政府機構提高了安全性和生產力

Quest 的 Microsoft 平台管理解決方案，讓中北德州地方政府議會能即時控管混合式 IT 環境的變動。

「使用之前的解決方案時，如果一個資料夾不見了，要等到隔天我才能瞭解情況。現在有了 Change Auditor，我可以馬上知道資料夾有何異狀。如果有人不小心移動了資料夾，我們可以請他們移回原位，或乾脆爲他們迅速處理。」

中北德州地方政府議會
資訊安全長 Brett Ogletree

客戶簡介

North Central Texas Council of Governments

公司	中北德州地方政府議會
行業	政府機關
國家/地區	美國
員工數	400
網站	nctcog.org

業務需求

中北德州地方政府議會 (NCTCOG) 沒有能力稽核 AD 變更，而檔案系統稽核也只有在經過第三方解決方案於夜間處理後才能進行，這使他們即時回應稽核請求和事件的能力受到限制。

解決方案

NCTCOG 採用 AD、Windows 檔案伺服器和 EMC 適用的 Change Auditor 解決方案後，現在已擁有所需的全方位即時稽核能力。解決方案的警示功能有助於快速回應重要事件、依排程發送報告可供業主定期審視，而內建 IT Security Search 則可有效簡化調查工作。議會組織現在還針對 SharePoint 和 SQL 投資了 Change Auditor 模組，並購入了 Enterprise Reporter 和 Security Explorer。

優點

- 針對整個環境提供即時稽核、報告和警示
- 透過內建的跨系統搜尋功能有效簡化事件調查工作
- 同樣的價格，提供的功能遠多於之前的解決方案

解決方案簡介

- Microsoft 平台管理

政府機關若要有效率地運作，需要的技術並不少於中小企業或大企業，但 IT 人員的編制通常須維持精簡。以中北德州地方政府議會 (NCTCOG) 爲例，他們不僅極度依賴電子郵件和網路電話 (VoIP) 系統等技術基礎，也相當依賴地理資訊系統、文件管理系統和道路建模應用程式等專業系統。爲了自動變更監控、加速資安調查，NCTCOG 的 IT 安全團隊採用一套 Quest 的 Windows 管理解決方案。

> 「Change Auditor 不僅能提高安全性，也能提升業務產能，並爲我省下大量時間。這樣的功能很難以金錢價值衡量，因爲這是無價的。」
>
> *中北德州地方政府議會資訊安全長 Brett Ogletree*

無法即時掌控 AD 和檔案系統將使風險急劇上升

中北德州地方政府議會是由達拉斯和沃斯堡及其周邊地區的 16 個郡和許多城市、學區和特區所組成的自願協會，目的在於幫助會員規劃共同需求、分辨地區機會並刪減不必要的重複項目。例如，NCTCOG 的運輸部門與當地政府機構合作，負責安排道路工程的優先順序，並根據優先順序分配資金；勞動力部門提供訓練機會、讓大眾獲得托兒服務；其他部門合作則是爲了增進地區利益，形成類似合作夥伴的關係。

NCTCOG 的 IT 團隊深知，Active Directory (AD) 儲存了有關使用者、群組和權限的重要資訊，因此對於所有這類應用程式的安全性和可用性至關重要。只要群組權限有任何不當的變更，就可能會使群組的所有成員無法存取關鍵資源，導致重要的業務程序嚴重癱瘓。更糟的是，群組中的所有人員可能會看到不應該看見的敏感資料，使組織陷於安全漏洞和違反法規的兩大風險。

很不幸地，這正是 NCTCOG 數年前面臨的危機。中北德州地方政府議會資訊安全長 Brett Ogletree 解釋：「我們無法得知 Active Directory 有何異狀。如果某人刪除了帳戶或變更群組原則物件，我們無法判斷是由誰所爲，也無從得知是意外或故意爲之。我們只能夠希望員工坦率承認自己的所做所爲。」

這還只是問題的一小部分。IT 團隊必須能即時稽核檔案系統和 AD。舉例來說，如果一個重要檔案遭到修改或刪除，他們必須能夠快速判斷變更者是誰、瞭解該名人員已在網路上存取哪些其他資源。雖然 NCTCOG 的 IT 團隊對檔案伺服器的掌控度高於 AD，但仍不足以解決問題。

Ogletree 回憶：「一開始我們嘗試使用原生工具來判斷是誰在檔案系統中進行變更，但效果不彰；我們必須花很多工夫釐清狀況。因此我們購買了一套解決方案，通知我們是誰修改或刪除了檔案，並讓我們得知特定使用者或使用者群組在網路上存取過哪些內容。」

產品和服務

軟體
Change Auditor for Active Directory
Change Auditor for EMC
Change Auditor for SharePoint
Change Auditor for SQL Server
Change Auditor for Windows File Servers
Enterprise Reporter Suite
Security Explorer

但這類資訊都是舊資訊，可能有 24 小時之久，實際上沒有非常實用。Ogletree 補充：「那套工具沒有即時稽核檔案伺服器的功能，而是依照排程每天晚上抓取我們的檔案伺服器，查閱是否有重要資料，因此我們得到的資訊都是舊的。如果某天中午有人詢問某個資料夾怎麼不見了，我要等到第二天早上才能找到答案。生產力可能因此下降，檔案系統也會陷於安全險境。」

QUEST 的全方位即時稽核功能

NCTCOG 的 IT 團隊決定先解決 AD 稽核功能缺失的問題。他們仔細研究了幾個解決方案後，決定選擇 Quest® Change Auditor for Active Directory。這個解決方案能夠即時追蹤 AD 的所有變更，讓使用者輕鬆快速偵測潛在的內部攻擊，或是任何可能危及安全性或業務連續性的意外修改；而且操作起來絲毫沒有原生工具的複雜度或不便之處。IT 團隊只要按一下按鈕，就能復原未經授權或以其他方式進行的不當變更，甚至還能主動阻止他人變更最重要的 AD 物件，像是特定的組織單位 (OU) 或群組原則物件 (GPO)。

解決方案相當成功，於是 NCTCOG 決定針對檔案稽核功能深入瞭解相關應用程式：Change Auditor for Windows File Servers 和 Change Auditor for EMC。更明確地說，NCTCOG 需要像掌控 AD 一樣即時掌控檔案系統，這一點是目前的解決方案做不到的。由於他們已安裝了 Change Auditor for Active Directory 適用的基礎架構，因此額外部署兩個應用程式進行評估再簡單不過了；他們只要部署試用金鑰即可。

有了 Change Auditor for Windows File Servers 和 Change Auditor for EMC，IT 團隊現在可以即時追蹤、稽核、報告和警示所有檔案和資料夾的變更，以便及時回應資安威脅、可用性問題和使用者請求。此外，Change Auditor 還提供「對象、目的、時間、地點及原始工作站」等所有詳細資訊，並附上原始數值和最新數值，這些都是快速完成故障診斷的必要資訊。另外，Change Auditor 也可保護關鍵檔案和資料夾，以防遭到修改或意外刪除。

改用 Quest 解決方案後，除了體驗到上述功能優勢之外，還發掘了兩項優點。第一，Change Auditor 系列解決方案的整合

> 「Quest 提供的產品數量遠多於之前的解決方案，而我們每年仍負擔同樣的維護成本。」
>
> *中北德州地方政府議會資訊安全長*
> *Brett Ogletree*

> 「如果發生高嚴重性事件，Change Auditor 會透過電子郵件提醒我們，讓我們可以判斷該項變更是經由變更管理流程所做的適當變更，或是由駭客所爲的惡意行爲。」
>
> *中北德州地方政府議會資訊安全長 Brett Ogletree*

簡化了維護和營運工作。第二，Change Auditor 系列解決方案帶來的價值遠遠超過想像。Ogletree 認爲：「Quest 提供一切必要的工具，我們認爲非常物超所值。Quest 提供的產品數量遠多於之前的解決方案，而我們每年仍負擔同樣的維護成本。」

可快速因應威脅的即時警示

採用 Change Auditor 應用程式後，NCTCOG 的 IT 團隊現在可以立即發現重要變更，不必等到隔天。Ogletree 解釋：「如果發生高嚴重性事件，Change Auditor 會透過電子郵件提醒我們，讓我們可以判斷該項變更是經由變更管理流程所做的適當變更，或是由駭客所爲的惡意行爲。如果是特定的敏感群組，例如負責處理受保護醫療資訊的群組，只要其中有成員的身份發生變更，Change Auditor for Active Directory 就會發出警示。」

Change Auditor 也爲 NCTCOG 的檔案系統提供類似的即時警示。Ogletree 說：「如果有未經授權人員存取安全資料夾，我們有多位主管會希望收到警示，之前的解決方案無法做到這點。但現在我們只要設定這些警示，然後交由 Change Auditor 自動監控可疑活動就好了。」

有效簡化事件調查工作

Change Auditor 提供靈活完整的報告功能，幫助 NCTCOG 進一步瞭解可疑變更和其他使用者行爲。Ogletree 解釋：「我們可以輕鬆鑑識事件，回頭仔細查看系統究竟發生了哪些變動。使用之前的解決方案時，如果一個資料夾不見了，要等到隔天我才能瞭解情況。現在有了 Change Auditor，我可以馬上知道資料夾有何異狀。如果有人不小心移動了資料夾，我們可以請他們移回原位，或乾脆爲他們迅速處理。如果資料夾遭到刪除，過去的處理方式是向外部訂購磁帶，並等到磁帶送達後再進行還原程序。現在我們可以立即還原資料夾。」

Change Auditor 甚至還能產生報告，並自動傳送給利益關係人。依排程發送報告可讓每位業主定期審視資料和系統的變更，確保及時偵測到不當的變更。Ogletree 說：「我設定了一些報告，以便顯示檔案系統的特定區域發生了哪些變動，並每週向資料擁有者發送。總有一些檔案不是部門每天都會接觸到的。我們採用 Change Auditor 之前，如果有一天部門發現其中一些檔案已遭修改或遺失，就必須請我幫忙重現最後一次使用檔案後系統發生的狀況。採用 Change Auditor 之後，部門可以每週審視文件發生哪些變更，而不是在事後才發現問題。」

此外，所有 Change Auditor 應用程式和其他幾項 Quest Windows 管理解決方案都隨附強大的互動式搜尋引擎：IT Security Search，可將來自眾多系統和裝置、且種類各異的 IT 資料整合至單一主控台，加快資安事件回應和鑑識調查分析的速度。

擴大對整個企業的掌控度

即時深入瞭解 Active Directory 和檔案系統，讓 NCTCOG 在許多方面都獲得好處。Ogletree 表示：「Change Auditor 不僅能提高安全性，也能提升業務產能，並爲我省下大量時間。這樣的功能很難以金錢價值衡量，因爲這是無價的。NCTCOG 利用 Change Auditor 解決方案成功稽核 Active Directory、Windows 檔案伺服器和 EMC，這讓我們更有理由購買其他兩個 Change Auditor 應用程式的授權：Change Auditor for SQL Server 和 Change Auditor for SharePoint。

Ogletree 認爲：「我們非常高興能夠加強掌控 AD、EMC 和檔案伺服器，如果對 SharePoint 和 SQL Server 也有同樣的掌控能力，那就太棒了。例如，在 SQL Server

環境中監控資料庫架構的變更和其他修改項目，可協助系統正常運行並保障資料安全。」

NCTCOG 最近也採用了 Enterprise Reporter Suite，其中包含全方位存取評估與內建報告功能，有助於深入掌控 Microsoft 環境中的使用者、群組、權限和其他組態。Ogletree 說：「過去，除非逐一查看每個伺服器，否則我們很難回答『這十幾個 SQL 伺服器中，哪個伺服器具有資料庫擁有者 (DBO) 的角色？』等類似的問題。現在有了 Enterprise Reporter，這類問題輕而易舉就能獲得解答。」 此外，NCTCOG 還投資了 Enterprise Reporter Suite，現在已擁有 Security Explorer 的完整功能；Security Explorer 結合報告和補救功能，讓 IT 團隊能夠在單一主控台中管理 Microsoft 平台上的存取控制、權限和安全性。

準備好邁向雲端

隨著 NCTCOG 逐漸成長，並將 IT 環境擴展到雲端，他們也將從 Quest 解決方案中獲取更多價值。例如，Change Auditor for Active Directory 可以稽核 Azure Active Directory，因此能確實追蹤純雲物件和屬性的變更並發送警示。同樣地，Change Auditor for SharePoint 支援 SharePoint Online 和商務用 OneDrive；Enterprise Reporter 則支援 Azure Active Directory、Exchange Online 和商務用 OneDrive。

關於 QUEST

Quest 的宗旨是以簡單的解決方案解決複雜的問題。爲了達成此理念，我們堅持提供優異的產品和服務，並秉持簡單經營業務的整體目標。我們期望能爲您帶來兼顧效率與效益的技術，讓您和貴組織可以減少耗費在 IT 管理上的時間，進而投入更多時間發展業務創新。

> 「過去，除非逐一查看每個伺服器，否則我們很難回答『這十幾個 SQL 伺服器中，哪個伺服器具有資料庫擁有者 (DBO) 的角色？』等類似的問題。現在有了 Enterprise Reporter，這類問題輕而易舉就能獲得解答。」
>
> *中北德州地方政府議會資訊安全長*
> *Brett Ogletree*

前往 Quest.com/Customer-Stories 檢視更多個案研究

CaseStudy-NCTCOG-US-GM-zh_TW-WL-34291