規存取或刪檔活動調查
- 掌握檔案存取權限適切性
- 機密檔案接觸史追查
- 惡意程式,勒索軟體感染的即時預警
- 輔助儲存檔案有效性分析(如冷資料)

AD及特權帳號活動稽核

- 可疑入侵AD風險預警
- 深入瞭解每個AD、GPO變動
- 嘗試登入失敗活動的深入調查
- 顯示AD物件系統快照
- 帳戶密碼變動,鎖定及風險調查
- 特權帳號、不活躍帳號變動追蹤

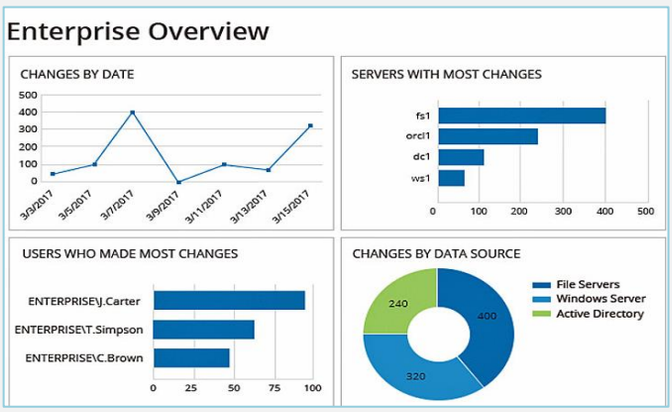


Feature

掌握AD帳號提權或異常變動，維護帳戶安全

針對AD物件、GPO物件、Logon登錄記錄發送變動偵測警示及詳細紀錄報表，有助於調查不尋常的變動，可能與提權攻擊、GPO原則被惡意修改..資安事件。

AD關鍵基礎架構中必須定期檢查是否有不尋常的設定變動，通常駭客最愛攻擊AD目錄服務，因此要確保任何AD變動都是經過合法授權才進行相關設定，也須盤點AD帳號及對應AD物件的權限，或是盤點是否有哪些帳戶密碼永不過期，並進而檢視這些帳號的密碼管理方式是否要調整，或是否有未經許可的臨時帳號提權活動，降低不必要設定可能帶來的風險，以落實AD伺服器的變動稽核。



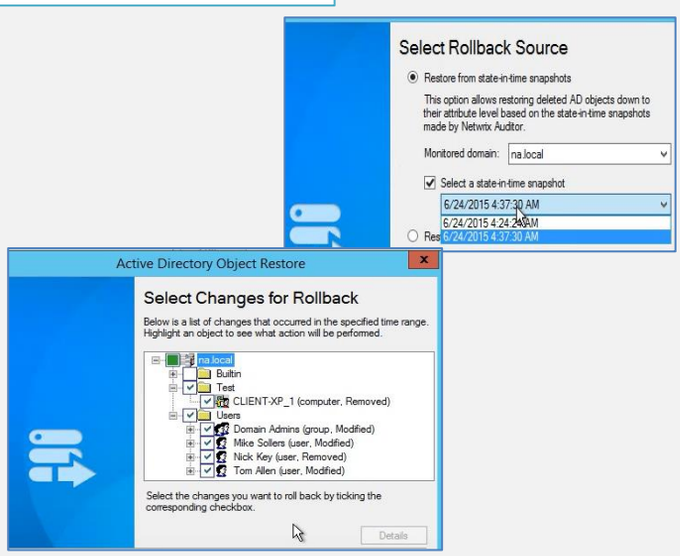
偵測調查可疑的嘗試登入或異常存取|變動，即時警示通知

運用Netwrix互動式搜尋並設定觸發門檻值，可設定違規或異常的變動一旦發生就會發送警示通知，搭配風險參數後，將觸發警示留存記錄並作為線上稽核，避免發生資訊安全事件，讓系統管理者即早處理；可追查是否有大量嘗試登入的攻擊活動，並深入分析其登入來源及失敗原因進行調查，或是存在哪些AD設定變更、臨時帳號提權活動，評估是否違反組織安全政策。

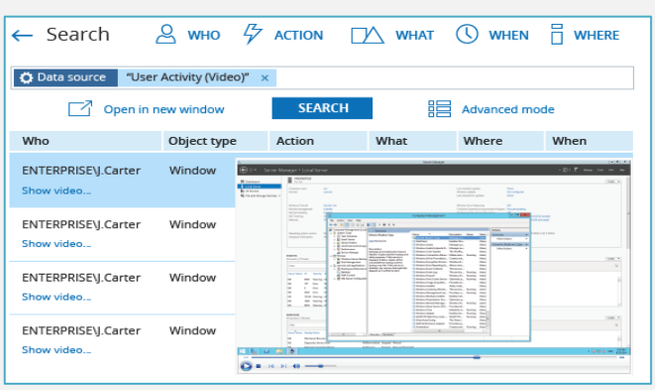
這些可疑的變動或操作(如:哪些使用者進行變更, 影響到哪些系統..等)，能看出特定變動是由何時、 誰、哪裡、 如何發生，可顯示發生”前”與”後”的相關資訊。

隨時掌握系統的設定狀態，回復不允許的設定

針對AD 、檔案伺服器、Windows Server提供系統快照類報表，如: AD帳號及物件的對應權限清冊、部門檔案資料夾的存取權限清冊、Windows Server的軟體清單、群組及帳號清單..等資訊， 定期審視有助於防範逾權存取的風險。內建AD物件還原工具(Active Directory Object Restore tool)，允許將不想要的帳號物件變動還原到指定過去時點的屬性值。



能看到各時點的系統設定屬性快照，如:根據某特定時間的群組規則及密碼規則，找出是哪些設定變更造成系統被鎖定。若發生未經授權存取或惡意程式感染事件，在系統未停機或從備份倒回資料前，都能回復到事件發生前的設定狀態，有助於迅速進行事件應變及回復。



發現偵測不到的異常行為

事件記錄無法呈現的異常活動，都能進行追蹤及舉證。可針對重要系統或可疑人員的操作進行操作歷程的螢幕側錄，可配合報表搜查可疑活動並播放影片，還原實際操作活動。

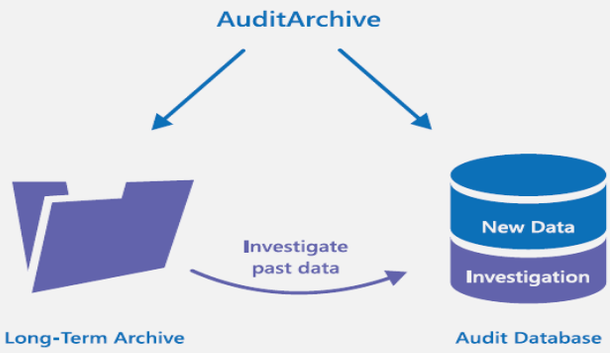
Feature

保護機敏資料，掌握人員存取權限的異常變動

無論是機敏文件、財務資料、營業秘密、個資..等，須定期檢查這些檔案或資料庫在何時被何人做哪些異常存取(讀檔、刪除、修改...)，必須定期檢查是否只有合法授權使用者才能存取，需要進行使用者及檔案物件的對應存取權限盤點，還能盤點檔案及擁有者排行，以掌握檔案伺服器的重要存取稽核資訊。

稽核軌跡記錄的長期保存及合規報表範本

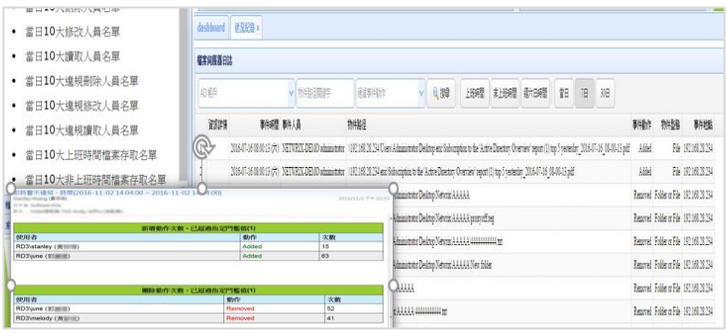
採用AuditArchive™兩層式儲存(檔案式File-based+資料庫SQL database) 長期保存稽核資料(長達10年以上) 。
提供250款以上稽核報表(含法規遵循套版-ISO 27001 PCI, GDPR... 等) ，配合中華數位的Netwrix關鍵性報表輔導顧問服務，有助於遵循法規及安全政策要求，落實變動管理及存取安全控管。

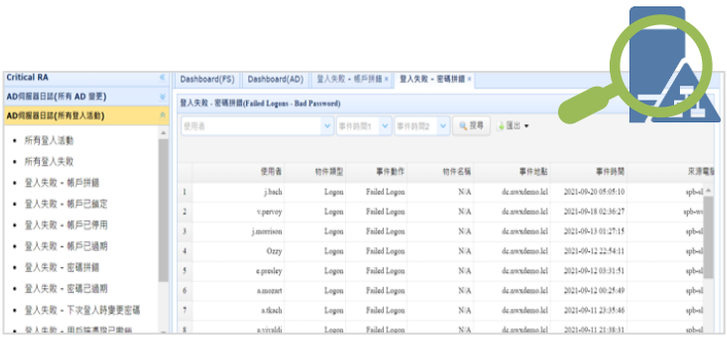


中華數位科技加值開發

Critical RA

部門資料夾路徑	事件人員	AD帳號	存取權限(英文)	存取權限(中文)	繼承關係
\\AT60\garfile (Permissions: Different from parent)	AT60\Administrator	陳小明	Modify (Read, Write, Execute, List folder content)	修改	Directly
\\AT60\garfile (Permissions: Different from parent)	AT60\LeoTing	丁里歐	Full Control	完全控制	Directly
\\AT60\garfile (Permissions: Different from parent)	AT60\MinChang	張民	Full Control	完全控制	Directly
\\AT60\garfile (Permissions: Different from parent)	AT60\TomChen	陳偉安	Read (Execute, List folder content)	讀取	Directly





CRA for NAS (Synology、QNAP)

New

CRA for NAS會直接收集QNAP或Synology檔案存取活動記錄，將檔案存取活動記錄處理和解析後，提供人員存取NAS中檔案及資料夾的存取活動日誌及分析報表，本系統也會收集QNAP或Synology共用資料夾或檔案的存取權限，提供資料夾或檔案存取權限盤點報表。運用本系統對於存取重要資料可留存軌跡紀錄，也能了解人員是否有合適的存取權限，對於資料保護及合規稽核兼具多重管理效益

CRA PA+ 檔案權限盤點追蹤系統

※須搭配Netwrix for Windows File Server 或EMC 或NetApp模組使用

運用 Netwrix 產製的檔案權限報表進行中文化的內容轉換，提供中文化權限盤點報表排程寄發、檢視報表及回覆意見的追蹤流程

CRA 中文化檔案存取稽核系統

※須搭配Netwrix for Windows File Server 或EMC 或NetApp模組使用

全中文化介面，支持網頁瀏覽器操作，提供檔案存取日誌查詢|存取活動的人員排行日報表及警示通知，記錄內容可同步顯示帳號的 AD 中文顯示姓名

CRA for AD 關鍵變動及風險稽核系統

※須搭配Netwrix Auditor for AD模組使用

查詢 AD 使用者帳號使用狀態及密碼管理情形，深入分析多種登入失敗類型活動、GPO 變動活動，基於 IT 管理實用情境，提供 AD 物件變動資訊的快查綜整儀表板，針對重要 AD 帳號變動情境發送警示通知信

Netwrix Auditor 模組一覽表

依監看伺服器種類而區分不同授權模組

監看伺服器模組	用途概述
Active Directory Server	可對被管理的AD網域(包含AD物件、群組政策設定、目錄分區等)的變動進行偵測，並產製管理監看報表(包含登錄活動摘要統計(包含有互動或無互動的使用者登錄)及嘗試登錄失敗等活動產製報表；也會偵測不活躍的使用者及密碼過期等情形)，發送即時警示通知，也產生每日網域架構的快照(若有變動都會留下歷史存檔)，也提供AD user及物件者的權限盤點報表。提供AD rollback tool，允許將不想要的AD使用者帳號物件的變更操作回復到它們的屬性層。
Windows Server	可偵測Windows-based伺服器的架構及所有設定變更並產製報表，包括硬體設備、驅動器、軟體、服務、應用程式、網路設定、註冊設定、DNS及其他更多設定變動，也提供本機user物件的權限盤點報表、安裝作業系統的軟體資產盤點報表。另外也提供事件記錄管理功能及使用者操作活動影片側錄功能。
MS-SQL Server	能偵測MS-SQL Server的個體實例(Instance)及資料庫內容的所有設定變更，包含監看SQL Server物件、個體實例、角色及資料庫、表單、儲存程序、資料列內容..等變動；及監看登錄活動(支持Windows Logon、SQL Logon，包含成功及失敗記錄) 所有變更並產製報表。
Oracle Database	能偵測Oracle資料庫物件如個體實例設定、權限及安全設定的相關變動，包含資料庫物件、目錄、使用者帳號、稽核政策、機敏資料、及觸發等變動；及監看登錄活動(包含成功及失敗) 所有變更並產製報表。
SharePoint	能偵測對SharePoint的farms、servers及sites的所有組態設定變更，包含對使用者的操作內容、安全性設定變動、許可權限/繼承許可權限/群組成員/安全性原則等的修改變更，並產製報表。
VMware	能偵測VMware vSphere、vCenter、ESXi的設定變動，包含對ESX伺服器、資料夾、叢集、資源集區、及安裝虛擬機器的硬體進行變更，並產製報表。
Exchange	可偵測Exchange伺服器及郵件信箱的設定及權限變更並產製報表。也會追蹤Exchange架構中郵件信箱的存取事件，也針對非本人存取郵件信箱的行為發出警告，通知信箱帳號的持有人。 ※使用本模組需搭配Active Directory 監看模組
Network Devices	能偵測對Cisco Firewall(ASA)、Cisco Switch|Router(IOS)、Fortigate Firewall、Palo Alto、SonicWall、Juniper..等品牌的防火牆、VPN網路設備的設定變動、硬體環境設定變動 、網路設備本機登入或VPN設備遠端登入活動稽核，並產製報表。

監看File Server類別

(分成Windows File Server、EMC (cifs)、 NetApp (cifs)三種模組)

監看伺服器模組	用途概述
1. For Windows File server 2. For EMC (cifs) 3. For NetApp (cifs)	可對Windows File server 或 NetAPP(cifs) 或 EMC NAS(cifs) 中所有檔案、資料夾、分享/權限的操作變更進行偵測並產製報表，以上變更包含存取行為的成功及失敗; 提供多款變動分析儀表板及人員存取活動排行報表、機敏資料存取活動監看報表；檔案系統快照類報表包含使用者存取權限清冊、部門檔案|資料夾權限盤點報表、及多款資料夾檔案屬性盤點報表，掌握檔案伺服器的重要存取稽核資訊。

Softnext 中華數位科技
TEL:+886-2-25422526 FAX:+886-2-25424838
Email: service@softnext.com.tw

經銷商：

www.softnext.com.tw