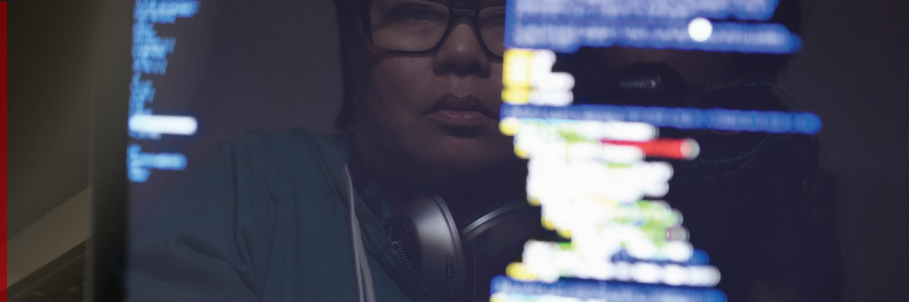

Centrify Audit and Monitoring Service

Proteja o Seu Ambiente com Alta Garantia

Para sessões privilegiadas, a melhor prática é, obviamente, auditar tudo. Com um registo documentado de todas as ações realizadas, os registos de auditoria podem ser utilizados não somente na análise forense para encontrar exatamente o problema, mas também para atribuir as ações tomadas a um utilizador específico. Devido ao nível de criticidade destas sessões, é também melhor prática guardar uma gravação em vídeo da sessão que possa ser revista ou utilizada como evidência para os seus ativos mais críticos, ou em setores altamente regulamentados. Existem várias regulamentações, incluindo PCI-DSS para dados de cartão de pagamento, que exigem especificamente este nível de auditoria. Se tiver um departamento de segurança, uma boa prática é integrar estes dados de auditoria com o seu sistema de Gestão de Informações e Eventos de Segurança (SIEM, Security Information and Event Management) existente para mineração automatizada, onde atividades de risco podem ser identificadas e alertas gerados.

Audite Tudo

Analistas do setor e reguladores governamentais reconheceram que, atualmente, a principal causa de falhas de segurança está associada ao abuso de acesso privilegiado. Credenciais privilegiadas representam as chaves do reino, permitindo uma "carona" por toda a infraestrutura. Basta uma credencial privilegiada comprometida para milhões serem afetadas. Por sua vez, auditores internos e exigências regulamentares estabelecem controlos específicos e requisitos de reporte para a utilização destas credenciais.

Mesmo organizações de pequeno e médio porte devem cumprir uma variedade de regulamentações do setor e governamentais, o que cria os seus próprios desafios quando se trata da coleta, agregação e comprovação de dados de acesso privilegiado.

Frequentemente, as organizações não dispõem da visibilidade contínua da sua postura de conformidade, o que faz com que auditorias e certificações se tornem uma corrida, durante a qual a carga de trabalho para auditores internos e a equipa de conformidade dispara.

Isto leva muitas vezes a uma abordagem por "amostragem", em que apenas um subconjunto de controlos específicos é avaliado, deixando muitos pontos cegos do ponto de vista da conformidade e da segurança. No geral, a busca de respostas de uma grande variedade de stakeholders e a avaliação de diversos conjuntos de dados têm um reflexo negativo sobre a eficiência e a precisão.

Do ponto de vista da segurança, é importante obter informações específicas e detalhadas sobre atividades de acesso privilegiado suspeitas. Gestores de segurança podem executar uma ação de remediação imediata para proteger contra riscos potenciais ou uma ameaça em curso, diretamente a partir do ecrã de alerta, e terminar manual ou automaticamente uma sessão com base no risco.

Nos últimos anos, falhas graves em matéria de segurança de dados foram possíveis graças a funcionários que criaram contas backdoor, contornando abordagens tradicionais de cofres de palavras-passe. Os utilizadores com privilégios também são conhecidos por encontrar maneiras de ignorar o cofre de palavras-passe no seu ambiente a fim de facilitar a sua rotina diária. Este tipo de acesso não controlado, que aproveita chaves SSH armazenadas localmente em servidores, expande a superfície de ataque de uma organização e coloca-a em maior risco de sofrer uma falha de segurança.

Proteja o Seu Ambiente com Alta Garantia

O Centrify Audit and Monitoring Service permite que os clientes cumpram as suas exigências de conformidade através de auditorias e relatórios, bem como encerrar quaisquer soluções alternativas perigosas, implementando a monitorização baseada no host. O serviço ajuda na gravação de todas as sessões privilegiadas e respetivos meta dados, atribuindo atividade a um indivíduo a fim de fornecer uma imagem abrangente de intenções e resultados.

GRAVAÇÃO E AUDITORIA DE SESSÕES

Registe e faça a gestão de uma visão holística da atividade privilegiada em todos os servidores Windows e Linux, IaaS e bases de dados, estabelecendo uma só fonte de informações para contas individuais e partilhadas. Prove a conformidade com relatórios sobre os privilégios de todos os utilizadores e atividades associadas.

MONITORIZAÇÃO E CONTROLO DE SESSÕES POR GATEWAY

Obtenha novos níveis de supervisão para sessões privilegiadas em infraestrutura crítica. Utilizadores administrativos monitorizam, em tempo real, a atividade em sessões remotas, podendo terminar, instantaneamente, sessões suspeitas através do Portal de Administração do Centrify.

AUDITORIA, GRAVAÇÃO E RELATÓRIOS DE SESSÕES BASEADOS NO HOST

Garanta que a gravação de sessões não pode ser ignorada através de auditoria baseada no host. Descubra atividades não controladas, como a criação e a instalação de pares de chaves SSH, que facilitariam ignorar os controlos de segurança e atribuir atividades ao utilizador individual. Audite, em detalhe forense, todas as atividades de sessões privilegiadas ao nível do processo para revisão da segurança, ação corretiva para relatórios de conformidade e para evitar falsificações.

> **"Não existe regulamentação que o Centrify não nos ajudou a cumprir. Hoje, sempre que um administrador toca num servidor, tenho um registo disso. Posso selecionar um relatório, imprimi-lo e entregá-lo ao auditor."**
>
> — Peter Manina, Especialista de TI e Engenheiro de Sistemas UNIX, Departamento de Tecnologia, Gestão e Orçamentação do Estado do Michigan

Gravação e Auditoria de Sessões para Acesso Privilegiado

Reporte e audite sessões privilegiadas que aproveitam tanto contas partilhadas como individuais, com captura de vídeo integral e meta dados. O Centrify Audit and Monitoring Service permite que os clientes realizem análises forenses e aproveitem registos de alta fidelidade para fins de auditoria e conformidade.

- Capture e armazene dados numa gravação de alta fidelidade de cada sessão privilegiada ao nível do gateway. O Centrify Audit and Monitoring Service armazena sessões numa base de dados SQL Server facilmente pesquisável para uma visão holística do que aconteceu exatamente. A funcionalidade de reprodução pesquisável do serviço confere aos gestores de segurança de TI e auditores a capacidade de ver exatamente o que os utilizadores fizeram e os resultados das suas ações, bom como identificar abusos de privilégios ou a origem de um incidente de segurança.
- Grave todas as sessões privilegiadas e respetivos meta dados, atribuindo atividade a um indivíduo a fim de fornecer uma imagem abrangente de intenções e resultados.
- Mostre que os controlos de segurança estão implementados e a funcionar conforme projetado e a fornecer provas de conformidade. Pesquise e localize gravações de sessão por servidores, utilizadores ou pesquisas personalizadas. Pode encontrar todas as sessões para um utilizador, ou servidor particular, ou para um conjunto de critérios personalizados, simplificando as investigações forenses e identificando, proativamente, ameaças internas ou atividades suspeitas.
- Obtenha visibilidade abrangente com acesso unificado e relatórios de atividade baseados numa plataforma comum. Consultas personalizáveis e integradas, bem como relatórios prontos para conformidade regulamentar com SOX e PCI, fornecem informações sobre controlos de acesso de contas privilegiadas, check-out de palavras-passe e sessões privilegiadas em todos os sistemas Windows, Linux e UNIX.

Monitorize e Controle Sessões Privilegiadas esteja em IaaS ou On-Premise

Aproveite uma infraestrutura de auditoria comum para capturar e registar atividades privilegiadas relativas à sua infraestrutura, seja on-premise ou na nuvem. Detete atividades suspeitas de um utilizador para alertar em tempo real sobre ataques que possam estar em curso. O Centrify Audit and Monitoring Service permite a monitorização e o controlo de sessões de acesso privilegiado que aproveitam contas partilhadas e individuais.

- Obtenha novos níveis de supervisão para sessões privilegiadas em infraestrutura crítica. Utilizadores administrativos monitorizam, em tempo real, a atividade em sessões remotas, podendo terminar, instantaneamente, sessões suspeitas através do Portal de Administração do Centrify. Este modo de "Quatro Olhos" permite que utilizadores administrativos supervisionem um funcionário remoto ou atividades de TI terceirizadas, acedendo diretamente à sessão em curso. Pode observar todas as ações que o utilizador com privilégios executa ou terminar a sessão se a atividade for suspeita.
- Dados de acesso privilegiado são capturados e armazenados a fim de permitir consultas robustas por ferramentas de gestão de registos e a integração com ferramentas de relatórios externas. Integração otimizada com ferramentas de SIEM e alerta, como Micro Focus® ArcSight™, IBM® QRadar™ e Splunk®, identificam rapidamente riscos ou atividades suspeitas.

Previna o Acesso Privilegiado Falsificado ou Ignorado com Auditoria, Gravação e Reporte de Sessões Baseados no Host

A adoção de uma abordagem baseada no host à auditoria, gravação e reporte de sessões resulta, em última análise, num melhor controlo sobre o acesso privilegiado no seu ambiente. O Centrify Audit and Monitoring Service amplia as suas capacidades baseadas no gateway com uma abordagem baseada no host, assegurando que os seus controlos de acesso privilegiado não sejam ignorados, como o podem ser com apenas um cofre de palavras-passe/segredos.

- Capture e recolha dados numa gravação de alta fidelidade de cada sessão privilegiada em qualquer servidor nas suas instalações e infraestruturas baseadas na nuvem. Armazene sessões numa base de dados SQL Server facilmente pesquisável para uma visão holística do que aconteceu exatamente em qualquer sistema, por qualquer ou todos os utilizadores e em qualquer momento especificado.
- A auditoria, gravação e relatórios de sessões baseados no host do Centrify inclui capacidades para monitorização avançada ao nível do processo combinadas com auditoria baseada na shell para identificar alterações suspeitas em aplicações.
- A Monitorização da Integridade de Ficheiros do Centrify identifica, em tempo real, alterações em configurações e ficheiros críticos, permitindo que alertas de segurança acionados no sistema SIEM de uma organização avisem sobre a criação de um backdoor para contornar o cofre de palavras-passe.
- Uma funcionalidade de reprodução pesquisável confere aos gestores de segurança de TI e auditores a capacidade de ver exatamente o que os utilizadores fizeram e identificar abusos de privilégios ou a origem de um incidente de segurança.
- Relatórios de acessos, verificações, sessões e a utilização de privilégios na infraestrutura Windows, Linux, UNIX e de rede.
- Integração otimizada com ferramentas de SIEM, alerta e relatórios.

EUA Sede +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Ásia Pacífico +61 1300 795 789
Brasil +55 11 3958 4876
América Latina +1 305 900 5354
sales@centrify.com

www.centrify.com