Government agency improves security and productivity

North Central Texas Council of Governments gains real-time control over changes across its hybrid IT environment with Microsoft Platform Management solutions from Quest.

"With our previous solution, if a folder came up missing, it'd be the next day before I could report and say what happened to it. Now, with Change Auditor, I can immediately tell what happened to the folder. If someone accidentally moved it, we can direct them to move it back or just quickly do it for them."

Brett Ogletree, Information Security Officer, North Central Texas Council of Governments

CUSTOMER PROFILE

North Central Texas Council of Governments

Company	North Central Texas Council of Governments
Industry	Government
Country	United States
Employees	400
Website	**nctcog.org**

BUSINESS NEED

The North Central Texas Council of Governments had no ability to audit AD changes and file system auditing was available only after nightly processing by a third-party solution, which limited their ability to respond to audit requests and incidents in a timely manner.

SOLUTION

With Change Auditor solutions for AD, Windows file servers and EMC, NCTCOG now has the comprehensive real-time auditing they need. Alerts enable quick response to critical events, scheduled reports facilitate regular review by business owners and the integrated IT Security Search streamlines investigations. The organization has now also invested in Change Auditor modules for SharePoint and SQL, as well as Enterprise Reporter and Security Explorer.

BENEFITS

- Delivers real-time auditing, reporting and alerting across the environment
- Streamlines incident investigations with integrated cross-system search
- Delivers far more functionality for the same price as the previous solution

SOLUTIONS AT A GLANCE

- Microsoft Platform Management

To operate efficiently, government agencies require technology just as much as SMBs and large enterprises do, and they usually run just as lean when it comes to IT staffing. The North Central Texas Council of Governments (NCTCOG), for instance, relies heavily on not just technology basics like email and voice over IP (VoIP) systems, but also specialized systems such as geographic information systems, document management systems and roadway modeling applications. To automate change monitoring and speed security investigations, NCTCOG's IT security team relies on a suite of Windows management solutions from Quest.

> "Change Auditor not only improves security, it also makes the business more productive — and saves me a lot of time as well. It's hard to put a monetary value on that functionality; it's invaluable."
>
> *Brett Ogletree, Information Security Officer, North Central Texas Council of Governments*

RISK SKYROCKETS WHEN YOU LACK REAL-TIME INSIGHT INTO AD AND FILE SYSTEMS

The North Central Texas Council of Governments is a voluntary association of 16 counties and numerous cities, school districts and special districts in and around Dallas and Fort Worth. NCTCOG help its members plan for common needs, recognize regional opportunities and eliminate unnecessary duplication. For example, its Transportation department partners with local governmental entities to prioritize roadway projects and allocate funding according to those priorities; the Workforce department offers training opportunities and facilitates access to childcare services; and other departments engage is similar partnerships for regional benefit.

NCTCOG's IT teams are acutely aware that Active Directory (AD) is essential to both the security and availability of all these applications because it stores crucial information about users, groups and permissions. A single improper change to a group's permissions could leave all members of that group unable to access critical resources, crippling important business processes. Even worse, it could enable everyone in the group to access sensitive data they should never see, putting the organization at risk of both security breaches and compliance failures.

Unfortunately, that was exactly the situation facing the organization a few years ago. "We had no way of knowing what was happening in our Active Directory," explains Brett Ogletree, information security officer at North Central Texas Council of Governments. "For instance, if someone deleted an account or changed a Group Policy object, we didn't have any way to determine who was responsible and whether it was accidental or deliberate. We simply had to hope that people would be honest with us about what they had done."

And that was just part of the problem. IT teams need real-time auditing of their file systems as well as AD. If an important file is modified or deleted, for instance, they need to be able to quickly determine who made the change — and what other resources on the network they had access to. While the IT team at NCTCOG had more visibility into its file servers than they did into AD, it was not nearly enough.

PRODUCTS & SERVICES

SOFTWARE

- 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

"Initially, we tried using native tools to determine who was making changes on the file system, and it was just unwieldy; we had to do a lot of work to try to ascertain what happened," recalls Ogletree. "So we purchased a solution that could tell us who modified or deleted a file, as well as what a particular user or group of users had access to on the network."

However, that information was up to 24 hours old, which limited its usefulness. "The tool did not provide us with real-time file server auditing; rather, it would crawl through our file servers each night on schedule, interrogating them for important data, so our information was always out of date," Ogletree adds. "For example, if a request came in at noon one day asking what happened to a missing folder, I was not able to answer that question until the following morning. That could result in productivity losses and also put file system security at risk."

COMPREHENSIVE REAL-TIME AUDITING FROM QUEST

The IT team at NCTCOG decided to tackle the lack of AD auditing first. After carefully reviewing several solutions, they chose Quest® Change Auditor for Active Directory. The solution tracks all changes to AD in real time, enabling users to quickly and easily detect potential insider attacks as well as accidental modifications that could threaten security or business continuity, all without the complexity and headache of native tools. IT teams can roll back unauthorized or otherwise improper changes with the click of a button, and even proactively prevent changes to their most important AD objects, such as specific organizational units (OUs) or Group Policy objects (GPOs).

The solution was such a success that NCTCOG decided to look into its sister applications for file auditing: Change Auditor for Windows File Servers and Change Auditor for EMC. In particular, the organization needed to get the same real-time insight into its file systems that it was now getting for AD — something their current solution simply could not deliver. Since they already had the infrastructure for Change Auditor for Active Directory installed, deploying the two additional applications for evaluation could not have been easier; all they had to do was deploy a trial key.

With Change Auditor for Windows File Servers and Change Auditor for EMC, the IT team now has real-time tracking, auditing, reporting and alerting on all changes to their files and folders, so they can respond promptly to security threats, availability issues and requests from users. Moreover, Change Auditor delivers all the "who, what, when, where and originating workstation" details, along with the original and current values, which are essential for fast troubleshooting. Plus, it can protect critical files and folders from

> "We're getting a multitude of products from Quest for the same annual maintenance cost we were paying for our previous solution."
>
> *Brett Ogletree, Information Security Officer, North Central Texas Council of Governments*

> "If high-severity events occur, Change Auditor alerts us by email, so we can can determine whether the change was made properly through our change management process or is a malicious act by a hacker."
>
> *Brett Ogletree, Information Security Officer, North Central Texas Council of Governments*

being modified or accidentally deleted in the first place.

In addition to the functionality advantages, switching to Quest solutions offered two additional benefits. First, consolidating on the Change Auditor family of solutions simplified maintenance and operations. Second, it delivered far more value. "By packaging everything we needed from Quest, we got more bang for our buck," Ogletree says. "We're getting a multitude of products from Quest for the same annual maintenance cost we were paying for our previous solution."

REAL-TIME ALERTS ENABLE QUICK RESPONSE TO THREATS

With the Change Auditor applications in place, the IT team at NCTCOG now knows about critical changes immediately, instead of up to a day later. "If high-severity events occur, Change Auditor alerts us by email, so we can determine whether the change was made properly through our change management process or is a malicious act by a hacker," explains Ogletree. "For example, we use Change Auditor for Active Directory to alert on changes to the membership of specific sensitive groups, such as groups that handle protected healthcare information."

Change Auditor provides similar real-time alerting for NCTCOG's file systems. "We've got managers who want to be alerted if their secure folders are accessed by an unauthorized person," Ogletree says. "The previous solution couldn't do that. But now we can simply set up those alerts and then sit back and let Change Auditor automatically monitor for the suspicious activity."

STREAMLINING INCIDENT INVESTIGATION

NCTCOG gets further insight into suspicious changes and other user behavior with Change Auditor's flexible, comprehensive reporting. "We can easily do forensics on incidents — go back and see exactly what happened on the system," Ogletree explains. "For example, with our previous solution, if a folder came up missing, it'd be the next day before I could say what happened to it. Now, with Change Auditor, I can immediately tell what happened to the folder. If someone accidentally moved it, we can direct them to move it back or just quickly do it for them. If the folder was deleted, in the past, we would have to order tapes from off site, wait until they were delivered and then go through the restoration process. Now we can restore the folder immediately."

Reports can even be generated and delivered automatically to stakeholders. This scheduled reporting facilitates regular review of changes to data and systems by the respective business owners, which helps ensure that errant changes are detected promptly. "I've set up some reports that show what changes are made to a specific area of the file system, and they are delivered to the data owner on a weekly basis," says Ogletree. "For example, a certain department might have a set of files that they don't touch every day. Before we had Change Auditor, they might have discovered one day that several of those files had been modified or had gone missing, and then they would have to come to me to help them recreate what happened on the system since they last used the files. With Change Auditor, they can review what's happening with their files on a weekly basis, instead of stumbling upon problems later."

Plus, all the Change Auditor applications, as well as several other Quest Windows management solutions, come with a powerful interactive search engine: IT Security Search correlates disparate IT data from numerous systems and devices into a single console to speed security incident response and forensic analysis.

EXPANDING VISIBILITY ACROSS THE ENTERPRISE

Having real-time insight into Active Directory and file systems benefits NCTCOG in multiple ways. "Change Auditor not only improves security, it also makes the business more productive — and saves me a lot of time as well," notes Ogletree. "It's hard to put a monetary value on that functionality; it's invaluable." NCTCOG's success with the Change Auditor solutions for auditing Active Directory, Windows file servers and EMC provided justification for adding two additional Change Auditor applications to their licensing: Change Auditor for SQL Server and Change Auditor for SharePoint.

"We appreciate the increased visibility we have into our AD, EMC and file servers, and we knew it would be great to have the same visibility into SharePoint and SQL Server," Ogletree says. "For example, monitoring database schema changes and other modifications within our SQL Server environment will help us keep those systems up and running, and the data in them secure."

The organization recently adopted Enterprise Reporter Suite as well. Its comprehensive access assessments and built-in reporting provide deep visibility into users, groups, permissions and other configurations across the Microsoft environment. "Before, it was hard to answer questions like, 'who has a database owner (DBO) role on any of the dozen or so SQL servers we have?' We would have had to look at each server individually," notes Ogletree. "With Enterprise Reporter, we'll be able to answer questions like that easily." Plus, with their investment in the Enterprise Reporter Suite, NCTCOG now has the full functionality of Security Explorer, which offers a combination of reporting and remediation capabilities that enable IT teams to manage access controls, permissions and security across their Microsoft platforms from a single console.

READY FOR THE CLOUD

As NCTCOG grows and expands its IT environment to the cloud, it will get even more value from its Quest solutions. For example, Change Auditor for Active Directory audits Azure Active Directory — ensuring that changes to cloud-only objects and attributes are tracked and alerted on. Similarly, Change Auditor for SharePoint supports SharePoint Online and OneDrive for Business, and Enterprise Reporter covers Azure Active Directory, Exchange Online and OneDrive for Business.

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

"Before, it was hard to answer questions like, 'who has a database owner (DBO) role on any of the dozen or so SQL servers we have?' We would have had to look at each server individually. With Enterprise Reporter, we'll be able to answer questions like that easily."

Brett Ogletree, Information Security Officer, North Central Texas Council of Governments

View more case studies at Quest.com/Customer-Stories

CaseStudy-NCTCOG-US-GM-34291