



LastPass voor professionele dienstverleners

Professionele dienstverleners werken in allerlei sectoren: boekhouding en accountancy, consultancy, techniek en architectuur, IT, juridische dienstverlening, marketing en meer.

Een onprofessionele omgang met wachtwoorden is een probleem voor professionele dienstverleners

De kenniswerkers in de professionele dienstverlening werken vaak op inhuurbasis. Daarbij krijgen ze over het algemeen toegang tot de systemen van hun klanten. Die toegang maakt ze een geliefd doelwit van hackers: die veroveren met één geslaagde aanval vaak de gegevens van meerdere organisaties.

Onveilige en gelekte aanmeldingsgegevens zijn de makkelijkste aanvalsroute voor cybercriminelen. Gegevenslekken, diefstal van intellectuele eigendommen, financiële fraude en reputatieschade liggen op de loer. Voor klanten veroorzaakt een gegevenslek vertrouwensverlies, hoge kosten en vaak ook blootstelling van gevoelige gegevens. Eén lek kan meerdere bedrijven en sectoren raken.

Maar ook afgezien van de veiligheidsrisico's vormt digitaal toegangsbeheer een uitdaging voor de sector. Gegevensuitwisseling is inherent aan het werk, zowel binnen teams als met externen: denk aan gedeelde logins voor toepassingen en accounts, maar ook aan interne databases met waardevolle informatie. Organisaties moeten toegang effectief kunnen verlenen, beheren en intrekken, want anders leidt dit al snel tot productiviteitsverlies en digitale kwetsbaarheid.

74% van alle gegevenslekken is te herleiden tot een menselijke factor, inclusief het gebruik van onveilige aanmeldingsgegevens, social engineering en vergissingen.

10% van de cybercriminaliteit in de professionele dienstverlening is het gevolg van een willekeurige fout.

Handig en veilig toegangsbeheer



LastPass loopt wereldwijd voorop als vertrouwde leverancier van software voor wachtwoord- en identiteitsbeheer, en heeft unieke mogelijkheden om professionele dienstverleners te helpen met het beheer van al hun aanmeldingsgegevens. De software is speciaal gemaakt voor de behoeften van werkplekken met veel accounts en systemen, en veel onderlinge samenwerking. Met LastPass kunnen organisaties sterke wachtwoorden maken, opslaan en beheren, en veilig toegang delen waar nodig. De handige interface versterkt de beveiliging en verhoogt tegelijkertijd het gebruiksgemak. Met een centraal en veilig platform voorkomt LastPass onveilige wachtwoordpraktijken en blokkeert het ongeoorloofde toegang tot gevoelige bedrijfs- en klantgegevens.



LastPass ondersteunt de onderlinge samenwerking, omdat het collega's en externen in staat stelt om veilig en gecontroleerd toegang te delen. Eenvoudig toegangsbeheer zorgt ervoor dat iedereen werkt op basis van "need-to-know", en toegang kan automatisch worden ingetrokken zodra dat nodig is. Met geavanceerde rapporten en tools voor meer inzicht ondersteunt LastPass bovendien de compliance en kunnen beheerders het gebruik van aanmeldingsgegevens effectief monitoren. Zo kunnen professionele dienstverleners soepel en veilig samenwerken, zowel bedrijfsintern als voor hun klanten.



Voordelen van LastPass voor professionele dienstverleners

De makkelijkste, meest betaalbare en meest betrouwbare manier voor professionele dienstverleners om hun cyberrisico en operationele risico terug te dringen, is door hun wachtwoordbeheer bedrijfsbreed te organiseren met LastPass.

Beveiliging	Voorkom ongeoorloofde toegang	Houd hackers en ongeoorloofde gebruikers buiten uw toepassingen, online accounts, gevoelige gegevens en systemen.
	Blokkeer overnames van uw accounts en gegevenslekken	Zorg dat online accounts en toepassingen betrouwbaar toegankelijk zijn voor geautoriseerde gebruikers en dat aanmeldingsgegevens beschermd blijven.
	Krijg schaduw-IT onder controle	Krijg zicht op toepassingen die medewerkers gebruiken zonder toestemming en beheer van de IT-afdeling. Voorkom onnodige abonnementen en volg wie er aanmeldingsgegevens deelt voor welke accounts. Beheer de toegangsrechten en herken kwetsbaarheden in het systeem.
	Breid veilig toegangsbeheer uit	Integreer naadloos met identiteitsproviders als Microsoft Entra en verbeter het gebruikersbeheer van inhuur tot aan vertrek.
Naleving	Voldoe aan voorwaarden van cyberverzekeraars	Toon eenvoudig aan dat u voldoet aan de vereisten die cyberverzekeraar stellen aan wachtwoord- en toegangsbeheer.
	Ondersteun compliance	Voldoe aan de vereisten van wet- en regelgeving, onder andere voor de AVG, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA en SOX, en voor kaders voor cyberbeveiliging zoals NIST, CISA, Zero Trust, en NERC-CIP.
	Garandeer de beveiliging die partners vereisen	Voldoe aan de strenge beveiligingsvereisten van partners, met krachtige systemen voor toegangscontrole, regels voor het delen van wachtwoorden, sterke verificatiemechanismen en nuttige rapportages.
Optimalisatie	Bied iedereen een intuïtieve gebruikservaring	Profiteer van uitgebreide instelbare beleidsregels, flexibele machtigingen, gedetailleerde rapportages, en verschillende opties voor de verificatie.
	Standaardiseer de wachtwoordbeveiliging	Vereenvoudig het wachtwoordbeheer voor alle medewerkers binnen de organisatie.
	Verlaag de werkdruk voor de helpdesk	Verlos de helpdesk van problemen door aanmeldingsgegevens, zoals vergeten wachtwoorden en geblokkeerde accounts.
Samenwerking	Stroomlijn teamwerk met gedeelde toegang	Maak het makkelijk om wachtwoorden en andere informatie zowel intern als extern veilig te delen, voor meer productiviteit en efficiency voor partners, freelancers en thuiswerkers.
	Optimaliseer aanname & gebruik	Bevorder de aanname en het gebruik door medewerkers met een intuïtieve, gebruiksvriendelijke interface, die alle taken rondom wachtwoordbeheer makkelijker maakt.
	Bouw een veiligheidscultuur	Zorg ervoor dat alle medewerkers actief bijdragen aan een hoog veiligheidsbewustzijn en de organisatie beschermen tegen veel voorkomende bedreigingen rondom gestolen of gelekte aanmeldingsgegevens.