ManageEngine
PAM360

Le début de l'administration sans mot de passe et comment s'y préparer

Avec l'adoption rapide de modèles de travail hybrides, les organisations sont confrontées à un défi de taille : se protéger des cybermenaces émergentes. Elles envisagent de plus en plus de nouveaux cadres de sécurité, tels que Zero Trust, pour renforcer leurs périmètres de sécurité, mais même avec de tels cadres avancés, les mots de passe restent la dernière ligne de défense.

Malgré leur polyvalence pour sécuriser l'accès aux actifs critiques, les mots de passe sont la cible principale des cyberattaques. En outre, l'abus de privilèges et les menaces internes sont de plus en plus répandus parmi les organisations qui s'apprêtent à rendre leur stratégie de sécurité infaillible. On sait que plus de 500 millions de mots de passe ont été compromis au cours des dernières années, et cette liste s'allonge de jour en jour.

Un rapport récent de HYPR et Cybersecurity Insiders indique que 96 % des personnes interrogées souhaitent ne plus utiliser de secrets partagés pour l'authentification. Le passage au travail à distance a rendu urgente la recherche d'options d'authentification sans mot de passe pour protéger les ressources et les systèmes privilégiés contre l'abus d'informations d'identification.

Administration sans mot de passe : Une lueur d'espoir à l'horizon

L'administration sans mot de passe est la possibilité d'effectuer des opérations administratives sans avoir besoin d'informations d'identification privilégiées. L'objectif principal de l'administration sans mot de passe n'est pas d'éliminer les mots de passe, mais d'éviter l'exposition des informations d'identification en clair et sous forme de code dur. L'administration sans mot de passe fonctionne selon

la logique simple que si les mots de passe ne sont pas exposés aux utilisateurs, ils ne peuvent jamais être compromis ou mal utilisés.

Lorsque l'administration sans mot de passe est mise en œuvre, les utilisateurs sont automatiquement authentifiés et se voient attribuer les privilèges appropriés pour accéder aux ressources confidentielles. En d'autres termes, ils disposent de tous les droits nécessaires, y compris l'authentification réseau, pour accéder aux applications, bases de données, systèmes d'exploitation, machines virtuelles et autres ressources privilégiées qui nécessitent plusieurs niveaux d'autorisation.

Grâce aux contrôles d'administration sans mot de passe, les équipes informatiques peuvent garantir que l'accès aux systèmes d'information privilégiés est sécurisé et que les informations d'identification ne sont pas partagées ou réutilisées, ce qui signifie que les utilisateurs ne seront pas la proie d'attaques par hameçonnage, par force brute ou par ingénierie sociale. Autre avantage en termes de sécurité, avec cette approche, les données d'authentification des utilisateurs ne sont jamais stockées dans les systèmes et les navigateurs des utilisateurs finaux.

Pourquoi l'absence de mot de passe n'est toujours pas pratique pour certaines entreprises

Bien que les contrôles sans mot de passe constituent une méthode d'administration informatique plus fiable et plus sûre, les entreprises sont confrontées à deux grands défis lorsqu'elles passent à un environnement sans mot de passe : le budget et la complexité de la migration. Le processus de migration implique l'installation de matériel biométrique, ce qui demande un capital initial

important. Il nécessite également de s'éloigner des mécanismes de sécurité existants qui traitent des mots de passe, ce qui peut interférer avec les opérations quotidiennes des organisations.

Contrairement à la biométrie, qui nécessite une marge d'erreur, la nature binaire des mots de passe préserve le processus d'authentification de tout biais. Les mots de passe restent la principale forme d'authentification et la plus efficace, il est donc difficile pour les alternatives sans mot de passe de remplacer les mots de passe. Bien que des améliorations constantes soient possibles, la gestion efficace, le stockage sécurisé et la rotation périodique des mots de passe permettent de protéger les comptes privilégiés sans nécessiter une infrastructure complexe.

Alors que les contrôles d'authentification basés sur la FIDO ont gagné en importance au fil des ans, ils ne peuvent agir que comme un gardien secondaire pour les données privilégiées. Par exemple, Apple donne aux utilisateurs la possibilité de déverrouiller leurs iPhones par reconnaissance faciale, mais la technologie nécessite toujours les mots de passe des utilisateurs pour encoder les données de cartographie du visage dans le stockage interne des appareils. Même si les données de cartographie sont perdues, les utilisateurs peuvent toujours déverrouiller leurs appareils à l'aide de mots de passe.

Une autre idée fausse courante liée à ces contrôles est qu'ils ne peuvent pas être dupliqués ; cependant, les données biométriques sont également vulnérables aux violations. En 2017, des chercheurs japonais ont prévenu que les hackers pouvaient avoir accès aux empreintes digitales à partir de photographies haute résolution.

Les meilleurs protocoles MFA ne font que renforcer les procédures d'authentification classiques basées sur les mots de passe, une entité intrinsèquement vulnérable. L'utilisation d'identifiants à des fins d'authentification oblige les équipes informatiques non seulement à maintenir une base de données de mots de passe en constante augmentation, mais aussi à en garder la trace pour les réinitialiser manuellement et les faire tourner. Si les solutions de gestion des mots de passe aident à appliquer une gouvernance stricte des mots de passe, elles s'appuient toujours sur des politiques rigoureuses et sur MFA pour protéger l'accès aux systèmes privilégiés. Après tout, les mots de passe ne peuvent qu'authentifier les utilisateurs, pas leurs intentions, et les informations d'identification doivent donc être gérées efficacement.

Administration sans mot de passe : Un cas pour la gestion des accès privilégiés (PAM)

L'administration sans mot de passe est un cas d'utilisation inhérent au processus PAM, qui fait le lien entre la gestion des sessions privilégiées, l'accès distant sécurisé et la gestion des comptes utilisateurs. Elle valide les utilisateurs privilégiés sans leur demander de saisir manuellement leurs informations d'identification, afin qu'ils puissent effectuer des actions administratives via des sessions distantes sécurisées (SSH, VNC, SQL ou RDP). L'administration sans mot de passe est différente de l'authentification sans mot de passe, qui implique l'approbation des demandes d'authentification basées sur la biométrie ou d'autres attributs, tels qu'un code PIN ou un mot de passe à usage unique.

Les comptes administratifs sont généralement dotés de privilèges élevés et d'un accès direct aux biens, bases de données et réseaux classifiés d'une entreprise. Cependant, ces comptes sont parfois

délégués à des utilisateurs normaux afin qu'ils puissent exécuter certaines fonctions administratives sur leurs terminaux locaux.

Par exemple, tout utilisateur standard de terminaux Linux peut avoir besoin de privilèges d'administration pour effectuer des activités telles que :

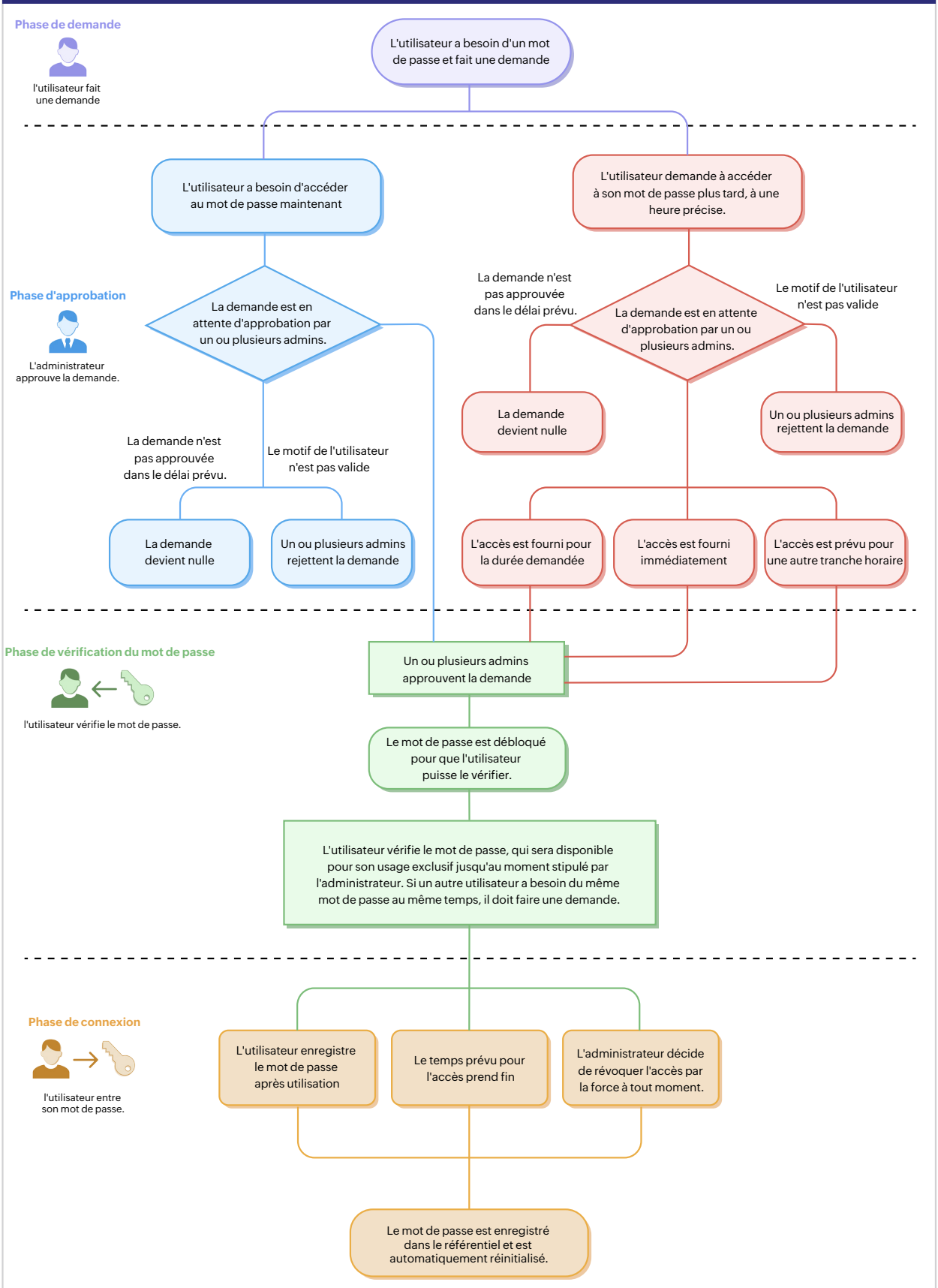
- L'installation de logiciels tiers.
- La configuration de dotfiles.
- Transfert de fichiers propriétaires via PowerShell.
- La mise à niveau vers le dernier système d'exploitation ou le dernier correctif de sécurité.

Dans les cas ci-dessus, les droits d'administration sont accordés soit en attribuant à l'utilisateur un compte administrateur secondaire, soit en faisant de lui un administrateur local temporaire. La duplication des comptes peut créer davantage de vecteurs d'attaque, augmentant ainsi les chances d'activités malveillantes via le phishing, les logiciels malveillants, et autres. Par conséquent, les identifiants administratifs de ces comptes devront être révoqués pour empêcher les acteurs de la menace d'abuser des privilèges qui leur sont associés.

Les environnements sans mot de passe facilitent la sécurisation de ces comptes en appliquant le principe du moindre privilège pour les comptes d'utilisateurs généraux et en élevant les privilèges uniquement lorsque cela est nécessaire. C'est ce que l'on appelle l'accès privilégié "juste à temps", où des utilisateurs sélectionnés reçoivent les privilèges nécessaires pour effectuer les tâches administratives demandées pendant une période donnée.

Au lieu de demander aux utilisateurs de saisir des informations d'identification pour toute tâche administrative temporaire, on leur fait confiance, on les authentifie et on leur accorde tous les droits nécessaires en fonction de la validité de leurs demandes et de leurs niveaux de privilèges actuels. Une fois les actions spécifiées terminées, les privilèges exclusifs sont révoqués, laissant les utilisateurs avec leurs privilèges par défaut.

Workflow du contrôle d'accès par mot de passe



L'authentification des utilisateurs peut être basée sur des mécanismes de confiance standard, tels que leurs mots de passe personnels, le SSO, la biométrie ou MFA, qui jouent un rôle majeur dans la création du contexte de la demande d'administration d'un utilisateur.

Tous les cas d'utilisation ci-dessus montrent que l'administration sans mot de passe est un mélange intéressant de moindre privilège, d'accès à distance et de gestion de comptes privilégiés.

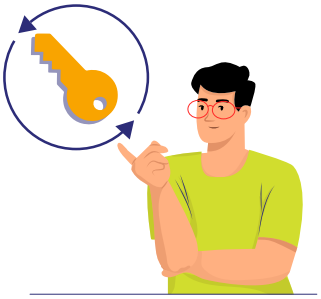
Mise en œuvre de l'administration sans mot de passe : Par où les entreprises peuvent commencer

Les mots de passe, bien que vulnérables, sont là pour rester jusqu'à ce que les options d'authentification sans mot de passe deviennent plus robustes et sans biais. Si les mots de passe des comptes personnels peuvent être protégés à l'aide de contrôles de sécurité standard conformes à la FIDO, tels que la MFA ou la biométrie, les organisations doivent aller au-delà des mots de passe pour protéger les entités privilégiées, telles que les comptes de service et de domaine, les points d'extrémité et les bases de données. Alors que les organisations passent lentement à des alternatives sans mot de passe, elles devraient envisager d'employer une stratégie PAM forte jusqu'à ce que les outils biométriques soient prouvés comme étant infaillibles.

5 étapes pour renforcer l'administration informatique avec des alternatives sans mot de passe

1. **Conservez** une liste complète de tous les comptes, ressources et informations d'identification privilégiés actifs sur votre réseau et mettez cette liste à jour dès qu'un nouveau compte est créé. Stockez les identités privilégiées comme les mots de passe, les identifiants SSH et les certificats SSL dans une chambre forte sécurisée utilisant des algorithmes de cryptage normalisés, tels que AES-256.

2. **Imposez** des politiques strictes en matière de mots de passe qui couvrent la complexité des mots de passe, la fréquence de réinitialisation des mots de passe, la génération de paires de clés SSH fortes, la réinitialisation automatique lors d'une utilisation unique et d'autres contrôles solides.



3. **Permettez aux utilisateurs** privilégiés de lancer des connexions sécurisées, en un clic, à des terminaux distants sans agents, plug-ins de navigateur ou modules complémentaires. Tunnelisez les sessions distantes avec des passerelles cryptées et sans mot de passe pour une protection optimale. Surveillez et enregistrez toutes les sessions et activités des utilisateurs privilégiés en temps réel.

4. **Renforcez** les contrôles du moindre privilège afin d'éliminer les privilèges inutiles de l'administrateur local et de veiller à ce que tous les utilisateurs humains et non humains aient juste assez de privilèges pour effectuer leur travail. Établissez un workflow de demande et de libération pour accorder un accès élevé, juste à temps, à des ressources privilégiées en fonction de la validité des besoins des utilisateurs. À l'expiration de la période demandée, révoquez les privilèges temporaires et changez automatiquement les mots de passe pour invalider les anciennes informations d'identification et empêcher toute tentative d'accès non autorisé à l'avenir.

5. **Auditez** toutes les opérations liées à l'identité, telles que les connexions d'utilisateurs privilégiés, les partages de mots de passe, les tentatives d'accès par mot de passe et les réinitialisations. Ces audits aideront les équipes informatiques à identifier et à éliminer les angles morts et à prendre des décisions éclairées en matière de sécurité.

Comment les entreprises peuvent-elles se préparer à surfer sur la vague du sans mot de passe ?

Le succès de toute entreprise dépend de la confidentialité et de l'exactitude des données qu'elle traite. Par conséquent, le contrôle de l'accès aux données et aux actifs de l'entreprise devrait être primordial pour toute organisation. Pour éviter toute sanction ou poursuite judiciaire due à des violations de données, les organisations doivent garantir un flux de travail rationalisé lorsqu'il s'agit de sécuriser l'accès à leurs données privilégiées.

Les mesures de sécurité traditionnelles ne suffisent plus, car la main-d'œuvre devient de plus en plus mobile et distribuée. Le climat socio-économique actuel, la transition rapide vers des lieux de travail hybrides et l'avènement des outils de travail à distance offrent aux cybercriminels des occasions parfaites de devenir plus créatifs chaque jour qui passe.

Le chemin vers une administration informatique sans mot de passe est un processus progressif avec de multiples étapes, dont la première est la protection des chemins privilégiés. Avec un plan PAM solide en place, les organisations peuvent sécuriser et gérer l'accès aux ressources critiques, améliorer leur posture de sécurité, déjouer efficacement les attaques et assurer la prospérité numérique.

Pour savoir comment les solutions PAM de ManageEngine peuvent vous donner une longueur d'avance sur l'administration sans mot de passe, identifier et éliminer les angles morts de la sécurité, et réduire les risques de menaces internes et d'abus de privilèges, contactez-nous dès aujourd'hui.

ManageEngine PAM360

ManageEngine PAM360 est une solution complète de gestion des accès privilégiés pour les entreprises. Elle permet aux administrateurs informatiques et aux utilisateurs privilégiés d'obtenir un contrôle complet et granulaire des ressources informatiques critiques, telles que les mots de passe, les signatures et certificats numériques, les clés de licence, les documents, les images, les comptes de service, etc.

Reconnu par Gartner et Forrester comme l'un des meilleurs fournisseurs de PAM de 2020, ManageEngine PAM360 comprend des intégrations contextuelles avec des solutions SIEM, de billetterie et d'analyse pour aider les équipes informatiques à construire des modèles de comportement des utilisateurs afin d'identifier et de mettre fin aux activités anormales, de générer des rapports d'audit et de conformité complets et de prendre des décisions de sécurité basées sur les données.