FICHE TECHNIQUE

One Identity Safeguard

Stockez, gérez, enregistrez et analysez les accès à privilèges en toute sécurité

Avantages

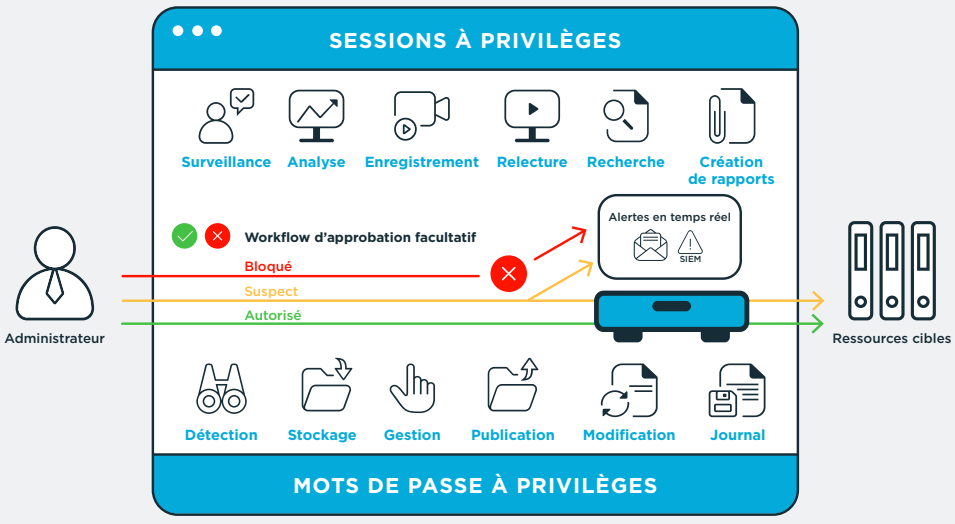
- Réduction des dommages potentiels dus à des failles de sécurité
- Respect des exigences en termes de conformité
- Accélération du retour sur investissement avec un déploiement et une gestion simplifiés
- Création efficace de rapports d'audits
- Identification des utilisateurs à privilèges représentent un risque élevé, des comportements à risques et des événements inhabituels
- Gestion simplifiée des comptes à privilèges

Introduction

Les méthodes employées par les pirates pour accéder à vos systèmes et vos données sont en constante évolution, leur but ultime étant d'accéder à vos comptes à privilèges. Dans la quasi-totalité des attaques de grande envergure, ce sont les comptes à privilèges qui ont été corrompus afin d'accéder aux systèmes et données stratégiques. Vous pouvez limiter les dommages lors d'une attaque en déployant des solutions assurant un moyen sécurisé, efficace et conforme de fourniture d'accès aux comptes à privilèges.

Pour les responsables des équipes informatiques, ces comptes à accès total sont difficiles à gérer pour plusieurs raisons, notamment la multitude de comptes à privilèges et le nombre d'utilisateurs ayant besoin d'y accéder. En plus de ces défis, les solutions classiques de gestion des accès à privilèges (PAM) impliquent des architectures complexes, des déploiements sur de longues durées et des exigences de gestion onéreuses.

Effectivement, la gestion des accès à privilèges peut présenter un défi monumental, mais il existe une solution. La solution One Identity Safeguard comprend un coffre-fort de mots de passe sécurisé et robuste, associé à des fonctions de gestion et de surveillance des sessions, de détection des menaces et d'analyse. Elle vous permet de stocker, de gérer, d'enregistrer et d'analyser les accès à privilèges en toute sécurité.



Sécurisation des accès à privilèges sans sacrifice

Protégez vos comptes à privilèges en toute sérénité en stockant, gérant, enregistrant et analysant les accès à privilèges de façon sécurisée tout en répondant aux exigences des auditeurs et des administrateurs avec la solution One Identity Safeguard.

Safeguard for Privileged Passwords

One Identity Safeguard for Privileged Passwords automatise, contrôle et sécurise le processus d'octroi d'informations d'identification privilégiées avec une gestion des accès basée sur les rôles et des workflows automatisés. La conception orientée sur l'utilisateur de Safeguard for Privileged Password permet de réduire l'apprentissage nécessaire pour son utilisation. En outre, la solution vous permet de gérer les mots de passe où que vous soyez et à partir de quasiment tout type d'appareil. Résultat : une solution qui sécurise votre entreprise et offre une liberté et une fonctionnalité accrues à vos utilisateurs privilégiés.

Safeguard for Privileged Sessions

One Identity Safeguard for Privileged Sessions 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 simple et automatique de rapports, et vous permettre ainsi de satisfaire aux exigences d'audit et de conformité. De plus, la solution Safeguard for Privileged Sessions peut 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.

Safeguard for Privileged Analytics

One Identity Safeguard for Privileged Analytics vous permet d'exploiter des analyses comportementales des utilisateurs et d'identifier les utilisateurs à privilèges qui représentent les plus grands risques. La solution vous permet également de découvrir des menaces internes et externes jusque-là inconnues et de mettre fin aux activités suspectes. Safeguard for Privileged Analytics classe les menaces selon leur niveau de risque potentiel pour que vous puissiez établir des priorités et prendre des mesures adéquates, et empêche la violation de données.

Fonctionnalités

Contrôle des versions basé sur des stratégies

Vous pouvez faire une demande d'accès et fournir les approbations pour les mots de passe et session à privilèges à partir d'un navigateur Internet sécurisé prenant en charge les appareils mobiles. Les demandes peuvent être approuvées automatiquement ou nécessiter deux approbations ou plus, selon la stratégie suivie par votre entreprise. Que vos stratégies tiennent compte de l'identité du demandeur et de son niveau d'accès, de l'heure et du jour de la demande, de la ressource demandée, ou encore de tous ces facteurs à la fois, vous pouvez configurer One Identity Safeguard pour qu'il réponde à vos besoins spécifiques. Vous pouvez également entrer des codes de motif et/ou intégrer la solution avec les systèmes de ticket.

Audit, enregistrement et relecture de sessions complètes

L'ensemble des activités de la session (frappes, mouvements de la souris et fenêtres affichées) est enregistré, indexé et stocké dans des pistes d'audit inviolables qui peuvent être lues comme une vidéo et consultées comme une base de données. Les équipes chargées de la sécurité peuvent rechercher certains événements dans des sessions et lire l'enregistrement à partir du moment précis où le critère de recherche apparaît. Les pistes d'audit sont chiffrées, horodatées et cryptographiquement signées à des fins d'analyse forensique et de conformité.

Contrôle des modifications

Il offre un contrôle des modifications granulaire et paramétrable des accès partagés sur la base de l'heure, de la dernière utilisation et du fait qu'il s'agisse d'une modification forcée ou manuelle.

Biométrie comportementale des utilisateurs

Chaque utilisateur présente un schéma comportemental caractéristique, même lorsqu'il s'agit d'actions communes à tous les utilisateurs, comme la saisie au clavier ou le déplacement de la souris. Les algorithmes intégrés à Safeguard for Privileged Analytics examinent les caractéristiques comportementales capturées par Safeguard for Privileged Sessions. L'analyse des schémas de frappe et des déplacements de la souris vous aident à identifier les violations, et permettent également d'assurer une authentification biométrique continue.

Approbation en tout lieu

L'authentification à deux facteurs de la solution One Identity Starling vous permet d'approuver ou de refuser des demandes où que vous soyez, même si vous n'êtes pas connecté au réseau VPN.

Favoris

Accédez rapidement aux mots de passe que vous utilisez le plus fréquemment directement dans l'écran de connexion. Vous pouvez regrouper plusieurs demandes de mot de passe dans un seul favori de manière à accéder à tous vos comptes en un seul clic.

Détection

Détectez rapidement tous les comptes ou systèmes à privilèges sur votre réseau avec les options de détection d'hôte, d'annuaire et de réseau.

Alertes et blocage et en temps réel

Safeguard for Privileged Sessions surveille le trafic en temps réel et exécute diverses opérations si un schéma spécifique apparaît dans la ligne de commande ou sur l'écran. Les schémas prédéfinis peuvent comprendre une commande dangereuse ou du texte dans un protocole orienté texte, ou un nom de fenêtre suspect dans une connexion graphique. Si une action suspecte d'un utilisateur est détectée, Safeguard peut consigner l'événement dans le journal, envoyer une alerte ou immédiatement interrompre la session.

Identification des utilisateurs à risques

Safeguard évalue les droits par rapport aux règles de classification par risque afin d'identifier les comptes présentant des risques élevés. Des notifications proactives sont envoyées en cas de modification des droits d'un utilisateur dont le profil passe à un niveau de haut risque. Ceci permet d'éliminer les risques liés aux droits inutiles ou inactifs avant qu'ils soient exploités ou fassent l'objet d'une utilisation inappropriée.

Contrôle des commandes et des applications

Safeguard for Privileged Sessions prend en charge la création de listes blanches et noires des commandes et des noms de fenêtres.

Solution prête à l'emploi

La solution Safeguard for Privileged Sessions peut être déployée en mode transparent, sans modifier les workflows des utilisateurs. Agissant comme une passerelle de proxy, la solution Safeguard fonctionne comme un routeur sur le réseau et est ainsi invisible pour les utilisateurs et le serveur. Les administrateurs peuvent continuer à utiliser les applications clientes qu'ils connaissent et peuvent accéder aux systèmes et serveurs cibles sans interrompre leurs activités quotidiennes.

Prise en charge étendue des protocoles

Prise en charge complète des protocoles SSH, Telnet, RDP, HTTP(s), ICA et VNC. De plus, les équipes chargées de la sécurité peuvent décider quels services réseau (transfert de fichiers, accès à l'interpréteur de commandes, etc.) doivent être activés/désactivés pour les administrateurs en fonction des protocoles.

Recherche en texte intégral

Le moteur de reconnaissance optique des caractères (OCR, Optical Character Recognition) permet aux auditeurs de rechercher du texte intégral dans les commandes et tous les textes consultés par les utilisateurs dans le contenu des sessions. Il peut même répertorier les opérations liées aux fichiers et extraire les fichiers transférés pour les examiner. La recherche dans les métadonnées et le contenu des sessions accélère et simplifie l'analyse forensique et le dépannage informatique.

Déploiement rapide

Avec un déploiement rapide basé sur l'appliance et une redirection du trafic simplifiée, la solution One Identity Safeguard vous permet d'enregistrer des sessions en quelques jours sans interruption pour les utilisateurs.

API REST

La solution Safeguard utilise une API modernisée basée sur REST pour se connecter à d'autres applications et systèmes. Chaque fonction est exposée via l'API afin de permettre une intégration simple et rapide, quoi que vous vouliez faire ou quelle que soit la langue dans laquelle vos applications sont écrites.

Abonnement One Identity hybride

Étendez les capacités de la solution Safeguard avec l'abonnement One Identity hybride, qui offre un accès immédiat aux fonctionnalités et aux services dans le Cloud. Vous pouvez bénéficier de l'offre Starling Two-Factor Authentication « tout compris » pour protéger l'accès à Safeguard et de l'offre Starling Identity Analytics & Risk Intelligence for Safeguard pour détecter de façon préventive les utilisateurs et les droits potentiellement dangereux. Un seul abonnement vous permet de déployer toutes les solutions One Identity.

L'approche One Identity de la gestion des accès à privilèges

La gamme One Identity comprend l'ensemble le plus complet de solutions de gestion des accès à privilèges. Vous pouvez tirer parti des fonctionnalités de One Identity avec des solutions conçues pour la délégation granulaire des comptes root UNIX et administrateur Active Directory ; des extensions pour que les commandes sudo open source répondent aux besoins des entreprises ; et l'enregistrement des frappes pour les activités root UNIX. Toutes ces fonctions sont étroitement intégrées avec la solution de pont Active Directory leader du marché.

À propos de One Identity

One Identity aide les entreprises à assurer une gestion réussie des accès et des identités. Grâce à notre combinaison unique d'offres, notamment une gamme de gestion des identités, de gestion des accès, de gestion des accès à privilèges, et des solutions d'identité « as a service » les entreprises peuvent réaliser leur potentiel sans être entravées par la sécurité et tout en étant protégées contre les menaces. En savoir plus sur le site OneIdentity.com