Centrify
ZERO TRUST PRIVILEGE

Service d'analyse des menaces liées aux privilèges de Centrify

Contrôles du machine learning pour faire face aux nouvelles menaces

Les contrôles de l'approche Zero Trust Privilege doivent s'adapter au contexte de risque. Gartner appuie ses recommandations sur le modèle CARTA (Continous, Adaptive, Risk, and Trust Assessment), et celui-ci doit également être appliqué pour les accès à privilèges. Le modèle Zero Trust Privilege instaure une vérification supplémentaire avant d'accorder l'accès au cas où un utilisateur à privilèges, même s'il dispose des identifiants nécessaires, émet une demande d'accès dans un contexte à risque. Les algorithmes modernes du machine learning sont désormais utilisés pour analyser avec précision le comportement d'un utilisateur à privilèges et identifier les activités « irrégulières » ou « anormales » (donc à risque) et appliquer un niveau de contrôle adapté au risque.

Les nouvelles menaces requièrent des contrôles intelligents

Les cybercriminels disposent de technologies de plus en plus sophistiquées. Par conséquent, il est recommandé d'instaurer plusieurs niveaux de sécurité à titre de protection contre les détournements d'accès à privilèges. Les nouvelles menaces requièrent des contrôles de sécurité qui s'adaptent au contexte de risque et qui utilisent le machine learning pour analyser avec précision le comportement d'un utilisateur à privilèges.

Un contrôle intelligent permet non seulement de repérer une activité à risque en temps réel, mais aussi d'intervenir de façon proactive en cas d'incident en mettant fin aux sessions, en activant une surveillance supplémentaire ou en marquant le problème en vue d'une analyse approfondie post-incident.

Le machine learning permet aux entreprises d'examiner des millions d'événements et de rechercher continuellement l'aiguille dans la botte de foin, chose impossible avec des analyses manuelles. Les analyses en ligne et en temps réel basées sur le machine learning sont d'autant plus importantes qu'elles permettent la mise en œuvre de contrôles intelligents et préventifs au lieu de simplement détecter les incidents après coup.

Identifier, en quasi-temps réel les détournements d'accès à privilèges

Le service d'analyse des menaces liées aux privilèges de Centrify se sert des analyses avancées du comportement ainsi que des capacités de l'authentification multifacteur intelligente Zero Trust Privilege pour ajouter une protection supplémentaire et appliquer une MFA adaptative pour les comportements d'utilisateurs anormaux. Tirer parti du service d'analyse de menaces liées aux privilèges de Centrify peut faire la différence entre être victime d'une intrusion et la stopper à temps.

AUTHENTIFICATION MULTIFACTEUR ADAPTATIVE

Ajoutez un niveau de sécurité supplémentaire pour stopper les intrusions grâce à une authentification multifacteur adaptative, prenant en compte les risques, pour les administrateurs informatiques qui accèdent aux systèmes Windows et Linux, élèvent les privilèges ou utilisent des identifiants à privilèges.

ANALYSE DU COMPORTEMENT UTILISATEUR

Utilisez les algorithmes modernes du machine learning pour analyser avec précision le comportement d'un utilisateur à privilèges, identifier les activités « irrégulières » ou « anormales » (donc à risque) et prévenir ou alerter la sécurité. La détection des activités à risque est également utile lors de la prise de décisions en temps réel liée aux contrôles d'accès, notamment dans un contexte d'authentification ou d'authentification renforcée. De plus, l'analyse du comportement des utilisateurs à privilèges peut servir à déterminer les privilèges les plus et les moins fréquemment utilisés et ainsi participer à la gouvernance en suggérant des modifications sur les rôles et les droits.

« Lorsque vous comprenez vraiment l'étendue des capacités des services Zero Trust Privilege de Centrify, vous vous apercevez qu'ils remplissent un nombre incroyable de critères de sécurité. Je suis encore surpris par la quantité de problèmes que j'ai pu résoudre avec cette seule solution. »

— Matt Horn, directeur des opérations informatiques chez GSI

Accès sécurisé renforcé aux systèmes critiques

Ajoutez un niveau de sécurité supplémentaire uniquement en cas de besoin, et selon le degré de risque, afin de réduire les menaces liées aux identifiants à privilèges compromis. Configurez le contrôle d'accès basé sur le comportement pour les administrateurs informatiques qui accèdent aux serveurs Windows et Linux, élèvent les privilèges ou utilisent des identifiants à privilèges.

- Identifiez les comportements anormaux en temps réel en appliquant des stratégies adaptées aux risques pour les utilisateurs qui initient des sessions à privilèges, qui obtiennent un mot de passe ou qui élèvent des privilèges. L'association des stratégies adaptées aux risques, des contrôles d'accès basés sur le rôle, du contexte utilisateur et de l'authentification multifacteur permet une prise de décision intelligente, automatisée et en temps réel concernant l'octroi des accès à privilèges. Ces stratégies d'accès dynamiques accordent l'accès à l'utilisateur, demandent un deuxième facteur d'authentification ou bloquent complètement l'accès.
- Les services Zero Trust Privilege de Centrify sont compatibles avec le plus large éventail d'authentifiants pour pouvoir authentifier votre équipe informatique grâce au facteur de forme le plus pratique, et pour vous permettre d'utiliser les systèmes MFA les authentifiants dont vous disposez déjà. Voici certains des authentifiants pris en charge par Centrify :
  - notification push mobile ;
  - questions de sécurité ;
  - appel téléphonique avec une vérification du code PIN ;
  - jetons OATH ;
  - serveurs de code unique ;
  - clés de sécurité FIDO U2F ; et
  - cartes à puces.
- Les capacités d'authentification multifacteur adaptatives de Centrify sont conçues pour fonctionner avec les investissements existants en matière de chiffrement RSA, de jetons OATH et de cartes à puces PIV/CAC. Tous ces systèmes peuvent être gérés de manière centralisée avec Centrify et appliqués à l'échelle de votre entreprise.
- L'application mobile de Centrify, compatible avec iOS et Android, offre aux utilisateurs à privilèges une interface intuitive où recevoir les notifications liées à la MFA ou les workflows de demandes et d'approbations. L'application comporte également une interface pour permettre à l'utilisateur de gérer les jetons OATH où les secrets/codes sources sont protégés par le service d'accès à privilèges de Centrify. Cela permet de supporter la validation utilisateur des codes OTP requise par plusieurs applications ou services à privilèges qui appliquent leur propre validation MFA conforme à OATH comme la Console AWS®. De plus, l'application mobile prend en charge l'obtention / l'enregistrement de mots de passe d'urgence.
- Centrify prend également en charge les services d'authentification multifacteur pour les périphériques réseau tels que les routeurs, les commutateurs ou les pare-feu, où l'accès administratif requiert une authentification multifacteur avant d'octroyer un accès utilisateur à privilèges.

Tirer parti des analyses de comportement utilisateur pour minimiser votre exposition aux risques

Les nouvelles menaces requièrent des contrôles de sécurité qui s'adaptent au contexte de risque, utilisant le machine learning pour analyser avec précision le comportement d'un utilisateur à privilèges. Un contrôle intelligent permet non seulement d'être informé d'une activité à risque en temps réel, mais aussi d'intervenir de manière active en cas d'incident en mettant fin aux sessions, en activant une surveillance supplémentaire ou en marquant le problème en vue d'une analyse approfondie post-incident.

- Utilisez une série de tableaux de bord personnalisables et de widgets interactifs pour mieux comprendre les risques informatiques et les schémas d'accès sur votre infrastructure. Ayez une meilleure visibilité en matière de risques liés aux comptes en adaptant les stratégies de sécurité au comportement de chaque utilisateur et en signalant automatiquement les attitudes à risque. Vous éliminerez par la même occasion les frais engendrés par l'analyse de millions de fichiers journaux et de quantités massives de données historiques.
- Améliorez votre compréhension des accès et des événements en explorant en détail les événements en fonction des systèmes, du lieu et de l'heure, des commandes à privilèges, etc. Les utilisateurs informatiques peuvent analyser les événements individuels pour comprendre les risques liés à un événement précis. Les risques sont calculés en temps réel pour chaque événement et les activités anormales sont classées en trois catégories : risque élevé, risque moyen, risque faible.
- Ayez une vision simplifiée des activités anormales avec une chronologie détaillée. Identifiez les facteurs spécifiques qui contribuent à une anomalie pour avoir une compréhension globale d'une menace potentielle, et ce depuis une console unique. Les équipes de sécurité peuvent afficher les accès aux systèmes et les détections d'anomalies en haute résolution grâce aux outils d'analyse tels que des tableaux de bord, des outils de recherche et d'investigation.
- 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 à l'aide d'outils de SIEM tels que Micro Focus® ArcSight™, IBM® QRadar™ et Splunk® permettent d'identifier rapidement les risques ou les activités suspectes.
- Utilisez toute application utilisant des webhooks (comme Slack® ou des systèmes de réponse aux incidents existants tels que PagerDuty®) pour envoyer des alertes en temps réel sans passer par de multiples étapes d'alerte et améliorer le temps de réponse. Lorsqu'un événement nécessite une alerte, le service d'analyse des menaces liées aux privilèges de Centrify permet à l'utilisateur de lancer facilement des alertes vers des applications tierces via webhook. Grâce à cette fonctionnalité, l'utilisateur peut répondre à une alerte de menace et contenir les effets de celle-ci.
- Obtenez des informations précises et détaillées sur les activités à privilèges suspectes. Les responsables informatiques 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.
- Les événements analysés par le service d'analyse de menaces liées aux privilèges de Centrify sont utilisés pour définir le comportement normal d'un utilisateur à chaque connexion ou activité à privilèges, notamment lors de l'exécution de commandes. Les anomalies peuvent ainsi être identifiées en temps réel et un contrôle d'accès basé sur le risque s'applique. Les événements à risque élevé font immédiatement l'objet d'un signalement, d'une alerte, d'une notification et sont transmis à l'équipe informatique. Cela accélère le processus d'analyse et minimise fortement les efforts requis pour évaluer les risques au sein des environnements informatiques hybrides d'aujourd'hui.

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