On Demand Audit Hybrid Suite for Office 365

Security and compliance auditing for hybrid Microsoft environments

According to Microsoft more than 50 percent of user accounts in Azure AD are hybrid.[1] Chances are your organization will make that transition soon if it hasn't already. However, even as you move to a hybrid Microsoft environment, you need to maintain your legacy infrastructure and this doubles the area that your IT team needs to manage and protect. As your data footprint expands due to more workloads moving to the cloud, your infrastructure is exposed to more and more security threats. Unfortunately, native on-premises and cloud-auditing tools are limited in their ability to address the security and compliance needs of this new hybrid business model.

What if you could secure your hybrid environment and ensure continuous compliance by searching any change made on premises or in the cloud from a single dashboard? What if you could normalize what individual changes look like across your on-premises and Office 365 workloads? What if you could delegate audit data access so users get exactly the reports they need and nothing more? What if you could keep as much audit data as you need for as long as you need it?

Quest® On Demand Audit Hybrid Suite for Office 365 provides a single, hosted view of user activity across hybrid Microsoft environments, giving you

Pair Change Auditor and On Demand Audit for a single, hosted view of hybrid activity from a SaaS dashboard.

1 https://www.microsoft.com/en-us/microsoft-365/blog/2017/11/13/how-organizations-are-connecting-their-on-premises-identities-to-azure-ad/

"Without On Demand Audit, I wouldn't be able to track privileged changes to critical systems."

Director, Large Enterprise Financial Services Company

TVID: C0A-DCB-775

BENEFITS:

- Pair Change Auditor and On Demand Audit for complete hybrid auditing
- Deliver a single, hosted view of hybrid activity from a security vulnerability dashboard
- Analyze all activity automatically to detect anomalous surges in sensitive activity
- Slash investigation time with a responsive, flexible search builder
- Simplify analysis with interactive data visualizations
- Normalize audit data with a simple format so it's easy to interpret
- Get instant, one-click access to detailed information on each change and related events, eliminating guesswork during investigation
- Send real-time alerts to email and mobile devices to prompt immediate action, even while you're not on site
- Enable your stakeholders to get exactly the reports they need with granular, delegated access
- Store audit history for up to 10 years, enabling you to keep as much data as necessary to satisfy compliance regulations

Keep all the audit data you need to satisfy security and compliance policies; On Demand Audit stores all audit history up to 10 years at a fixed subscription price.

visibility to all changes taking place, whether on-premises Active Directory (AD), Azure AD or Office 365 workloads such as Exchange Online, SharePoint Online, OneDrive for Business and Teams.

The hybrid suite is delivered as a subscription service that gives you licenses to Change Auditor for Active Directory, Change Auditor for Logon Activity and On Demand Audit. We make it easy to pair them together in just a few clicks.

CHANGE AUDITOR FOR ACTIVE DIRECTORY AND LOGON ACTIVITY

Change Auditor is the industry's leading solution for in-depth, high-fidelity auditing of on-premises Microsoft environments. It provides real-time auditing, alerting and forensics on all critical configuration, user and administrator changes across AD, including those made to Group Policy Objects (GPOs), your DNS, server configurations, nested groups and much more.

ON DEMAND AUDIT

On Demand Audit is an Azure-hosted SaaS that tracks all activity across Azure AD, Exchange Online, SharePoint Online and OneDrive for Business. As part of the hybrid suite, it consolidates and correlates the on-premises audit data gathered by Change Auditor together with cloud activity from Azure AD and Office 365 workloads.

HOW THE ON DEMAND AUDIT HYBRID SUITE WORKS

With Change Auditor and On Demand Audit combined in the On Demand Audit Hybrid Suite for Office 365, you get a single view for your on-premises and cloud audit data from which you can quickly investigate incidents with responsive search and interactive data visualization, and store audit history for up to 10 years in the On Demand tenant.

Most cloud-based auditing products on-premises activity, and those that do (e.g. SIEM tools) rely on native event logs, which lack the fidelity of auditing that Change Auditor provides.

Change Auditor gets data from a lightweight agent installed on each domain controller. As a result, it can audit faster and more accurately than native auditing tools. Change Auditor displays all events in an easy-to-read, normalized format of the five Ws — who, what, when, where and originating workstation. Change Auditor can even prevent changes to critical data, such as privileged groups, GPOs and sensitive mailboxes, even if the user has the native pe rmissions to make those changes.

On Demand Audit surfaces on-premises Change Auditor events, while also auditing activity across Azure AD and Office 365 workloads, to provide a single, hosted view of:

- AD and Azure AD users, groups, roles, identities and more
- AD logon/logoff activity, including both Kerberos and NTLM authentications
- Azure AD sign-in failures and their source
- Exchange Online mailbox logins, activity, non-owner mailbox access, distribution groups and more
- SharePoint Online and OneDrive for Business file access, external sharing of data, anonymous links and more
- Teams configuration and settings changes, guest user activity and when new Teams or channels are created

Hybrid identity auditing

On Demand Audit enables you to search by both on premises and cloud identities, so you can find all user activity regardless of where the activity originated.

Real-time alerts on the move

Maintain constant visibility and respond from anywhere — and on any device — to vital policy changes and suspicious events, regardless of whether they occur on premises or in the cloud. With the On Demand Audit Hybrid Suite for Office 365, you can send real-time alerts to email and mobile devices to prompt immediate action, even while you're not on site

EXTEND CHANGE AUDITOR FUNCTIONALITY WITH NEW CLOUD-EXCLUSIVE CAPABILITIES

Responsive, flexible search

Slash investigation time with fast, intuitively built searches across tenants that deliver immediate results. On Demand Audit provides flexible searches on any event or any field, including by actor, changed attributes, activity details or cloud-only objects.

Security vulnerability dashboard

Analyze event data from on-prem and Office 365 workloads for a single view of security vulnerabilities and anomalous activity across your hybrid environment. Be alerted to critical activity including Kerberos exploits, suspicious AD database access attempts, changes to sensitive groups and roles, as well as unusual spikes in sign-in failures, account lockouts, and activity by external guest users. Accelerate investigations through interactive visualizations to detect and stop breaches before they wreak havoc in your network.

Interactive data visualizations

Transform hundreds and millions of on-premises and Office 365 audit events into stunning, visual dashboards that help you simplify compliance reporting and investigate incidents faster.

Integrated anomaly detection

Automatically analyze all activity from your on-prem AD, Azure AD and Office 365 workloads to detect anomalous surges in sensitive activity that could be indicative of attack or compromise. Be proactively notified of suspicious increases in sign-in failures, account lockouts, permission changes, external guest activity, files shared externally, and more. Visualize anomalies in context to highlight true threats and speed investigations.

Normalized audit view

Unlike native auditing, On Demand Audit translates raw audit logs into a meaningful, normalized format. On Demand highlights the most important event details from every on-premises and cloud change event, including before and after values, so you can make quick decisions where your security is concerned.

Granular, delegated access

In just a few clicks, you can give your security and compliance teams, help desk staff, IT managers and even external auditors and partners exactly the reports they need and nothing more. On Demand Audit provides granular, delegated access, safely empowering users to get the insights they need without making any configuration changes and setting up additional infrastructure.

Long-term storage

On Demand Audit stores all audit history for up to 10 years at a fixed subscription price. This enables you to keep as much audit data as you need to satisfy security and compliance policies — without increasing your own Azure storage costs.

Secure, scalable and reliable SaaS

On Demand Audit delivers the security standards, service level and scalability that you need, backed by award-winning, global support ready to help you 24/7/365. Certifications include ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018:2019.

Fast, easy setup of hosted auditing dashboard

Onboard to Quest On Demand with ease. Start auditing in minutes. No installation, no upgrades, no complex configuration. — no sweat!

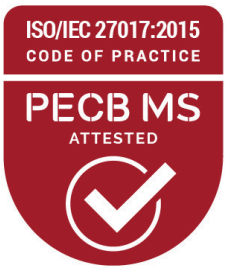
Rapid innovation

We keep pace with Microsoft updates so you don't have to. As an Azure-hosted SaaS platform, Quest On Demand automatic updates deliver new features, customer-requested enhancements and security patches quickly and without any effort on your part.

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.

Quest On Demand Audit is included in the scope of the Platform Management ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018:2019 Certifications.



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-MPM-OnDemandAudit-US-LR-68859