Change Auditor for Active Directory

Überprüfungen in Echtzeit für Active Directory und Azure Active Directory

Probleme in Zusammenhang mit Active Directory (AD) können zu ungeplanten und kostspieligen Serviceunterbrechungen sowie geschäftsschädigenden Netzwerkausfällen führen. Darüber hinaus können Datenlecks und Verletzungen von Richtlinien wie SOX, PCI, HIPAA und DSGVO erhebliche Geldstrafen nach sich ziehen. Sie benötigen Überwachungs- und Sicherheitsfunktionen für Active Directory, die gewährleisten, dass Sie rechtzeitig über kritische Änderungen innerhalb von AD und Azure AD benachrichtigt werden.

Quest® Change Auditor for Active Directory fördert die Sicherheit und Kontrolle von AD und Azure AD durch Nachverfolgen kritischer Konfigurationsänderungen und deren Konsolidierung in einer einzigen Konsole. Change Auditor verfolgt, überprüft, meldet und warnt bei Änderungen, die sich auf Ihre lokalen und Cloud-Umgebungen auswirken, ohne den Aufwand einer nativen Überprüfung. Mit Change Auditor for AD erhalten Sie eine normalisierte Ansicht jeglicher Änderungen und damit verbundener Ereignisdetails, einschließlich Vorher- und Nachher-Werten, sowie die damit in Beziehung stehenden lokalen und Cloud-Identitäten. Außerdem können Sie Anmerkungen hinzufügen, um den Hintergrund bestimmter Änderungen zu erläutern und Überprüfungsanforderungen gerecht zu werden. Mit Change Auditor for AD können Sie alle kritischen Änderungen schnell und effizient überprüfen, um Ihre kostbaren Daten und Ressourcen sicher zu halten.

ÜBERWACHUNG ALLER WICHTIGEN ÄNDERUNGEN

Profitieren Sie von umfangreicher benutzerdefinierter Überprüfung und Berichterstellung bei allen kritischen Änderungen in AD und Azure AD wie solchen an Gruppenrichtlinien-Objekten, an Ihrem Domänennamensystem, Serverkonfigurationen, verschachtelten Gruppen und mehr. Anders als bei nativen Überprüfungen erhalten Sie eine konsolidierte Ansicht aller Änderungen am lokalen, Cloud- und Hybrid-AD mit umfassenden Untersuchungen der Verbindung zu anderen Ereignissen im Laufe der Zeit in chronologischer Reihenfolge und über Ihre gesamten AD und Azure AD Umgebungen hinweg.

Mit Change Auditor for Active Directory erhalten Sie Informationen in chronologischer Reihenfolge darüber, wer was wann wo und an welcher Workstation geändert hat, auch die in Beziehung stehenden lokalen und Cloud-Identitäten.

VORTEILE:

- Minutenschnelle Installation mit schneller Ereigniserfassung für sofortige Analysen in Windows Umgebungen
- Unternehmensweite Überprüfung (lokal und in der Cloud) und Compliance über einen einzigen Client
- Proaktive Erkennung von Bedrohungen auf Grundlage von Benutzerverhaltensmustern
- Schließung unentdeckter Sicherheitslücken und Sicherstellung von unterbrechungsfreiem Zugriff auf Anwendungen, Systeme und Benutzer durch Nachverfolgung aller Ereignisse sowie aller mit bestimmten Vorfällen zusammenhängenden Änderungen
- Sekundenschnelle Entschärfung von Sicherheitsrisiken dank Echtzeitbenachrichtigungen an jedes beliebige Gerät, für sofortige Reaktion immer und überall
- Stärkung der internen Kontrollen dank Schutz vor ungewollten Änderungen und Einschränkung der Steuerungsmöglichkeiten autorisierter Benutzer
- Höhere Verfügbarkeit durch proaktive Fehlerbehebung bei Kontosperrungen
- Geringerer Leistungsabfall auf Servern und Einsparung von Massenspeicherressourcen durch Erfassung von Ereignissen ohne Rückgriff auf native Überwachungsfunktionen
- Optimierte Compliance mit betrieblichen und behördlichen Richtlinien und Bestimmungen, inklusive DSGVO, SOX, PCI DSS, HIPAA, FISMA, SAS 70 und vielen weiteren
- Intelligente und tiefgreifende forensische Datenanalyse für Auditoren und das Management

„Insgesamt ist Change Auditor sehr nützlich. Kein anderes der Produkte, die wir uns angesehen haben, bot dasselbe Niveau an Echtzeitüberwachung und -schutz, ohne dass dafür die Windows Überwachung für alle Active Directory Änderungen aktiviert sein musste."

Patrick Rohe
Senior IT Architect
Towson University

SYSTEMANFORDERUNGEN

Eine vollständige Liste der aktuellen Systemanforderungen finden Sie unter quest.com/products/change-auditor-for-active-directory.

Mithilfe von proaktiven Benachrichtigungen bleiben Sie stets auf dem Laufenden und haben die Möglichkeit, von überall und von jedem Gerät aus umgehend auf entscheidende Richtlinienänderungen und Sicherheitsverletzungen zu reagieren. Dadurch verringern Sie die durch alltägliche Modifikationen entstehenden Risiken.

NACHVERFOLGUNG VON BENUTZERAKTIVITÄTEN UND VERHINDERUNG UNGEWOLLTER ÄNDERUNGEN

Stärken Sie unternehmensweit die Einhaltung von Änderungs- und Kontrollrichtlinien: Das Tool verfolgt die Aktivität von Benutzern und Administratoren bei Kontosperrungen und dem Zugriff auf wichtige Registrierungseinstellungen. Dank proaktiver Kontrollen zur Verhinderung kritischer Änderungen, Benachrichtigungen rund um die Uhr, detaillierten Analysen, der Möglichkeit, frühere Werte wiederherzustellen, und Berichterstellungsfunktionen wird Ihr Active Directory zuverlässig vor Sicherheitsrisiken wie verdächtigem Verhalten und nicht autorisiertem Zugriff geschützt und erfüllt stets sämtliche Compliance-Anforderungen des Unternehmens und der relevanten Behörden.

GEHOSTETES ÜBERPRÜFUNGS-DASHBOARD MIT ON DEMAND AUDIT

Nehmen Sie ein Upgrade auf die On Demand Audit Hybrid Suite for Office 365 vor, um sich Zugang zu Change Auditor for Active Directory und On Demand Audit zu sichern. Sie können beide Lösungen im Handumdrehen mit nur wenigen Klicks zu einer zentralen, gehosteten Ansicht jeglicher Änderungen in Zusammenhang mit AD, Azure AD, Exchange Online, SharePoint Online und OneDrive for Business kombinieren. Vereinfachen Sie Überprüfungsvorgänge mit einer reaktionsschnellen Suchfunktion sowie interaktiven Datenvisualisierungen, und speichern Sie Ihren Überprüfungsverlauf während bis zu 10 Jahren.

PROAKTIVE ERKENNUNG VON BEDROHUNGEN MIT CHANGE AUDITOR THREAT DETECTION

Vereinfachen Sie die Erkennung von Bedrohungen durch Benutzer, indem Sie außergewöhnliche Aktivitäten analysieren, um die Benutzer in Ihrem Unternehmen mit dem größten Gefahrenpotential einzustufen, mögliche Bedrohungen zu erkennen und die Anzahl falscher Treffer zu verringern.

EFFEKTIVE DATENAUSWERTUNG FÜR HÖHERE SICHERHEIT UND ZUVERLÄSSIGERE COMPLIANCE

Verfolgen Sie kritische Änderungen und übersetzen Sie die so erhobenen Rohdaten in aussagekräftige, intelligente Informationen. So können Sie Sicherheit und Compliance in Ihrer Infrastruktur nachhaltig optimieren. Change Auditor for AD liefert Ihnen Informationen darüber, welche Nutzer wann und wo welche Änderungen an welcher Workstation vorgenommen haben, sowie damit verbundene Ereignisdetails wie Vorher- und Nachher-Werte, damit Sie schnelle Entscheidungen treffen können, die Ihre Sicherheit betreffen. Mit der leistungsstarken Change Auditor Überprüfungs-Engine gehören Überprüfungsbeschränkungen überdies der Vergangenheit an. Und wenn Sie keine Protokolle von nativen Überprüfungen benötigen, sehen Sie schneller Ergebnisse und sparen Speicherkapazität.

INTEGRIERTE EREIGNISWEITERLEITUNG

Nehmen Sie problemlos Integrationen mit SIEM-Lösungen vor, um Change Auditor Ereignisse an Splunk, ArcSight oder QRadar weiterzuleiten. Darüber hinaus können Sie Change Auditor mit Quest® InTrust® integrieren, um von einer komprimierten Ereignisspeicherung im Verhältnis 20:1, einer zentralisierten Erhebung nativer und externer Protokolle sowie leistungsstarken Parsing- und Analysefunktionen zu profitieren – einschließlich Meldungen und automatisch ausgelöster Maßnahmen im Falle verdächtiger Ereignisse.

AUTOMATISCHE BERICHTERSTELLUNG FÜR COMPLIANCE MIT INTERNEN UND BEHÖRDLICHEN VORGABEN

Dank der integrierten Compliance-Bibliothek sowie benutzerdefinierten Berichten ist es ganz einfach, die Einhaltung behördlicher Normen wie DSGVO, SOX, HIPAA, PCI DSS, FISMA und SAS 70 nachzuweisen.

ÜBER QUEST

Quest liefert Softwarelösungen für die ständig im Wandel befindliche Welt der Unternehmens-IT. Wir helfen, die durch Datenexplosion, Cloud-Erweiterung, Hybrid-Rechenzentren, Sicherheitsbedrohungen und gesetzliche Bestimmungen hervorgerufenen Schwierigkeiten zu verringern. Unser Portfolio beinhaltet Lösungen für Datenbankverwaltung, Datenschutz, vereinheitlichte Endpunktverwaltung, Identitäts- und Zugriffsverwaltung sowie Verwaltung von Microsoft-Plattformen.

Quest
quest.com/de
Sie finden Informationen zu lokalen Niederlassungen auf (quest.com/de-de/locations)

DataSheet-ChangeAuditor4AD-US-KS-DE-WL-40680