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。

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。(屬於Netwrix for Windows Server 模組功能)

FORRESTER

國際資訊研究機構Forrester 指出"組態設定稽核技術" 是未來5年內重要性名列第一:
netwrix.com/configuration-auditing

Gartner

Gartner指出 "組態設定稽核工具能幫助您依據最佳實作來分析系統組態設定，強制推動設定標準以遵循法規要求" 。

知名客戶

MITSUBISHI　CISCO　IBM　NASA　Allianz　AT&T

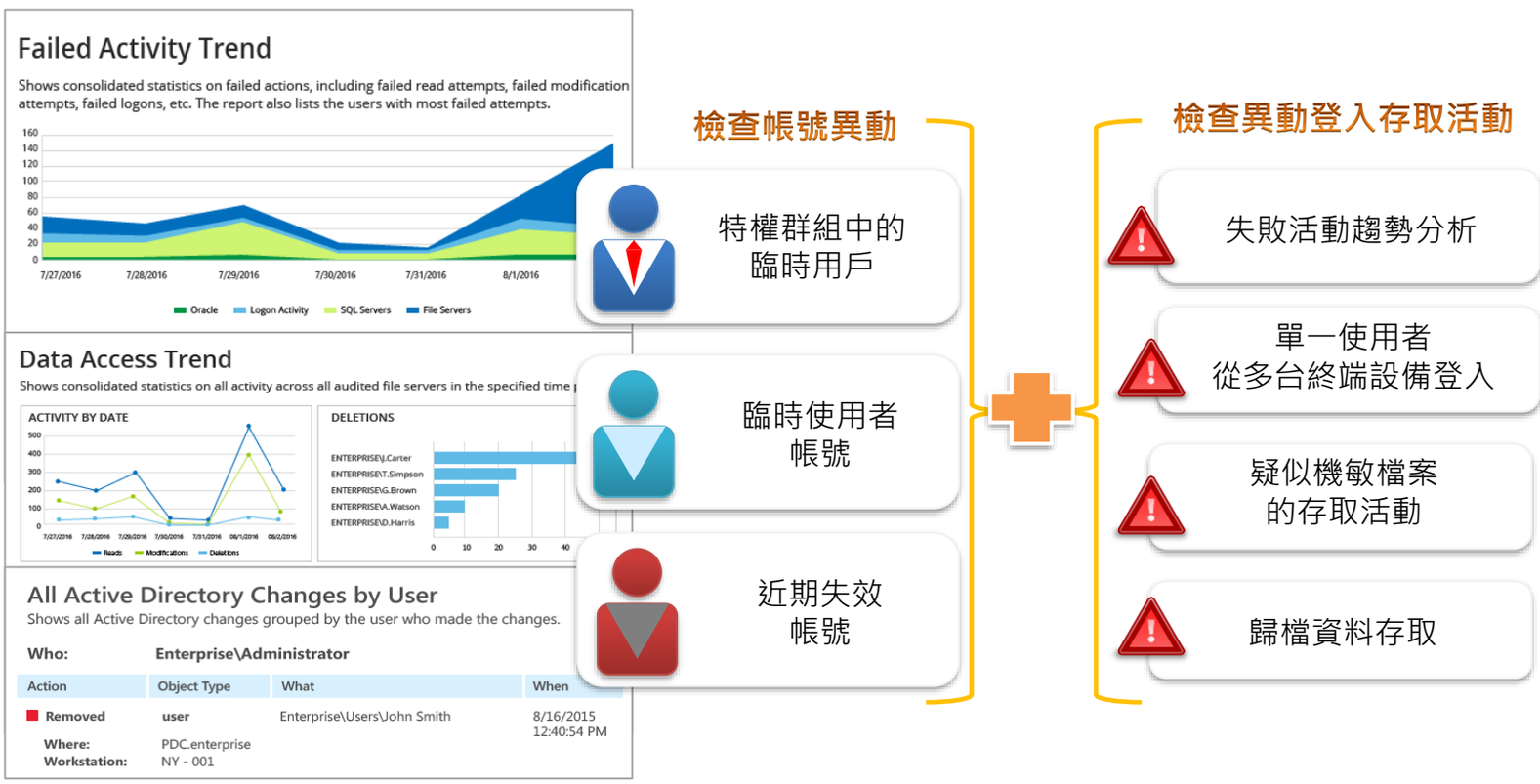
我們必須遵守國際稽核法規，我們也被稽核部門要求，必須找到能滿足具體稽核要求的解決方案。Netwrix能讓我們對微軟應用環境的各個關鍵面向進行監控，因此能滿足這些嚴格的資訊稽核要求。

Mervyn Govender, CIO, CreditEdge
Read the case study:
netwrix.com/creditedge

Updated:202004_NW9.9_AD

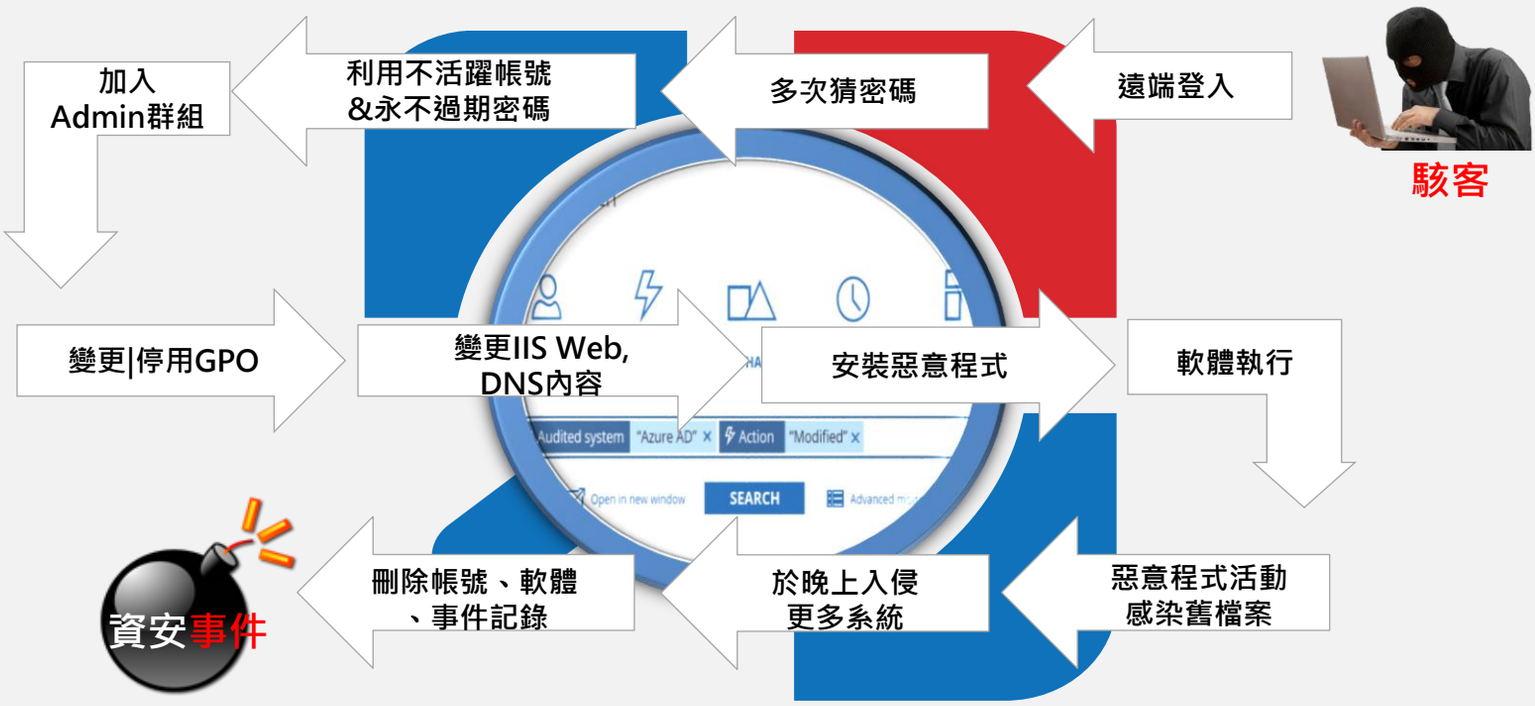
運用 Netwrix找出可疑的使用者異常存取活動

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)。



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。

抓住 Hacker的入侵軌跡

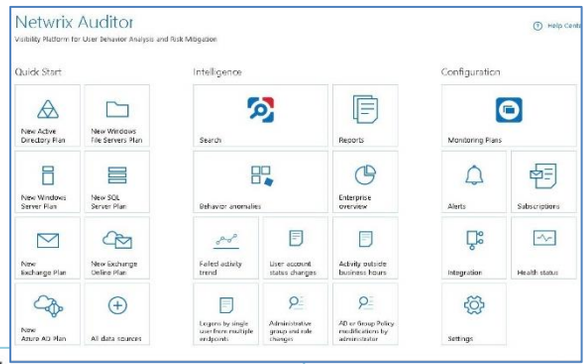


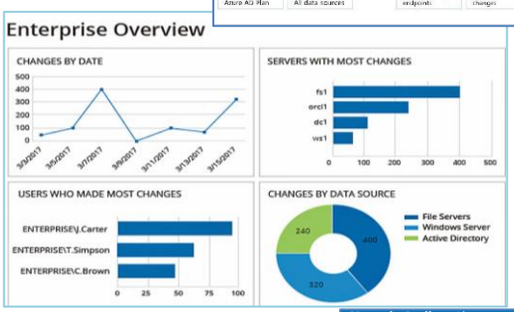
Feature

掌握AD帳號提權或異常設定變動，維護帳戶安全

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。

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





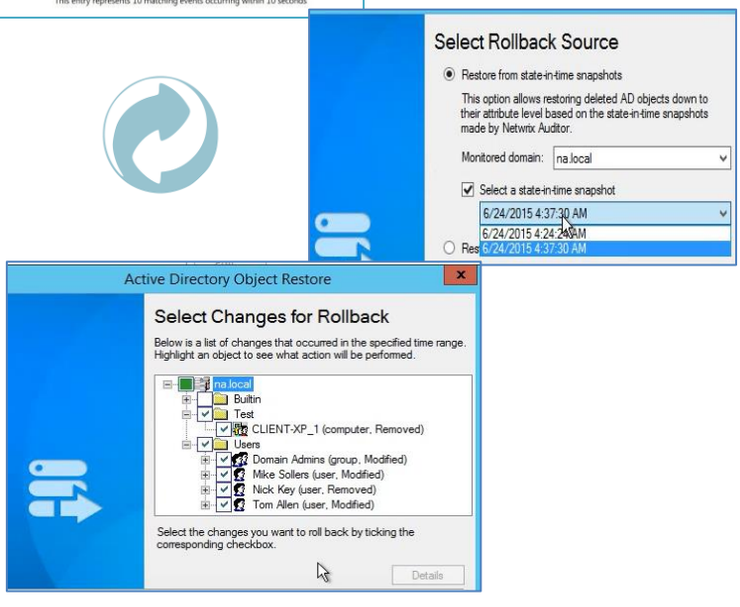
偵測調查可疑的嘗試登入或AD異常變動，即時警示通知

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。

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User或Computer物件變動還原到指定過去時點的屬性值。

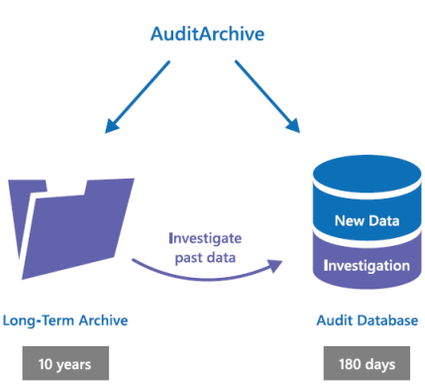
能看到各時點的系統設定屬性快照，如:根據某特定時間的群組規則及密碼規則，找出是哪些設定變更造成系統被鎖定。若發生未經授權存取或惡意程式感染事件，在系統未停機或從備份倒回資料前，都能回復到事件發生前的設定狀態，有助於迅速進行事件應變及回復。

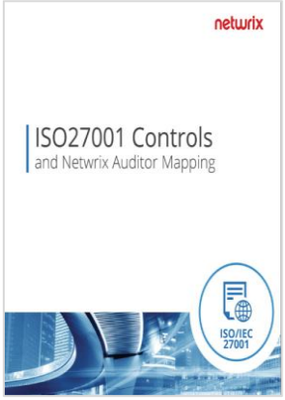


稽核軌跡記錄的長期保存及合規報表範本

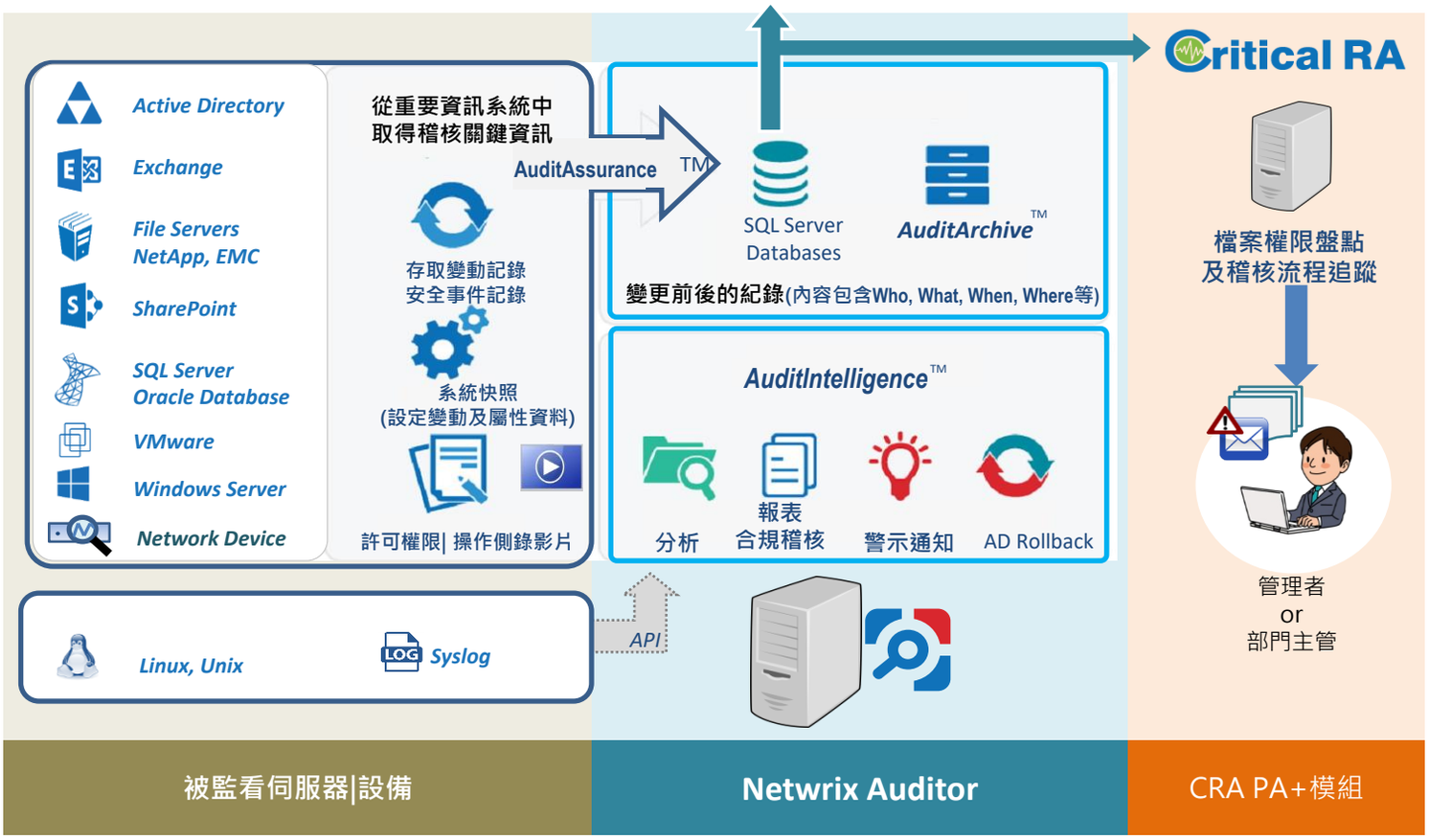
採用AuditArchive™兩層式儲存(檔案式File-based+資料庫 SQL database) 長期保存稽核資料(長達10年以上)。

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。





運用API 與 SIEM 設備整合



可支持監看類型	用途概述	支持規格/版本
AD Server	• Netwrix Auditor for Active Directory偵測所有AD網域內的變動並產製報表，包含AD 物件、群組政策設定、目錄分區及更多資訊。 • 還能產生每日管理網域架構的快照，可用來評估任何時候的AD管理狀態。 • 提供多款變動管理監看報表，也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。 • 也提供內建的AD物件還原工具(Active Directory Object Restore tool)，允許將不想要的AD物件變更操作還原到它們的屬性層。	網域控制站作業系統版本： • Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2 • Windows Server 2016 • Windows Server 2019
	• Active Directory Federation Services • 收集登入(成功|失敗)紀錄	• AD FS 3.0-Windows Server 2012 R2 • AD FS 4.0-Windows Server 2016 • AD FS 5.0-Windows Server 2019

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