FICHE TECHNIQUE

Safeguard for Sudo

Développer et améliorer Sudo grâce à une gestion centralisée

Avantages

- Améliore l'efficacité et la cohérence des stratégies grâce à la gestion centralisée de sudo sur tous vos serveurs Unix/Linux
- Renforce la sécurité en enregistrant et rapportant toutes les activités de frappes clavier sudo
- Simplifie le respect des exigences en matière de conformité et d'audit en fournissant des rapports de contrôle d'accès et d'activité des utilisateurs
- Simplifie la gestion administrative en utilisant une console unique et pratique pour gérer sudo, Active Directory et la délégation root de l'organisation

Aperçu du contenu

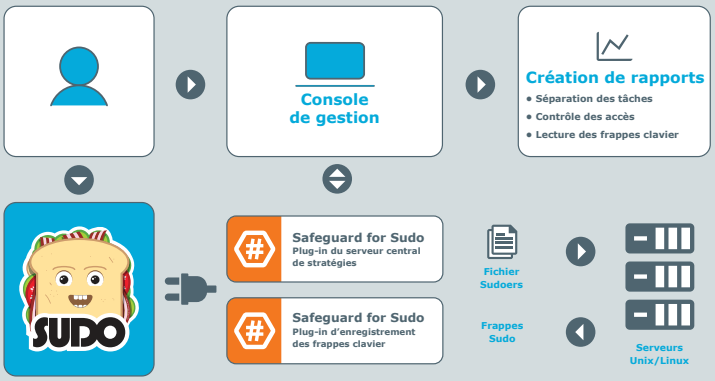
La grande majorité des organisations Unix/Linux utilisent le projet open-source sudo pour aider à déléguer le compte root Unix afin d'atteindre les objectifs de gestion des comptes à privilèges. Sudo a déjà prouvé sa valeur. Cependant, la gestion de sudo peut se révéler fastidieuse. La stratégie de sudo est souvent écrite et exécutée de façon incohérente sur plusieurs serveurs, et sudo ne permet pas de contrôler les accès et les activités des super utilisateurs, pourtant si importants en matière de sécurité et de conformité.

L'outil Safeguard for Sudo aide les organisations utilisant Unix ou Linux à faire évoluer la gestion des comptes à privilèges par le biais de sudo. Les plug-ins de Safeguard for Sudo améliorent sudo 1.8.1 (et versions plus récentes) en fournissant un serveur central de stratégies, une gestion centralisée de sudo et des dossiers de stratégies des sudoers, des rapports centralisés sur les droits d'accès et les activités des sudoers ainsi que l'enregistrement des frappes clavier de toutes les activités effectuées via sudo.

Safeguard for Sudo peut être utilisé pour l'administration de sudo sur quelques dizaines, centaines ou milliers de serveurs Unix/Linux de façon simple, intuitive et cohérente. Ce système permet de supprimer la gestion au cas par cas de sudo, à l'origine de tant d'inefficacités et d'incohérences, et permet aux organisations de voir réellement qui fait quoi avec sudo. Et comme Safeguard for Sudo améliore sudo au lieu de le remplacer, les utilisateurs finaux et les administrateurs n'ont pas besoin de se former à nouveau, ce qui se traduit par une diminution du nombre d'appels au service d'assistance et un délai de rentabilisation plus court. De plus, l'approche centralisée permet de rendre compte des activités et de la stratégie de sudo (sudoers) ou encore de modifier l'historique des sudoers, ce qui simplifie le contrôle des accès et la création de rapports d'audit et de conformité. Enfin, un plug-in séparé étend l'administration centralisée de sudo pour inclure également l'enregistrement des frappes clavier avec des capacités de recherche et de lecture.

Renforcez la sécurité et gagnez en efficacité

Safeguard for Sudo enrichit sudo grâce à un serveur central de stratégies et à des plug-ins d'enregistrement des frappes clavier qui renforcent la sécurité et optimisent l'efficacité.



Fonctionnalités

Extensions de sudo

Améliorez sudo avec de nouvelles capacités en utilisant des plug-ins (serveur central de stratégies et enregistrement des frappes clavier) qui intègrent et étendent le cadre modulaire de sudo.

Stratégie sudo centrale

Utilisez un service central pour appliquer la stratégie sur l'ensemble de vos serveurs UNIX/Linux. Les administrateurs n'ont donc plus besoin de gérer le déploiement des sudoers sur chaque système, ce qui améliore la sécurité et réduit la charge administrative.

Rapports centralisés

Découvrez les différentes modifications opérées aux sudoers, leurs auteurs et leurs dates, y compris la gestion des versions et la possibilité de revenir à une version antérieure. Vous pouvez savoir quelles ont été les modifications apportées au fichier de stratégie sudo, à quelle date et par qui. Vous pouvez également découvrir quel utilisateur a utilisé telle ou telle commande acceptée ou rejetée sur l'ensemble des systèmes gérés.

Aucune formation nécessaire

Évitez les sessions de formation et réduisez le nombre d'appels au service d'assistance. Safeguard for Sudo étend les capacités de sudo, permettant aux utilisateurs de tirer profit de leurs connaissances actuelles et d'obtenir des délais de rentabilisation plus courts. D'autres solutions nécessitent l'apprentissage de nouvelles commandes et d'une nouvelle syntaxe, ce qui augmente le nombre de formations et d'appels au service d'assistance.

Enregistrement des frappes

Suivi des frappes clavier pour les administrateurs effectuant des actions via sudo. Le plug-in d'enregistrement des frappes pour Safeguard for Sudo fournit un journal complet des activités réalisées et des commandes exécutées sur l'ensemble des systèmes. Plusieurs filtres peuvent être appliqués au rapport afin de vous aider à trouver rapidement les données dont vous avez besoin. Vous pouvez par exemple appliquer un filtre sur des commandes spécifiques ou voir les commandes exécutées sur une période donnée.

Gestion centralisée

Utilisez la solution Management Console for Unix afin de gérer sudo ainsi que d'autres solutions One Identity. Les tâches d'administration et d'audit sont grandement simplifiées sur l'ensemble de votre environnement UNIX.

Application de la séparation des responsabilités

À l'aide de la solution Management Console for Unix, vous pouvez appliquer la séparation des responsabilités et attribuer aux utilisateurs un rôle spécifique leur permettant d'exécuter uniquement un ensemble défini de tâches.

Mise en cache hors connexion de la stratégie sudo

Cette fonctionnalité permet d'assurer la continuité des services en cas de panne de serveur ou de panne réseau.

Compatibilité des scripts

Assurez la compatibilité avec les fichiers de script existants comprenant des commandes sudo intégrées. D'autres solutions de gestion privilégiée utilisent des commandes et une syntaxe différentes, entraînant l'échec d'exécution des scripts existants et des coûts potentiellement élevés pour tester et réparer les scripts sur plusieurs systèmes Unix.

À propos de One Identity

One Identity, une entité Quest, aide les organisations à mettre en place une stratégie de sécurité axée sur les identités, aussi bien sur site, dans le Cloud ou dans un environnement hybride. Avec notre vaste portefeuille intégré d'offres de gestion des identités, comprenant la gestion des comptes, l'administration et la gouvernance des identités, ainsi que la gestion des accès à privilèges, les organisations peuvent réaliser tout leur potentiel et bénéficier d'une sécurité efficace grâce à une stratégie axée sur les identités, qui assure un accès adéquat à tous les types d'utilisateurs, tous les systèmes et toutes les données. En savoir plus sur le site OneIdentity.com

Datasheet_2020_PrivilegedMgrSUDO_RS_60268

Safeguard for Privileged Sessions

Réduisez les risques en contrôlant, surveillant et enregistrant les privilèges d'accès

Avantages

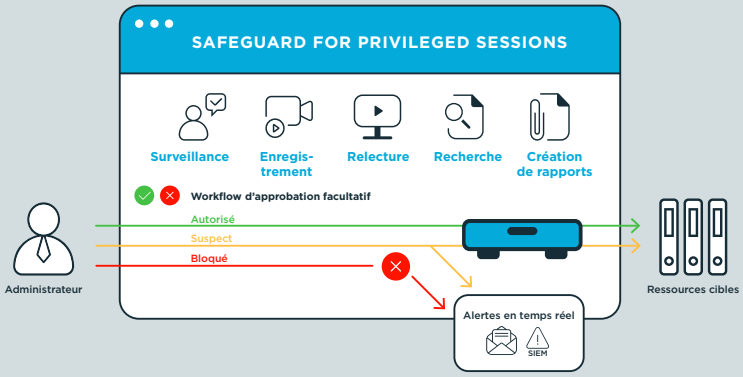
- Réduction du risque lié à une violation de sécurité en contrôlant les accès aux actifs informatiques sensibles
- Simplification du respect des exigences de conformité pour la surveillance des comptes à privilèges
- Accélération du retour sur investissement avec le déploiement et la gestion simplifiés
- Satisfaction des administrateurs avec la possibilité d'utiliser des outils familiers pour gérer les systèmes
- Optimisation de la productivité avec une courbe d'apprentissage réduite et une conception d'interface utilisateur élégante
- Réduction des efforts de génération de rapports d'audit avec l'accès rapide à toutes les informations nécessaires
- Suivi de l'accès à tous les types de systèmes grâce à une conception sans agent indépendante de l'hôte
- Accélération de la réponse aux incidents avec la possibilité d'effectuer des recherches rapides en texte intégral dans les sessions enregistrées

Introduction

L'octroi d'un accès à privilèges non contrôlé aux administrateurs internes, aux fournisseurs tiers, aux sous-traitants et aux prestataires de services peut engendrer des risques importants. Les comptes à privilèges peuvent en effet être détournés par des pirates ou exploités à mauvais escient par des administrateurs malhonnêtes. Les conséquences, qui peuvent être déplorables et coûteuses, ont été maintes fois démontrées avec les récents incidents fortement médiatisés. Pour bénéficier d'une sécurité et d'une conformité totale, vous devez aller au-delà du simple contrôle des comptes d'utilisateurs à privilèges en surveillant et enregistrant ce qu'ils font de leur accès à privilèges.

One Identity Safeguard for Privileged Sessions de Quest vous permet de contrôler, surveiller et enregistrer les sessions des administrateurs, des fournisseurs distants et des utilisateurs à haut risque qui bénéficient d'un accès à privilèges. Le contenu des sessions enregistrées est indexé afin de simplifier la recherche d'événements et la création de rapports et vous permettre de satisfaire aux exigences d'audit et de conformité.

La solution Safeguard for Privileged Sessions peut également être utilisée en tant que proxy. Elle inspecte le trafic de protocoles au niveau des applications et peut refuser tout trafic violant un protocole, constituant ainsi un bouclier efficace contre les attaques. En mode transparent, seuls des changements réseau mineurs sont requis et les utilisateurs n'ont pas besoin de modifier leur workflow actuel ou leurs applications clientes. L'implémentation est donc extrêmement simple. Toutefois, des règles de workflow plus strictes peuvent être configurées pour exiger l'autorisation préalable des utilisateurs, limiter l'accès à des ressources spécifiques et recevoir des alertes si des connexions excèdent une durée prédéfinie. Safeguard peut également surveiller les sessions en temps réel et exécuter diverses opérations : si une commande ou une application dangereuse apparaît, One Identity Safeguard peut vous envoyer une alerte ou immédiatement interrompre la session.



Enregistrement et surveillance des accès à privilèges

Avec la recherche en texte intégral et les alertes et blocages en temps réel, Safeguard vous permet de réduire les risques tout en facilitant l'application des exigences de conformité.

Safeguard for Privileged Sessions

Réduisez les risques en contrôlant, surveillant et enregistrant les privilèges d'accès

Avantages

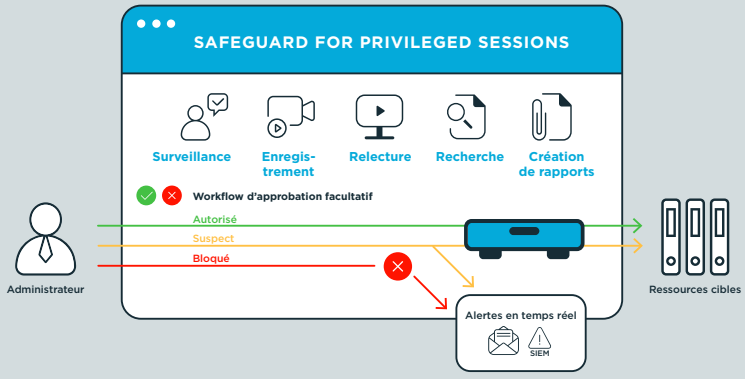
- Réduction du risque lié à une violation de sécurité en contrôlant les accès aux actifs informatiques sensibles
- Simplification du respect des exigences de conformité pour la surveillance des comptes à privilèges
- Accélération du retour sur investissement avec le déploiement et la gestion simplifiés
- Satisfaction des administrateurs avec la possibilité d'utiliser des outils familiers pour gérer les systèmes
- Optimisation de la productivité avec une courbe d'apprentissage réduite et une conception d'interface utilisateur élégante
- Réduction des efforts de génération de rapports d'audit avec l'accès rapide à toutes les informations nécessaires
- Suivi de l'accès à tous les types de systèmes grâce à une conception sans agent indépendante de l'hôte
- Accélération de la réponse aux incidents avec la possibilité d'effectuer des recherches rapides en texte intégral dans les sessions enregistrées

Introduction

L'octroi d'un accès à privilèges non contrôlé aux administrateurs internes, aux fournisseurs tiers, aux sous-traitants et aux prestataires de services peut engendrer des risques importants. Les comptes à privilèges peuvent en effet être détournés par des pirates ou exploités à mauvais escient par des administrateurs malhonnêtes. Les conséquences, qui peuvent être déplorables et coûteuses, ont été maintes fois démontrées avec les récents incidents fortement médiatisés. Pour bénéficier d'une sécurité et d'une conformité totale, vous devez aller au-delà du simple contrôle des comptes d'utilisateurs à privilèges en surveillant et enregistrant ce qu'ils font de leur accès à privilèges.

One Identity Safeguard for Privileged Sessions de Quest vous permet de contrôler, surveiller et enregistrer les sessions des administrateurs, des fournisseurs distants et des utilisateurs à haut risque qui bénéficient d'un accès à privilèges. Le contenu des sessions enregistrées est indexé afin de simplifier la recherche d'événements et la création de rapports et vous permettre de satisfaire aux exigences d'audit et de conformité.

La solution Safeguard for Privileged Sessions peut également être utilisée en tant que proxy. Elle inspecte le trafic de protocoles au niveau des applications et peut refuser tout trafic violant un protocole, constituant ainsi un bouclier efficace contre les attaques. En mode transparent, seuls des changements réseau mineurs sont requis et les utilisateurs n'ont pas besoin de modifier leur workflow actuel ou leurs applications clientes. L'implémentation est donc extrêmement simple. Toutefois, des règles de workflow plus strictes peuvent être configurées pour exiger l'autorisation préalable des utilisateurs, limiter l'accès à des ressources spécifiques et recevoir des alertes si des connexions excèdent une durée prédéfinie. Safeguard peut également surveiller les sessions en temps réel et exécuter diverses opérations : si une commande ou une application dangereuse apparaît, One Identity Safeguard peut vous envoyer une alerte ou immédiatement interrompre la session.



Enregistrement et surveillance des accès à privilèges

Avec la recherche en texte intégral et les alertes et blocages en temps réel, Safeguard vous permet de réduire les risques tout en facilitant l'application des exigences de conformité.