ManageEngine
PAM360

Gestion des accès privilégiés dans un monde de Zero Trust

Melanie Karunaratne

www.manageengine.com/pam360

Introduction

Dans les premiers mois de la pandémie de COVID-19, avec le recours à grande échelle au travail à domicile, la connectivité a été la principale préoccupation des organisations. Les administrateurs informatiques ont rapidement mis en place des réunions virtuelles, du streaming en direct, de l'éducation virtuelle, des applications sur le cloud et des ressources pour soutenir leurs utilisateurs finaux à distance. De nombreuses organisations ayant signalé leur intention d'étendre le travail à domicile, il est clair que le travail à distance et la dynamique du travail hybride sont là pour rester. Ce document décrit les implications de ce nouvel environnement de travail en matière de sécurité, explique l'évolution des organisations vers un état d'esprit de Zero Trust, et l'importance de la gestion des accès privilégiés pour soutenir un modèle de sécurité Zero Trust.

Accès à toutes les zones

Les changements provoqués par les mandats de travail à domicile et la nécessité de maintenir à tout prix la productivité des travailleurs ont donné lieu à un accès rapide à la technologie. Cet accès a souvent contourné les contrôles réguliers des demandes d'accès. Voici quelques-unes des conclusions qui découlent de l'adoption croissante des politiques de Travail à distance :

- Les entreprises, le secteur de la santé, l'éducation et les gouvernements ont accéléré l'adoption de la technologie de l'informatique dématérialisée, en faisant rapidement migrer certains services des locaux vers des applications SaaS (Software as a Service) qui utilisent des points d'entrée publics sur Internet.

- Les employés ont été autorisés à accéder à des ressources en dehors du réseau de l'entreprise.

- De nouveaux contrats avec les fournisseurs de TI ont été adoptés rapidement, ce qui a eu pour effet d'accroître l'accès de tiers aux infrastructures et aux applications de l'entreprise.

- Les VPN se sont développés, augmentant les coûts de licence et le nombre d'incidents informatiques enregistrés.

- Des ordinateurs portables ont été achetés, approvisionnés et mis à disposition avec des droits d'accès élevés afin que les employés puissent être opérationnels rapidement.

- Les travailleurs ont installé des bureaux à domicile, accédant aux systèmes à partir de téléphones, d'ordinateurs portables et de tablettes personnels et, dans certains cas, d'appareils familiaux partagés. Ces appareils personnels ont souvent des configurations de sécurité plus faibles. Ces mêmes appareils se connectent à des sites d'achat grand public, à des médias sociaux et à des sites de divertissement à domicile en utilisant les mêmes informations d'identification. Cela augmente la probabilité que des appareils compromis accèdent à des applications stockant des données d'entreprise.

- Les entreprises qui n'ont pas été conçues pour le travail à distance doivent désormais faire face à une explosion de points d'extrémité connus et inconnus accédant à leurs réseaux sur des réseaux Wi-Fi non sécurisés.

Les données d'entreprise auparavant hébergées dans des logiciels contrôlés et maintenus par les équipes informatiques résident désormais dans des applications SaaS non contrôlées avec des mots de passe partagés qui peuvent être utilisés sur des appareils personnels, ce qui augmente le risque d'exposition à la sécurité en élargissant les surfaces d'attaque. Le travail à distance étant devenu la nouvelle normalité, nous avons assisté à

une recrudescence et à une persistance des cyberattaques au cours de la même période. Les acteurs de la menace ont profité du passage au travail à domicile pour pénétrer de manière persistante dans les périmètres des réseaux. Des attaques sophistiquées perturbent les entreprises, les chaînes d'approvisionnement et les soins de santé à un coût énorme.

Zero Trust - Ne faites confiance à personne

Avec des utilisateurs travaillant sur de multiples appareils, sur et hors du réseau de l'entreprise, il est devenu un véritable défi de sécuriser le périmètre du réseau contre les efforts des mauvais acteurs. L'approche "castle-and-moat"régit l'accès à partir d'un périmètre de réseau statique. Mais la combinaison désordonnée de VPN, de sécurité du courrier électronique, de pare-feu, etc. est obsolète dans notre nouvel environnement de vie professionnelle. Les environnements complexes multi-clouds, utilisant des plateformes comme Amazon AWS et Microsoft Azure, les environnements hybrides et l'adoption rapide des applications dans le cloud signifient qu'une approche basée sur le périmètre n'est plus défendable. Les adversaires utilisent l'approche de sécurité basée sur le périmètre contre les organisations. Certaines des pires attaques ont réussi parce que les cybercriminels ont pénétré les pare-feu. Ils se déplaçaient sans être détectés d'un appareil à l'autre en utilisant des informations d'identification fiables, en exploitant des privilèges ou en élevant les privilèges de l'intérieur.

Faire confiance à tout le monde à l'intérieur du périmètre n'est plus efficace. C'est pourquoi les grandes entreprises adoptent des modèles de Zero Trust pour renforcer leur sécurité et éviter les pires effets des attaques et des violations. Un modèle de sécurité de Zero Trust reconnaît que des menaces potentielles existent à l'intérieur et à l'extérieur du périmètre traditionnel. Il part du principe que vous n'êtes jamais à l'abri. Une attaque est inévitable ou déjà en cours. Les dispositifs peuvent déjà être compromis

et les demandes d'accès ne sont pas fiables tant qu'elles ne sont pas vérifiées. Il s'agit d'un changement d'état d'esprit qui élimine la confiance implicite. Les organisations fonctionnent en ne faisant confiance à personne, que ce soit à l'intérieur ou à l'extérieur des périmètres du réseau. Au lieu de cela, elles traitent chaque utilisateur et chaque appareil comme une menace potentielle.

Dans un environnement de Zero trust, tous les utilisateurs, appareils et applications sont vérifiés avant de pouvoir se connecter aux réseaux d'entreprise. Ils sont continuellement évalués pendant une session pour détecter toute activité inhabituelle jusqu'à ce qu'ils quittent le réseau, offrant ainsi une protection en temps réel. L'évaluation utilise des détails granulaires et l'application des politiques. Elle tient compte du contexte et de l'emplacement, de la posture des terminaux et des applications, des contrôles d'accès aux données et de l'automatisation limitant l'accès à ce qui est nécessaire.

Accès privilégié

Le modèle de sécurité "Zero Trust" s'applique à l'ensemble des réseaux et fait appel à plusieurs couches d'outils et de méthodes de sécurité pour minimiser les risques. Nous allons ici nous focaliser sur une seule couche : la gestion des accès privilégiés (PAM).

Les outils et les politiques de PAM constituent l'une de vos dernières lignes de défense pour déjouer les adversaires une fois qu'ils se sont infiltrés. Dans le nouveau monde de la Zero Trust, les outils PAM traitent tout le monde, à l'intérieur comme à l'extérieur de l'organisation, comme une menace potentielle, afin de réduire le risque que les attaquants obtiennent vos données critiques si les systèmes sont compromis. Même sans une approche de Zero Trust, la gestion des accès privilégiés était un élément fondamental reconnu de la cybersécurité que de nombreuses

organisations ont mis en place. Mais quand votre organisation a-t-elle examiné pour la dernière fois les paramètres et les politiques des outils de gestion des accès à privilèges ? Il n'y a pas de place pour la complaisance. Il peut y avoir des centaines ou des milliers de serveurs dans votre environnement et de nombreux administrateurs superutilisateurs dont les actions sur les ressources ne sont pas identifiables à l'heure actuelle. Le logiciel PAM ne peut pas être considéré comme une activité "à tout faire". L'informatique évolue au fil du temps dans les opérations et les dispositifs s'adaptent très bien aux commandes de travail à domicile. Les responsables de la sécurité et de la gestion des risques doivent considérer la gestion des privilèges comme un processus continu. Identifiez, vérifiez, protégez et surveillez constamment tous les comptes privilégiés. Il s'agit notamment des comptes d'administration de domaine, des comptes d'administration de services externes, des comptes d'administration locale et d'autres comptes permettant d'installer et de gérer des logiciels.

Définir des contrôles granulaires

L'examen et l'audit de l'accès sont une composante principale du Zero trust, qui s'attaque de front à l'intention des cybercriminels de se déplacer latéralement. Et votre logiciel de gestion des privilèges et des accès est un outil fondamental.

Le moment est venu de recalibrer vos politiques et technologies PAM. Appliquez des politiques d'accès à granularité fine basées non seulement sur le rôle de l'utilisateur, mais aussi sur le lieu, l'état de conformité du dispositif, la santé et les données accessibles. Un utilisateur accédant à une application dans l'environnement du bureau est probablement moins risqué qu'en accédant à l'application sur un Wi-Fi public, le contexte est donc essentiel.

Définir les niveaux de privilèges

Reconnaissez que différents types de comptes sont utilisés dans l'organisation. Il s'agit notamment de comptes à privilèges personnels ou partagés, de comptes de service, de comptes d'administrateur local et de comptes principaux, d'identifiants d'application à application et de niveaux de privilèges individuels. Ces différents comptes doivent tous être configurés et déployés sur la base de politiques de privilèges. L'identification des niveaux d'accès, tels que les utilisateurs standard, les utilisateurs de services et les super-utilisateurs, simplifiera le processus de limitation de l'accès aux niveaux supérieurs de privilèges, réduisant ainsi l'exposition.

Identifier les comptes privilégiés

Dans les premiers jours de la pandémie, les équipes informatiques ont accordé aux utilisateurs davantage de droits d'accès en raison de l'urgence à maintenir la productivité. Par exemple, pour installer de nouveaux programmes afin d'accélérer les opérations. Mais ces autorisations élevées sont souvent restées en place des mois après que l'utilisateur en ait eu besoin. Pourtant, nous avons constaté une augmentation de l'ingénierie sociale sophistiquée pendant la pandémie.

Des courriels de hameçonnage sur le thème du coronavirus ont diffusé le malware Emotet Trojan permettant aux pirates de s'introduire dans les comptes. Une fois à l'intérieur, les attaquants ont utilisé des comptes utilisateurs privilégiés pour se déplacer sur le réseau. Il est donc essentiel de passer en revue les comptes administratifs accordés pour une tâche spécifique et de les rétablir en comptes d'utilisateur standard.

Les comptes privilégiés et les comptes de service oubliés, orphelins et non gérés depuis longtemps offrent des portes dérobées accessibles

qui font courir des risques inutiles à votre organisation. L'existence d'un accès privilégié non géré comporte un risque important, élargissant la surface d'attaque des cybercriminels.

C'est ici que vos outils PAM doivent trouver les comptes privilégiés. Commencez par analyser et découvrir chaque compte privilégié et chaque cas d'utilisation. Déterminez qui a accès au compte administrateur et qui a des privilèges élevés. Classez les accès en fonction du risque et de l'exposition aux actifs et données critiques. Examinez tous les scénarios. Par exemple, un utilisateur disposant d'un accès privilégié pour travailler sur une tâche dans un actif peut-il, par inadvertance, accéder à d'autres contrôles ou applications ?

Il est essentiel de savoir à quels comptes privilégiés on accède, d'enregistrer qui est propriétaire des ressources et de gérer la délivrance des accès. Il est également important de mettre en place des processus pour découvrir les serveurs ou les applications qui offrent des droits d'accès privilégiés. Comparez les personnes qui ont été précédemment autorisées à accéder aux comptes, aux applications et aux bases de données avec celles qui y ont accès.

Nous avons souligné précédemment que le contexte est essentiel, et il est tout aussi important de considérer et d'enregistrer où l'accès a lieu et quand. Une fois que les personnes disposant d'un accès administrateur ou élevé sont identifiées, déterminez si les privilèges supplémentaires sont toujours nécessaires en fonction des politiques granulaires et supprimez les accès excessifs. Pour suivre l'évolution constante du personnel, des appareils, des systèmes et de l'infrastructure, la découverte et l'identification complètes des accès privilégiés doivent être une activité permanente.

Utiliser le principe des privilèges réduits

Le principe de Zero Trust consiste à appliquer le principe du moindre privilège à nos utilisateurs, applications et périphériques. Accordez juste assez de privilèges aux utilisateurs, aux administrateurs système et aux administrateurs de base de données, et n'autorisez des privilèges élevés qu'en cas de besoin. Pour suivre ce principe, accordez aux utilisateurs des droits d'accès privilégiés en fonction de la personne qui demande les autorisations. Déterminez pourquoi une personne a besoin d'un accès. Garantissez le niveau d'accès minimal requis pour remplir un rôle et le moins de temps possible. Il est tout aussi important d'appliquer le principe du moindre privilège aux entités non humaines. Examinez tout ce qui utilise des informations d'identification, comme les outils d'automatisation des processus robotiques, les scripts PowerShell ou les informations d'identification codées en dur dans les outils DevOps tels que Chef et Puppet. Tirez parti de votre solution PAM pour utiliser des appels d'API pour la récupération des mots de passe et éliminer les mots de passe codés en dur.

Le recours plus fréquent à l'externalisation des fonctions de back-office et des fonctions centrales a conduit à un accès plus important des fournisseurs aux systèmes critiques tels que les systèmes de santé. Appliquez le même principe du moindre privilège à chaque décision d'accès aux fournisseurs et sous-traitants tiers. Veillez à surveiller et à consigner leur activité d'accès dans le cadre de vos processus. Lorsque les travailleurs ont besoin de privilèges plus élevés, utilisez des contrôles juste-à-temps pour limiter l'exposition. La meilleure façon d'y parvenir est de mettre en place des demandes d'accès et des processus d'approbation juste à temps. Demandez aux utilisateurs de soumettre des demandes d'élévation de privilèges pour une durée déterminée. Un processus de demande et d'approbation défini garantit que la productivité n'est pas affectée, mais la sécurité Zero Trust reste au premier plan des décisions

d'accès. L'utilisation de vos outils de gestion de l'accès aux privilèges pour gérer comment et pourquoi les comptes à privilèges sont configurés empêchera toute prolifération future.

Verrouiller les appareils et les applications

En suivant l'approche de Zero Trust, prenez des mesures pour passer en revue les ordinateurs portables et les postes de travail des utilisateurs finaux. Verrouillez chacun d'entre eux en supprimant les droits d'administration locale. Même une action aussi simple que la possibilité pour un utilisateur de modifier la date et l'heure de sa machine peut entraîner des complications et affecter les efforts d'audit. Ensuite, soyez plus précis. Par exemple, mettez à jour les paramètres et sélectionnez les processus et les applications qu'un utilisateur peut arrêter sur son ordinateur. En régulant les paramètres, les utilisateurs éviteront de désactiver par inadvertance les logiciels de protection de la sécurité. Réduisez le risque d'introduction de logiciels malveillants en limitant les téléchargements d'applications. N'autorisez que les applications de confiance à s'exécuter et bloquez les autres. Les applications de confiance doivent toujours être exécutées avec des privilèges standard afin d'atténuer les risques de sécurité. Lorsqu'une application n'est plus utilisée, déprovisionnez-la. Le déprovisionnement permet non seulement de sécuriser les systèmes, mais aussi de réaliser des économies grâce à la récupération et à la réutilisation des licences.

Séparer les informations d'identification

Pour des raisons de rapidité, de nombreux administrateurs ne séparent pas aujourd'hui leurs comptes d'administrateur des comptes de travail des utilisateurs finaux. Ces mêmes informations d'identification sont également utilisées sur tous les serveurs. Pourquoi est-ce un problème ? Les acteurs de la menace ciblent les comptes dotés de privilèges

administratifs pour accéder aux ressources de l'entreprise et exécuter des charges utiles. L'attaque SolarWinds Sunburst de décembre 2020 en est un excellent exemple, car d'autres entreprises de sécurité sont devenues une voie d'accès pour d'autres attaques. La portée de l'explosion a touché des centaines de grandes entreprises et d'agences gouvernementales américaines. Les super-utilisateurs ne doivent pas effectuer de tâches d'utilisateur final, comme l'accès aux e-mails, lorsqu'ils sont connectés à l'aide de comptes d'administrateur Windows ou de privilèges de compte principal Linux. Faites respecter la séparation des privilèges. Créez des comptes surveillés distincts pour les tâches administratives. Séparez-les des comptes standard des utilisateurs finaux et des comptes d'audit.

Gérer les comptes privilégiés

En appliquant la règle "ne faites confiance à personne", il est important de gérer les comptes privilégiés, même légitimes. Commencez par des contrôles de cyberhygiène de base. Par exemple, assurez-vous que ces comptes n'utilisent pas de mots de passe par défaut. N'oubliez pas que les attaquants détournent les comptes à privilèges pour lancer des attaques de l'intérieur et ne pas être détectés. Les comptes à privilèges doivent donc être vérifiés lors de la connexion au réseau. Pendant que la session est en cours, utilisez vos outils PAM pour continuer à surveiller l'activité du compte. Examinez toute déviation du comportement de l'utilisateur pour vous assurer qu'un compte n'a pas été compromis. Les activités à risque identifiées doivent déclencher automatiquement la fin de la session pour éviter l'abus de privilèges. Exercez les mêmes niveaux de gestion et de supervision sur les fournisseurs tiers et les sous-traitants ayant un accès privilégié à vos systèmes. Surveillez de près les sessions privilégiées ou même les sessions fantômes des fournisseurs et entrepreneurs tiers. Mettez fin à toute session qui semble suspecte ou qui viole les politiques d'accès privilégié.

Automatiser et intégrer

Pour établir une visibilité et un contrôle complets dans votre modèle de Zero-Trust, automatisez et intégrez les outils autant que possible. Facilitez l'expérience des demandes d'accès privilégié. Intégrez les outils PAM à vos outils de gestion des services informatiques. Créez des flux de travail pour gérer les demandes d'élévation en temps réel à partir de vos outils de gestion des services. Utilisez également des flux de travail automatisés pour révoquer efficacement les accès temporaires. Évitez que le scénario du "set it and forget it" ne se produise. Empêchez les hackers de trouver des comptes orphelins ou abandonnés et d'élever les privilèges. Ajoutez des flux de travail automatisés pour identifier et supprimer ces comptes et économiser du temps de recherche à l'avenir. Parfois, des administrateurs de confiance accèdent à des comptes et apportent des modifications en dehors des outils de protection PAM. Éliminez ces zones d'ombre. Le partage des données et la corrélation des événements avec d'autres outils tels que les outils de gestion des informations et des événements de sécurité (SIEM) soutiennent votre approche de Zero Trust.

Il est plus facile de détecter les accès ou les anomalies dans les opérations d'accès privilégiés à l'intérieur et à l'extérieur de votre environnement PAM, avec une meilleure visibilité.

Soyez prêt pour l'audit

Les normes de conformité et les réglementations sectorielles telles que SOX, HIPAA et PCI DSS obligent les organisations à suivre et à surveiller l'accès aux systèmes critiques et à prouver aux auditeurs que les contrôles de sécurité nécessaires sont en place. Utilisez des outils de PAM pour alléger la charge d'audit. Vos outils de PAM doivent enregistrer, surveiller et auditer toute activité d'accès privilégié et de session privilégiée. Veillez également à enregistrer les données relatives aux approbations d'accès.

Des rapports granulaires et des enregistrements de sessions inviolables facilitent la gouvernance et la responsabilité des accès privilégiés.

Comment ManageEngine peut vous aider dans votre démarche de Zero Trust ?

Alors que les entreprises adoptent des environnements de travail distants ou hybrides et se tournent vers des modèles Zero Trust pour la protection, il est essentiel de s'assurer qu'aucun accès privilégié aux systèmes, données ou autres actifs critiques n'est laissé sans gestion, inconnu ou non surveillé. ManageEngine fournit des solutions pour gérer les comptes utilisateurs privilégiés, l'accès administratif aux actifs informatiques critiques et les mandats de conformité. PAM360 de ManageEngine est une solution complète de gestion des accès à privilèges qui s'intègre facilement au modèle de Zero trust d'une organisation. Elle défend les organisations contre l'abus de privilèges en régulant l'accès aux informations sensibles de l'entreprise. PAM360 permet de gérer les accès pour l'ensemble de l'infrastructure informatique, y compris les bases de données, les commutateurs, les routeurs, les pare-feu et les équilibreurs de charge. La solution intègre une puissante gouvernance des accès privilégiés, l'automatisation des flux de travail et des analyses avancées.

PAM360 comprend également des intégrations contextuelles avec divers services informatiques pour une corrélation plus approfondie des données d'accès privilégié et des données globales du réseau. Ces intégrations permettent un contrôle et une gouvernance plus stricts de vos autorisations administratives et de l'accès à l'ensemble de votre infrastructure informatique - utilisateurs, systèmes et applications.

Soutenir la gouvernance des comptes

La première étape vers Zero Trust consiste à comprendre votre environnement de sécurité. PAM360 découvre automatiquement tous les comptes privilégiés de l'infrastructure informatique, y compris les applications dans le cloud. La solution peut réinitialiser à distance les mots de passe des comptes d'administrateur local Windows et des comptes de route Linux. Il est simple de capturer tous les événements associés aux comptes à privilèges sous forme de journaux et de rapports d'audit riches en contexte. Les rapports granulaires et les enregistrements de session facilitent la gouvernance et fournissent une meilleure vision des sessions privilégiées. PAM360 fournit un point central de gestion pour l'audit et la conformité. Évitez de vous démener pour rassembler des données pour les audits de conformité à la dernière minute ; démontrez facilement la conformité aux auditeurs et aux enquêteurs judiciaires avec les rapports prêts à l'emploi de PAM360 sur diverses réglementations de conformité telles que PCI-DSS, NERC-CIP, ISO/IEC 27001 et RGPD.

Élévation des privilèges

PAM360 est un outil puissant de régulation des privilèges. Il permet l'autorisation, l'attribution et le suivi des contrôles pour les comptes de domaine et les comptes locaux. Le logiciel peut élever les privilèges pour une durée limitée, ce qui réduit le risque d'exposition permanente. Pour les demandes d'accès juste-à-temps, PAM360 fournit un mécanisme de flux de travail demande-approbation permettant aux utilisateurs de soumettre une demande. Grâce aux applications iPhone, Android et Windows, les administrateurs peuvent autoriser les demandes depuis n'importe où.
Lorsque plusieurs équipes possèdent un seul appareil, il est également possible d'obtenir des approbations doubles avec PAM360.

Surveillance des privilèges

Une fois les privilèges accordés, dans le cadre de l'approche " ne faire confiance à personne ", il est essentiel de surveiller étroitement les activités des utilisateurs privilégiés. PAM360 offre la possibilité de filtrer les sessions privilégiées en temps réel, par exemple pour vérifier les activités des contractants ou des fournisseurs tiers. La solution permet de mettre fin immédiatement à la session en cas de détection d'une utilisation abusive des privilèges. PAM360 peut également enregistrer, sauvegarder et lire une session sous forme de fichiers vidéo à des fins de suivi et d'audit.

Gestion des sessions

Pour empêcher tout accès non autorisé et garantir la sécurité des systèmes, les administrateurs informatiques doivent désactiver les autorisations d'accès SSH et les services de bureau à distance sur les appareils de l'entreprise. PAM360 agit comme une passerelle pour démarrer une session à distance, lancer des connexions à distance et se connecter aux machines cibles via des connexions RDP, SSH, SQL, VNC ou Web. Exploitez la fonctionnalité de PAM360 pour un contrôle granulaire et pour restreindre les activités des utilisateurs. La solution peut contrôler les applications auxquelles un utilisateur a accès grâce à des fonctionnalités de liste blanche.

Automatisation et intégration des flux de travail

La prise en charge par PAM360 d'un modèle de Zero Trust est très étendue. L'intégration contextuelle de PAM360 avec les applications et les appareils de l'infrastructure informatique permet d'automatiser les tâches et d'améliorer la visibilité. Les organisations peuvent éliminer les informations d'identification codées en dur dans les scripts d'automatisation avec PAM360. La solution s'intègre aux outils DevOps pour récupérer les

informations d'identification en temps réel. Utilisez l'API RESTful et l'API SSH CLI pour remplacer les noms d'utilisateur et les mots de passe dans PowerPoint. les noms d'utilisateur et les mots de passe dans les scripts PowerShell, les fichiers de configuration ou tout autre élément contenant des informations d'identification codées en dur. Intégrez PAM360 aux outils d'automatisation des processus robotiques pour récupérer en toute sécurité les informations d'identification et les transmettre aux robots pour qu'ils effectuent des opérations.

PAM360 s'intègre également à vos outils de gestion des services informatiques. Cette intégration permet aux demandes et aux approbations d'habilitations d'avoir lieu dans l'environnement ITSM. Sans le contexte nécessaire, il est facile de se laisser induire en erreur par les angles morts des incidents de sécurité. PAM360 associe les données privilégiées aux journaux d'événements des points d'extrémité pour une corrélation des événements en fonction du contexte. L'intégration avec des outils SIEM permet de transmettre toutes les données d'audit brutes de PAM360 à des solutions SIEM, telles que Splunk, pour une analyse plus approfondie. Les intégrations garantissent un accès complet, augmentant la sensibilisation et la visibilité pour permettre des décisions plus éclairées.

Gestion des clés SSH et des certificats SSL

Gérez les clés SSH et les certificats SSL en toute simplicité. PAM360 fournit un référentiel centralisé permettant de stocker les clés SSH pour l'administration du cycle de vie et l'application des politiques. La solution découvre les clés, supprime les clés inutilisées, et génère et déploie de nouvelles clés sur les systèmes cibles. De même, PAM360 découvre, consolide et gère les certificats SSL. La solution peut envoyer des alertes d'expiration et vérifier les certifications pour détecter les vulnérabilités. Elle peut également automatiser les flux de travail pour la génération de certificats.

Détecter les anomalies

Le plus vite vous pouvez déraciner les menaces nuisibles, le plus vite vous pouvez limiter les dégâts. S'intégrant à Analytics Plus de ManageEngine, PAM360 permet une analyse complète des activités des comptes à privilèges. Les capacités d'intelligence artificielle et d'apprentissage automatique détectent en permanence les activités suspectes et nuisibles. En utilisant les données de PAM360, une évaluation et un score de risque sont désignés pour chaque opération. Si un score de risque est dépassé, une notification de seuil est envoyée. La solution peut déclencher des contrôles d'atténuation, comme la fermeture de la session. Elle apprend continuellement le comportement et les modèles des utilisateurs pour détecter les anomalies.

Un signal d'alarme

Le travail à distance, les plateformes et les applications cloud ont redéfini le périmètre de sécurité d'une organisation. Les responsables de la sécurité et de la gestion des risques doivent réévaluer le périmètre de sécurité et renforcer les défenses avec Zero Trust. Ce modèle englobe notre environnement de travail pandémique et post-pandémique, en protégeant les utilisateurs, quel que soit leur emplacement ou leur appareil. Plutôt que de sécuriser le périmètre du réseau, l'approche Zero Trust place les mesures de sécurité à proximité de l'application, du système ou de la ressource à protéger.

Pour vous mettre en position de force et construire une base Zero Trust, exploitez toute l'étendue des pratiques et processus PAM mis en œuvre par des outils efficaces. Utilisez les outils PAM pour tirer parti de la fonctionnalité d'audit afin d'identifier une base de référence et de poursuivre le reporting. Appliquer des politiques plus granulaires. Introduisez des flux de travail pour demander et révoquer l'accès. Vérifiez les accès privilégiés et

administratifs à vos systèmes. Enregistrez et surveillez les sessions d'accès de façon continue. Atténuer les attaques et utiliser PAM comme la pierre angulaire d'un modèle Zero Trust. COVID-19 est notre signal d'alarme à tous les niveaux.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360