

Veiligheid zonder wachtwoorden

Eenvoudige aanmelding bij de LastPass-kluis



Kies voor maximale beveiliging met minimale inspanning

Alles is digitaal, en er is geen ontkomen aan: iedereen maakt regelmatig accounts en wachtwoorden aan. Bedrijven en medewerkers kunnen niet zonder voor hun werk en hun dagelijkse doelen. Dit vraagt om beveiligingsbeleid dat goede wachtwoordgewoontes afdwingt van alle medewerkers, zodat u iedereen veilig kunt houden.

En daarom worstelen bedrijven van klein tot groot om het juiste evenwicht te vinden tussen veiligheid en gebruiksgemak. U hebt beleidsregels en tools nodig, met een eenvoudige configuratie, laagdrempelige toegang en probleemloos beheer. Het alternatief is onveilig gedrag van uw medewerkers. En veiligheid kan ook zonder extra drempels: met wachtwoordloze aanmelding bij de LastPass-kluis.

Zet de hoofdwachtwoorden op de automatische piloot

Alle eindgebruikers van LastPass kunnen wachtwoordloze aanmelding voor hun kluis met de LastPass Authenticator inschakelen bij hun eerste aanmelding, tijdens het aanmaken van hun account of via de accountinstellingen. Als ze de begeleide configuratie hebben voltooid, hoeven ze op vertrouwde apparaten nooit meer hun wachtwoord in te voeren.

Nog geen afscheid van het hoofdwachtwoord

De technologie voor wachtwoordloze toegang ontwikkelt zich razendsnel. Het doel is om helemaal zonder hoofdwachtwoord te kunnen werken, maar dat is een proces van meerdere stappen. Voorlopig blijft het hoofdwachtwoord nog bestaan om wijzigingen in de beveiligingsinstellingen van het account te bevestigen, en voor mislukte verificatiepogingen. Gebruikers hebben hun wachtwoord minder vaak nodig, dus zorg ervoor dat ze hun opties voor accountherstel zo configureren dat ze altijd nog een back-up hebben om bij hun kluis te komen.



Vereenvoudigde gebruikerservaring



Minder wachtwoord-frustraties



Hogere productiviteit voor IT-beheerders



Veilige verificatie

Probeer wachtwoordloze aanmeldingen

Het is tijd om te denken over een wereld zonder wachtwoorden

Vereenvoudigde gebruikerservaring

Met de LastPass Authenticator kunnen medewerkers hun kluis openen en belangrijke aanmeldingsgegevens beheren, zonder dat ze hiervoor hun hoofdwachtwoord nodig hebben. Geef direct probleemloos toegang en voorkom frustraties en vertragingen door wachtwoorden. Werk met een wachtwoordbeheerder om de digitale assets van uw bedrijf te beveiligen, en versoepel de toegang met aanmeldingen zonder wachtwoorden.

Sterkere beveiligingsstandaarden

Uw medewerkers kunnen een nog sterker hoofdwachtwoord instellen – tenslotte hoeven ze het niet te onthouden! En u kunt dit simpel afdwingen met een strengere beleidsregel. Als medewerkers hun hoofdwachtwoord minder vaak hoeven te gebruiken en in te voeren, werken ze veiliger – en zo houdt u hackers en cybercriminelen buiten te deur.

Minder gedoe betekent meer gebruik

Als aanmelden nog makkelijker wordt, gebruiken mensen hun LastPass-kluis vaker. Dit verbetert de aanname voor uw hele organisatie. Een betere aanname zorgt voor betere algehele wachtwoordgewoontes en verlaagt uw digitale risico's aanzienlijk.

Verhoog de productiviteit

Als er geen wachtwoorden meer nodig zijn voor aanmeldingen, gaat er geen kostbare werktijd meer verloren aan wachtwoordherstel of vertragingen als mensen accounts niet kunnen gebruiken. En ook uw IT-afdeling kan zich bezighouden met nuttigere zaken. Iedereen kan zich weer richten op echte toegevoegde waarde, in plaats van gedoe rondom wachtwoorden.



Werk zonder wachtwoorden met LastPass Business