FICHE TECHNIQUE

Solution One Identity de gestion des accès à privilèges

Éliminez la problématique dite des « clés du château » avec la gestion des accès à privilèges

Avantages

- Contrôle des accès administratifs sur l'ensemble de l'entreprise
- Renforcement de l'efficacité, de la sécurité et de la conformité
- Suivi et audit simples pour toutes les activités des comptes à privilèges

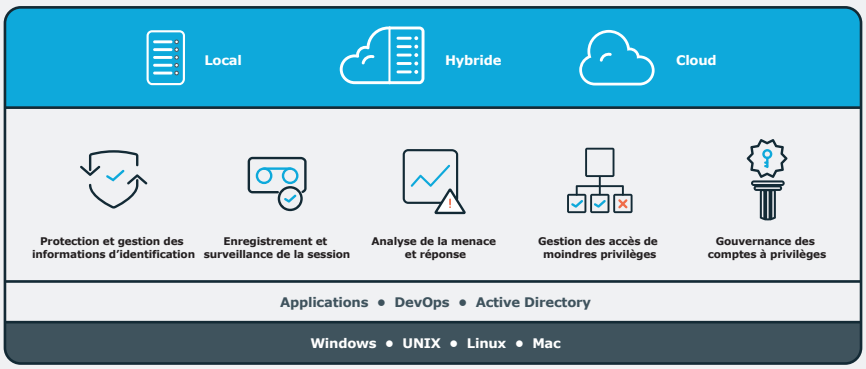
Les solutions IAM (gestion des accès et des identités) proposées par One Identity vous donnent le contrôle des accès administratifs dans l'entreprise. La solution One Identity de gestion des accès privilégiés vous permet de gagner en efficacité tout en renforçant la sécurité et la conformité : les administrateurs ne reçoivent que les droits dont ils ont besoin et toute activité fait l'objet d'un suivi et d'un audit.

Plus particulièrement, les solutions One Identity comprennent la délégation granulaire et basée sur les stratégies pour les identifiants superutilisateurs, la relecture et l'audit des sessions, l'enregistrement des frappes et des workflows sécurisés et automatisés afin d'attribuer les identifiants à privilèges aux administrateurs et dans les configurations application à application et application à base de données. La suite logicielle One Identity de solutions de gestion des accès à privilèges comprend :

La solution One Identity Safeguard for Privileged Passwords fournit un stockage sécurisé, le contrôle des versions et des modifications pour les mots de passe à privilèges afin d'assurer la responsabilité individuelle à travers divers déploiements de systèmes, d'appareils et d'applications. Elle garantit que lorsque les administrateurs nécessitent un accès élevé (généralement par le biais d'identifiants partagés comme les comptes root UNIX ou les comptes administrateurs Windows), l'accès est accordé selon la stratégie établie avec les approbations appropriées. Les actions font toutes l'objet d'un audit et d'un suivi complet, et le mot de passe est modifié dès son retour. One Identity Safeguard for Priviledge Password Manager remplace les mots de passe codés en dur des applications et des bases de données par des appels automatiques pour récupérer les identifiants de compte.

One Identity Safeguard for Privileged Session offre le contrôle, le proxy, l'audit, l'enregistrement et la relecture de session pour les utilisateurs à

Les solutions de sécurité de One Identity intègrent des offres complètes qui répondent aux besoins des entreprises les plus diverses et exigeantes en matière de gestion des accès à privilèges.



haut risque, comme les administrateurs et les prestataires distants. Le contenu des sessions enregistrées est indexé afin de simplifier la recherche d'événements et la création automatique de rapports et vous permettre 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.

Les solutions proposées par One Identity vous donnent le contrôle des accès administratifs dans l'ensemble de l'entreprise.

One Identity Safeguard for Privileged Analytics surveille les comportements suspects et identifie les menaces jusque-là inconnues, internes ou externes à votre entreprise. En utilisant la technologie d'analyse comportementale des utilisateurs, Safeguard for Privileged Analytics détecte les anomalies, les classe selon leur dangerosité pour que vous puissiez établir des priorités et prendre des mesures adéquates, et empêche la violation de données.

L'outil One Identity Safeguard for Sudo permet aux organisations utilisant UNIX ou Linux d'optimiser la gestion des accès privilégiés par le biais de sudo. Ses plug-ins 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 utilisateurs sudo, des rapports centralisés sur les droits d'accès et les activités des utilisateurs sudo ainsi que l'enregistrement des frappes clavier des activités effectuées via sudo. Cela facilite l'administration des utilisateurs sudo sur l'ensemble de l'entreprise, la rend intuitive et cohérente et élimine la gestion point par point.

La solution One Identity Authentication Services complète Safeguard for Sudo en unifiant les identités UNIX/Linux dans Microsoft® Active Directory®, ce qui vous permet d'utiliser une interface de gestion et un ensemble de stratégies pour le contrôle de la délégation root UNIX. Safeguard Authentication Services centralise l'authentification et fournit l'authentification unique pour UNIX et Linux, en unifiant les identités et en consolidant les annuaires, ce qui simplifie la gestion et facilite la conformité.

Active Roles fournit une délégation granulaire du compte administrateur Active Directory et le contrôle central des accès administratifs avec un seul ensemble de rôles, de règles et de stratégies bien défini.

Privilege Manager for Windows accorde aux utilisateurs les moindres privilèges nécessaires selon les bonnes pratiques et élève les permissions à des applications spécifiques lorsque les contrôles ActiveX sont requis. Vous pouvez définir l'exécution de privilèges élevés uniquement pour les applications, les fonctionnalités et les contrôles que vous choisissez. Les droits d'accès peuvent être ciblés à un utilisateur particulier, un groupe d'utilisateurs, une unité organisationnelle, un système d'exploitation, un groupe de postes de travail, un bureau ou une application. Toutes les activités de comptes à privilèges peuvent être auditées par le biais de rapports en un clic.

Identity Manager s'intègre avec Safeguard pour fournir la gouvernance des accès à privilèges. Le provisionnement des comptes, la gestion du cycle de vie et l'accès aux fonctionnalités de gouvernance d'Identity Manager peuvent être utilisés tout en continuant à utiliser les fonctionnalités de gestion des comptes et sessions à privilège de Safeguard. La gouvernance des accès à privilèges assure que les utilisateurs de comptes à privilèges obtiennent et conservent le niveau adapté d'accès aux comptes, alors que des attestations ponctuelles assurent que l'accès à privilèges est attesté régulièrement et correctement attribué.

Informations supplémentaires

Pour en savoir plus sur la gestion des accès à privilèges, visitez oneidentity.com/solutions/privileged-access-management/

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