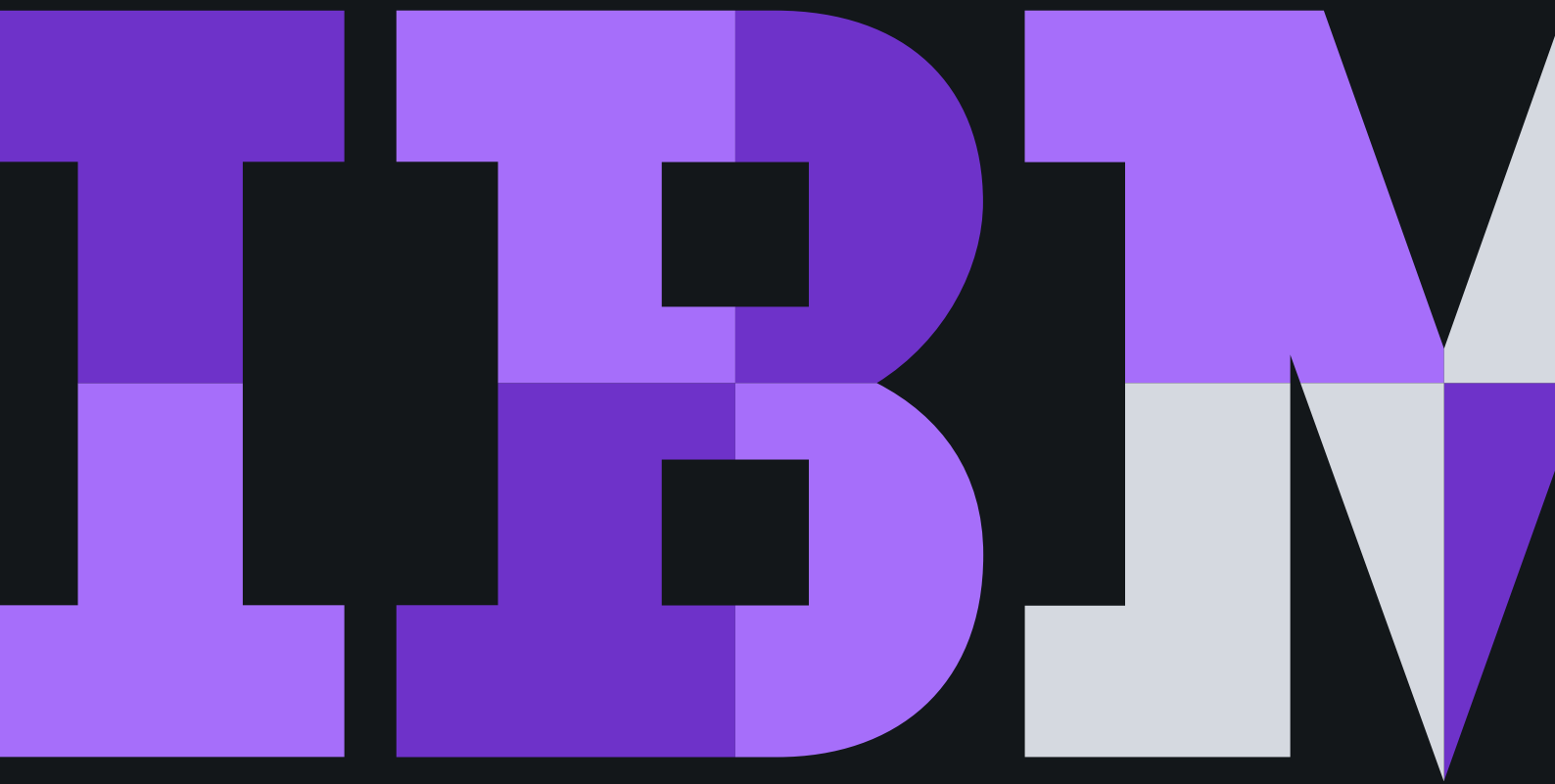
Septembre 2019

Authentifiez en toute transparence les identités numériques des consommateurs et des employés

Transformez votre programme d'IAM avec l'identité sous forme de service



IBM

Sommaire

Validation des identités de l'utilisateur

« La sécurisation des identités en ligne » est une expression que l'on entend très souvent dans de nombreux secteurs d'activité. La plupart des entreprises mettent en œuvre des mesures de grande ampleur pour valider les identités des utilisateurs et protéger leurs ressources critiques contre les attaques. En revanche, les violations et les agressions continuent de constituer une menace.

Les violations des identités numériques sont l'une des raisons principales des pertes des données des consommateurs : pertes d'informations personnelles, pertes financières, pertes de données internes de l'entreprise, telles que l'accès aux enregistrements et aux contrôles internes. Le coût moyen d'une violation de données est de $3,92 millions, et sa portée moyenne est d'environ 25 575 enregistrements.[1] Les entreprises subissant une violation de données ne perdent pas seulement des données, mais aussi la confiance du public. A la suite d'une violation de sécurité, les consommateurs considèrent souvent les entreprises impactées comme non fiables, avec pour conséquences des pertes de clientèle et de contrats.

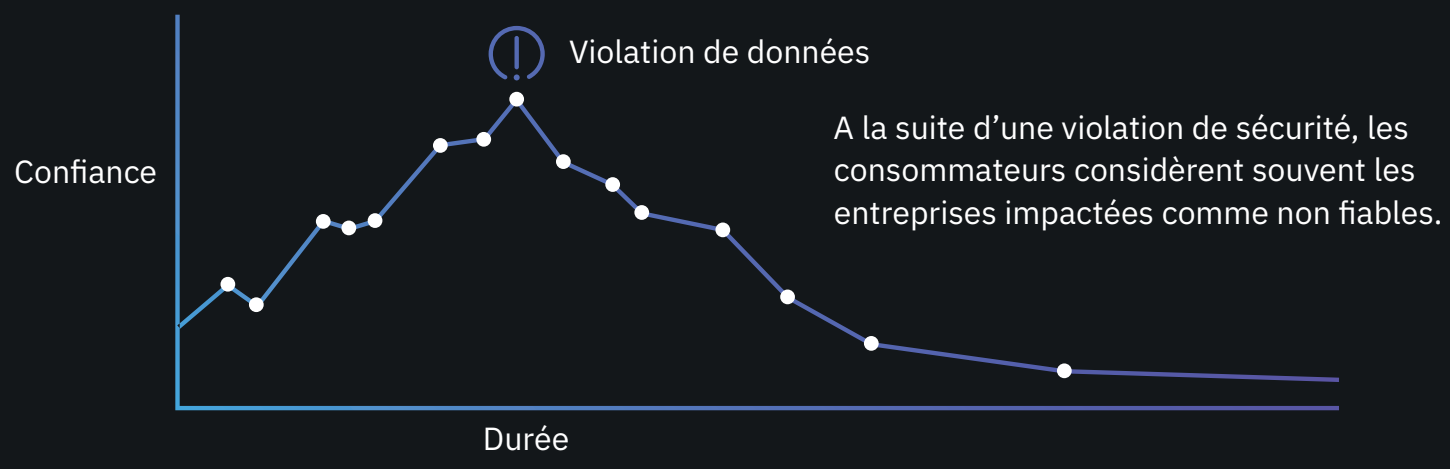
Alors que les entreprises sont de plus en plus nombreuses à migrer vers le cloud, la recherche de mesures de sécurité permettant d'autoriser et d'authentifier les utilisateurs internes et externes sans impact négatif sur le parcours utilisateurs se poursuit.

L'identité sous forme de service devrait connaître un taux de croissance annuel composite de 14,1% au cours des cinq prochaines années, le nombre d'entreprises cherchant à engranger les avantages du cloud computing se multipliant. [2] L'objectif des entreprises est de mettre en œuvre une validation à la fois fluide et simple des identités des consommateurs et des employés.

L'IDaaS est-elle forcément complexe ?

Connectez partout les utilisateurs et les appareils cloud, mobiles et sur site aux applications métier. Découvrez la puissance de l'IDaaS (identité sous forme de service) dans cette courte vidéo.

Voir la vidéo



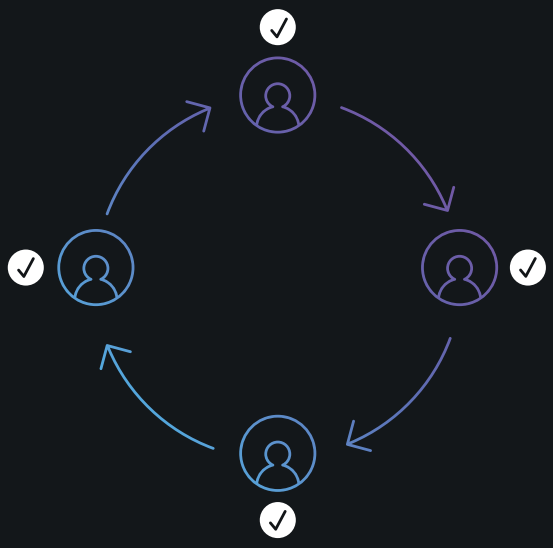
La fluidité, en toute simplicité

Les entreprises doivent aujourd'hui relever de nombreux défis liés à la gestion des identités et des accès. Un grand nombre de ces défis proviennent de la nécessité de recourir à des processus sécurisés qui offrent en même temps une expérience fluide. Pour fournir ces expériences, les entreprises doivent :

Confirmer les identités des clients et des employés
Les entreprises doivent confirmer et autoriser de façon parfaitement fluide toutes les interactions des utilisateurs et garantir une authentification continue pendant tout le parcours utilisateur.

Surveiller les événements d'authentification
L'identification des comportements suspects reste un défi. Pour reconnaître un utilisateur frauduleux, les entreprises doivent avoir des informations sur toutes les activités des utilisateurs. Elles doivent aussi pouvoir surveiller et identifier les comportements inhabituels.

Garantir la sécurité dans toutes les plateformes numériques
L'utilisation en hausse de la mobilité contraint à renforcer la protection d'appareils de plus en plus nombreux dans les applications, dans l'IoT et dans la gestion des appareils mobiles. Ce changement nécessite une mise en application et une protection fluides des identités numériques.



Les entreprises doivent pouvoir confirmer et autoriser de façon parfaitement fluide toutes les interactions des utilisateurs et garantir une authentification continue pendant tout le parcours utilisateur.

Avec IBM Cloud™ Identity, les administrateurs peuvent facilement suivre l'utilisation des applications, les problèmes de performance et les activités de connexion. Découvrez le tableau de bord de l'administrateur dans cette vidéo de 3 minutes.

Voir la vidéo

Les mots de passe sans efforts

Sécuriser l'identité numérique d'un utilisateur, qu'il soit un employé, un partenaire ou un client, est un défi pour les entreprises. **Les clients, en particulier, veulent avoir la certitude que leur identité numérique est protégée lorsqu'ils utilisent une application, mais ils veulent aussi une expérience conviviale et sans difficultés.**

Mesures de sécurité complexes

La sécurité est essentielle pour que les clients puissent faire confiance à une entreprise. En revanche, les utilisateurs ne veulent pas avoir à gérer des mesures de sécurité complexes. Ils estiment que la partie concernant la sécurité des applications doit s'exécuter en arrière-plan et ne doit pas les gêner.

Suivi de nombreux noms d'utilisateurs et mots de passe

Les clients sont contraints de mémoriser une multitude de noms d'utilisateurs et de mots de passe dans chaque application utilisée. Chaque application exigeant des données d'identification différentes est perçue comme un obstacle par l'utilisateur.

Comptes sécurisés

Les utilisateurs recherchent un processus parfaitement fluide, mais ne veulent pas sacrifier la protection des données au profit de la convivialité. Ils s'attendent à recevoir un certain niveau de protection lorsqu'ils confient leurs informations aux entreprises.

Les utilisateurs estiment que la partie concernant la sécurité des applications doit s'exécuter en arrière-plan et ne doit pas les gêner.

Les critères à rechercher dans une solution de gestion des identités et des accès (IAM)

Pour garantir une gestion des identités fluide et sécurisée, vos plateformes d'IAM doivent proposer :

Des options de connexion unique

- Eliminez les tracas causés par la multiplication des noms d'utilisateur et des mots de passe, en fournissant la possibilité de se connecter à toutes les applications avec un ensemble unique de données d'identification.

L'authentification multi-facteurs

- Renforcez la sécurité à l'aide de l'authentification d'utilisateur multi-facteurs.

La gestion du cycle de vie des utilisateurs

- Rationalisez les processus d'intégration et de désactivation des utilisateurs.

L'intégration aux annuaires d'utilisateurs et aux applications existants

- Stockez les annuaires d'utilisateurs sur le cloud ou sur site.

Des informations sur les utilisateurs et les appareils

- Réalisez une intégration aux plateformes de détection des fraudes et de gestion des appareils mobiles pour incorporer les renseignements aux décisions d'accès.

Une expertise garantissant la réussite de votre programme

- Faites équipe avec un partenaire proposant des services intégrés de planification, de support et de déploiement.

IBM Cloud Identity

La solution IBM Cloud Identity permet aux responsables de la fonction IT, de la sécurité et de l'activité métier de s'adapter à la nouvelle ère du cloud computing, et aussi de tirer parti des dernières innovations en matière de productivité des utilisateurs. Protégez pour demain votre investissement en gestion des identités et des accès avec IBM Cloud Identity.

IBM Cloud Identity permet aux entreprises de fournir un accès rapide et sécurisé aux applications métier. Découvrez comment la technologie IDaaS d'IBM connecte les utilisateurs et les applications dans cette vidéo de 2 minutes.

Voir la vidéo

Sources

1. 2019 Cost of a Data Breach Report. Réalisé par le Ponemon Institute, sponsorisé par IBM Security

2. « Forrester Analytics: IAM Software Forecast, 2018 to 2023 (Global), » Forrester Research, Inc., 10 mai 2019. Sponsorisé par IBM.

IBM **Sécurité**

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

La page d'accueil d'IBM est accessible à l'adresse suivante : **ibm.com**

Pensez à recycler ce document

IBM

28028728-FRFR-00