LastPass ••• | MFA

Aperçu de la solution

LastPass MFA est un moyen plus intelligent de s'authentifier

Les solutions d'authentification évoluent rapidement à mesure que les entreprises deviennent des espaces de travail dans le nuage orientés PAP (Prenez votre appareil personnel). Les employés sont sensibilisés aux exigences de sécurité, mais ils attendent une technologie simple, commode et rapide. Face à ce manque de visibilité et une complexité élevée, le SI est plus que jamais mis au défi de gérer l'authentification dans un environnement hybride sans déranger les utilisateurs finaux.

À l'heure où 81 pour cent des failles de sécurité sont provoquées par des mots de passe faibles, il est évident qu'ils ne peuvent pas à eux seuls protéger votre entreprise. Comment garantir la sécurité des informations critiques sans ajouter de points de friction pour les utilisateurs ? L'authentification à deux facteurs (2FA) est un bon point de départ, mais une approche unique ne fonctionne pas lorsque les utilisateurs ont des comportements, des appareils personnels, des niveaux d'accès et des attributs distincts.

LastPass MFA protège votre entreprise avec une technologie de pointe actuelle tout en simplifiant l'expérience de connexion des employés. LastPass MFA va au-delà de l'authentification à deux facteurs standard pour s'assurer que les bons utilisateurs ont accès aux bonnes données au moment adéquat, sans complexité supplémentaire. Conçu sur un modèle unique de sécurité, LastPass MFA garantit la confidentialité et la sécurité des données biométriques tout en tirant parti de facteurs humains et facteurs cachés pour identifier et authentifier les utilisateurs. LastPass MFA offre une expérience intuitive à plusieurs facteurs que les administrateurs peuvent déployer en toute simplicité et sans trop d'effort pour répondre à la demande des employés.

Authentification adaptative adaptée aux utilisateurs

En associant les données biométriques et l'intelligence contextuelle, LastPass MFA prouve l'identité de l'utilisateur à l'aide d'une combinaison de facteurs, sans augmenter les points de friction au niveau de l'expérience de connexion. L'utilisateur prouve son identité à l'aide de facteurs humains comme la reconnaissance faciale, les empreintes digitales, la voix et l'iris. L'appareil est authentifié dans l'environnement de l'entreprise à l'aide de facteurs cachés comme la localisation du téléphone ou l'adresse IP. Tout ce processus d'authentification est vécu comme une expérience sans mot de passe.

Accès sans mot de passe

Les mots de passe représentent une source infinie de frustrations et de risques. À l'aide de données biométriques et d'authentification adaptative, LastPass MFA peut éliminer les mots de passe et rationaliser l'accès employé aux apps de travail pour améliorer la productivité.

Déploiement simplifié pour les équipes informatiques

LastPass MFA est simple et facile à déployer pour les équipes du SI, sans besoin de formation ou de services supplémentaires. LastPass MFA offre une sécurité rapide tout en économisant le temps et les ressources nécessaires à la récupération des mots de passe ou à la résolution des problèmes d'accès.

Modèle de sécurité zéro-connaissance

Authentification adaptative

Déploiement et gestion simplifiés

Contrôles de sécurité exhaustifs

Une expérience utilisateur sans points de friction

La sécurité renforcée ne doit pas être un obstacle à la productivité des employés. LastPass MFA renforce la sécurité de tous les points d'accès, des apps qu'elles soient anciennes, mobiles, dans le nuage ou sur site. LastPass MFA authentifie les utilisateurs en toute transparence sur tous les appareils, permettant au SI de sélectionner les méthodes d'authentification au cas par cas, depuis le SMS aux méthodes push à l'authentification adaptative, offrant une meilleure flexibilité et assistance à tous les cas d'utilisation.

Contrôle centralisé et granulaire

Protégez votre entreprise avec une liste exhaustive de règles pour gérer les utilisateurs au niveau individuel, collectif et organisationnel. Définissez des règles granulaires, comme autoriser l'accès à une app en fonction de certaines localisations ou certaines heures prédéfinies. Tout est géré depuis un tableau de bord centralisé simple à utiliser.

Intégrations plug-and-play

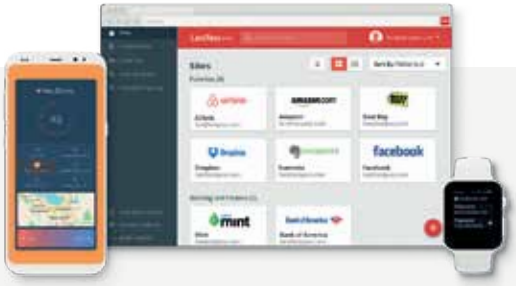
Automatisez le provisionnement utilisateur à l'aide d'intégrations avec les annuaires d'utilisateurs tel que AD, Azure AD, Okta et OneLogin. Avec une installation simple et une gestion minimale quotidienne, LastPass MFA évolue au même rythme que votre entreprise.

Solution d'authentification tout-en-un

Avec son assistance pour les apps anciennes sur site, dans le nuage, ou sur mobile, LastPass MFA gère l'authentification pour toutes les applications d'entreprise depuis une interface unique. Les équipes du SI peuvent gérer l'authentification de façon centralisée dans toute l'organisation en gardant une visibilité sur toutes les connexions depuis une plate-forme unique.

Sécurité intégrée dans la conception

LastPass MFA est conçue pour protéger la confidentialité et la sécurité des données. Les données biométriques ne quittent jamais l'appareil utilisateur et sont chiffrées à son niveau. Elles ne sont jamais stockées dans un emplacement centralisé qui pourrait être compromis, ce qui protège les données biométriques des attaques côté serveur.



Visitez www.lastpass.com/multifactor-authentication pour en savoir plus

05.28.2019/LMI06385b/PDF