

Beveilig ieder toegangspunt met één eenvoudige oplossing.



LastPass Business: wachtwoordbeheer met geavanceerde single sign-on (SSO)

Meer apparaten, toepassingen, netwerken en gebruikers verhogen de complexiteit van het beheer – en de beveiliging – van toegang voor medewerkers. Medewerkers willen gewoon efficiënt hun werk doen, maar bedrijven moeten hierbij wel zorgen voor goede beveiligingsmechanismen.

Maak het werknemers gemakkelijker en geef uw IT-team meer mogelijkheden voor inzicht en controle. LastPass biedt u een eenvoudig te beheren en gebruiksvriendelijke toegangsooplossing. LastPass levert single sign-on voor de belangrijkste toepassingen, en wachtwoordbeheer om alle andere toegangsgegevens veilig op te slaan. Zo kunnen uw medewerkers in een mum van tijd veilig verbinding maken met hun zakelijke accounts.

LastPass Business

Met het wachtwoordbeheer van LastPass Business kunnen medewerkers probleemloos sterke wachtwoorden aanmaken en ze op een veilige manier delen met collega's, terwijl de infrastructuur van LastPass op basis van zero knowledge de beveiliging garandeert. Beheerders krijgen bovendien waardevolle inzichten en meer controle.

Geavanceerde single sign-on van LastPass

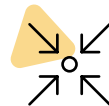
LastPass Single Sign-On zorgt ervoor dat uw medewerkers zich zo snel mogelijk kunnen aanmelden bij een onbeperkt aantal cloud-toepassingen, en het maakt het eenvoudiger voor uw IT-afdeling om software beschikbaar te maken voor gebruikers. En dat allemaal in hetzelfde programma dat ze al kennen en gebruiken voor hun wachtwoorden.



Single sign-on en wachtwoordbeheer



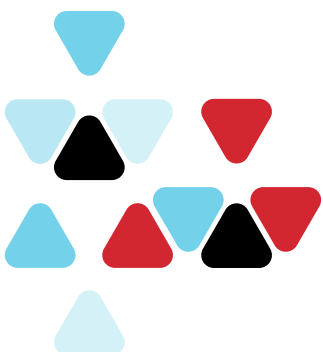
Uitgebreide opties voor uw beveiliging



Flexibele integratiemogelijkheden



Eenvoudig gebruikersbeheer en rapportage



Een krachtige combinatie: single sign-on en wachtwoordbeheer

Met een geïntegreerde oplossing voor wachtwoordbeheer en single sign-on kunnen bedrijven SSO voor hun hele organisatie afdwingen om alle aanmeldingen te beveiligen, in combinatie met wachtwoordbeheer om alle aanmeldingsgegevens veilig op te slaan. De combinatie van single sign-on en wachtwoordbeheer garandeert zowel consequent beveiligingsbeleid als een zeer gebruiksvriendelijke ervaring van het aanmeldingsproces.

Naadloze gebruikerservaring

Maak digitaal werk eenvoudig voor uw medewerkers, met één centrale locatie voor toegang tot alle toepassingen die voor hen relevant zijn. LastPass zorgt dat uw mensen via single sign-on eenvoudig toegang hebben tot ondersteunde cloud-toepassingen. En al hun andere accounts en gegevens kunnen ze veilig opslaan in hun digitale LastPass-kluis. LastPass doet zijn werk: wachtwoorden aanmaken, onthouden en invullen. Zo kunnen uw medewerkers ook hun werk doen.

Geconsolideerd beheer

Krijg met één handig dashboard een 360-gradenoverzicht van alle activiteiten van uw eindgebruikers met wachtwoordbeheer en single sign-on. Met LastPass kunnen bedrijven de juiste toegang geven aan de juiste mensen, op het juiste moment. Maak vervelende routinetaken verleden tijd en krijg inzicht in de toegangsbeveiliging voor uw gehele organisatie.

Flexibele controles, gedetailleerd instelbaar

Complete beveiliging hoeft niet complex te zijn. LastPass biedt ruim 100 instelbare regels voor een beveiligingsbeleid op maat, om gebruikers te beheren op het niveau van de toepassing, individueel, per groep of organisatieniveau. Zo kunt u de toegangsvereisten precies aanpassen aan uw bedrijfsbehoeften. En u kunt ervoor zorgen dat het beleid consequent is voor single sign-on en wachtwoordbeheer.

Handig wachtwoorden delen

Laat teamleden veilig en flexibel toegang delen tot de accounts die ze nodig hebben, en behoud zicht op de verantwoording. LastPass maakt sterke wachtwoorden aan en toegang kan worden ingetrokken met onmiddellijke ingang. Mensen die uw bedrijf verlaten, kunnen dus geen gegevens meenemen.

Snelle aanname, snelle resultaten

LastPass is niet alleen eenvoudig te configureren en onderhouden. Het biedt ook uitgebreide materialen en handige dashboards voor beheerders die de software implementeren en ondersteunt de communicatie richting uw medewerkers. Zo kunt u betere resultaten behalen zonder extra dienstverlening in te kopen.

Dark Web Monitoring om direct actie te kunnen ondernemen

Geen zorgen meer over gegevenslekken. LastPass monitort de accounts van uw medewerkers continu en verstuurt waarschuwingen als hun aanmeldingsgegevens op het dark web worden gevonden. Zo kunnen ze direct hun wachtwoord wijzigen bij een lek – en uw zakelijke accounts veilig houden.

Gebouwd op veiligheid

Als het gaat om gegevensbeveiliging, doen we geen concessies. Gebruikersgegevens worden op apparaatniveau versleuteld en ontsleuteld. Het hoofdwachtwoord en alle gevoelige gegevens die in LastPass worden opgeslagen, blijven geheim – zelfs voor ons. Bovendien kunt u met meervoudige verificatie een extra beveiligingslaag toevoegen aan alle LastPass-accounts.



Met de volgende functies krijgt uw bedrijf meer controle, en uw medewerkers meer gebruiksgemak:

Centrale beheerconsole	Het dashboard voor de beheerder biedt geautomatiseerd gebruikersbeheer, beleidsregels, overzichtelijke dashboards en nog veel meer.
Universeel wachtwoordbeheer	Vereenvoudig de toegang tot alle relevante toepassingen en genereer voor iedere aanmelding veilige aanmeldingsgegevens, met automatisch registreren, opslaan en invullen.
Gebruikersintegraties	Via AD, Azure AD, Okta, OneLogin, Google Workspace, PingOne, PingFederate of een eigen API kunt u onder andere federatieve, nieuwe en vertrekkende gebruikers en gebruikersgroepen beheren.
Ruim 100 opties voor beveiligingsbeleid	Dwing best practices af en garandeer goed wachtwoordgedrag voor uw hele organisatie.
Gedetailleerde beveiligingsrapporten	Met geautomatiseerde, gedetailleerde rapporten kunt u acties koppelen aan gebruikers en de compliance voor uw bedrijf garanderen. Duik nog dieper in uw bedrijfsgegevens met SIEM-integraties, waaronder Splunk en Azure Sentinel.
Veilig wachtwoorden delen	Zorg dat uw teams op een veilige en flexibele manier de toegang tot hun apps kunnen delen, zonder concessies te doen op het gebied van beveiliging of verantwoordelijkheid.
Monitoring van het dark web	LastPass monitort de accounts van uw medewerkers en verstuurt waarschuwingen als hun aanmeldingsgegevens op het dark web worden gevonden. Zo kunnen ze direct hun wachtwoord wijzigen bij een lek en uw zakelijke accounts veilig houden.
Geavanceerde single sign-on	Maak uw belangrijkste zakelijke tools toegankelijk voor uw medewerkers met vereenvoudigde toegang tot een onbepert aantal toepassingen in de cloud.
Meervoudige verificatie	Koppeling met de LastPass Authenticator-app voor meervoudige verificatie bij aanmeldingen voor de wachtwoordkluis en de single sign-on-toepassingen.
Families as a Benefit	Uw medewerkers krijgen een persoonlijk LastPass-account plus vijf extra licenties die ze cadeau kunnen geven aan familie of vrienden, zodat ook hun wachtwoorden goed worden beschermd met LastPass.

Extra mogelijkheden:

Geavanceerde meervoudige verificatie van LastPass	Geavanceerde meervoudige verificatie van LastPass (MFA) beveiligt ieder toegangspunt tot uw bedrijf. Cloudtoepassingen, verouderde software, VPN, werkstations: LastPass MFA zorgt voor wachtwoordloze toegang met maximale beveiliging, dankzij adaptieve verificatietechnologie en instelbare beleidsregels voor gebruikers en groepen. Met LastPass MFA kan uw organisatie alle online aanmeldingen beveiligen en verificatie toevoegen voor de gebruikte endpoints – allemaal met één handige mobiele app.
--	--