yubico

UN LIVRE BLANC DE YUBICO
OCTOBRE 2020

Passer au sans mot de passe

avec FIDO2 et WebAuthn

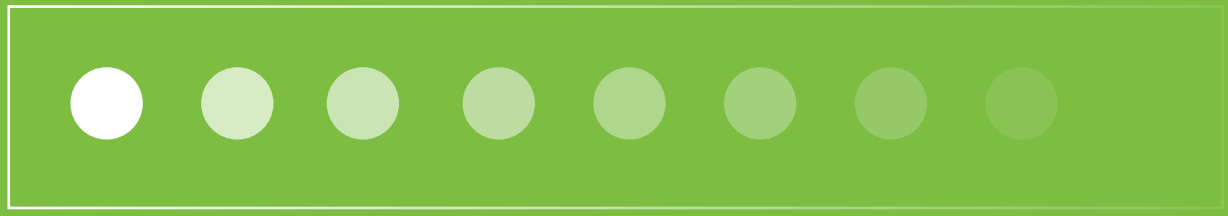


Table des matières

Résumé

Imaginez un monde où les utilisateurs n'ont plus besoin de définir, de réinitialiser, d'oublier et de réinitialiser de nouveau de nombreux mots de passe. Les mots de passe sont connus comme le maillon faible de la sécurité d'entreprise et constituent un obstacle aux parcours des clients et aux processus internes rationalisés. Le monde est sur le point de changer avec l'introduction de l'authentification sans mot de passe. Une enquête mondiale du Ponemon Institute menée auprès de 2 507 praticiens de la sécurité informatique et de 563 utilisateurs individuels a révélé que 49 % des professionnels de la sécurité informatique et 51 % des particuliers partagent leurs mots de passe de leurs comptes professionnels avec des collègues. Cela illustre les mauvaises pratiques qui exacerbent les problèmes de sécurité liés aux mots de passe[1].

Les nouvelles normes d'authentification FIDO2/WebAuthn offrent la possibilité aux organisations de résoudre les problèmes inhérents à la sécurité basée sur les mots de passe. FIDO2 est une norme ouverte, codéveloppée par Yubico, Microsoft et d'autres membres de l'Alliance FIDO, qui permet d'élargir les options d'authentification forte, y compris la possibilité d'offrir désormais aux utilisateurs une authentification forte sans mot de passe à facteur unique ou multifactorielle, en plus de prendre en charge le scénario existant d'authentification à deux facteurs.

L'authentification sans mot de passe offre la possibilité de transformer la sécurité de l'entreprise et les expériences des utilisateurs dans tous les secteurs, y compris les soins de santé, le secteur manufacturier et la vente au détail, ainsi que pour les employés de bureau, les partenaires et les fournisseurs. Il peut simplifier l'intégration des utilisateurs et, étant donné que la réinitialisation des mots de passe représente actuellement le coût le plus important de l'assistance informatique, la connexion sans mot de passe promet de réduire considérablement les charges de travail dans les centres d'appels informatiques où les agents passent aujourd'hui un temps considérable à définir et à réinitialiser les mots de passe des utilisateurs.

Comment les parcours des clients et des employés pourraient-ils être rationalisés grâce à une connexion sans mot de passe ? Quels nouveaux produits et services deviennent possibles lorsque les mots de passe ne sont plus nécessaires ? Ce sont les questions que les dirigeants d'entreprises et de services informatiques avant-gardistes devraient se poser dès maintenant.

Le temps et le coût des mots de passe

Les entreprises cherchent aujourd'hui des moyens de tirer parti de la technologie du cloud et du mobile afin de fournir des produits et services améliorés plus rapidement et plus efficacement. Cependant, les entreprises qui poursuivent des plans ambitieux de rationalisation du parcours des clients et employés se trouvent rapidement confrontées à des défis de sécurité.

Les technologies et les contrôles de sécurité sont mis en place pour protéger l'entreprise, cependant ces mêmes contrôles de sécurité peuvent frustrer les utilisateurs. Les mots de passe figurent en haut de la liste des contrôles de sécurité pénibles et irritants.

Les mots de passe sont une réalité depuis les années 1950, tant pour les utilisateurs professionnels que pour les consommateurs. Presque toutes les expériences numériques en ont besoin, des réseaux sociaux comme Facebook, aux banques et détaillants comme H&M et Zara, en passant par les applications commerciales comme Salesforce et QuickBooks Online.

Le consommateur américain moyen essaie de se rappeler de plus de 70 mots de passe différents, qu'il utilise sur tous ses sites Web et services[2], tandis que les utilisateurs professionnels seraient responsables de la mémorisation et l'utilisation d'un nombre encore plus important de mots de passe, jusqu'à 191.[3] Avec la génération du millénaire qui compose une part croissante de la population active, les résultats d'une étude IBM montrent qu'ils font preuve de moins de patience avec la mémorisation de tous ces secrets. Ils sont plus susceptibles de réutiliser les mots de passe, n'en mémorisant pas plus de huit, compromettant la sécurité au nom de la commodité.[4]

La fatigue des mots de passe entraîne des violations de données

Les utilisateurs sont fatigués de créer de nouveaux mots de passe pour différents services et de devoir changer de mot de passe tous les quelques mois en fonction des exigences des politiques de sécurité. Pour réduire la mémorisation, de nombreux utilisateurs finissent par se fier à des mots de passe simplistes qui sont malheureusement faciles à craquer ou par les réutiliser sur plusieurs sites, où la violation d'un service peut ouvrir la porte à plusieurs autres.

Selon le rapport d'enquête sur les atteintes à la protection des données de Verizon (DBIR) de 2019, 80 % des piratages sont encore liés à des identifiants compromis et faibles.[5] Il est incroyable de constater qu'après des années de piratage de données très médiatisés, la plupart impliquent un mot de passe faible. L'analyse des failles de sécurité de la NCSC 2019 UK Cyber Survey a révélé que 23,2 millions de comptes de victimes dans le monde entier utilisaient 123456 comme mot de passe.[6]

80 % des brèches liées à du piratage impliquent encore des identifiants faibles et compromis.[5]

Violations de données Verizon
Enquête sur les violations

À mesure que les entreprises ajoutent de plus en plus d'applications commerciales à leur portefeuille, le coût des mots de passe ne fait qu'augmenter. En fait, les entreprises consacrent 30 à 60 % de leurs appels au service d'assistance à la réinitialisation des mots de passe.

Les mots de passe oubliés entraînent des coûts d'assistance élevés

Lorsque les utilisateurs oublient leurs mots de passe, ils finissent souvent par appeler les services ou les centres d'assistance, ce qui leur fait perdre un temps précieux. Les demandes de réinitialisation de mot de passe représentent jusqu'à 6 % des activités des centres d'appels, ce qui coûte aux grandes entreprises entre 5 et 20 millions de dollars par an.

L'équipe informatique de Microsoft est passée à l'authentification sans mot de passe et aujourd'hui 90 % des employés de Microsoft se connectent sans entrer de mot de passe. En conséquence, les coûts matériels et immatériels liés à la prise en charge des mots de passe ont diminué de 87 %. À mesure que les entreprises continuent d'ajouter de nouvelles applications commerciales à leur portefeuille, le coût des mots de passe ne fait qu'augmenter. En fait, les entreprises consacrent 30 à 60 % de leurs appels au service d'assistance à la réinitialisation des mots de passe.[7]

Les attaques de phishing ciblent le vol d'identifiants

Le phishing continue d'être un énorme problème de sécurité au fur et à mesure que les techniques d'attaques continuent à évoluer. De faux messages électroniques incitant les utilisateurs à saisir à nouveau leurs informations d'identification peuvent être utilisés pour récolter les informations d'identification et les utiliser pour les piratages de comptes. Environ 30 % des e-mails de phishing sont ouverts par leurs destinataires et plus de 7 % des destinataires d'e-mails ont été persuadés d'ouvrir une pièce jointe ou de cliquer sur un lien, qui est souvent un lien de connexion. La plupart des attaques de phishing conduisent ensuite à l'installation de logiciels malveillants qui aident à perpétrer une brèche.[8] Même si les utilisateurs définissent des mots de passe complexes, les pirates peuvent y accéder par le biais du phishing et pénétrer dans les comptes des utilisateurs.

Listes d'identifiants volés disponibles à la vente

Lorsque des pirates informatiques s'introduisent dans une organisation et volent des identifiants, ils accèdent non seulement aux comptes de cette organisation, mais aussi aux comptes d'autres organisations où les consommateurs ont utilisé la même paire nom d'utilisateur-mot de passe. Par exemple, lorsque les pirates ont volé 1 milliard d'identifiants de connexion de Yahoo! en 2016, ils ont obtenu l'accès à tous les autres comptes accessibles avec les mêmes paires adresse e-mail-mot de passe. Des milliards d'identifiants volés sont disponibles à la vente sur le Dark Web et les cybercriminels lancent maintenant des tentatives de connexion automatisées avec ce trésor de mots de passe volés. Aujourd'hui, neuf tentatives de connexion sur dix sur des sites populaires de vente au détail et de banque sont en fait des attaques de robots.[9]

Tant que l'informatique de l'entreprise doit s'appuyer sur des mots de passe pour l'authentification, des besoins d'assistance coûteux, une sécurité faible et des expériences clients frustrantes sont inévitables. Les mots de passe oubliés et volés dégradent l'expérience des clients, réduisent la fidélité à la marque et contribuent à la perte de revenus.

Résolution du problème de mot de passe avec FIDO2

Imaginez que vous puissiez offrir des services rapides, pratiques et sécurisés de toutes sortes aux utilisateurs, qu'ils soient clients ou employés, sans avoir besoin de mots de passe et sans avoir à supporter les coûts opérationnels liés à la gestion des mots de passe. Imaginez que les clients, les partenaires et les employés sur leurs ordinateurs de bureau et leurs périphériques mobiles puissent accéder instantanément au contenu et aux services qu'ils souhaitent sans avoir à faire apparaître des mots de passe en mémoire ou à appeler le service d'assistance pour obtenir de l'aide. Imaginez de nouveaux services qui pourraient être activés si l'authentification était instantanée et facile. Imaginez que les services informatiques se libèrent de la corvée et des dépenses quotidiennes liées à la gestion et à la réinitialisation des mots de passe.

La norme d'authentification FIDO2 offre la possibilité d'une authentification sans mot de passe.

Les avantages de l'authentification sans mot de passe

Convivialité améliorée

L'authentification sans mot de passe libère les utilisateurs de l'obligation de se souvenir et de saisir des mots de passe.

Sécurité améliorée

L'authentification sans mot de passe élimine les risques de sécurité associés aux mots de passe volés et aux attaques par force brute contre les écrans de connexion.

Efficacité améliorée

L'authentification sans mot de passe élimine la nécessité pour les services informatiques de gérer les mots de passe.

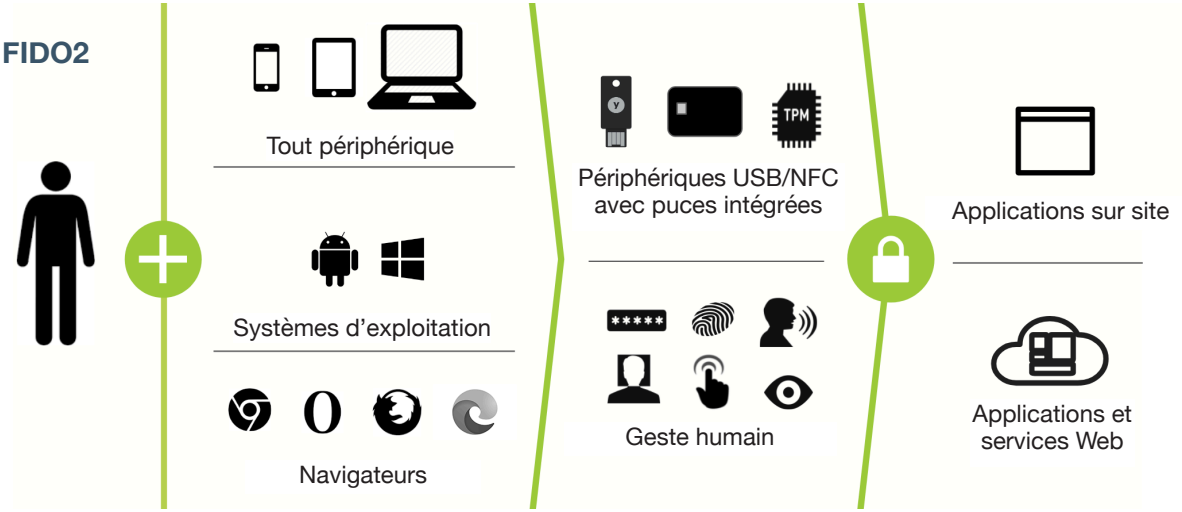
Ces avantages de l'authentification sans mot de passe peuvent désormais être obtenus grâce aux normes d'authentification ouvertes FIDO2/WebAuthn.

Présentation de l’authentification sans mot de passe

La norme d’authentification FIDO2 cosignée par Yubico, Microsoft et les membres de l’Alliance FIDO, en collaboration avec le World Wide Web Consortium (W3C), prend en charge de multiples scénarios et expériences d’utilisation.

FIDO2 comprend deux composants standardisés, une API Web (WebAuthn) et un protocole CTAP (Client to Authenticator Protocol, Protocole client à authentificateur). Les deux travaillent ensemble et sont nécessaires pour obtenir une expérience de connexion sans mot de passe. WebAuthn définit une API Web standard qui peut être intégrée dans les navigateurs et l’infrastructure de la plateforme Web pour donner aux utilisateurs de nouvelles méthodes d’authentification sécurisée sur le Web. CTAP permet à un authentificateur externe, comme une clé de sécurité, de communiquer localement des informations d’authentification fortes par USB, NFC ou Bluetooth au PC ou au téléphone portable de l’utilisateur.

Écosystème FIDO2



FIDO2 s’appuie sur une paire asymétrique (public/privé) de clés cryptographiques pour authentifier les utilisateurs. La clé publique est stockée sur tout service ou périphérique informatique prenant en charge l’authentification FIDO2, tandis que la clé privée est conservée par l’utilisateur et est protégée par une clé de sécurité physique, telle que la série de clés YubiKey 5 et la Security Key par Yubico. L’authentification elle-même est rapide et facile : il suffit d’insérer ou de toucher la clé de sécurité pour que le défi d’authentification soit terminé, et la connexion est immédiate.

Avec FIDO2, la clé de sécurité peut être utilisée seule ou en conjonction avec un code PIN ou un geste pour fournir une authentification forte sans mot de passe. En outre, le mode d'authentification à deux facteurs avec un mot de passe continue d’être pris en charge.

Compatibilité du World Wide Web Consortium (W3C) avec FIDO2

La spécification de l'API d'authentification Web (WebAuthn) offre aux utilisateurs de navigateurs de nouvelles méthodes d'authentification sécurisée sur le Web basées sur la spécification FIDO2. Les navigateurs Microsoft Edge, Google Chrome et Mozilla prennent tous en charge la spécification de l'API WebAuthn.

Les choix d'authentification FIDO2/WebAuthn

Facteur unique (sans mot de passe)
Utilisation de la clé de sécurité en tant que premier facteur d'authentification forte, ne nécessitant que la possession du périphérique et permettant une expérience tap-and-go sans mot de passe

Deux facteurs (Mot de passe + Authentificateur)
Utilisation de la clé de sécurité comme second facteur dans une solution d'authentification à deux facteurs

Authentification multi-facteurs (sans mot de passe + code PIN ou biométrique)
Utilisation de la clé de sécurité pour l'authentification multi-facteurs nécessitant la possession du périphérique ET d'un code PIN ou biométrique, afin de répondre à des exigences élevées en matière de protection

FIDO2 est pris en charge sur la dernière version des appareils Windows 10, y compris les systèmes de bureau et mobiles Windows. Cela rend FIDO2 disponible sur plus de 700 millions d'appareils dans le monde et sur des milliards de comptes Azure AD.

Avantages de passer au sans mot de passe

Ergonomie améliorée

La connexion sans mot de passe FIDO2 rend l'authentification rapide et facile, en éliminant le besoin de mots de passe.

La connexion sans mot de passe FIDO2 rend l'authentification rapide et facile en éliminant le besoin de mots de passe. Avec FIDO2, un seul authentificateur matériel, tel qu'une clé YubiKey, peut être utilisé pour authentifier tous les services avec lesquels un utilisateur interagit, y compris les services et applications professionnels, les réseaux sociaux, et d'autres applications grand public à la maison sans aucun secret partagé.

En même temps, FIDO2 peut être utilisée pour prendre en charge plusieurs identités pour un utilisateur unique. La même clé YubiKey peut être utilisée pour accéder à des applications, des sites Web, des services, des serveurs et des périphériques d'entreprises et de consommateurs, allant des bâtiments aux véhicules conçus pour prendre en charge FIDO2.

Grâce à l'authentification sans mot de passe, les personnes voyageant dans des avions ou des métros sans accès Wi-Fi ou cellulaire peuvent toujours s'authentifier sur leur ordinateur portable et travailler de manière productive et sécurisée, même si leur manque d'accès au réseau les empêche de recevoir des informations d'identification SMS ou OTP pour l'authentification des utilisateurs.

FIDO2 élimine la nécessité d'un accès au réseau (cellulaire ou Internet) pour recevoir les seconds facteurs. En plus de renforcer la sécurité informatique, FIDO2 permet aux utilisateurs d'accéder plus facilement aux périphériques dont ils ont besoin pour travailler, en permanence et partout.

FIDO2 est pris en charge sur la dernière version des appareils Windows 10, y compris les systèmes de bureau et mobiles Windows. Windows 10 compte plus d'un milliard d'utilisateurs dans le monde, ce qui rend environ 700 millions d'appareils compatibles avec FIDO2.[10]

Parce que FIDO2 a été développée comme une norme industrielle ouverte et est largement défendue par Microsoft et le World Wide Web Consortium (W3C) avec le soutien de Google et Mozilla, l'adoption ne dépend pas d'une seule entité. FIDO2 permet aux entreprises d'éviter d'avoir à investir dans le développement et la maintenance de modèles de sécurité personnalisés pour résoudre les problèmes de mots de passe. Désormais, les entreprises de tous les secteurs d'activité peuvent profiter d'une norme d'authentification industrielle ouverte, approuvée par les leaders du secteur.

Sécurité améliorée

FIDO2 améliore considérablement la sécurité de l'authentification des utilisateurs et de la gestion des accès.

FIDO2 améliore considérablement la sécurité de l'authentification des utilisateurs et de la gestion des accès.

Avec la connexion sans mot de passe, les utilisateurs ne peuvent pas être amenés à divulguer des mots de passe de manière inattendue, puisque les mots de passe ne sont plus nécessaires. Les utilisateurs s'authentifient avec un authentificateur matériel tel qu'une clé YubiKey, qui à un niveau élevé fonctionne comme suit :

- La clé YubiKey crée et gère les identifiants FIDO2 (une paire de clés publiques/privées), y compris la liaison des identifiants au service spécifique, connue sous le nom d'origine. La liaison d'origine empêche les attaques « man in the middle ».
- Lorsqu'on présente à un service comme Azure AD un défi d'authentification, la clé privée est utilisée pour signer la réponse qui est envoyée sur le réseau et vérifiée par le service en ligne au moyen de la clé publique.

Les informations d'identification FIDO2, qui sont stockées sur une puce sécurisée dans la clé YubiKey et qui ne quittent jamais le périphérique, sont conçues pour empêcher les pirates informatiques d'usurper l'identité des utilisateurs qui se connectent aux sites.

FIDO2 réduit les risques pour les applications, les sites Web, les services, les serveurs et les périphériques en supprimant le stockage et la gestion centralisés des informations d'identification sensibles. Les comptes FIDO2 n'ont pas besoin de mot de passe ; il n'y a donc plus de trésor de mots de passe à voler. Les sites Web et autres services ne stockent que les clés publiques que les utilisateurs ont enregistrées, ainsi le secret (clé privée) est maintenu en toute sécurité sur l'authentificateur matériel, et n'est jamais envoyé sur le réseau comme un mot de passe traditionnel. Ces clés publiques peuvent valider les signatures générées par les clés privées, mais elles sont inutiles toutes seules pour initier l'accès à d'autres ressources. Seul un utilisateur final possédant la clé privée FIDO2 peut s'authentifier avec succès auprès d'un service. La sécurité s'améliore, tout en rendant l'accès à la connexion plus rapide, plus facile et plus fiable pour les utilisateurs finaux.

Les privilèges d'authentification peuvent être accordés conformément aux politiques de sécurité propres à l'organisation ou exigés par les règlements de l'industrie, comme le GLBA et le HIPAA, ou les règlements gouvernementaux, comme la norme NIST SP800-63. En se conformant à la norme NIST SP800-63, FIDO2 assure la conformité avec un large éventail d'autres réglementations qui s'appuient sur les normes NIST. Les administrateurs informatiques et les responsables de la conformité peuvent être sûrs que les utilisateurs ne contournent pas les contrôles d'authentification en partageant leurs mots de passe sur des post-its ou par e-mail. Chaque utilisateur reçoit une clé unique qui l'authentifie auprès des services et applications enregistrés.

Respect des normes d'authentification NIST

FIDO2 peut être soit un token chiffré à facteur unique ou un token chiffré multi-facteurs. Selon la publication spéciale 800-63 du NIST, le token chiffré multi-facteurs est classé comme étant de niveau d'assurance d'authentification 3, qui est le plus haut niveau d'assurance déclaré par cette norme. L'utilisation de FIDO2 avec un code PIN répond donc aux exigences d'authentification les plus élevées sur les marchés réglementés où la conformité avec la norme NIST SP800-63 est obligatoire.[11]

« FIDO2 ne nécessite pas un environnement PKI complexe pour gérer les certificats »

Efficacité améliorée

FIDO2 permet aux départements informatiques, y compris les centres de service et les centres d'appels, de ne plus avoir à créer, stocker, changer et réinitialiser les mots de passe.

La connexion sans mot de passe offre la possibilité d'intégrer sans problème les employés et les sous-traitants, éliminant ainsi les coûts d'assistance liés à l'émission et à la gestion des mots de passe. Au lieu de fournir des mots de passe temporaires pour les nouveaux employés et sous-traitants qui doivent être changés immédiatement et ensuite changés à nouveau selon un calendrier prescrit, avec l'authentification FIDO2, chaque utilisateur reçoit simplement une clé de sécurité FIDO2 et l'utilisateur spécifie de façon optionnelle un code PIN lors de la fourniture initiale. Les privilèges d'authentification FIDO2 peuvent être facilement révoqués lorsqu'un employé ou un sous-traitant termine son service pour l'entreprise.

En utilisant la clé de sécurité FIDO2, les utilisateurs peuvent s'authentifier auprès d'un service central comme Azure AD, établissant leurs identités afin de pouvoir enregistrer de nouveaux périphériques, tels que les smartphones. Dans les organisations où les périphériques informatiques sont partagés, chaque utilisateur peut s'authentifier rapidement et facilement sans avoir à se souvenir et à saisir des mots de passe. En insérant ou en touchant simplement une clé YubiKey compatible NFC, les utilisateurs peuvent déverrouiller leurs périphériques et accéder à leurs comptes.

De plus, FIDO2 ne nécessite pas un environnement PKI complexe pour gérer les certificats. Les services informatiques peuvent réorienter leur temps et leurs efforts vers des tâches plus stratégiques et plus productives.

Répondre aux exigences d'une entreprise en matière d'authentification des utilisateur

FIDO2 répond à toutes ces exigences critiques pour l'authentification des utilisateurs :

- **Fournit des informations d'identification qui ne peuvent pas être piratées ou usurpées**
- **Fournit une méthode d'authentification qui empêche le phishing**
- **Offre une meilleure expérience à l'utilisateur final que les mots de passe**
- **Fournit une authentification et une autorisation liées à la machine. L'authentification ne peut pas être transférée entre les machines**
- **Prend en charge différents niveaux d'authentification**
- **Prend en charge plusieurs informations d'identification**
- **N'exige qu'un seul geste de l'utilisateur, comme une touche ou un glissement de doigt, pour accorder l'accès**

Une connexion facile augmente l'utilisation des services numériques de 10 à 20 %

Source : Enquête McKinsey ClickFox[13]

Aussi pratique qu'une carte bancaire

Pour apprécier la commodité d'une connexion sans mot de passe avec une clé YubiKey, considérez la commodité de votre carte bancaire. Vous avez probablement votre carte bancaire avec vous partout. Vous la protégez, vous ne le laissez pas traîner en public. Pour la déverrouiller à un guichet automatique bancaire (GAB), vous saisissez un code PIN court. Le code PIN est très rarement changé, voire pas du tout, il n'y a pas de mot de passe à retenir, ni de nom d'utilisateur, et pourtant votre accès au GAB est très sécurisé.

Une clé YubiKey sans mot de passe est similaire. Vous l'emportez partout. Pour déverrouiller un périphérique — qu'il s'agisse d'un ordinateur de bureau, d'un smartphone, d'un système de contrôle de fabrication, d'un portail de santé ou d'un autre périphérique — il vous suffit de connecter la clé YubiKey sur un port USB ou de placer la clé près d'un capteur NFC. Ensuite, lorsque vous y êtes invité, vous touchez la clé et saisissez éventuellement un code PIN ou utilisez un contrôle biométrique, selon l'application ou le service.

Comme le code PIN de votre carte bancaire, le code PIN FIDO2 garantit votre accès au mécanisme de la clé de sécurité. Le code PIN déverrouille votre clé de sécurité FIDO2 et lui permet de lancer un échange de clé avec tout ce vers quoi elle s'authentifie : le périphérique local, un service d'annuaire distant, un site Web, un réseau social ou un autre service informatique.

En option, les services peuvent être configurés pour authentifier les utilisateurs sans exiger de code PIN ou de gestes. Par exemple, dans le but de fournir le service le plus rapide possible aux clients, un commercial de vente au détail peut être autorisé à s'authentifier simplement en plaçant sa clé sur un capteur NFC, ce qui déverrouille instantanément un système informatique. Si le système informatique est configuré avec un capteur de pression qui détecte la présence d'un utilisateur, le système peut automatiquement déconnecter l'utilisateur du système lorsque le commercial authentifié s'éloigne.[12] Comme FIDO2 modifie radicalement le processus d'authentification des utilisateurs, les entreprises peuvent raisonnablement se permettre ces mesures d'authentification supplémentaires, car les expériences des utilisateurs de FIDO2 sont si simples et rapides, ce qui améliore la productivité tout en réduisant les coûts d'assistance.

Dans tous ces scénarios, la connexion sans mot de passe FIDO2 offre une expérience plus rapide et plus sûre que les noms d'utilisateur et les mots de passe. La connexion sans mot de passe transforme l'expérience de l'utilisateur qui se connecte à des applications, des sites Web, des services, des serveurs et des périphériques, en une fraction de seconde comme c'est le cas habituellement pour l'accès à un GAB.

La connexion sans mot de passe FIDO2 nécessite l'utilisation d'un authentificateur certifié FIDO2, comme la série YubiKey 5.

FIDO2, WebAuthn et FIDO U2F

Comment FIDO2 et WebAuthn fonctionnent-ils avec FIDO U2F ?

U2F est une norme d'authentification ouverte qui permet aux authentificateurs matériels, aux téléphones mobiles et autres périphériques d'accéder en toute sécurité à un nombre illimité de services Web — instantanément et sans pilote ni logiciel client. La norme U2F a été cocréée par Google et Yubico, avec la contribution de NXP, et est aujourd'hui hébergée par le consortium industriel d'authentification ouverte, l'Alliance FIDO.

U2F est une solution d'authentification forte, mais c'est aussi une solution à deux facteurs, s'appuyant sur les noms d'utilisateurs et les mots de passe comme premier facteur. En fait, le 2F dans son nom fait référence au 2e facteur.

FIDO2 est la deuxième génération d'U2F. FIDO2 s'appuie sur U2F en ajoutant les éléments nécessaires pour qu'un utilisateur puisse être identifié et authentifié sans avoir besoin d'un mot de passe. L'authentification FIDO2 prend en charge l'authentification forte à un facteur, à deux facteurs et multi-facteurs.

Le composant WebAuthn de FIDO2 est rétrocompatible avec les authentificateurs FIDO U2F. Cela signifie que toutes les clés de sécurité FIDO U2F, incluant les clés YubiKey déjà certifiées continueront à fonctionner comme une expérience de connexion d'authentification de second facteur avec les navigateurs Web et les services en ligne supportant WebAuthn.

Nouveaux cas d'utilisation avec connexions sans mot de passe

Employés

Lors de l'intégration de nouveaux employés, les entreprises n'ont plus besoin d'émettre des mots de passe temporaires ou des mots de passe de quelque nature que ce soit. Au lieu de cela, ils peuvent simplement fournir un authentificateur matériel, comme la clé YubiKey. En utilisant la clé YubiKey, un utilisateur peut s'authentifier à Azure AD ou à d'autres services avec ou sans un court code PIN, selon l'application. La clé YubiKey peut également être utilisée pour enregistrer des périphériques supplémentaires, tels que des smartphones ou des ordinateurs portables, qui serviront également d'authentificateurs.

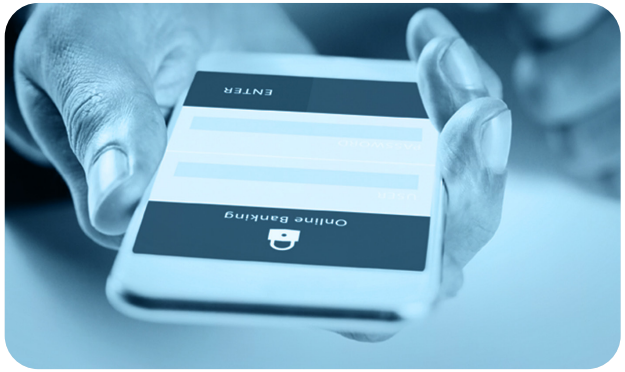
Le processus d'authentification peut devenir remarquablement rapide et facile. Par exemple, au lieu de s'asseoir et de saisir un nom d'utilisateur et un mot de passe, un employé de bureau peut simplement s'asseoir, toucher la clé YubiKey et commencer la journée de travail.

Vente au détail

Les vendeurs, les responsables de rayon, les chefs d'équipe, les caissiers et les autres employés de la vente au détail ont besoin d'un accès rapide et facile aux systèmes informatiques. Les connexions sans mot de passe rationalisent l'intégration et l'accès tout en fournissant une authentification rigoureuse comme garde-fou contre la fraude.

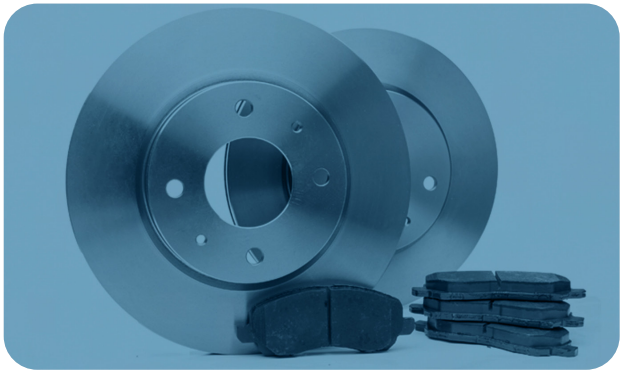
Les détaillants embauchent souvent du personnel saisonnier. Par exemple, au moins un détaillant nord-américain bien connu embauche généralement 30 000 travailleurs temporaires pour la période des fêtes. Traditionnellement, tous ces travailleurs auraient eu besoin de noms d'utilisateur et de mots de passe. Avec FIDO2, il est possible de leur fournir simplement des clés de sécurité. Les services autorisés peuvent être désactivés de façon centralisée par un service d'annuaire comme Azure AD lorsque l'activité saisonnière prend fin.

FIDO2 évite au service informatique de devoir créer, réinitialiser et annuler des mots de passe. Si les employés sont réembauchés, leurs clés de sécurité peuvent simplement être réactivées et réaffectées pour l'accès aux services en magasin.



Finances

La mise à disposition d'une authentification sans mot de passe rapide et sans tracas améliore l'expérience de la marque, rationalise les interactions entre le commerce électronique et l'assistance client et permet même la création de nouveaux produits et services. Une banque, une coopérative de crédit ou une institution financière qui offre des clés de sécurité et une authentification sans mot de passe à ses clients réduit le risque de piratage de comptes tout en simplifiant la vie des titulaires de compte.



Secteur manufacturier

Comme les détaillants, les fabricants ont des ouvriers en postes multiples. FIDO2 simplifie la gestion des accès pour cette main-d'œuvre en constante évolution. Parce que les employés n'ont pas à saisir de mots de passe, mais peuvent toujours s'authentifier de manière unique, FIDO2 rationalise l'accès aux systèmes informatiques tout en prenant en charge les politiques internes de sécurité et de gestion des identités. En même temps, elle élimine le risque que les politiques de gestion des mots de passe (comme le cycle périodique des mots de passe) n'introduisent des retards ou d'autres problèmes dans les opérations.

Le ministère de la sécurité intérieure des États-Unis (U.S. Department of Homeland Security) a averti que le secteur manufacturier demeure une cible de choix pour les attaques de phishing, en partie parce que les pirates informatiques s'intéressent au vol de la propriété intellectuelle.[14] En remplaçant les mots de passe sensibles au phishing par les clés de sécurité FIDO2, les fabricants peuvent aider à fermer la porte à ce type d'attaque, en fournissant une authentification forte qui se défend contre le phishing.

Soins de santé

Les organisations de soins de santé (HCO) sont vulnérables aux atteintes à la protection des données de divers types. Les renseignements sur la santé du patient, y compris les antécédents du patient et les renseignements sur le payeur, ont dix fois plus de valeur sur le marché noir que les données sur les cartes de crédit.[15] Pourquoi ? Parce que la fraude médicale, y compris le dépôt de fausses réclamations d'assurance, est lucrative.

Les HCO sont également susceptibles de faire l'objet d'attaques par ransomware, dont beaucoup sont lancées par le biais du phishing. En remplaçant les mots de passe par des clés de sécurité, les HCO et leurs associés peuvent réduire considérablement leur vulnérabilité à ces types d'attaques.

FIDO2 peut également aider les HCO à garantir que les renseignements médicaux personnels (PHI ou RPS) ne sont accessibles qu'aux utilisateurs autorisés, conformément aux règlements de l'HIPAA (Health Insurance Portability and Accountability Act of 1996). Les résultats d'une enquête publiée dans Healthcare Informatics Research révèlent que 73 % des personnes interrogées ont déclaré avoir utilisé les identifiants d'un collègue pour accéder à des renseignements médicaux personnels.[16] La simplification des processus de connexion encourage les médecins à n'utiliser que leurs propres informations d'identification pour accéder aux renseignements médicaux personnels et à d'autres données et services protégés, et à cesser de partager leurs informations d'identification. Au minimum, elle les limite au partage de l'accès uniquement avec d'autres personnes physiquement présentes. En revanche, les mots de passe partagés permettent l'accès à partir de n'importe quel endroit.

FIDO2 offre un autre avantage important pour l'industrie de la santé : une authentification rapide et facile. Les médecins et les infirmières et infirmiers doivent se connecter des douzaines de fois par jour pour se déplacer de patient en patient, de chambre en chambre et de périphérique en périphérique. L'accès peut désormais être immédiat et plus sûr grâce aux connexions sans mot de passe. Les soignants peuvent se concentrer sur les soins à donner au lieu de s'encombrer de procédures de connexion fastidieuses.

Réseaux de vendeurs et fournisseurs

Le nombre de violations de données liées à des fournisseurs tiers a augmenté de 22 % depuis 2015.[17]

Le renforcement de l'authentification du portail partenaire avec les clés de sécurité FIDO2 rationalise l'accès des partenaires tout en éliminant la possibilité que des mots de passe volés soient utilisés pour infiltrer une entreprise par le biais de son portail partenaire.

De plus, FIDO2 n'exige pas qu'une entreprise gère toutes les identités de ses fournisseurs. Au lieu de cela, une entreprise peut simplement adopter une politique « sans mot de passe » et exiger des fournisseurs qu'ils s'authentifient à l'aide d'une clé de sécurité. Les vendeurs peuvent facilement acquérir eux-mêmes les clés de sécurité FIDO2. Ce type de fédération n'était pas possible auparavant avec d'autres technologies d'authentification, ce qui rendait la sécurisation des réseaux de fournisseurs prohibitive du point de vue financier.

Conclusion

Pendant trop longtemps, les mots de passe ont gêné les utilisateurs finaux, les équipes de sécurité et les équipes informatiques. En permettant une sécurité sans mot de passe, FIDO2 ouvre une nouvelle ère dans l'informatique d'entreprise, le service client et les interactions personne-machine.

En utilisant la connexion sans mot de passe FIDO2, les entreprises peuvent renforcer la sécurité de leur réseau, réduire leurs dépenses informatiques, améliorer leur productivité et créer une nouvelle classe de services rentables grâce à une confiance rapide, pratique et omniprésente. La connexion sans mot de passe offre :

- **Amélioration de la convivialité** Grâce à la connexion sans mot de passe, les utilisateurs n'ont plus à s'arrêter pour saisir leurs mots de passe ni à lutter pour les mémoriser. L'accès devient rapide et facile.
- **Sécurité améliorée** Éliminer les mots de passe élimine les vulnérabilités de sécurité des mots de passe volés, récoltés par phishing et des attaques par force brute sur des mots de passe simples.
- **Efficacité améliorée** Un monde sans mot de passe libère les administrateurs informatiques de l'obligation de fournir des dizaines ou des centaines de milliers de mots de passe. La charge de l'assistance informatique diminue, même si la sécurité et la convivialité s'améliorent.

FIDO2 est une solution qui est maintenant disponible pour des centaines de millions d'appareils Windows 10 avec une mise à niveau vers la dernière version de Windows 10. C'est une solution avec laquelle les fournisseurs informatiques et les services informatiques des entreprises peuvent commencer à travailler pour répondre non seulement aux besoins internes de sécurité informatique, mais aussi à ceux des clients.

Comment les parcours des clients pourraient-ils être rationalisés grâce à une connexion sans mot de passe ? Comment peut-on concevoir de nouveau les expériences des utilisateurs sans avoir besoin de mots de passe ? Et si l'accès aux applications et aux services pouvait être rapide, facile et sécurisé partout ?

Quels nouveaux produits et services deviennent possibles lorsque les mots de passe ne sont plus nécessaires, lorsque les ordinateurs de bureau et les périphériques mobiles distants peuvent être facilement approvisionnés et fiables, et lorsque les risques de violation de données et de fraude – enfin – diminuent considérablement ?

Ce sont les questions que les dirigeants d'entreprises et de services informatiques avant-gardistes devraient se poser dès maintenant.

La connexion sans mot de passe FIDO2 fait de ces questions non pas une question spéculative pour les futuristes, mais plutôt une question pratique, voire une question pressante, pour les RSSI, les chefs de produit, les concepteurs d'UX, les spécialistes du marketing et autres professionnels qui se consacrent à fournir les meilleurs produits, services et expériences possibles tout en s'assurant que l'authentification est toujours sécurisée.

Recommandations

Comment les dirigeants d'entreprise, les DSI, les directeurs de la technologie et les autres responsables informatiques doivent-ils se préparer à un monde sans mot de passe ? Yubico offre les recommandations suivantes.

Restez informé

Abonnez-vous aux mises à jour de Yubico en visitant www.yubico.com/go-passwordless

Rejoignez le programme des développeurs Yubico

Les développeurs devraient rejoindre le programme des développeurs Yubico pour avoir accès aux ateliers, aux logiciels libres et à l'assistance de développement.

Mettez à niveau les options d'authentification à deux facteurs dès aujourd'hui

Pour inclure la prise en charge des clés de sécurité FIDO2 et être prêt à passer à une connexion sans mot de passe.

Élaborez une stratégie pour passer au sans mot de passe

Rassemblez une équipe de responsables commerciaux et informatiques au sein de votre organisation pour réfléchir à la meilleure façon de tirer parti de l'authentification sans mot de passe. Pour commencer, l'équipe pourrait vouloir :

- Élaborer un modèle de coût pour les mots de passe. Combien de demandes d'assistance et de requêtes auprès des centres d'appels sont liées à des mots de passe ? Combien de temps prend généralement chaque demande ? Combien de temps faut-il aux administrateurs pour attribuer des mots de passe aux nouveaux utilisateurs ? Combien de productivité est perdue à cause des verrouillages de comptes ? Faites une analyse comparative du temps et des dépenses liés à vos pratiques d'authentification actuelles afin de comprendre les économies réalisées.
- Identifiez des projets pilotes qui permettront à votre équipe de déployer la connexion sans mot de passe à une communauté d'utilisateurs sélectionnée. Concentrez-vous sur les domaines qui nécessitent une authentification forte et où l'optimisation de l'expérience utilisateur offrirait des avantages importants. Surveillez la progression du déploiement et appliquez les leçons apprises aux déploiements futurs.

Références

1. ”2020 State of Password and Authentication Security Behaviors Report”. Ponemon Institute. https://pages.yubico.com/2020-password-and-authentication-report
2. “New Research: Most People Have 70-80 Passwords”. Newswire. https://www.newswire.com/news/new-research-most-people-have-70-80-passwords-21103705
3. “Average Business User Has 191 Passwords”. Security Magazine. https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
4. Kessem, Limor. “Millennial Habits May Bring An End To The Password Era | SC Media”. SC Media. https://www.scmagazine.com/millennialhabits-may-bring-an-end-to-the-password-era/article/746144/
5. “Data Breach Investigation Report”. Verizon Enterprise. https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/
6. “Most hacked passwords revealed as UK cyber survey exposes gaps in online security”. National Cyber Security Center, 2019 Cyber Security Survey. https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security
7. “Protect your accounts with smarter ways to sign in on World Passwordless Day”. Microsoft. https://www.microsoft.com/security/blog/2020/05/07/protect-accounts-smarter-ways-sign-in-world-passwordless-day/
8. Verizon, ibid.
9. Ward, Kelsey. “Credential stuffing rules the day as 90% of login attempts no longer made by humans”. Secureidnews.com. https://www.secureidnews.com/news-item/credential-stuffing-rules-the-day-as-90-of-login-attempts-no-longer-made-by-humans/
10. “Statistic: the total market share of Windows 10 version 1903/1909 edition reach 75.2%”. Meterpreter. https://meterpreter.org/statistic-the-total-market-share-of-windows-10-version-1903-1909-edition-reach-75-2/
11. “NIST SP 800-63 Digital Identity Guidelines”. Nist.Gov. https://www.nist.gov/itl/tig/projects/special-publication-800-63
12. “Pcprox® Mat | RF Ideas”. Rfideas.Com. https://www.rfideas.com/products/presence-detectors/pcprox-mat
13. “Is Cybersecurity Incompatible With Digital Convenience?” McKinsey & Company. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience
14. “Energy Sector Tops List Of US Industries Under Cyber Attack, Says Homeland Security Report - Iot Now - How To Run An Iot Enabled Business”. Iot Now - How To Run An Iot Enabled Business. https://www.iot-now.com/2015/03/12/30962-energy-sector-stays-top-of-the-list-ofus-industries-under-cyber-attack-says-homeland-security-report
15. “Your Medical Record Is Worth More To Hackers Than Your Credit Card”. Reuters. https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
16. “Survey Reveals Sharing EHR Passwords is Commonplace”. HIPAA Journal. https://www.hipaajournal.com/sharing-ehr-passwords-commonplace/
17. “Data trust pacesetters show how to create and protect value from data”. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity/data-trust-pacesetters.html

yubico

À propos de Yubico Yubico établit de nouvelles normes mondiales pour un accès facile et sécurisé aux ordinateurs, serveurs et comptes Internet. Fondée en 2007, Yubico est une entreprise privée qui possède des bureaux en Australie, en Allemagne, à Singapour, en Suède, au Royaume-Uni et aux États-Unis. Découvrez pourquoi neuf des 10 plus grandes marques Internet et des millions d'utilisateurs dans plus de 160 pays utilisent notre technologie sur **www.yubico.com.**

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 États-Unis
844-205-6787 (numéro vert)
650-285-0088