Quest ChangeAuditor

軌跡紀錄稽核的最佳解決方案

面對各式各樣的存取軌跡紀錄，必須符合法令合規性與資安事件預防及追查，大量的軌跡紀錄稽核趨勢也朝向集中化方式，以達到事半功倍的效果，節省企業人力與金錢的成本支出。

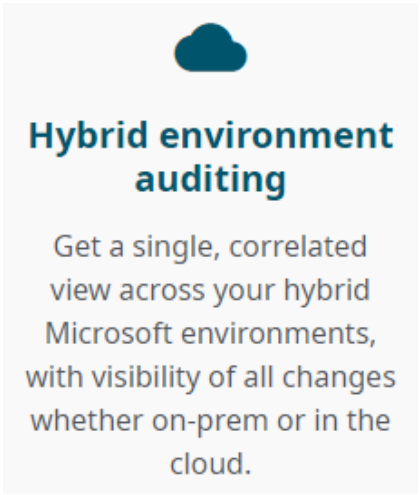
在 Windows 平台上，Quest 推出一個最佳圖形化的軌跡紀錄稽核解決方案：ChangeAuditor，以下簡述方案的優勢。

軌跡紀錄稽核的首要，即是進行即時 IT 資訊稽核與監控。

一個事件所形成的軌跡資訊，無外乎所須瞭解的是：

1. 何人
2. 何事
3. 何地
4. 何物
5. 來源

以上五個特點，均可以使軌跡紀錄稽核達成可及性運用之目的。



針對現今企業地端與雲端混合 IT 基礎架構，可利用 Change Auditor 進行微軟平台地雲混合環境中的所有異動進行詳細的稽核。以達成單一連動的全觀檢視。

面對日益頻繁的網域資料盜取及驗證檔案與身份識別程式遭非法探勘，Change Auditor 可針對此種資安威脅進行即時監控。

Golden Ticket detection

Detect and alert on common Kerberos authentication vulnerabilities used during Golden Ticket / Pass-the-ticket attacks.

針對常見之利用 Kerberos 認證系統弱點挾持萬能票證攻擊網域控制器之資安威脅行為，Change Auditor 可進行偵測並發出告警通知。

Object protection

Protect against changes to critical data within AD, Exchange and Windows file servers, including privileged groups, GPOs and sensitive mailboxes.

Change Auditor 可針對關鍵性的 AD 與 Exchange 物件，如特權帳號群組、關鍵性高的群組關係原則設定或具機敏性的郵件信箱，進行防止變更之物件保護。

Normalized 5W audit details

Translate cryptic native logs into a simple, normalized format highlighting the who, what, when, where and workstation details and before and after values.

Change Auditor 可馭繁化簡地將複雜的原生日誌內文，轉化為人事時地物之 5W 易讀性佳的即時顯示稽核事件詳細資訊，並輔以變更前後的資訊訊息，以供比對。

Change Auditor 可隨時隨地將關鍵變更與告警，利用電子郵件推送通知，甚至您不在辦公處所，都能以行動裝置得知。

Real-time alerts on the move

Send critical change and pattern alerts to email and mobile devices to prompt immediate action, even while you're not on site.

SIEM integration

Integrate with SIEM solutions to forward Change Auditor events to Splunk, ArcSight, QRadar or any platform supporting Syslog.

Change Auditor 可轉送稽核事件至安全資訊與事件管理(SIEM)，提供其整合分析資料：支援 Splunk、ArcSight、QRadar 或是其他可支援 Syslog 之 SIEM 平台。

Change Auditor 支援全方位的合規報表產出，以符合相關法規要求。如 GPDR、PCIDSS、HIPPA、SOX、FISMA/NIST、GLBA 等。

Auditor-ready reporting

Generate comprehensive reports to support regulatory compliance mandates for **GDPR**, PCI DSS, HIPAA, SOX, FISMA / NIST, GLBA and more.

想了解更多 Change Auditor 的詳盡內容嗎? 歡迎前往下列網址瀏覽：

https://www.mpinfo.com.tw/product/det/208

◎如您有任何問題，歡迎隨時與我們聯繫：

雲安事業部

副理 廖文志 Albert

02-27316868 分機 420 / albertliao@mpinfo.com.tw