



FICHE TECHNIQUE

One Identity Safeguard On Demand

Solution fournie par SaaS pour stocker, gérer, enregistrer et analyser les accès à privilèges en toute sécurité

Avantages

- Réduisez les dommages potentiels dus à des failles de sécurité
- Respectez les exigences de conformité
- Accélérez le retour sur investissement avec un déploiement et une gestion simplifiés
- Créez des rapports d'audits efficacement
- Identifiez et interrompez les comportements à risques et les événements inhabituels
- Simplifiez la gestion des comptes à privilèges

Le Cloud sans compromis

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. Mais vous pouvez limiter les dommages en adoptant une solution à la demande qui offre un moyen sécurisé, efficace et conforme pour la gestion des comptes à privilèges.

Pour les responsables des équipes informatiques, les comptes d'administration qui bénéficient d'un accès complet 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 privilégiés (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. One Identity Safeguard On Demand est une solution fournie par SaaS qui associe un coffre-fort de mots de passe sécurisé et une solution de gestion et de surveillance des sessions avec la détection et l'analyse des menaces, le tout géré et fourni dans le Cloud.

Safeguard On Demand automatise, contrôle et sécurise le provisioning d'informations d'identification privilégiées avec une gestion des accès basée sur les rôles et des workflows automatisés. Avec sa conception orientée sur l'utilisateur, Safeguard On Demand permet de réduire l'apprentissage nécessaire pour son utilisation. En outre, cette solution flexible et pratique 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 On Demand vous permet également de contrôler, de surveiller et d'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 On Demand 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.

Par ailleurs, Safeguard On Demand vous permet d'exploiter les analyses comportementales des utilisateurs en découvrant des menaces internes et externes jusque-là inconnues et en mettant fin aux activités suspectes. Safeguard On Demand classe les menaces selon leur niveau de risque potentiel pour que vous puissiez établir des priorités, (prendre des mesures immédiates sur les menaces imminentes) et empêcher 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 sessions 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. Ainsi, 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 de tous les facteurs à la fois), vous pouvez configurer One Identity Safeguard On Demand de sorte à répondre 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.

Solution prête à l'emploi

La solution Safeguard On Demand peut être déployée en mode transparent sans modifier les workflows des utilisateurs. Agissant comme une passerelle de proxy, la solution Safeguard On Demand fonctionne comme un routeur sur le réseau, devenant 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.

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 On Demand inspectent ces caractéristiques comportementales. 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

One Identity Cloud Assistant vous permet d'approuver ou de refuser des demandes en tout lieu, à l'aide de n'importe quel appareil.

Coffre-fort de mots de passe personnel

Tous les salariés de votre organisation peuvent stocker et générer des mots de passe aléatoires pour les comptes professionnels non fédérés dans un coffre-fort de mots de passe personnel et gratuit. Votre organisation peut ainsi utiliser un outil approuvé qui permet de partager et de récupérer les mots de passe en toute sécurité, tout en offrant une protection indispensable et une visibilité sur les comptes professionnels.

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 On Demand 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 On Demand peut consigner l'événement dans le journal, envoyer une alerte ou immédiatement interrompre la session.

Contrôle des commandes et des applications

Safeguard On Demand prend en charge la création de listes blanches et noires des commandes et des noms de fenêtres.

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.

API REST

La solution Safeguard On Demand 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.

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.

Certification ISO 27001

One Identity est une succursale de Quest et le leader mondial dans la sécurité des identités. Ses infrastructures et processus dans le Cloud ont reçu la certification ISO/IEC 27001. Il s'agit d'une norme internationale décrivant les bonnes pratiques concernant les systèmes de gestion de la sécurité des informations.

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 Safeguard On Demand 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 de l'entreprise ; 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, une entité Quest, aide les organisations à mettre en place une stratégie de sécurité axée sur les identités, aussi bien sur site que 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](https://www.oneidentity.com)

© 2021 One Identity LLC. TOUS DROITS RÉSERVÉS. One Identity et le logo One Identity sont des marques et des marques déposées de One Identity LLC aux États-Unis et dans d'autres pays. Pour obtenir la liste complète des marques déposées One Identity visitez notre site Web www.oneidentity.com/fr-fr/legal. Toutes les autres marques, marques de service, marques déposées et marques de service déposées appartiennent à leurs propriétaires respectifs.

Datasheet-Safeguard-OnDemand-PG-FR-WL-64557