Change Auditor

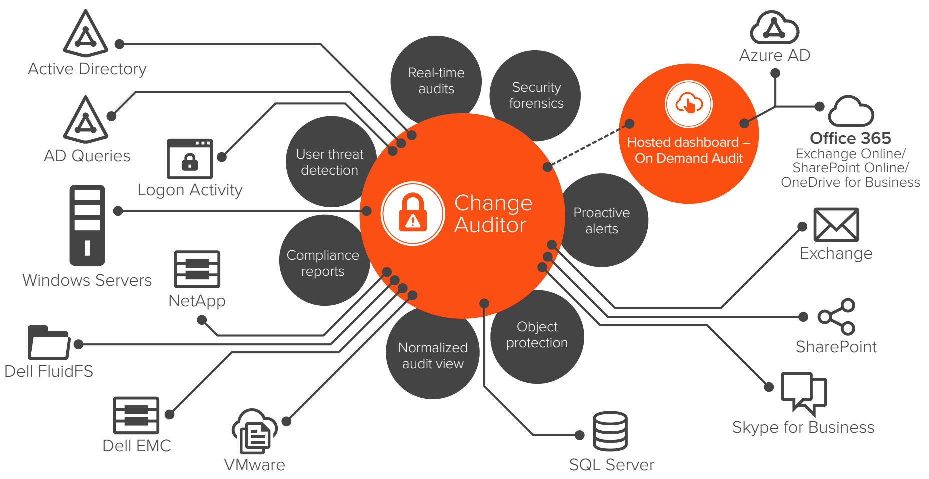
Real-time change auditing for your Microsoft platform environment

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 events 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, Skype for Business, VMware, EMC, NetApp, SQL Server and Windows file servers, as well as LDAP queries against AD — all in real time and without enabling native auditing.

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.



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.

> "Change Auditor was by far the best solution in terms of both functionality and cost. We were seduced by the simplicity and usability of the tool, which allowed us to create queries without any particular technical expertise."
>
> *Stephane Malagnoux,*
> *Head of the Computer*
> *Department BPCE Insurance*

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 SOX, PCI DSS, HIPAA, FISMA, SAS 70 and more.
- Provide managers and auditors evidence of appropriate IT controls for peace of mind.

> “Change Auditor has been a very intuitive, but very powerful, tool allowing me to have an understanding of the changes that staff are making. This has allowed me to enforce policies, restrict access and receive alerts concerning breaches.”
>
> *Senior IT Architect, Medium Enterprise Professional Services Company*
>
> Source: TechValidate. TVID: B4A-A84-619

PRODUCTS

- Change Auditor Threat Detection
- Change Auditor for Active Directory
- Change Auditor for Active Directory Queries
- Change Auditor for EMC
- Change Auditor for Exchange
- Change Auditor for FluidFS
- Change Auditor for Logon Activity
- Change Auditor for NetApp
- Change Auditor for SQL Server
- Change Auditor for SharePoint
- Change Auditor for Skype for Business
- Change Auditor for VMware vCenter
- Change Auditor for Windows File Servers

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 — Audit hybrid environments, including AD/Azure AD, Exchange/Exchange Online, SharePoint/SharePoint Online/OneDrive for Business as well as AD logons and Azure AD sign-ins. 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.

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 SOX, PCI DSS, HIPAA, FISMA, GLBA, GDPR and more.

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.

Proactive threat detection with Change Auditor Threat Detection — Simplify user threat detection by analyzing anomalous activity to rank the highest risk users in your organization, identify potential threats and reduce the noise from false positive alerts.

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 or QRadar. Additionally, Change Auditor integrates with Quest® InTrust® for 20:1 compressed event storage and centralized native or third-party log collection, parsing and analysis with alerting and automated response actions to suspicious events.

ABOUT QUEST

Quest provides software solutions for the rapidly changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid data centers, security threats and regulatory requirements. Our portfolio includes solutions for database management, data protection, unified endpoint management, identity and access management and Microsoft platform management.

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

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.