FOLHETO

One Identity Safeguard

Armazene, gerencie, grave e analise o acesso privilegiado com segurança

Benefícios

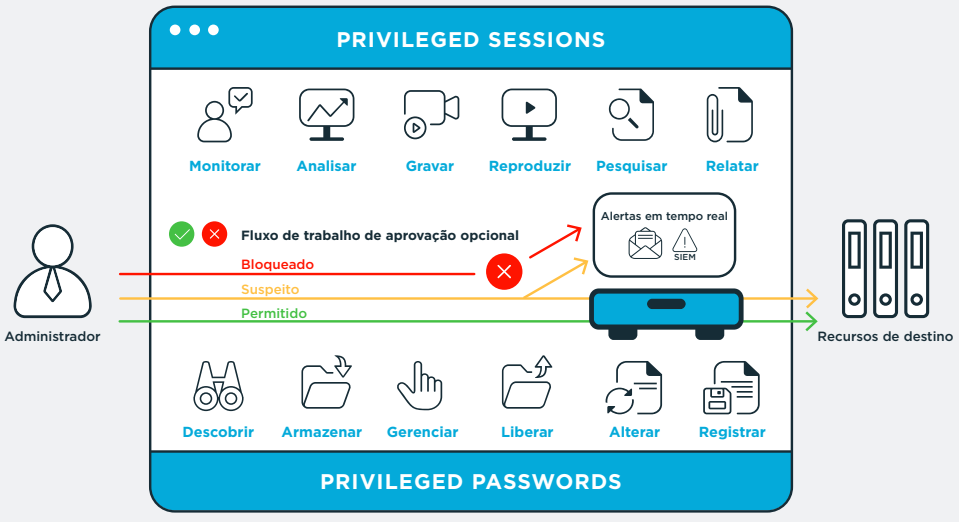
- Reduzir os possíveis danos de violações de segurança
- Atender aos requisitos de conformidade
- ROI rápido com implementação e gerenciamento simplificados
- Criação eficiente de relatórios de auditoria
- Identificar usuários privilegiados de alto risco, comportamentos arriscados e eventos incomuns
- Simplificar o gerenciamento de contas privilegiadas

Introdução

Os hackers evoluem continuamente os métodos usados para obter acesso aos seus sistemas e dados. Por fim, eles querem acessar suas contas privilegiadas. Em quase todas as violações recentes de alto perfil, as contas privilegiadas foram comprometidas para obter acesso a sistemas e dados críticos. Você pode limitar os danos causados por uma violação ao implementar soluções que forneçam uma maneira segura, eficiente e compatível de acessar contas privilegiadas.

Para os gerentes de TI, essas contas com todo o acesso são difíceis de gerenciar por diversos motivos, inclusive o grande número de contas privilegiadas e o número de pessoas que têm acesso a elas. No topo desses desafios, as soluções tradicionais de gerenciamento de acesso privilegiado (PAM) envolvem arquiteturas complexas, tempos de implementação demorados e requisitos de gerenciamento dispendiosos.

Sim, o PAM pode ser um enorme desafio, mas ele não precisa ser. O One Identity Safeguard é uma solução integrada que combina uma segurança protegida por senha e uma solução de gerenciamento e monitoramento de sessões com detecção e análise de ameaças. Ele armazena, gerencia, grava e analisa o acesso privilegiado com segurança.



Acesso privilegiado seguro sem sacrifício

Não enfrente problemas para proteger suas contas privilegiadas ao armazenar, gerenciar, gravar e analisar com segurança o acesso privilegiado, ao mesmo tempo que atende aos administradores e auditores com o One Identity Safeguard.

Safeguard for Privileged Passwords

O One Identity Safeguard for Privileged Passwords automatiza, controla e protege o processo de concessão de credenciais privilegiadas com fluxos de trabalho automáticos e gerenciamento de acessos baseado em função. O design centrado no usuário do Safeguard for Privileged Passwords significa uma curva de aprendizado reduzida. Além disso, a solução permite que você gerencie as senhas de qualquer lugar com o uso de praticamente qualquer dispositivo. O resultado é uma solução que protege a sua empresa e oferece aos seus usuários privilegiados um novo nível de liberdade e funcionalidade.

Safeguard for Privileged Sessions

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, o que facilita a localização posterior de eventos de sessão e ajuda a simplificar e automatizar os relatórios. Ambas as funcionalidades facilitam os requisitos de auditoria e conformidade. Além disso, o Safeguard for Privileged Sessions funciona como um proxy, inspeciona o tráfego do protocolo no nível da aplicação e pode rejeitar qualquer tráfego que viole o protocolo, o que o torna um escudo eficaz contra ataques.

Safeguard for Privileged Analytics

Com o One Identity Safeguard for Privileged Analytics, você pode colocar a análise de comportamento do usuário para trabalhar para você e saber quais usuários privilegiados apresentam mais riscos, descobrir ameaças internas e externas anteriormente desconhecidas e localizar e interromper atividades suspeitas. O Safeguard for Privileged Analytics classifica o nível de risco potencial das ameaças para que você possa priorizar sua resposta (tomar medidas imediatas sobre as ameaças mais iminentes) e, por fim, evitar violações de dados.

Recursos

Controle de liberação baseado em políticas

Com o uso de um navegador da Web seguro que ofereça suporte para dispositivos móveis, você pode solicitar acesso e fornecer aprovação para sessões e senhas privilegiadas. As solicitações podem ser aprovadas automaticamente ou precisar de aprovações duplas/múltiplas com base na política da sua organização. Portanto, se as suas políticas considerarem a identidade e o nível de acesso do solicitante, a hora e o dia da tentativa de solicitação e o recurso específico solicitado, ou todos eles, você poderá configurar o One Identity Safeguard para atender às suas necessidades personalizadas. Além disso, você pode inserir códigos de motivo e/ou integrá-los com sistemas de tíquetes.

Auditoria, registro e reprodução da sessão inteira

Toda a atividade da sessão – até o pressionamento de tecla, 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 ocorreram. As trilhas de auditoria são criptografadas, com registro de data e hora e assinadas criptograficamente para propósitos forenses e de conformidade.

Controle de alterações

Oferece suporte ao controle de alteração granular e configurável de credenciais compartilhadas, inclusive baseado em tempo e último uso, além de alteração manual ou forçada.

Biometria comportamental do usuário

Cada usuário tem o próprio padrão de comportamento idiossincrático, mesmo ao executar ações idênticas, como digitar ou mover um mouse. Os algoritmos incorporados no Safeguard for Privileged Analytics inspecionam essas características comportamentais (capturadas pelo Safeguard for Privileged Sessions). A dinâmica do pressionamento de teclas e a análise do movimento do mouse ajudam a identificar violações e também servem como uma autenticação biométrica contínua.

Aprovação em qualquer lugar

Com a Autenticação por dois fatores do One Identity Starling, você pode aprovar ou recusar solicitações de qualquer lugar e com praticamente qualquer dispositivo sem estar na VPN.

Favoritos

Acesse rapidamente as senhas mais utilizadas diretamente da tela de login. Você pode agrupar várias solicitações de senha em um único favorito para ter acesso a todas as contas necessárias com um único clique.

Descoberta

Descubra rapidamente os sistemas ou as contas privilegiadas na sua rede com opções de host, diretório e descoberta de rede.

Alertas e bloqueios em tempo real

O Safeguard for Privileged Sessions 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.

Identifique os usuários arriscados

O Safeguard avalia as concessões de direitos em relação às regras de classificação de risco para identificar contas de alto risco. São enviadas notificações proativas quando as alterações a concessões de direitos movem um perfil de usuário para um status de alto risco. Isso elimina o risco de direitos desnecessários ou inativos antes que alguém possa abusar ou explorá-los.

Comando e controle de aplicações

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

Instant on

O Safeguard for Privileged Sessions pode ser implementado no modo transparente sem exigir alterações nos fluxos de trabalho do usuário. Ao atuar como um proxy gateway, o Safeguard pode operar como um roteador na rede, invisível para o usuário e para o servidor. Os administradores podem usar as aplicações clientes com as quais estão familiarizados e acessar servidores e sistemas de destino sem qualquer interrupção em sua rotina diária.

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.

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.

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.

API RESTful

O Safeguard utiliza uma API modernizada com base no REST para conectar-se com outros aplicativos e sistemas. Cada função é exposta por meio da API para permitir uma integração rápida e fácil, independentemente do que você deseja fazer e da linguagem em que suas aplicações foram gravadas.

Assinatura híbrida do One Identity

Expanda os recursos do Safeguard com a Assinatura híbrida do One Identity que oferece acesso imediato aos recursos e serviços fornecidos pela nuvem. Eles incluem todos os recursos da Autenticação de dois fatores Starling para proteger o acesso ao Safeguard, além da análise de identidade e inteligência de risco Starling para o Safeguard para que você possa detectar preventivamente usuários e direitos de risco. Uma única assinatura permite todas as implementações da solução One Identity.

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 os recursos do One Identity Safeguard com 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