LastPass

L'authentification unique ne suffit pas : l'avenir appartient au sans mot de passe

Continuer →

L'authentification unique (SSO) aide les organisations à gérer les comptes de façon centralisée et offre aux employés un moyen pratique et sécurisé d'accéder à de nombreuses applications professionnelles dans le cloud.

Toutefois, le SSO n'élimine pas tous les risques.

Sachant que dans 8 cas sur 10, les fuites de données sont causées par des identifiants de connexion compromis, chaque identité dans votre entreprise doit être sécurisée.

Voyons pourquoi le SSO, malgré son utilité dans votre pile technologique, ne suffit pas à protéger entièrement votre organisation – et ce que vous pouvez faire pour combler ces lacunes.

**Verizon DBIR

Comment expliquer que le SSO crée des failles dans votre sécurité ?

Toutes les applications ne sont pas compatibles avec les technologies SSO.

Si votre organisation utilise une application spécialisée ou un logiciel inhabituel, il y a de fortes chances qu'il ne fonctionne pas avec le SSO, ce qui laisse une porte (ou plusieurs) ouverte aux pirates.

Comment Le Sans Mot De Passe Comble Ces Failles ?

Une solution sans mot de passe permet de gérer TOUS les points d'entrée de votre organisation, offrant aux employés un accès instantané et sans effort à TOUS les sites et à TOUTES les applications.

Qu'est-ce qu'on gagne en éliminant un mot de passe ?

MEILLEURE ADOPTION

Les employés peuvent accéder instantanément à leur coffre-fort, sans saisir de mot de passe.

MEILLEURE PRODUCTIVITÉ

Les employés (et le département IT) peuvent se consacrer à des tâches à valeur ajoutée au lieu de chercher à se souvenir d'un mot de passe.

SÉCURITÉ RENFORCÉE

Un nombre réduit de mots de passe implique une diminution des possibilités d'intrusion ou de piratage.

L'avenir appartient au sans mot de passe

Sécurisez chaque identité avec LastPass.

Nous contacter