THE CHALLENGE
Microsoft® Active Directory® is at the heart of your mission-critical network infrastructure. Issues with your directory can result in unplanned and costly service disruptions and business-crippling network downtime, as well as harmful security breaches and non-compliance with critical government regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI) and the Health Insurance Portability and Accountability Act (HIPAA). Organizations need to be notified — in real time — of critical changes to Active Directory.

THE SOLUTION
Quest’s award-winning Change Auditor software drives the security and control of Active Directory by tracking all key Active Directory configuration changes in real time. From Group Policy Objects (GPO) and schema changes to critical nested group and operational changes, Change Auditor tracks, audits, reports and alerts on the changes that impact your directory — without the overhead of turning on native auditing. With Change Auditor for Active Directory, you’ll get the who, what, when, where and workstation of changes and any related event details with before and after values. You can also add comments explaining why a specific change was made in order to fulfill your audit requirements.

AUDIT ALL CRITICAL CHANGES
Change Auditor provides extensive, customizable auditing and reporting for all critical Active Directory and file system changes, including GPO, Domain Name System (DNS), server configurations and nested groups. You’ll get complete visibility into all changes with in-depth forensics on the relation of

BENEFITS:
• Installs in minutes with fast event collection for immediate analysis into Windows environments
• Enables enterprise-wide auditing and compliance from a single client
• Eliminates unknown security concerns, ensuring continuous access to applications, systems and users by tracking all events and those changes related to specific incidents
• Reduces security risks in seconds with real-time alerts to any device for immediate response, in or out of the office
• Strengthens internal controls with protection from unwanted changes and limits control of authorized users
• Drives availability by enabling proactive troubleshooting for account lockouts
• Reduces the performance drag on servers and saves storage resources by collecting events without the use of native auditing
• Streamlines compliance to corporate and government policies and regulations, including SOX, PCI DSS, HIPAA, FISMA, SAS 70 and more
• Turns information into intelligent, in-depth forensics for auditors and management

With Change Auditor for Active Directory, you’ll get the who, what, when, where and workstation of all changes in chronological order.
“Overall, Change Auditor has been very useful. No other product we evaluated offered the same level of real-time auditing and protection, without requiring Windows auditing be enabled for all Active Directory changes.”

Patrick Rohe
Senior IT Architect
Towson University

SYSTEM REQUIREMENTS
For a detailed and current list of system requirements, please visit quest.com/products/change-auditor-for-active-directory.

Related searches gives you security in context with details on specific users and all the changes they’ve made.

© 2016 Quest Software, Inc. ALL RIGHTS RESERVED. Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademarks.aspx. All other trademarks and registered trademarks are property of their respective owners.

DATE:Sheet-Change-Auditor4AD-US-KS-24824