



LastPass voor advocatenkantoren en juridische dienstverleners

De juridische dienstverlening werkt voor particulieren, bedrijven en overheidsinstanties. Juristen stellen documenten op, geven advies, vertegenwoordigen klanten in de rechtbank en verwerken transacties.

Los een zwakke beveiliging op met goed beheer van aanmeldingsgegevens

Juridische dienstverleners werken als vertrouwde adviseurs met extreem gevoelige klantgegevens, van financiële documenten tot aan intellectuele eigendomsrechten en juridische strategieën. Met deze materialen zijn ze een aantrekkelijk doelwit voor hackers, die kwetsbaarheden in de beveiliging misbruiken om ongeoorloofd toegang te krijgen. Gestolen, gekraakte of gelekte aanmeldingsgegevens kunnen leiden tot gegevenslekken, fraude en reputatieschade. Voor klanten veroorzaken dit soort incidenten wantrouwen. Vertrouwelijke gegevens kunnen in de verkeerde handen vallen, en vaak zijn de financiële en juridische consequenties groot.

Naast het beveiligingsrisico is de omgang met digitale toegang ook een operationele uitdaging voor juridische kantoren. Collega's moeten regelmatig onderling toegang delen tot dossiers, klantenportalen en databases. Zonder goede tools voor het beheer is het al snel onmogelijk om te volgen wie er wanneer toegang heeft tot welke gegevens. Dat is inefficiënt en onveilig, om van de compliance nog maar te zwijgen. Regelgeving vanuit de overheid en de branche vereist een sterke gegevensbescherming. Dat betekent dat kantoren een effectief systeem nodig hebben voor wachtwoord- en toegangsbeheer om klantgegevens veilig te houden.

42% van de kantoren met 100 of meer medewerkers heeft al eens te maken gehad met een gegevenslek.

- American Bar Association

Moderne toegang voor de juridische praktijk van nu



LastPass loopt wereldwijd voorop als vertrouwde leverancier van software voor wachtwoord- en identiteitsbeheer, en heeft unieke mogelijkheden om juridische professionals te helpen met hun cyberbeveiliging en toegangsbeheer. Met LastPass kunnen kantoren aanmeldingsgegevens veilig aanmaken, opslaan, beheren en delen, met handige toegang zonder concessies aan de vertrouwelijkheid. Zo blijven gevoelige klantgegevens goed beschermd. LastPass is gemaakt voor sectoren die afhankelijk zijn van vertrouwen en discretie. Het levert centraal beheer van aanmeldingsgegevens en verlaagt zo het risico op ongeoorloofde toegang en gegevenslekken door een slechte omgang met wachtwoorden.



Kantoren hebben te maken met strenge compliancevereisten, maar tegelijkertijd moeten hun juristen soepel kunnen samenwerken met collega's, klanten en externe partners. LastPass maakt het makkelijk om overal in te loggen en veilig toegang te delen, met een cloudplatform dat een beveiligingsbeleid op maat afdwingt, activiteiten rondom aanmeldingsgegevens monitort en gedetailleerde rapporten levert voor audits. Kantoren kunnen zo eenvoudig aantonen dat ze voldoen aan de vereisten van kaders, standaarden en regelgeving.



Met LastPass kunnen kantoren hun klanten beschermen en vertrouwen behouden, met een beveiliging die aansluit bij de dagelijkse realiteit van hun werk.



Voordelen van LastPass voor advocatenkantoren en juridische dienstverleners

De makkelijkste, meest betaalbare en meest betrouwbare manier voor juridische professionals 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.
	Breid veilig toegangsbeheer uit	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.