jamf

Comment assurer votre sécurité sans mot de passe

Motsdepasse, Motsdep@sse1, Mot$dep@asse1234!

Depuis longtemps, les mots de passe aident à empêcher l'accès aux personnes non autorisées et à accorder l'accès à celles qui sont autorisées. Ils sont les gardiens de votre appareil et de vos données et les défendent avec toute la puissance que huit caractères minimum, un chiffre et un caractère spécial peuvent rassembler.

Notre empreinte numérique continue d'augmenter, l'écosystème des appareils se développe et les besoins des utilisateurs en déplacement évoluent, de sorte que les mots de passe sont de moins en moins pratiques et appréciés. Les utilisateurs interagissent avec de plus en plus d'appareils et d'applications et chaque accès présente un risque pour la sécurité si le mot de passe associé est compromis.

Tous les administrateurs informatiques connaissent la terrible liste des mots de passe les plus utilisés, car les utilisateurs finaux doivent prouver qu'ils sont bien la personne qu'ils disent être pour pratiquement chacune des interactions avec leur appareil et les données qui s'y trouvent.

Les 10 mots de passe les plus utilisés[1]

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

1. D'après Cybernews.com

Dans ce livre blanc, nous allons aborder les points suivants :

- Sécurité renforcée vs facilité d'utilisation
- Ce que signifie « sans mot de passe »
- Pourquoi les organisations devraient s'intéresser aux workflows sans mot de passe
- La réponse de Jamf aux problèmes de mots de passe

Sécurité renforcée vs facilité d'utilisation

Le problème de sécurité numéro 1 pour les organisations aujourd'hui est **le vol d'identifiants de connexion.** Cela vous surprend ? Et que pensez-vous du fait que **80 % des fuites de données impliquent des mots de passe volés ou faibles** ? Même avec la mise en place de règles de mots de passe plus forts, les violations de serveurs peuvent révéler des mots de passe et, par conséquent, des informations sur l'entreprise et les employés. De plus, les adversaires de la sécurité de l'information utilisent des méthodologies et des types d'attaques de plus en plus sophistiqués. Les attaques de phishing, les notifications push et le piratage de compte visent directement des utilisateurs crédules, en tentant d'obtenir un accès à leurs appareils et données essentielles.

Au fil du temps, le besoin d'une sécurité renforcée a conduit les services informatiques à exiger des mots de passe plus complexes et une rotation des mots de passe pour répondre au problème. Si ces mesures supplémentaires ont aidé et doivent être considérées comme de « bonnes pratiques », elles ont également créé des difficultés dans l'expérience utilisateur. De nombreux utilisateurs se sont simplifié les choses en créant des mots de passe plus faibles, en les notant et parfois même en les cachant sous leurs claviers où n'importe qui peut les trouver. Ceux ayant créé et utilisé des mots de passe complexes ont aussi essuyé des revers : une augmentation des tickets d'assistance en raison d'oublis.

Même si une réinitialisation de mot de passe n'est pas un type de ticket particulièrement complexe à résoudre, cette tâche répétitive peut devenir fastidieuse pour les administrateurs informatiques embauchés pour gérer des objectifs plus ambitieux. Plus encore, le temps passé par votre équipe informatique à résoudre des tickets ingrats vous coûte de l'argent. **La réinitialisation d'un mot de passe coûte aux sociétés 70 $ en moyenne**. Et lorsque vous additionnez tout le temps consacré à ces tickets, cela représente une somme très importante pour certaines entreprises. Pour l'utilisateur final, l'oubli d'un mot de passe et le temps perdu à attendre qu'il soit réinitialisé ralentissent le travail et la productivité. Cependant, ces coûts en temps et en argent ne suffisent pas toujours à motiver les équipes de sécurité ou les utilisateurs à se pencher sérieusement sur la question des mots de passe.

L'augmentation des besoins en sécurité pour empêcher les attaques et protéger les données de l'entreprise et des clients a entraîné une augmentation des budgets de sécurité des organisations. Toutefois, les violations augmentent également, et l'augmentation du budget alloué à la prévention des mots de passe compromis n'est pas proportionnelle au problème que ces violations posent. En fait, **moins de 10 % du budget global est consacré à l'élimination des identifiants compromis, alors qu'ils représentent plus de 80 % de toutes les violations**. C'est là que les workflows sans mot de passe peuvent aider.

Que signifie « sans mot de passe » ?

D'ici 2022, **Gartner prévoit que 60 % des grandes entreprises et des multinationales, ainsi que 90 % des entreprises de taille moyenne adopteront des méthodes sans mot de passe dans plus de 50 % des cas d'utilisation**.

Pourquoi ? Parce que, par nature, un workflow sans mot de passe pour l'authentification des utilisateurs élimine le problème des mots de passe faibles tout en supprimant les contraintes liées aux mots de passe pour les utilisateurs. Cela signifie aussi que les organisations n'ont pas besoin de stocker des mots de passe qui risquent d'être exposés et compromis. En d'autres termes, ce workflow permet de remédier à quasiment tous les inconvénients des mots de passe dont nous avons parlé.

Pour lancer avec succès des workflows sans mot de passe, une organisation doit offrir à ses utilisateurs un moyen de s'authentifier (de prouver leur identité) au moment de la connexion aux ressources, données ou logiciels auxquels le service informatique les a autorisés à accéder. Il est essentiel que les responsables de la sécurité et de la gestion des identités et des accès connaissent bien les concepts d'authentification et d'autorisation pour la gestion des identités.

Le système de cartes à puce est un exemple de méthode d'authentification. Une carte à puce est une carte physique, qui ressemble à une carte de crédit, contenant des clés cryptographiques directement liées à un utilisateur et qui constitue une méthode sécurisée pour s'authentifier. Le problème, c'est que ces systèmes sont longs à mettre en œuvre, très coûteux et représentent un matériel supplémentaire que l'utilisateur final doit gérer. À moins que votre organisation ne soit un cas d'utilisation à haut risque, le coût et le risque que les utilisateurs finaux perdent ou endommagent leur carte à puce l'emportent sur la menace potentielle, ce qui rend ce niveau de sécurité inutilement excessif.

Qu'est-ce que l'authentification sans mot de passe ?

L'authentification sans mot de passe est une méthode d'authentification au cours de laquelle l'utilisateur peut se connecter à un système informatique sans saisir de mot de passe ni répondre à une question secrète.

Qu'est-ce que l'authentification basée sur les certificats ?

L'authentification basée sur les certificats est l'utilisation d'un certificat numérique pour identifier un utilisateur, un ordinateur ou un appareil avant d'accorder l'accès à une ressource, un réseau, une application, etc.

Qu'est-ce que l'authentification multifacteur ?

L'authentification multifacteur est un processus d'authentification qui oblige l'utilisateur à fournir plusieurs facteurs de vérification pour accéder à une ressource. Il peut s'agir d'un code PIN sur son téléphone, de la fonctionnalité **Face ID**, d'une vérification de l'empreinte digitale ou autre.

L'exemple le plus commun de solution sans mot de passe est la biométrie. Les fonctionnalités Face ID et Touch ID sont des exemples connus de tous les utilisateurs Apple. La biométrie permet à l'utilisateur de s'authentifier sans saisir de mot de passe ou sans avoir besoin d'un code secret ou d'une question de vérification qui risquent d'être volés ou devinés. Votre visage est à vous, et votre pouce est à vous - difficile de les voler. Ajoutez des codes PIN tournants et vous avez une sécurité deux fois plus efficace.

Nous avons expliqué pourquoi les mots de passe ne sont plus la méthode la plus sûre pour l'accès aux appareils et aux ressources, et pourquoi ils sont également pénibles pour les utilisateurs qui doivent les saisir à longueur de journée. Avec l'évolution vers le travail à distance et hybride, les organisations doivent désormais envisager de meilleures mesures de sécurité prenant en compte l'expérience de l'utilisateur final. Voyons comment la transformation numérique pousse les organisations à adopter des workflows sans mot de passe.

Pourquoi les organisations doivent-elles s'intéresser aux solutions sans mot de passe ?

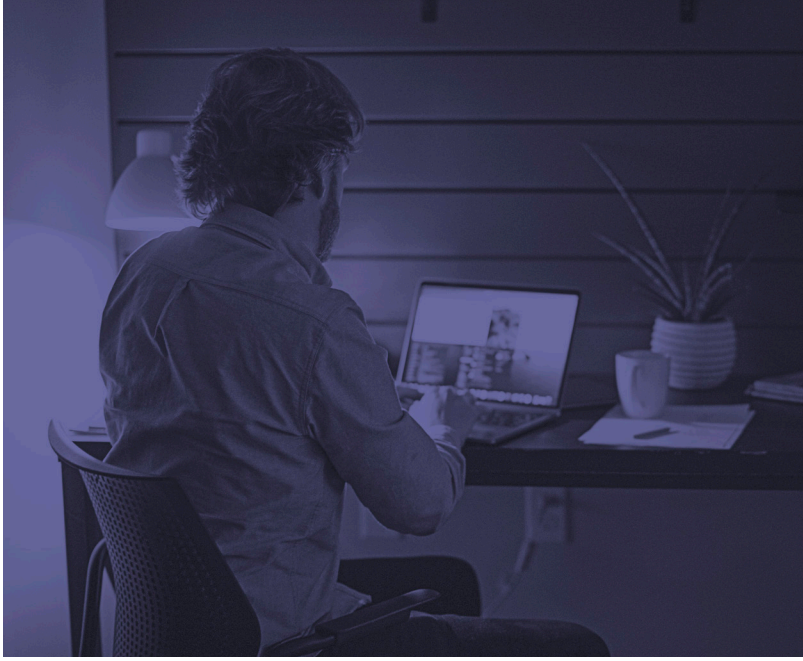
Si les failles de sécurité associées aux mots de passe brièvement décrites au début de ce document ne suffisent pas pour vous convaincre d'adopter des workflows sans mot de passe, explorons la transformation numérique et son effet sur les mots de passe de façon plus approfondie.

Employés à distance

Le travail à distance et hybride met l'accent sur l'importance d'une expérience utilisateur et d'une sécurité à distance excellentes, accélérant ainsi l'urgence de l'authentification sans mot de passe. La connexion à distance des utilisateurs finaux joue ici un rôle clé. Les utilisateurs peuvent accéder à leurs appareils et ressources de n'importe où : chez eux, au bureau, au café, au parc, etc. Cette flexibilité et cette commodité s'accompagnent d'un risque, car les utilisateurs sont en dehors du périmètre de l'entreprise. Ils peuvent se trouver sur des réseaux non sécurisés, ce qui crée des failles dans la couche de sécurité et ouvre la voie aux attaques. L'utilisation d'un workflow sans mot de passe fiable et clair pour accéder à tout ce dont l'utilisateur a besoin est un moyen facile de réduire les risques de menaces. Plus besoin de saisir des mots de passe qui peuvent être volés et moins de tickets support : la sécurité sans les contraintes liées aux mots de passe.

Travail dans le Cloud

L'informatique dans le Cloud a changé la plupart des infrastructures informatiques modernes. Puisque le périmètre d'entreprise sur site est obsolète et que les organisations passent au Cloud, leur stratégie de gestion des identités doit faire de même. Les applications et les ressources sont partout dans le Cloud. Le service informatique doit trouver un moyen sécurisé d'accorder un accès aux employés et d'assurer leur productivité. Une solution sans mot de passe offre un accès sécurisé et en toute transparence au Cloud et aux applications qui s'y trouvent.



Réduction des coûts de gestion des mots de passe

D'après le **Forum économique mondial**, les employés du monde entier passent en moyenne 11 heures chaque année à saisir ou à réinitialiser des mots de passe. Multipliez ce chiffre par le nombre d'employés au sein de votre organisation : cela représente énormément de temps perdu à gérer des mots de passe. Si l'implémentation d'une nouvelle solution a un coût, celui-ci est mineur par rapport aux heures gaspillées à réinitialiser des mots de passe et à la perte de productivité des employés.

Un tremplin pour une productivité accrue

S'ils passent moins de temps à gérer des mots de passe, les employés peuvent consacrer plus de temps à leurs tâches, avec un accès illimité à leurs ressources : leurs journées sont plus productives. Non seulement les coûts sont réduits s'il y a moins de mots de passe et de risques associés à gérer, mais l'amélioration de la productivité des employés entraîne également une augmentation des revenus.

Il s'agit là simplement de quelques exemples illustrant comment les mots de passe, sujet largement ignoré pendant des années, peuvent être améliorés pour contribuer à la stratégie de sécurité globale d'une société, ainsi qu'à ses résultats et à sa santé financière. Il n'est pas difficile de comprendre pourquoi les workflows sans mot de passe sont considérés par beaucoup d'entreprises comme une part essentielle de leurs plans de transformation numérique.

La réponse de Jamf aux soucis de mots de passe : Jamf Unlock

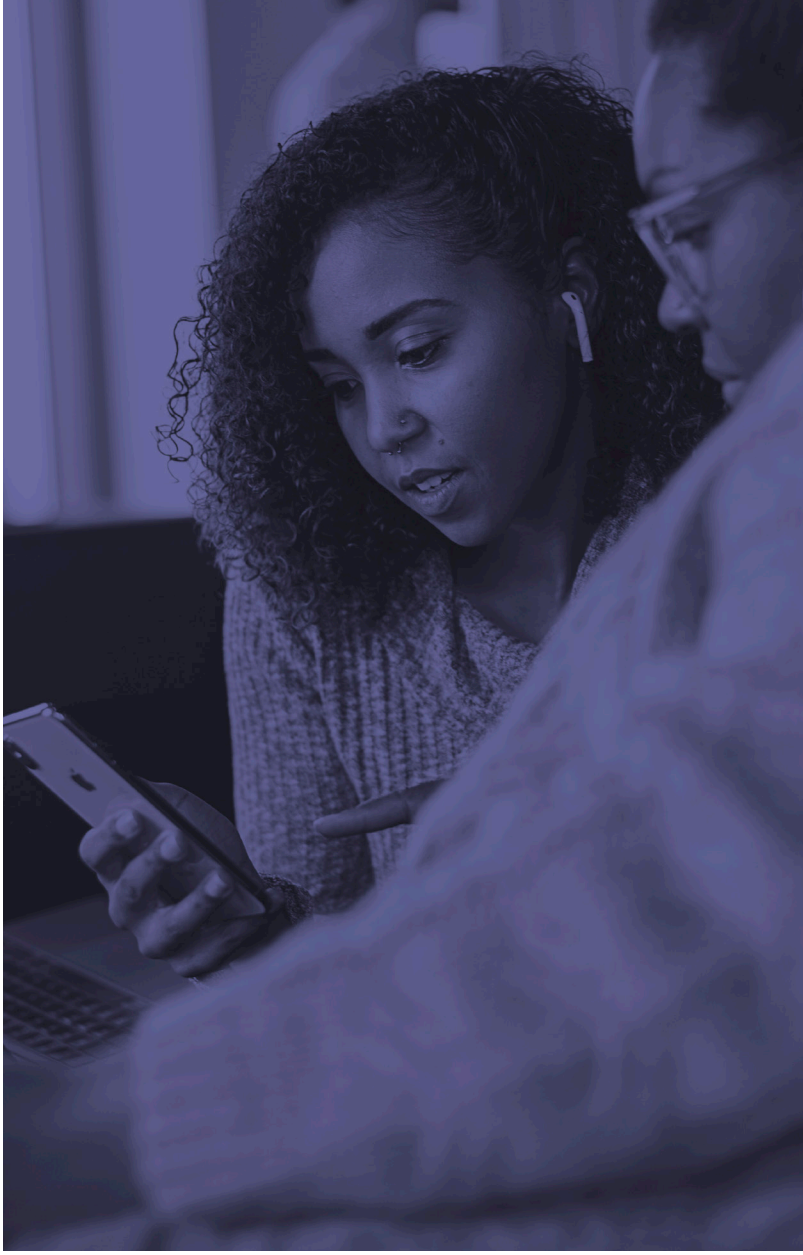
Au lieu de s'appuyer sur un matériel non géré et coûteux – comme les cartes à puce – Jamf Unlock, une fonctionnalité intégrée à Jamf Connect, fournit un workflow sans mot de passe sur l'appareil que les utilisateurs ont toujours sur eux (leur iPhone) pour déverrouiller leur Mac en toute sécurité. Le workflow Jamf Unlock offre une connexion et un processus d'authentification plus sécurisés en plus d'une expérience simple et transparente pour l'utilisateur final. Il répond aux besoins d'authentification du système Mac avec un authentifiant exécuté sur l'appareil iOS d'un utilisateur plutôt qu'une saisie de mot de passe sur son Mac.

1. Les utilisateurs ouvrent l'application iOS Jamf Unlock sur leur iPhone et se connectent pour la première fois avec leurs identifiants Cloud.
2. Les utilisateurs jumellent ensuite leur iPhone avec leur Mac via un code QR.
3. Sur le Mac, les utilisateurs saisissent leur mot de passe local lorsqu'ils sont invités à autoriser le jumelage de l'appareil.
4. Une fois le jumelage terminé, les utilisateurs peuvent commencer à utiliser l'application pour déverrouiller leur Mac en toute sécurité avec la méthode requise par le service informatique : biométrie avec ou sans codes PIN tournants.

Jamf Unlock utilise les frameworks Multipeer Connectivity, CryptoTokenKit et Core Bluetooth d'Apple pour réaliser une authentification sans fil basée sur des certificats entre l'appareil mobile et le Mac d'un utilisateur.

Améliorez votre sécurité et franchissez une nouvelle étape avec Private Access : Unlock n'est qu'un aspect de la sécurisation des données et ressources. Jamf Private Access, véritable plateforme d'accès réseau Zero Trust, assure la sécurisation des connexions de l'entreprise, après l'authentification de l'utilisateur sur son appareil.

En savoir plus sur Private Access



Les workflows sans mot de passe vont sans doute continuer d'évoluer, mais ils ne doivent pas être le seul élément d'une stratégie d'identité et de sécurité moderne. Jamf Unlock est un composant de Jamf Connect pour Mac qui offre aux organisations l'approvisionnement de comptes juste-à-temps, des capacités de **gestion des identités** et une identité Cloud unique pour accéder au Mac et aux ressources. En s'intégrant à un fournisseur d'identités Cloud, Jamf Connect permet aux services informatiques de gérer à distance les données rattachées à l'identité de chaque utilisateur final, et les logiciels et ressources autorisés pour chaque compte. Non seulement cela améliore la sécurité, mais l'approvisionnement de comptes est simplifié. Les utilisateurs peuvent déballer leur nouveau Mac, l'allumer et obtenir immédiatement un accès sécurisé à tout ce dont ils ont besoin.

Renforcez votre sécurité dès aujourd'hui

Le monde du travail est en constante évolution, et cette évolution s'accompagne de défis et d'opportunités. Le télétravail risque d'offrir aux attaquants et aux pirates de nouvelles opportunités, mais il aboutit également à la création de nouveaux workflows et solutions pour les administrateurs informatiques, les responsables de la sécurité de l'information et les utilisateurs finaux.

Bien que les spécialistes de la sécurité de l'information donnent la priorité à la sécurité, ils doivent également répondre aux besoins des utilisateurs finaux soucieux de leur interaction quotidienne avec les appareils. Les utilisateurs finaux ne veulent pas de workflows laborieux ni de mesures de sécurité qui les ralentissent, et, si la plupart d'entre eux comprennent l'importance de la sécurité des données, leur tolérance a des limites.

À cet égard, la simplicité d'intégration de Jamf Unlock avec des workflows existants bénéficie aux utilisateurs finaux comme aux équipes informatiques et de sécurité de l'information. Les pirates ne sont pas près d'abandonner leurs tentatives, mais l'adoption d'un workflow sans mot de passe via Jamf Unlock et Jamf Connect est un moyen simple de fournir une couche de sécurité supplémentaire qui atténue les risques, tout en offrant une expérience de qualité pour l'utilisateur final.

L'implémentation d'un environnement sans mot de passe doit être un processus bien pensé pour toute organisation, mais c'est une amélioration qui fait progresser l'organisation. L'accent doit être mis sur la simplification de votre processus et la réduction des frais généraux, plutôt que sur l'intégration de matériel inutile et l'ajout de coûts supplémentaires. C'est exactement ce que Jamf Unlock fait, et c'est précisément pourquoi c'est la meilleure méthode pour sécuriser les Mac de votre organisation.

Contactez-nous, ou votre revendeur Apple, pour découvrir les solutions sans mot de passe de Jamf Connect.