

## OVERZICHT VAN DE OPLOSSING

# Sterke bedrijfsbeveiliging makkelijk gemaakt



## LastPass Business: wachtwoordbeheer met geavanceerde meervoudige verificatie (MFA)

Slechte wachtwoordgewoonten veroorzaken 80% van de gegevenslekken<sup>1</sup>. U kunt dus niet alleen op wachtwoorden vertrouwen om uw bedrijf te beveiligen. Hoe kunt u garanderen dat essentiële informatie veilig is, zonder drempels op te werpen voor uw medewerkers? Medewerkers begrijpen wel dat beveiliging nodig is, maar in de praktijk verwachten ze vooral dat technologie eenvoudig, handig en snel werkt. Het is voor bedrijven lastiger dan ooit om de wachtwoordbeveiliging en verificatie te regelen in een hybride omgeving, met aanmeldingen vanaf kantoor en vanuit huis. Sterke beveiliging en gebruiksgemak staan elkaar vaak in de weg.

LastPass biedt een oplossing met wachtwoordbeheer en meervoudige verificatie, die helpt om frustraties rondom wachtwoordgebruik weg te nemen bij medewerkers. Tegelijkertijd zorgt LastPass voor inzicht en controle voor de IT-afdeling, met eenvoudig beheer en moeiteloos gebruik. De combinatie van wachtwoordbeheer met meervoudige verificatie kan alle online aanmeldingen beveiligen en creëert een extra beveiligingslaag voor alle endpoints in uw organisatie. Zo blijven alle toegangspunten tot uw bedrijfsnetwerk veilig.

### 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.

### LastPass Meervoudige verificatie – geavanceerd

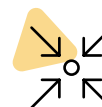
LastPass Multi-Factor Authentication (MFA) beveiligt ieder toegangspunt in uw bedrijf. LastPass MFA voegt een extra beveiligingslaag toe voor cloud-toepassingen, legacy-software, VPN's en werkstations. Zo beveiligt u al uw endpoints voor maximale zekerheid.



**Wachtwoordbeheer  
en meervoudige  
authenticatie.**



**Uitgebreide  
beveiligingsopties**



**Flexibele integratie-  
mogelijkheden**



**Eenvoudig  
gebruikersbeheer  
en rapportage**

### Probleemloze gebruikerservaring

Extra beveiliging mag de productiviteit van uw werknemers niet in de weg staan. Kies voor één leverancier voor toegang en verificatie voor al uw tools. Met LastPass krijgen medewerkers snel toegang tot alle websites, accounts en programma's die ze nodig hebben voor hun werk, terwijl de extra meervoudige verificatie onbevoegden buiten de deur houdt.

### 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.

### Flexibele controles, gedetailleerd instelbaar

Bescherm uw bedrijf met een uitgebreide set van beleidsregels voor het wachtwoordbeheer en de meervoudige verificatie en beheer gebruikers op individueel niveau, per groep of op organisatieniveau. Stel gedetailleerd beleid samen en bepaal bijvoorbeeld dat een toepassing alleen mag worden gebruikt op bepaalde tijden of vanaf bepaalde locaties.

### Toegang zonder wachtwoorden

Wachtwoorden zijn een eindeloze bron van frustratie en risico. Met LastPass kunnen bedrijven hun medewerkers hiervan verlossen. De wachtwoordbeheerder registreert alle online wachtwoord en slaat ze op, terwijl de meervoudige verificatie wachtwoorden waar mogelijk overbodig maakt met een soepelere verificatie. De combinatie van wachtwoordbeheer en meervoudige verificatie versterkt de beveiliging en laat medewerkers productiever werken, zonder ergernissen over wachtwoorden.

### Intelligent gebruik van context en biometrische gegevens

Door biometrische en omgevingsinformatie te combineren, controleert LastPass MFA de identiteit van gebruikers op

basis van verschillende factoren, zonder dat de aanmelding hierdoor lastiger wordt. Gebruikers kunnen hun identiteit bevestigen met een menselijke factor, bijvoorbeeld met een vingerafdruk of gezichtsherkenning. Hun smartphone of tablet ondersteunt verificatie op de achtergrond met contextfactoren, zoals de locatie of het IP-adres. Het resultaat: een veilige aanmelding zonder wachtwoord.

### Gebruiksklare integraties

LastPass bevat schaalbare, geautomatiseerde integraties met de meest gebruikte gebruikersdirectories: Microsoft Active Directory, Microsoft Azure AD, OneLogin, Okta, Google Workspace, PingOne en PingFederate. Zo kunnen IT-teams eenvoudiger alles opzetten voor nieuwe medewerkers en weer afsluiten voor personeel dat vertrekt.

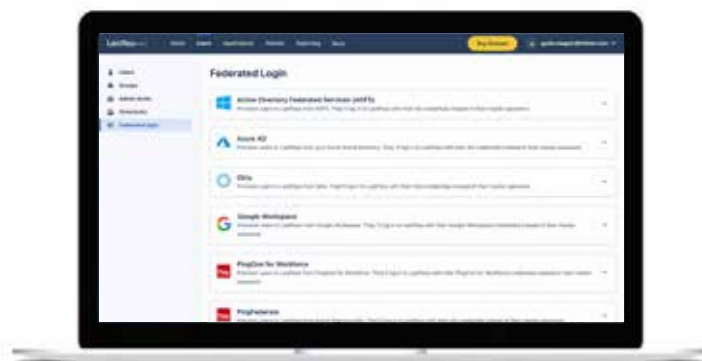
Daarnaast biedt LastPass integratie met SIEM-oplossingen (Security Information and Event Management) voor dieper inzicht in het netwerk van uw bedrijf en geavanceerde rapportage- en waarschuwingmogelijkheden. LastPass Business kan op dit moment geïntegreerd worden met Splunk en Azure Sentinel, en er zullen er snel nog meer volgen.

### Dark Web Monitoring met hulpmiddelen 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.

### Ingebouwde beveiliging

LastPass is erop gebouwd om gegevens privé en veilig te houden. Gebruikersgegevens worden op apparaatniveau versleuteld en ontsleuteld. Het hoofdwachtwoord en alle gevoelige gegevens die in LastPass worden opgeslagen, blijven geheim – zelfs voor ons. Ook biometrische gegevens worden op apparaatniveau versleuteld en verlaten nooit het apparaat.



## Met de volgende functies krijgt uw bedrijf de controle, terwijl uw medewerkers profiteren van meer gebruiksgemak:

<b>Centrale console voor beheer</b>	Het dashboard voor de beheerder biedt geautomatiseerd gebruikersbeheer, beleidsregels, overzichtelijke dashboards en nog veel meer.
<b>Universeel wachtwoordbeheer</b>	Vereenvoudig de toegang tot alle relevante toepassingen en genereer voor iedere aanmelding veilige aanmeldingsgegevens, met automatisch registreren, opslaan en invullen.
<b>Gebruikersintegraties</b>	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.
<b>Ruim 100 opties voor beveiligingsbeleid</b>	Dwing best practices af en garandeer goed wachtwoordgedrag voor uw hele organisatie.
<b>Gedetailleerde beveiligingsrapporten</b>	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.
<b>Veilig wachtwoorden delen</b>	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.
<b>Monitoring van het dark web</b>	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.
<b>Geavanceerde meervoudige verificatie</b>	Gebruik de LastPass Authenticator-app voor veilige toegang zonder wachtwoorden voor cloud-toepassingen, verouderde software, VPN's en werkstations. Gedetailleerde beleidsregels voor geofencing, tijd en IP-adressen bieden beheerders meer controle en versterken uw beveiliging.
<b>Single sign-on</b>	Maak uw belangrijkste zakelijke tools toegankelijk voor uw medewerkers met vereenvoudigde toegang tot drie toepassingen in de cloud.
<b>Families as a Benefit</b>	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:

<b>LastPass Single Sign-On – geavanceerd</b>	LastPass Single Sign-On zorgt ervoor dat uw medewerkers zich op de meest eenvoudige manier 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 alles in hetzelfde programma dat ze al vertrouwen voor hun wachtwoorden. 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.
--	---

