Change Auditor

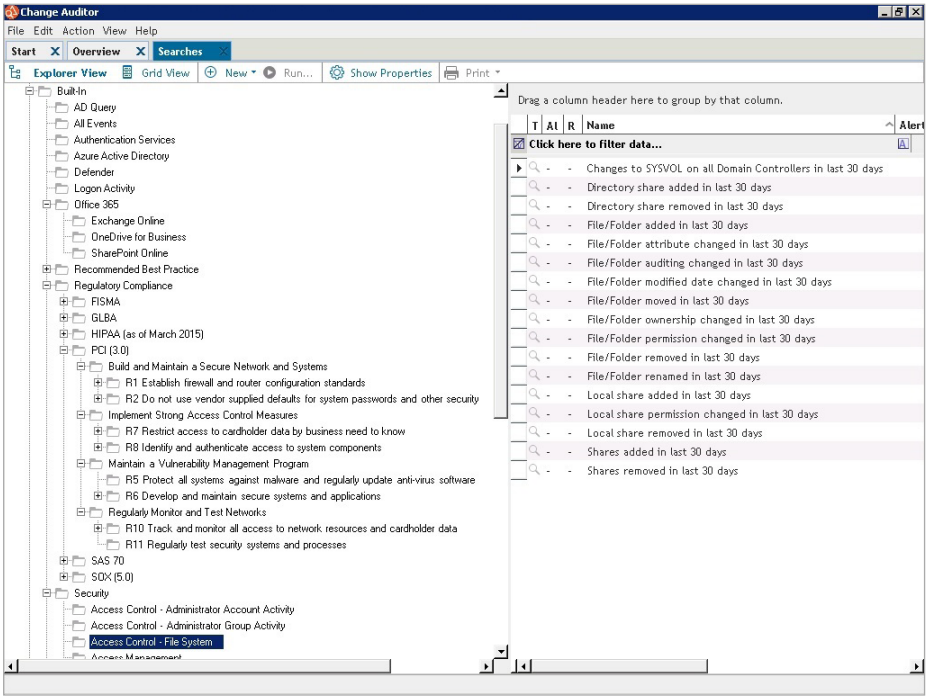
Real-time change auditing for your Microsoft platform environment

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 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

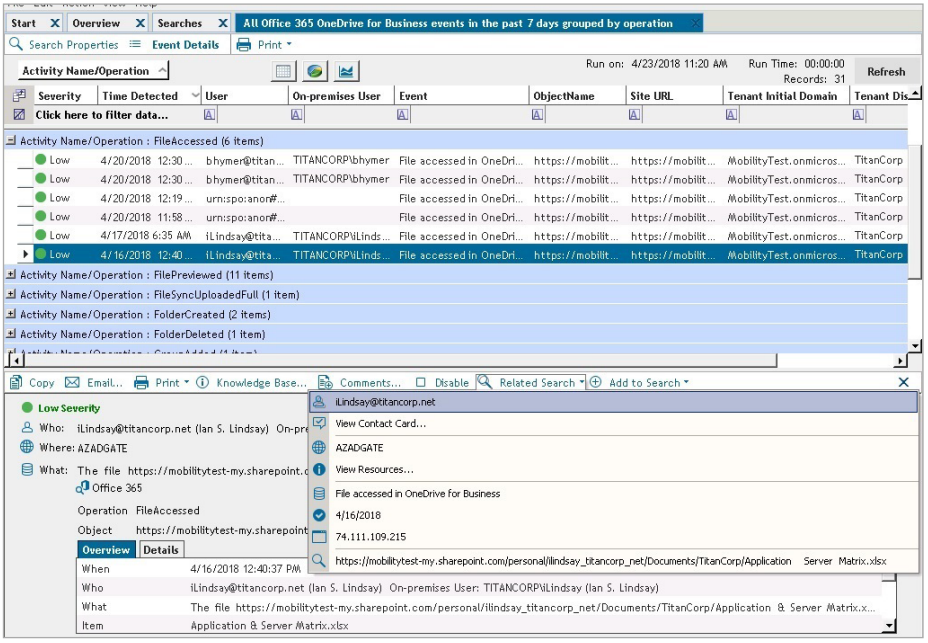


Get more than 700 out-of-the-box compliance and best-practice reporting events with real-time alerts into who, what, when, where and workstation of all changes.

> "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.



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

> "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

displayed in simple terms, giving you the requisite six Ws — who, what, when, where, workstation and why, 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 — 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.

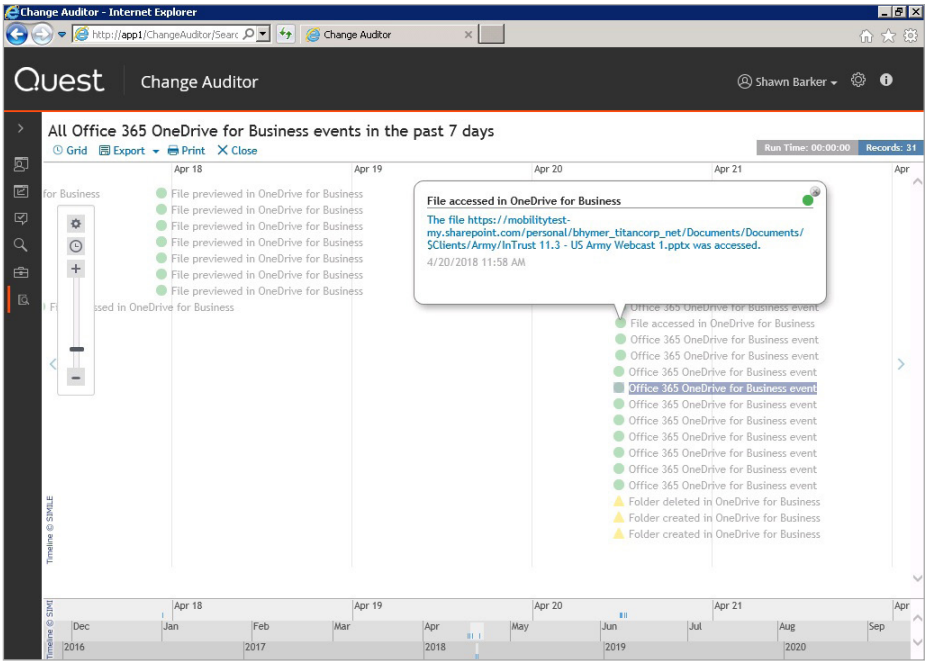
Auditor-ready reporting — Generate comprehensive reports for best practices and regulatory compliance mandates for SOX, PCI DSS, HIPAA, FISMA, GLBA, GDPR and more.

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.*

Improved insights with IT Security Search — Correlate disparate IT data from numerous systems and devices into an interactive search engine for fast security incident response and forensic analysis. Include user entitlements and activity, event trends, suspicious patterns and more with rich visualizations and event timelines.

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.

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



View, report and analyze audit activity in an event timeline from a web-based console.

SYSTEM REQUIREMENTS

For a full list of detailed requirements, please review the Release Notes Guide.

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.

Security timelines — View, highlight and filter change events and discover their relation to other security events in chronological order across your AD and Microsoft platforms for better forensic analysis and security incident response.

Related searches — Get one-click, instant access to information on the change you're viewing and all related events, such as what other changes came from specific users and workstations, eliminating additional guesswork and unknown security concerns.

Event archiving — Schedule the archiving of older data to an archive database, enabling organizations to keep critical and relevant data online while improving overall performance of search and data retrieval.

Integrated event forwarding — Easily integrate with SIEM solutions to forward Change Auditor events to Splunk, HP ArcSight or IBM QRadar. Additionally, Change Auditor integrates with Quest® InTrust® for long-term 20:1 compressed event storage and aggregation of native or third-party logs to reduce storage costs on SIEM forwarding and create a highly compressed log repository.

Role-based access — Configure access so auditors can run searches and reports without making any configuration changes to the application, and without requiring the assistance and time of the administrator.

Web-based access with dashboard reporting — Search from anywhere using a web browser and create targeted dashboard reports to provide upper management and auditors with access to the information they need without having to understand architecture or administration.

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.

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-ChangeAuditor-US-KS-34738