Portrait

de la sécurité informatique chez les PME québécoises

Devolutions

SÉCURITÉ ET TI, MAINTENANT RÉUNIES

Devolutions est fière de dévoiler la toute première édition de son portrait de la sécurité informatique chez les petites et moyennes entreprises (PME) québécoises et plus spécifiquement sur la gestion des accès et des mots de passe.

Le sondage nous apprend que les PME québécoises sont sans aucun doute sensibilisées à l'enjeu de la cybersécurité. Avec les mesures de gouvernance comprises dans la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels à appliquer d'ici septembre 2022, les organisations n'ont d'autre choix que d'en faire une priorité. Cela se manifeste notamment par l'allocation d'un budget plus important en matière de cybersécurité et la mise en place de mesures de protection, ce qui est encourageant.

Néanmoins, ne pas déployer l'ensemble de mesures de protection dites « de base » ne garantit pas une pleine protection des entreprises. Il est essentiel pour elles de rehausser leur protection afin de réduire ou d'éviter les cyberattaques (dont les PME sont, par ailleurs, les principales victimes).

Vous retrouverez d'ailleurs dans ce portrait quelques conseils ainsi que les points de vue de nos experts.

Bonne lecture!

Signé par David Hervieux, président-fondateur de Devolutions

Table des matières

Méthodologie 2

Section 1 3
Des entreprises préoccupées par la cybersécurité

Section 2 10
Des mesures de protection insuffisantes

Section 3 15
Responsabilités et bonnes pratiques incomprises

À propos de Devolutions 20

Nous joindre 21

Méthodologie

Ce sondage Web a été réalisé de septembre 2021 à février 2022 par la firme SOM, en collaboration avec Devolutions et des organisations du secteur des TI, auprès de 151 professionnels des TI et décideurs provenant de PME québécoises.

Section 1

DES ENTREPRISES PRÉOCCUPÉES PAR LA CYBERSÉCURITÉ

Le sondage nous démontre que les entreprises sont soucieuses de leur cybersécurité. De fait, 85 % des organisations sondées se disent préoccupées par la confidentialité et la sécurité des données de leur entreprise.

Ce sont, dans l'ordre, les rançongiciels (73 %), l'hameçonnage (68 %) et les logiciels malveillants (66 %) qui s'avèrent être les cybermenaces les plus redoutées.

NIVEAU DE PRÉOCCUPATION DES ENTREPRISES

EN LIEN AVEC LA CONFIDENTIALITÉ ET LA SÉCURITÉ DE LEURS DONNÉES

85%
très ou assez préoccupées

15%
peu ou pas préoccupées

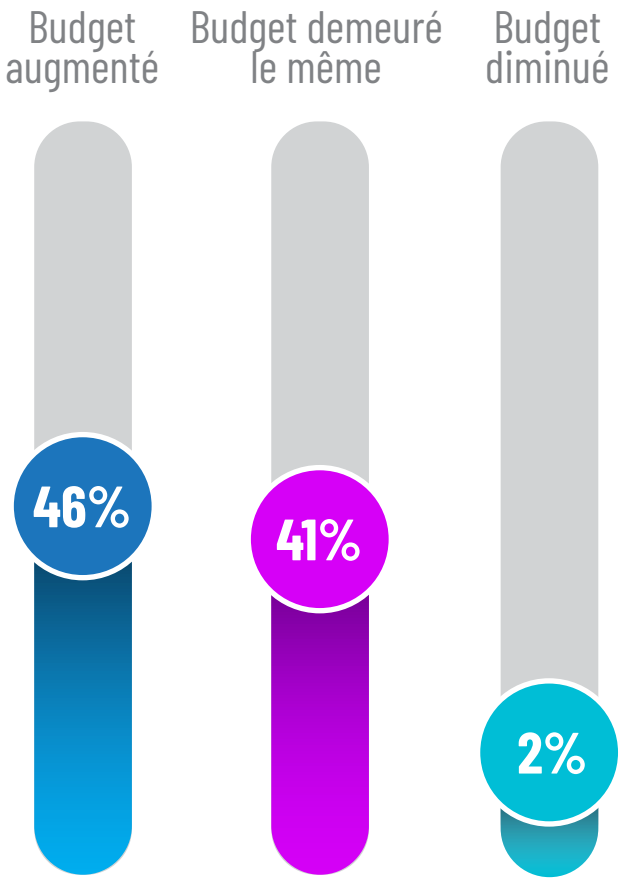
« Il y a réellement au Québec une sensibilisation accrue et une importance plus grande accordée à la cybersécurité dans les dernières années. Pensons à l'adoption de la loi 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, de même que l'annonce de la création d'un ministère de la Cybersécurité et du Numérique. »

- David Hervieux, président-fondateur de Devolutions.

Cette priorité se manifeste notamment par l'allocation d'un budget plus élevé sur le plan de la cybersécurité.

À cet égard, un peu plus de la moitié des entreprises québécoises ont augmenté leurs dépenses en matière de cybersécurité au cours de la dernière année.

LES DÉPENSES TOTALES EN MATIÈRE DE CYBERSÉCURITÉ ONT CHANGÉ AU COURS DE L'ANNÉE DERNIÈRE

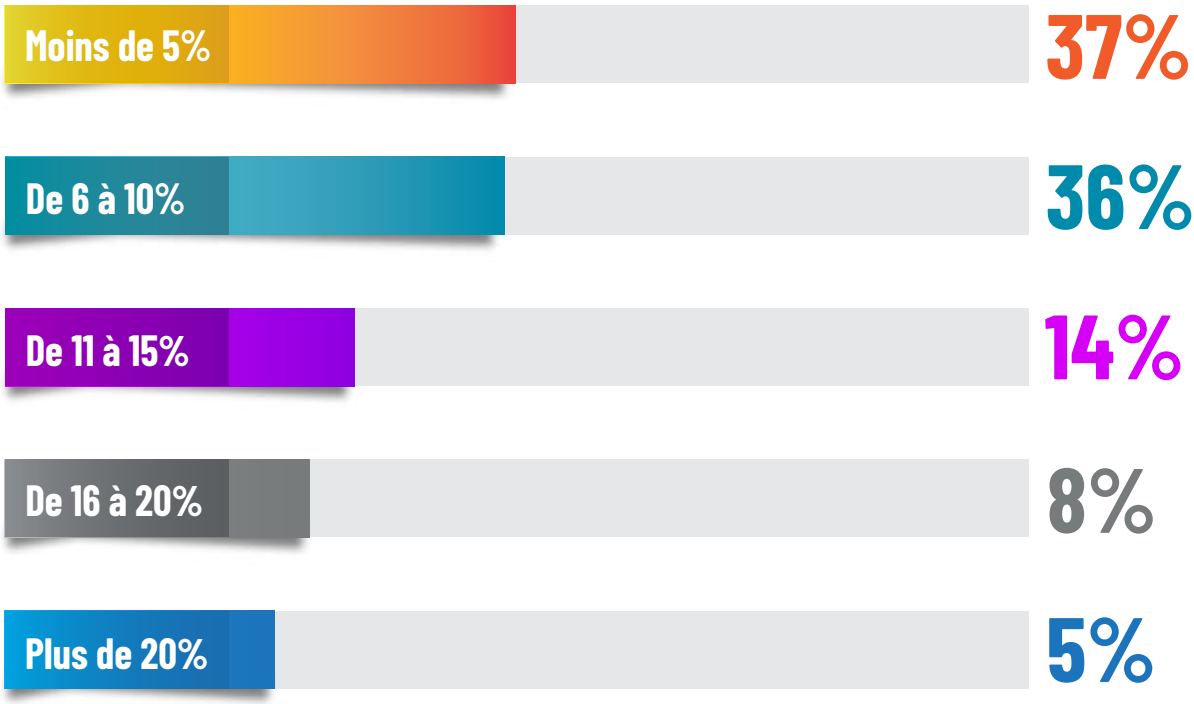


Bien que la hausse des investissements prévus soit encourageante, **le tiers des organisations (37 %) alloue moins de 5 % de leur budget TI en cybersécurité.**

Le niveau de sécurité d'une organisation ne se mesure pas qu'à son budget, mais également par la constance de son approche. Idéalement, une PME devrait investir un budget moyen de 7 à 14 % des dépenses TI pour sa cybersécurité, mais le plus important, c'est de maintenir des efforts au fil du temps en priorisant les risques et opportunités clés qu'elle doit gérer

- Martin Lemay, chef de la sécurité.

BUDGET RÉSERVÉ À LA CYBERSÉCURITÉ EN POURCENTAGE DU BUDGET TOTAL EN TI



Les PME craignent avec raison les cyberattaques.

L'inquiétude évoquée ci-haut a bien lieu d'exister alors que la moitié des répondants affirme que leur entreprise a été victime d'un cyberincident au cours de la dernière année.

CYBERATTAQUES DONT LES ENTREPRISES ONT ÉTÉ VICTIMES DANS LA DERNIÈRE ANNÉE

Hameçonnage

56%

Logiciels malveillants ou virus

42%

Rançongiciels

27%

16% Menaces internes intentionnelles ou non

14% Vulnérabilités infonuagiques

12% Logiciels tiers

Section 2

DES MESURES DE PROTECTION INSUFFISANTES

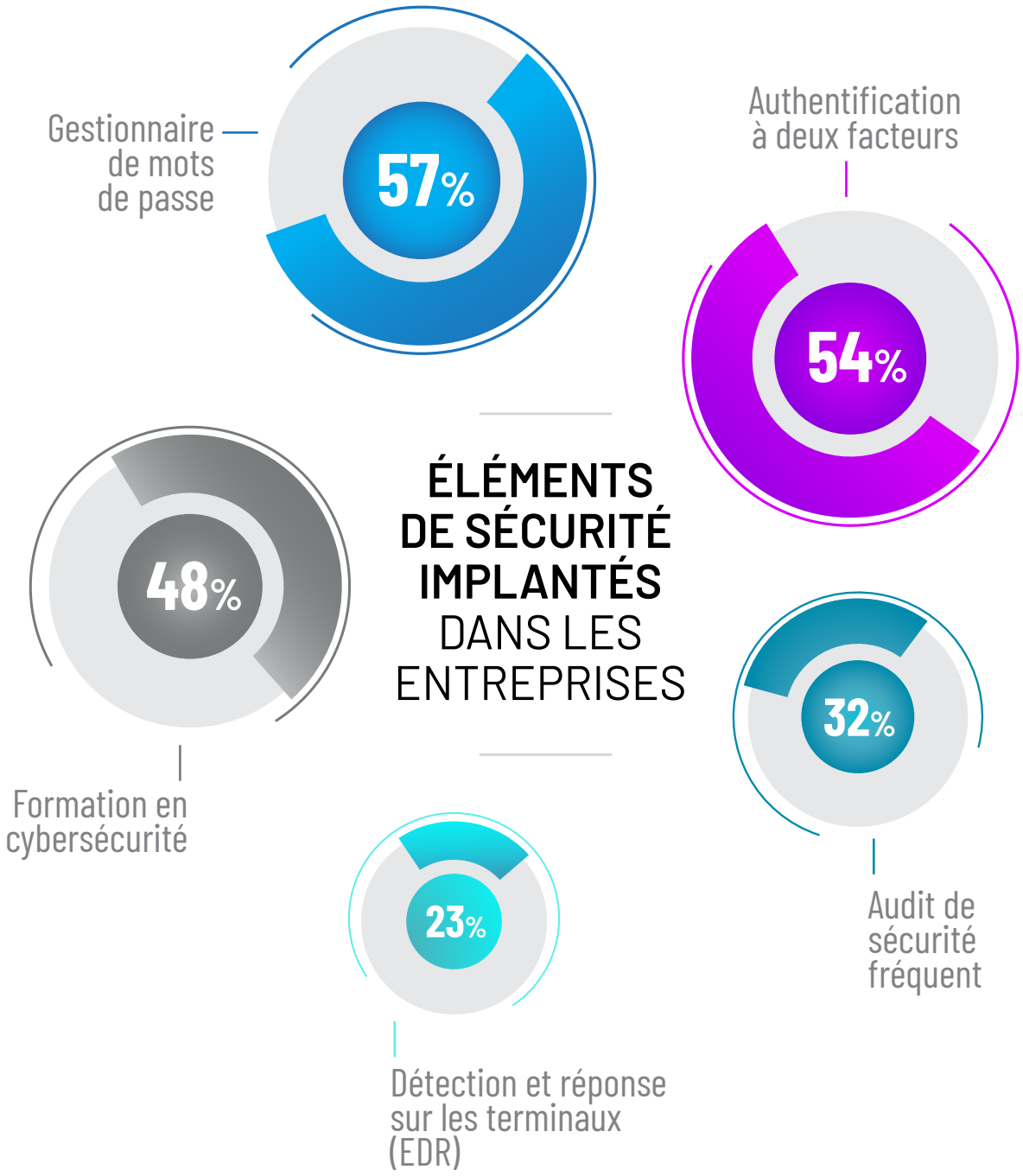
Près de neuf entreprises sondées sur dix estiment avoir un bon niveau de protection contre les cyberattaques alors que l'on constate une faible adoption de mesures de contrôle considérées « de base » comme un gestionnaire de mots de passe (57 %), l'authentification à deux facteurs (54 %), la formation en cybersécurité (48 %) et un audit de sécurité fréquent (32 %).

Néanmoins, **seulement 23 % des répondants ont mis en place l'ensemble de ces mesures fondamentales pour maximiser leur sécurité.**

Par ailleurs, près d'une entreprise sur cinq omet de révoquer l'accès aux anciens employés qui conservent ainsi des informations confidentielles sur l'organisation. Bien qu'il s'agisse d'une faible proportion, elle n'en demeure pas moins préoccupante selon les experts de Devolutions.

Force est de constater que les mesures déployées par les entreprises québécoises sont inadéquates pour assurer la protection optimale de leurs données malgré leur souci pour leur cybersécurité. Ce portrait nous permet d'ailleurs de constater que les PME québécoises sont à la traîne concernant l'adoption de certaines mesures de protection.

- **Martin Lemay**, chef de la sécurité.



ÉLÉMENTS DE SÉCURITÉ IMPLANTÉS DANS LES ENTREPRISES

ENTREPRISES QUI APPLIQUENT
UNE POLITIQUE FORMELLE
POUR RÉVOQUER L'ACCÈS AUX COMPTES DES ANCIENS EMPLOYÉS

oui
82%

non
18%

« Lorsque je constate les résultats mentionnés ci-dessus, je suis préoccupé par le niveau de préparation des entreprises à se conformer aux nouvelles mesures de gouvernance qui devront être appliquées à partir de septembre 2022 dans le cadre des modifications récemment apportées à la Loi sur la protection des renseignements personnels dans le secteur privé. »

- **Guillaume Beaupré**, directeur, Affaires juridiques et protection des renseignements personnels.

Section 3

RESPONSABILITÉS ET BONNES PRATIQUES INCOMPRISES

Près de trois organisations sur quatre (70 %) croient que les entreprises et les utilisateurs finaux, en l'occurrence les employés, partagent le même degré de responsabilité lors d'une brèche de données alors que cette responsabilité relève majoritairement de l'employeur.

Ces entreprises auraient donc tout intérêt à former davantage leur personnel. Néanmoins, seulement la moitié (51 %) des organisations offre une formation en cybersécurité selon le sondage.

LES ENTREPRISES ET LES UTILISATEURS FINAUX PARTAGENT LE MÊME DEGRÉ DE RESPONSABILITÉ LORS D'UNE BRÈCHE

Très ou assez en accord

75%

Peu ou pas du tout en accord

18%

« Les utilisateurs finaux ne partagent pas le même degré de responsabilité que l'organisation dans la prévention, la détection et la réponse à une brèche de données. Cependant, ils ont assurément leurs propres responsabilités à respecter comme le respect des politiques, des normes et des procédures internes en matière de sécurité et de protection des renseignements personnels. La négligence est rarement tolérée et entraîne des sanctions. Il est de la responsabilité de l'organisation d'établir ces politiques, normes et procédures, tout en implantant les incitatifs et la formation requis pour leur réussite. »

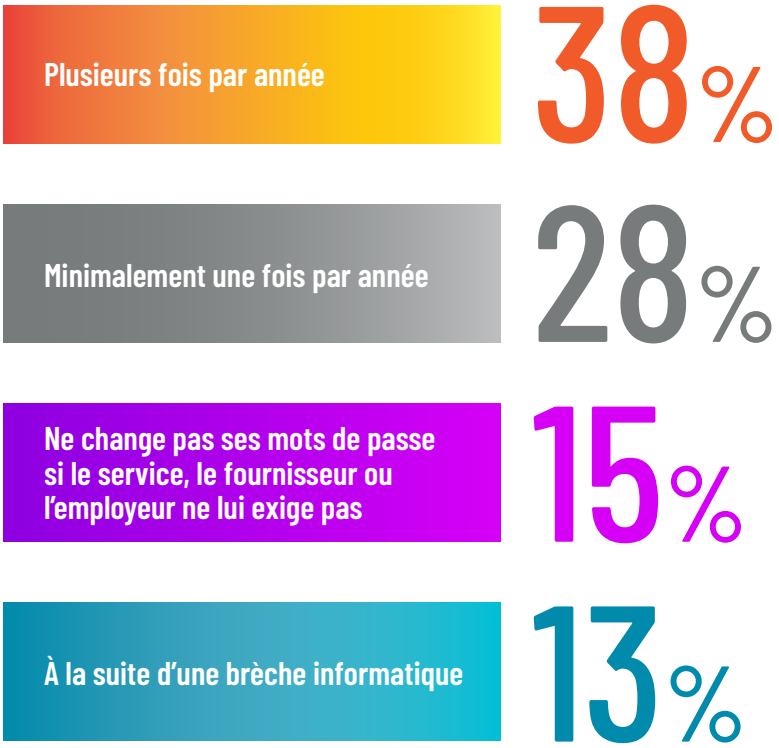
- Martin Lemay, chef de la sécurité

Plus de la moitié des répondants changent régulièrement leur mot de passe au travail, tel que le démontre le tableau ci-dessous.

Si cela peut sembler être une bonne pratique, cette procédure est plutôt déconseillée.

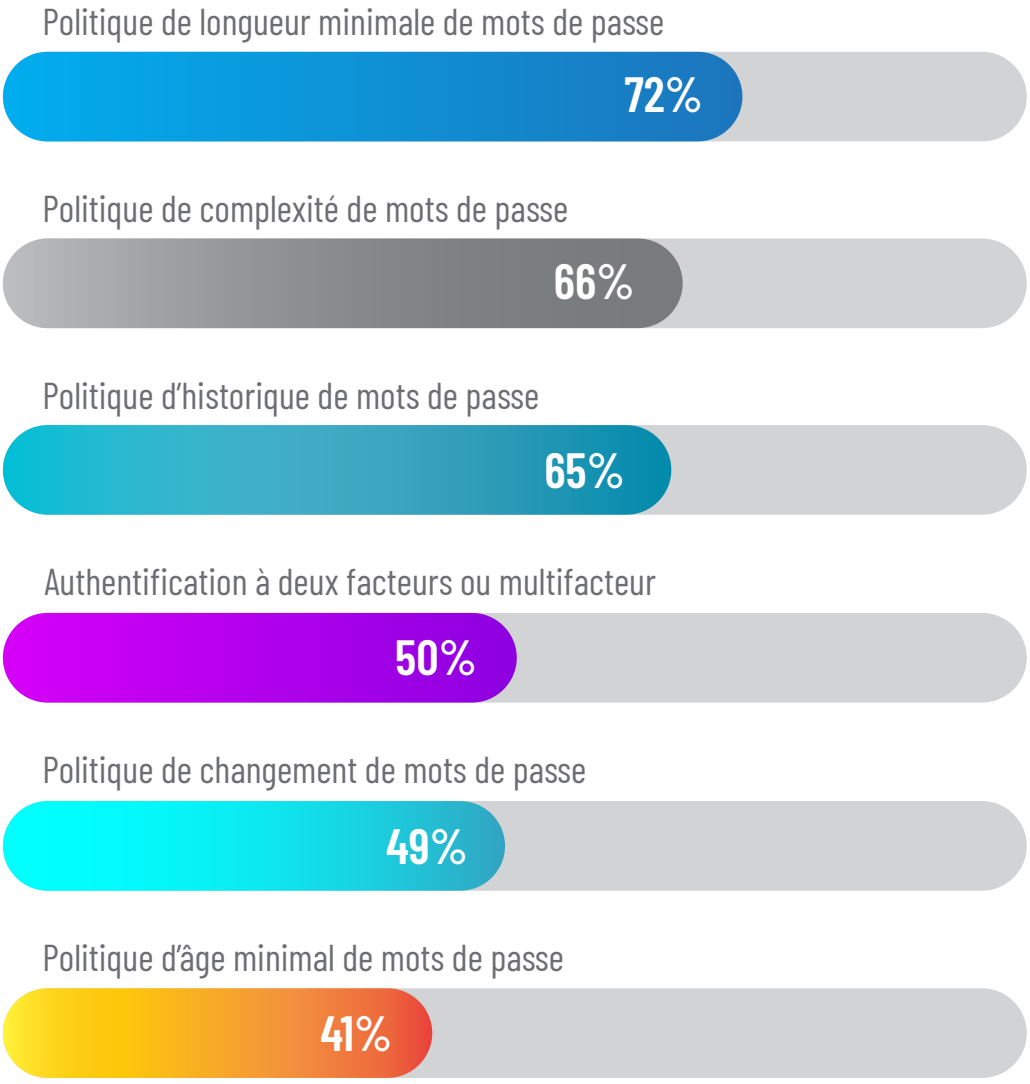
Par le passé, la Norme de sécurité de l'industrie des cartes de paiement (PCI DSS) recommandait de modifier son mot de passe après 90 jours. Toutefois, le National Institute of Standards and Technology a réagi en conseillant aux entreprises de modifier leurs accès seulement à la suite d'une brèche puisque les usagers ont tendance à utiliser des mots de passe similaires (e.g. Mai2022, Janvier2022, Octobre2021, ...), lesquels peuvent être facilement devinés par les pirates informatiques.

FRÉQUENCE DE CHANGEMENT DES MOTS DE PASSE POUR LES COMPTES PROFESSIONNELS



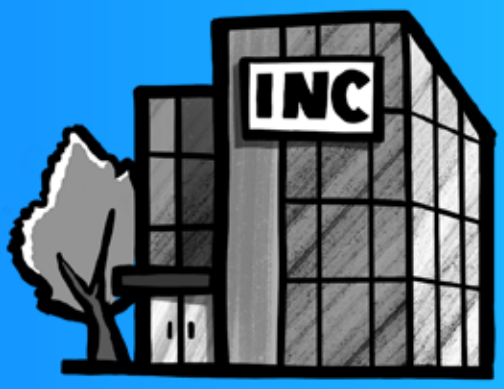
Le tableau suivant présente les différentes politiques et pratiques mises en place par les PME québécoises.

POLITIQUES ET PRATIQUES LIÉES AUX MOTS DE PASSE UTILISÉES PAR L'ENTREPRISE



Devolutions

Établie au Québec depuis 2010 et présente dans plus de 140 pays avec plus de 800 000 utilisateurs principalement au Canada, aux États-Unis, en Allemagne, en Australie, en France, aux Pays-Bas et au Royaume-Uni, Devolutions est aux premières loges de l'état de la cybersécurité des entreprises québécoises et ailleurs dans le monde.



L'entreprise propose des solutions de gestion de bureau à distance, de mots de passe et d'accès privilégiés ainsi que de cybersécurité, spécialement conçues pour aider les petites et moyennes entreprises ainsi que les grandes organisations. Devolutions aide ses clients à gérer efficacement leurs infrastructures technologiques, à renforcer la sécurité de leurs systèmes et à augmenter la productivité de leurs équipes. En 2019, Devolutions a reçu le prix *Deloitte Technology Fast 500™* en reconnaissance de sa croissance rapide, de son esprit entrepreneurial et de ses innovations remarquables.

Devolutions

Comment nous joindre

Pour consulter l'un de nos experts, pour toute question ou demande d'essai gratuit, veuillez communiquer avec nous :

Par courriel : sales@devolutions.net

Par téléphone : +1 844 463.0419

Par clavardage sur notre site Web : devolutions.net/fr