2024

Le point sur l'adoption du MFA et les authentificateurs

The Secure Sign-in Trends Report

okta

Il a fallu un certain temps pour convaincre les entreprises et les utilisateurs des avantages de l'authentification multifacteur, ou MFA (Multi-Factor Authentication).

Dès le départ, la communauté de la sécurité a été unanime à affirmer que le MFA était indispensable pour se protéger contre la marée d'attaques axées sur les mots de passe. Pourtant, la plupart des entreprises n'imposaient une demande d'authentification MFA que pour l'accès à leurs systèmes les plus critiques.

Lors de la pandémie cependant, l'adoption du MFA s'est généralisée. Okta a constaté une augmentation de 15 % dans l'utilisation du MFA en quelques mois, lorsque le monde s'est mis à l'heure du télétravail. À l'heure actuelle, la plupart des administrateurs Okta, et la majorité des utilisateurs, accèdent à leurs applications professionnelles après une authentification MFA. Partout dans le monde, les organismes de réglementation et de normalisation exigent que les entreprises sécurisent les accès au moyen de ces méthodes de connexion plus robustes.

Dans le rapport « The Secure Sign-in Trends Report » de cette année, nous relevons une forte croissance de l'adoption des méthodes de connexion sans mot de passe (passwordless) et résistantes au phishing. En janvier de cette année, 5 % des utilisateurs de la plateforme Okta Workforce Identity Cloud se sont connectés à leurs applications sans jamais utiliser de mot de passe. Ce petit pourcentage dissimule pourtant un énorme potentiel latent. Il implique en effet que nous sommes bel et bien entrés dans l'ère du passwordless. C'est de l'ordre du possible. Si ces clients Okta l'ont adopté, pourquoi pas vous ?

Nous pensons que la prochaine vague d'adoption du MFA ne sera pas déclenchée par les puristes de la sécurité, ni même par ces décideurs très sensés exigeant que les entités réglementées imposent aux utilisateurs une authentification multifacteur. Elle sera motivée par l'exigence d'une meilleure expérience utilisateur et d'un plus haut degré d'assurance de la sécurité. Que ce soit en tant que collaborateur ou client, une fois que vous aurez essayé le passwordless, vous ne ferez plus jamais marche arrière.

J'espère que nos analyses et statistiques vous intéresseront. Merci de votre attention.

Todd McKinnon
CEO, Okta

Sommaire

Comment mesurer l'adoption du MFA

Avant de vous plonger dans le rapport, il est important de savoir que ses données et conclusions reflètent les choix en matière d'authentification opérés par les entreprises, leurs administrateurs et leurs collaborateurs. Même si nous faisons souvent référence aux « utilisateurs », ces derniers sont généralement des collaborateurs en entreprise et leurs options d'authentification sont souvent limitées par les politiques de l'organisation.

Il existe plusieurs façons de mesurer l'adoption de l'authentification multifacteur (MFA), comme l'illustre le tableau ci-dessous. Pour les besoins de cette étude, nous avons mesuré l'adoption de l'utilisation réelle du MFA, soit le pourcentage d'utilisateurs qui se sont connectés à l'aide du MFA au cours d'une période donnée.

Option de mesure	Définition
Taux d'attachement du MFA	% des clients qui ont acheté un SKU incluant le MFA
Taux d'inscription au niveau des tenants	% de tenants, ou organisations Okta, qui ont configuré le MFA en vue de son utilisation
Taux d'inscription au niveau des utilisateurs	% des utilisateurs qui ont configuré des authentificateurs MFA
Utilisation du MFA au niveau des utilisateurs	**% des utilisateurs qui se sont connectés au moyen du MFA sur une période donnée**

Nous avons également décidé d'agréger les données d'utilisation du MFA au niveau des utilisateurs étant donné que nous cherchons à mesurer l'adoption du MFA par ceux-ci :

Option d'agrégation	Définition
Taux d'adoption du MFA au niveau des tenants	% des tenants clients Okta avec des utilisateurs qui se sont connectés au moyen du MFA au moins une fois par mois
Taux d'adoption du MFA au niveau des utilisateurs	**% des utilisateurs qui se sont connectés au moyen du MFA au cours d'un mois**
Taux d'adoption du MFA au niveau des connexions	% des connexions réussies impliquant une demande d'authentification MFA au cours d'un mois

Il faut également rappeler que cette étude ne recense que les authentifications MFA directes dans Okta Workforce Identity Cloud (WIC). Si les utilisateurs s'authentifient exclusivement à l'aide du MFA d'autres fournisseurs d'identité et utilisent la fédération d'entreprise ou l'authentification sociale pour se connecter à Okta, ils ne sont pas repris dans nos données d'adoption du MFA. Dès lors, il est probable que le taux d'adoption rapporté sous-estime légèrement le taux global d'utilisation du MFA au sein de notre clientèle. Nous avons également exclu les comptes de test. Toutes les données relatives à l'adoption et aux métriques sont dérivées des tenants/organisations de production associés à des clients payants.

Propriétés de sécurité et de facilité d'utilisation des authentificateurs

Pour mieux appréhender les obstacles à l'adoption du MFA, nous devons d'abord répondre à plusieurs questions essentielles. Pouvons-nous mettre au point un framework et proposer ainsi une vue quantitative et systématique des propriétés des authentificateurs ? Pouvons-nous utiliser des informations axées sur des données pour former les clients à mieux protéger leurs entreprises et à guider le développement produits en ce sens ?

Dans ce but, nous avons évalué les authentificateurs du point de vue de la sécurité et de la facilité d'utilisation, comme le montre le tableau 2. Mesurer ces critères est une tâche difficile, étant donné que la logique et les flux d'interface utilisateur de chaque authentificateur varient et sont parfois hautement personnalisés. Pour assurer la cohérence, nous avons utilisé Okta Identity Engine (OIE), qui offre des flux et des expériences d'identité plus flexibles et mieux conçus.

Nous avons mesuré les propriétés des méthodes d'authentification suivantes : mot de passe, e-mail, mot de passe à usage unique (OTP), notification push, OTP logiciel, question de sécurité, SMS, OTP vocal, Okta FastPass, FIDO2 WebAuthn et carte à puce. Sauf indication contraire, nous avons recueilli les données en janvier 2024 auprès d'organisations de production de clients Okta Workforce Identity Cloud utilisant Okta Identity Engine.

Nous avons pris grand soin de mettre au point des méthodes de collecte de données qui permettent des comparaisons pertinentes entre les authentificateurs. Ce rapport précise les conditions qui compliquent ces comparaisons et explique les implications possibles au niveau de nos résultats. Nous avons également vérifié les variations mensuelles au niveau des données pour nous assurer que les tendances générales restaient cohérentes au fil du temps.

Résumé des principaux constats

L'adoption du MFA reste en hausse

Depuis janvier 2024, l'adoption du MFA a progressé de 66 % parmi les collaborateurs en entreprise utilisant Okta, et 91 % des administrateurs utilisent le MFA.

Les taux d'adoption du MFA varient fortement selon le secteur d'activité

Dans le secteur public et celui de l'enseignement, l'adoption du MFA a enregistré une croissance annuelle de 5 %, qui pourrait encore s'amplifier avec la récente entrée en vigueur de décrets-lois aux États-Unis et les nouvelles modifications réglementaires.

Les authentificateurs résistants au phishing ont la cote

L'adoption des authentificateurs résistants au phishing a augmenté de façon significative. Le taux d'adoption de FIDO2 WebAuthn a progressé, passant de 2 % en 2023 à 3 % en 2024, et celui d'Okta FastPass a bondi de 2 % à 6 % au cours de la même période.

Le passwordless s'installe progressivement

Le nombre de clients Okta qui utilisent des mots de passe commence enfin à baisser grâce à l'adoption de méthodes d'authentification modernes dans les entreprises. Un peu moins de 5 % des utilisateurs n'ont pas utilisé de mot de passe du tout pour leurs connexions au cours du mois de janvier 2024.

Sécurité ou expérience utilisateur : le faux dilemme

Les authentificateurs résistants au phishing offrent une meilleure expérience utilisateur. Dans notre évaluation des performances et de la facilité d'utilisation des authentificateurs, FastPass et FIDO2 WebAuthn s'imposent comme des options d'authentification plus sûres et conviviales que les autres, même avec des critères d'évaluation révisés, plus pratiques.

Introduction

> « Le MFA [authentification multifacteur] est largement reconnu comme l'un des principaux contrôles de sécurité préventifs disponibles à ce jour, sinon le plus important. Il offre une défense robuste contre diverses techniques d'attaques, notamment le password spray, la réutilisation de mots de passe compromis et, dans certains cas, le phishing. Toutefois, l'un des grands défis est qu'il est notoirement difficile à déployer, ce qui retarde sa mise en œuvre dans les entreprises de toutes tailles, même si elles en reconnaissent la valeur[1]. »

Nous sommes tous conscients que le MFA confère un certain degré d'assurance aux connexions des utilisateurs.

En matière de gestion des identités et des accès, l'un des compromis les plus délicats consiste à déterminer le degré de friction que vous êtes disposé à imposer à vos utilisateurs finaux pour sécuriser l'accès aux données et applications de l'entreprise. Trop peu de friction crée des opportunités pour les cybercriminels, et trop de friction pousse les collaborateurs à utiliser des applications non autorisées, ce qui pose également un risque.

Face à l'augmentation des incidents de sécurité graves et des coûts qui leur sont associés, la plupart des entreprises et des collaborateurs finissent par reconnaître qu'une authentification forte est une exigence non négociable, surtout lorsqu'il s'agit de sécuriser l'accès distant aux ressources. Le défi consiste désormais à appliquer une authentification à niveau d'assurance élevé tout en minimisant les points de friction imposés aux utilisateurs finaux.

Dans ce rapport, nous examinons les diverses approches adoptées aujourd'hui par les entreprises pour vérifier l'identité de leurs utilisateurs et empêcher l'accès non autorisé. En nous basant sur les données anonymisées issues des milliards d'authentifications mensuelles des clients Okta, nous avons quelque peu revu notre méthode d'évaluation de la situation actuelle en matière d'authentification, en identifiant les tendances et en analysant les approches en fonction de considérations telles que le secteur, la région et la taille de l'entreprise.

Au final, le rapport de cette année révèle que si l'évolution est positive, elle n'est pas suffisamment rapide. Au cours de la pandémie de COVID-19, nous avons assisté à une hausse de 15 % dans l'adoption du MFA, à une période où les entreprises cherchaient par tous les moyens à sécuriser le télétravail. Il est donc assez décevant de constater le ralentissement de cet élan : l'adoption de l'authentification multifacteur n'a augmenté que de 2 % par an depuis 2023, même si elle partait d'un point de référence déjà élevé. En janvier 2024, 66 % des utilisateurs s'authentifiaient avec le MFA.

Il semble que nous soyons à un moment charnière. Le décret-loi américain sur l'amélioration de la cybersécurité nationale entre en vigueur et les entreprises, tout comme les fournisseurs cloud, multiplient les initiatives pour inciter les utilisateurs à employer des méthodes d'authentification plus sûres. Parallèlement, les leaders technologiques tels que Salesforce, GitHub, Okta et Microsoft entreprennent tous des projets pour imposer le MFA aux utilisateurs à privilèges, ce qui devrait motiver les entreprises à s'intéresser au développement et à l'adoption de méthodes d'authentification offrant un niveau d'assurance élevé sans créer de friction pour les utilisateurs.

Avec ce rapport, nous cherchons à offrir aux professionnels IT et sécurité une perspective orientée données sur les solutions disponibles aujourd'hui et à briser le mythe selon lequel une authentification forte se traduit inévitablement par un surcroît de friction pour les utilisateurs. En fait, c'est tout le contraire : l'authentification résistante au phishing et sans mot de passe est à la fois plus sûre et plus simple à utiliser.

Toutes les données et conclusions de ce rapport s'appuient sur notre analyse des données Okta anonymisées, sauf indication contraire.

[1] https://media.defense.gov/2023/Oct/04/2003313510/-1/-1/0/ESF%20CTR%20IAM%20MFA%20SSO%20CHALLENGES.PDF

Comment utiliser les données

Ce rapport offre un cadre pour mesurer les propriétés de sécurité et de facilité d'utilisation d'un large éventail d'authentificateurs. Nous avons posé des questions critiques pour aider les DSI, les RSSI et les décideurs à comprendre les raisons de la variation du taux d'adoption du MFA. Au nombre de ces questions :

- Comment l'adoption du MFA a-t-elle évolué au fil du temps ?
- Le secteur d'activité, la situation géographique ou la taille d'une entreprise affectent-ils les taux d'adoption du MFA ?
- Quelles caractéristiques de facilité d'utilisation observables sont pertinentes pour l'adoption du MFA ?
    - Combien de temps faut-il généralement à un utilisateur pour s'authentifier avec un authentificateur donné ?
    - Combien de temps faut-il généralement à un utilisateur pour configurer/s'inscrire à un authentificateur donné ?
    - Quelle est la fréquence d'échec des authentifications à l'aide d'un authentificateur donné ?
- Quelles caractéristiques de sécurité observables sont pertinentes pour l'adoption du MFA ?
    - Quelle couverture offre un authentificateur donné en matière de résistance au phishing ?
    - À quelle fréquence les cybercriminels ciblent-ils des comptes utilisant un authentificateur donné dans les attaques par force brute ?

Les réponses à ces questions peuvent aider les responsables IT et sécurité à évaluer les coûts et les avantages des différents authentificateurs afin de déterminer la meilleure solution pour leur entreprise et leurs utilisateurs.

“Cela fait quelques années déjà qu'Okta tire parti de l'authentification sans mot de passe et résistante au phishing. Au cours des 12 mois qui se sont écoulés depuis le dernier rapport « The Secure Sign-in Trends Report », nous avons investi dans l'implémentation de la résistance au phishing tout au long du cycle de vie des utilisateurs — de l'inscription des utilisateurs jusqu'à l'accès et à la récupération des comptes. La bonne nouvelle ? C'est parfaitement réalisable.”

David Bradbury
Chief Security Officer

okta

Bilan de l'adoption du MFA

Le MFA est une composante essentielle de n'importe quelle posture de sécurité à niveau d'assurance élevé. Lors d'une connexion par MFA, un utilisateur doit fournir au moins deux facteurs distincts pour que le système puisse vérifier son identité. Ces facteurs incluent une information qu'il connaît (facteur de connaissance, p. ex. un mot de passe), un élément qu'il possède (facteur de possession, p. ex. un terminal enregistré) ou une caractéristique qui lui est propre (facteur d'inhérence, p. ex. une caractéristique biométrique).

Si le MFA est généralement considéré comme indispensable à une connexion sécurisée, plusieurs facteurs internes et externes influencent son adoption. Dans cette section, nous examinons le taux d'adoption dans son évolution au fil du temps ainsi que par région, secteur d'activité, taille d'entreprise, type d'authentificateur et type d'utilisateur (p. ex. administrateur). Les résultats servent à la fois de point de référence pour évaluer les progrès accomplis au niveau des entreprises et du secteur, et pour identifier les axes d'amélioration.

Facteur ou authentificateur

Ce rapport emploie les termes « authentificateur » et « facteur » conformément aux définitions du NIST (National Institute of Standards and Technology) :

Authentificateur : mécanisme détenu ou contrôlé par le demandeur et utilisé pour authentifier son identité.

Facteur : caractéristique de l'authentification, par exemple un facteur de connaissance (une information que vous connaissez, p. ex. un mot de passe ou une question de sécurité), un facteur de possession (un élément que vous possédez, p. ex. un terminal enregistré) ou un facteur d'inhérence (une caractéristique qui vous est propre, p. ex. votre empreinte digitale).

Remarque : chaque authentificateur possède un ou plusieurs facteurs d'authentification. Il peut y avoir confusion lorsque « facteur » est utilisé à la place du terme « authentificateur » ou quand un authentificateur peut proposer plusieurs facteurs. Par exemple, Okta FastPass peut fournir à la fois un facteur de possession (terminal enregistré) et un facteur d'inhérence (vérification biométrique).

Bilan de l’adoption du MFA

Évolution de l’adoption du MFA

La figure 1 présente les taux d’adoption du MFA par les utilisateurs pour les clients Okta Workforce Identity Cloud (qui utilisent Okta pour offrir à leurs collaborateurs, prestataires et partenaires un accès sécurisé à leurs ressources d’entreprise) d’octobre 2019 à janvier 2024. Chaque donnée représente l’adoption du MFA au cours du mois concerné.

Comme nous l’avons mentionné dans notre rapport de 2023, de février à mars 2020, le taux d’adoption du MFA est passé de 35 % à 50 %, stimulé par le passage rapide au télétravail et la nécessité de sécuriser un périmètre s’étendant désormais bien au-delà du réseau d’entreprise. Depuis lors, la croissance annuelle du taux d’adoption du MFA a atteint 6 % par an de 2020 à 2023, avant de ralentir pour s’établir à 2 % en 2024. En janvier 2024, 66 % des utilisateurs se connectaient à l’aide du MFA.

Ce taux de croissance est loin de suivre le rythme de progression des attaques basées sur l’identité. En 2024, nous avons observé de nombreuses attaques visant des comptes utilisateurs et machines dépourvus de l’authentification multifacteur. En réponse, de nombreux fournisseurs cloud imposent désormais l’adoption du MFA pour les comptes utilisateurs à privilèges, voire pour tous les comptes.

À noter

Puisque l’application du MFA pour les comptes à privilèges devient un contrôle de base attendu par les entreprises, il est probable qu’un plus grand nombre de fournisseurs de services vont exiger le MFA pour les comptes à privilèges. Les professionnels IT et sécurité devraient tirer parti de la situation pour accélérer l’adoption du MFA dans leur entreprise.

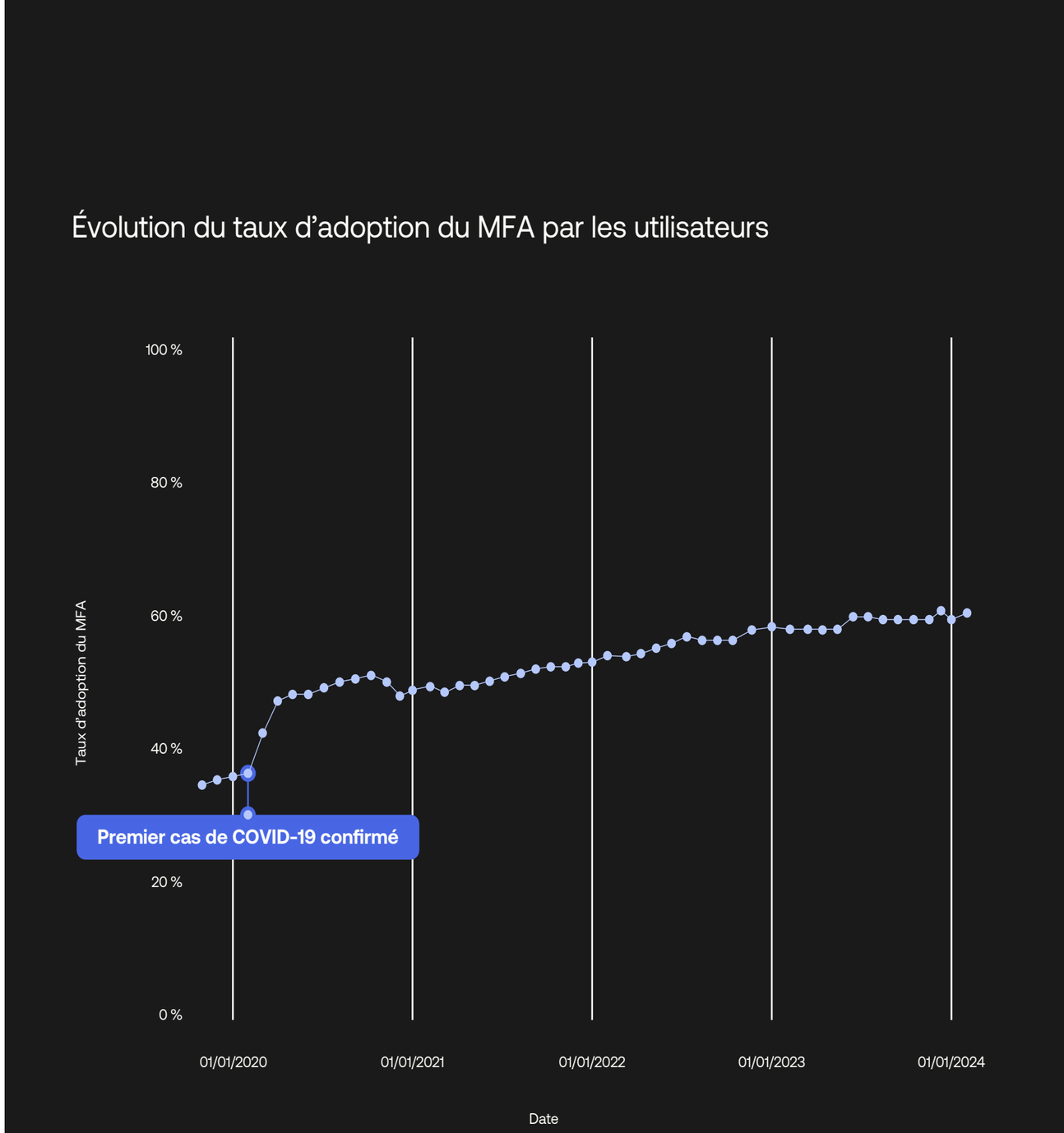

Figure 1. Taux d’adoption du MFA par les utilisateurs d’octobre 2019 à janvier 2024. Les données reflètent les cas d’usage relatifs aux collaborateurs en entreprise pour Okta Workforce Identity Cloud et n’incluent pas celles d’Okta Customer Identity Cloud (anciennement Auth0), ni les cas d’usage orientés clients de la plateforme Okta. Elles excluent également les données relatives aux clients Okta FedRAMP (Federal Risk and Authorization Management Program) High et DoD Impact Level 4.

Bilan de l’adoption du MFA

Adoption du MFA par région

Dans le rapport 2023, nous notions que l’adoption du MFA était relativement uniforme dans les différentes zones géographiques et que nous nous attendions à ce que cette tendance se maintienne en 2024. Les clients Okta sont plus enclins à appliquer le MFA aux utilisateurs que n’importe quel autre service concurrent, indépendamment de la région.

Nos données confirment cette position : les taux d’adoption varient en effet entre 61 % et 68 % pour les régions AMER (continent américain), APAC (Asie-Pacifique) et EMEA (Europe, Moyen-Orient et Afrique). Nous avons constaté une progression de 3 % des taux d’adoption dans les régions AMER et EMEA par rapport à 2023 et une diminution de 1 % pour l’APAC.

À noter

Nous pouvons dès lors en conclure que, dans les régions où Okta est présent, la situation géographique d’une entreprise et de ses utilisateurs ne représente pas un facteur déterminant dans l’adoption du MFA, au moins au niveau régional agrégé.

Taux d’adoption du MFA par les utilisateurs, par région

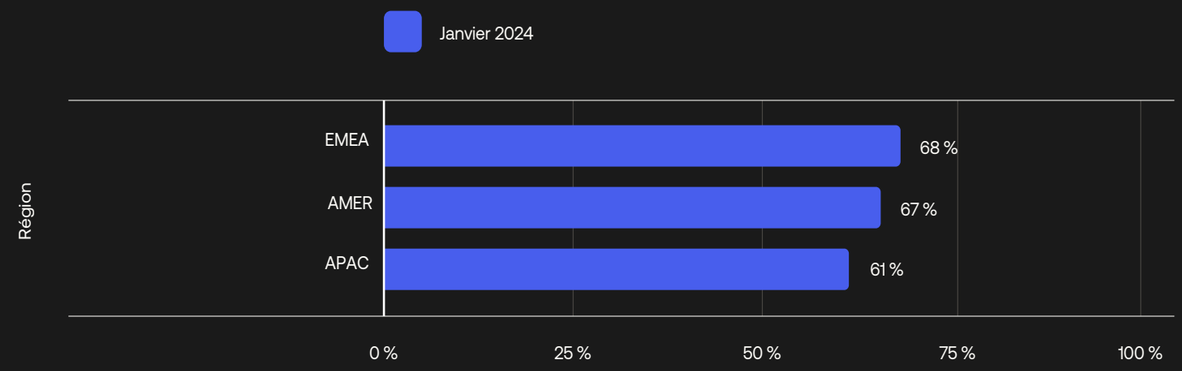

Figure 2. Taux d’adoption du MFA par les utilisateurs en Amérique du Nord, Amérique centrale et Amérique du Sud (AMER), en Asie-Pacifique (APAC) et en Europe, au Moyen-Orient et en Afrique (EMEA).

Bilan de l’adoption du MFA

Adoption du MFA par secteur

En 2024, nous continuons d’observer une grande variation de l’adoption du MFA par secteur, avec un écart allant jusqu’à 50 % entre le secteur au taux d’adoption le plus élevé (technologies) et celui au taux le plus faible (transport et entreposage). Comme c’est souvent le cas, le secteur des technologies joue un rôle de primo-adoptant et continue d’enregistrer le taux d’adoption du MFA le plus élevé (88 %) parmi les clients d’Okta Workforce Identity Cloud.

L’adoption du MFA a monté en puissance dans pratiquement tous les secteurs au cours de l’année dernière. Le secteur public (qui est passé de 48 % à 55 %)[2] et celui de l’enseignement (de 64 % à 69 %) ont enregistré une croissance de plus de 5 % en un an. Très réglementés, les deux secteurs ont commencé avec des taux d’adoption relativement bas, mais sont en train de combler leur retard, et nous pensons que les récents décrets-lois et amendements réglementaires aux États-Unis vont encore accentuer cette tendance. Par contre, nous avons observé une baisse de l’adoption du MFA dans le secteur des arts, divertissement et loisirs (de 57 % à 53 %) et dans celui des assurances (de 77 % à 71 %). Ces secteurs figurent parmi ceux qui misent sur l’expérience utilisateur pour se différencier lors de l’authentification de grands réseaux de partenaires commerciaux (comme les courtiers d’assurance, par exemple). Compte tenu des données sensibles auxquelles ces petites entreprises ont accès, nous estimons toutefois peu probable qu’à plus long terme, l’authentification par mot de passe seul ou par mot de passe avec un facteur supplémentaire de type SMS soit jugée suffisante par les organismes de réglementation. Ce rapport présente plusieurs méthodes possibles pour offrir une expérience utilisateur de grande qualité sans sacrifier la sécurité.

À noter

Nous tenions à souligner les progrès réalisés par le secteur public. Les entreprises qui proposent des services au secteur public ou un autre secteur fortement réglementé devraient au minimum implémenter le MFA pour les comptes à privilèges. Dans le rapport de 2023, le taux d’adoption du MFA pour les organismes publics était inférieur de plus de 16 % à celui du secteur privé. Cette année, il a progressé de 7 % pour s’élever à 55 %, soit l’un des plus grands bonds de l’année selon nos données. Avec l’entrée en vigueur des décrets-lois aux États-Unis[3] ainsi que l’appui de la CISA (Cybersecurity and Infrastructure Security Agency) au MFA et à l’authentification résistante au phishing, nous constatons actuellement de réels progrès dans le secteur public aux USA.

[2] Certains fonctionnaires utilisent une carte PIV (Personal Identity Verification) ou une autre carte à puce comme méthode d’authentification et se connectent à Okta via la fédération d’entreprise. Le taux d’adoption MFA de 55 % du secteur public ne tient pas compte de ce cas d’usage et peut sous-représenter le taux réel d’adoption du MFA de ce secteur. Okta a introduit la carte à puce comme type d’authentificateur natif en 2023. Nous recommandons aux clients du secteur public fédéral étasunien d’abandonner la fédération X.509 au profit des authentificateurs basés sur une carte à puce afin de profiter des fonctionnalités avancées telles que les politiques d’authentification au niveau de l’application et Okta Device Access.

[3] https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028

Taux d’adoption du MFA par les utilisateurs, par secteur

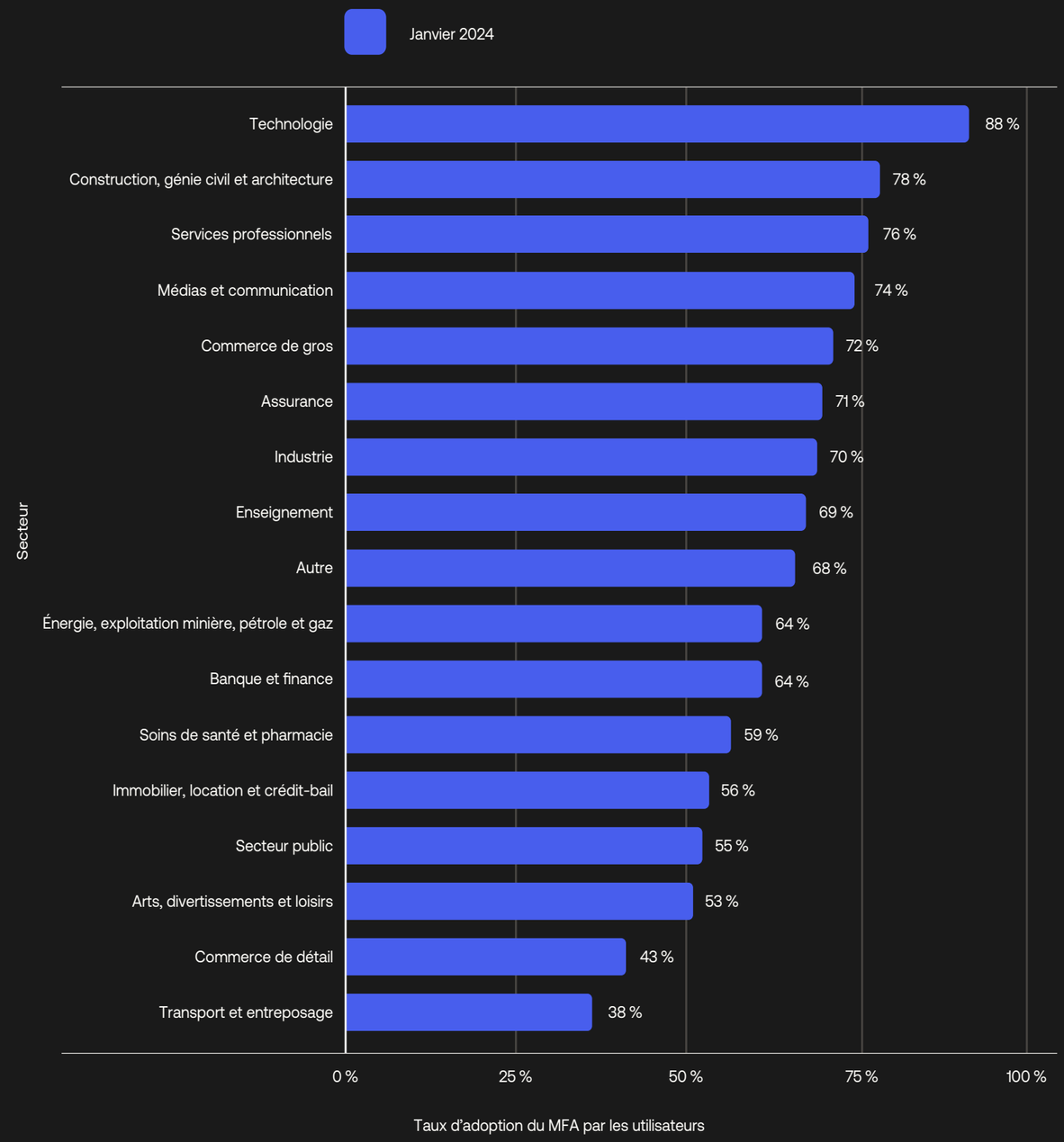

Figure 3. Taux d’adoption du MFA par les utilisateurs dans les différents secteurs, par ordre décroissant.

Bilan de l’adoption du MFA

Adoption du MFA par taille d’entreprise

Lorsque nous analysons l’adoption du MFA par taille d’entreprise, nous constatons une corrélation plus ou moins inverse entre le nombre de collaborateurs et le taux d’adoption du MFA : plus l’entreprise est grande, plus le taux d’adoption est faible. Les entreprises avec moins de 300 collaborateurs tendent à présenter le taux d’adoption le plus élevé (≥ 82 %), tandis que celles en comptant plus de 20 000 ont le taux le plus bas (59 %). En dépit de leur dernière place, ces grandes entreprises ont progressé plus que la moyenne (5 %) d’année en année.

Plusieurs facteurs peuvent contribuer à cet écart entre grandes et petites entreprises : à l’instar des organismes publics et des institutions financières, les organisations de grande envergure sont ralenties dans l’adoption de frameworks d’identité modernes par la complexité qu'implique le remplacement de l’infrastructure héritée. Les grandes entreprises sont également plus susceptibles d’utiliser plusieurs fournisseurs d’identité et de faire appel à des solutions MFA autres qu’Okta. (Notre rapport se concentre uniquement sur l’utilisation du MFA via la plateforme Okta.)

À noter

L’absence de vue centralisée de la gestion des identités et des accès (IAM) est problématique, quelle que soit la taille de l’entreprise. Les grandes entreprises, souvent plus préoccupées par les incidents de sécurité susceptibles d’éroder la confiance de leurs clients, devraient être plus motivées à étendre la couverture MFA.

Taux d’adoption du MFA par les utilisateurs, par taille d’entreprise

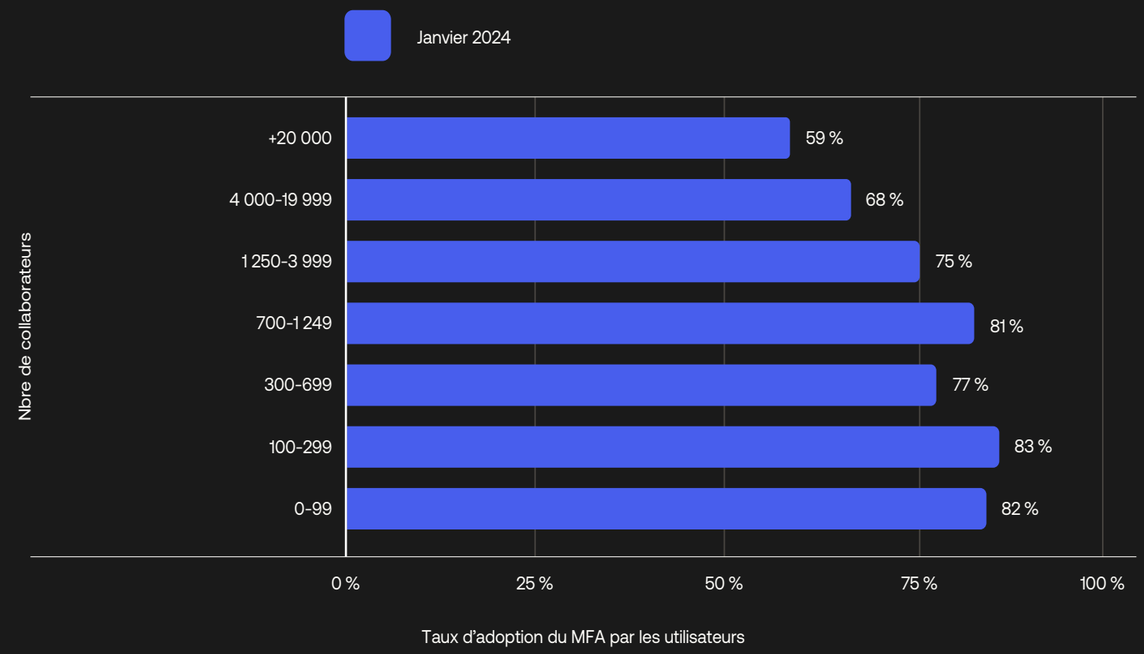

Figure 4. Taux d’adoption du MFA par les utilisateurs dans les entreprises de différentes tailles, par ordre croissant du nombre de collaborateurs.

Bilan de l’adoption du MFA

Adoption du MFA par type d’utilisateur

Dans le cadre de cette évaluation, nous définissons un « administrateur Okta » comme une personne possédant au moins un rôle administrateur dans une organisation Okta. Ce titre inclut de nombreux collaborateurs, du support IT aux équipes IAM et sécurité. Les chiffres relatifs à l’adoption du MFA sont très bons puisqu’ils atteignent 91 %, soit 1 % de plus que l’an dernier. Par ailleurs, les administrateurs ont tendance à faire figure de modèles en ce qui concerne l’utilisation du MFA résistant au phishing. Le taux d’adoption de FIDO2 WebAuthn parmi les utilisateurs disposant d’autorisations administrateur est passé de 8 % à 9 % au cours de l’année dernière, tandis que l’utilisation d’Okta FastPass chez ceux-ci a progressé de 5 % à 13 %.

En août 2024, dans le cadre de son engagement Okta Secure Identity Commitment, Okta a commencé à imposer aux clients de configurer le MFA pour l’accès aux consoles d’administration et de gestion des accès[4]. Avant le début de l’application du MFA pour la console d’administration WIC, nous avons constaté une adoption élevée, mais pas totale[5]. Notre objectif est de parvenir à une adoption complète en ciblant le reste des utilisateurs pourvus d’autorisations administrateur.

Afin de minimiser l’impact sur nos clients, cette mesure imposée est échelonnée en fonction de la complexité des flux de connexion existants. Certains administrateurs se connectent directement dans Okta WIC, alors que d’autres utilisent la fédération de fournisseurs d’identité (IdP) ou des intégrations avec un logiciel de gestion des accès à privilèges (PAM). Okta interdit désormais la création de politiques d’authentification à un seul facteur pour l’accès direct à la console d’administration Okta et a appliqué le MFA pour l’accès à la console pour 62 % des tenants Okta Workforce Identity Cloud existants.

Nous espérons qu’une fois que les utilisateurs à privilèges auront constaté à quel point il est facile de se connecter avec des authentificateurs sans mot de passe et résistants au phishing, l’adoption du MFA s’accélérera pour tous les utilisateurs.

À noter

La décision d’Okta d’appliquer le MFA pour l’accès aux applications d’administration peut être un catalyseur pour les équipes IT et sécurité, les incitant à revoir la stratégie d’authentification globale de leur entreprise. Nous encourageons nos clients à profiter de l’occasion pour réexaminer en profondeur les politiques de connexion pour toutes les consoles de gestion et autres applications critiques ou à haut risque.

La mise en place de politiques d’authentification spécifiques aux différentes applications peut faciliter ce déploiement en exigeant une authentification forte pour les applications critiques ou à haut risque, tout en permettant aux employés d’utiliser des formes d’authentification plus faibles pour les applications moins risquées. Une telle stratégie permet aux administrateurs d’améliorer la sécurité de l’entreprise sans impacter la cadence des activités.

[4] https://support.okta.com/help/s/blog/a674z000000147HAAQ/mfa-enforcement-for-the-admin-console?language=en_US

[5] Veuillez noter que le pourcentage d’administrateurs utilisant le MFA pour accéder à la console d’administration Okta est différent du taux d’adoption du MFA par les administrateurs. La première métrique examine uniquement l’accès à la console d’administration, tandis que la seconde analyse l’accès à n’importe quelle application. De plus, la première métrique impose aux administrateurs l’utilisation systématique du MFA pour accéder à la console d’administration, tandis que la seconde exige au moins une authentification MFA par mois.

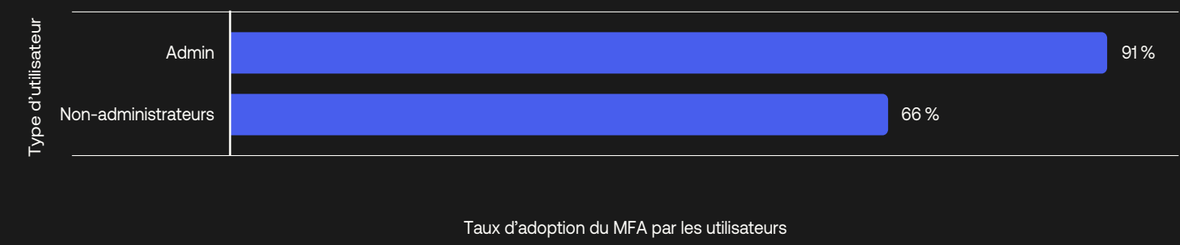

Figure 5. Taux d’adoption du MFA pour les administrateurs et les non-administrateurs.

Bilan de l’adoption du MFA

Adoption du MFA par type d’authentificateur

Au cœur de la conception de la plateforme, le caractère agnostique d’Okta Identity Cloud permet aux clients d’utiliser les technologies qui leur conviennent le mieux. Okta offre un large choix d’authentificateurs MFA propriétaires et tiers, adaptés à tous les cas d’usage. Selon les mécanismes d’authentification sous-jacents, les authentificateurs peuvent être classés en trois groupes : mots de passe, MFA traditionnel et MFA résistant au phishing.

Parmi les authentificateurs reposant sur le MFA traditionnel, citons l’e-mail, le token matériel, la notification push, la question de sécurité, le SMS et le token logiciel. Les authentificateurs MFA résistants au phishing incluent Okta FastPass, FIDO2 WebAuthn et les cartes à puce. Comme illustré dans le tableau 1, nous incluons autant d’offres fournisseurs que possible pour chaque type d’authentificateur. Toutefois, si les données relatives à l’authentification ne peuvent pas être distinguées par types d’authentificateur ou concernent des options personnalisées, nous les avons placées dans la catégorie « Autre » et les avons exclues de la suite de l’étude.

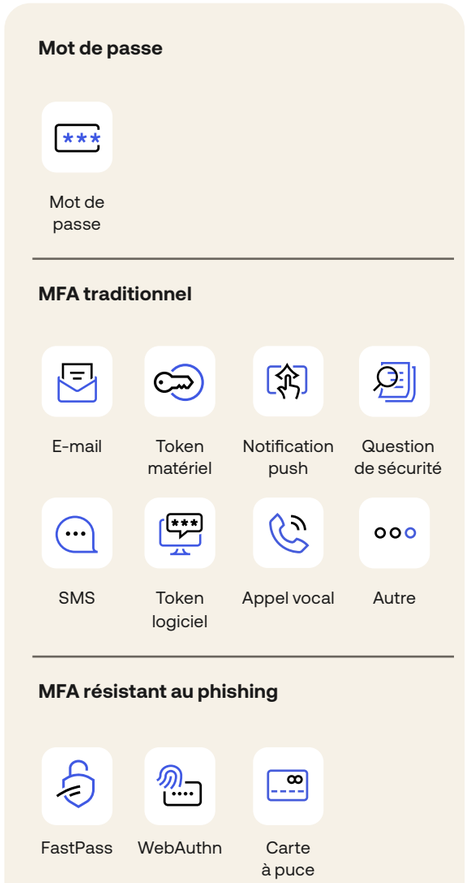

Tableau 1. Types et propriétés des authentificateurs

Le tableau recense les types d’authentificateurs utilisés pour analyser l’adoption du MFA, les propriétés de sécurité et de facilité d’utilisation, ainsi que les caractéristiques des principaux authentificateurs.

Type d’authentificateur	Authentificateurs pris en charge par Okta, utilisés pour l’analyse des propriétés des authentificateurs	Noms des authentificateurs : types, utilisés pour l’étude sur les propriétés de sécurité et de facilité d’utilisation	Type de facteur	Niveau d’assurance
Mot de passe	Mot de passe	Mot de passe	Connaissance	Faible
E-mail	Combinaison de lien et code e-mail (aussi appelé « magic link »)	Combinaison de lien et code e-mail	Possession	Faible
Token matériel	OTP YubiKey, RSA SecurId, TOTP (OTP à durée limitée) personnalisé	OTP YubiKey	Possession	Moyen
Notification push	Okta Verify Authenticator, notification push, authentificateur Duo	Notification push Okta Verify	Possession Possession + Biométrie	Moyen
Question de sécurité	Questions de sécurité	Questions de sécurité	Connaissance	Faible
SMS	SMS, authentificateur Duo	SMS	Possession	Faible
Token logiciel	OTP Okta Verify, Google Authenticator, RSA SecurId, TOTP personnalisé, authentificateur Duo	OTP Okta Verify, Google Authenticator	Possession	Faible
Appel vocal	Méthode d’authentification vocale par téléphone, authentificateur Duo	Méthode d’authentification vocale par téléphone	Possession	Faible
FastPass	Okta Verify Authenticator, méthode FastPass	Okta FastPass	Possession Possession + Biométrie	Élevé
WebAuthn	Authentificateurs WebAuthn (combinaison de Mac Touch ID, Android Fingerprint, Windows Hello, YubiKey, Google Titan, PassKey), authentificateur Duo	Authentificateurs WebAuthn (combinaison de Mac Touch ID, Android Fingerprint, Windows Hello, YubiKey, Google Titan, PassKey)	Possession Possession + Biométrie	Élevé
Carte à puce	Carte à puce	Combinaison des cartes PIV, CAC	Possession + Connaissance	Élevé

Il n'est pas surprenant de constater que les mots de passe continuent d'être utilisés par les collaborateurs dans l'environnement d'entreprise. Cela dit, nous observons également une augmentation de l'expérience passwordless, qui est passée de moins de 2 % en janvier 2023 à près de 5 % en janvier 2024. La notification push (29 %) est l'authentificateur par MFA le plus populaire, suivi du SMS (17 %) et du token logiciel (14 %).

Les taux d'adoption des authentificateurs par MFA traditionnel ont augmenté par rapport à l'année dernière, mais de peu (+1,3 % au total). Nous avons observé une très faible croissance du taux d'adoption du MFA par SMS (+1,2 %) sur les trois dernières années en dépit de l'augmentation de 14 % du taux global d'adoption du MFA au cours de la même période. Par contre, l'adoption des authentificateurs résistants au phishing a fortement augmenté. Par exemple, le taux d'adoption de WebAuthn a progressé, de 2 % d'utilisateurs en 2023 à 3 % en 2024 ; de même, celui d'Okta FastPass est passé de 2 % à 6 % pour la même période.

Trois facteurs critiques contribuent à l'adoption en hausse des authentificateurs résistants au phishing. Le premier est la menace grandissante posée par le phishing. Par exemple, l'équipe sécurité Okta a observé que le nombre d'entreprises dont l'identité a été usurpée a bondi de 50 % entre février 2023 et janvier 2024 par rapport à la même période de l'année précédente. Pareillement, à l'analyse des données recueillies par ses solutions de sécurité réseau, Zscaler a constaté une augmentation de 58 % des attaques de phishing l'an dernier[6].

Le second facteur est la disponibilité des options résistantes au phishing. Okta prend en charge un large choix d'authentificateurs résistants au phishing, par exemple Okta FastPass et FIDO2 WebAuthn. La simplification de l'accès à ces technologies a un impact direct sur l'adoption. Okta a intégré FastPass, méthode de connexion sans mot de passe et résistante au phishing, à Okta Verify. Tous les clients peuvent en profiter dans le cadre de la mise à niveau gratuite vers Okta Identity Engine. Nous avons relevé que 7 % des tenants OIE (nouveaux ou migrés) qui ont effectué la mise à niveau vers OIE entre février 2023 et janvier 2024 ont essayé FastPass dans les 90 premiers jours.

En troisième lieu, la conformité réglementaire devrait également contribuer à l'adoption de facteurs résistants au phishing. Les administrations publiques australiennes, par exemple, doivent employer des méthodes d'authentification résistantes au phishing pour parvenir aux niveaux de maturité 2 et 3 des contrôles prévus dans le framework Essential Eight du pays.

À noter

Le moteur OIE offre davantage de flexibilité dans la gestion des flux de connexion, notamment grâce aux politiques de connexion aux applications qui permettent aux administrateurs de configurer des règles individuelles pour accéder aux applications et de proposer aux utilisateurs un authentificateur sans mot de passe et résistant au phishing dans Okta FastPass. Nous conseillons aux clients Okta d'évaluer et d'implémenter des authentificateurs plus forts pour maximiser les avantages offerts aux utilisateurs, et pas seulement pour la commodité des administrateurs. Par exemple, il est connu que l'authentification par SMS offre un niveau d'assurance faible, est vulnérable aux attaques d'échange de carte SIM et présente un coût supérieur à d'autres méthodes. Pour améliorer les résultats, les équipes IT et sécurité devraient toutes deux participer à la mise à niveau pour en tirer rapidement le plein potentiel et évaluer la meilleure stratégie d'authentification pour l'entreprise.

[6] https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report

Taux d'adoption du MFA par les utilisateurs, par authentificateur

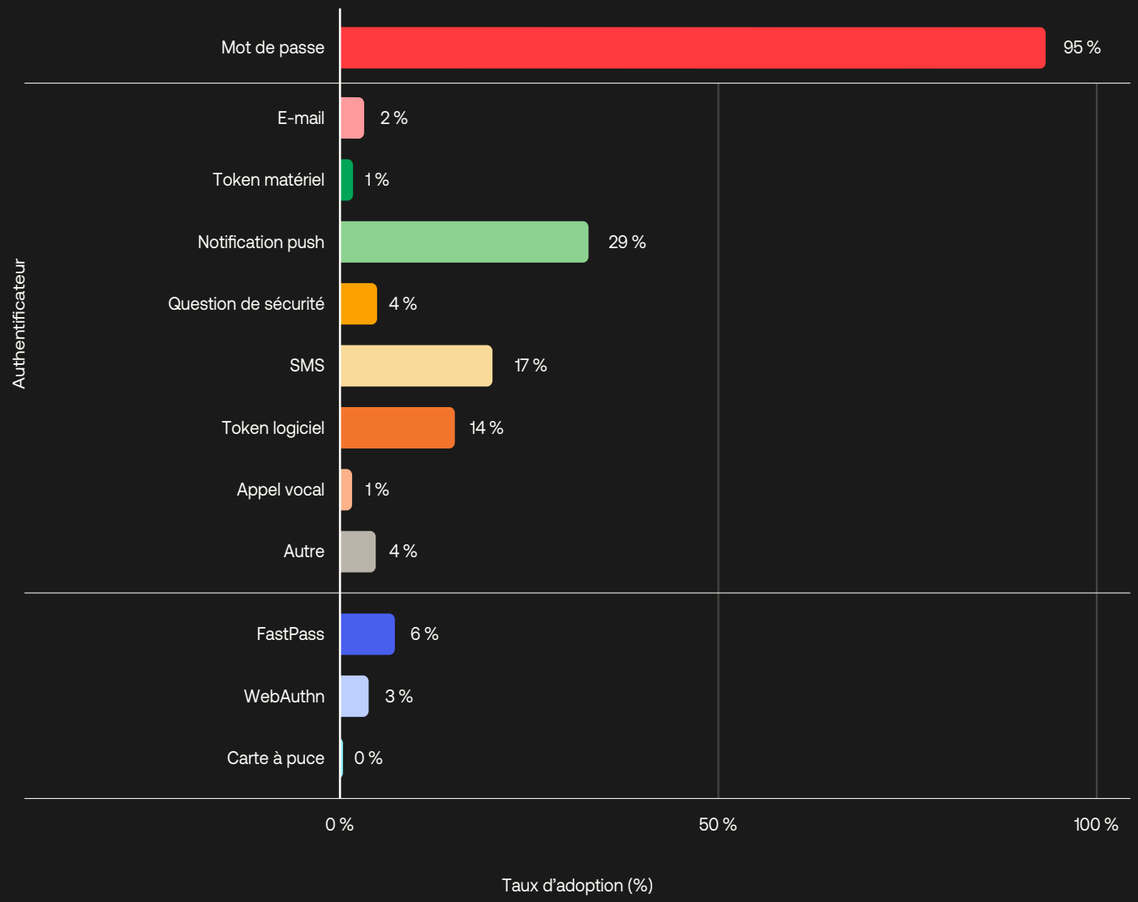

Figure 6. Taux d'adoption du MFA par les utilisateurs, pour les authentificateurs proposés par Okta Workforce Identity Cloud. La somme du taux d'adoption pour chaque authentificateur est supérieure au taux d'adoption du MFA, étant donné que les utilisateurs peuvent s'authentifier avec plusieurs authentificateurs.

Évaluation axée sur les données de la sécurité et de la facilité d'utilisation des authentificateurs

Si l'adoption du MFA progresse, il reste encore quelques obstacles à surmonter. Pour aider les DSI, RSI et autres décideurs à prendre des décisions plus avisées sur les authentificateurs à adopter, il est préférable de comprendre les avantages et inconvénients de chacun d'eux.

À cette fin, nous avons mis au point un framework pour évaluer ces authentificateurs, tant du point de vue de la sécurité que de la facilité d'utilisation. Les catégories d'évaluation sont indiquées dans le tableau 2. Les résultats nous donnent des informations axées sur les données qui pourront aider les responsables IT et sécurité à mieux protéger leurs entreprises et à guider le développement produits.

Si vous avez lu l'édition 2023 du rapport « The Secure Sign-In Trends Report », cette section vous semblera très familière. Pour l'édition 2024, nous avons actualisé les métriques, mais les changements sont mineurs : le temps nécessaire pour saisir un mot de passe ou recevoir un code e-mail reste assez constant. Toutefois, le nombre d'utilisateurs et d'événements inclus dans l'étude de cette année a augmenté étant donné que les entreprises sont plus nombreuses à avoir migré vers OIE. De plus, la méthodologie a été optimisée grâce aux contributions des professionnels IT et sécurité Okta pour déterminer la pondération des métriques. En dépit des critères révisés et plus pratiques, les avantages conférés par l'utilisation d'un authentificateur résistant au phishing restent identiques. Enfin, l'étude inclut aussi les données relatives aux métriques de l'authentification par carte à puce. Selon nous, les informations de cette enquête peuvent s'avérer utiles pour l'évaluation des méthodes d'authentification modernes telles que FastPass ou WebAuthn.

Propriétés de sécurité et de facilité d'utilisation des authentificateurs

Durée de la demande d'authentification

Deux approches d'analyse des mots de passe

Nous avons inclus les durées des demandes d'authentification par mot de passe selon deux configurations possibles de l'interface utilisateur :

- **Dans le flux de noms d'utilisateur/mots de passe**, un utilisateur est invité à compléter le champ du nom d'utilisateur et celui du mot de passe sur la même page à la connexion.
- **Dans le flux de mots de passe uniquement**, un utilisateur indique son nom d'utilisateur dans une page et est invité à saisir son mot de passe dans la suivante.

La durée médiane de la demande d'authentification par mot de passe dans le deuxième scénario (saisie du mot de passe uniquement) est plus adaptée à la comparaison, car les autres authentificateurs MFA n'exigent pas d'identification du compte avant la demande. Les deux flux sont toutefois représentés dans le graphique.

La durée de la demande d'authentification mesure le temps médian nécessaire pour répondre correctement à l'invite d'un authentificateur.

Les durées médianes des demandes sont constantes d'une année à l'autre pour les authentificateurs. La durée médiane de demande d'authentification par mot de passe reste d'environ 6 secondes. Nous estimons que ce délai tend à être plus court si l'utilisateur fait appel à un gestionnaire de mots de passe et à la fonction de saisie automatique des navigateurs. Pour les flux d'authentification qui commencent par les mots de passe, la saisie d'un mot de passe à usage unique (OTP) ajoute au moins 12 secondes au flux d'authentification si l'utilisateur doit récupérer ce dernier dans un e-mail ou un appel vocal.

Nos données indiquent que les authentificateurs alliant possession et inhérence (notamment via la biométrie) offrent les délais d'authentification les plus rapides (4 secondes). FIDO2 WebAuthn, Okta FastPass (comme son nom l'indique) et les cartes à puce offrent un processus d'authentification utilisateur bien plus efficace que n'importe quel autre authentificateur. Compte tenu de cette vitesse, ces authentificateurs permettent aussi aux entreprises d'envisager une réauthentification à une fréquence plus élevée ou en tant que mesure d'authentification renforcée pour l'accès aux applications sensibles. Les deux constituent une défense essentielle contre le détournement de session.

À noter

Si l'accès à une application professionnelle exige deux facteurs distincts (exigence minimum pour le niveau d'assurance AAL2 du NIST), les meilleures options envisageables en termes d'expérience utilisateur (au vu de la durée de la demande d'authentification) doivent inclure FIDO2 WebAuthn ou Okta FastPass, qui offrent par ailleurs le meilleur niveau de sécurité (résistance au phishing).

Ces authentificateurs offrent généralement un facteur de possession et un facteur d'inhérence en moins de 4 secondes, ce qui est nettement plus rapide que la combinaison des mots de passe et des demandes d'authentification OTP.

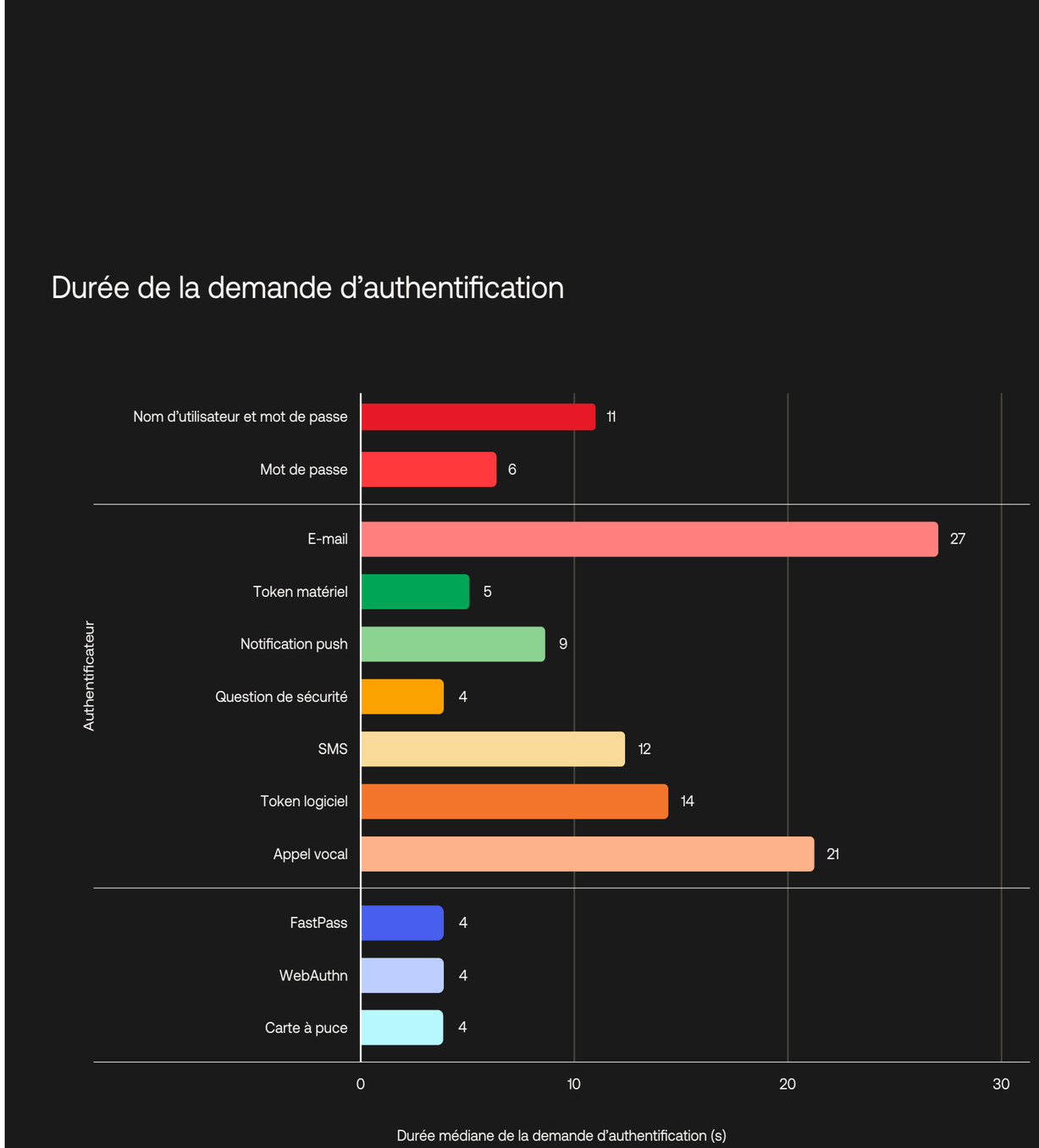

Figure 7. Durées médianes de la demande d'authentification pour les authentificateurs considérés : mot de passe (flux avec nom d'utilisateur/mot de passe et avec mot de passe uniquement), e-mail, token matériel, notification push, question de sécurité, SMS, token logiciel, appel vocal, FastPass, WebAuthn et carte à puce.

“Une simple authentification MFA ne suffit plus pour se protéger des acteurs malveillants. Avec Okta FastPass, il est facile d’optimiser la sécurité et de bénéficier non seulement d’un MFA résistant au phishing, mais aussi d’informations contextuelles sur la posture des terminaux. Il est possible de réduire considérablement l’éventail de sources d’attaque possibles en implémentant la résistance au phishing et en limitant l’accès aux applications sensibles aux seuls terminaux gérés. Grâce aux contrôles du niveau d’assurance, nous pouvons également faire en sorte que ces terminaux disposent des correctifs nécessaires et que les contrôles prévus soient appliqués au moment de l’accès.

Toutefois, il ne s’agit pas ici de renforcer continuellement la sécurité. Si des contrôles plus stricts dégradent l’expérience utilisateur, l’approche devient contre-productive. C’est pourquoi nous avons également implémenté le passwordless. Grâce à la résistance au phishing, à l’emploi de terminaux gérés, à la vérification des utilisateurs par biométrie et à la posture de sécurité des terminaux, nous pouvons bénéficier au minimum du niveau d’assurance AAL2, tout en améliorant en même temps l’expérience de nos utilisateurs finaux au quotidien.”

Andrew Meinert
Director of System Operations

HubSpot

Propriétés de sécurité et de facilité d'utilisation des authentificateurs

Durée d'inscription aux authentificateurs

La durée d'inscription aux authentificateurs est mesurée comme étant le délai médian nécessaire à un utilisateur pour s'inscrire à un authentificateur, à partir du moment où la page d'inscription s'affiche jusqu'au moment où il termine l'inscription après avoir suivi les instructions données.

L'inscription à un authentificateur, la réinitialisation et la récupération de mots de passe donnent temporairement lieu des périodes de risque plus élevé. Pour chaque inscription ou réinitialisation, les administrateurs peuvent (et devraient) appliquer des règles imposant aux authentificateurs d'initier et de vérifier l'identité de l'utilisateur. Nous recommandons de configurer à cette fin des authentificateurs résistants au phishing.

La durée médiane de création d'un mot de passe avoisine les 35 secondes, ce qui inclut le temps nécessaire pour créer un nouveau mot de passe, le confirmer (c'est-à-dire le saisir à nouveau) et décider de se déconnecter ou non d'autres terminaux authentifiés. La durée d'inscription médiane la plus longue (40 secondes) est celle associée à la question de sécurité. En effet, celle-ci exige que les utilisateurs sélectionnent ou créent les questions de sécurité et saisissent ensuite les réponses.

Le flux d'inscription des authentificateurs d'Okta est conçu de telle sorte qu'Okta Verify OTP, Okta Verify Push et Okta FastPass puissent être inscrits ensemble à l'aide de l'application Okta Verify. Étant donné que plusieurs types d'authentificateurs sont inscrits en même temps, la durée médiane est d'environ 38 secondes, en ce compris le temps nécessaire à un utilisateur pour scanner un code QR et terminer le processus de configuration d'Okta Verify. L'OTP matériel, l'appel vocal, le SMS et FIDO2 WebAuthn présentent les durées d'inscription les plus courtes, moins de 25 secondes. L'inscription des cartes à puce implique la vérification hors ligne des utilisateurs, la fabrication d'une carte à puce et son expédition. Il faut parfois plusieurs semaines pour obtenir une nouvelle carte à puce. La plateforme de gestion des identités Okta n'a aucune visibilité sur ce processus.

À noter

Étonnamment, nous avons constaté une légère augmentation des durées d'inscription depuis 2023. Comme l'inscription est un processus manuel, plusieurs facteurs techniques et humains peuvent y avoir contribué.

Les entreprises se tournent de plus en plus vers des processus d'inscription automatisés pour remédier au problème. Par exemple, en avril 2024, Okta a annoncé la signature d'un partenariat avec YubiKey qui permet aux administrateurs de livrer directement des YubiKeys pré-inscrites au domicile des collaborateurs. L'expérience utilisateur est alors limitée au temps qu'il faut pour insérer la clé et taper le code initial, ce qui permet aux collaborateurs d'être presque immédiatement opérationnels.

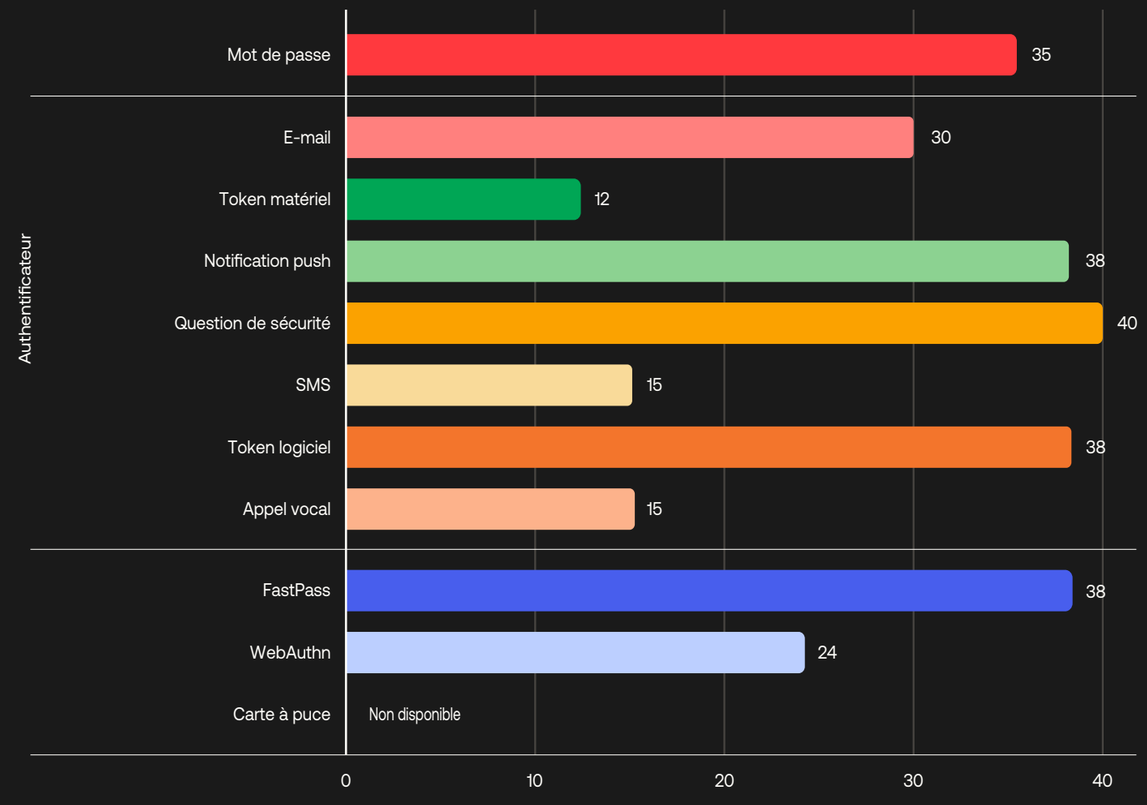

Figure 8. Durées médianes d'inscription pour les authentificateurs considérés : mot de passe, e-mail, token matériel, notification push, question de sécurité, SMS, token logiciel, appel vocal, FastPass, WebAuthn et carte à puce. Le temps de vérification utilisateur a été exclu de l'analyse, car il est déterminé par les politiques d'inscription et de récupération plutôt que par l'authentificateur lui-même.

Propriétés de sécurité et de facilité d'utilisation des authentificateurs

Taux d'échec des demandes d'authentification

Le taux d'échec des demandes d'authentification mesure le nombre de tentatives d'authentification ayant échoué, divisé par le nombre total des tentatives d'authentification reçues par les serveurs backend d'Okta à l'aide d'un authentificateur donné.

Les échecs d'authentification sont plus fréquents qu'on ne le penserait. L'utilisateur peut, par exemple, taper un mot de passe erroné ou une réponse incorrecte à une question de sécurité, saisir un OTP non valide, ignorer une demande push ou fournir une signature incorrecte en réponse à une demande d'authentification d'un authentificateur biométrique tel que FastPass ou FIDO2 WebAuthn.

Le taux d'échec des demandes d'authentification est à la fois une métrique de sécurité et de facilité d'utilisation, puisqu'un échec d'authentification peut être d'origine malveillante ou non. Pour les tentatives non malveillantes, un taux d'échec plus élevé signifie que les utilisateurs sont plus susceptibles de commettre des erreurs avec un authentificateur donné pendant l'authentification, ce qui ralentit leur productivité. En ce qui concerne les tentatives d'authentification suspectes, un taux d'échec plus élevé indique généralement que les cybercriminels considèrent ces méthodes comme une cible plus facile. Malheureusement, distinguer les événements anodins des tentatives malveillants exige des connaissances plus approfondies des tendances d'utilisation qui ne sont pas disponibles dans les données anonymisées dont nous disposons pour ce rapport. Votre équipe sécurité peut être en mesure de générer ce type de rapport pour votre environnement.

Nos données révèlent que les authentificateurs basés sur la connaissance sont plus fastidieux à utiliser pour les utilisateurs, suivis des diverses formes de mot de passe à usage unique (OTP). C'est le mot de passe qui présente le taux d'échec le plus élevé (près de 10 %), suivi par les tokens logiciels, les demandes d'authentification envoyées par e-mail et les questions de sécurité.

L'authentification FIDO2 WebAuthn et par carte à puce limite assez logiquement les erreurs utilisateurs accidentelles (erreurs de saisie) et les tentatives suspectes, ce qui diminue les taux d'échec. Cependant, ces résultats doivent être considérés avec prudence. L'implémentation de WebAuthn et des cartes à puce diffère quelque peu des autres méthodes d'authentification. De par sa conception, le processus d'authentification de ces méthodes intervient sur le système de l'utilisateur. Le fournisseur d'identité (Okta) ne peut donc pas capturer tous les échecs pour ces authentificateurs. Par exemple, si un utilisateur emploie FIDO2 WebAuthn pour tenter de se connecter à un proxy de phishing et que l'authentificateur détecte une non-concordance de domaines, il n'existe aucun mécanisme permettant d'envoyer ces informations aux serveurs backend du fournisseur d'identité. Il est alors impossible pour l'administrateur de générer un rapport précis sur le nombre de tentatives d'authentification malveillantes.

À noter

Même en tenant compte de la mise en garde concernant le taux d'échec de WebAuthn, nous constatons une fois encore que les formes d'authentification résistantes au phishing offrent la meilleure expérience utilisateur.

Taux d'échec des demandes d'authentification

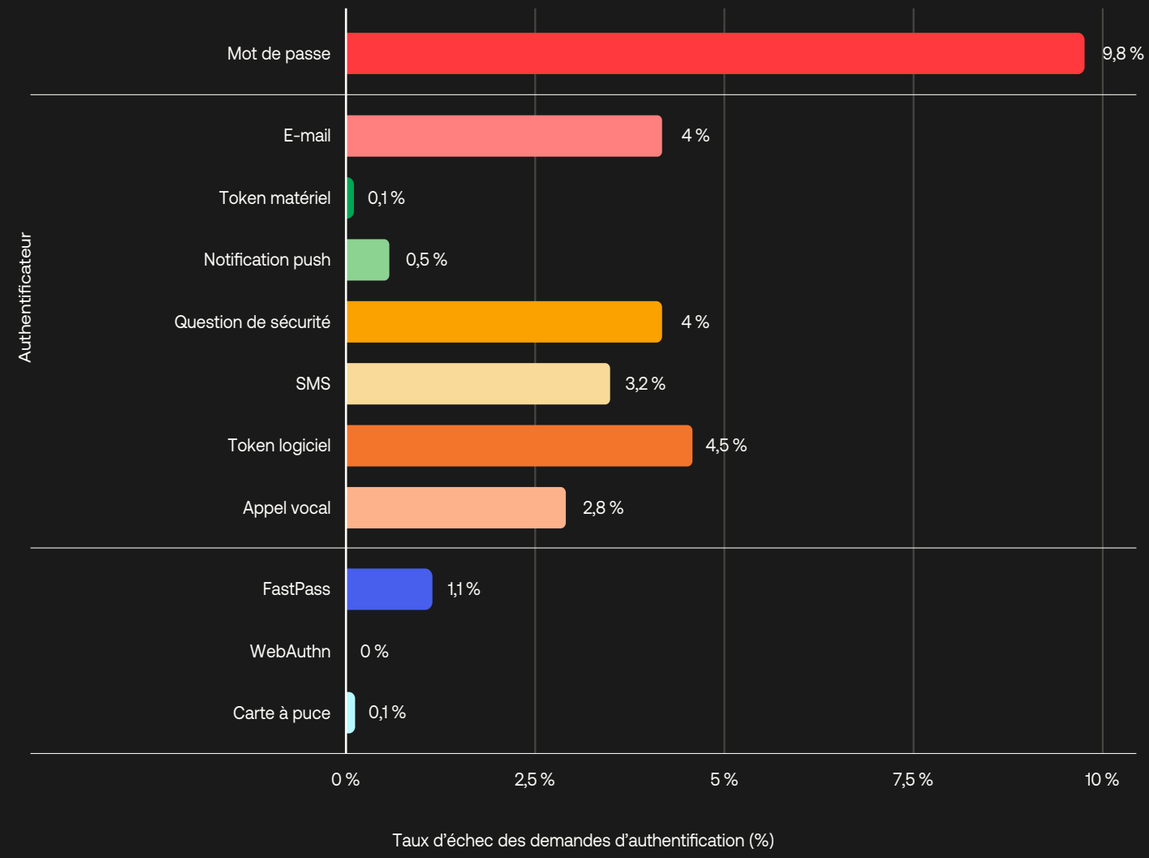

Figure 9. Taux d'échec pour les authentificateurs considérés : mot de passe, e-mail, token matériel, notification push, question de sécurité, SMS, token logiciel, appel vocal, FastPass, WebAuthn et carte à puce.

Propriétés de sécurité et de facilité d'utilisation des authentificateurs

Couverture de la résistance au phishing

La couverture de la résistance au phishing décrit le pourcentage potentiel d'utilisateurs protégés par un authentificateur répondant à la définition de la résistance au phishing donnée par le NIST.

Si un authentificateur n'est pas résistant au phishing, sa couverture de résistance au phishing correspond à zéro. Un authentificateur résistant au phishing a une couverture égale au pourcentage d'utilisateurs dont les navigateurs et systèmes d'exploitation prennent en charge ces fonctionnalités. Sur base de ces critères, trois authentificateurs ont une couverture de résistance au phishing supérieure à zéro : Okta FastPass, FIDO WebAuthn et les cartes à puce.

FIDO 2 WebAuthn permet aux sites web de mettre à jour leurs pages de connexion en ajoutant une authentification FIDO résistante au phishing aux navigateurs et plateformes pris en charge. D'après caniuse.com, 96 % des terminaux peuvent utiliser WebAuthn avec leurs navigateurs et plateformes. Toutefois, la couverture de résistance au phishing de WebAuthn relevée ici indique la limite supérieure des authentificateurs WebAuthn. Ainsi, il se peut que certains authentificateurs WebAuthn ne prennent en charge que des plateformes bien précises ; dans ce cas, leur couverture de résistance au phishing pourrait être nettement inférieure au taux optimal représenté dans le graphique.

Okta FastPass est également efficace pour se protéger contre les attaques par phishing d'identifiants. Pour ce faire, il vérifie l'URL d'origine pour chaque tentative d'authentification. FastPass offre cette résistance au phishing sur les plateformes Windows, macOS, Android et iOS. Dans un contexte professionnel, si nous partons du même éventail de navigateurs et plateformes que celui indiqué sur le site caniuse.com, environ 95 % des utilisateurs peuvent avoir accès à la fonctionnalité résistante au phishing FastPass.

À noter

WebAuthn et FastPass offrent tous deux une résistance au phishing. Habituellement, les implémentations WebAuthn sont des identifiants d'un seul appareil sous la forme d'authentificateurs itinérants, tels que des clés de sécurité physiques, ou d'authentificateurs de plateforme, par exemple FaceID et Windows Hello. L'année dernière, FIDO et les principaux fournisseurs de systèmes d'exploitation ont introduit les passkeys multi-terminaux comme identifiants WebAuthn que les utilisateurs peuvent synchroniser sur différents terminaux.

Si toutes les implémentations WebAuthn sont résistantes au phishing, elles ne sont pas toutes identiques. Ces incohérences entre Windows, MacOS, iOS et Android, par exemple, peuvent entraîner une certaine confusion et donc une expérience utilisateur de piètre qualité. L'introduction des passkeys multi-terminaux représente un pas en avant important pour les cas d'usage liés à l'authentification des clients, mais peut être problématique dans un contexte professionnel, où la possibilité de déplacer une clé d'authentification entre les terminaux peut constituer une violation de la politique de l'entreprise. De plus, certains éditeurs de systèmes d'exploitation ont récemment arrêté la prise en charge d'une authentification WebAuthn liée au terminal en faveur des passkeys multi-terminaux, qui rendent l'expérience utilisateur contre-intuitive[7].

FastPass est également adapté aux cas d'usage et aux modèles de sécurité destinés aux collaborateurs en entreprise, en fournissant par exemple des contrôles renforcés de la liaison des terminaux et du niveau d'assurance du terminal. Par ailleurs, il offre une interface cohérente sur toutes les plateformes (desktops/mobiles), ce qui encourage les utilisateurs à employer les méthodes d'authentification disponibles les plus fortes.

Comme les cartes à puce exigent du matériel spécialisé, le déploiement de cette technologie est généralement limité aux secteurs très réglementés qui peuvent se permettre une infrastructure IT homogène.

[7] https://passkeys.dev/device-support/

Couverture de la résistance au phishing, par authentificateur

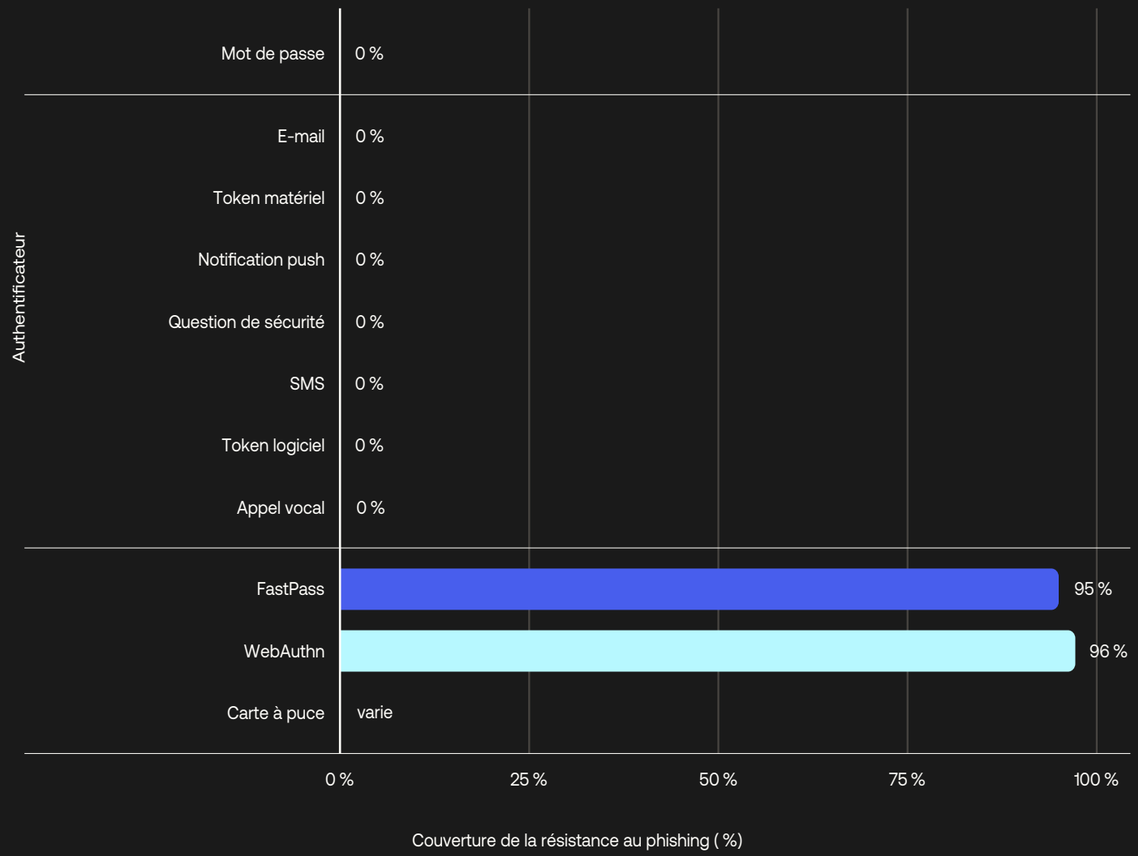

Figure 10. Couverture de la résistance au phishing pour les authentificateurs considérés : mot de passe, e-mail, token matériel, notification push, question de sécurité, SMS, token logiciel, appel vocal, FastPass, WebAuthn et carte à puce.

Propriétés de sécurité et de facilité d'utilisation des authentificateurs

Couverture des alertes associées à la résistance au phishing

La couverture des alertes associées à la résistance au phishing correspond au pourcentage d'utilisateurs potentiellement protégés par un authentificateur capable de consigner les demandes dont les vérifications de l'origine ont échoué, ce qui est un indicateur courant des attaques Adversary-in-the-middle (AiTM).

Aujourd'hui, Okta FastPass est le seul authentificateur capable de créer des événements côté serveur lorsqu'une tentative de phishing entraîne un échec de la vérification de l'origine. En cas de détection d'une non-concordance de cookies ou d'un nom de domaine liée à un site de phishing, FastPass rejette la demande et avertit l'utilisateur final et les administrateurs. Il sensibilise également les utilisateurs et l'entreprise aux menaces, améliorant ainsi leur capacité à détecter et à répondre aux activités malveillantes.

Une catastrophe évitée grâce à FastPass

L'étude de cas ci-dessous relate l'expérience d'un client Okta ayant procédé à une mise à niveau vers OIE et déployé FastPass au début de l'année 2023.

En juillet 2024, en cours de soirée, l'un des collaborateurs a reçu un appel téléphonique relevant d'une vaste campagne de social engineering qui visait des centaines d'entreprises. Le correspondant, qui parlait avec un accent américain et appelait depuis un numéro de téléphone usurpé correspondant à un des numéros de l'entreprise, s'est présenté comme un membre de l'équipe IT et a demandé au collaborateur de se connecter à un site web frauduleux, très similaire à un nom de domaine de la société. L'utilisateur avait configuré Okta FastPass. FastPass a rejeté la tentative de connexion car le domaine et le certificat ne correspondaient pas à l'organisation Okta du client. Au cours des minutes qui ont suivi, le cybercriminel a convaincu l'utilisateur de tenter de se reconnecter à plusieurs reprises via le site de phishing, mais FastPass a rejeté toutes les tentatives. L'équipe sécurité, déjà avertie de ces tentatives de social engineering par d'autres utilisateurs, a pu rapidement visualiser ces échecs dans le journal système et répondre à l'attaque, jusqu'à révoquer temporairement l'accès de l'utilisateur pris pour cible. Le lendemain matin, ce dernier a pu récupérer son accès et reprendre le travail.

L'investigation qui a suivi a révélé que FastPass et sa fonction d'alerte ont évité au client d'être victime d'une usurpation de compte (ATO) par l'acteur malveillant et ont permis de limiter l'impact sur la productivité des collaborateurs.

Il est intéressant de noter que FastPass n'est pas uniquement un authentificateur selon la définition classique du terme. Il est également capable de collecter les informations contextuelles du terminal, par exemple son état de gestion, la version du système d'exploitation, le verrouillage, le chiffrement de disque et la détection du débridage/accès root. FastPass s'intègre par ailleurs avec des solutions UEM (Unified Endpoint Management) et EDR (Endpoint Detection and Response) telles que Jamf, Microsoft Intune, Workspace One, CrowdStrike, Windows Security Center, et Chrome Device Trust[8] pour s'assurer qu'un terminal qui s'authentifie est géré ou possède le niveau de sécurité approprié. Ces informations contextuelles peuvent encore renforcer la détection des menaces et améliorer l'application des politiques d'authentification.

À noter

Nous estimons que la capacité à donner l'alerte en cas de détection de campagnes de social engineering et de phishing AiTM va revêtir une importance critique, dans la mesure où la vitesse de détection et de réponse deviendra un facteur de différenciation clé dans la lutte contre les cyberattaques. L'utilisation de la fonctionnalité d'alerte d'Okta FastPass permet aux entreprises de bénéficier d'une détection et d'une protection en temps réel contre le phishing.

[8] https://support.okta.com/resource/device_context_deployment_guide

Couverture des alertes associées à la résistance au phishing, par authentificateur

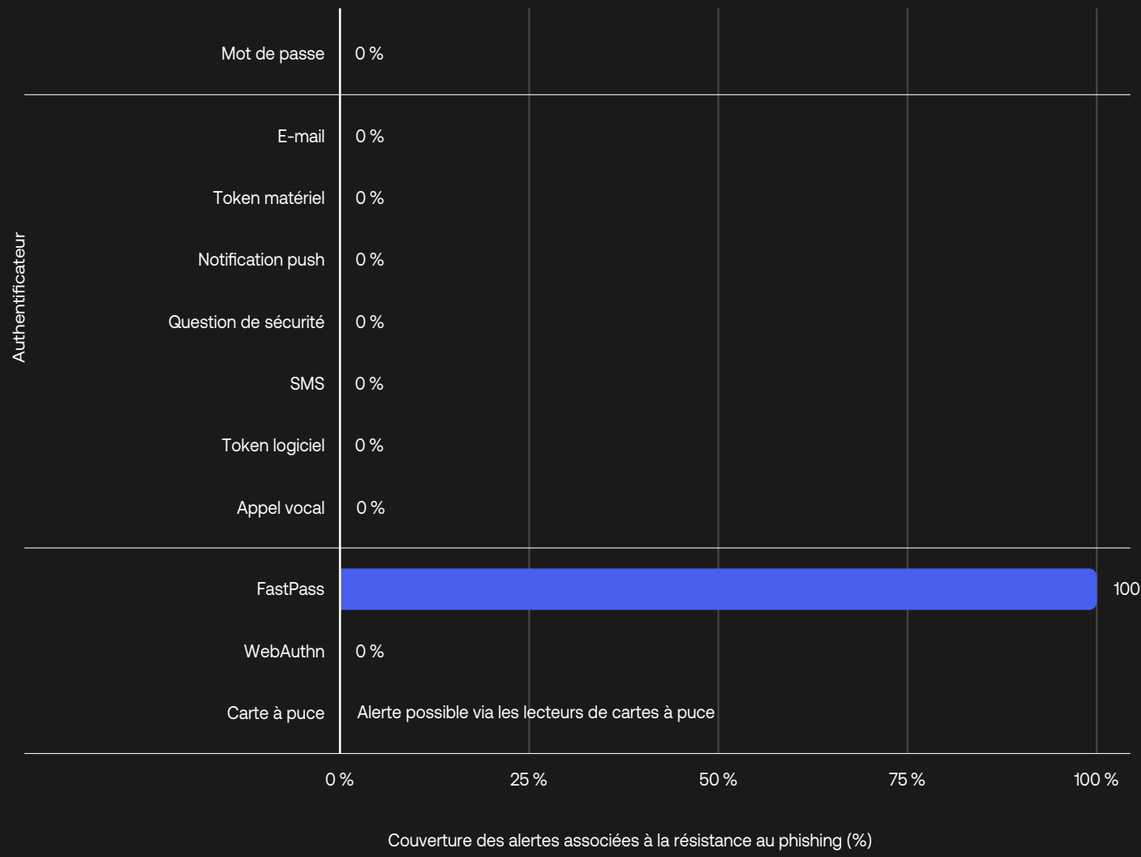

Figure 11. Couverture des alertes associées à la résistance au phishing pour les authentificateurs considérés : mot de passe, e-mail, token matériel, notification push, question de sécurité, SMS, token logiciel, appel vocal, FastPass, WebAuthn et carte à puce.

Propriétés de sécurité et de facilité d'utilisation des authentificateurs

Taux d'échec des attaques par force brute

Le taux d'échec des attaques par force brute décrit le pourcentage d'utilisateurs présentant plus de N vérifications par un authentificateur qui ont échoué, exprimé comme un pourcentage des utilisateurs s'étant connectés à l'aide de l'authentificateur.

Un échec d'attaque par force brute se produit lorsqu'un utilisateur malveillant ou légitime ne réussit pas à s'authentifier plus de N fois, N étant le seuil utilisé pour définir un possible échec d'attaque par force brute. Pour ce rapport, nous avons utilisé N=10 dans l'analyse, étant donné qu'il serait hautement improbable qu'un utilisateur légitime tente de s'authentifier autant de fois. Comme les cybercriminels peuvent automatiser la découverte d'un mot de passe ou d'un OTP, ou générer des demandes d'authentification à répétition dans l'espoir de tromper ou forcer un utilisateur à approuver l'accès, un échec d'attaque par force brute reflète également les préférences de l'adversaire à mener des attaques par force brute contre un authentificateur donné.

Comme dans le rapport 2023, ce sont les secrets basés sur la connaissance qui continuent d'être le plus ciblés par les outils automatisés des attaquants ou créent le plus de friction pour les utilisateurs légitimes qui poursuivent leurs tentatives de connexion en dépit de plusieurs échecs. FIDO2 WebAuthn affiche le taux d'échec des attaques par force brute le plus faible, mais comme précédemment, ces résultats doivent être considérés avec circonspection : en raison de l'implémentation du standard, il est possible que tous les échecs ne soient pas rapportés à Okta, ce qui donne un score artificiellement faible.

FastPass ne fonctionne pas de la même manière que les autres authentificateurs et possède deux modèles d'interrogation. L'interrogation silencieuse, ou authentification silencieuse, permet au widget d'authentification Okta de vérifier automatiquement si FastPass est configuré sur le terminal et peut être utilisé pour authentifier un utilisateur sans interaction de sa part. L'interrogation interactive, ou authentification standard, repose sur un modèle de fonctionnement plus classique et se déclenche lorsqu'un utilisateur se connecte à l'aide d'un authentificateur FastPass. L'authentification silencieuse s'exécute en arrière-plan, procédant à de nombreuses vérifications des terminaux et des utilisateurs, sans friction supplémentaire pour ces derniers. Par conséquent, la demande d'authentification FastPass est plus fréquente que les autres types d'authentificateurs, ce qui explique probablement la valeur relativement élevée du taux d'échec des attaques par force brute associé à FastPass.

À noter

Même si les tentatives de contournement du MFA ont tendance à augmenter, les attaques par force brute traditionnelles continuent de se concentrer en priorité sur les authentificateurs basés sur la connaissance. L'utilisation d'authentificateurs basés sur un facteur biométrique ou de possession peut considérablement réduire la probabilité d'une usurpation de compte (ATO) résultant d'une attaque par force brute.

Taux d'échec des attaques par force brute, par authentificateur

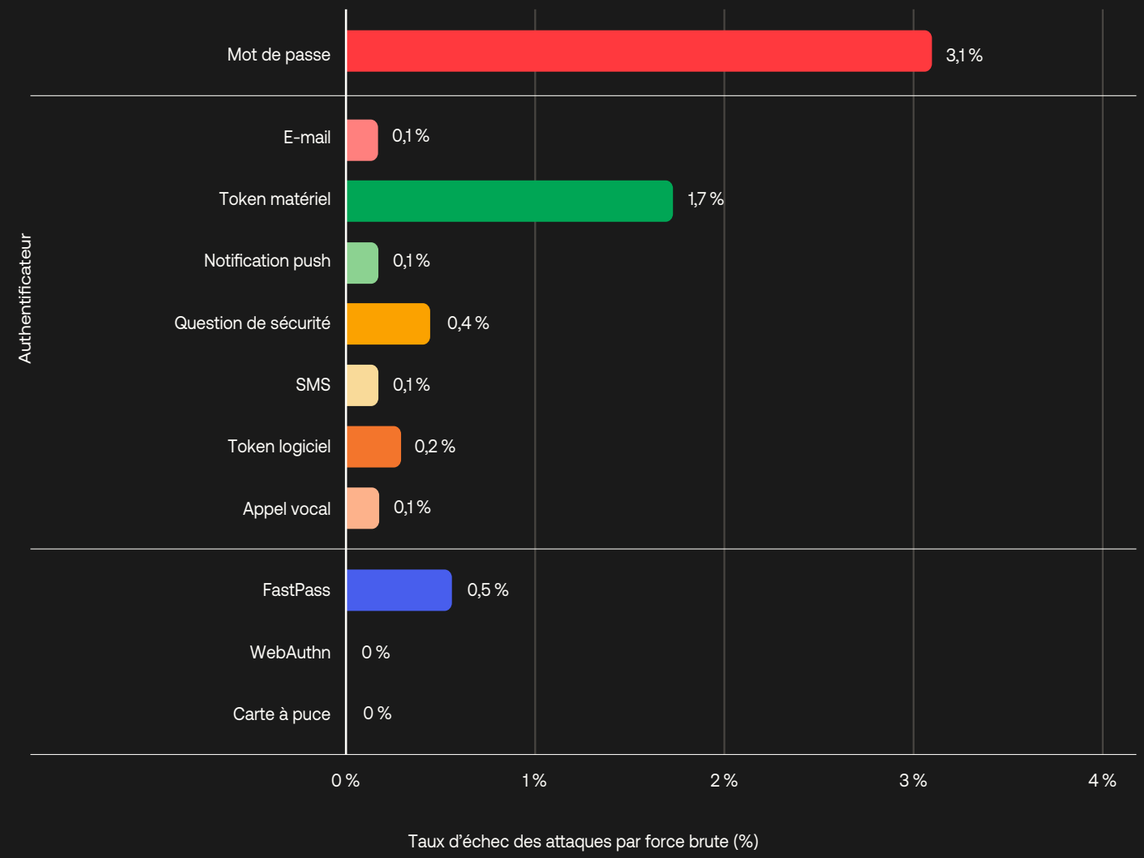

Figure 12. Taux d'échec des attaques par force brute pour les authentificateurs considérés : mot de passe, e-mail, token matériel, notification push, question de sécurité, SMS, token logiciel, appel vocal, FastPass et WebAuthn. Les données ont été recueillies entre novembre 2023 et janvier 2024.

Propriétés de sécurité et de facilité d'utilisation des authentificateurs

Enquête sur les métriques liées aux authentificateurs

Dans le rapport de l'année dernière, nous avons utilisé la pondération des métriques pour décrire l'importance relative des métriques associées aux divers authentificateurs. Ces pondérations sont basées sur notre connaissance interne des propriétés des authentificateurs et la fréquence à laquelle les clients y font référence.

Après la publication du rapport 2023, nous avons cherché à développer une méthode de pondération plus pratique. Nous avons décidé de mener une enquête auprès de professionnels IT et sécurité pour comprendre l'importance relative de chacune des métriques de sécurité et de facilité d'utilisation d'un authentificateur donné. Les résultats de cette enquête nous permettent d'aligner les données collectées dans nos logs sur l'importance que nos administrateurs accordent à ces métriques, comme illustré dans le tableau 2, et non les estimations utilisées précédemment.

En rassemblant toutes ces informations, nous avons pu utiliser les résultats de l'enquête pour calculer et représenter les scores de sécurité et de facilité d'utilisation des authentificateurs. Dans un premier temps, nous avons pris les scores maximum et minimum dans chaque catégorie pour normaliser les métriques pour chaque authentificateur dans une plage de 0 à 1. Par exemple, WebAuthn obtient un score de taux d'échec en réponse aux demandes d'authentification de 1, tandis que le mot de passe obtient un score de 0. Ensuite, nous avons pondéré ces scores en fonction de leur impact sur la sécurité et la facilité d'utilisation des authentificateurs en nous basant sur les résultats de l'enquête. Cela nous permet de représenter les scores de sécurité et de facilité d'utilisation des authentificateurs dans des conditions et avec des priorités réelles. Découvrez les performances de votre authentificateur favori par rapport aux autres.

À noter

Pour renforcer votre infrastructure de sécurité, il est impératif d'obtenir l'alignement et l'engagement complets des parties prenantes IT et sécurité. L'enquête sur les métriques liées aux authentificateurs peut être un moyen efficace d'obtenir un consensus sur les principaux risques et considérations à envisager dans le choix des méthodes d'authentification.

Tableau 2. Catégories d'évaluation de la sécurité et de la facilité d'utilisation des authentificateurs

Adoption		Facilité d'utilisation		Sécurité	
Métrique	**Pondération**	**Métrique**	**Pondération**	**Métrique**	**Pondération**
Taux d'adoption au niveau des utilisateurs	Non disponible	Durée de la demande d'authentification	7,33/10	Taux d'échec des demandes d'authentification	5,71/10
		Durée de l'inscription	5,14/10	Taux d'échec des attaques par force brute	7,14/10
		Taux d'échec des demandes d'authentification	6,25/10	Couverture de la résistance au phishing	8,65/10
				Couverture des alertes associées à la résistance au phishing	7,47/10
Scores d'adoption des authentificateurs		**Scores de facilité d'utilisation des authentificateurs**		**Scores de sécurité des authentificateurs**	

“Demander aux utilisateurs de multiplier et de mémoriser des mots de passe forts et uniques est une approche dépassée et vouée à l’échec. Le gros avantage des options MFA sans mot de passe est qu’elles sont à la fois plus pratiques et plus sûres. C’est très rare.

Les avantages en matière de sécurité ne comptent que s’ils accélèrent le développement de l’activité et offrent des possibilités de croissance. Le passwordless y contribue indéniablement. Les facteurs MFA qui excluent les mots de passe sont plus rapides et plus simples. De plus, ils réduisent les coûts et ouvrent la porte à davantage de partenariats d’intégration.”

Shana Uhlmann
Directrice IT et RSSI

Tattarang

Propriétés de sécurité et de facilité d'utilisation des authentificateurs

Évaluation des performances et de l'adoption des authentificateurs

Les authentificateurs résistants au phishing offrent une meilleure expérience utilisateur

Quel rôle peuvent jouer toutes ces observations dans le choix d'authentificateurs d'une entreprise et comment les responsables IT et sécurité peuvent-ils favoriser l'adoption d'authentificateurs conviviaux et sécurisés ?

Dans le domaine de la sécurité de l'information, on part souvent du principe que les décideurs technologiques doivent faire des compromis de sécurité pour préserver l'expérience utilisateur.

Notre analyse montre qu'il n'en est rien. Bien que l'étude ne cherche pas à interroger les utilisateurs sur leurs préférences, les données brutes concernant l'authentification suggèrent que l'authentification résistante au phishing offre une expérience utilisateur de meilleure qualité. Avec FastPass ou FIDO2 WebAuthn, les utilisateurs renforcent la sécurité des comptes sans sacrifier la qualité de leur expérience.

À noter

L'implémentation du MFA et du passwordless à grande échelle est plus un défi culturel que technique. Les entreprises ont besoin de choix et de flexibilité. La plateforme de gestion des identités Okta offre un large éventail d'options pour répondre aux besoins uniques de votre entreprise. Vous pouvez implémenter la méthode et le framework qui vous conviennent le mieux. Nous espérons que l'approche que nous avons adoptée pour définir la pondération relative des propriétés des authentificateurs et pour aligner ces métriques sur les principales parties prenantes vous incitera à réfléchir à de nouvelles façons de promouvoir une authentification plus forte dans votre entreprise.

Figure 7. Durée de la demande d'authentification

Performances et adoption des authentificateurs

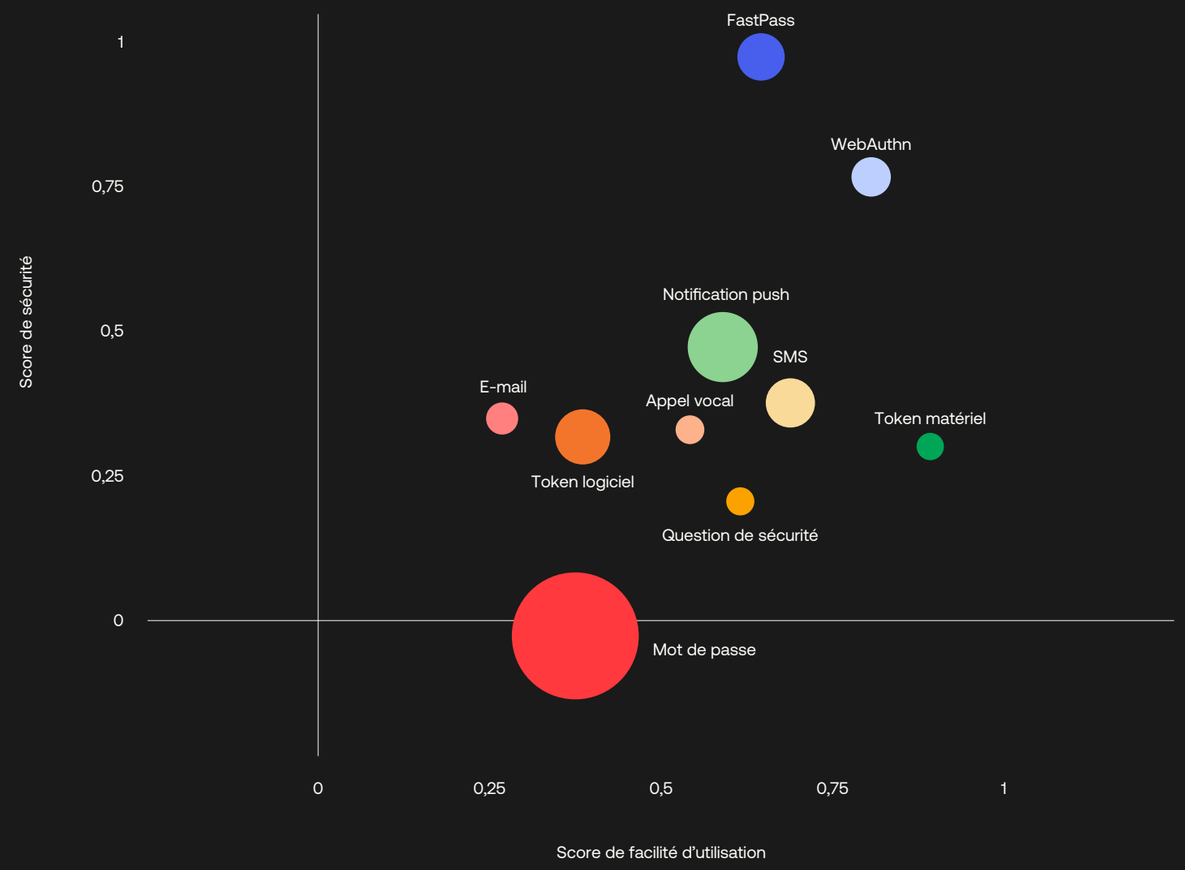

Figure 13. Performances et adoption des authentificateurs considérés : mot de passe, e-mail, token matériel, notification push, question de sécurité, SMS, token logiciel, appel vocal, FastPass et WebAuthn. Les performances de chaque authentificateur sont représentées par ses scores de sécurité et de facilité d'utilisation, comme illustré dans la matrice 2x2. La taille du cercle reflète le taux d'adoption de l'authentificateur sur une échelle de 0 à 100 %.

La voie à suivre

Si l'on considère le succès rencontré par les cybercriminels au cours des 12 derniers mois grâce à des techniques de social engineering et de phishing, on pourrait espérer un taux plus élevé d'adoption de méthodes d'authentification résistantes au phishing. Au cours des mois qui ont suivi la collecte de ces données, un certain nombre d'incidents de sécurité très médiatisés ont quelque peu forcé la main aux entreprises du secteur. Salesforce, GitHub, Okta et Microsoft sont tous déterminés à imposer le déploiement du MFA pour une partie de leurs utilisateurs. L'adoption de FastPass s'accélère chez les clients Okta, et les préoccupations quant aux menaces de phishing favorisées par les progrès de l'IA font l'objet d'une attention soutenue, tant dans les médias qu'au sein des conseils d'administration. L'optimisme est donc de mise.

Le MFA résistant au phishing est sûr, convivial et réalisable. Tout le monde y tire avantage, des administrateurs aux utilisateurs. C'est une technologie capitale pour se protéger contre des menaces omniprésentes et nous devons aider nos entreprises à l'adopter plus largement. Nous espérons que ce rapport vous sera utile dans vos échanges avec vos dirigeants et utilisateurs en faveur d'une authentification plus simple et plus forte, en vous permettant de comparer la position de votre entreprise par rapport à celle de vos pairs.

Besoin de conseils plus personnalisés ? Contactez-nous. Nous sommes là pour vous aider à protéger votre entreprise et à simplifier la vie de vos utilisateurs.

5 conseils pour améliorer votre stratégie d'authentification

Même si l'adoption d'une stratégie d'authentification plus robuste peut sembler difficile de prime abord, les entreprises peuvent prendre des mesures relativement simples pour commencer.

1. Exigez le MFA dans les politiques de connexion et appliquez la résistance au phishing pour l'accès administrateur aux applications et données sensibles. Nous recommandons vivement de tirer parti des propriétés de résistance au phishing et des fonctionnalités Device Assurance offertes par Okta FastPass, notre authentificateur sans mot de passe.
2. Faites de l'adoption du MFA une priorité de l'équipe de direction. Compte tenu de son efficacité démontrée à sécuriser les ressources et informations les plus précieuses de l'entreprise, le taux d'adoption du MFA doit être visible aux plus hauts niveaux de l'entreprise.
3. Adoptez une approche Zero Trust en matière d'accès, ce dernier étant octroyé en fonction des propriétés d'identité par session individuelle et selon le principe du moindre privilège, et déterminé conformément aux niveaux d'assurance requis pour les applications ou données demandées.
4. Créez des politiques d'accès dynamiques qui évaluent les attributs utilisateurs, le contexte lié au terminal (terminal connu, géré ou à la sécurité renforcée), les attributs réseau (réseau fiable ou non) et qui déterminent si la demande est conforme aux comportements précédents de l'utilisateur.
5. Formulez un plan à plus long terme pour limiter ou éliminer l'utilisation des mots de passe.

Méthodologie

Pour créer ce rapport, nous nous sommes appuyés sur les données d'Okta Workforce Identity Cloud. Nous avons anonymisé et agrégé les données de milliards d'authentifications et de vérifications aux quatre coins du monde. Nos clients et leurs collaborateurs, prestataires, partenaires ainsi que leurs propres clients utilisent Okta pour se connecter en toute sécurité aux terminaux, sites web, applications et services, tout en tirant parti des fonctionnalités de sécurité pour protéger leurs données. Nos clients sont issus d'un large éventail de secteurs, qu'il s'agisse de PME ou de grandes entreprises mondiales.

La taille d'entreprise des clients est définie par le nombre de collaborateurs à plein temps de l'entreprise. La taxinomie des secteurs d'activité correspond à celle du système NAICS (North American Industry Classification System). La taille d'entreprise, le secteur et la région géographique sont validés à l'aide de ressources tierces.

Sauf indication contraire, ce rapport se concentre exclusivement sur les données d'Okta Workforce Identity Cloud et sur les cas d'usage relatifs aux collaborateurs en entreprise. Il n'inclut aucune donnée d'Okta Customer Identity Cloud.

À propos d'Okta

Spécialiste mondial de l'identité, Okta permet à chacun d'utiliser en toute sécurité n'importe quelle technologie, partout, sur n'importe quel terminal ou application. Les plus grandes marques font confiance à Okta en ce qui concerne l'accès sécurisé, l'authentification et l'automatisation. De par leur flexibilité et neutralité, les solutions Okta Workforce Identity Cloud et Customer Identity Cloud offrent aux dirigeants d'entreprises et aux développeurs la possibilité de se concentrer sur l'innovation et d'accélérer leur transformation digitale, grâce à des solutions personnalisables et plus de 7 000 préintégrations. Nous construisons un monde où l'identité vous appartient. Pour en savoir plus, consultez notre site à l'adresse www.okta.com/fr.

Clause de non-responsabilité

Le présent document et toute recommandation concernant vos pratiques de sécurité ne constituent pas des conseils juridiques, commerciaux ou de sécurité. Le contenu de ce document revêt un caractère purement informatif et pourrait ne pas refléter les normes de sécurité et les réglementations les plus récentes, ou tous les problèmes juridiques ou de sécurité pertinents. Pour obtenir de tels conseils, il vous revient de vous adresser à votre conseiller juridique ou à tout autre conseiller professionnel et de ne pas vous en remettre aux recommandations formulées dans le présent document. Okta décline toute responsabilité quant aux pertes ou dommages pouvant résulter de la mise en œuvre des recommandations fournies dans le présent document.

okta

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie – France
+33 01 85 64 08 80