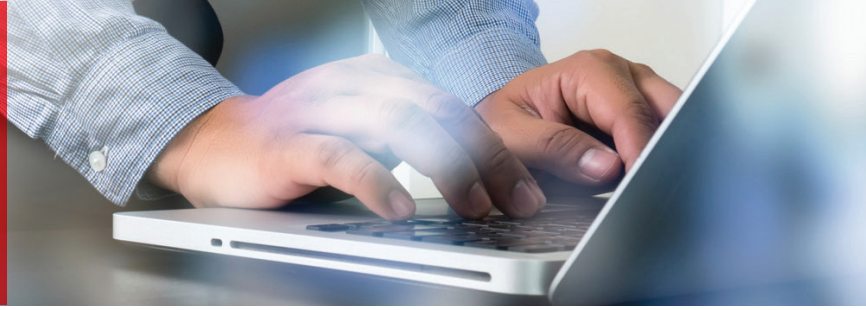
Centrify
ZERO TRUST PRIVILEGE



Service d'authentification de Centrify

Consolider les identités afin de réduire la surface d'attaque

Les nouvelles menaces sont bien différentes de celles du passé, lorsque des humains accédaient à l'infrastructure, aux bases de données et aux périphériques réseau d'une organisation à l'intérieur d'un espace bien défini. Aujourd'hui, la gestion des accès à privilèges (PAM) doit faire face à des requêtes qui ne viennent pas seulement de personnes mais aussi de machines, de services et d'API. Il existera toujours des comptes partagés, mais pour une plus grande sécurité, les bonnes pratiques recommandent désormais l'utilisation d'identités individuelles pour pouvoir appliquer le principe de moindre privilège. Pour limiter les risques émanant des menaces internes et des menaces avancées persistantes et répondre aux normes PCI DSS, SOX, ou autres impératifs sectoriels et réglementations gouvernementales, dans un environnement de plus en plus hétérogène et distribué, les services informatiques ont besoin d'une solution Zero Trust Privilege adaptée au Cloud apportant une visibilité et un contrôle centralisés sur les identités, la gestion des accès à privilèges et l'activité des utilisateurs à privilèges.

L'ancien modèle de gestion des accès à privilèges n'est pas suffisant contre les nouvelles menaces

La gestion des accès à privilèges existante date de plusieurs décennies, à une époque où tous les accès à privilèges étaient limités à des systèmes et ressources internes au réseau d'une organisation. L'environnement consistait en plusieurs administrateurs systèmes qui partageaient un compte « racine » qu'ils obtenaient depuis un coffre-fort de mots de passe afin d'accéder à un serveur, une base de données ou un périphérique réseau. Cet ancien modèle d'accès à privilèges a fait son temps.

Cependant, en plus du changement d'environnement, les cybercriminels exploitent désormais les identifiants à privilèges compromis lorsqu'ils passent à l'attaque. Par conséquent, les entreprises doivent se débarrasser des comptes locaux et partagés, basés sur des identifiants statiques, sur leurs systèmes. Pour réduire leur surface d'attaque et renforcer leur sécurité, elles peuvent les remplacer par des comptes individuels fédérés dont l'accès temporaire s'effectue au moyen de tickets. De leur côté, de nombreuses normes réglementaires et sectorielles telles que la NIST 800-63 et la PCI DSS exigent des contrôles de sécurité plus poussés que ceux assurés par les coffres-forts.

Aller au-delà de la découverte et de la sécurisation des mots de passe par coffre-fort

Le service d'authentification de Centrify offre aux clients les capacités nécessaires pour renforcer la sécurité au-delà des coffres-forts et vérifier correctement les émetteurs de demandes d'accès à privilèges. Cela est possible en tirant parti de l'annuaire des identités de l'entreprise, en éliminant les comptes locaux et en réduisant le nombre total de comptes et de mots de passe afin de diminuer la surface d'attaque.

CONTRÔLE MULTI-RÉPERTOIRE

Simplifiez l'authentification des utilisateurs sur les serveurs depuis tout service de répertoire dont Active Directory, LDAP, ou les répertoires dans le Cloud. Les entreprises peuvent bénéficier des avantages du Cloud sans créer de nouveaux répertoires d'identités cloisonnés ou des mécanismes de synchronisation complexes.

TECHNOLOGIE DE GESTION DE ZONES DE CENTRIFY

Consolidez rapidement les identités d'utilisateurs UNIX et Linux complexes et dispersées dans Active Directory grâce à la technologie brevetée de gestion de Zones de Centrify, sans avoir à rationaliser toutes les identités d'utilisateurs au préalable. La Technologie de gestion de Zones de Centrify vous permet de gérer les utilisateurs, les ordinateurs, les rôles et les droits au sein d'un modèle hiérarchique que vous pouvez adapter à vos besoins.

COMPATIBILITÉ ACTIVE DIRECTORY

Sécurisez Linux et UNIX avec les mêmes services d'identité utilisés pour protéger les accès aux systèmes Windows. Centralisez la gestion des stratégies et l'administration des utilisateurs sur les systèmes Linux et UNIX pour permettre une consolidation rapide des identités dans Active Directory. Profitez d'une intégration profonde dans Active Directory même pour les architectures les plus complexes.

GESTION DES COMPTES LOCAUX ET DES GROUPES

Gérez les comptes système de la même manière que les comptes d'utilisateurs dans Active Directory. Gagnez du temps et de l'argent tout en augmentant la productivité de votre équipe informatique.

GESTION DES IDENTITÉS DES MACHINES ET DES IDENTIFIANTS

Gérez de manière centralisée les identités des machines et leurs identifiants au sein d'Active Directory ou des services Zero Trust Privilege de Centrify afin d'établir une base de confiance pour les authentifications de machine à machine basées sur un modèle de confiance centralisé.

GESTION DES STRATÉGIES DE GROUPE

Gérez l'authentification, le contrôle des accès et les stratégies de groupe pour les systèmes hors Windows de la même manière que pour Windows. Utilisez les stratégies de groupe Active Directory pour automatiser la configuration SSH et du pare-feu, choisir les utilisateurs qui peuvent se connecter à chaque système, mettre fin aux sessions inactives et agir comme une authentification basée sur le réseau.

AUTHENTIFICATION MULTIFACTEUR LORS DE LA CONNEXION AU SYSTÈME

Les connexions aux systèmes à privilèges sont souvent la première interface d'attaque qu'il faut protéger contre les cybercriminels qui veulent dérober les informations ou nuire à l'environnement. L'authentification multifacteur (MFA) lors de la connexion aux serveurs Linux, UNIX et Windows limite le risque d'exposition et respecte les normes réglementaires les plus rigoureuses comme la PCI DSS et la NIST 800-63A. Avec Centrify, vous pouvez aller au-delà de l'authentification multifacteur lors de la connexion au serveur et l'appliquer sur l'ensemble de vos systèmes.

Simplifier le déplacement des workloads vers le Cloud à l'aide du contrôle multi-répertoire

Simplifiez l'authentification des utilisateurs sur les serveurs depuis tout service de répertoire dont Active Directory, LDAP, ou les répertoires dans le Cloud tels que ceux de Google. Les organisations peuvent bénéficier des avantages du Cloud sans créer de nouveaux silos d'identité, reproduire des répertoires d'identité ou compromettre leur niveau actuel de sécurité des accès à privilèges et d'entreprise sur site. De plus, les responsables informatiques gagnent du temps dans la gestion d'un environnement hétérogène, aidant l'organisation à réaliser d'importantes économies.

- Authentifiez l'accès aux ressources à privilèges grâce à un service de répertoire, aussi bien localement que dans le Cloud.
- Instaurez une authentification et des contrôles d'accès centralisés pour les infrastructures géographiquement dispersées, en tirant parti des identités d'un ou plusieurs environnements Active Directory, LDAP ou Cloud comme Centrify Directory ou Google Directory.

Une gestion et une consolidation des identités pour Linux et Unix compatibles avec Active Directory

Le service d'authentification de Centrify permet aux clients d'unifier leur infrastructure informatique en consolidant les identités, l'authentification et la gestion des accès pour Linux et UNIX au sein de Microsoft Active Directory. À cet égard, Centrify a été le premier fournisseur à intégrer UNIX et Linux dans Active Directory, prenant en charge plusieurs identités pour un seul utilisateur. Dans son Magic Quadrant for Privileged Access Management de 2018, Gartner souligne en particulier les performances uniques de Centrify dans ce domaine. Ce service est prisé par les clients et les prospects en raison de l'augmentation potentielle de la productivité informatique, de la réduction des coûts liés à la maintenance et de la diminution de la surface d'attaque.

- Connectez les systèmes Linux et UNIX à Active Directory de façon native, convertissant le système hôte en un client Active Directory. Sécurisez les systèmes au moyen des services d'authentification et de stratégie de groupe actuellement déployés pour les systèmes Windows.
- Consolidez les profils d'utilisateurs et séparez les fonctions.
- Appliquez la gestion des stratégies de groupe aux systèmes hors Windows. C'est la seule solution qui offre des stratégies en matière d'utilisateurs et d'ordinateurs dotées de fonctionnalités avancées telles que le filtrage par groupe et le traitement des bouclages. Les paramètres de configuration des stratégies de groupe sont parfaitement intégrés à l'agent UNIX de Centrify afin de gérer la configuration du système et de l'environnement utilisateur.
- Alors que de nombreux fournisseurs prétendent prendre en charge Kerberos, seul Centrify offre une prise en charge native de l'ensemble de la complexité et des nuances d'Active Directory.
- La mise en place d'une automatisation permettant de gagner du temps est facilitée par une CLI et des options de script optimisées, prenant en charge la gestion des mots de passe d'application à application (AAPM).

Gérer les comptes et groupes locaux de manière efficace

Grâce au service d'authentification de Centrify, les clients peuvent simplifier la gestion des comptes et groupes locaux au sein de leur infrastructure hétérogène. Centrify automatise le cycle de vie des comptes locaux et intègre, le cas échéant, la sécurisation des mots de passe par coffre-fort pour les services ou applications dans le but de centraliser l'ensemble de la gestion des comptes et des groupes dans une seule plateforme.

- Gérez de façon centralisée le cycle de vie des comptes d'applications et de services et sécurisez automatiquement les identifiants et les accès.
- Intégrez la gestion des mots de passe des comptes locaux aux coffres-forts existants permettant d'automatiser l'enregistrement et la sécurisation des nouveaux comptes.
- Centralisez la gestion des groupes locaux.

Centraliser rapidement la gestion des serveurs Windows, Linux et Unix

La Technologie de gestion de Zones de Centrify vous permet de gérer votre environnement hétérogène en consolidant les droits dont dispose un utilisateur sur un système Windows, Linux ou UNIX en une seule identité, stockée et gérée dans Active Directory.

- Établissez les hiérarchies et les droits.
- Activez la migration rapide des identités UNIX vers Active Directory.
- Tirez parti de Centrify Computer Roles pour bénéficier d'une gestion unique et d'avantages en termes de sécurité.

Appliquer des stratégies de groupe pour les utilisateurs et les systèmes hétérogènes

Centrify fournit une assistance complète pour le déploiement de la gestion des stratégies de groupe sur les systèmes hors Windows. C'est la seule solution qui offre des stratégies en matière d'utilisateurs et d'ordinateurs dotées de fonctionnalités avancées telles que le filtrage par groupe et le traitement des bouclages.

- Appliquez les stratégies de groupe Active Directory sur les plateformes hors Windows.
- Gérez l'authentification, le contrôle des accès et les stratégies de groupe pour les systèmes hors Windows.

Vérifier que seules les personnes autorisées accèdent à votre infrastructure critique via une authentification multifacteur lors de la connexion au système

Les connexions aux systèmes à privilèges sont souvent la première interface d'attaque qu'il faut protéger contre les cybercriminels qui veulent dérober des informations ou nuire à l'environnement. Pour vérifier que seules les personnes autorisées accèdent à vos systèmes sensibles, vous devez appliquer une authentification multifacteur robuste. Centrify fournit une technologie basée sur l'hôte, qui ne peut pas être contournée, pour appliquer une authentification multifacteur lors des connexions aux systèmes pour les serveurs Linux, UNIX, Windows et les postes de travail.

- Renforcez les principes Zero Trust via l'application d'une authentification multifacteur au niveau de l'hôte, impossible à contourner, sur chaque ordinateur.
- Intégration centralisée du service d'authentification multifacteur.
- Capacités d'authentification multifacteur locales pour UNIX et Linux.
- Intégration native de l'authentification multifacteur Windows lors du processus de connexion.

Nous avons pour mission de mettre fin à la cause principale d'intrusions : le détournement des identifiants à privilèges. Centrify renforce la protection de nos clients grâce à une approche Zero Trust Privilege adaptée au Cloud qui sécurise les accès aux infrastructures, DevOps, réseaux Cloud, conteneurs, projets big data et autres surfaces d'attaque des entreprises modernes. Pour en savoir plus, rendez-vous sur www.centrify.com.

Siège social aux États-Unis +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asie-Pacifique +61 1300 795 789
Brésil +55 11 3958 4876
Amérique latine +1 305 900 5354
sales@centrify.com

Centrify
ZERO TRUST PRIVILEGE