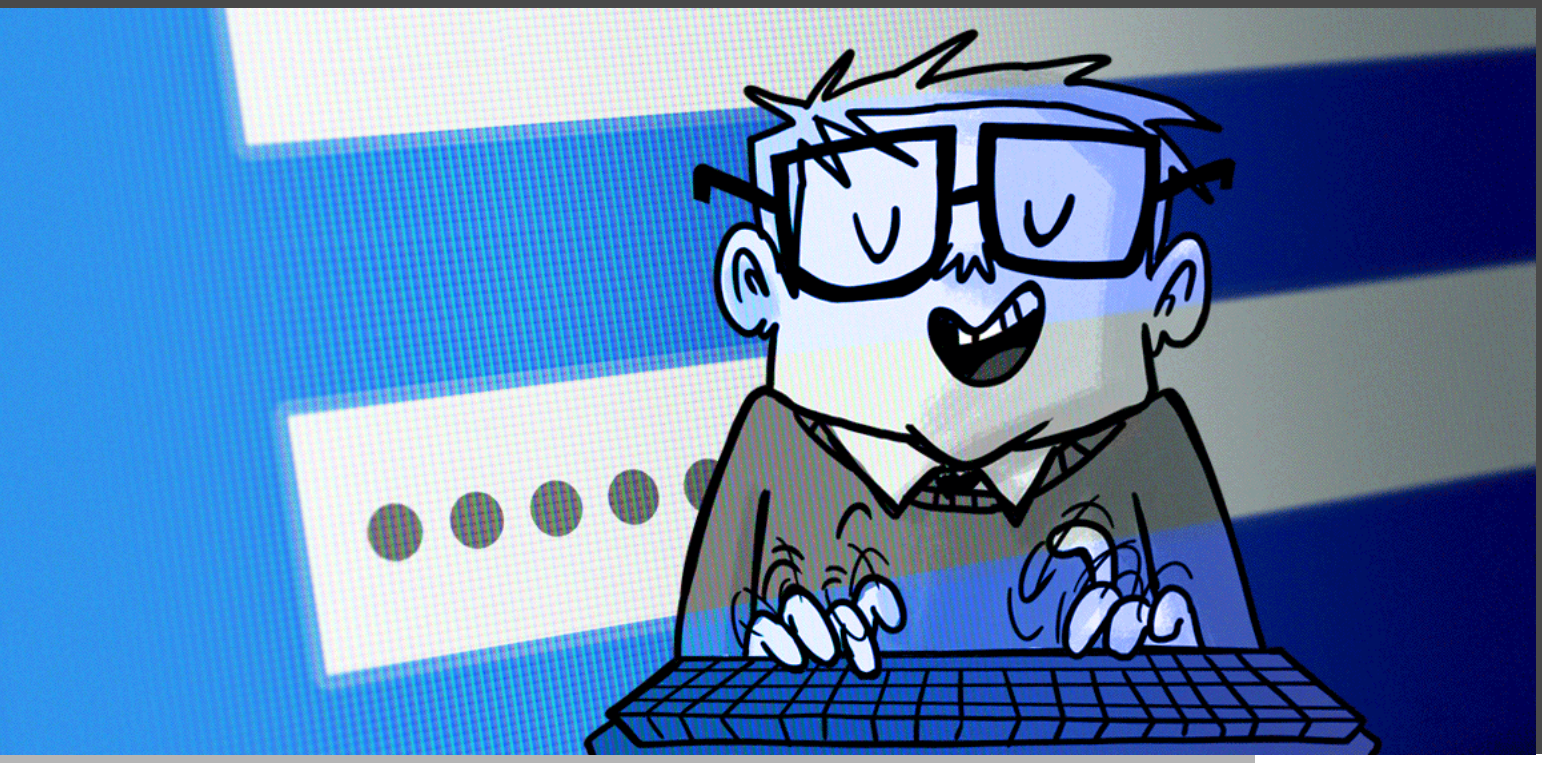
Devolutions

10 raisons de renforcer la sécurité de l'identité avec l'authentification unique

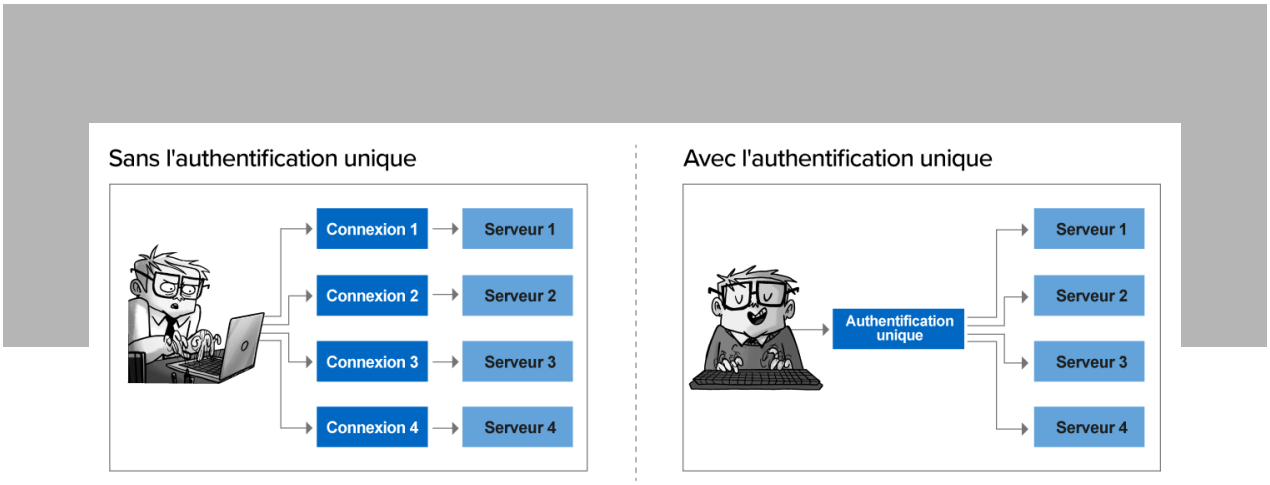


NOUS VIVONS DES MOMENTS HISTORIQUES

Nous vivons des moments historiques. Je ne peux pas croire qu'un jour, nous allons dire à nos enfants: « Je me souviens quand les gens se battaient pour du papier toilette pendant la pandémie de COVID-19. » En fait, nos enfants seront peut-être plus choqués quand on va leur dire : « Je me souviens de l'époque où certaines entreprises n'utilisaient pas l'authentification unique pour renforcer la sécurité de l'identité. »

Qu'est-ce que l'authentification unique?

Chaque fois qu'un utilisateur se connecte à une application, ça ouvre une porte aux pirates informatiques. L'authentification unique (ou SSO, de l'anglais ***Single Sign-On***) permet aux utilisateurs de se connecter une seule fois avec un seul ensemble d'informations d'identification, et d'accéder à toutes les applications, données et sites Web pour lesquels ils ont une autorisation. Par exemple, le compte Devolutions prend en charge le SSO. Donc, avec une authentification unique, les utilisateurs ont accès à tous les services Web de Devolutions, y compris le portail client, Devolutions Online Database, Devolutions Online Drive, la sauvegarde en ligne, le service d'installateur, le forum et notre programme d'affiliation.



Voici 10 avantages d'utiliser l'authentification unique pour renforcer la sécurité de l'identité :

1. Augmente la sécurité de manière générale

L'authentification unique utilise diverses normes (par exemple, SAML 2.0, OAuth, SCIM et OpenID Connect) pour transmettre en toute sécurité les accès utilisateur. L'utilisation du SSO, combinée au contrôle d'accès basé sur les rôles et à l'authentification à deux facteurs/multifacteur améliore considérablement la sécurité d'une organisation.

2. Renforce les politiques d'utilisation des mots de passe

Les mots de passe restent l'un des maillons les plus faibles de la chaîne de cybersécurité. Par exemple, 80 % des fuites de données liées au piratage impliquent des informations d'identification compromises et faibles, 59 % des personnes utilisent le même mot de passe pour plusieurs comptes (et la plupart utilisent le même mot de passe aussi longtemps que possible), et 34 % des employés partagent leurs mots de passe au travail. L'authentification unique permet de réduire le risque de mauvaises pratiques en matière de gestion des mots de passe : fini les mots de passe multiples. Les utilisateurs finaux ne pourront choisir que des mots de passe ou des phrases secrètes complexes.

3. Réduit la fatigue des mots de passe

L'utilisateur final moyen doit garder la trace de 191 mots de passe! L'authentification unique réduit la fatigue des mots de passe en permettant aux utilisateurs finaux de choisir et de se souvenir d'un seul mot de passe (à condition, bien sûr, qu'il soit suffisamment fort comme indiqué ci-dessus). Devoir se souvenir de plusieurs mots de passe est une tâche quasiment impossible et ça augmente le risque de réutiliser le même mot de passe. Ça favorise aussi les fuites de mots de passe, surtout quand ils sont stockés dans un endroit peu sûr comme des fichiers Word et des ***Post-it*** sous le clavier ou dans le tiroir du bureau.

4. Améliore l'expérience de l'utilisateur

L'utilisateur professionnel moyen doit saisir ses informations d'identification pour divers sites Web et applications 154 fois par mois (et pour certains utilisateurs, ce nombre peut atteindre des milliers par mois). L'authentification unique élimine cette tâche fastidieuse et inefficace, ce qui rend les utilisateurs plus productifs.

5. Accélère l'adoption des applications

Avec l'authentification unique, les ressources sont accessibles à partir d'un seul endroit, ce qui favorise l'adoption par les utilisateurs finaux des applications utilisées dans l'organisation.

6. Diminue la charge de travail

Les équipes TI sont très sollicitées et doivent en faire toujours plus, avec de moins en moins de budget et de ressources. L'authentification unique réduit leur charge de travail, puisque les utilisateurs finaux n'ont plus besoin de faire des tonnes de demandes parce qu'ils ont (encore!) oublié leur mot de passe. Ça permet également de réduire les coûts. Des études ont montré qu'une seule réinitialisation de mot de passe coûte en moyenne 70 $ aux entreprises et que 20 % à 50 % de tous les appels aux équipes de soutien informatique concernent des réinitialisations de mot de passe.

7. Déprovisionne les anciens utilisateurs

Avec l'authentification unique, les utilisateurs finaux, y compris les employés, les sous-traitants, les partenaires et d'autres personnes qui ne font plus partie de l'organisation, peuvent être déprovisionnés rapidement - ou même automatiquement.

8. Augmente la vitesse

L'authentification unique est particulièrement utile pour les organisations où un grand nombre de services et de personnes exigent un accès rapide et illimité aux mêmes applications (par exemple, les services d'urgence et les hôpitaux).

9. Empêche les *Shadow IT*

Grâce à l'authentification unique, les administrateurs système peuvent surveiller les applications infonuagiques auxquelles les utilisateurs finaux accèdent et empêcher les téléchargements non autorisés.

10. Support compliance

Le déploiement d'une authentification unique peut aider les organisations à répondre à des critères spécifiques associés à diverses réglementations, comme SOX (les contrôles TI doivent être documentés et des contrôles de données doivent être en place), HIPAA (les utilisateurs qui accèdent aux dossiers électroniques ou qui nécessitent un contrôle d'audit doivent être authentifiés) et PCI DSS (intégré à Active Directory pour garantir un mécanisme adéquat d'identification des utilisateurs).

Les inconvénients de l'authentification unique

Toute solution apporte son lot de défis et l'authentification unique ne fait pas exception. Les inconvénients incluent :

1. Un anneau (ou mot de passe) pour les gouverner tous

Si un compte d'authentification unique est piraté, les autres comptes sous la même authentification sont également à risque. Pour renforcer cette vulnérabilité, il est essentiel d'utiliser des mots de passe ou des phrases secrètes uniques et solides et d'utiliser l'authentification à deux facteurs ou multifacteur.

2. Lorsque l'authentification unique est hors service, l'accès aux sites connectés est aussi hors service

Un système d'authentification unique doit être très fiable et il doit y avoir un plan de secours solide pour faire face aux pannes.

3. La mise en place d'une authentification unique peut prendre plus de temps que prévu

C'est comme les meubles IKEA : ça peut avoir l'air simple, mais une fois que vous commencez à assembler toutes les pièces, vous vous rendez compte que c'est assez compliqué (bien que, contrairement aux meubles IKEA, les organisations qui mettent en place une authentification unique n'ont pas à résoudre tous les problèmes avec une clé Allen!). Les PME qui ne disposent pas de compétences internes dans ce domaine doivent travailler avec un fournisseur de services gérés pour s'assurer que l'authentification unique soit mise en œuvre et gérée correctement.

En bref

Si l'authentification unique n'est pas sans failles, les avantages l'emportent de loin sur les inconvénients. Toutes les organisations – y compris les PME qui sont de plus en plus attaquées – devraient en faire une priorité absolue.