

Passwortfrei arbeiten - die neue Realität in Ihrem Unternehmen.



IT-Administratoren zufolge nutzen Mitarbeiter **durchschnittlich 63 Passwörter** bei ihrer täglichen Arbeit.¹



Fast drei Viertel (73 %) der IT-Administratoren sagen, dass ihr Unternehmen mindestens alle drei Monate eine Passwortrücksetzung anfordert. **Bei 92 % geschieht dies mindestens alle sechs Monate.**



Viele Zugangsdaten, ständige Passwortrotation: **Fast ein Drittel (31 %) der Helpdesk-Anfragen haben Passwörter zur Ursache.**

Es ist keine Frage, ob es in Ihrem Unternehmen zu einer Datenschutzverletzung kommt, sondern wann.



35%

Gut ein Drittel (35 %) der IT-Administratoren haben in den letzten 2 Jahren in ihrem Unternehmen eine Datenschutzverletzung erlebt.

Schluss mit dem Austarieren von Sicherheit und Einfachheit. Sie können Ihren Mitarbeitern beides bieten: **durch einen passwortfreien Zugriff auf ihren Vault.**



Ihr Unternehmen hat bereits ...

Alle erforderlichen Komponenten: Passwort-Manager und MFA sind das Fundament einer Zukunft ohne Passwörter.

64%

der Unternehmen nutzen einen Passwort-Manager. Ebenso viele nutzen SSO. **Noch mehr Unternehmen nutzen MFA: 67 %.**

Die richtige Strategie: IT-Administratoren sind Early Adopter und denken zukunftsgerichtet.

57%

Gut die Hälfte (57 %) der IT-Administratoren haben passwortfreie Lösungen auf der Roadmap für ihr Unternehmen.



PASSWORTFREI ARBEITEN - WARUM?



Ohne Eingabe von Passwörtern haben Mitarbeiter schnellen Zugriff auf häufig benötigte Anwendungen und Zugangsdaten.



Ein einfacher Zugang verbessert die Akzeptanz und Nutzung und damit auch die allgemeinen Passwortgewohnheiten.



Sie können das Master-Passwort strengerem Anforderungen unterwerfen, denn die Benutzer müssen es zum Öffnen ihres Vaults nicht mehr eingeben.

Passwortfrei arbeiten - wie funktioniert das?

Benutzer können für ihren passwortfreien Zugriff auf den LastPass-Vault einen der folgenden drei Authentifizierungsmechanismen einrichten: den LastPass Authenticator, FIDO2-kompatible Biometrie oder einen FIDO2-kompatiblen Hardwareschlüssel.

Passwortfreies Arbeiten schließt weiterhin Passwörter ein - noch. Zum Registrieren eines LastPass-Kontos und für andere sicherheitsrelevante Kontoänderungen ist auch künftig noch das Master-Passwort erforderlich.

Es ist Zeit für eine Welt ohne Passwörter

IT-Administratoren würden sich entspannter und sicherer fühlen, wenn sie eine passwortfreie Technik einführen könnten.

44%

entspannter

33%

sicherer

32%

weniger gestresst

Sicherheit oder Nutzerkomfort? Bei LastPass bekommen Sie beides.

Ihr Unternehmen ist besser vor Cyberrisiken geschützt, wenn Mitarbeiter ihren Vault über eine sichere Authentifizierungsmethode öffnen, anstelle schwache und mehrfach genutzte Passwörter zu nutzen.

Machen Sie das passwortlose Arbeiten mit LastPass zur Realität

Quellen:

1. Die Umfrage wurde von Lab42 mit Teilnehmern aus Australien, Deutschland, Frankreich, Großbritannien, Kanada und den USA durchgeführt.