

Change Auditor for Active Directory

Auditoria em tempo real para Active Directory e Azure Active Directory

Problemas do Active Directory (AD) podem resultar em interrupções de serviço e tempo de inatividade de rede não planejados e dispendiosos que afetam os negócios. Violações de dados prejudiciais e não conformidade com SOX, PCI, HIPAA, GDPR, entre outras, também podem causar custos pesados. Você precisa ter auditoria e segurança do Active Directory que assegurem que você seja notificado em tempo real sobre alterações críticas do AD e do Azure AD.

O Quest® Change Auditor for Active Directory conduz a segurança e o controle do AD e do Azure AD ao rastrear todas as principais alterações de configuração e depois consolidá-las em um único console. Controles, auditorias, relatórios e alertas do Change Auditor das alterações que impactam os ambientes locais ou de nuvem sem o gasto adicional de ativar a auditoria nativa. Com o Change Auditor for AD, você tem uma visão normalizada de todas as alterações e de detalhes de eventos relacionados, incluindo valores anteriores

e posteriores, além de identidades local e de nuvem correlacionadas. Você também pode adicionar comentários explicando por que uma alteração específica foi feita para atender aos requisitos de auditoria. Com o Change Auditor for AD, você pode realizar auditoria rápida e eficiente de todas as alterações essenciais para manter a segurança dos seus dados e recursos valiosos.

AUDITE TODAS AS ALTERAÇÕES ESSENCIAIS

Obtenha auditoria e relatórios extensos e personalizáveis para todas as alterações críticas do AD e do Azure AD, incluindo as que foram realizadas em Objetos da Diretiva de Grupo (GPOs), seu Sistema de Nome de Domínio (DNS), configurações de servidor e grupos aninhados, entre outros. Diferentemente da auditoria nativa, você terá uma visão consolidada de todas as atividades de alteração de AD local, na nuvem ou híbrido, com análise aprofundada em relação aos eventos ao longo do tempo, em ordem



Com o Change Auditor for Active Directory, você saberá o autor, o conteúdo, o momento, o local e a workstation de origem de todas as alterações em ordem cronológica, incluindo identidades correlacionadas locais e na nuvem.

BENEFÍCIOS:

- É instalado em apenas alguns minutos com rápida coleta de eventos para análise imediata em ambientes Windows
- Possibilita auditoria e conformidade em toda a empresa, localmente ou na nuvem, por meio de um único cliente
- Detecta ameaças proativamente com base em padrões de comportamento do usuário
- Elimina problemas desconhecidos de segurança, garantindo o acesso contínuo a aplicações, sistemas e usuários ao controlar todos os eventos e as alterações relacionadas a incidentes específicos
- Reduz riscos de segurança em apenas alguns segundos com alertas em tempo real para qualquer dispositivo, proporcionando resposta imediata, dentro ou fora do escritório
- Fortalece controles internos com a proteção contra alterações não desejadas e limita o controle de usuários autorizados
- Conduz a disponibilidade ao habilitar soluções de problemas proativas relacionadas a bloqueios de conta
- Reduz quedas de performance em servidores e economiza recursos de armazenamento ao coletar eventos sem a utilização de auditoria nativa
- Simplifica a conformidade com normas e políticas governamentais e corporativas, incluindo GDPR, SOX, PCI DSS, HIPAA, FISMA, SAS 70 e muito mais
- Transforma informações em análises forenses inteligentes e profundas para auditores e gerentes

"No geral, o Change Auditor foi muito útil. Nenhum outro produto avaliado ofereceu o mesmo nível de proteção e auditoria em tempo real sem exigir a ativação da auditoria do Windows para todas as alterações do Active Directory."

Patrick Rohe
Arquiteto sênior de TI
Towson University

REQUISITOS DO SISTEMA

Para conferir a lista detalhada atual de requisitos de sistema, acesse quest.com/products/change-auditor-for-active-directory.

cronológica, em seus ambientes do AD e do Azure AD. E, com alertas proativos, será possível manter conhecimento constante e responder de qualquer lugar e em qualquer dispositivo a alterações importantes em políticas e violações de segurança conforme elas ocorrerem, reduzindo os riscos associados a alterações diárias.

CONTROLE A ATIVIDADE DOS USUÁRIOS E EVITE ALTERAÇÕES INDESEJADAS

Fortaleça as políticas de controle e alteração em toda a empresa ao acompanhar a atividade de administradores e usuários relativa a bloqueios de conta e acesso a configurações de registro essenciais. Com controles proativos para evitar a ocorrência de alterações críticas em alertas 24x7, análises aprofundadas, possibilidade de restaurar valores anteriores e recursos de relatório, os ambientes do AD e do Azure AD são protegidos contra a exposição a comportamentos suspeitos e acessos não autorizados, além de estarem sempre em conformidade com os padrões governamentais e corporativos.

PAINEL DE AUDITORIA HOSPEDADO COM ON DEMAND AUDIT

Atualize para o On Demand Audit Hybrid Suite for Office 365, que inclui o Change Auditor for Active Directory e On Demand Audit. Utilize-os em conjunto facilmente com apenas alguns cliques para ter uma visão única e hospedada de alterações feitas no AD, Azure AD, Exchange Online, SharePoint Online e OneDrive for Business. Simplifique as investigações com visualização de dados interativa e pesquisa com grande capacidade de resposta e retenha o histórico de auditoria por até 10 anos.

DETECÇÃO PROATIVA DE AMEAÇAS COM O CHANGE AUDITOR THREAT DETECTION

Simplifique a detecção de ameaças de usuários ao analisar atividades anormais para classificar os usuários de maior risco na sua organização, identificar possíveis ameaças e reduzir o ruído de alertas falsos positivos.

TRANSFORME DADOS IRRELEVANTES EM INFORMAÇÕES IMPORTANTES PARA PROPORCIONAR SEGURANÇA E CONFORMIDADE

Controle as alterações críticas e converta dados brutos em insights inteligentes e significativos para ajudar a proteger a segurança e a conformidade da sua infraestrutura. O Change Auditor for AD ajuda a descobrir o autor, o conteúdo, o momento, o local e a workstation de origem das alterações, assim como detalhes de eventos relacionados, incluindo valores anteriores e posteriores, para que você possa tomar decisões rápidas quando se trata de segurança. Além disso, as limitações de auditoria ficarão para trás com o mecanismo de auditoria de alto desempenho do Change Auditor. E, sem a necessidade de registros de auditoria nativos, você terá resultados mais rápidos e economia de armazenamento.

ENCAMINHAMENTO INTEGRADO DE EVENTO

Integre-se facilmente a soluções SIEM para encaminhar eventos do Change Auditor ao Splunk, ArcSight ou QRadar. Além disso, o Change Auditor se integra ao Quest® InTrust® para armazenamento de evento compactado de 20:1 e coleta de registro nativa centralizada ou de terceiros, analisando com ações de respostas automáticas e alertas a eventos suspeitos.

RELATÓRIOS AUTOMATIZADOS PARA NORMAS GOVERNAMENTAIS E CORPORATIVAS

Com uma biblioteca integrada de conformidade, além de relatórios personalizáveis, é muito fácil manter a conformidade com normas governamentais como GDPR, SOX, HIPAA, PCI DSS, FISMA e SAS 70.

SOBRE A QUEST

A Quest fornece soluções de software para o mundo de TI corporativa em rápida transformação. Ajudamos a simplificar os desafios causados por explosão de dados, expansão da nuvem, data centers híbridos, ameaças contra a segurança e exigências reguladoras. O nosso portfólio inclui soluções para gerenciamento de banco de dados, proteção de dados, gerenciamento de endpoint unificado, gerenciamento de identidades e acessos e gerenciamento em plataforma Microsoft.

Quest
quest.com/br

Acesse (quest.com/br-pt/locations) para informações sobre escritórios locais

Quest, InTrust e o logotipo Quest são marcas comerciais e marcas registradas da Quest Software Inc. Para conferir a lista completa de marcas da Quest, acesse www.quest.com/legal/trademark-information.aspx. Todas as outras marcas comerciais pertencem a seus respectivos proprietários.

© 2019 Quest Software Inc. TODOS OS DIREITOS RESERVADOS.

DataSheet-ChangeAuditor4AD-US-KS-pt_BR-WL-40680

Quest