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)的設定變更及存取稽核，偵測是否有異常的設定、操作，提供報表及即時警示通知。Netwrix稽核記錄支持長期歸檔保存，提供多款法規遵循報表，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**：能支持虛擬化或其他系統/應用程式，即使它無產生任何日誌記錄(logs)，可運用對特權使用者的螢幕活動側錄，配合儲存於資料庫中相關設定進行追蹤、搜尋並播放操作活動影片。

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 · CAT · BR · IBM · NASA · BOEING Forever New Frontiers

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

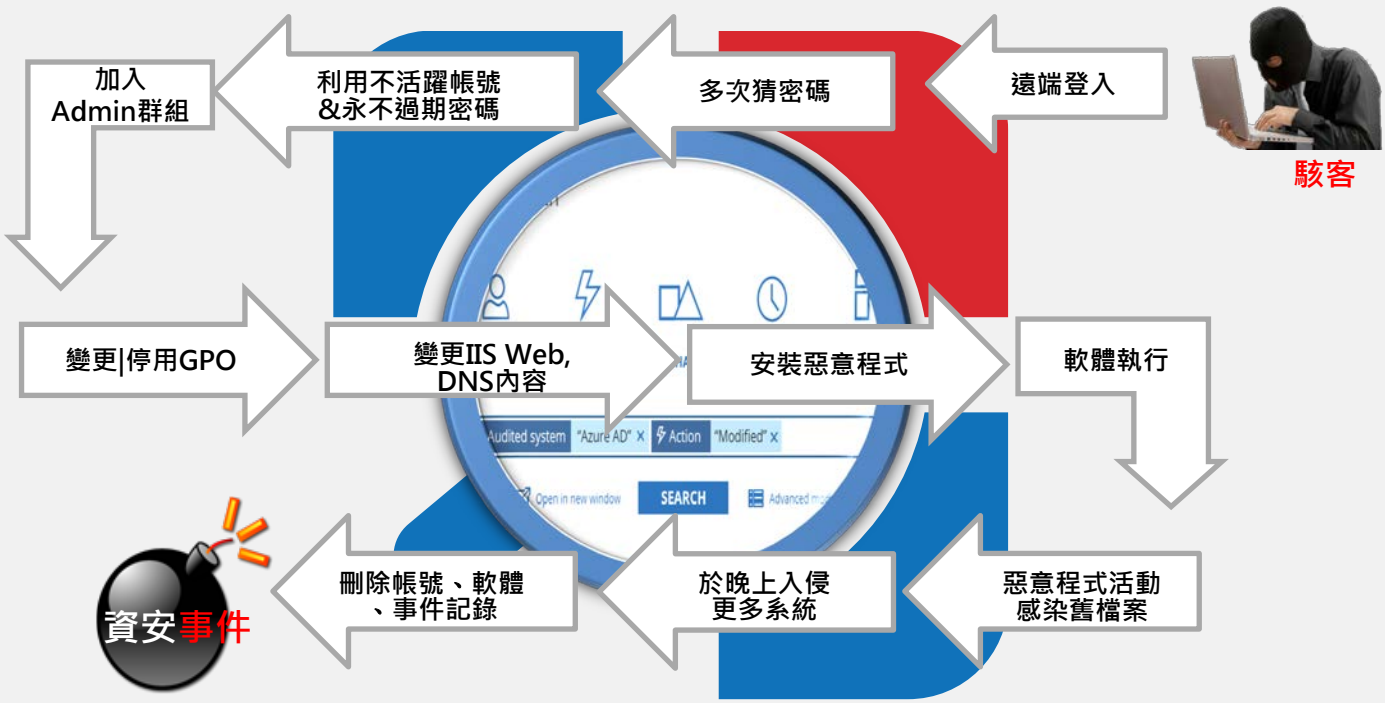
# Application

## 追查資料外洩發生前<br>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。

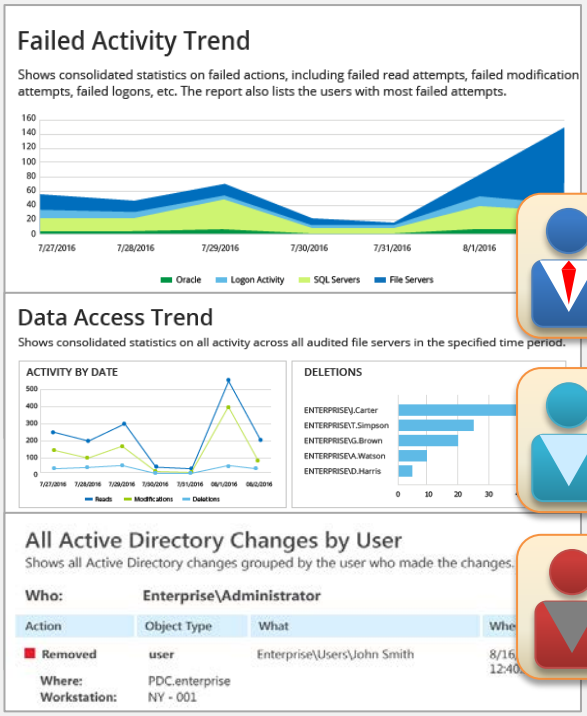
- 深入瞭解每次異常存取的使用者活動，找出更詳細的行為資訊。
- 關注異常的資料存取或異常登入等行為，找出潛在威脅的徵兆。
- 即早識別出受害的帳戶，以免災情擴大。
- 深入稽核特權帳戶以識別非法|不當的操作活動。
- 全盤掌握IT環境內的所有使用者活動，消除安全性盲點。
- 注意關鍵性變化、可疑的登錄活動及不尋常的失敗活動，利於快速回應資安事件。

## 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)。




檢查帳號異動

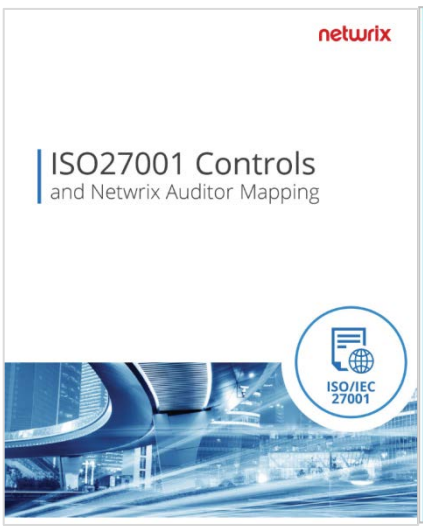
- 特權群組中的臨時用戶
- 臨時使用者帳號
- 近期失效帳號

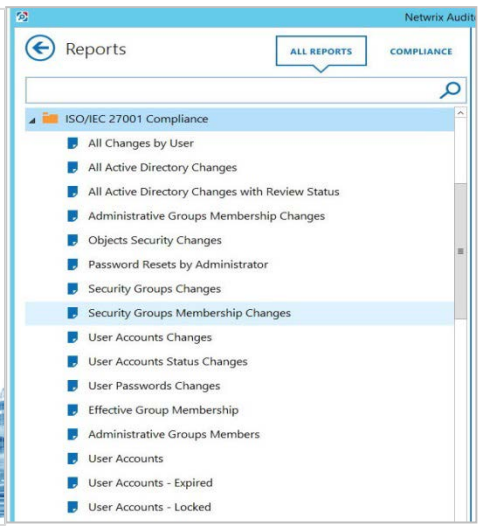
檢查異動登入存取活動

- 失敗活動趨勢分析
- 單一使用者從多台終端設備登入
- 疑似機敏檔案的存取活動
- 歸檔資料存取

# Netwrix內建多款國際法規遵循稽核報表集

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, FISMA...等其他法規標準，開箱及用的稽核工具，可作為合規性稽核檢查及符合資安規範的舉證報表。




NERC · FERPA · FISMA · PCI · HIPAA · GLBA · SOX · ISO/IEC 27001

# Benefit

## Streamline Compliance 簡化合規

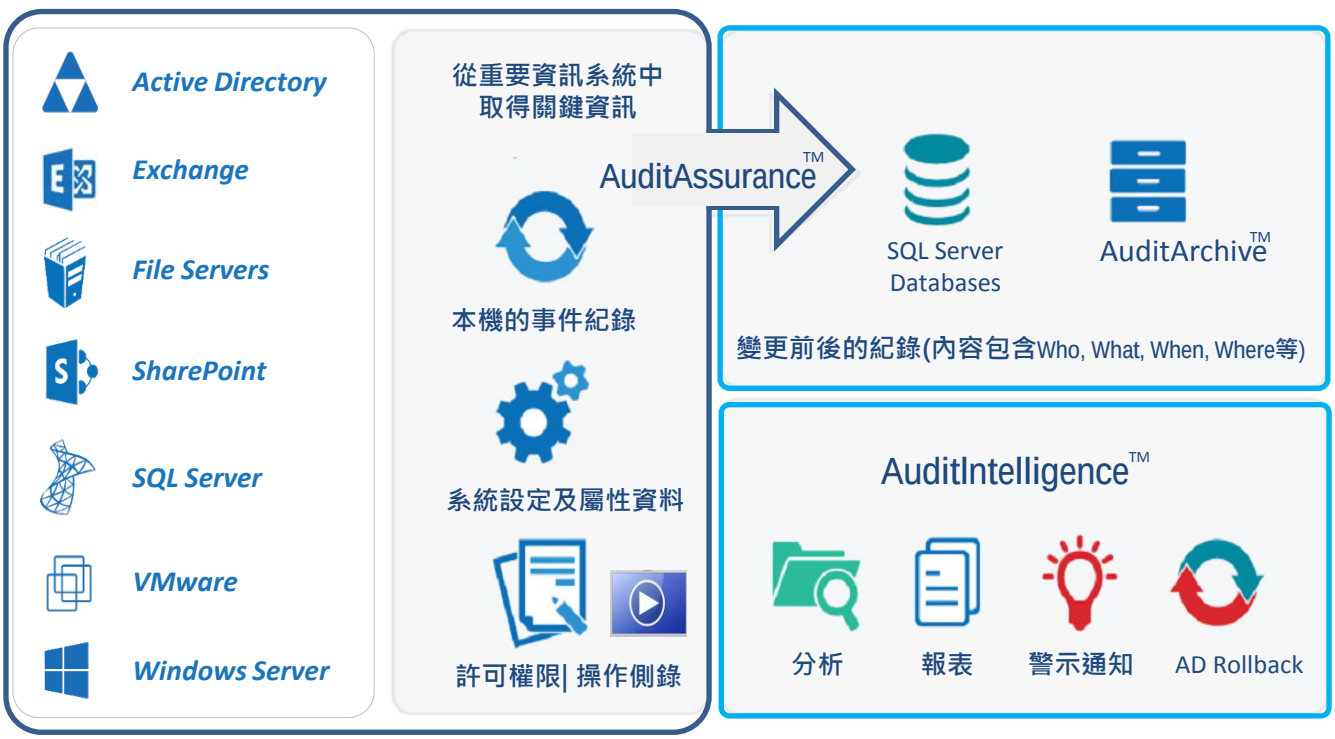
- **通過符合法規的稽核活動：**如ISO 27001, PCI, SOX, FISMA及其他法規標準或內部政策要求，提供多款合規性報表範本, 運用AuditArchive™兩層式儲存長期保存資料(10年以上)，能集中分析、快速取得所需要的記錄報表 。
- **持續性法規遵循：**持續稽核授權者或未經授權的操作設定變動。
- **完整涵蓋：**能支持虛擬化或其他系統/應用程式，即使它無產生任何日誌記錄(logs)。

## Strengthen Security 強化安全

- **偵測及調查安全事件：**分析對系統設定的未經授權或惡意性設定變更。
- **偵測及防範外洩：**針對機敏資訊去稽核使用者的內容或許可權限的操作設定變動。
- **克服本機稽核的限制及強化輔助SIEM:**運用AuditAssurance™技術，能填補資料稽核的缺口及消除複雜而干擾分析的資料。

## Simplify Root Cause Analysis 易於分析根本原因

- **持續營運：**透過即早偵測到事件相關的變動及有破壞性的系統設定。
- **根本原因分析：**針對事件進行故障排除及系統被破壞性設定的回復處理。
- **減少系統停機時間：**找出肇因於人為操作錯誤或不當的設定變更，以緊急修正。
- **變更管理：**內建簡化的變更管理流程或可整合第三方 ITIL-based的變更管理系統。
- **建立可歸責性：**針對特權用戶、透過遠端提供服務的廠商及被管理的服務提供商(MSPs)，可運用針對特權使用者的螢幕活動側錄，可搜尋並播放這些影片記錄。

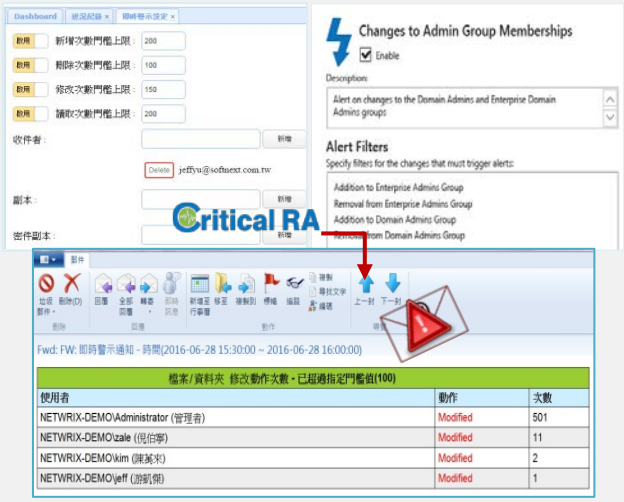


# Feature

## 偵測調查可疑的存取活動，即時警示通知

運用Netwrix的互動式搜尋功能，可追查是否有哪些變更/存取活動是違反組織安全政策 ；可設定違規或異常的變動一旦發生，就會發送警示通知，避免發生資訊安全事件，讓系統管理者即早處理。

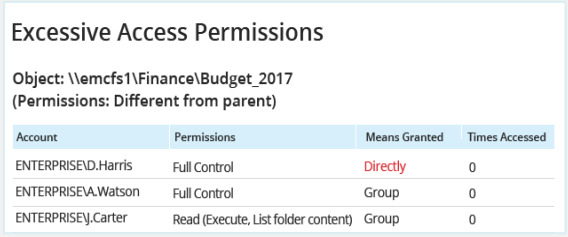
這些可疑的變動或操作(如:哪些使用者進行變更, 影響到哪些系統..等) ，能看出特定變動是由何時、 誰、哪裡、 如何發生，可顯示發生”前”與”後”的相關資訊。




## 保護機敏資料，掌握存取權限的異常變動

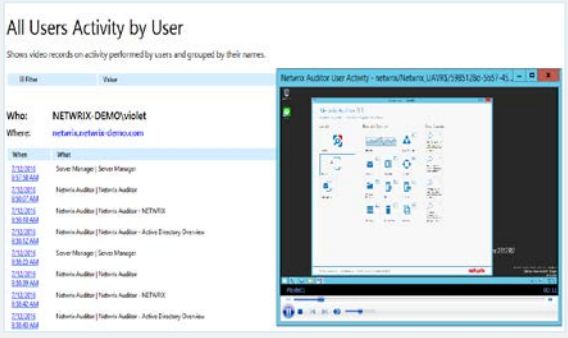
無論是機敏文件、財務資料、營業秘密、個資..等，須定期檢查這些檔案何時被何人做哪些異常存取(讀檔、刪除、修改...) ，運用Critical RA提供更密集發送的關鍵稽核報表、及偵測可疑(大量)檔案操作活動的即時警示通知，即時稽核檔案違規存取。

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。

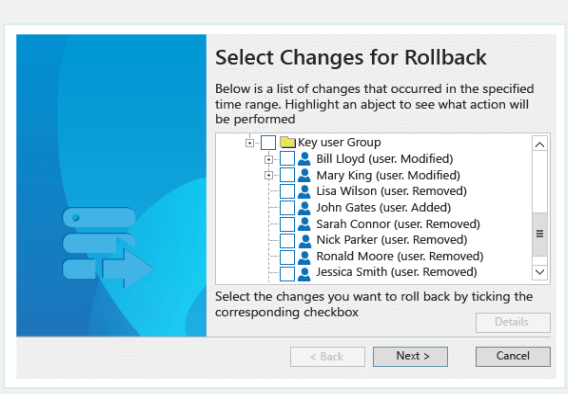

## 發現偵測不到的異常行為

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。




## 隨時掌握系統的設定狀態，回復不允許的設定

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200款以上稽核報表(含法規遵循套版-ISO 27001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。

| 監看伺服器模組 | 用途概述 |
| --- | --- |
| Active Directory Server | 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。<br>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。<br>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。<br>也提供內建的目錄服務標的回復工具(Active Directory Object Restore tool)，可將不允許變動的AD物件(系統快照)回復到原先的屬性值，有助於變動復原。 |
| Windows File server | 能偵測Windows檔案伺服器的存取活動及變更(包含對檔案、資料夾、分享及許可權進行修改，及嘗試存取成功及失敗的行為)並產製報表。<br>還能盤點檔案及擁有者排行、進行使用者及檔案物件的對應存取權限盤點，掌握檔案伺服器的重要存取稽核資訊。<br>提供關鍵稽核報表、大量異常存取警示通知的模組(Critical RA)，即時稽核檔案違規存取。 |
| Windows Server | 能偵測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。<br>提供事件記錄管理功能及使用者操作活動影片側錄功能。 |
| EMC (CIFS) | 能偵測EMC Celerra、VNX/VNXe及 Isilon storages的所有變更(包含對檔案、資料夾、分享及許可權進行修改，及嘗試存取成功及失敗的行為)並產製報表。 |
| NetApp (CIFS) | 能偵測NetApp Filer appliances(包含 cluster- 及 7- modes)的所有變更(包含對檔案、資料夾、分享及許可權進行修改，及嘗試存取成功及失敗的行為)並產製報表。 |
| MS-SQL Server | 能偵測MS-SQL Server的所有變更並產製報表，包含對SQL Server的設定變更，及資料庫內容的變動。 |
| SharePoint | 能偵測對SharePoint的farms、servers及sites的所有設定變動及讀檔存取，包含修改內容、修改安全性設定、修改許可權限等，並產製報表。 |
| VMware | 能偵測VMware vSphere、vCenter、ESXi伺服器的設定變動，包含對ESX伺服器、資料夾、叢集(clusters)、資源集區(resource pools)、及安裝虛擬機器( virtual machines)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。<br>**使用本模組需搭配Active Directory 監看模組** |

## Netwrix 獲獎榮耀


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


經銷商：

www.softnext-inc.com