Stratégies de sécurisation du travail d'équipe et de la collaboration à distance

Dropbox

+

Insérer logo ici

Introduction

La technologie cloud a joué un rôle essentiel dans l'évolution du télétravail et de la collaboration entre les équipes sur site et à distance. De plus en plus d'employés travaillent aujourd'hui de chez eux, rendant la collaboration à distance plus essentielle que jamais. Longtemps attendu, le bouleversement numérique a enfin eu lieu, et la transformation numérique suit son cours dans tous les secteurs d'activité et les entreprises de toute taille.

Les équipes distribuées s'accompagnent de nouveaux défis, notamment en matière de sécurité. Dans cette nouvelle ère du travail, il est crucial que les données, les équipes et les appareils soient protégés en toutes circonstances. Les entreprises qui font appel à des solutions telles que Dropbox doivent trouver un juste équilibre entre workflows distribués et sécurité. Lorsque vous simplifiez la collaboration, vous devez également penser à gérer les risques liés au cloud. Les stratégies de gestion des risques visent à assurer la confidentialité de la propriété intellectuelle, l'intégrité des données stockées et partagées, et surtout la disponibilité des données pour garantir la continuité de l'activité non seulement pour les employés, mais aussi pour tout l'écosystème de fournisseurs. Lorsque la sécurité n'est pas intégrée dans la solution cloud, il est plus difficile pour les entreprises de collaborer efficacement tout en protégeant les données internes et externes.

Mais si les solutions cloud doivent être les plus sécurisées possibles, elles doivent également être faciles à utiliser. Parce qu'ils utilisent des applications grand public depuis des décennies, les employés ont envie de solutions aussi simples à prendre en main qu'un navigateur Web. S'ils peinent à adopter une solution, ils n'hésiteront pas à utiliser leur propre technologie qui ne sera pas toujours aussi sécurisée que la solution approuvée par l'entreprise.

Cet eBook présente les fonctionnalités de sécurité des produits Dropbox et décrit l'engagement de la marque en matière de confidentialité et de transparence, ainsi que les politiques internes et les mesures de conformité réglementaire qui font de Dropbox la solution de sécurité de choix pour toutes les entreprises.

Pour obtenir une description technique et complète des fonctionnalités de sécurité, reportez-vous au livre blanc Dropbox Business et la sécurité.

Présentation du programme de sécurité

Les équipes ne devraient pas avoir à se préoccuper de la sécurité de leurs programmes de collaboration. L'essentiel pour elles est que la technologie fonctionne. Les équipes informatiques n'ont pas cette chance : elles doivent tenir compte des risques liés à la sécurité. La pandémie a entraîné un boom du télétravail, mais aussi des cyberattaques : 91 % des entreprises ont enregistré une hausse des cyberattaques lorsque la majorité de leurs employés travaillaient à domicile.

Dans un tel contexte, les équipes informatiques ont besoin d'outils pour anticiper et prévenir les failles de sécurité. Et les entreprises doivent aussi respecter des règles et des directives de conformité. L'approche Dropbox répond à ces deux exigences en combinant les normes les plus reconnues avec des mesures de conformité adaptées aux besoins des clients.

Les produits Dropbox reposent sur le guide de confiance Dropbox qui promeut une approche globale de la sécurité basée sur plusieurs niveaux de protection et sur le concept "zero trust". Celui-ci implique l'identification et la vérification de chaque composant, afin que les employés aient uniquement accès à ce dont ils ont besoin et que les données héritées ne représentent plus un risque pour la sécurité.

Dropbox inclut des fonctionnalités qui permettent aux équipes de sécurité de mettre en place un écosystème informatique d'entreprise sûr. Les mesures opérationnelles en matière de gouvernance des données, de gestion du personnel, d'équipes et de technologie sont conformes à notre engagement qui vise à garantir la sécurité de vos données.

Deux autres options améliorent les processus et les contrôles de sécurité pour les clients Dropbox : le contrôle avancé des équipes et du contenu, et la gouvernance des données. Le contrôle avancé des équipes et du contenu assure la protection des données, la visibilité, l'auditabilité et le contrôle de la gestion du cycle de vie des utilisateurs. L’option de gouvernance des données offre quant à elle des fonctionnalités telles que l'historique étendu des versions, la conservation des données, la destruction des données et la conservation légale. Ensemble, ces deux options garantissent la gestion et la protection des données de l'entreprise dans le respect des règles de conformité.

Accès aux fichiers et infrastructure

Pour être productifs, les télétravailleurs ont besoin d'une technologie efficace. Ils doivent pouvoir accéder aux fichiers et dossiers requis où qu'ils se trouvent. Et dans un tel environnement, ils devraient également pouvoir y accéder depuis l'appareil de leur choix.

Dropbox relève ces défis : les utilisateurs peuvent à tout moment accéder aux fichiers et aux dossiers à partir des applications de bureau et mobile, du site Web, mais également par l'intermédiaire des applications tierces connectées à Dropbox. Ils bénéficient d'un niveau de sécurité d'entreprise qui leur permet de partager des fichiers en interne et en externe, et de synchroniser les appareils associés lorsque des fichiers sont ajoutés, modifiés ou supprimés.

Infrastructure

Stockage des données de fichiers

Dropbox fournit au département informatique et aux utilisateurs les contrôles d'administration et la visibilité dont ils ont besoin pour sécuriser et gérer efficacement les données. Dropbox stocke essentiellement deux types de données : les métadonnées sur les fichiers (par exemple, la date et l'heure de la dernière modification du fichier) et le contenu des fichiers (blocs de fichiers).

Les métadonnées sont conservées sur les serveurs Dropbox. Les blocs de fichiers sont stockés sur Amazon Web Services (AWS) ou sur Magic Pocket, le système de stockage interne de Dropbox. Composé de logiciels et de matériel propriétaires, le système Magic Pocket a été conçu pour assurer fiabilité et sécurité à ses utilisateurs. Magic Pocket et AWS chiffrent les blocs de fichiers et offrent des niveaux élevés de fiabilité.

Chiffrement

Pour protéger les données en transit entre les applications Dropbox et les serveurs, Dropbox utilise les protocoles SSL/TLS (Secure Sockets Layer/ Transport Layer Security), créant ainsi un tunnel sécurisé protégé par un chiffrement AES (Advanced Encryption Standard) d'au moins 128 bits. Les données en transit entre un client Dropbox (client de bureau, application mobile, API ou site Web) et le service hébergé sont chiffrées au moyen de ces protocoles.

En ce qui concerne les points de terminaison que Dropbox contrôle (applications de bureau et mobile) et les navigateurs récents, le groupe utilise un algorithme renforcé, et prend en charge l'épinglage des certificats et la technologie PFS (Perfect Forward Secrecy). En outre, sur le Web, tous les cookies d'authentification sont marqués comme sécurisés et le dispositif de sécurité HSTS (HTTP Strict Transport Security) est activé avec l'attribut includeSubDomains. Ce ne sont là que quelques-unes des mesures appliquées par les solutions Dropbox pour protéger les fichiers sensibles.

La visibilité du contenu est la clé de la collaboration

Voici quelques-unes des fonctionnalités de sécurité Dropbox :

- Les **alertes et les notifications** permettent aux administrateurs de détecter les comportements suspects en temps réel. Grâce à des alertes envoyées au moment où le comportement se produit, les administrateurs peuvent réagir rapidement pour éviter toute perte de données. D'autres améliorations leur permettent de configurer des seuils d'alerte, de modifier les destinataires des notifications et de déclencher des alertes lorsque des dossiers contenant des fichiers sensibles sont partagés en externe.
- Les **rapports de partage à l'extérieur de l'équipe** affichent une liste de tous les composants partagés en externe. Grâce à cette vue d'ensemble sur les données partagées en dehors de l'entreprise, les administrateurs peuvent identifier et répondre plus rapidement aux activités suspectes.
- La **classification des données** protège les données sensibles. Les administrateurs reçoivent des alertes de protection contre la perte de données par e-mail lorsque des fichiers ou des dossiers contenant des informations sensibles sont partagés en dehors de leur équipe. Les administrateurs Dropbox peuvent activer la classification automatique des données à partir de l'interface d'administration.
- La **destruction des données** permet aux administrateurs de supprimer définitivement les données à une date précise dans le respect des exigences de conservation et de destruction des données. Les administrateurs d'équipe pourront à terme surveiller les opérations grâce à des rapports les informant des suppressions de fichiers à venir.
- Les **différents types d'administrateurs** incluent l'accès à la facturation, le contenu, la conformité, les rapports et la sécurité. Ils permettent aux administrateurs informatiques d'accorder uniquement le niveau d'accès requis à l'interface d'administration.

Visibilité et contrôle

Flux d'activité

Les employés ont besoin d'une interface centrale où consulter l'activité liée aux fichiers et les interactions correspondant à un fichier spécifique. Dropbox enregistre les actions liées aux fichiers dans le flux d'activité de l'équipe, consultable depuis l'interface d'administration. Celui-ci offre des options de filtrage flexibles qui permettent aux administrateurs d'effectuer des enquêtes ciblées sur l'activité des comptes, des fichiers ou des documents Paper. Ils peuvent notamment consulter l'historique complet d'un fichier ou d'un document Paper et afficher toutes les interactions des utilisateurs avec celui-ci, ou voir toutes les activités de l'équipe pour une période donnée.

Les administrateurs peuvent également exporter le flux d'activité au format CSV afin de le présenter à d'autres collaborateurs. Le flux d'activité peut être exporté sous forme de rapport téléchargeable ou encore intégré directement dans des outils de gestion des informations et des événements de sécurité (SIEM) ou d'autres outils d'analyse via des solutions partenaires tierces.

Contrôle des équipes

Chaque entreprise étant différente, les administrateurs disposent de plusieurs outils pour personnaliser Dropbox en fonction des besoins spécifiques de leurs équipes. La solution intègre des outils permettant aux utilisateurs de renforcer la protection de leur compte et de leurs données : l'authentification, la récupération, la journalisation et d'autres fonctionnalités de sécurité sont disponibles dans les différentes interfaces utilisateur de Dropbox.

Quand sécurité rime avec simplicité

La sécurité et la simplicité d'utilisation ne sont pas incompatibles. Les employés souhaitent pouvoir accéder à leurs contenus depuis diverses interfaces sans trop de manipulation. Avec Dropbox, c'est possible.

API

Les employés ont besoin d'accéder à leurs fichiers et données sur l'appareil de leur choix et où qu'ils se trouvent. Dropbox est accessible via plusieurs interfaces, dont les fonctionnalités et paramètres de sécurité traitent et protègent les données utilisateur tout en offrant un accès simple.

Application de bureau

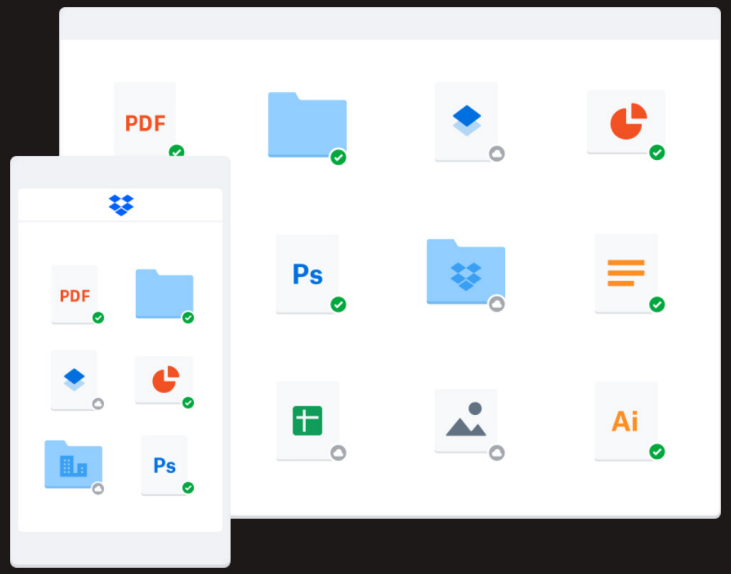
L'application de bureau Dropbox est compatible avec les systèmes d'exploitation Windows et Mac, et offre aux utilisateurs un accès complet à leurs comptes Dropbox. Les fichiers peuvent être consultés et partagés directement depuis le gestionnaire de fichiers de chaque système d'exploitation.

Application mobile

Disponible sur les appareils iOS et Android, l'application mobile Dropbox permet aux utilisateurs d'accéder à tous leurs fichiers, même en déplacement. L'application mobile permet également le stockage local des fichiers pour les rendre accessibles hors ligne.

Web

Cette interface est accessible via n'importe quel navigateur Web. Elle permet aux utilisateurs d'importer, de télécharger, d'afficher et de partager leurs fichiers. L'interface Web leur permet également d'ouvrir les copies locales de leurs fichiers dans l'application par défaut de leur ordinateur.

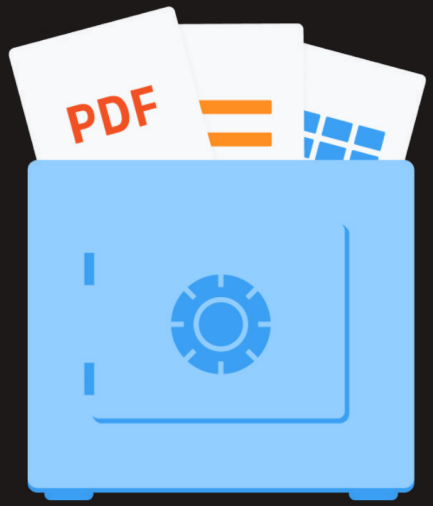


Le guide de confiance Dropbox

Les relations que Dropbox entretient avec des millions de particuliers et d'entreprises à travers le monde reposent sur la confiance. Reconnaissant de la confiance qui lui est accordée, le groupe prend très au sérieux la responsabilité qui est la sienne de protéger vos informations. Afin de mériter votre confiance, il a conçu et continue de développer Dropbox en mettant un accent tout particulier sur la sécurité, la transparence et la conformité.

Dropbox suit une approche multicouche pour sécuriser l'entreprise, l'infrastructure, les applications et les produits qui ont un impact sur votre organisation. Le guide de confiance Dropbox définit un processus d'évaluation des risques. Celui-ci a été conçu pour faire face aux risques relatifs à l'environnement, à l'accès physique, aux utilisateurs, aux tierces parties, aux lois et réglementations applicables, aux obligations contractuelles et aux autres risques susceptibles d'affecter la sécurité, la confidentialité, l'intégrité et la disponibilité des systèmes. Des examens des performances sont réalisés au moins une fois par an.

Pour plus d'informations, consultez la page www.dropbox.com/business/trust.



À propos de <nom du partenaire>

<insérer la présentation du partenaire ici>

À propos de Dropbox

Dropbox est un outil central qui permet de gérer vie personnelle et professionnelle et qui sécurise le travail et la collaboration des équipes. Avec plus de 700 millions d'utilisateurs inscrits dans 180 pays, l'entreprise s'est fixé pour mission de réinventer la façon de travailler. Le siège de Dropbox se trouve à San Francisco, en Californie.

Pour en savoir plus sur notre mission et nos produits, consultez la page experience.dropbox.com.