LastPass pour les fabricants

L'industrie manufacturière englobe un énorme éventail de produits essentiels dans des secteurs clés, de l'automobile à la construction, en passant par les cosmétiques, l'agroalimentaire, les produits pharmaceutiques, le textile, le plastique, les machines-outils, etc.

Ajouter la protection par mots de passe aux lignes de production

L'industrie manufacturière dont dépend tant l'infrastructure mondiale est une cible séduisante pour les cybercriminels qui souhaitent perturber les chaînes d'approvisionnement, voler de la propriété intellectuelle ou bloquer l'exploitation. Pour les cybercriminels, le piratage d'identifiants est souvent le moyen le plus simple et efficace d'obtenir un accès illicite aux systèmes sensibles. Une fois connectés, ils peuvent entreprendre tout un éventail d'activités malveillantes, qu'il s'agisse de détourner des comptes, de manipuler les systèmes opérationnels ou encore de dérober des données confidentielles. Les fabricants sont ainsi particulièrement vulnérables, car les enjeux sont énormes, une seule fuite pouvant avoir un effet domino sur toute la chaîne d'approvisionnement.

L'impact d'une cyberattaque sur un fabricant n'est pas limité aux pertes financières immédiates. La perturbation de l'exploitation peut stopper les lignes de production, retarder les expéditions et ternir la réputation de la marque, tandis que le vol de propriété intellectuelle peut conférer un avantage indu à la concurrence. Les conséquences de tels incidents peuvent se propager tout au long de la chaîne d'approvisionnement en affectant tous les intervenants, des fournisseurs de pièces détachées au client final.

En outre, les fabricants sont souvent soumis à des normes gouvernementales très strictes régissant la protection des données, et toute fuite peut ainsi devenir un cauchemar réglementaire et juridique. Plus les fabricants deviennent dépendants de technologies interconnectées, plus il est essentiel de protéger les identifiants afin de minimiser ces risques et de protéger l'intégrité du secteur tout entier.

Les rançongiciels étaient impliqués dans 71 % des incidents, et avec une augmentation des attaques de 125 % par an, les cybermenaces sont désormais considérées comme l'un des trois principaux risques externes pour les fabricants.

Protéger et rationaliser votre entreprise tout entière

Dans l'industrie manufacturière, où il existe souvent un fossé important entre les équipes informatiques et les travailleurs en première ligne, utiliser une solution de gestion des mots de passe dans l'ensemble de l'organisation est l'un des moyens les plus simples et efficaces de diminuer les risques liés aux identifiants. En déployant LastPass dans toute l'organisation, les fabricants peuvent s'assurer que tous les employés, qu'ils soient informaticiens ou travaillent dans l'usine, suivent la même procédure simple et sûre de gestion des mots de passe. Cette approche diminue l'utilisation des identifiants faibles, réutilisés ou mal gérés, qui constituent un point d'accès privilégié pour les cybercriminels.

LastPass fournit une solution dans la cloud facile à utiliser qui simplifie la sécurité des mots de passe pour tous les employés, quel que soit leur niveau en informatique. Il permet la création, le stockage et le partage d'identifiants en toute sécurité, tout en imposant un contrôle strict des accès. En adoptant LastPass à tous les niveaux, les fabricants peuvent combler le fossé de sécurité qui existe entre le personnel informatique et de première ligne, minimiser les vulnérabilités et simplifier la conformité, afin d'améliorer tant la sécurité que l'efficacité opérationnelle.

Les avantages de LastPass pour les fabricants

Le moyen le plus simple, abordable et fiable pour les fabricants 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.