FOLHETO

Safeguard for Privileged Sessions

Reduza o risco ao controlar, monitorar e gravar o acesso privilegiado

Benefícios

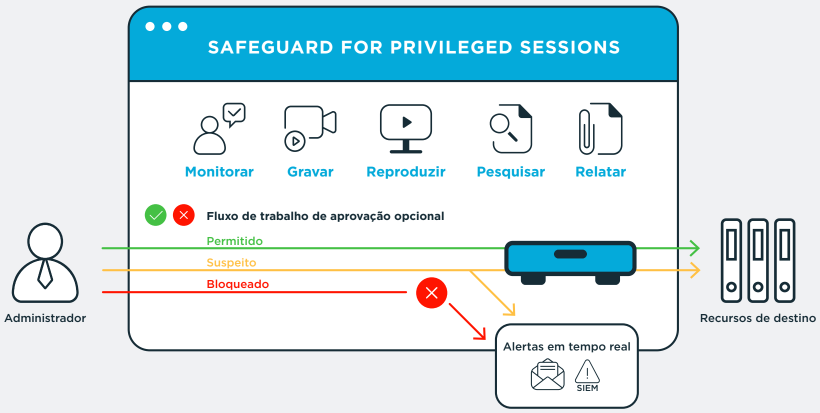
- Reduzir o risco de uma violação de segurança ao controlar o acesso a ativos de TI confidenciais
- Atender facilmente aos requisitos de conformidade para monitorar acessos privilegiados
- Obter valor mais rapidamente com implementação e gerenciamento simples
- Manter os administradores felizes ao permitir o uso de ferramentas familiares para administrar sistemas
- Aumentar a produtividade com uma pequena curva de aprendizado e design de IU elegante
- Reduzir os esforços dos relatórios de auditoria com acesso rápido a todas as informações necessárias
- Controlar o acesso a qualquer tipo de sistema graças a um design sem agente e independente de host
- Acelerar a resposta a incidentes por meio de uma pesquisa rápida de texto completo em sessões gravadas

Introdução

A concessão de acesso privilegiado não controlado a administradores internos, fornecedores terceirizados, contratantes e prestadores de serviços pode criar riscos significativos. Isso abre a porta para invasores que sequestram contas privilegiadas e administradores invasores. O infeliz - e caro - impacto desse tipo de risco tem sido demonstrado repetidas vezes por incidentes recentes e altamente divulgados. Para obter segurança e conformidade verdadeiras, você deve fazer mais do que simplesmente controlar contas de usuários com privilégios. Você deve monitorar e gravar o que eles fazem com o acesso privilegiado

Com o One Identity Safeguard for Privileged Sessions, você pode controlar, monitorar e gravar sessões privilegiadas de administradores, fornecedores remotos e outros usuários de alto risco. O conteúdo das sessões gravadas é indexado para simplificar a busca por eventos, além de ajudar a automatizar os relatórios para atender facilmente aos requisitos de auditoria e conformidade.

O Safeguard for Privileged Sessions também serve como um proxy para inspecionar o tráfego do protocolo no nível da aplicação. Isso cria um escudo eficaz contra ataques ao rejeitar todo o tráfego que viola o protocolo. De modo claro, são necessárias alterações mínimas em sua rede e os usuários não precisam alterar seu fluxo de trabalho ou aplicações clientes atuais, o que torna a implementação mais fácil. Entretanto, as regras de fluxo de trabalho podem ser configuradas para serem mais rigorosas, inclusive ao exigir a autorização prévia do usuário, limitar o acesso a recursos específicos e receber alertas se as conexões excederem os limites de tempo predefinidos. O Safeguard também pode monitorar sessões em tempo real e executar várias ações: se um comando ou aplicação arriscado for exibido, o One Identity Safeguard poderá enviar um alerta ou encerrar a sessão imediatamente.



Grave e monitore todos os acessos privilegiados

Com pesquisa de texto completo, alertas e bloqueios em tempo real, o Safeguard reduz o risco, ao mesmo tempo que facilita o cumprimento dos requisitos de conformidade.

Recursos

Auditoria, registro e reprodução da sessão inteira

Toda a atividade da sessão – até o pressionamento de tecla individual, movimento do mouse e janelas visualizadas – é capturada, indexada e armazenada em trilhas de auditoria invioláveis que podem ser visualizadas como um vídeo e pesquisadas como um banco de dados. As equipes de segurança podem pesquisar eventos específicos em todas as sessões e reproduzir a gravação a partir do local exato em que os critérios de pesquisa foram identificados. As trilhas de auditoria são criptografadas, com registro de data e hora e assinadas criptograficamente para propósitos forenses e de conformidade.

Alertas e bloqueios em tempo real

Monitora o tráfego em tempo real e executa várias ações se um determinado padrão for exibido na linha de comando ou na tela. Padrões predefinidos podem ser um comando ou texto arriscado em um protocolo orientado por texto ou um título de janela suspeito em uma conexão gráfica. Ao detectar uma ação suspeita do usuário, o Safeguard pode registrar o evento, enviar um alerta ou encerrar imediatamente a sessão.

Dois modos de operação

Escolha o modo adequado às suas necessidades.

- **Workflow Engine:** um mecanismo de fluxo de trabalho que oferece suporte a restrições de tempo, revisores, múltiplos aprovadores, acesso de emergência e expiração da política. Ele também inclui a capacidade de inserir códigos de motivo e/ou integrar-se diretamente a sistemas de emissão de tíquetes. Uma solicitação de senha pode ser aprovada automaticamente ou exigir qualquer nível de aprovação.
- **Instant On:** implemente no modo transparente para que não sejam necessárias alterações nos fluxos de trabalho do usuário. Ele pode atuar como um proxy gateway que opera como um roteador na rede - invisível para o usuário e para o servidor. Os administradores podem continuar a usar aplicações clientes conhecidas, além de acessar servidores e sistemas de destino sem qualquer interrupção em sua rotina diária.

Utilize proxy para conceder acesso

Como os usuários não têm acesso direto aos recursos, a empresa está protegida contra acesso não autorizado e irrestrito a dados e sistemas confidenciais. O Safeguard for Privileged Sessions pode usar proxy e gravar em muitos recursos de destino, inclusive UNIX/Linux, Windows, dispositivos de rede, firewalls, roteadores e muito mais.

Comando e controle de aplicações

O Safeguard for Privileged Sessions oferece suporte à lista branca e negra de comandos e títulos de janelas.

Trabalhe do jeito que você quiser

Mesmo quando o fluxo de trabalho está ativado, os administradores podem escolher seus clientes, ferramentas e preferências ao acessar sessões privilegiadas. Isso cria uma solução simples que oferece o acesso necessário aos administradores, ao mesmo tempo que atende aos regulamentos de segurança e conformidade.

Pesquisa de texto completo

Com seu mecanismo de Reconhecimento Óptico de Caracteres (OCR), os auditores podem realizar pesquisas de texto completo para ambos os comandos e qualquer texto visto pelo usuário no conteúdo das sessões. Ele pode até mesmo listar operações de arquivos e extrair arquivos transferidos para análise. A capacidade de pesquisar conteúdo de sessão e metadados acelera e simplifica a análise forense e a solução de problemas de TI.

Login automático

Com a funcionalidade de injeção de senha, o acesso pode ser configurado para login automático, o que aumenta a segurança e a conformidade sem nunca expor a senha ao usuário.

Amplo suporte a protocolos

Suporte total para protocolos SSH, Telnet, RDP, HTTP (s), ICA e VNC. Além disso, as equipes de segurança podem decidir quais serviços de rede (por exemplo, transferência de arquivos, acesso ao shell, etc.) que desejam ativar/desativar para administradores nos protocolos.

Instant off

Ao agir como um firewall virtual, o One Identity Safeguard aumenta a proteção dos servidores ao encerrar acessos questionáveis ou mal-intencionados quase que instantaneamente. Além de evitar a configuração incorreta acidental e outros erros humanos, a solução oferece suporte ao princípio de autorização dos "quatro olhos" sob o qual o administrador de monitoramento pode encerrar a sessão a qualquer momento.

Queda na implementação

Com uma implementação rápida baseada em appliance e roteamento de tráfego simplificado, o One Identity Safeguard pode fazer com que você grave sessões em questão de dias sem interromper seus usuários.

Pronto para análise

Colete todas as informações necessárias para analisar usuários e comportamentos privilegiados e detectar ameaças internas e externas.

Acesso seguro para sistemas legados

Use o Smart Card, 2FA ou outros métodos eficientes de autenticação para conceder acesso seguro aos sistemas. Uma vez que o Safeguard atua como um proxy gateway para o sistema, ele permite uma forte autenticação a destinos que não aceitam ou não oferecem suporte a esses métodos de forma nativa.

A abordagem do One Identity ao gerenciamento de acesso privilegiado

O portfólio One Identity inclui o conjunto mais abrangente do setor de soluções de gerenciamento de acesso privilegiado. Você pode aproveitar a eficiente funcionalidade de gerenciamento de sessões do Safeguard for Privileged Sessions com nossas soluções de análise seguras e privilegiadas de senha privilegiada. Nossa oferta de produtos inclui soluções para delegação granular da conta raiz do UNIX e da conta de administrador do Active Directory; suplementos para preparar o sudo de código aberto para a empresa e registros de pressionamento de tecla para atividades raiz do Unix. Tudo isso é firmemente integrado à solução de ponte do Active Directory líder do setor.

Sobre o One Identity

O One Identity ajuda as organizações a obter o melhor Gerenciamento de Identidades e Acessos (IAM). Com a nossa combinação exclusiva de ofertas, inclusive um portfólio de soluções de governança de identidades, gerenciamento de acessos, gerenciamento privilegiado e identidade como serviço, as organizações podem alcançar total potencial, sem obstáculos de segurança e protegidas contra ameaças. Saiba mais em OneIdentity.com