LastPass

Acceso sin contraseña: una realidad sencilla y segura para su empresa.

Los problemas con las contraseñas existen.

Los administradores de TI nos dicen que los usuarios usan **una media de 63 contraseñas** para hacer su trabajo cada día.[1]

Casi tres cuartas partes (73%) de los administradores de TI afirman que su organización necesita un restablecimiento de la contraseña cada tres meses o más y un **92% necesita un restablecimiento al menos cada seis meses.**

A consecuencia de este continuo cambio de credenciales, casi **un tercio (31%) de los tickets del servicio de asistencia tiene relación con las contraseñas.**

La exposición es inevitable. La única pregunta es cuándo se producirá.

35% Más de un tercio (35%) de los administradores de TI han sufrido un robo de datos en su empresa en los últimos dos años.

Deje de intentar encontrar el equilibrio perfecto entre seguridad y simplicidad. Ahora puede tenerlo todo con **el acceso a la bóveda digital sin contraseña.**

Su empresa ya tiene...

Todos los componentes necesarios. Los gestores de contraseñas y la MFA son la base para un futuro sin contraseñas.

64% de los administradores de TI manifiestan que sus empresas usan un gestor de contraseñas, y el porcentaje es el mismo para el SSO. **La utilización de la MFA se sitúa incluso un poco por encima, con un 67%.**

La estrategia correcta. Los administradores de TI son innovadores por naturaleza y adoptan las nuevas tecnologías antes que nadie.

57% Más de la mitad de los administradores de TI (57%) tienen la tecnología sin contraseña en la hoja de ruta de sus empresas.

¿POR QUÉ DECIR ADIÓS A LAS CONTRASEÑAS?

Al eliminar las barreras relacionadas con las contraseñas, los empleados pueden acceder rápidamente a las aplicaciones y las credenciales que más necesitan.

La simplicidad impulsa la adopción entre los empleados, lo que se traduce en importantes mejoras en sus hábitos relacionados con las contraseñas.

Incluso puede imponer requisitos más estrictos para la contraseña maestra, porque los usuarios no la necesitarán para acceder a su bóveda.

¿Cómo funciona el acceso sin contraseña?

Los usuarios de LastPass pueden acceder a la bóveda de LastPass al iniciar sesión por primera vez, a través de uno de estos tres métodos: LastPass Authenticator, biométrica compatible con FIDO2 y claves de hardware compatibles con FIDO2.

El acceso sin contraseña no prescinde de las contraseñas por ahora. Las contraseñas maestras se utilizarán para registrar una cuenta de LastPass y para otros cambios en la cuenta relacionados con la seguridad.

Es hora de imaginar un mundo sin contraseñas

En general, los administradores de TI ganarían tranquilidad y seguridad si pudieran adoptar la tecnología sin contraseña.

44% **más tranquilos**

33% **más seguros**

32% **menos estresados**

No renuncie a la seguridad a cambio de más simplicidad. Ahora puede tenerlo todo.

Su empresa está mejor protegida frente a los ciberriesgos si los empleados utilizan métodos de autenticación seguros para acceder a su bóveda en lugar de contraseñas poco seguras o reutilizadas.

Adiós a las contraseñas con LastPass

Fuentes:
1. Estudio realizado por Lab42 con participantes de Estados Unidos, Australia, Canadá, Francia, Alemania y Reino Unido.

07.17.2023/PDF/LP2023