LastPass pour les cabinets d'avocats

Les cabinets d'avocats fournissent divers services juridiques aux particuliers, aux entreprises et aux entités gouvernementales, dont des services de conseil, de représentation, de rédaction de documents juridiques et de gestion des transactions.

Sécurité ? Affaire classée : gérer les identifiants en toute confiance.

Les cabinets d'avocats fonctionnent en tant que conseillers de confiance qui gèrent des informations hautement sensibles sur leurs clients, qu'il s'agisse de données financières, de propriété intellectuelle ou de stratégies juridiques. Ces responsabilités en font des cibles privilégiées des cybercriminels qui exploitent les vulnérabilités pour obtenir un accès illicite. Les identifiants piratés ou volés peuvent entraîner des fuites de données, des détournements financiers et une atteinte à la réputation. Pour les clients, de tels incidents peuvent ruiner la confiance, exposer des informations confidentielles. et avoir des conséquences juridiques et financières.

En plus des risques de sécurité, les cabinets d'avocats doivent gérer des problèmes de gestion des accès liés à la collaboration. Les équipes juridiques partagent des accès aux dossiers, portails clients et bases de données de référence entre avocats, assistants juridiques et partenaires externes. Sans outils pour gérer, surveiller et révoquer les accès en toute sécurité, les firmes risquent de cumuler inefficacités, failles de sécurité et infractions réglementaires. Alors que les réglementations gouvernementales et sectorielles imposent des normes de protection des données plus strictes, les cabinets d'avocats sont obligés d'assurer une gestion efficace des identifiants et des accès afin de protéger les données des clients, et pour assurer la conformité.

42 % des cabinets d'avocats de plus de 100 employés ont connu une fuite de données

- American Bar Association

Gestion sécurisée des accès et des identifiants pour les cabinets d'avocat d'aujourd'hui

Un leader de la gestion des mots de passe et des identités, LastPass est particulièrement bien positionné pour résoudre les problèmes de sécurité et d'accès particuliers rencontrés par les cabinets d'avocats. En protégeant les données sensibles sur les clients, LastPass permet aux cabinets de créer, stocker, partager et protéger les identifiants en toute sécurité, assurant une disponibilité transparente sans sacrifier la confidentialité. Conçu pour les secteurs d'activité basés sur la confiance et la discrétion, LastPass fournit une gestion centralisée des identifiants qui limite les risques de fuites et d'accès illicites liés aux mots de passe.

Les cabinets d'avocats doivent concilier des exigences de conformité strictes et de collaboration efficace entre les avocats, le personnel et les partenaires externes. LastPass simplifie l'accès et le partage sécurisé grâce à une plate-forme dans le cloud qui impose des règles sur mesure, surveille l'activité liée aux identifiants et fournit des rapports détaillés à des fins d'audit. Les firmes peuvent facilement documenter le respect des cadres, normes et réglementations.

Avec LastPass, les cabinets d'avocats peuvent protéger leurs clients, préserver la confidentialité et fonctionner en toute confiance, offrant une sécurité aussi solide que leurs argumentaires.

Avantages de LastPass pour les cabinets d'avocats

Le moyen le plus simple, abordable et fiable pour les cabinets d'avocats de diminuer radicalement les risques de cyberattaques et opérationnels consiste à standardiser la gestion des mots de passe avec LastPass à l'échelle de l'entreprise.

Sécuriser	**Empêcher les accès non autorisés**	Empêchez les acteurs malveillants et les utilisateurs non autorisés d'accéder aux applications, aux comptes en ligne et aux informations et systèmes sensibles.
	Stopper les détournements de comptes et les fuites de données	Assurez la fiabilité et l'accessibilité des comptes et applications en ligne, et la confidentialité des identifiants.
	Contrôler le shadow IT	Donnez aux organisations une visibilité et la maîtrise des applications SaaS non approuvées et surprovisionnées, en permettant aux administrateurs de suivre le partage d'identifiants, de gérer les droits d'accès et de repérer les vulnérabilités.
	Renforcer la gestion sécurisée des accès	Intégrez de manière transparente avec les principaux fournisseurs d'identité (IdP) comme Microsoft Entra, pour améliorer la gestion des utilisateurs tout au long du cycle de vie des employés.
Se conformer	**Répondez aux conditions de cyberassurance**	Simplifiez la tâche aux organisations qui doivent répondre aux exigences de gestion des mots de passe et des accès pour obtenir une cyberassurance.
	Favoriser la conformité	Aide les organisations à répondre aux normes de conformité et réglementaires comme RGPD, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA et SOX, ainsi que les cadres de cybersécurité comme NIST, CISA, Zero Trust et NERC-CIP.
	Répondre aux exigences de sécurité des partenaires	Aide les organisations à respecter les normes de sécurité strictes de partenaires grâce à un contrôle efficace des accès, des règles de partage de mots de passe, des mécanismes d'authentification forte et des rapports exploitables.
Rationaliser	**Offrir une expérience intuitive à chaque utilisateur**	Fournit des centaines de stratégies personnalisables, des autorisations souples, des rapports détaillés et plusieurs options d'authentification, pour devenir un outil indispensable de la pile technologique.
	Renforcer la gestion sécurisée des accès	Simplifiez la gestion des identifiants pour les employés à l'échelle de l'organisation.
	Alléger la frustration du service d'assistance	Diminuez le fardeau du service d'assistance informatique dû aux problèmes de mots de passe, comme les mots de passe oubliés et les comptes verrouillés.
Collaborer	**Maximiser le travail d'équipe grâce au partage**	Rationalisez le partage de mots de passe et d'informations à l'intérieur et à l'extérieur de l'organisation, pour stimuler la productivité et l'efficacité des partenaires, des indépendants et des télétravailleurs.
	Maximiser adoption et l'utilisation	Boostez l'adoption et l'utilisation chez les employés en offrant une interface utilisateur intuitive qui simplifie les tâches de gestion des mots de passe.
	Promouvoir une culture de la sécurité	Aidez les administrateurs à s'assurer que tous les employés contribuent activement à une culture de la sécurité, pour se protéger contre les menaces courantes comme le vol ou le piratage d'identifiants afin d'assurer la responsabilité fiduciaire.