FICHE TECHNIQUE

One Identity Safeguard for Privileged Passwords

Sécurisation des informations d'identification partagées et privilégiées

Avantages

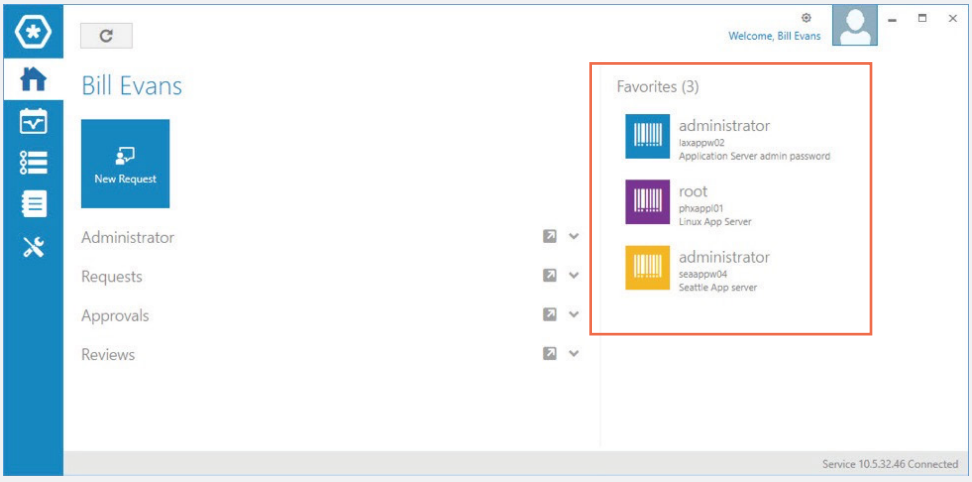
- Réduction des dommages résultant d'une violation de sécurité en contrôlant les accès aux comptes à privilèges
- Simplification du respect des exigences de conformité des comptes à privilèges
- Accélération du retour sur investissement avec le déploiement simplifié et la gestion continue
- Optimisation de la productivité avec une courbe d'apprentissage réduite et une conception d'interface utilisateur élégante
- Création de rapports d'audit plus simple et rapide

Introduction

Plusieurs incidents ont récemment démontré que les mots de passe des comptes à privilèges sont l'élément le plus vulnérable, voire le plus dévastateur, de la sécurité des systèmes. Ces mots de passe sont les clés du royaume. Dès que des pirates s'en emparent, ils jouissent d'un accès illimité à vos systèmes et données. De plus, comme vous l'avez vu, une réputation entachée et une propriété intellectuelle perdue peuvent coûter très cher à une entreprise affectée.

La sécurisation des informations d'identification privilégiées constitue généralement une source de frictions et une cause de ralentissement de la productivité des opérations quotidiennes et à long terme. Elle place souvent les responsables des technologies de l'information et de la sécurité face à un dilemme cornélien : choisir entre sécurité et facilité d'utilisation. Jusqu'à présent. Avec One Identity Safeguard for Privileged Passwords, vous pouvez avoir les deux.

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 solution peut être déployée sous forme d'appliance renforcée, ce qui élimine le besoin de sécuriser l'accès à la solution elle-même. Cela permet également d'accélérer l'intégration avec vos systèmes et vos stratégies informatiques. De plus, sa conception axée sur l'utilisateur réduit la courbe d'apprentissage et permet de gérer les mots de passe en tout lieu et sur n'importe quel appareil. Résultat : une solution qui sécurise votre entreprise et offre une liberté et une fonctionnalité accrues à vos utilisateurs privilégiés.



Accès rapide à vos mots de passe

Les favoris vous permettent d'accéder rapidement aux mots de passe que vous utilisez le plus fréquemment directement depuis l'écran de connexion.

Fonctionnalités

Contrôle des versions

La solution gère les demandes de mot de passe des utilisateurs autorisés pour les comptes sur lesquels ils ont un droit d'accès via une connexion sécurisée par navigateur Web avec prise en charge des appareils mobiles.

Moteur de workflows

Le moteur de workflows prend en charge les contraintes de temps, les réviseurs, plusieurs approbateurs, l'accès d'urgence et l'expiration des stratégies. Il permet également d'entrer des codes de raison et/ou peut s'intégrer directement avec les systèmes de tickets. Une demande de mot de passe peut être automatiquement approuvée ou nécessiter plusieurs niveaux d'approbation.

Détection

Détectez rapidement tout compte ou système à privilèges sur votre réseau avec les options de détection d'hôte, d'annuaire et de réseau.

Approbation en tout lieu

One Identity Starling vous permet d'approuver ou de refuser des demandes en tout lieu, 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.

Disponibilité permanente

Vous bénéficiez d'une véritable haute disponibilité, car cette solution a été conçue pour la mise en cluster distribuée. De plus, les fonctionnalités d'équilibrage de charge accélèrent le débit et écourtent les temps de réponse lorsque vous demandez des mots de passe et des sessions depuis n'importe quelle appliance.

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.

Centre d'activité

Vous pouvez rapidement et facilement visualiser toutes les activités avec un générateur de requêtes. En fonction de la personne qui a demandé un rapport (ex., opérations informatiques ou dirigeants), vous pouvez ajouter et supprimer des données pour obtenir les informations dont vous avez besoin. De plus, vous pouvez planifier des requêtes et enregistrer ou exporter les données dans divers formats.

Authentification à deux facteurs

Protéger l'accès aux mots de passe avec un autre mot de passe ne suffit pas. Renforcez la sécurité en appliquant l'authentification à deux facteurs à Safeguard. Safeguard prend en charge la solution 2FA basée sur RADIUS et inclut l'authentification à deux facteurs illimitée avec l'abonnement One Identity hybride.

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. Bénéficiez notamment en illimité de l'authentification à deux facteurs Starling pour protéger l'accès à Safeguard et de la certification Starling Access pour Safeguard afin de garantir des droits d'accès à privilèges et d'en assurer la conformité. Un seul abonnement vous permet de déployer toutes les solutions One Identity.

Prise en charge des cartes à puce

Utilisez vos méthodes d'authentification forte pour sécuriser l'accès à votre banque.

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 association unique d'offres, notamment une gamme de gestion des identités, de gestion des accès, de gestion des accès privilégiés, 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

Datasheet_2019-Safeguard-PrivPass_RS_41020