Quest

Change Auditor

Change Auditor

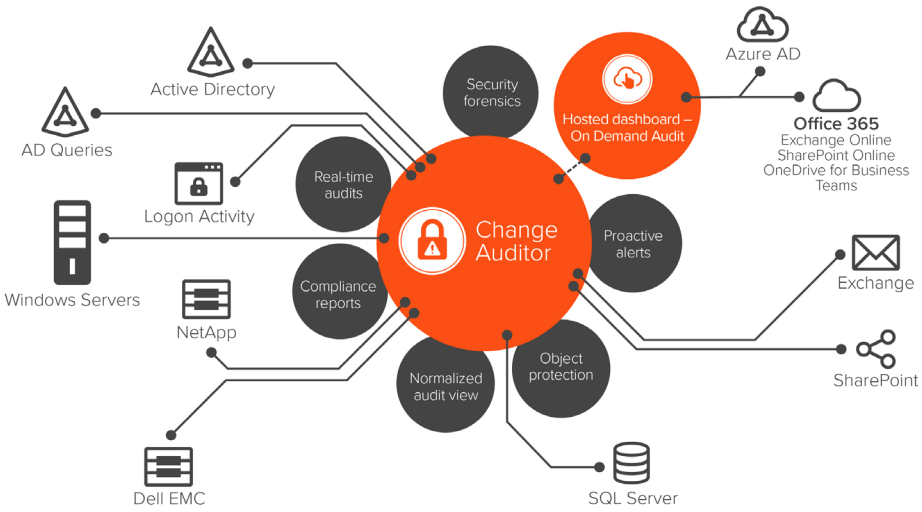
Real-time security auditing for your hybrid Microsoft environment

Event logging and change reporting for applications and services in the enterprise are cumbersome, time-consuming and, in some cases, impossible using native auditing tools. Because there's no central console, you've got to repeat the process for each server, and you end up with a huge volume of data with no context and a myriad of reports.

That means proving compliance or reacting quickly to threats is a constant challenge. Your data security is also at risk because native event details are sparse and difficult to interpret. As a result, you may not find out about problems until it is too late. And because native tools cannot prevent a privileged user from clearing an event log, you could lose log data — defeating the purpose of auditing in the first place.

Fortunately, there's Quest® Change Auditor. This product family enables you to audit, alert and report on all changes made to Active Directory (AD), Azure AD, Exchange, Office 365, SharePoint, EMC, NetApp, SQL Server and Windows file servers, as well as LDAP queries against AD — all in real time and without enabling native auditing.

With Change Auditor, you get complete, real-time IT auditing, in-depth forensics and security threat monitoring on all key configuration, user and administrator changes for Microsoft Active Directory, Azure AD, Exchange, Office 365, file servers and more. Change Auditor also tracks detailed user activity for logons, authentications and other key services across enterprises to enhance threat detection and security monitoring.



With Change Auditor, you'll get the who, what, when, where and originating workstation of all changes, in chronological order, including correlated on-premises and cloud identities.

> "We've had pen testers come in and be very surprised that they could not get past the Change Auditor object protection."
>
> *Enterprise Administrator, Large Retail Chain*

BENEFITS:

- Eliminate unknown security concerns, ensuring continuous access to applications, systems and users by tracking all events and those changes related to specific incidents.
- Alleviate stress and complexity by automatically interpreting cryptic data and its severity for faster and better decision-making.
- Mitigate security risks in seconds with real-time alerts to any device for immediate response, in or out of the office.
- Reduce the performance drag on servers by collecting events without the use of native auditing.
- Streamline compliance reporting, isolated for internal policies and external regulations, including GDPR, PCI DSS, HIPAA, FISMA/NIST and more.
- Provide managers and auditors evidence of appropriate IT controls for peace of mind.

"Previously, investigating an issue could easily take an hour. Change Auditor cuts that time to just 5–10 minutes."

Dennis Persson, IT Systems Technician, Region Halland

PRODUCTS
Change Auditor for Active Directory
Change Auditor for Active Directory Queries
Change Auditor for EMC
Change Auditor for Exchange
Change Auditor for Logon Activity
Change Auditor for NetApp
Change Auditor for SQL Server
Change Auditor for SharePoint
Change Auditor for Windows File Servers

You can easily install, deploy and manage your environment from one central console. Tracking creates, deletes, modifications and access attempts could not be any easier, and understanding what happened is a breeze because each event and all related events are displayed in simple terms, giving you the requisite five Ws — who, what, when, where and originating workstation, plus the previous and current settings.

This breadth of data analysis enables you to take immediate action when issues arise, such as what other changes came from specific users and workstations, eliminating additional guesswork and unknown security concerns. Whether you are trying to meet mounting compliance demands or satisfy internal security policies, Change Auditor is the solution you can rely on.

FEATURES

Hybrid environment auditing with a correlated view — Unlike native auditing, Change Auditor offers a single, correlated view of activity across hybrid environments, ensuring visibility to all changes taking place — whether on premises or in the cloud.

Security threat monitoring — Audit and block exploits such as credential theft and AD database copies, and identify applications using authentications over insecure protocols.

Golden Ticket detection — Detect and alert on common Kerberos authentication vulnerabilities used during Golden Ticket / Pass-the-ticket attacks.

Change prevention — Protect against changes to critical data within AD, Exchange and Windows file servers, including privileged groups, Group Policy objects and sensitive mailboxes.

Auditor-ready reporting — Generate comprehensive reports for best practices and regulatory compliance mandates for GDPR, PCI DSS, HIPAA, SOX, FISMA/NIST, GLBA and more.

High-performance auditing engine — Remove auditing limitations and capture change information without the need for native audit logs, resulting in faster results and significant savings of storage resources.*

Account lockout — Capture the originating IP address and workstation name for account lockout events, and view related logon and access attempts in an interactive timeline. This helps simplify detection and investigation of internal and external security threats.

Real-time alerts on the move — Send critical change and pattern alerts to email and mobile devices to prompt immediate action, enabling you to respond faster to threats even while you're not on site.

Integrated event forwarding — Easily integrate with SIEM solutions to forward Change Auditor events to Splunk, ArcSight, QRadar or any platform supporting Syslog. Additionally, Change Auditor integrates with Quest® InTrust® for 20:1 compressed event storage and centralized native or third-party log collection, parsing and analysis.

Hosted dashboard with On Demand Audit — View hybrid AD and Office 365 activity together from a hosted SaaS dashboard with responsive search, interactive data visualization and long-term event storage.

ABOUT QUEST

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

* Does not apply to SharePoint, EMC, and NetApp.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

DataSheet-ChangeAuditorFamily-US-JY-74387