Quest

Change Auditor

Change Auditor

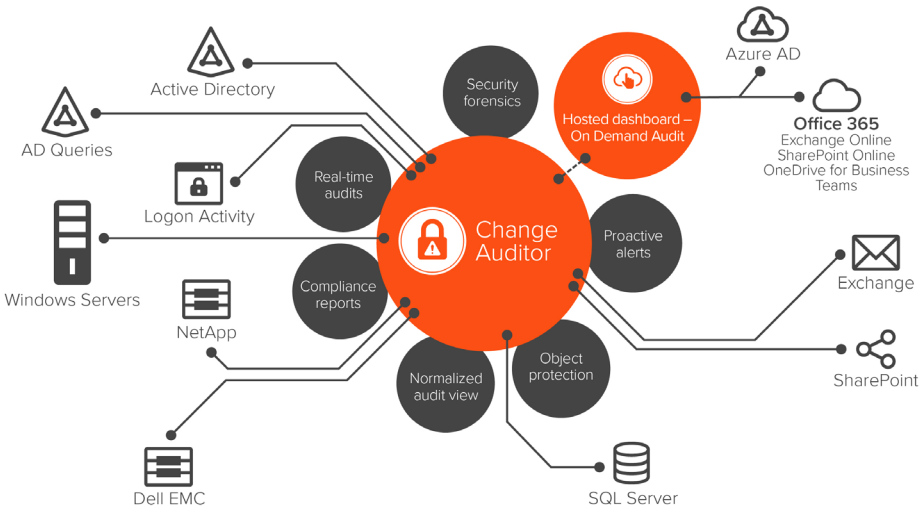
為您的混合 Microsoft 平台環境提供實時安全審核

企業中的應用程式和伺服器的事件日誌紀錄及變更報告繁瑣又費時，有時甚至無法使用本機審核工具來完成。由於沒有中央控制台，您必須為每個伺服器重複該過程，最終將獲得大量沒有上下文的資料和許多報告。

這意味著，證明合規性或對事件做出快速回應是一個持續的挑戰。由於本機端事件詳細資訊非常分散且難以理解，導致您的資料安全性也存在風險，等您發現問題時可能為時已晚。因本機工具無法阻止特權使用者清除事件日誌，您可能會失去日誌資料，無法實現最初的審核目的。

幸運的是 Quest® Change Auditor 可以提供幫助。Change Auditor 系列解決方案使您無需啟用本機審核功能，即可實時對 Active Directory (AD)、Azure AD、Exchange、 Office 365、SharePoint、EMC、NetApp、SQL Server 和 Windows file servers，以及針對 AD 的 LDAP 查詢所做的所有更改進行審核、發出提醒、提供報告。

透過 Change Auditor，您可以對 Microsoft Active Directory、Azure AD、Exchange、Office 365、file servers 等的所有關鍵配置、使用者和管理員異動，進行完整的實時 IT 審核、深入取證和安全監控威脅。Change Auditor 同時追蹤企業內的登入、身分驗證和其他關鍵服務的使用者活動資訊，以增強威脅檢測和安全監控。



借助 Change Auditor，您可以了解所有更改的人員、內容、時間、地點以及來源工作站，並且所有項目均按時間順序列出，包括關聯的內部部署身分和雲身分。

> “我們的團隊進行滲透測試時，對於他們無法入侵受 Change Auditor 保護的對象感到很驚奇。”
>
> *企業管理者*
> *大型零售連鎖店*

優點：

- 藉由追蹤所有事件以及與特定事件相關的更改，消除未知的安全問題，確保持續存取應用程式、系統和使用者。
- 利用自動解釋加密資料及其嚴重程度，以便更快、更好地做出決策，從而減輕壓力和降低複雜性。
- 無論使用者是否在辦公室，均可透過任何設備接收即時警報，立即做出回應，降低安全風險。
- 透過在不使用本機審核的情況下收集事件，以減少對伺服器的效能影響。
- 簡化合規性報告，獨立於內部政策和外部法規，包括 GDPR、PCI DSS、HIPAA、FISMA/NIST 等。
- 向管理人員和審核人員證明相應的 IT 管制，讓您能更加安心。

“以往調查問題可能需要耗費一小時，而 Change Auditor 可以將時間縮短為 5-10 分鐘。”

Dennis Persson
IT 系統技術員, Region Halland

產品
Change Auditor for Active Directory
Change Auditor for Active Directory Queries
Change Auditor for EMC
Change Auditor for Exchange
Change Auditor for Logon Activity
Change Auditor for NetApp
Change Auditor for SQL Server
Change Auditor for SharePoint
Change Auditor for Windows File Servers

您可以從一個中央控制台輕鬆安裝、部署和管理您的環境。您可以非常容易的追蹤建立、刪除、修改和存取嘗試，並了解發生的詳情。每個事件和其相關事件都藉由簡單的術語顯示，分別為您提供五大要素：人員、內容、時間、地點和來源工作站，以及過往當今的設定。

這種廣泛的資料分析功能使您可以在出現問題時立即採取措施 (例如特定使用者和工作站進行了哪些其他更改)，消除了其他的不確定性和未知的安全問題。無論您要滿足日益增長的合規性要求，還是內部安全策略，Change Auditor 都是您可以信賴的解決方案。

功能

具有關聯視圖的混合環境審核— 與本機審核不同，Change Auditor 可為混合環境中的活動提供單個關聯視圖，確保發生的所有更改的可見性 (無論是內部部署或雲環境中) 。

安全的威脅監控— 審核和阻止如憑證竊取和 AD 資料庫拷貝等漏洞，並辨別透過不安全協定使用憑證的應用程式。

Golden Ticket 檢測 — 檢測並警告 Golden Ticket/ Pass-the-ticket 攻擊期間使用的常見 Kerberos 身分驗證漏洞。

防止更改 — 防止更改 AD、Exchange 和 Windows file servers 中的關鍵資料 (包括特權群組、群組原則物件和敏感信箱)。

可直接呈遞審核員的報告 — 為 GDPR、PCI DSS、HIPAA、SOX、FISMA/NIST、GLBA 等的最佳實踐和法規遵從性要求生成全面的報告。

高效能審核引擎 — 不使用本機審核日誌即可消除審核限制並擷取更改資訊，可以更快速地生成結果並節省大量儲存資源。*

帳號鎖定 — 擷取帳號鎖定事件的原始 IP 地址和工作站名稱，並在交互式時間軸中查看相關的登錄和存取嘗試。這有助於簡化內外部安全威脅的檢測和調查。

隨時隨地獲得警報 — 向電子郵件地址和移動設備發送關鍵更改和模式警報，以提醒立即採取措施，即便不在現場也能針對威脅更快做出響應。

整合的事件轉發 — 輕鬆與 SIEM 解決方案整合，將 Change Auditor 事件轉發到 Splunk、Arcsight 或I BM QRadar。此外，Change Auditor 與 Quest® InTrust® 互相整合，實現 20:1 的壓縮事件儲存和集中化的本地或第三方日誌收集， 進行解析和分析並對可疑事件發出警報和自動執行響應操作。

包含 On Demand Audit 的托管控制板 — 利用具有響應式搜索、交互式資料可視化和長期事件儲存功能的託管 SaaS 控制板，查看 AD 和 Office 365 混合活動。

關於Quest

Quest 提供許多軟體解決方案，在日益複雜的 IT 環境中發揮新技術的優勢。從資料庫道系統管理，到 Active Directory 和 Office 365 管理，以及網路韌性，Quest 幫助客戶解決他們所面臨的下一個 IT 挑戰。

* Does not apply to SharePoint, EMC, and NetApp.

威雲科技 WeiCloudTech
台北市內湖區瑞光路335號5樓/(02)7721-8168
contact@weicloud.com.tw