Authentification unique (SSO) : **Quatre grands mythes à remettre en question**

De plus en plus d'entreprises perçoivent l'intérêt de l'authentification unique (SSO, Single Sign-On).

Selon une récente enquête réalisée pour le compte d'Okta :

88% des entreprises interrogées utilisent déjà une solution de type SSO.

95% des décideurs IT considèrent l'authentification SSO comme un élément important de leur pile IT.

20 applications au moins sont protégées par une solution SSO, ce chiffre allant jusqu'à 30 dans de nombreuses entreprises.

Malgré les avantages évidents de l'authentification SSO, certains mythes persistent. Jetons un œil aux idées fausses les plus répandues.

Le mythe
L'authentification SSO est chère

Aujourd'hui encore, certains décideurs IT estiment que l'authentification SSO est un outil non essentiel, qui ne justifie pas une dépense supplémentaire. Ils devraient pourtant s'intéresser aux coûts liés à l'*absence* de SSO.

La réalité

Dans les entreprises qui n'adoptent pas de solution SSO :

MOTDEPASSE2

Les équipes IT passent l'essentiel de leur temps à gérer les demandes de réinitialisation de mot de passe. Ils dépensent en moyenne 8 euros par demande, la note augmentant rapidement lorsque l'entreprise se développe.[1]

Les collaborateurs n'aiment pas gérer d'innombrables identifiants, ce qui réduit leur productivité et ralentit l'activité. Pour les entreprises, chaque réinitialisation de mot de passe d'un collaborateur entraîne une perte de productivité de 10 euros, ce qui se produit en moyenne une fois par an[2].

0100111001000111001
0111010001001110010
1100101001001101
1001 11 00

Le risque de piratage est plus important. Aux États-Unis, une brèche coûte en moyenne 7,9 millions de dollars[3] et dans 81 % des cas, ces compromissions sont liées à un vol d'identifiants[3], ce que l'authentification SSO limite considérablement.

Le mythe
L'authentification SSO crée un point de défaillance unique

Dans la mesure où l'authentification SSO ne délivre qu'un seul mot de passe pour l'ensemble des applications, elle est parfois accusée de créer un point de défaillance unique — les pirates n'ayant plus qu'un seul mot de passe à voler, contre plusieurs auparavant.

La réalité

Il existe déjà un point de défaillance unique : l'utilisateur. Les gens ont tendance à réutiliser des mots de passe simples pour leurs différents comptes, ce qui permet aux pirates d'accéder à plusieurs comptes au moyen d'un jeu d'identifiants unique. Une solution SSO moderne élimine ce point de défaillance par des mesures de sécurité supplémentaires, comme l'authentification multifacteur (MFA) :

Avec l'authentification SSO, l'équipe IT peut instaurer des règles pour garantir que chaque mot de passe :

- **Expire** après une durée définie.
- **Diffère** des précédents.
- Ne corresponde pas à des **identifiants piratés**.
- **Soit verrouillé** après un certain nombre d'échecs de connexion.

L'authentification SSO examine le contexte d'une demande de connexion et tient compte des facteurs suivants :

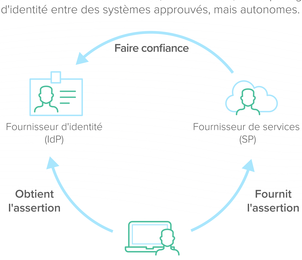
- Quelle est l'**application** concernée ?
- De quel **groupe** l'utilisateur fait-il partie ?
- Quelle est la **localisation** de l'utilisateur ? Est-elle digne de confiance ?
- Quel est le **terminal** utilisé ? A-t-il déjà été employé auparavant ?
- Quelle est l'**adresse IP** de l'utilisateur ? Est-elle suspecte ?

Le mythe
L'authentification SSO équivaut à un gestionnaire de mots de passe

Dans la mesure où l'authentification SSO permet d'accéder à différentes applications à l'aide d'un mot de passe unique, elle est parfois assimilée à un gestionnaire de mots de passe.

La réalité

L'authentification SSO n'est pas centrée sur les mots de passe, mais sur l'accès. Elle repose sur la fédération des identités, autrement dit, sur le partage d'attributs d'identité entre des systèmes approuvés, mais autonomes.



Les solutions SSO modernes utilisent des protocoles de fédération, comme SAML 2.0 et OpenID Connect. Parmi les personnes interrogées, 91 % indiquent utiliser ces protocoles avec leur solution SSO.

Les solutions SSO modernes s'intègrent également avec les éléments suivants :

Le mythe
L'authentification SSO est difficile à déployer

La plupart des entreprises dépendent à la fois d'une infrastructure on-premise et d'applications cloud, et il leur est difficile de déployer une solution SSO couvrant le tout.

La réalité

Les solutions SSO modernes proposent des préintégrations avec la totalité des ressources IT, qu'elles soient on-premise ou dans le cloud, et ne nécessitent aucun serveur sur site supplémentaire ni modification du pare-feu.

- Préintégrations complètes pour des milliers d'applications courantes
- Intégrations standard (SAML, OIDC, SCIM, etc.) utilisables avec des applications on-premise et cloud
- Toolkits facilitant la prise en charge du protocole SAML par des applications personnalisées
- Possibilité de se connecter à un annuaire Active Directory ou LDAP et d'y enregistrer automatiquement les utilisateurs

Pour en savoir plus

Parcourez notre série de publications sur l'authentification SSO :

- Mythe ou réalité : l'authentification unique (SSO) équivaut à un gestionnaire de mots de passe
- Mythe ou réalité : l'authentification unique (SSO) crée un point de défaillance unique
- Mythe ou réalité : l'authentification unique (SSO) ralentit l'IT
- Mythe ou réalité : l'authentification unique (SSO) est difficile à déployer

Vous pouvez aussi visionner notre webinar :

- Tout ce que vous ignorez sur l'authentification unique (SSO)

Ou consultez notre page produit sur l'authentification unique (SSO)

okta

Sources
1. Forrester, Making The Business Case For Identity And Access Management, août 2018
2. Rapport 2018 de Ponemon : https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf
3. Verizon