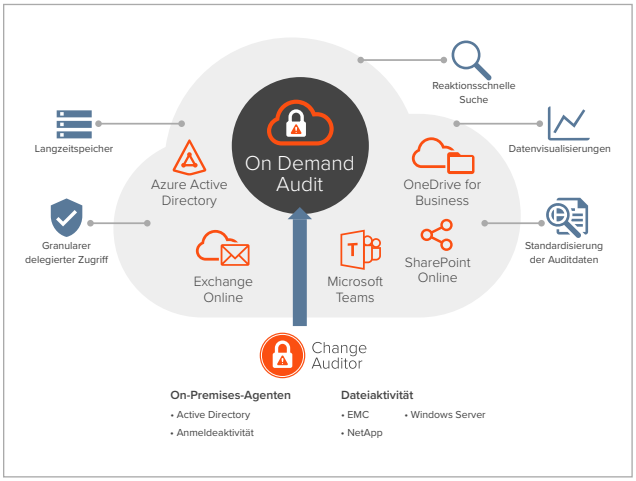
On Demand Audit Hybrid Suite for Office 365

Sicherheits- und Compliance-Auditierung für hybride Microsoft-Umgebungen

Nach Angaben von Microsoft sind mehr als 50 Prozent der Benutzerkonten in Azure AD hybride Konten.[1] Falls Ihr Unternehmen diesen Übergang nicht bereits vollzogen hat, wird es dies also wahrscheinlich bald tun. Aber auch wenn Sie zu einer hybriden Microsoft-Umgebung wechseln, müssen Sie Ihre Legacy-Infrastruktur weiterhin warten, und damit verdoppelt sich der Bereich, den Ihr IT-Team verwalten und schützen muss. Da Ihr Datenbestand durch die Verlagerung von Workloads in die Cloud immer größer wird, ist Ihre Infrastruktur immer mehr Sicherheitsbedrohungen ausgesetzt. Leider sind native On-Premises- und Cloud-Auditierungs-Tools nur begrenzt in der Lage, die Sicherheits- und Compliance-Anforderungen dieses neuen hybriden Geschäftsmodells zu erfüllen.

Wie wäre es, wenn Sie Ihre Hybrid-Umgebung absichern und kontinuierliche Compliance gewährleisten könnten, indem Sie jede Änderung, die lokal oder in der Cloud vorgenommen wurde, einfach über Ihr zentrales Dashboard finden könnten? Wie wäre es, wenn Sie standardisieren könnten, wie einzelne Änderungen in Ihren On-Premises- und Office 365-Workloads aussehen? Wie wäre es, wenn Sie den Zugriff auf Auditdaten delegieren könnten, so dass die Benutzer genau die Berichte erhalten, die sie benötigen, und nicht mehr? Wie wäre es, wenn Sie so viele Auditdaten



Koppeln Sie Change Auditor und On Demand Audit für eine einzige, gehostete Ansicht der Hybrid-Aktivitäten von einem SaaS-Dashboard aus.

Vorteile:

- Koppeln Sie Change Auditor und On Demand Audit für eine vollständige hybride Auditierung
- Über das Sicherheitsschwachstellen-Dashboard erhalten Sie eine zentrale, gehostete Ansicht aller hybriden Aktivitäten
- Analysieren Sie alle Aktivitäten automatisch, um anomale Schwankungen bei sensiblen Aktivitäten zu erkennen
- Verkürzen Sie die Untersuchungszeit mit einem reaktionsschnellen, flexiblen Suchmodul
- Vereinfachen Sie Analysen mit interaktiven Datenvisualisierungen
- Standardisieren Sie Auditdaten in einem einfachen Format, damit sie leicht zu interpretieren sind
- Erhalten Sie sofortigen Zugriff mit nur einem Mausklick auf detaillierte Informationen zu jeder Änderung und den damit verbundenen Ereignissen, sodass Sie bei der Untersuchung nicht mehr raten müssen
- Senden Sie Warnmeldungen in Echtzeit per E-Mail und an Mobilgeräte, wenn sofortige Maßnahmen erforderlich sind – selbst wenn Sie gerade nicht vor Ort sind
- Ermöglichen Sie es Ihren Stakeholdern, genau die Berichte abzurufen, die sie benötigen – mit granularem, delegiertem Zugriff
- Speichern Sie den Auditverlauf bis zu 10 Jahre lang und bewahren Sie so viele Daten wie nötig auf, um Compliance-Vorschriften zu erfüllen

aufbewahren könnten, wie Sie benötigen, und zwar so lange, wie Sie sie benötigen?

Quest® On Demand Audit Hybrid Suite for Office 365 bietet eine einzige, gehostete Ansicht der Benutzeraktivitäten in hybriden Microsoft-Umgebungen und verschafft Ihnen so einen Einblick in alle Änderungen – ganz gleich, ob es sich um On-Premises-AD, Dateiserver, Netzwerkspeicher, Azure AD oder Office 365-Workloads wie Exchange Online, SharePoint Online, OneDrive for Business und Teams handelt.

Die Hybrid Suite wird als Abonnement-Service angeboten, mit dem Sie Lizenzen für Change Auditor for Active Directory, Change Auditor for Logon Activity und On Demand Audit erhalten. Wir machen es Ihnen leicht, sie mit nur wenigen Klicks zu kombinieren.

> **Ohne On Demand Audit wäre ich nicht in der Lage, privilegierte Änderungen an kritischen Systemen nachzuverfolgen.**
>
> *Direktor bei einem großen Finanzdienstleistungsunternehmen, TVID: C0A-DCB-775*

Change Auditor

Change Auditor ist die branchenweit führende Lösung für tiefgreifende, zuverlässige Auditierungen von On-Premises-Microsoft-Umgebungen. Sie bietet Echtzeit-Auditierungen, Warnmeldungen und Forensiken für alle kritischen Konfigurations-, Benutzer- und Administratoränderungen im gesamten AD, einschließlich Änderungen an GPOs, verschachtelten Gruppen und vielem mehr. Darüber hinaus verfolgt das Logon Activity-Modul alle Authentifizierungen bei AD und die Module für die Dateiaktivität überwachen EMC, NetApp und Windows Server auf verdächtige Dateizugriffe.

On Demand Audit

On Demand Audit ist eine von Azure gehostete SaaS-Lösung, die alle Aktivitäten in AD, Azure AD, Exchange Online, Teams, SharePoint Online und OneDrive for Business nachverfolgt. Als Teil der Hybrid Suite konsolidiert und korreliert sie die von Change Auditor gesammelten On-Premises-Auditdaten mit den Cloud-Aktivitäten von Azure AD und Office 365-Workloads.

Bewahren Sie alle Auditdaten auf, die Sie zur Einhaltung von Sicherheits- und Compliance-Richtlinien benötigen. On Demand Audit speichert den gesamten Auditverlauf bis zu 10 Jahre zu einem festen Abonnementpreis.

So funktioniert die On Demand Hybrid Suite

Mit der Kombination von Change Auditor und On Demand Audit in der On Demand Audit Hybrid Suite for Office 365 erhalten Sie eine zentrale Ansicht für Ihre On-Premises- und Cloud-Auditdaten, von der aus Sie Vorfälle mit reaktionsschneller Suche und interaktiver Datenvisualisierung schnell untersuchen und den Auditverlauf für bis zu 10 Jahre im On-Demand-Tenant speichern können.

Die meisten Cloud-basierten Auditierungsprodukte erfassen keine On-Premises-Aktivitäten, und diejenigen, die es tun (z. B. SIEM-Tools), stützen sich auf vom System bereitgestellte Ereignisprotokolle, die nicht die gleiche Auditierungstreue wie Change Auditor bieten.

Change Auditor bezieht die Daten von einem leichtgewichtigen Agent, der auf jedem Server installiert ist. Dadurch kann es schneller und genauer auditieren als die vom System bereitgestellten Audit-Tools. Change Auditor zeigt alle Ereignisse in einem leicht zu lesenden, standardisierten Format mit den fünf Ws an: Wer, Was, Wann, Wo und die Workstation, von der das Ereignis ausging. Change Auditor kann sogar Änderungen an kritischen

Daten wie privilegierten Gruppen, GPOs und sensiblen Postfächern verhindern, selbst wenn der Benutzer über die nativen Berechtigungen verfügt, um diese Änderungen vorzunehmen.

On Demand Audit zeigt lokale Change Auditor Ereignisse an und auditiert gleichzeitig Aktivitäten in Azure AD- und Office 365-Workloads, um Folgende Informationen in einer einzigen, gehosteten Ansicht darzustellen:

- Benutzer, Gruppen, Rollen, Identitäten und mehr bei AD und Azure AD
- AD-An- und Abmeldeaktivitäten, einschließlich Kerberos- und NTLM-Authentifizierungen
- Dateizugriff, Umbenennung, Löschung und mehr von EMC, NetApp und Windows-Servern
- Fehler bei der Azure AD-Anmeldung und deren Ursache
- Anmeldungen, Aktivitäten, Zugriff Dritter auf den Posteingang, Verteilergruppen und mehr bei Exchange Online
- SharePoint Online und OneDrive for Business-Dateizugriff, externe Freigabe von Daten, anonyme Links und mehr
- Teams-Konfigurations- und -Einstellungsänderungen, Aktivitäten von Gastbenutzern und Erstellung von neuen Teams oder Kanälen

Hybrid-Identitätsauditierung

Mit On Demand Audit können Sie nach On-Premises- und Cloud-Identitäten suchen, um alle Benutzeraktivitäten unabhängig davon zu finden, von wo die Aktivität ausging.

Echtzeitwarnmeldungen für unterwegs

Bewahren Sie ständige Transparenz und reagieren Sie von überall und von jedem beliebigen Gerät auf wichtige Richtlinienänderungen und verdächtige Ereignisse, unabhängig davon, wo sie lokal oder in der Cloud auftreten. Mit der On Demand Audit Hybrid Suite for Office 365 können Sie Echtzeitwarnmeldungen per E-Mail und an Mobilgeräte senden, um sofortige Maßnahmen einzuleiten, auch wenn Sie nicht vor Ort sind.

Erweitern Sie die Funktionalität von Change Auditor um neue Cloud-exklusive Funktionen

Reaktionsschnelle, flexible Suche

Verringern Sie die Untersuchungszeit mit schnellen, intuitiv gestalteten Suchen über mehrere Tenants, die umgehend Ergebnisse liefern. On Demand Audit bietet flexible Suchen zu jedem Ereignis oder jedem Feld, z. B. nach Akteur, geänderten Attributen, Aktivitätsdetails oder reinen Cloud-Objekten.

Sicherheitsschwachstellen-Dashboard

Analysieren Sie Ereignisdaten von lokalen und Office 365-Workloads in einer zentralen Sicherheits-schwachstellenansicht mit Aktivitäten in Ihrer gesamten Hybrid-Umgebung. Erhalten Sie Warnmeldungen zu kritischen Aktivitäten wie zum Beispiel den Folgenden: Kerberos Exploits, verdächtige Zugriffe auf die AD-Datenbank, Änderungen an sensiblen Gruppen und Rollen, ungewöhnlich hohe Zahl von Anmeldefehlern, Kontosperrungen und Aktivitäten von externen Gast-benutzern. Beschleunigen Sie Untersuchungen durch interaktive Visualisierungen, um Sicherheitsverletzungen zu erkennen und zu stoppen, bevor sie in Ihrem Netzwerk Schlimmeres anrichten.

Interaktive Datenvisualisierungen

Verwandeln Sie Millionen von On-Premises- und Office 365-Auditereignissen in beeindruckende visuelle Dashboards, die Ihnen helfen, die Compliance-Bericht-erstellung zu vereinfachen und Vorfälle schneller zu untersuchen.

Integrierte Erkennung von Anomalien

Analysieren Sie automatisch sämtliche Aktivitäten in Ihren On-Premises-AD-Umgebungen, Authentifizierungen, Dateiservern und Cloud-Aktivitäten in Azure AD- und Office 365-Workloads, um eine anormale Zunahme von sensiblen Aktivitäten zu erkennen, die auf einen Angriff oder eine Kompromittierung hindeuten könnte. Lassen Sie sich proaktiv über die verdächtige Zunahme von Anmeldefehlern, Kontosperrungen, Berechtigungsänderungen, Datei-umbenennungen, Aktivitäten externer Gastbenutzer, extern freigegebenen Dateien und vieles mehr informieren. Visualisieren Sie Anomalien im Kontext, um echte Bedrohungen hervorzuheben und Untersuchungen zu beschleunigen.

Normalisierte Auditansicht

Anders als native Auditierungen überträgt On Demand Audit unbearbeitete Auditprotokolle in ein aussagekräftiges, standardisiertes Format. On Demand Audit hebt die wichtigsten Ereignisdetails jedes lokal und in der Cloud stattfindenden Änderungsereignisses mit Angabe der Werte vor und nach dem Ereignis hervor, damit Sie schnell sicherheitsbezogene Entscheidungen treffen können.

Granularer delegierter Zugriff

Mit nur wenigen Klicks können Sie Ihren Sicherheits- und Compliance-Teams, Helpdesk-Mitarbeitern, IT-Verantwortlichen und sogar externen Auditoren sowie Partnern genau die Berichte zur Verfügung stellen, die sie benötigen, und nicht mehr. On Demand Audit bietet einen granularen delegierten Zugriff und ermöglicht es Benutzern so, auf sichere Weise die benötigten Erkenntnisse zu gewinnen, ohne dass Konfigurationsänderungen und die Einrichtung zusätzlicher Infrastruktur erforderlich werden.

Langzeitspeicher

On Demand Audit speichert die gesamte Audithistorie bis zu 10 Jahre lang zu einem festen Abonnementpreis. Auf diese Weise können Sie so viele Auditdaten aufbewahren, wie Sie gemäß Sicherheits- und Compliance-Richtlinien benötigen, ohne Ihre eigenen Azure-Speicherkosten in die Höhe zu treiben.

Sichere, skalierbare und zuverlässige SaaS-Lösung

On Demand Audit bietet die Sicherheitsstandards, Servicelevel und Skalierbarkeit, die Sie benötigen – rund um die Uhr unterstützt durch preisgekrönten weltweiten Support. Zertifiziert ist die Lösung beispielsweise mit ISO/IEC 27001:2013, ISO/IEC 27017:2015 und ISO/IEC 27018:2019.

Schnelle, einfache Einrichtung des gehosteten Auditierungs-Dashboards

Starten Sie jetzt ganz einfach durch – mit Quest On Demand. Auditierungen können in wenigen Minuten gestartet werden. Keine Installation, keine Upgrades, keine komplizierte Konfiguration – kein Stress!

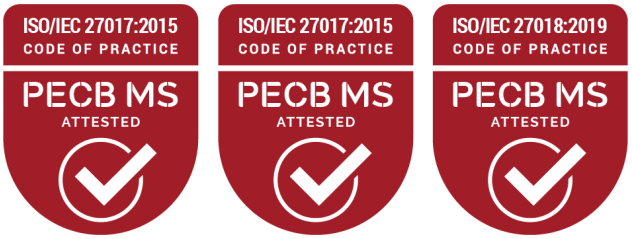
Schnelle Innovation

Wir bleiben für Sie bei Microsoft-Updates auf dem Laufenden. Die automatischen Aktualisierungen von Quest On Demand als auf Azure gehostete SaaS-Plattform liefern schnell und ohne Ihr Zutun neue Funktionen, von Kunden gewünschte Verbesserungen und Sicherheits-Patches.

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das Potenzial neuer Technologien in einer immer komplexeren IT-Landschaft ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Verwaltung von Active Directory und Office 365 bis hin zur Cyber Resilience: Quest hilft Kunden, bereits jetzt ihre nächste IT-Herausforderung zu bewältigen.
Quest Software. Where Next Meets Now.

Quest On Demand Audit ist nach ISO/IEC 27001:2013, ISO/IEC 27017:2015 und ISO/IEC 27018:2019 für die Plattformverwaltung zertifiziert.



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