Change Auditor

Auditoria de alterações em tempo real para o ambiente da sua plataforma Microsoft

O registro de eventos e a criação de relatórios de alterações para aplicações e serviços na empresa são complicados, demorados e, em alguns casos, impossíveis se forem utilizadas ferramentas de auditoria nativas. Pelo fato de não existir nenhum console central, é necessário repetir o processo para cada servidor, gerando um grande volume de dados sem contexto e inúmeros relatórios.

Isso significa que a comprovação da conformidade ou a reação rápida aos eventos é um desafio constante. A segurança dos dados também está em risco porque detalhes de eventos nativos são escassos e difíceis de interpretar. Como resultado, você pode não descobrir os problemas até que seja tarde demais. E o fato de as ferramentas nativas não impedirem um usuário privilegiado de limpar um registro de eventos, é possível perder os dados do registro, destruindo o propósito de auditoria em primeiro lugar.

Felizmente, existe o Quest® Change Auditor. Essa família de produtos permite fazer auditoria, alertar e reportar as alterações no Active Directory (AD), Azure AD, Exchange, Office 365, SharePoint, Skype for Business, VMware, EMC, NetApp, SQL Server e servidores de arquivos do Windows, assim como consultas LDAP em relação ao AD, todos em tempo real e sem ativar a auditoria nativa.

É possível instalar, implementar e gerenciar seu ambiente facilmente a partir de um console central. O controle cria, exclui, faz modificações e tentativas de acesso que não poderiam ser mais fáceis, entendendo que o que aconteceu é uma projeção, já que cada evento e todos os eventos relacionados

Com o Change Auditor, você saberá quem, o que, quando, onde e a workstation de origem de todas as alterações em ordem cronológica, incluindo identidades correlacionadas locais e na nuvem.

"O Change Auditor foi de longe a melhor solução em termos de funcionalidade e custo. Fomos conquistados pela simplicidade e usabilidade da ferramenta, o que nos permitiu criar consultas sem qualquer conhecimento técnico especial."

Stephane Malagnoux, Chefe do Departamento de Computação BPCE Seguros

BENEFÍCIOS:

- Elimina preocupações desconhecidas de segurança, garantindo o acesso contínuo a aplicações, sistemas e usuários ao controlar todos os eventos e as alterações relacionadas a incidentes específicos.
- Alivia o stress e a complexidade por meio da interpretação automática de dados criptografados e de sua severidade para tomada de decisão melhor e mais rápida.
- Diminui riscos de segurança em apenas alguns segundos com alertas em tempo real para qualquer dispositivo, para resposta imediata, dentro ou fora do escritório.
- Reduz quedas de desempenho em servidores ao coletar eventos sem a utilização de auditoria nativa.
- Otimiza relatórios de conformidade, isolados por políticas internas e regulamentações externas, incluindo SOX, PCI DSS, HIPAA, FISMA, SAS 70 e outras.
- Fornece aos gerentes e auditores evidências de controles de TI adequados para tranquilidade.

"O Change Auditor tem sido uma ferramenta muito intuitiva e eficiente que permite que eu entenda as mudanças feitas pela equipe. Isso me permitiu reforçar políticas, restringir acesso e receber alertas referentes às violações."

Arquiteto de TI sênior, Medium Enterprise Professional Services Company

Fonte: TechValidate. TVID: B4A-A84-619

PRODUTOS
ChangeAuditor Threat Detection
ChangeAuditor for Active Directory
Change Auditor for Active Directory Queries
Change Auditor for EMC
ChangeAuditor for Exchange
Change Auditor for FluidFS
ChangeAuditor for Logon Activity
Change Auditor for NetApp
Change Auditor for SQL Server
Change Auditor for SharePoint
ChangeAuditor for Skype for Business
ChangeAuditor for VMware vCenter
ChangeAuditor for Windows File Servers

são apresentados em termos simples, proporcionando os 5 Ws: who, what, when, where e workstation de origem (quem, o que, quando, onde, workstation de origem), além das configurações anteriores e atuais.

Essa amplitude de análise de dados permite que uma ação imediata seja tomada quando surgem os problemas, como quais outras alterações vieram de workstations e usuários específicos, o que elimina suposições e questões de segurança desconhecidas. Se você estiver tentando atender às demandas cada vez maiores de conformidade ou buscando satisfazer as políticas internas de segurança, o Change Auditor é a solução que você pode confiar.

RECURSOS

Auditoria de ambiente híbrido com uma visualização correlacionada — ambientes de auditoria híbrida, incluindo AD/Azure AD, Exchange/Exchange Online, SharePoint/SharePoint Online/OneDrive for Business assim como logons de AD e registros no AD. Ao contrário da auditoria nativa, o Change Auditor fornece uma visualização única e correlacionada da atividade em ambientes híbridos, garantindo a visibilidade de todas as alterações em curso, sejam locais ou na nuvem.

Prevenção de alterações — Proteja contra alterações dos dados críticos no AD, no Exchange e nos servidores de arquivos do Windows, inclusive grupos privilegiados, objetos da diretiva de Grupo e caixas de correio confidenciais.

Relatórios prontos para o auditor — Gera relatórios abrangentes para as melhores práticas e exigências de conformidade com normas para SOX, PCI DSS, HIPAA, FISMA, GLBA, GDPR e outras.

Painel hospedado com On Demand Audit — Visualização híbrida AD e atividade do Office 365 juntamente com um painel hospedado SaaS com pesquisa com grande capacidade de resposta, visualização de dados interativos e armazenamento de eventos em longo prazo.

Detecção de ameaças proativas 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.

Mecanismo de auditoria de alto desempenho — Elimine as limitações de auditoria e capture as informações de alteração, sem a necessidade de registros de auditoria nativos, resultando em resultados mais rápidos e uma economia significativa de recursos de armazenamento.*

Bloqueio de conta — Capture o endereço IP e o nome da workstation de origem para eventos de bloqueio de conta e visualize tentativas de acesso e login relacionadas em um cronograma interativo. Isso ajuda a simplificar a detecção e a investigação de ameaças de segurança internas e externas.

Alertas em tempo real em qualquer lugar— Envie mudanças e alertas de padrão críticos para e-mail e dispositivos móveis para avisar uma ação imediata, permitindo que você responda mais rapidamente a ameaças mesmo quando não estiver no local.

Encaminhamento integrado de evento — Integre facilmente com 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, avaliando e analisando com ações de respostas automáticas e alertas a eventos suspeitos.

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.

* Não se aplica a FluidFS, SharePoint, EMC, NetApp e VMware.

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

Ficha técnica do ChangeAuditor-US-KS-pt_BR-WL-40681