Intentions de sécurité et
Persistance des mots de passe

Noir
& Blanc

Mai 2022

Commandée par

bitwarden

451 Research

S&P Global
Market Intelligence

À propos de ce papier

Un article en noir et blanc est une étude basée sur des données d'enquête de recherche primaire qui évalue la dynamique du marché d'un segment clé de la technologie d'entreprise à travers le prisme de l'expérience "sur le terrain" et des opinions de vrais praticiens - ce qu'ils font et pourquoi ils le font.

A propos de l'auteur

Justin Lam

Analyste de recherche sur la sécurité des

données Justin Lam est analyste de recherche dans le canal de la sécurité de l'information chez 451 Research, une filiale de S&P Global Market Intelligence, spécialisée dans la sécurité des données. Il a occupé divers postes au sein de fournisseurs de sécurité des données établis et émergents au cours des 15 dernières années, à la fois dans des fonctions techniques et commerciales. Justin est titulaire d'un BS en commerce de l'Université Carnegie Mellon et est basé dans la région de la baie de San Francisco.

Introduction

Avant l'informatique électronique, les humains authentifiaient les autres humains en fonction de ce qu'ils avaient ou de ce qu'ils savaient. N'importe qui aurait pu prendre n'importe quel nom, mais les signatures manuscrites, les sceaux des sceaux ou la connaissance de la lignée étaient utilisées pour vérifier son identité. Depuis l'avènement de l'informatique partagée, les mots de passe ont été utilisés pour distinguer les utilisateurs les uns des autres. Les mots de passe ont été conçus pour permettre aux ordinateurs et aux réseaux d'authentifier les utilisateurs sur la base d'un secret partagé que seul l'utilisateur humain connaissait et que l'ordinateur pouvait vérifier.

Les attaques automatisées par de mauvais acteurs pour deviner par force brute le mot de passe d'un utilisateur légitime ont opposé les capacités toujours croissantes d'un ordinateur à la capacité limitée d'une personne à se souvenir de mots de passe forts et uniques. La capacité défensive des utilisateurs à se souvenir de mots de passe forts et uniques n'a pas suivi les capacités offensives de craquage de mots de passe. Alors que les directives gouvernementales nationales telles que NIST SP 800-63B détaillent les meilleures pratiques de gestion des mots de passe, des écarts entre ces meilleures pratiques et le comportement réel des utilisateurs et des entreprises persistent.

La plupart des comptes d'entreprise sont fournis avec un nom d'utilisateur et sécurisés avec le mot de passe de l'utilisateur. Les employés de l'entreprise peuvent disposer d'un grand nombre de comptes, par exemple pour le CRM, la chaîne d'approvisionnement, les finances, la collaboration, les e-mails et la messagerie. Sans application de l'unicité ou de la force du mot de passe, les utilisateurs utilisent généralement par défaut des mots de passe plus faibles et même les réutilisent. La vulnérabilité des mots de passe perdus ou facilement compromis sur plusieurs comptes d'entreprise peut être extrêmement dommageable pour les entreprises.
De nombreuses entreprises et utilisateurs peuvent même connaître ces risques mais ne disposent pas des outils pour les atténuer.

Ce rapport présente les principales conclusions et conclusions d'une enquête menée par Bitwarden en collaboration avec 451 Research (qui fait partie de S&P Global Market Intelligence) pour comprendre les préférences et les tendances d'adoption en matière de gestion des mots de passe dans l'entreprise. Cette étude examine les cas d'utilisation, les habitudes de dépenses et le sentiment envers les gestionnaires de mots de passe, ainsi que les normes associées et leur adoption. Nous dévoilons et réconcilions les tensions entre le désir de sécurité et l'action, la priorité et les dépenses. L'analyse tente également de saisir les différences entre les utilisateurs, les secteurs verticaux et les tailles d'entreprise, dans la mesure du possible.

Nous définissons largement les gestionnaires de mots de passe comme des programmes spécialement conçus qui suggèrent, stockent et synchronisent en toute sécurité les noms d'utilisateur, mots de passe et autres authentificateurs. Cela peut inclure des programmes installés dans une variété d'emplacements mobiles, de bureau et de navigateur.

Principales conclusions

– En raison de l'augmentation du travail à domicile, les gestionnaires de mots de passe sont devenus l'une des meilleures technologies de sécurité.

- Plus de la moitié (57 %) de tous les répondants utilisent la gestion des mots de passe.
- 15 % supplémentaires ont déclaré qu'ils adopteraient la gestion des mots de passe.

– Près d'un tiers (29%) des répondants ont eu un incident de sécurité lié aux mots de passe.

- Parmi ceux-ci, 37 % ont eu un impact significatif ou modéré sur les opérations internes.

– Pour stimuler l'adoption, l'utilisation du gestionnaire de mots de passe doit combiner des cas d'utilisation personnels et professionnels.

- Un peu plus de la moitié (52 %) des répondants américains ont choisi eux-mêmes la gestion des mots de passe à des fins personnelles et identités de travail.
- En outre, 46 % des répondants américains ont déclaré que la gestion des mots de passe devrait être assurée par l'entreprise employés, tant au travail qu'à la maison.
- De même, 44 % des répondants américains utilisent et préfèrent un outil qui permet une utilisation à des fins personnelles et professionnelles mots de passe.

– Les coûts de sécurité matériels sont plus importants pour justifier les gestionnaires de mots de passe que les gains de productivité souples.

- La fraude au compte était la principale raison de la gestion des mots de passe, choisie par 51 % des répondants.
- Seuls 25 % ont déclaré que le « gain de temps » et 32 % ont déclaré que la « convivialité de l'utilisateur » étaient des raisons d'adopter des gestionnaires de mots de passe.

– Il existe un décalage entre le niveau de risque du personnel et l'adoption parmi les utilisateurs actuels du gestionnaire de mots de passe.

- Plus de la moitié (55 %) des répondants américains ont déclaré que les utilisateurs tiers sont les utilisateurs les plus risqués.
- Pourtant, seuls 41 % des répondants américains avaient déployé des gestionnaires de mots de passe pour des utilisateurs tiers.

– La gestion des mots de passe basée sur le système d'exploitation ou le navigateur se fait au détriment de l'auditabilité centrale.

- La gestion des mots de passe basée sur le navigateur et le système d'exploitation était la plus populaire, à 53 % et 39 %, respectivement.
- Pourtant, il existe des lacunes importantes dans la politique de mise en œuvre et l'audit : 45 % de tous les répondants auditent régulièrement les changements de mot de passe et ont une politique de mot de passe solide dans leurs systèmes de gestion des identités et des accès (IAM).

– Les mots de passe ne disparaissent pas.

- Une majorité (55 %) des personnes interrogées ont déclaré que l'omniprésence des mots de passe permet aux entreprises d'utiliser des mots de passe.
- Pendant ce temps, 56 % des répondants aux États-Unis ont déclaré que seulement 34 % à 66 % de leurs applications utilisent l'authentification unique (SSO). De nombreuses les applications n'utilisant pas SSO signifient plus de combinaisons de nom d'utilisateur et de mot de passe.

– Il existe encore une confusion sur ce qu'est l'authentification « sans mot de passe ».

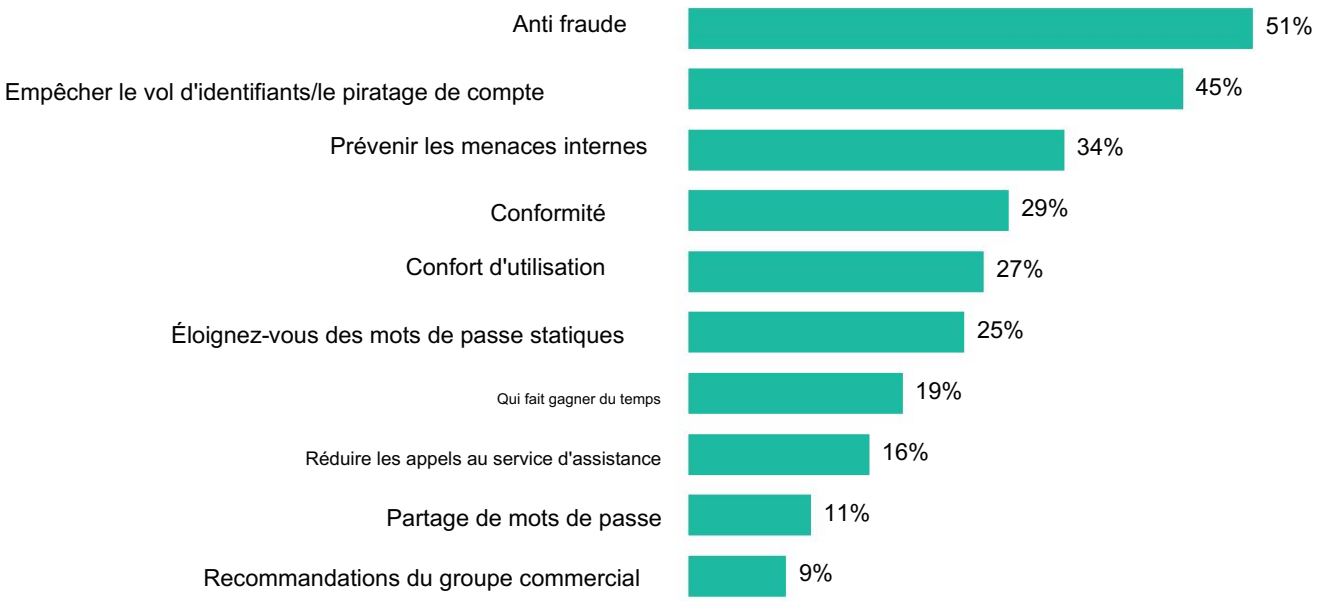
- Près des deux tiers (61 %) des personnes interrogées ont déclaré que les codes d'accès à usage unique (OTP, SMS, e-mail) sont une forme d'authentification sans mot de passe.

Budgets dépensés vs bénéfices perçus

Les dépenses globales de sécurité des entreprises continuent de croître. Selon le dernier rapport 451 Research Voice of the Enterprise (VoTE): Budgets & Outlook 2021, 86 % des entreprises prévoient d'augmenter leurs budgets de sécurité annuels, 93 % des entreprises interrogées ont déclaré qu'elles maintiennent ou augmentent leurs budgets de gestion des mots de passe, et 76 % des personnes interrogées ont déclaré avoir déployé ou prévoir de déployer la gestion des mots de passe en raison de problèmes de travail à domicile. Les professionnels de la gestion des identités et des accès ont déclaré que les gestionnaires de mots de passe sont la meilleure valeur pour l'investissement en sécurité ; curieusement, ces professionnels IAM ont classé la gestion des mots de passe devant les solutions de sécurité des e-mails (anti-hameçonnage) et de sensibilisation des utilisateurs.

Lors du choix de la gestion des mots de passe, l'impact des conséquences sur la sécurité motive la prise de décision plus que les incitations positives à l'utilisabilité ; les bâtons dépassent les carottes pour justifier le budget de gestion des mots de passe. Dans le vote préférentiel, la lutte contre la fraude, la prévention des attaques de prise de contrôle de compte et la prévention des menaces internes étaient les raisons les plus prioritaires, choisies par 51 %, 45 % et 34 % des répondants, respectivement. En comparaison, la commodité pour l'utilisateur, le gain de temps et la réduction des appels au service d'assistance figuraient parmi les raisons les moins prioritaires, choisies par seulement 27 %, 19 % et 16 %, respectivement.

Figure 1 : Principales raisons de l'adoption du gestionnaire de mots de passe



Q : Quelles sont les principales raisons d'adopter des gestionnaires de mots de passe ?

Base : Tous les répondants (n=400)

Source : enquête personnalisée 2022 sur la gestion des identités et des accès de 451 Research

Les entreprises ont été impactées négativement, 29 % de tous les répondants ayant subi un incident de sécurité résultant d'une mauvaise gestion des mots de passe. Les industries qui ont des dépenses de sécurité de l'information plus élevées et des capacités de sécurité plus élevées ont été plus touchées. Les entreprises technologiques, les services financiers et les sociétés de conseil affichaient des taux d'incidents respectifs de 37 %, 31 % et 38 %. Parmi tous les répondants qui ont subi un incident de sécurité, 73 % ont également eu d'autres répercussions sur les opérations internes et externes.

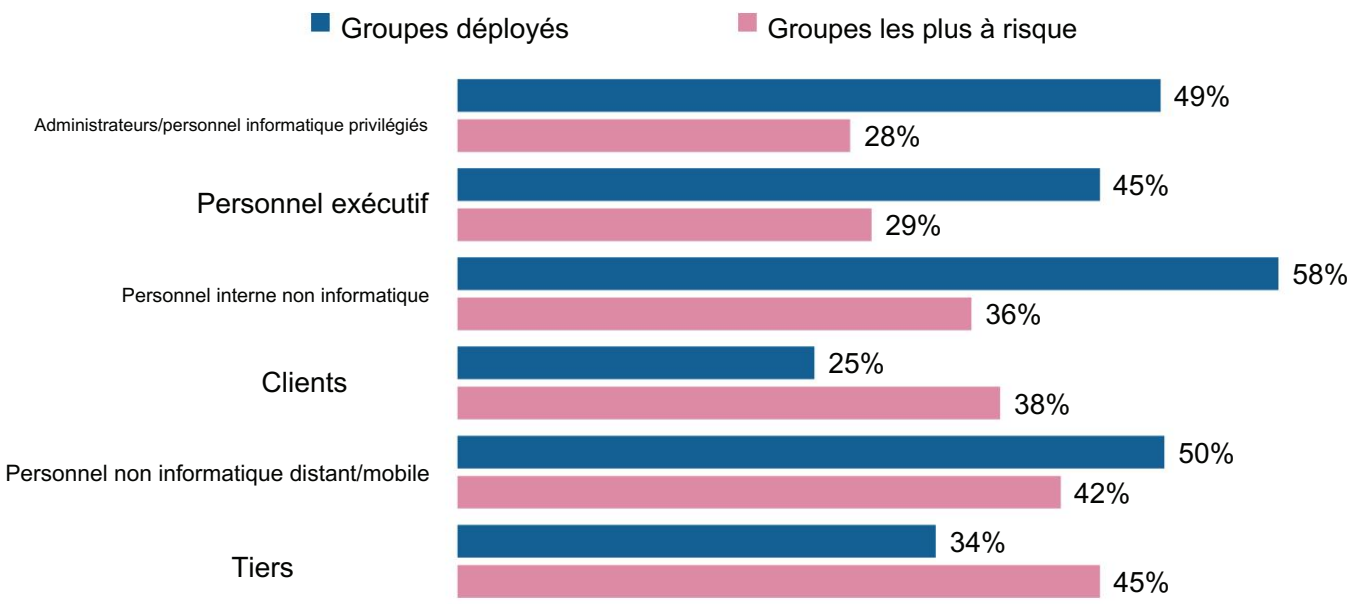
Il reste des obstacles à la réalisation de la valeur. Dans un autre vote de choix classé, les répondants ont respectivement sélectionné l'expérience utilisateur et la complexité de la gestion à 29 % et 36 % comme les principaux obstacles au déploiement réussi du gestionnaire de mots de passe. Ainsi, alors que les conséquences en matière de sécurité justifient des investissements dans des gestionnaires de mots de passe, la mise en œuvre est compliquée par des considérations d'expérience et de fonctionnement de l'utilisateur final. Dans les sections suivantes, l'étude examine si cela a un impact sur l'adoption par les entreprises et maintient les entreprises moins protégées.

Besoins perçus vs action

L'étude s'est concentrée sur les moyennes et grandes entreprises de plus de 1 000 employés ; 27 % des répondants travaillent pour des organisations de plus de 10 000 employés. De plus, notre étude s'est concentrée uniquement sur les employés et n'a pas intégré le personnel temporaire, sous-traitant ou affilié qui pourrait avoir accès aux mêmes ressources du réseau. En général, nous avons observé une tension entre les priorités perçues et les réponses réelles. Nos répondants occupaient eux-mêmes des postes au sein de l'informatique et de la sécurité, et lorsqu'on leur a demandé quels membres du personnel constituaient les utilisateurs les plus à risque, ils ont sélectionné des tiers (45 %) et des travailleurs distants/mobiles (42 %) lors du vote par classement. Curieusement, les répondants considèrent que les administrateurs (28 %) et le personnel de direction (29 %) sont les moins risqués, montrant peut-être des biais de confirmation parce qu'intuitivement, les administrateurs informatiques, la sécurité informatique et le personnel de direction ont une compétence unique et le pouvoir d'affecter tous les départements et activité des parties prenantes.

L'étude a demandé à quel personnel la gestion des mots de passe était déjà déployée ou la ferait déployer ensuite. Le personnel interne non informatique (employés généraux) était le choix le plus courant dans la sélection classée, à 58 %. Les répondants ont accordé une moindre priorité aux tiers (34 %) et au personnel à distance (50 %) – qu'ils avaient cités comme le personnel le plus « à risque », soulignant un écart entre les besoins perçus et l'action. Les administrateurs privilégiés et le personnel de direction ont été sélectionnés pour le déploiement du gestionnaire de mots de passe à des pourcentages modérés de 49 % et 45 %, respectivement.

Figure 2 : Groupes à risque – Groupes déployés pour la gestion des mots de passe



Q : Parmi les groupes d'utilisateurs suivants, lesquels considérez-vous comme présentant le risque le plus élevé ?

Q : Pour quels groupes d'utilisateurs avez-vous déployé des gestionnaires de mots de passe ?

Base : Tous les répondants (n=400)

Source : enquête personnalisée 2022 sur la gestion des identités et des accès de 451 Research

Si les entreprises veulent mieux gérer leurs risques, elles doivent appliquer les ressources telles que les gestionnaires de mots de passe proportionnellement au personnel le plus à risque. Agir sur les besoins perçus permettra aux entreprises de réduire ou d'atténuer les conséquences négatives sur la sécurité plus rapidement et mieux. Parce qu'il est important de donner la priorité à la sécurité du personnel à risque, il est également important que la sécurité par mot de passe pour ce personnel soit facile à adopter. L'acceptation réussie du gestionnaire de mots de passe par le personnel plus risqué reste essentielle pour combler les lacunes d'exposition perçues.

Productivité de l'utilisateur (ascendante) vs. Sécurité d'entreprise (descendante)

Notre étude a révélé une dichotomie claire entre les préoccupations de sécurité d'entreprise « descendantes » et les préoccupations d'utilisabilité « ascendantes ». Interrogés sur les politiques de mot de passe, 80 % ont répondu que les politiques de mot de passe constituaient une protection suffisante pour leur organisation. Aux États-Unis, 88 % des personnes interrogées ont déclaré que leurs politiques de mot de passe étaient suffisantes.
Alors que des normes telles que NIST SP 800-63B sont à la base de la politique de mot de passe, l'adhésion réelle de l'utilisateur est une tout autre affaire. Plus de la moitié (57 %) de tous les répondants ont identifié le comportement des utilisateurs comme le principal obstacle à la mise en œuvre de meilleures pratiques de gestion des mots de passe.

Les entreprises peuvent d'abord penser qu'elles disposent de capacités de gestion des mots de passe, peut-être via des navigateurs ou des systèmes d'exploitation. Dans la sélection des choix classés, les gestionnaires de mots de passe les plus populaires faisaient partie d'un navigateur, comme Safari ou Google Chrome, ou ils faisaient partie du système d'exploitation, via Windows Credential Manager ou MacOS Keychain. Un peu plus de la moitié (53 %) des personnes interrogées ont identifié des navigateurs, tandis que 39 % ont choisi la gestion des mots de passe basée sur le système d'exploitation. Pourtant, malgré l'omniprésence de navigateurs tels que Google Chrome et de systèmes d'exploitation courants tels que MacOS, iOS, Android et Windows, 66 % des personnes interrogées ont déclaré qu'il serait plus facile pour les employés d'adopter de meilleures pratiques de mot de passe s'ils disposaient des outils appropriés. Le stockage de mot de passe basé sur le système d'exploitation ou le navigateur n'est peut-être pas le plus facile à utiliser, en particulier dans divers environnements. Les utilisateurs peuvent avoir un mélange de navigateurs et de systèmes d'exploitation pour les appareils personnels, mobiles et professionnels. Les mots de passe stockés dans iCloud Keychain ne sont pas facilement accessibles à l'utilisateur Windows ou Android. La disponibilité incohérente des mots de passe sur les plates-formes crée une expérience utilisateur négative. Avec une combinaison croissante de travail à domicile et une combinaison accrue d'appareils et de services personnels et professionnels, l'expérience utilisateur pour la gestion des mots de passe doit être cohérente tout au long.

Alors que la croyance dans les politiques de mot de passe est élevée, la pratique consistant à effectuer des audits de mot de passe est plus faible. Environ deux répondants sur cinq (41 %) ont déclaré ne pas vérifier la force ou la réutilisation des mots de passe. Ainsi, alors que la sécurité d'entreprise favorise idéalement un comportement de mot de passe sain, la vérification de l'utilisation d'un mot de passe fort prend du retard. Fournir des outils qui stockent en toute sécurité les informations d'identification et qui sont auditables et accessibles sur toutes les plates-formes permettrait une expérience utilisateur cohérente et des pratiques de sécurité cohérentes. Le désir de sécurité d'entreprise de haut niveau ne doit pas être échangé contre une meilleure expérience de l'utilisateur final. Le désir théorique de haut niveau pour la sécurité d'entreprise doit tenir compte de la facilité d'adoption ascendante pour réussir. Répondre aux préoccupations des utilisateurs de bas en haut et donner la priorité au bon comportement des utilisateurs ne peut qu'améliorer les résultats de l'audit et de la sécurité de l'entreprise.

Des attitudes négatives persistent quant à l'expérience de l'utilisateur final. Lors de l'examen des avantages du gestionnaire de mots de passe, seulement 16 % des personnes interrogées ont déclaré "réduire les appels au service d'assistance". Pourtant, il y a un nombre important d'appels au service d'assistance, 56 % des entreprises déclarant que les réinitialisations de mot de passe/gestion des mots de passe représentent 20 % à 60 % de toutes les demandes d'assistance.

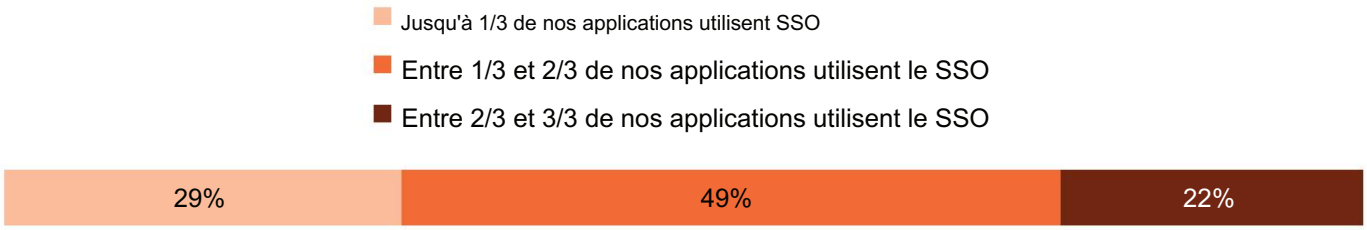
Heureusement, toutes les demandes d'amélioration de l'expérience utilisateur ne sont pas ignorées. Le travail à domicile devenant de plus en plus courant alors même que les restrictions liées à la pandémie s'atténuent, les répondants reconnaissent l'évolution des relations entre les employés et les employeurs en ce qui concerne la technologie. Lors du vote par classement, 54 % des répondants basés aux États-Unis ont cité le désir des employés d'utiliser des services personnels préférés tels que les e-mails et les vidéoconférences plutôt que les normes de l'entreprise, et 52 % des répondants américains ont déclaré que les utilisateurs préféraient choisir un gestionnaire de mots de passe pour le travail et le personnel. identités. Près de la moitié (47 %) de tous les répondants ont déclaré que l'entreprise devrait fournir des outils aux employés à la maison et au travail, et 59 % préféreraient un outil de gestion des mots de passe personnels et professionnels.

La persistance des mots de passe vs. Autres authentificateurs

Ce rapport a couvert l'évolution de l'expérience utilisateur et des objectifs de sécurité plus stricts. Les tendances sont interdépendantes et devraient continuer à pousser à une plus grande adoption de la gestion des mots de passe. En raison du vol ou de la compromission de mots de passe, les applications continuent d'adopter l'authentification multifacteur (MFA) telle que le mot de passe à usage unique (OTP), les codes envoyés par e-mail, les SMS, les certificats et les facteurs biométriques. Presque tous les répondants (96 %) ont indiqué qu'ils connaissaient une certaine forme de ces authentificateurs sans mot de passe. Pourtant, 55 % de tous les répondants ont déclaré que les mots de passe sont omniprésents.

Les entreprises ont également adopté des solutions d'authentification unique (SSO) pour améliorer à la fois l'expérience utilisateur et la sécurité. Ce n'est pas encore une panacée, étant donné que le nombre d'applications non compatibles SSO ajoutées augmente plus rapidement que jamais. Près de la moitié (49 %) des répondants ont déclaré que 34 % à 66 % de leurs applications et connexions étaient couvertes par leur solution SSO. À mesure que le travail à domicile et les applications personnelles, l'utilisation de l'identité, des appareils et du réseau augmentent, tous les services ne peuvent pas être couverts par l'authentification unique. Le processus d'authentification pour ces applications en dehors du contrôle SSO implique généralement un nom d'utilisateur et un mot de passe, le mot de passe étant le seul facteur d'authentification commun.

Figure 3 : Approche d'adoption de l'authentification unique



Q : Comment décririez-vous l'approche de votre organisation en matière de gestion des mots de passe/d'adoption de l'authentification unique ?
Base : Tous les répondants (n=400)
Source : enquête personnalisée 2022 sur la gestion des identités et des accès de 451 Research

La fourniture de gestionnaires de mots de passe à usage personnel et professionnel améliore non seulement la productivité des utilisateurs, mais les gestionnaires de mots de passe améliorent également les résultats en matière de sécurité. Comme cité dans le rapport du FBI sur la criminalité sur Internet en 2021, l'ingénierie sociale agressive et le phishing/smishing/vishing ciblant les identités personnelles, les appareils et les réseaux ont permis des incidents de compromission de messagerie professionnelle plus coûteux pour transférer des fonds ou effectuer d'autres fausses transactions financières. L'expérience utilisateur et la sécurité ne doivent pas être un compromis ; l'augmentation des applications, la diversité des utilisateurs et les tendances du travail à partir de n'importe où continuent d'offrir à la gestion des mots de passe une opportunité d'aider les utilisateurs à réussir et à rester en sécurité.

Regarder vers l'avenir

L'obsolescence du mot de passe est prédite depuis un certain temps. L'Alliance FIDO, un vaste groupe de normalisation, est la tentative la plus récente et la plus importante d'aller au-delà des mots de passe. Le travail de FIDO avec WebAuthn et l'authentification biométrique est de s'assurer que l'authentification est plus facile avec la biométrie qu'avec les mots de passe. Il reste encore beaucoup de travail à faire, y compris l'interopérabilité des informations d'identification FIDO multi-appareils. Le système Keychain d'Apple et son utilisation biométrique trouvée sur iPhone, Mac et iPad montrent à quoi pourrait ressembler l'interopérabilité des informations d'identification FIDO multi-appareils. Cela dit, iOS demande toujours par défaut un mot de passe pour activer TouchID ou FaceID.

Les mots de passe ont une inertie. Avec plus de 1,5 milliard d'utilisateurs actifs d'iPhone et plus de 800 millions d'utilisateurs actifs d'iCloud, la création d'un compte Apple ID sous-jacent nécessite toujours une combinaison de nom d'utilisateur et de mot de passe. Bien que les mots de passe et les codes d'accès puissent être moins utilisés avec la biométrie ou WebAuthn, les mots de passe continueront d'être un moyen courant d'authentification. Les cas marginaux, tels que le verrouillage de compte, nécessitent toujours des mots de passe. En tant que tels, les mots de passe valent toujours la peine d'être volés, piratés et abusés. Les défis de sécurité auxquels les entreprises sont confrontées en ce qui concerne l'utilisation des mots de passe existent depuis un certain temps et ils ne reculent pas. Les utilisateurs doivent toujours disposer d'une solution pour stocker ces mots de passe à travers les identités et les appareils dans un monde de travail de n'importe où.

Conclusion

Les entreprises doivent accorder une attention particulière à l'expérience utilisateur pour que la sécurité réussisse. Ils doivent également se rendre compte que les utilisateurs finaux sont de plus en plus avertis par à-coups. Selon le Voice of the Connected User Landscape: Connected Customer, Trust & Privacy – Insight Report, 86 % des répondants conviennent que le fait d'avoir un point de référence unique pour gérer leurs préférences en matière de sécurité et de confidentialité améliorerait leur expérience avec n'importe quel service en ligne. En d'autres termes, les utilisateurs qui font l'expérience d'une sécurité simple sont plus susceptibles de faire confiance à un service donné et de s'y engager. En simplifiant la sécurité via des solutions telles que les gestionnaires de mots de passe, les responsables de la sécurité peuvent équiper et permettre aux utilisateurs de réussir leurs tâches et d'atteindre les objectifs de sécurité globaux.

CONTACTS

Les Amériques
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Moyen-Orient et Afrique +44
20 7176 1234
market.intelligence@spglobal.com

Asie-Pacifique
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence