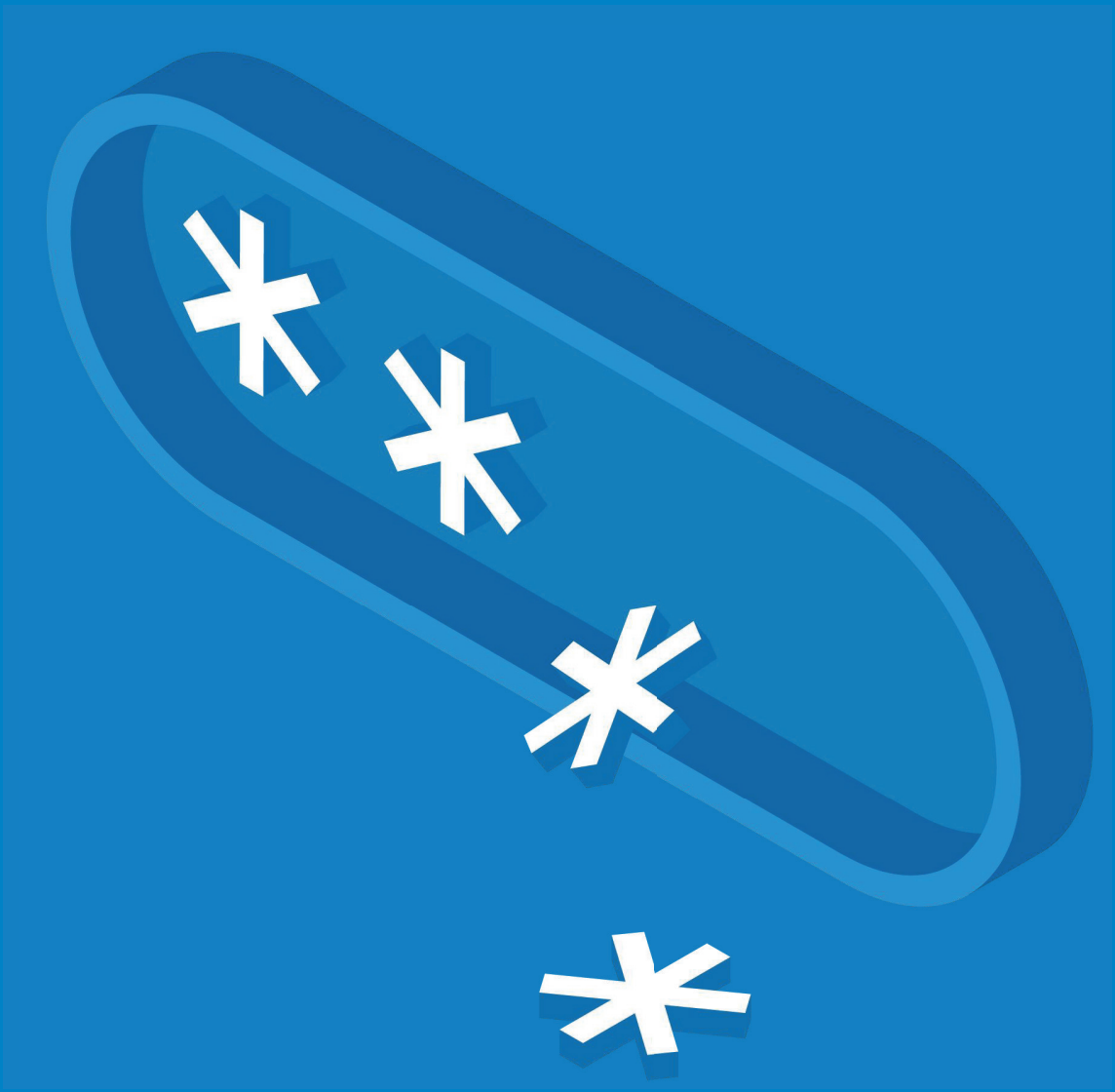
Passwordless : Adopter l'authentification sans mot de passe



okta

Sommaire

Introduction 3

À la recherche d'une solution pour abandonner les mots de passe 4

Évaluation de la méthode d'authentification actuelle 6

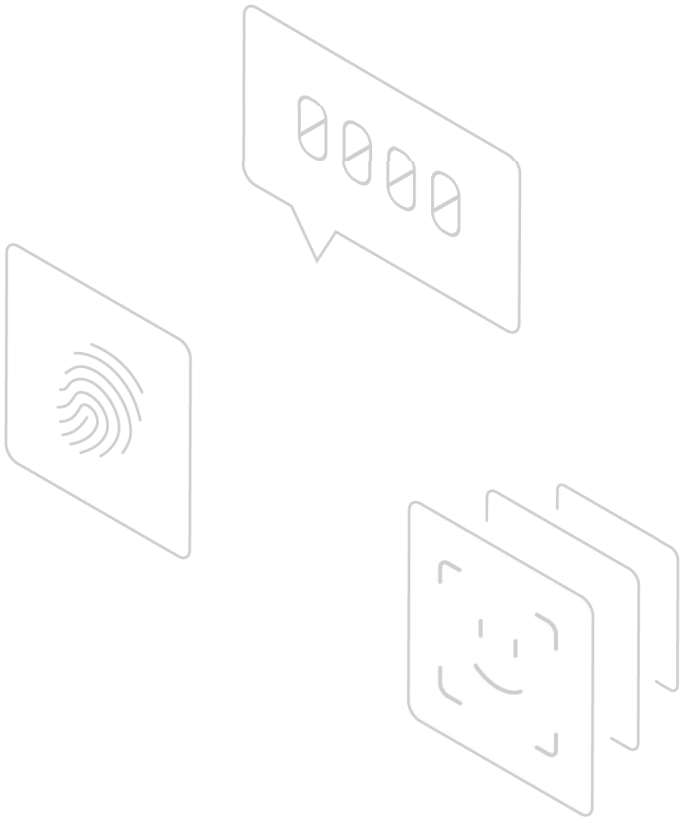
Prise en main de l'authentification sans mot de passe 8

Approches courantes de l'accès sans mot de passe 9

- Envoi de magic links par e-mail 9
- Facteurs séquentiels 10
- WebAuthn 12

Se préparer à un fonctionnement sans mot de passe 14

Introduction



Depuis plus de 50 ans, la sécurité et la gestion des identités numériques sont fondées sur l'authentification traditionnelle à l'aide d'un nom d'utilisateur et d'un mot de passe. Or, la multiplication des comptes utilisateurs crée de nombreux problèmes : difficulté pour les utilisateurs de se souvenir de plusieurs mots de passe, coûts d'assistance et, surtout, risques pour la sécurité liés aux identifiants compromis. Ces nouvelles problématiques remettent en cause l'utilité des mots de passe. L'idée d'éliminer les mots de passe de l'expérience d'authentification séduit de plus en plus les entreprises.

Les nouvelles normes de sécurité sans mot de passe, l'attente de meilleures expériences client ou apparentées, et l'explosion des coûts sont à l'origine de ce nouvel attrait pour la suppression des mots de passe. Ce livre blanc présente l'authentification sans mot de passe pour les clients et les collaborateurs, et explique comment les entreprises peuvent entamer leur transition vers l'élimination des mots de passe.

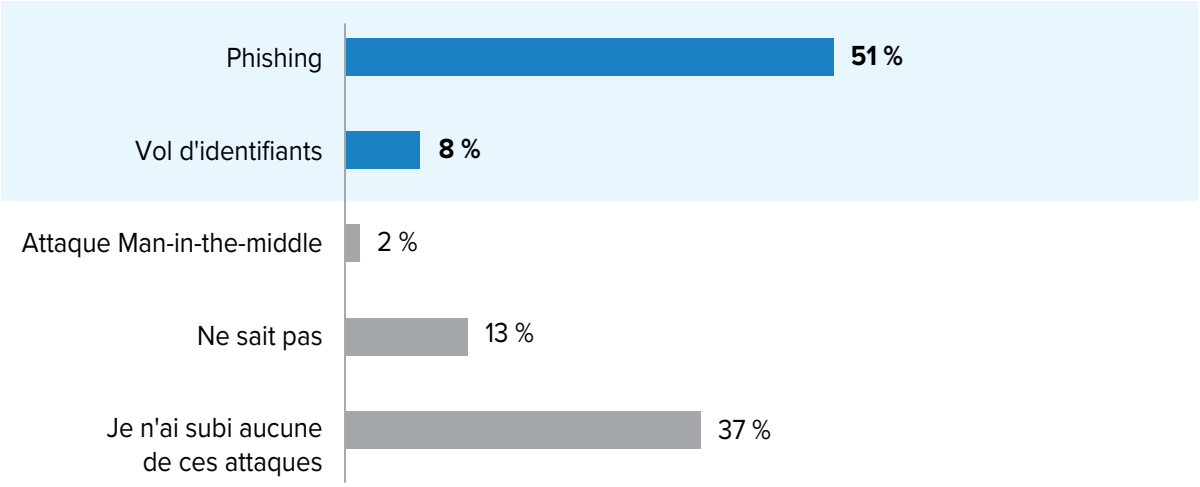
À la recherche d'une solution pour abandonner les mots de passe

Pour saisir l'intérêt de l'authentification sans mot de passe, il faut comprendre les problèmes que posent les mots de passe. En voici les principaux :

Protection insuffisante des comptes

Les mots de passe sont à l'origine de nombreux types d'attaques axées sur les identités. Mots de passe compromis lors de vols d'identifiants, phishing, password spray ou non-respect des bonnes pratiques de création de mots de passe sont autant de causes potentielles des attaques par piratage de comptes. Pour se protéger efficacement, les entreprises doivent recourir à une couche d'authentification supplémentaire, l'authentification multifacteur (MFA, Multi-Factor Authentication).

> *« 81 % des brèches liées au piratage sont dues à des mots de passe trop faibles ou dérobés »*
>
> *— Data Breach Investigations Report 2017 de Verizon*



59 % des participants ont déjà subi un vol d'identifiants ou une attaque par phishing
Rapport 2019 de Ponemon sur l'authentification

Mais l'authentification MFA n'est pas une solution parfaite. Le problème de cette technologie est qu'elle s'appuie en grande partie sur des facteurs secondaires vulnérables, comme les SMS, dont la fragilité est connue et exploitée par les pirates.

Expérience utilisateur médiocre

Les mots de passe sont source de frustration. Si les bonnes pratiques varient concernant le choix des mots de passe, nous savons toutefois que ces derniers doivent être uniques et difficiles à deviner, tout en étant faciles à mémoriser. D'après une enquête de l'Université d'Oxford, environ un tiers des achats en ligne sont abandonnés au moment du paiement par des clients ayant oublié leurs mots de passe.

Augmentation des coûts

Les coûts associés aux mots de passe annihilent les avantages liés à leur utilisation. La gestion des mots de passe est l'un des principaux motifs de contact des centres d'appels. Pour les entreprises, il est donc essentiel de réduire les demandes d'assistance imposées par les mots de passe.

12,6
minutes/semaine

Temps moyen passé par semaine à saisir ou réinitialiser des mots de passe

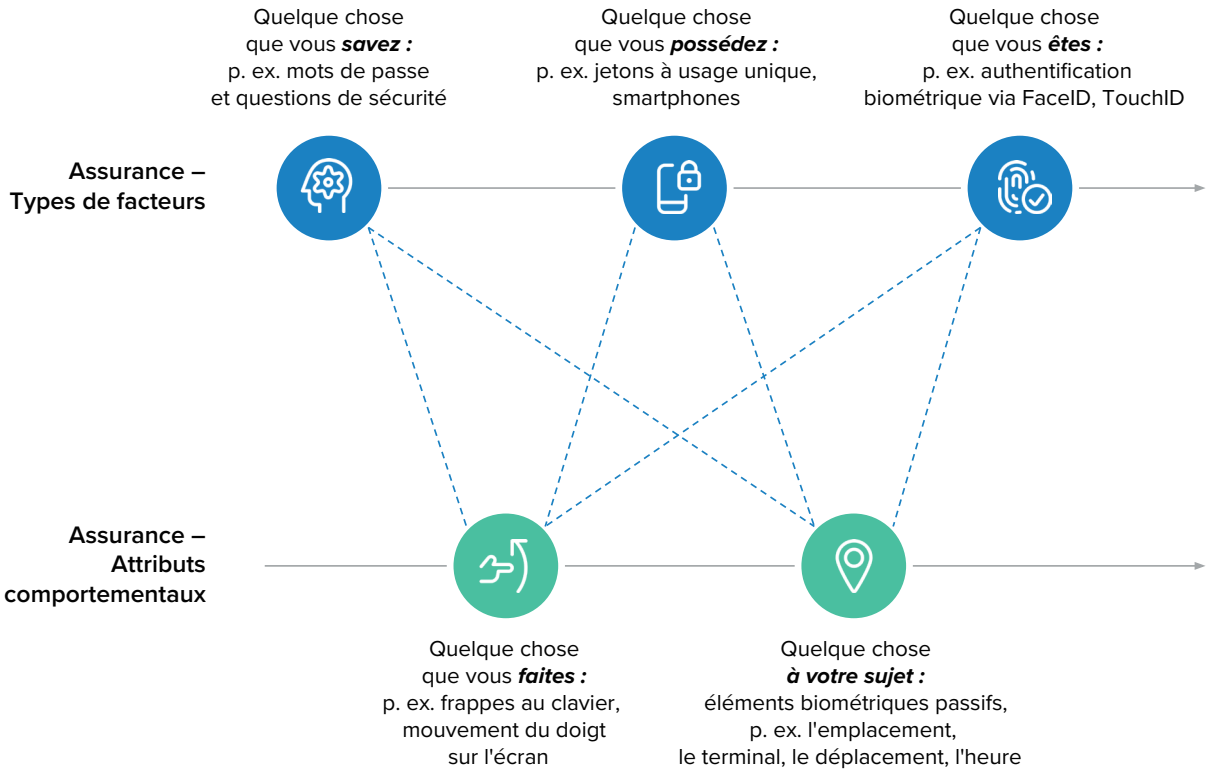
5 217 456 $

Coût annuel de la perte de productivité et de main d'œuvre par entreprise en moyenne

Source : Rapport 2019 de Ponemon sur l'authentification

Évaluation de la méthode d'authentification actuelle

Les méthodes d'authentification actuelles utilisent des facteurs de connaissance, de possession ou de biométrie. Les entreprises combinent souvent un ou plusieurs facteurs et attributs comportementaux pour déterminer les décisions d'accès. En multipliant les couches de sécurité, elles pensent diminuer le risque qu'un pirate accède à un compte utilisateur.



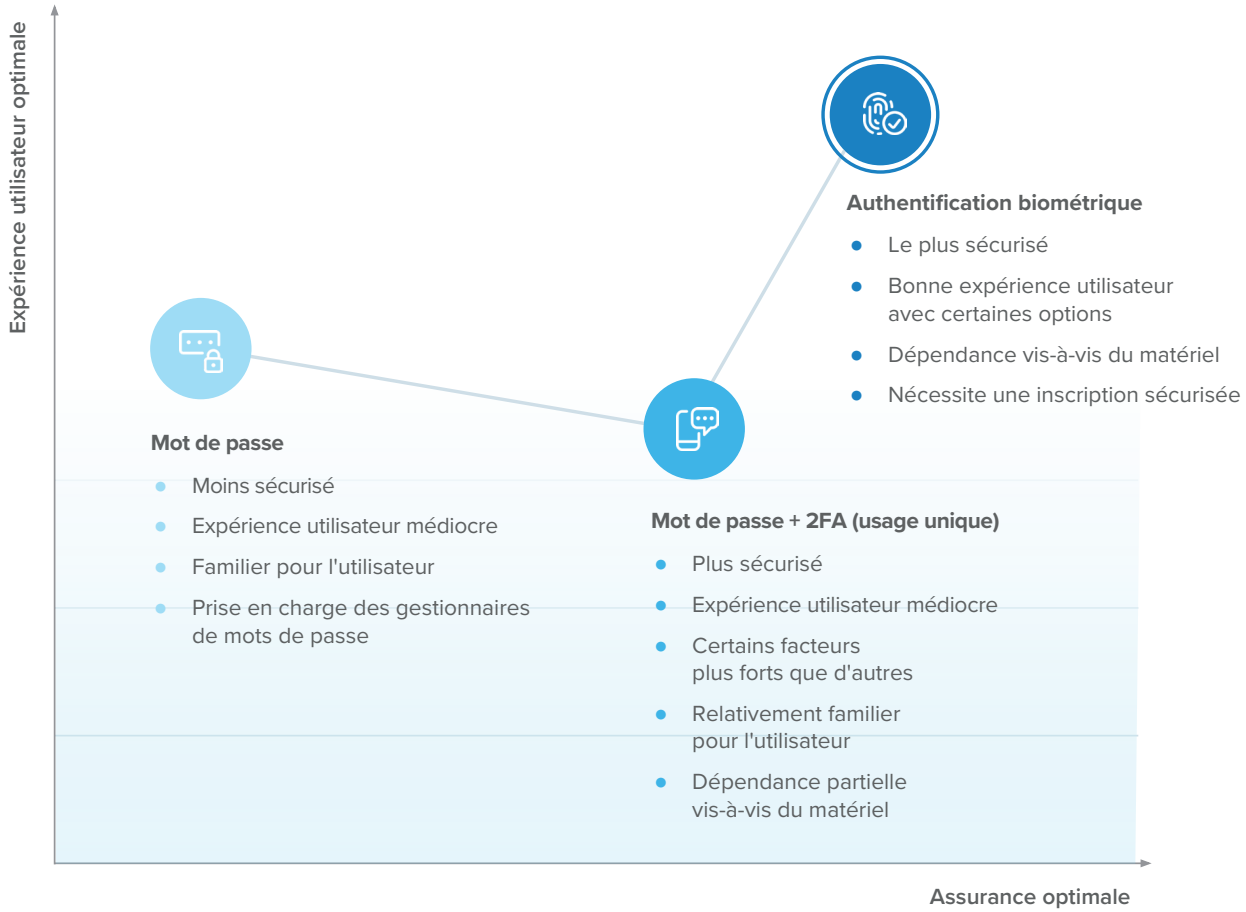
Pour évaluer les méthodes d'authentification, vous devez vous concentrer sur deux attributs clés :

Assurance / sécurité

Le mécanisme d'authentification permet-il de s'assurer que seul l'utilisateur autorisé a accès au compte ?

Expérience utilisateur

- Le mécanisme d'authentification assure-t-il la fluidité du processus d'enregistrement, d'authentification et de récupération ?
- L'authentificateur prend-il en charge l'authentification de l'ensemble des groupes d'utilisateurs, types de terminaux et plateformes logicielles ?



Prise en main de l'authentification sans mot de passe

L'abandon des mots de passe doit être le fruit d'une réflexion aboutie. Nous recommandons aux entreprises qui souhaitent s'engager dans cette voie d'opter pour une approche graduelle en examinant des aspects tels que les menaces, les technologies, les parcours utilisateurs, les coûts, les difficultés d'adoption et l'implémentation.

Menaces

- Vols d'identifiants
- Attaques Man-in-the-Middle
- Attaques Man-in-the-Browser
- Password spray
- Attaques par force brute

Technologie

- Prise en charge des navigateurs
- Approche technologique
- Authentificateurs de plateforme et authentificateurs externes

Parcours utilisateur

- Flux d'enregistrement
- Flux d'authentification
- Flux de récupération

Considérations relatives à l'entreprise

- Assistance
- ERP
- Adoption des terminaux
- Exigences de conformité

Difficultés d'adoption

- Les mots de passe sont courants
- Les gestionnaires de mots de passe sont également courants
- Le provisioning des mots de passe est facile

Implémentation

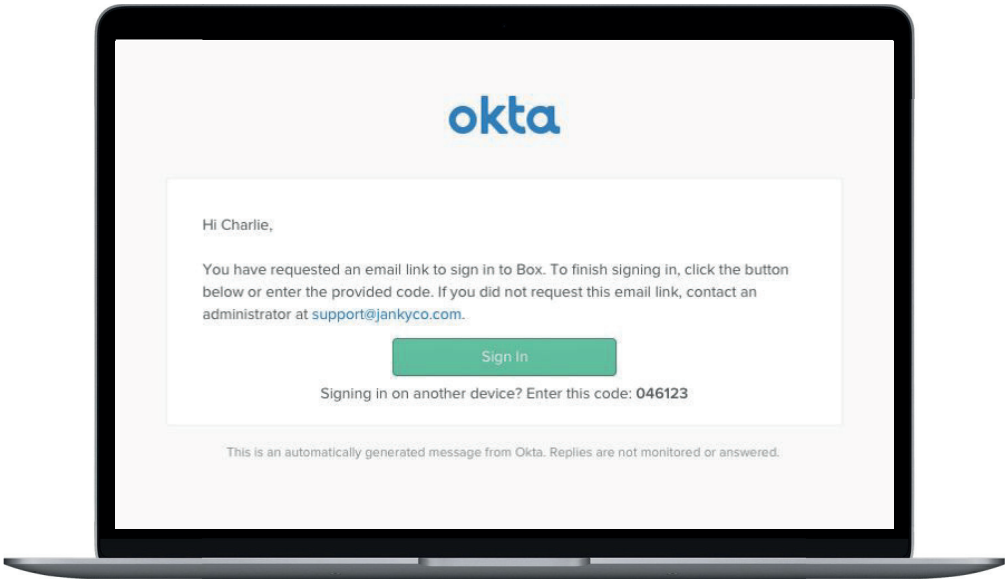
- Exigences de sécurité et de conformité
- Prise en charge des sites web

Approches courantes de l'accès sans mot de passe

L'élimination des mots de passe et la mise en place d'un accès sans mot de passe peuvent être accomplies à l'aide de différentes technologies. Les approches comme l'envoi de magic links par e-mail reposent sur la présence d'un jeton OTP codé ou d'un lien actif dans le corps d'un e-mail sécurisé, tandis que les approches comme WebAuthn exploitent la cryptographie basée sur des jeux de clés publique/privée pour assurer une authentification sécurisée.

Okta propose différentes approches d'authentification sans mot de passe. Cette section présente les principales méthodes possibles.

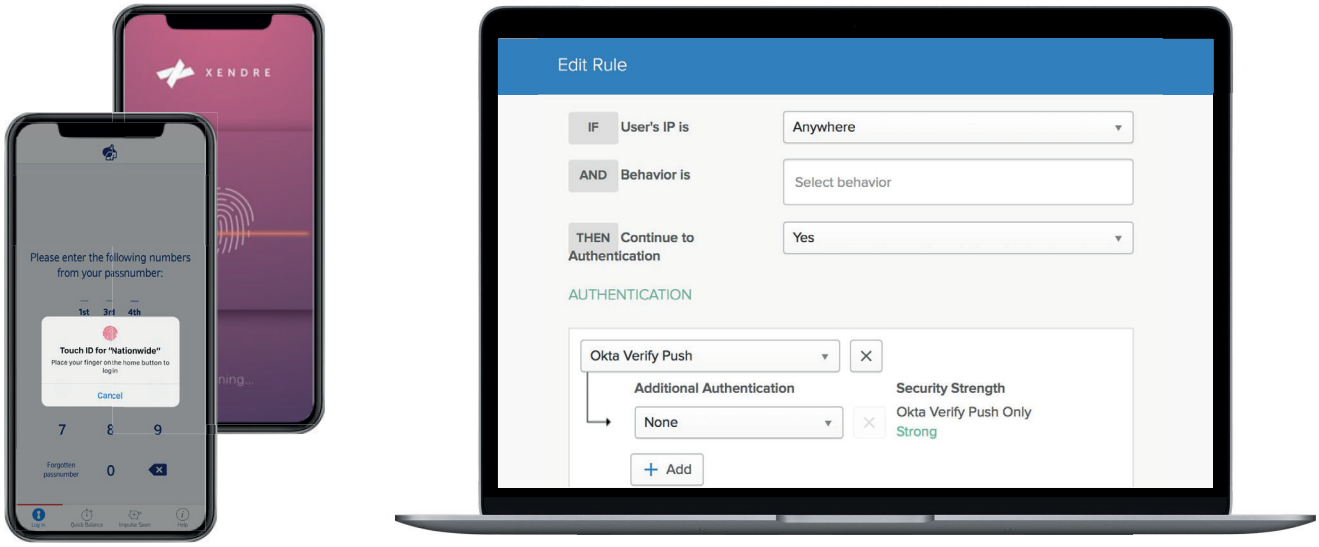
Envoi de magic links par e-mail



L'authentification sans mot de passe basée sur les e-mails est devenue très courante. Cette méthode est en fait un flux de réinitialisation de mot de passe. Elle consiste à envoyer un lien secret à l'utilisateur, qui n'a pas à saisir son mot de passe mais doit en définir un nouveau. Cette méthode d'authentification est bien connue de la plupart des utilisateurs puisqu'ils l'ont déjà utilisée des dizaines, voire des centaines de fois. Elle a été popularisée par des applications comme Slack et Medium. La véritable authentification sans mot de passe va au-delà de ce processus. Les concepteurs d'applications éliminent le mot de passe (et le processus de réinitialisation associé) en envoyant un lien secret à usage unique, limité dans le temps ou limité au cycle de vie de l'utilisateur, à l'adresse e-mail de ce dernier. En cliquant sur le lien, l'utilisateur est authentifié et un cookie ayant une longue durée de vie est installé pour qu'il reste connecté. L'utilisateur n'a jamais besoin de définir, d'enregistrer ou de saisir un mot de passe, ce qui est très pratique, en particulier sur les terminaux mobiles. Cette méthode d'authentification sans mot de passe est indépendante de tout matériel et particulièrement intéressante pour les applications grand public.

Cas d'usage	Avantages	Inconvénients
• Modèles de connexion peu fréquents • Autre méthode d'authentification sans mot de passe pour WebAuthn • Arrêt des attaques axées sur les mots de passe	• Facilité de déploiement et d'utilisation • Onboarding fluide • Indépendance vis-à-vis du matériel • Expérience utilisateur satisfaisante et familière • Expérience homogène sur ordinateur et sur mobile	• Externalisation de la sécurité des comptes e-mail • Pas de contrôle ni de visibilité sur le partage du lien (e-mail) • Exposition aux attaques Man-in-the middle si l'e-mail n'est pas chiffré

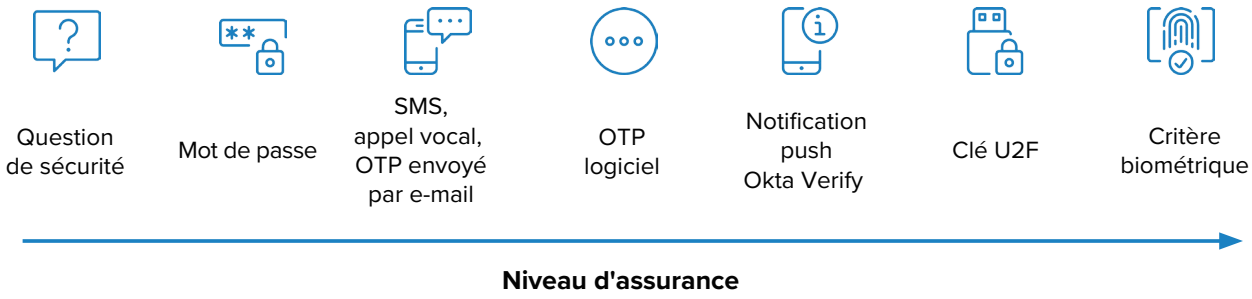
Facteurs séquentiels



En combinant la solution Okta Adaptive Multi-Factor Authentication et les informations sur les menaces fournies par ThreatInsight, les entreprises peuvent configurer en toute sécurité une solution sans mot de passe utilisant divers facteurs d'authentification. Lorsque le risque est faible, l'expérience de connexion des utilisateurs peut être simplifiée pour leur permettre d'accéder facilement aux données et aux applications dont ils ont besoin. Par contre, lorsqu'une connexion présente un risque élevé, des facteurs d'authentification supplémentaires s'imposent. Un administrateur peut, par exemple, définir l'application mobile Okta Verify comme facteur d'authentification principal. Si l'utilisateur se connecte depuis un emplacement et un terminal connus, Okta envoie une demande d'authentification via l'application que l'utilisateur doit accepter pour obtenir l'accès.

Toutefois, si l'authentification multifacteur adaptative détecte une anomalie qui augmente le niveau de risque de la demande de connexion, Okta peut inviter l'utilisateur à faire appel à un deuxième facteur d'authentification comme WebAuthn.

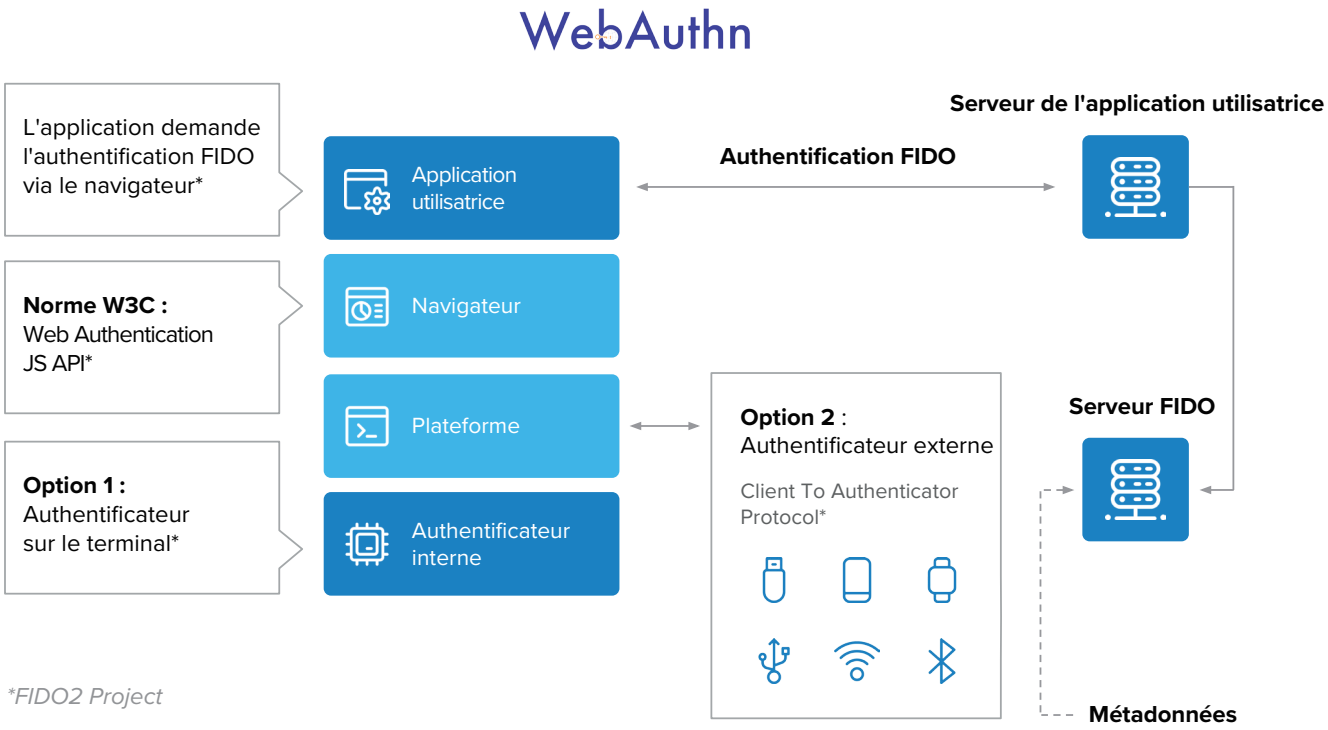
Il est important que les administrateurs tiennent compte du niveau d'assurance lorsqu'ils choisissent une méthode d'authentification et des facteurs. Ils doivent se baser sur le contexte lié à l'utilisateur pour simplifier la connexion et améliorer l'ergonomie chaque fois que la situation le permet. Un facteur de connaissance, comme une question de sécurité, est facile à utiliser, mais aussi moins sécurisé qu'un facteur de possession comme U2F. Dans cette perspective, il est logique d'opter pour un facteur de possession simple lorsqu'un utilisateur se connecte depuis son réseau ou son emplacement habituel au siège, et de réserver les facteurs plus sécurisés aux instances dans lesquelles un terminal, un réseau ou un emplacement augmente le niveau de risque.



Bien entendu, les administrateurs doivent également choisir des facteurs adaptés aux technologies de l'entreprise. L'utilisation d'Okta Verify, par exemple, n'a de sens que si tout le monde a accès à un smartphone. Dans certains scénarios, il est donc préférable d'utiliser un autre facteur, comme un mot de passe à usage unique envoyé par SMS.

Cas d'usage	Avantages	Inconvénients
• Modification de l'expérience de connexion en fonction du risque de la session • Intégration de facteurs offrant un niveau d'assurance plus élevé dans l'expérience d'authentification	• Connexion offrant un niveau d'assurance élevé • Expérience homogène sur ordinateur et sur mobile	• Dépendances potentielles vis-à-vis du matériel

WebAuthn



WebAuthn est un framework d'authentification sans mot de passe, basé sur des normes, qui permet de simplifier et de sécuriser l'authentification des utilisateurs sur les applications web en utilisant des terminaux enregistrés (téléphones, ordinateurs portables, etc.) comme facteurs. Avec cette nouvelle norme, n'importe quelle application web exécutée dans un navigateur compatible peut désormais tirer parti des terminaux enregistrés comme authentificateurs pour identifier les utilisateurs de manière sécurisée. La prise en charge par Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari et Opera, sans oublier l'adoption rapide par différentes plateformes (Microsoft Edge avec Windows Hello, Google Android, etc.) signifie en outre qu'il existe enfin un moyen pratique de déployer FIDO2/ WebAuthn. Aujourd'hui, les entreprises peuvent utiliser des authentificateurs itinérants (des clés YubiKey, par exemple) ou se servir directement des plateformes prises en charge, puisque le terminal lui-même est utilisé pour WebAuthn.

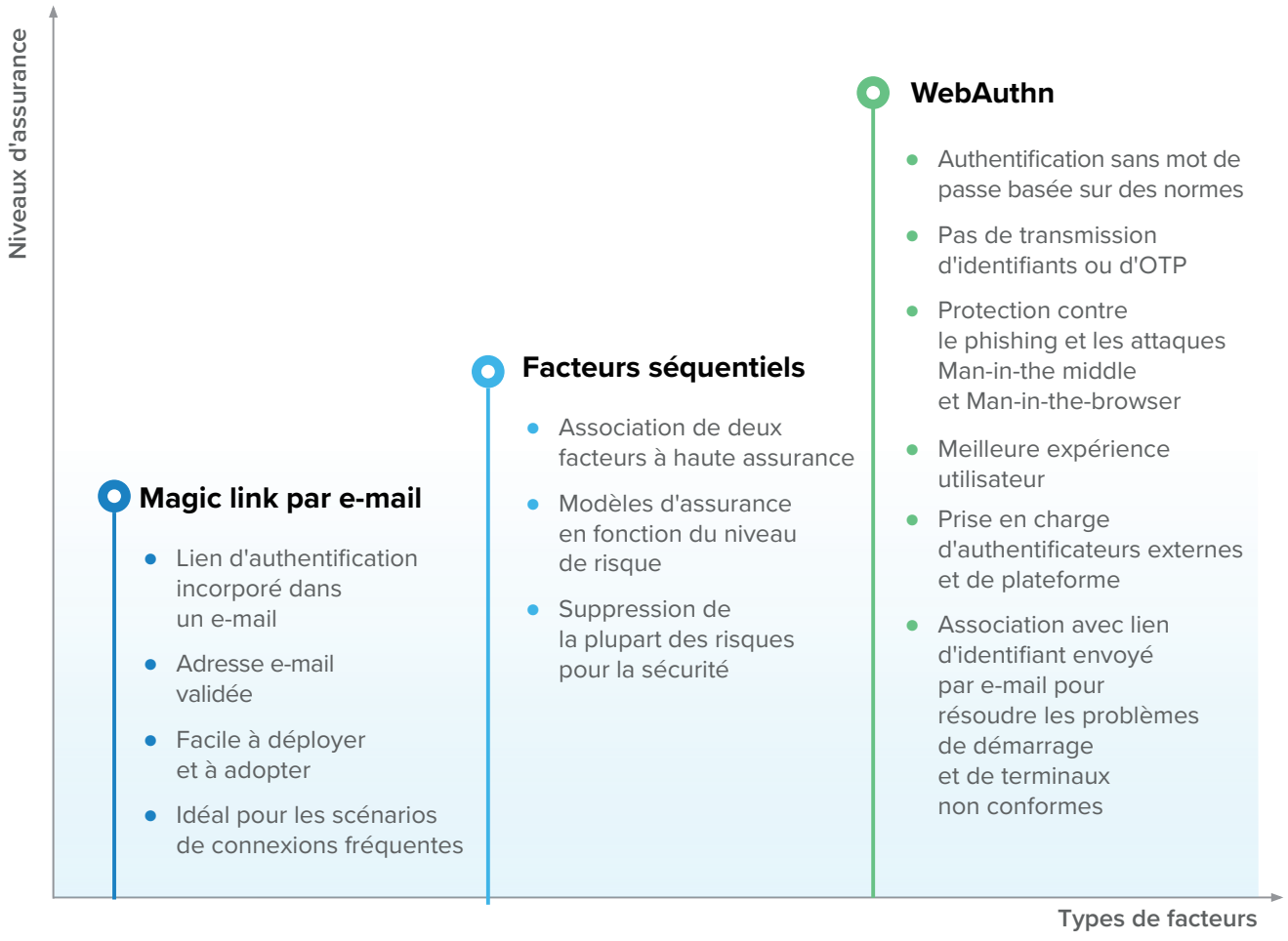
Cas d'usage	Avantages	Inconvénients
• Authentification sans mot de passe basée sur des normes • Expérience d'authentification évolutive	• Piratage de comptes : blocage des attaques d'usurpation d'identité comme le phishing, le piratage des identifiants, le password spray, etc. • Aucune gestion des identifiants requise • Amélioration de l'expérience d'authentification des utilisateurs • Réduction des demandes d'assistance liées à la gestion des mots de passe	• Obligation de prise en charge du matériel et des navigateurs • Nécessité d'un flux sécurisé de récupération et d'adoption par les utilisateurs • Association requise avec d'autres méthodes d'authentification sans mot de passe, comme les liens d'identification envoyés par e-mail, en cas de besoin d'un autre moyen d'authentification

Pour plus d'informations, consultez notre livre blanc sur WebAuthn.

Se préparer à un fonctionnement sans mot de passe

L'adoption d'une authentification sans mot de passe est une étape cruciale pour les entreprises et les services qui veulent gérer les nombreux risques pour la sécurité et offrir une expérience client fluide. De plus en plus d'entreprises envisagent cette transition, mais elles ne doivent pas oublier que ce processus doit être évolutif et sans rupture brutale. C'est pourquoi nous mettons à votre disposition une roadmap récapitulant les étapes simples à suivre pour réussir votre transition et mettre en œuvre une véritable authentification sans mot de passe. L'abandon des mots de passe est un processus qui doit être réfléchi et planifié avec soin. Le cycle de vie de l'authentification doit être abordé dans son intégralité, de l'inscription sécurisée, à la migration à partir des mots de passe, en passant par la facilité de déploiement, la récupération et l'offboarding. Pour réussir leur transition vers l'authentification sans mot de passe, et ainsi éliminer les attaques d'usurpation d'identité, assurer des expériences satisfaisantes et développer leur activité, les entreprises doivent prendre en compte ces différents aspects et besoins.

Entamez votre transition vers l'élimination des mots de passe avec Okta



À propos d'Okta

Okta est la première société indépendante spécialisée dans la gestion et la protection des données d'identification. Conçue pour les professionnels, la solution Okta Identity Cloud permet de connecter en temps et en heure et de façon sécurisée les utilisateurs aux technologies dont ils ont besoin. Dans un souci de simplicité, nous proposons plus de 6 000 intégrations clés en main pour les applications et les fournisseurs d'infrastructures. Nos clients peuvent ainsi profiter en toute sécurité des technologies les mieux adaptées à leur activité. Plus de 6 100 entreprises nous font confiance pour les aider à protéger les données d'identification de leurs employés et de leurs clients. Parmi celles-ci, on retrouve notamment 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America ou encore Twilio.

www.okta.com/fr