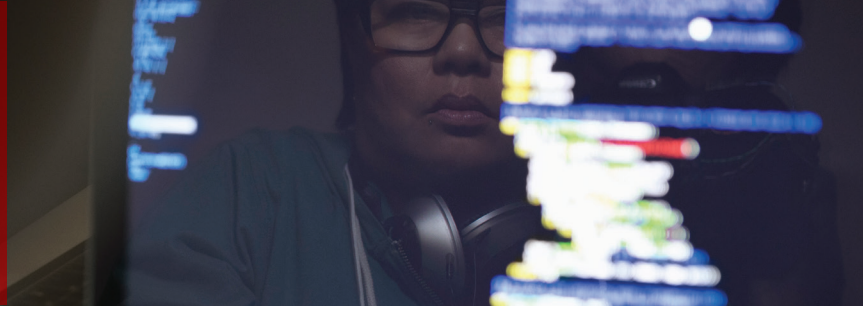
Centrify
ZERO TRUST PRIVILEGE



Services d'audit et de surveillance de Centrify

Renforcer la sécurité de votre environnement

Il est conseillé d'auditer l'ensemble du système pour les sessions à privilèges. Grâce à un enregistrement détaillé de toutes les actions effectuées, les journaux d'audit peuvent non seulement être utilisés dans des analyses approfondies post-incident pour trouver le problème exact, mais aussi pour corréler des activités avec un utilisateur particulier. En raison du caractère critique de ces sessions, pour les ressources les plus critiques ou dans les secteurs fortement réglementés, il est également recommandé de conserver un enregistrement vidéo pouvant être visionné ou utilisé à titre de preuve. Plusieurs réglementations, notamment la norme PCI DSS pour les données de cartes de paiement, nécessitent ce niveau d'audit en particulier. Si vous disposez d'un département en charge de la sécurité, il est recommandé d'intégrer ces données d'audit à votre système existant de gestion de l'information et des événements de sécurité (SIEM) pour automatiser l'exploration des données de manière à identifier et signaler les activités à risque.

Audit de l'ensemble des systèmes

Les analystes du secteur et les autorités gouvernementales de réglementation ont reconnu que la cause principale des vols de données repose aujourd'hui sur le détournement des identifiants à privilèges. Les identifiants à privilèges sont la clé permettant d'accéder librement à l'infrastructure entière d'un système. Il suffit qu'un seul identifiant à privilèges soit compromis pour exposer des millions de personnes. De leur côté, les auditeurs internes et les mandats réglementaires établissent des exigences précises en matière de contrôles et de rapports pour l'usage de ces identifiants.

Même les petites et moyennes entreprises doivent respecter diverses réglementations sectorielles et gouvernementales, ce qui constitue un défi unique à l'heure de collecter, d'agréger et d'attester les données liées aux accès à privilèges.

Bien souvent, les entreprises n'offrent pas une transparence continue en matière de conformité. Les audits et les certifications donnent alors lieu à une course lors de laquelle la charge de travail des auditeurs internes et des équipes de conformité explose.

Cela découle généralement sur une stratégie « d'échantillonnage », selon laquelle seul un sous-ensemble de contrôles précis est évalué, laissant des zones d'ombre sur le plan de la conformité et de la sécurité. De manière générale, chercher des réponses auprès de plusieurs intervenants et évaluer différents ensembles de données a des répercussions sur l'efficacité et la fiabilité.

Du point de vue de la sécurité, il est important d'obtenir des informations précises et détaillées sur les activités suspectes liées aux accès à privilèges. Les responsables de la sécurité peuvent prendre des mesures immédiates afin de protéger les systèmes contre les risques potentiels ou menaces en cours directement depuis l'écran d'alerte, et ils peuvent mettre fin manuellement ou automatiquement à la session selon le risque.

Récemment, les atteintes majeures à la protection des données ont été causées par des personnes internes aux entreprises ayant créé des comptes de porte dérobée capables de contourner les solutions traditionnelles de sécurisation des mots de passe par coffre-fort. Les utilisateurs à privilèges sont aussi réputés pour trouver le moyen de contourner le coffre-fort de mots de passe dans leur environnement afin de simplifier leur routine quotidienne. Ces accès non autorisés exploitent souvent des clés SSH stockées sur les serveurs locaux. Cela agrandit la surface d'attaque des organisations et les expose davantage aux intrusions.

Renforcer la sécurité de votre environnement

Les services d'audit et de surveillance de Centrify permettent aux clients de respecter leurs mandats de conformité via des audits et des rapports et de mettre fin aux solutions de contournement dangereuses en instaurant une surveillance au niveau de l'hôte. Les services permettent aussi d'enregistrer toutes les sessions à privilèges et métadonnées, corrélant l'activité avec un individu afin d'avoir une vision complète des intentions et des conséquences.

ENREGISTREMENT DE SESSION ET AUDIT

Enregistrez et gérez une vision globale des activités à privilèges sur l'ensemble des serveurs Windows et Linux, IaaS et bases de données, afin d'établir une source unique d'informations fiables pour les comptes individuels et partagés. Prouvez votre conformité au moyen de rapports sur les privilèges de chaque utilisateur et les activités associées.

SURVEILLANCE ET CONTRÔLE DE SESSION PASSERELLE

Ayez une meilleure vision globale des sessions à privilèges sur les infrastructures critiques. Les utilisateurs administratifs surveillent l'activité des sessions à distance en temps réel. Ils peuvent immédiatement mettre fin aux sessions suspectes à l'aide du portail administrateur de Centrify.

AUDIT, ENREGISTREMENT ET RAPPORT DE SESSION SUR L'HÔTE

Assurez-vous que les enregistrements de sessions ne peuvent pas être contournés au moyen d'un audit de l'hôte. Découvrez des activités non autorisées telles que la création et l'installation de paires de clés SSH qui faciliteraient le contournement des contrôles de sécurité, et corrélez l'activité avec un utilisateur individuel. Auditez en détail l'ensemble des activités liées aux sessions à privilèges au niveau du processus afin d'évaluer la sécurité, de prendre des mesures correctives, d'établir des rapports de conformité et d'éviter toute usurpation.

« Centrify nous a aidés à respecter toutes les réglementations applicables. Désormais, chaque fois qu'un administrateur est actif sur un serveur, je reçois un enregistrement. Je peux extraire un rapport, l'imprimer et le donner à un auditeur. »

Peter Manina, expert en informatique et architecte systèmes UNIX, Département de technologie, de gestion et du budget de l'État du Michigan

Enregistrement et audit de session pour les accès à privilèges

Rédigez des rapports et effectuez des audits sur les sessions à privilèges qui exploitent les comptes individuels et partagés grâce à une fonction d'enregistrement vidéo intégrale et de saisie des métadonnées. Les services d'audit et de surveillance de Centrify permettent aux clients de réaliser des analyses approfondies post-incident et de tirer parti des enregistrements haute-fidélité à des fins d'audit et de conformité.

- Saisissez et collectez les données à l'aide d'un enregistrement haute-fidélité de chaque session à privilèges au niveau de la passerelle. Les services d'audit et de surveillance de Centrify stockent les sessions dans une base de données SQL Server facilement consultable afin d'avoir une vision globale des événements. La fonctionnalité de lecture du service offre aux responsables de sécurité informatique et aux auditeurs la possibilité de voir exactement les actions des utilisateurs et leurs répercussions et d'identifier les détournements d'identifiants à privilèges ou la source d'un incident de sécurité.
- Enregistrez toutes les sessions à privilèges et métadonnées, corrélant l'activité avec un individu afin d'avoir une vision complète des intentions et des conséquences.
- Montrez que les contrôles de sécurité sont en place et fonctionnent correctement, et fournissez des preuves de conformité. Recherchez des enregistrements de session par serveurs, utilisateurs ou selon des critères personnalisés. Vous pouvez trouver toutes les sessions pour un utilisateur ou un serveur en particulier, ou pour un ensemble de paramètres personnalisés, ce qui simplifie les analyses approfondies post-incident et permet d'identifier de manière proactive les menaces internes ou les activités suspectes.
- Obtenez une visibilité exhaustive grâce à un accès unifié et des analyses d'activités sur une plateforme commune. Un système de requête intégré et personnalisable, ainsi que des rapports prêts à l'emploi en matière de conformité envers les réglementations SOX et PCI, fournissent des informations sur les contrôles d'accès pour les comptes à privilèges, sur l'obtention des mots de passe et sur les sessions à privilèges sous Windows, Linux et UNIX.

Surveiller et contrôler les sessions à privilèges sur les structures IaaS et locales

Tirez parti d'une infrastructure d'audit commune pour saisir et enregistrer les activités à privilèges pour votre infrastructure, qu'elle soit locale ou dans le Cloud. Détectez toute activité suspecte de la part des utilisateurs afin de recevoir des alertes en temps réel sur les attaques potentielles en cours. Les services d'audit et de surveillance de Centrify vous permettent de surveiller et de contrôler les sessions d'accès à privilèges qui exploitent des comptes partagés et individuels.

- Ayez une meilleure vision globale des sessions à privilèges sur les infrastructures critiques. Les utilisateurs administratifs surveillent l'activité des sessions à distance en temps réel. Ils peuvent immédiatement mettre fin aux sessions suspectes à l'aide du portail administrateur de Centrify. Ce principe des 4 yeux permet aux utilisateurs administratifs de superviser un employé à distance ou des activités informatiques externalisées et de contrôler en direct la session en cours. Vous pouvez observer chaque action entreprise par l'utilisateur à privilèges ou bien mettre fin à la session si l'activité est suspecte.
- Les données des accès à privilèges sont collectées et stockées pour permettre l'exécution de requêtes par des outils robustes de gestion de connexion et l'intégration avec des outils de rapports externes. Une intégration simplifiée avec des outils de SIEM et d'alertes tels que Micro Focus® ArcSight™, IBM® QRadar™ et Splunk® permettent d'identifier rapidement les risques ou les activités suspectes.

Éviter toute usurpation ou tout contournement d'accès à privilèges avec les audits, enregistrements et rapports de session sur l'hôte

Adopter une approche au niveau de l'hôte en matière d'audit, d'enregistrement et de rapports de session vous permet d'avoir plus de contrôle sur les accès à privilèges au sein de votre environnement. Les services d'audit et de surveillance de Centrify enrichissent leurs capacités d'exécution à la passerelle d'une approche au niveau de l'hôte afin de garantir que vos contrôles des accès à privilèges ne soient pas contournés, comme ce peut être le cas avec la sécurisation de mots de passe/secrets par coffre-fort.

- Saisissez et capturez les données via un enregistrement haute-fidélité de chaque session à privilèges sur tous les serveurs de votre infrastructure locale ou dans le Cloud. Stockez les sessions dans une base de données SQL Server facilement consultable pour avoir une vision globale permanente des événements pour tous les utilisateurs sur tous les systèmes.
- L'audit, l'enregistrement et les rapports de session sur l'hôte de Centrify sont réalisés grâce à des capacités de surveillance avancée au niveau du processus, associées à un audit de l'interface système afin d'identifier les modifications d'application suspectes.
- La surveillance de l'intégrité des fichiers de Centrify permet d'identifier les modifications apportées aux configurations et aux fichiers critiques en temps réel. Des alertes de sécurité se déclenchent au sein du système SIEM de l'organisation pour avertir de la création d'une porte dérobée visant à contourner la sécurisation des mots de passe par coffre-fort.
- La fonctionnalité de lecture des enregistrements offre aux responsables de sécurité informatique et aux auditeurs la possibilité de voir exactement les actions des utilisateurs et d'identifier les détournements d'identifiants à privilèges ou la source d'un incident de sécurité.
- Rédigez des rapports sur les accès, les obtentions de mots de passe, les sessions et l'utilisation de privilèges sous Windows, Linux, UNIX et sur votre infrastructure réseau.
- Une intégration simplifiée à l'aide d'outils de SIEM, d'alertes et de rapports.

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

www.centrify.com