Change Auditor

Microsoft 平台環境適用的即時變更稽核

在企業中，應用程式及服務的事件記錄和變更報告相當麻煩、耗費時間，而且在某些情況下無法使用原生稽核工具。因爲沒有中央主控台，您必須在每個伺服器上重複同樣的程序，最後就是取得大量沒有脈絡的資料以及一堆報告。

這表示證明事件符合法規遵循，或對事件快速做出反應，是一項持續不斷的挑戰。您的資料安全也處於風險之中，因爲原生的事件詳細資料非常少且難以解譯。因此，當您找到問題所在時，可能已經太遲了。此外，由於原生工具無法防止特殊權限使用者清除事件記錄，您可能會遺失記錄資料，以至於從一開始就無法達成稽核的目標。

慶幸的是，我們有 Quest® Change Auditor。此產品系列可讓您稽核、警示及回報所有 Active Directory (AD)、Azure AD、Exchange、Office 365、SharePoint、Skype for Business、VMware、EMC、NetApp、SQL Server 和 Windows 檔案伺服器上的即時變更，以及 LDAP 對 AD 的查詢，且無需啓用原生稽核作業。

您可以從單一中央主控台輕鬆安裝、部署和管理您的環境。追蹤那些嘗試建立、刪除、修改和存取活動變得輕鬆無比，而您還能毫不費力地瞭解前因後果，因爲每個事件和所有相關事件均以簡單的詞彙呈現必要的五大資訊：人員、內容、時間、位置和來源工作站，以及過去與目前的設定。

有了 Change Auditor，您可以按時間順序掌握各項變更的人員、內容、時間、位置和原始工作站資訊，包括具有關聯的內部部署和雲端身分。

「Change Auditor 是目前兼具功能和成本考量的最佳解決方案。我們深知工具必須簡潔又好用，讓我們不必具備任何特定的技術專業，即可使用工具建立查詢。」

Stephane Malagnoux，
BPCE Insurance 電腦部門主管

優點：

- 消除未知安全疑慮，透過追蹤所有事件以及與特定事件相關的變更，確保能夠持續存取應用程式、系統和使用者。
- 自動解譯隱密資料和其嚴重性，以減輕壓力和複雜度，更快制定更好的決策。
- 向所有裝置發布即時警示，讓公司內外都能立即回應，在短時間內降低安全風險。
- 不使用原生稽核方式來收集事件資訊，以降低對伺服器效能的影響。
- 簡化法規遵循報告，並區隔內部政策及外部規範，包括 SOX、PCI DSS、HIPAA、FISMA 和 SAS 70 等。
- 爲管理員和稽核人員提供適當的 IT 控管證據，以讓他們安心。

「Change Auditor 是一款非常簡單易懂卻又極爲強大的工具，讓我清楚瞭解員工所做的變更。這樣我就可以強制執行原則、限制存取，並收到資料外洩疑慮的警示。」

資深 IT 架構設計師，中型企業專業服務公司

資料來源：TechValidate。TVID：B4A-A84-619

產品
Change Auditor Threat Detection
Change Auditor for Active Directory
Change Auditor for Active Directory Queries
Change Auditor for EMC
Change Auditor for Exchange
Change Auditor for FluidFS
Change Auditor for Logon Activity
Change Auditor for NetApp
Change Auditor for SQL Server
Change Auditor for SharePoint
Change Auditor for Skype for Business
Change Auditor for VMware vCenter
Change Auditor for Windows File Servers

這種大範圍資料分析可讓您在發生問題時立即採取行動，例如還有哪些變更來自特定使用者和工作站，以免去額外的猜測和未知的資安疑慮。不論您想試著配合越來越多的法規遵循要求或滿足內部安全性政策，都可以仰賴 Change Auditor 解決方案。

功能特色

以關聯式檢視執行混合式環境稽核：稽核混合式環境，包括 AD/Azure AD、Exchange/Exchange Online、SharePoint/SharePoint Online/商務用 OneDrive 以及 AD 登入和 Azure AD 登入。與原生稽核不同，Change Auditor 提供單一關聯式檢視，可讓您查看混合式環境中的所有活動，不論是在內部部署或雲端，都可確保您全盤掌握所有變更活動。

變更防護：防範 AD、Exchange 和 Windows 檔案伺服器中的重要資料發生變更，包括特殊權限群組、群組原則物件和敏感信箱。

支援稽核的報告：針對 SOX、PCI DSS、HIPAA、FISMA、GLBA、GDPR 等規範產生詳盡的報告，以達成最佳實務並符合法規遵循。

On Demand Audit 的主控操作介面：透過主控 SaaS 操作介面使用回應迅速的搜尋、互動式資料視覺化及長期儲存事件等功能，同時查看混合式 AD 和 Office 365 活動。

使用 Change Auditor Threat Detection 主動偵測威脅：透過分析異常活動來評斷組織中風險最高的使用者，以找出潛在威脅，並減少誤判警示的干擾，進而簡化使用者威脅偵測作業。

高效能稽核引擎：移除稽核限制並擷取變更資訊，不需要原生稽核記錄，即可更快得出結果且節省大量儲存資源。*

帳戶鎖定：擷取帳戶鎖定事件的原始 IP 位址和工作站名稱，並在互動式時間軸中查看相關的登入和存取活動。這有助於簡化內部和外部安全性威脅的偵測與調查。

靈活的即時警示：傳送重大變更與模式警示至電子郵件和行動裝置，提醒您立即採取行動，讓您迅速對威脅做出回應，即使不在現場也不會錯過第一時機。

整合式事件轉送：輕鬆與 SIEM 解決方案整合，將 Change Auditor 事件轉送至 Splunk、ArcSight 或 QRadar。此外，Change Auditor 可整合 Quest® InTrust®，以 20:1 的壓縮率儲存事件，並透過對可疑事件的警示和自動化回應動作，集中收集、剖析及分析原生或第三方記錄。

關於 QUEST

Quest 爲快速變遷的企業 IT 世界提供軟體解決方案。我們可協助簡化資料暴增、雲端擴張、混合式資料中心、安全性威脅和法規要求所帶來的難題。我們的產品組合包含用於資料庫管理、資料保護、統一端點管理、身分識別與存取權管理，以及 Microsoft 平台管理的解決方案。

* 不適用於 FluidFS、SharePoint、EMC、NetApp 和 VMware。

Quest
quest.com
請前往網站 (quest.com) 以瞭解當地辦事處的資訊。

DataSheet-ChangeAuditor-US-KS-zh_TW-WL-40681