政府机构提高安全性和工作效率

依托Quest的Microsoft平台管理解决方案，德州中北部政府理事会可以实时控制其整个混合IT环境中的变更。

“使用之前的解决方案时，如果一个文件夹失踪，我可能要到第二天才能报告并明白是怎么回事。现在，凭借Change Auditor，我可以立即了解该文件夹发生了什么。如果是有人不小心移动了文件夹，我们可以指导他们再将它移回来，或者直接代他们移回来。”

Brett Ogletree,
德州中北部政府理事会信息安全专员

客户概况

North Central Texas Council of Governments

公司	德州中北部政府理事会 (North Central Texas Council of Governments)
行业	政府
国家/地区	美国
员工数	400
网站	nctcog.org

业务需求

德州中北部政府理事会(North Central Texas Council of Governments)没有能力审核AD变更，文件系统审核也只能在夜间经过第三方解决方案处理后进行，这无疑限制了他们及时响应审核请求和事件的能力。

解决方案

依托适用于AD、Windows文件服务器和EMC的Change Auditor解决方案，NCTCOG现在拥有所需的进行全面、实时审核的能力。提醒便于快速响应关键事件，计划的报告便于业务所有者定期审查，而集成的IT Security Search简化了调查过程。该组织现已投资购买用于SharePoint和SQL的Change Auditor模块，以及Enterprise Reporter和Security Explorer。

优势

- 在整个环境提供实时审核、报告和提醒
- 利用集成式跨系统搜索功能简化事件调查过程
- 以与之前解决方案相同的价格提供更多的功能

解决方案一览

- Microsoft平台管理

为了有效运作，同中小型企业和大型企业一样，政府机构也需要相应的技术，但他们在IT人员配置方面往往很精简。举例来说，德州中北部政府理事会(NCTCOG)不仅特别依赖电子邮件和IP语音(VoIP)系统等基础技术，还依赖诸如地理信息系统、文档管理系统和道路建模应用程序等专用系统。为自动化变更监控和加快安全调查速度，NCTCOG的IT安全团队依赖Quest提供的一套Windows管理解决方案。

> “Change Auditor不仅提升了安全性，还提高了企业的生产效率，同时帮助我节省了大量时间。这项功能很难用金钱来衡量；它堪称无价之宝。”
>
> *Brett Ogletree，德州中北部政府理事会信息安全专员*

当您缺乏对AD和文件系统的实时洞察力，风险将会急剧增加

德州中北部政府理事会是由达拉斯和沃斯堡市内及其周边16个县和众多城市、学区和特殊区域自发组织的协会。NCTCOG帮助其成员针对共同需求制定相应的计划，识别区域机遇，以及消除不必要的重复项目。例如，运输部门与当地政府实体合作，优先实施道路项目并根据这些优先项目分配资金；劳动力部门提供培训机会，推进儿童保育服务；其他部门也建立有类似的合作伙伴关系，共同为地区谋福利。

NCTCOG的IT团队深刻意识到，Active Directory (AD)对于所有这些应用程序的安全性和可用性至关重要，因为它存储着用户、组和权限相关重要信息。对组权限的一个不当变更就有可能导致该组的所有成员都无法访问关键资源，致使重要业务流程陷入瘫痪。更糟糕的是，它可能使组中的每个成员都可以访问他们绝不应查看的敏感数据，使组织面临安全漏洞和违规双重风险。

很不幸的是，几年前该组织就曾有此遭遇。“我们对Active Directory发生了什么一无所知，”德州中北部政府理事会信息安全专员 Brett Ogletree解释说，“例如，如果有人删除了一个帐户或更改了组策略对象，我们没有任何办法来确定谁是负责人，是意外发生还是有人故意为之。我们只能寄望于人们诚实地告诉我们他们做了什么。”

然而，这还只是问题的一部分。IT团队需要实时审核他们的文件系统和AD。举例来说，如果有重要文件被修改或被删除，他们需要能够快速确定是谁进行了更改，以及这些人有权访问网络上的哪些其他资源。NCTCOG的IT团队拥有的文件服务器可见性比AD可见性高，但这远远不够。

“最初，我们尝试使用本地工具来确定谁正在对文件系统进行更改，但此方法很笨拙；我们不得不做大量工作试图弄清是怎么回事，”Ogletree回忆说，“因此，我们购买了一个可以告诉我们是谁修改或删除了文件，以及特定用户或用户组可以访问网络上哪些内容的解决方案。”

不过，这些信息最长只能保留24小时，大大限制了其实用性。“此工具并不能为

产品及服务

软件
Change Auditor for Active Directory
Change Auditor for EMC
Change Auditor for SharePoint
Change Auditor for SQL Server
Change Auditor for Windows 文件服务器
Enterprise Reporter Suite
Security Explorer

我们提供文件服务器实时审核能力，而是每天晚上按计划抓取我们的文件服务器，向它们查询重要数据，因此我们的信息总是过时的，”Ogletree补充道，“例如，如果某天中午传入一个请求，询问有个文件夹丢失是怎么回事，我要等到第二天早上才能回答这个问题。这导致工作效率降低，同时使文件系统面临安全风险。”

QUEST提供全面实时的审核

NCTCOG的IT团队决定首先解决AD审核能力缺乏的问题。在仔细研究多款解决方案后，他们最终选择了Quest® Change Auditor for Active Directory。此解决方案可以实时跟踪对AD所做的所有更改，让用户可以轻松快速地检测到潜在的内部攻击，以及可能威胁安全性或业务连续性的意外修改，这一切都不需要复杂而又麻烦的本地工具。IT团队只需点击一下按钮即可回滚未经授权或其他不当的更改，甚至可以主动阻止对诸如特定组织单位(OU)或组策略对象(GPO)等重要AD对象进行更改。

此解决方案如此成功，NCTCOG决定了解一下其用于文件审核的姊妹应用程序：Change Auditor for Windows File Servers和Change Auditor for EMC。特别是，该组织需要获得与AD相同的文件系统实时洞察力，这是他们当前的解决方案无法提供的。由于他们已经安装了用于Change Auditor for Active Directory的基础架构，因此部署这两个待评估的应用程序是再容易不过了；他们只需部署一个试用密钥即可。

凭借Change Auditor for Windows File Servers和Change Auditor for EMC，IT团队现在拥有对文件和文件夹所有更改的实时跟踪、审核、报告和提醒，从而能够迅速响应安全威胁、可用性问题以及用户请求。此外，Change Auditor可以提供“执行更改的人员、更改内容、时间、地点和来源工作站”等所有详细信息，以及原始值和当前值，这些信息对于快速排除故障至关重要。而且，它可以从一开始就保护关键文件和文件夹免遭修改或意外删除。

除了功能优势外，改用Quest解决方案还有两个益处。第一，通过整合Change Auditor系列解决方案，简化维护和操作。第二，它提供更高价值。“通过将所需的所有Quest解决方案打包在一起，我们获得了更高的投资回报，”Ogletree说道，“我们以与之前解决方案相同的年度维护成本，从Quest获得许多产品。”

> “我们以与之前解决方案相同的年度维护成本，从Quest获得许多产品。”
>
> *Brett Ogletree，德州中北部政府理事会信息安全专员*

Quest

> “如果发生特别严重的事件，Change Auditor会通过电子邮件提醒我们，因此我们可以判断此变更是通过我们的变更管理流程适当进行的，还是黑客的恶意行为。”
>
> *Brett Ogletree，德州中北部政府理事会信息安全专员*

实时提醒便于快速响应威胁

安装Change Auditor应用程序后，NCTCOG的IT团队现在可以立即知道重要变更，再也不用等到一天后了。“如果发生特别严重的事件，Change Auditor会通过电子邮件提醒我们，因此我们可以判断此变更是通过我们的变更管理流程适当进行的，还是黑客的恶意行为，”Ogletree解释说，“例如，我们使用Change Auditor for Active Directory提醒对特定敏感组的成员资格所做的变更，比如负责处理受保护医疗信息的组。 ”

Change Auditor为NCTCOG的文件系统提供类似的实时提醒。“我们有些经理希望在有未经授权的人员访问他们的安全文件夹时收到提醒，”Ogletree说道，“以前的解决方案做不到这一点。然而，我们现在只需轻松设置这些提醒，无需进行其他工作，Change Auditor会自动监控可疑活动。”

简化事件调查

依托Change Auditor灵活、全面的报告功能，NCTCOG可以更加深入地洞察可疑变更及其他用户行为。“我们可以轻松地进行事件取证，回来就可以明白系统到底发生了什么，”Ogletree解释道，“例如，使用之前的解决方案时，如果一个文件夹失踪，我可能要到第二天才能明白是怎么回事。现在，凭借Change Auditor，我可以立即了解该文件夹发生了什么。如果是有人不小心移动了文件夹，我们可以指导他们再将它移回来，或者直接代他们移回来。如果文件夹被删除，在过去，我们必须要异地订购磁带，等待交货，然后再完成恢复过程。而现在我们可以立即恢复文件夹。”

甚至可以自动生成报告并自动将报告传送给利益相关方。这个计划报告功能方便相应的业务所有者定期审核对数据和系统所做的变更，从而帮助确保及时检测到不当变更。“我已经设置一些报告，这些报告会显示对文件系统特定区域做了哪些变更，并且每周会发送一次报告给数据所有者，”Ogletree说道，“例如，某个部门每天会收到一系列他们未接触的文件。有一天他们发现其中多个文件已被修改或缺失。在我们使用Change Auditor之前，发生此情况时，他们就必须来找我帮助他们重新创建自他们最后一次使用文件以来系统上发生变化的内容。现在，凭借Change Auditor，他们可以每周查看一次文件发生的变化，而不是在以后无意中发现。”

此外，所有Change Auditor应用程序以及很多其他Quest Windows管理解决方案都带有强大的交互式搜索引擎：IT Security Search将来自很多系统和设备的完全不同的IT数据关联到一个控制台中，从而加快了安全事件响应和取证分析速度。

将可见性扩展到整个企业

实时洞察Active Directory和文件系统的能力让NCTCOG在多个方面获益匪浅。“Change Auditor不仅提升了安全性，还提高了企业的生产效率，同时帮助我节省了大量时间，”Ogletree表示，“这项功能很难用金钱来衡量；它堪称无价之宝。“在使用Change Auditor解决方案对Active Directory、Windows文件服务器和EMC进行审核方面，NCTCOG非常成功。这让他们有充分的理由向其许可中添加另外两个Change Auditor应用程序：Change Auditor for SQL Server和Change Auditor for SharePoint。

“我们可以拥有对AD、EMC和文件服务器的更高可见性，对此我们深为感激，而且我们知道，对SharePoint和SQL Server也具有相同的可见性，那真是太棒了，”Ogletree说道，“例如，通过监控数据库架构变更以及SQL Server环境中的其他修改，可以帮助我们使这些系统保持正常运行，并保护这些系统中数据的安全。”

该组织最近还采用了Enterprise Reporter Suite。其全面的访问评估和内置的报告功能可以提供对整个Microsoft环境中用户、组、权限及其他配置的深度可见性。“以前，很难回答‘在我们十几个SQL服务器的任一服务器上，谁拥有数据库所有者(DBO)角色？’此类问题，因此我们不得不逐一查看每一个服务器，”Ogletree表示，“然而，凭借Enterprise Reporter，我们将能够轻松回答此类问题。”此外，通过投资购买Enterprise Reporter Suite，NCTCOG现在拥有Security Explorer的全部功能，Security Explorer兼具报告和修正功能，让IT团队能够从单个控制台管理其所有Microsoft平台的访问控制、权限和安全性。

可用于云

随着NCTCOG发展并将其IT环境扩展到云，它将从Quest解决方案获得更高价值。例如，Change Auditor for Active Directory审核Azure Active Directory —确保跟踪对仅位于云中的对象和属性所做的变更并发出相关提醒。同样，Change Auditor for SharePoint支持SharePoint Online和OneDrive for Business，Enterprise Reporter涵盖Azure Active Directory、Exchange Online和OneDrive for Business。

关于QUEST

Quest的宗旨是通过简单的解决方案解决复杂的问题。为实现此宗旨，我们秉持注重卓越产品和优质服务的理念，并且追求易于合作这一总体目标。我们的愿景是提供技术来避免在效率与有效性之间做出取舍，从而使您和您的企业可以减少用于IT管理的时间，并将更多时间用于业务创新。

> “以前，很难回答‘在我们十几个SQL服务器的任一服务器上，谁拥有数据库所有者(DBO)角色？’此类问题，因此我们不得不逐一查看每一个服务器。然而，凭借Enterprise Reporter，我们将能够轻松回答此类问题。”
>
> *Brett Ogletree，德州中北部政府理事会信息安全专员*

若需查看更多案例研究，请访问Quest.com/Customer-Stories

CaseStudy-NCTCOG-US-GM-zh_CN-WL-34291