Dropbox Business et la sécurité

Un livre blanc Dropbox

Dropbox

Sommaire

Présentation

Alors que la transformation numérique suit son cours dans différents secteurs, il est crucial que les données, les équipes et les appareils soient protégés en toutes circonstances. Les organisations qui s'appuient sur des solutions cloud comme Dropbox Business pour mettre en place des workflows à distance et distribués doivent simplifier la collaboration, gérer de manière proactive les risques liés au cloud et mettre en place des contrôles efficaces afin de garantir la confidentialité de leur propriété intellectuelle, l'intégrité des données stockées et partagées, ainsi que la disponibilité des données via des services cloud gérés et résilients.

Plus de 600 000 entreprises et organisations utilisent Dropbox Business pour permettre à leurs équipes distribuées et distantes de collaborer de façon sécurisée. La solution Dropbox Business comprend l'espace de travail intelligent pour la collaboration, ainsi que des fonctionnalités de partage et de synchronisation de fichiers. Nos solutions s'appuient sur une infrastructure de pointe ainsi que sur des fonctionnalités avancées de sécurité d'entreprise, de sécurité des équipes et du contenu, de signature électronique, de transfert sécurisé et de gouvernance des données. Sauf indication contraire, les informations contenues dans ce livre blanc s'appliquent à l'ensemble des produits Dropbox Business (Standard, Advanced et Enterprise) et Dropbox Education. Paper est une fonctionnalité de Dropbox Business et Dropbox Education.

Dropbox Business repose sur le programme de confiance Dropbox. Cette approche globale de la sécurité est basée sur plusieurs niveaux de protection, ce qui est essentiel à l'heure où le télétravail est en pleine mutation.

Ce livre blanc détaille les fonctionnalités de sécurité des produits Dropbox Business, les mesures de sécurité opérationnelles de Dropbox, notre engagement en matière de confidentialité et de transparence, ainsi que les politiques internes, les certifications indépendantes et les mesures de conformité réglementaire qui font de Dropbox la solution de sécurité de choix pour votre organisation.

Sauf indication contraire, les informations contenues dans ce livre blanc s'appliquent à l'ensemble des produits Dropbox Business (Standard, Advanced et Enterprise) et Dropbox Education. Paper est une fonctionnalité de Dropbox Business et Dropbox Education.

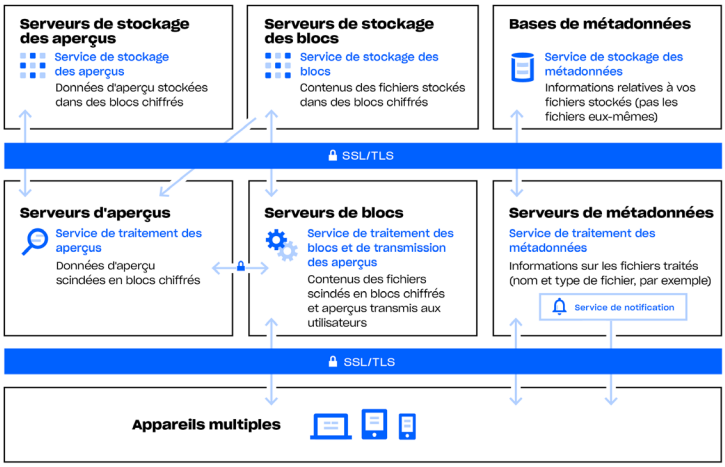
Infrastructure

Simples d'utilisation, nos interfaces reposent sur une infrastructure en arrière-plan qui assure la rapidité et la fiabilité de la synchronisation, du partage et de la collaboration. Pour parvenir à ce résultat, nous améliorons notre produit et notre architecture en permanence afin de garantir les meilleurs taux de transfert, d'optimiser la fiabilité et de nous adapter à l'évolution de l'environnement informatique. Vous découvrirez dans cette section comment les données sont transférées, stockées et traitées de façon sécurisée.

Infrastructure de fichiers

Les utilisateurs Dropbox peuvent accéder à leurs fichiers et à leurs dossiers à tout moment à partir du client de bureau, du site Web et des applications mobiles, mais aussi par le biais d'applications tierces connectées à Dropbox. Tous ces clients se connectent à des serveurs sécurisés pour fournir l'accès aux fichiers, permettre leur partage et mettre à jour les appareils associés lorsque des fichiers sont ajoutés, modifiés ou supprimés.

L'infrastructure de fichiers de Dropbox est composée des éléments suivants :



- ***Serveurs de métadonnées***

  Certaines informations de base sur les données des utilisateurs, que l'on appelle également "métadonnées", sont stockées par un service de stockage dédié. Ce service sert également d'index pour les données stockées dans les comptes des utilisateurs. Les métadonnées comprennent les informations de base sur les comptes et les utilisateurs, telles que les adresses e-mail, les noms d'utilisateur ou les noms d'appareil. Elles incluent également des informations de base sur les fichiers, telles que leur nom et leur type, et sont notamment utilisées par les fonctionnalités d'historique des versions, de récupération et de synchronisation.

- ***Bases de métadonnées***

  Les métadonnées des fichiers sont stockées dans un magasin transactionnel de valeurs clés avec un contrôle de concurrence multi-version. Elles sont partitionnées et répliquées autant de fois que nécessaire pour atteindre les niveaux de performance et de disponibilité attendus.

- ***Serveurs de blocs***

  Pour protéger les données des utilisateurs, Dropbox intègre un dispositif de sécurité unique qui va bien au-delà des systèmes de chiffrement traditionnels. Les serveurs de blocs traitent les fichiers issus des applications Dropbox en les scindant en plusieurs blocs, en chiffrant chacun d'eux à l'aide d'un algorithme renforcé et en synchronisant uniquement les blocs modifiés entre les révisions. Lorsqu'une application Dropbox détecte la présence d'un nouveau fichier ou d'un fichier modifié, elle le signale aux serveurs de blocs. Les blocs de fichiers nouveaux ou modifiés sont ensuite traités et transférés aux serveurs de stockage des blocs, qui servent aussi à transmettre les fichiers et les aperçus aux utilisateurs. Pour en savoir plus sur le dispositif de chiffrement utilisé par ces services pour les données au repos et en transit, consultez la section Chiffrement ci-dessous.

- ***Serveurs de stockage des blocs***

  Le contenu des fichiers des utilisateurs est stocké dans des blocs chiffrés sur les serveurs de stockage des blocs.

  Avant leur transmission, le client Dropbox scinde ces fichiers en blocs afin de les préparer au stockage. Ces serveurs fonctionnent comme un système de stockage CAS (Content-Addressable Storage), chaque bloc de fichier chiffré étant récupéré en fonction de sa valeur de hachage.

- ***Serveurs d'aperçus***

  Les serveurs d'aperçus génèrent un aperçu des fichiers. Il s'agit en réalité d'afficher le fichier d'un utilisateur dans un format différent, mieux adapté pour un affichage rapide sur l'appareil de l'utilisateur. Les serveurs d'aperçus récupèrent des blocs de fichiers auprès des serveurs de stockage des blocs afin de générer un aperçu. Lorsqu'un aperçu est demandé, les serveurs d'aperçus récupèrent l'aperçu mis en cache dans les serveurs de stockage des aperçus et le transfèrent vers les serveurs de blocs. Les aperçus sont ensuite fournis aux utilisateurs par l'intermédiaire des serveurs de blocs.

- ***Serveurs de stockage des aperçus***

  Les aperçus mis en cache sont stockés dans un format chiffré sur les serveurs de stockage des aperçus.

- ***Service de notification***

  Ce service indépendant détecte les modifications apportées aux comptes Dropbox. Il n'implique aucun stockage ni transfert de fichiers ou de métadonnées. Chaque client établit une connexion d'interrogation longue avec le service de notification. En cas de modification d'un fichier dans Dropbox, le service de notification en informe le ou les clients concernés en fermant cette connexion. La fermeture de la connexion indique que le client doit se connecter aux serveurs de métadonnées de manière sécurisée afin de synchroniser les modifications.

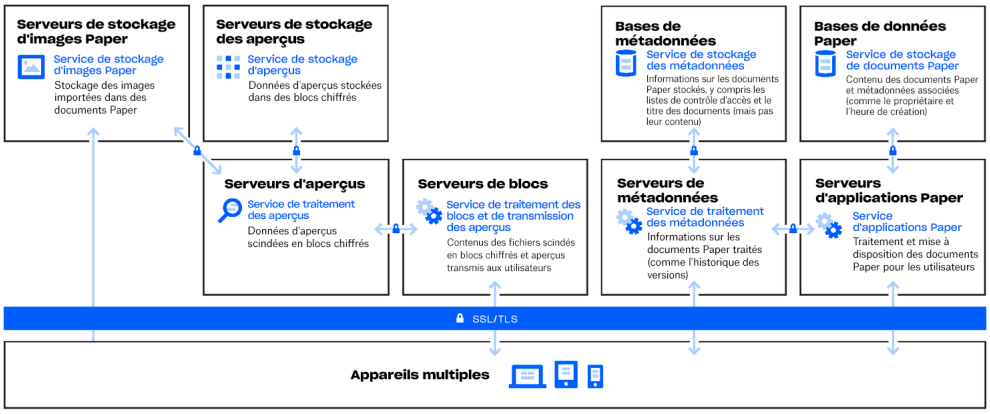
Stockage des données de fichiers

Dropbox stocke principalement deux types de données de fichiers : les métadonnées sur les fichiers (date et heure de la dernière modification d'un fichier, etc.) et le contenu des fichiers en lui-même (blocs de données). Les métadonnées sont conservées sur les serveurs Dropbox, tandis que les blocs de données sont stockés sur AWS ou 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 données au repos et offrent des niveaux élevés de fiabilité. Pour en savoir plus, consultez la section Fiabilité ci-dessous.

Infrastructure Paper

Les utilisateurs Dropbox peuvent accéder à leurs documents Paper à tout moment à partir du site Web et des applications mobiles, mais aussi par le biais d'applications tierces connectées à Dropbox Paper. Tous ces clients se connectent à des serveurs sécurisés pour permettre l'accès aux documents Paper et leur partage, et pour mettre à jour les appareils associés lorsque des documents sont ajoutés, modifiés ou supprimés.

L'infrastructure de Dropbox Paper est composée des éléments suivants :



- ***Serveurs d'applications Paper***

  Les serveurs d'applications Paper traitent les demandes des utilisateurs, effectuent le rendu des documents Paper modifiés et assurent les services de notification. Ils écrivent les modifications utilisateur entrantes dans les bases de données Paper, où elles sont placées sur du stockage persistant. Les sessions de communication entre les serveurs d'applications et les bases de données Paper sont sécurisées à l'aide du protocole HTTPS (Hypertext Transfer Protocol Secure).

- ***Bases de données Paper***

  Le contenu des documents Paper des utilisateurs, ainsi que certaines métadonnées sur ces documents, sont chiffrés dans le stockage persistant des bases de données Paper. Cela inclut les informations sur le document Paper (son titre, son propriétaire, son heure de création et d'autres informations), ainsi que le contenu du document Paper en lui-même, y compris les commentaires et les tâches. Les bases de données Paper sont partitionnées et répliquées autant de fois que nécessaire pour atteindre les performances et les niveaux de disponibilité attendus.

- ***Serveurs de métadonnées***

  Paper utilise les mêmes serveurs de métadonnées que ceux décrits dans le diagramme d'infrastructure Dropbox pour traiter les informations sur les documents Paper, telles que leur historique des versions et l'appartenance à des dossiers partagés. Dropbox gère directement les serveurs de métadonnées, qui sont situés dans les mêmes datacenters tiers.

- ***Bases de métadonnées***

  Paper utilise les mêmes bases de métadonnées que celles décrites dans le diagramme d'infrastructure Dropbox pour stocker les informations sur les documents Paper, telles que le partage, les autorisations et les dossiers associés. Les métadonnées des documents Paper sont stockées dans un service de base de données MySQL. Elles sont partitionnées et répliquées autant de fois que nécessaire pour atteindre les niveaux de performance et de disponibilité attendus.

- ***Serveurs de stockage d'images Paper***

  Les images importées dans les documents Paper sont stockées et chiffrées au repos sur les serveurs de stockage des images Paper. La transmission des données d'image entre l'application Paper et les serveurs de stockage des images Paper s'effectue dans le cadre d'une session chiffrée.

- ***Serveurs d'aperçus***

  Les serveurs d'aperçus génèrent un aperçu des images ajoutées dans les documents Paper et des liens hypertexte qui y sont intégrés. Pour les images ajoutées dans les documents Paper, les serveurs d'aperçus récupèrent les données d'image stockées sur les serveurs de stockage des images Paper via un canal chiffré. Pour les liens hypertexte intégrés dans les documents Paper, les serveurs d'aperçus récupèrent les données d'image et génèrent un aperçu de l'image chiffré, conformément à ce qu'indique la source du lien. Les aperçus sont ensuite transmis aux utilisateurs par l'intermédiaire des serveurs de blocs.

- ***Serveurs de stockage des aperçus***

  Paper utilise les mêmes serveurs de stockage des aperçus décrits dans le diagramme d'infrastructure Dropbox pour stocker les aperçus des images mises en cache. Les blocs d'aperçus mis en cache sont stockés dans un format chiffré sur les serveurs de stockage des aperçus.

Stockage des documents Paper

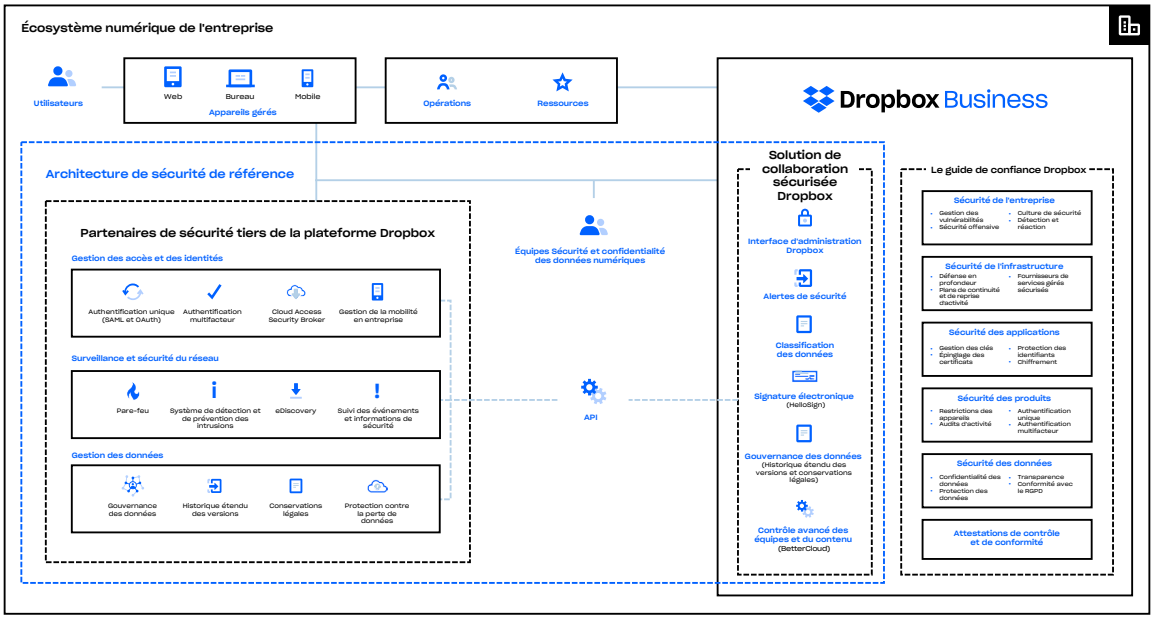
Dropbox stocke principalement les données Paper suivantes : les métadonnées sur les documents Paper (comme les autorisations de partage) et le contenu des documents Paper importés par les utilisateurs. On les nomme communément : données de document Paper. Les images ajoutées dans les documents Paper sont quant à elles nommées : données d'image Paper. Ces deux types de données sont stockés dans Amazon Web Services (AWS), qui offre des niveaux élevés de fiabilité. Les documents Paper sont chiffrés au repos dans AWS. Pour en savoir plus, consultez la section Fiabilité ci-dessous.

Programme de confiance Dropbox

Les relations que nous entretenons avec des millions de particuliers et d'entreprises à travers le monde reposent sur la confiance. Nous sommes très reconnaissants de celle que vous nous accordez et nous prenons très au sérieux la responsabilité qui est la nôtre de protéger vos informations. Afin de mériter votre confiance, nous avons conçu et continuons de développer Dropbox en mettant un accent tout particulier sur la sécurité, la transparence et la conformité.

Le programme de confiance Dropbox définit un processus d'évaluation des risques. Il 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 en savoir plus sur le programme de confiance Dropbox, rendez-vous sur dropbox.com/business/trust.

Nous suivons une approche multiniveau pour sécuriser l'entreprise, l'infrastructure, les applications et les produits qui ont un impact sur votre organisation.



Une sécurité à toute épreuve

Dropbox a mis en place un cadre régissant la sécurité des informations qui décrit l'objectif, les moyens, les principes et les règles de base utilisés pour maintenir une protection efficace. Pour ce faire, nous évaluons les risques et améliorons constamment la sécurité, la confidentialité, l'intégrité et la disponibilité des systèmes Dropbox Business. Nous vérifions et mettons à jour régulièrement nos règles de sécurité, nous formons nos collaborateurs aux questions de sécurité, nous testons la sécurité des applications et du réseau, nous surveillons la conformité avec les règles de sécurité, et nous menons des évaluations internes et externes des risques.

Nos règles

Nous avons défini un ensemble complet de règles de sécurité qui sont mises en application par l'équipe de sécurité et de lutte contre les abus de Dropbox. Ces règles sont examinées et validées au moins une fois par an. Lorsqu'ils rejoignent notre entreprise, les collaborateurs, stagiaires et sous-traitants doivent suivre une formation obligatoire sur la sécurité. Par la suite, ils sont continuellement sensibilisés aux questions de sécurité.

- ***Sécurité des informations***

  Règles applicables aux informations relatives aux utilisateurs et à Dropbox.

- ***Authentification***

  Règles décrivant les méthodes d'authentification devant être utilisées par les employés Dropbox pour accéder aux systèmes d'information et aux données.

- ***Sécurité des appareils***

  Exigences de sécurité minimales pour les appareils mobiles servant à accéder aux informations de l'entreprise.

- ***Contrôle d'accès logique***

  Règles permettant de sécuriser l'accès aux systèmes Dropbox, aux informations des utilisateurs et aux données Dropbox. Ces règles couvrent l'accès aux environnements d'entreprise et de production.

- ***Sécurité des données***

  Règles que nous nous sommes fixées pour protéger les données grâce à des exigences spécifiques en matière de stockage, d'accès et d'utilisation.

- ***Sécurité en déplacement***

  Mesures que doivent prendre les employés Dropbox avant de voyager à l'étranger.

- ***Directives de sécurité pour le service commercial et l'expérience client***

  Règles permettant d'assurer la sécurité des informations sur les utilisateurs, de protéger nos employés et de fournir une assistance à nos utilisateurs.

- ***Sécurité physique***

  Règles nous permettant de maintenir un environnement sécurisé pour les personnes et les équipements Dropbox.

- ***Directives sur la sécurité physique dans les sites de production***

  Règles permettant de gérer l'accès physique aux installations de production.

- ***Gestion des incidents***

  Exigences que nous nous sommes fixées pour gérer les événements rapportés concernant la sécurité, la confidentialité et le site, et documenter les plans de réponse pour chaque incident.

- ***Documents protégés par des droits d'auteur***

  Règles interdisant aux employés d'utiliser Dropbox ou les systèmes Dropbox pour stocker ou partager des contenus non autorisés.

- ***Gestion des modifications***

  Règles relatives aux modifications apportées aux systèmes de production. Ces règles s'appliquent à tous les employés Dropbox, sous-traitants et stagiaires ayant accès aux systèmes.

- ***Confidentialité des données des utilisateurs***

  Exigences que nous nous sommes fixées pour protéger et traiter les informations relatives aux utilisateurs et les données des utilisateurs conformément à notre politique de confidentialité.

- ***Politique de continuité d'activité et gestion des urgences***

  Règles décrivant la préservation, la protection et la sécurité des personnes (employés Dropbox), des biens et des processus (métiers).

- ***Programme de confidentialité Dropbox***

  Objectif, principes et politique de responsabilité du programme de confidentialité Dropbox.

- ***Programme de confiance Dropbox***

  Document expliquant comment Dropbox fonctionne et pourquoi nous sommes dignes de confiance.

- ***Sécurité de l'environnement de paiement***

  Règles relatives à la sécurité et à la gestion de l'environnement de paiement dédié utilisé pour accepter le paiement par carte de crédit.

Règles applicables aux employés et accès

Au moment de son embauche, chaque employé Dropbox fait l'objet d'une vérification de ses antécédents. Il doit également confirmer qu'il comprend et accepte les règles de sécurité, signer un accord de non-divulgation et suivre une formation sur la sécurité. Seuls les individus qui se sont conformés à ces procédures reçoivent un accès physique et logique aux environnements d'entreprise et de production, en fonction des responsabilités qu'implique leur fonction. Par ailleurs, tous les employés doivent suivre, chaque année, une formation sur la sécurité. Des e-mails informatifs, des présentations, ainsi que les ressources disponibles sur notre intranet leur permettent également de se sensibiliser constamment aux questions de sécurité.

L'accès de nos employés à l'environnement Dropbox est géré par un annuaire central, et authentifié grâce à une combinaison de mots de passe sécurisés, de clés SSH protégées par un code secret et de l'authentification à deux facteurs. Pour les accès distants, nous exigeons l'utilisation d'un VPN avec authentification à deux facteurs, et les éventuels accès spéciaux sont contrôlés de façon drastique par l'équipe de sécurité. La restriction d'accès aux réseaux d'entreprise et de production est définie selon les règles en vigueur. Par exemple, l'accès au réseau de production est protégé par une clé SSH et limité aux équipes d'ingénieurs qui en ont besoin pour mener à bien leurs tâches. La configuration du pare-feu fait l'objet d'un contrôle strict, et seuls quelques administrateurs peuvent la modifier.

Par ailleurs, nos règles internes obligent les employés qui accèdent aux environnements d'entreprise et de production à respecter les bonnes pratiques en matière de création et de stockage de clés SSH privées. L'accès aux autres ressources, y compris aux datacenters, aux utilitaires de configuration des serveurs et de développement de code source, ainsi qu'aux serveurs de production, est soumis à une approbation expresse de la part des responsables concernés. Ces derniers tiennent un registre des demandes, motifs et octrois d'accès, celui-ci étant toujours accordé par des personnes habilitées.

Dropbox met en œuvre des contrôles d'accès technique et des règles internes afin d'empêcher ses collaborateurs d'accéder sans raison aux fichiers des utilisateurs, et de limiter l'accès aux métadonnées et aux autres informations relatives aux comptes de ces derniers. Pour protéger la confidentialité et la sécurité des utilisateurs, seuls quelques ingénieurs responsables du développement des principaux services Dropbox ont accès à l'environnement de stockage des fichiers des utilisateurs. Si un collaborateur quitte l'entreprise, son accès est supprimé dans les plus brefs délais.

À l'heure où Dropbox devient un véritable prolongement de l'infrastructure des clients, ceux-ci ont la garantie que nous traitons leurs données avec la plus grande vigilance. Pour en savoir plus, consultez la section Sécurité des données, confidentialité et transparence ci-dessous.

Gestion des vulnérabilités

Notre équipe de sécurité effectue des tests automatiques et manuels réguliers de la sécurité et gère les correctifs. Elle collabore par ailleurs avec des spécialistes externes pour identifier et résoudre les vulnérabilités potentielles et les bugs.

Conformément aux exigences de notre système de gestion de la sécurité de l'information, les conclusions et les recommandations issues de tous ces tests sont communiquées aux responsables Dropbox et évaluées afin de prendre les mesures nécessaires. Les points dont le niveau de gravité est élevé sont documentés, analysés et résolus par les ingénieurs en sécurité compétents.

Gestion des modifications

L'ensemble des processus de développement, de résolution des problèmes et de correction suit nos règles de gestion des modifications pour garantir que les modifications apportées à un système ont été autorisées avant leur mise en production. Les modifications du code source sont effectuées par les développeurs qui souhaitent apporter une amélioration à l'application ou au service Dropbox. Toutes les modifications sont stockées dans un système de contrôle des versions et doivent faire l'objet de tests automatiques d'assurance qualité pour vérifier que toutes les exigences de sécurité sont respectées. Une fois les tests d'assurance qualité effectués, la modification est implémentée automatiquement dans l'environnement de production. Notre cycle de développement de logiciels exige le respect de consignes de codage sécurisé, ainsi que l'identification des failles potentielles liées aux modifications du code via nos processus d'examen manuel et d'assurance qualité. Les modifications qui passent en production sont consignées et archivées, et des alertes sont envoyées automatiquement aux responsables de l'équipe d'ingénieurs Dropbox.

Les modifications apportées à l'infrastructure Dropbox sont limitées au personnel autorisé. L'équipe de sécurité Dropbox est chargée d'assurer la sécurité de l'infrastructure et de garantir la conformité des configurations des serveurs, des pare-feu et des autres dispositifs de sécurité avec les pratiques en vigueur dans le secteur informatique. Les règles de pare-feu et la liste des personnes pouvant accéder aux serveurs de production font l'objet d'examens réguliers.

Analyses de la sécurité et tests d'intrusion (internes et externes)

Notre équipe de sécurité effectue régulièrement des tests automatiques et manuels de la sécurité des applications pour identifier et corriger les vulnérabilités potentielles et les bugs au niveau du client de bureau, du site Web (Dropbox et Paper) et des applications mobiles (Dropbox et Paper).

Dropbox fait également appel à des fournisseurs tiers pour qu'ils réalisent des tests périodiques d'intrusion et de vulnérabilité dans les environnements de production. Pour nous assurer que nos applications sont bien protégées, nous collaborons avec des spécialistes externes, d'autres équipes de sécurité informatique et la communauté de chercheurs actifs dans ce domaine. Nous utilisons également des systèmes d'analyse automatique pour identifier les vulnérabilités, notamment des systèmes développés en interne, des systèmes open source que nous adaptons à nos besoins et des systèmes appartenant à des fournisseurs tiers à qui nous confions l'analyse automatisée en continu.

Lutte contre les contenus dangereux

Nos outils d'analyse permettent d'empêcher le stockage et la diffusion de contenus dangereux dans Dropbox. Nous nous appuyons sur des technologies développées en interne ainsi que sur les solutions de pointe de partenaires, tels que Microsoft et Google, pour faire de Dropbox un lieu sûr pour nos clients.

Programme de lutte contre les failles de sécurité informatique

Bien que nous fassions appel à des sociétés spécialisées pour effectuer des tests d'intrusion et que nous procédions à nos propres tests internes, les programmes de lutte contre les failles de sécurité, ou bug bounty, exploitent l'expertise d'une communauté plus vaste d'experts de la sécurité. Notre programme incite les chercheurs à identifier et dévoiler de manière responsable les vulnérabilités de nos produits. La participation de la communauté externe permet à notre équipe de sécurité de bénéficier d'une analyse indépendante de nos applications afin d'assurer la protection des utilisateurs. Nous nous efforçons de proposer le meilleur programme de bug bounty du secteur, notamment en matière de récompenses et de délais de réponse et de correction.

Nous avons défini les applications Dropbox et les vulnérabilités applicables, ainsi qu'une politique de divulgation responsable qui encourage la détection et le signalement des vulnérabilités tout en améliorant la sécurité des utilisateurs. En voici les lignes directrices :

- Nous indiquer en détail le problème de sécurité constaté.
- Respecter nos applications existantes. Le spam de formulaires par l'intermédiaire de scanners de vulnérabilité automatisés ne donnera lieu à aucune prime ou récompense, car il est explicitement hors de la portée définie.
- Nous accorder un délai de réponse raisonnable avant de publier toute information relative à une faille de sécurité.
- Ne jamais modifier les données d'un utilisateur ou ne jamais y accéder sans avoir reçu l'accord préalable du propriétaire du compte.
- Ne jamais consulter, modifier, enregistrer, stocker, transférer ou accéder de toute autre manière aux données, et purger immédiatement toute information locale dès que vous signalez la vulnérabilité à Dropbox.
- Agir en toute bonne foi pour éviter toute violation de la confidentialité, destruction des données et interruption ou dégradation de nos services (déni de service, par exemple).

Pour signaler un bug, remplissez un rapport sur le site de Bugcrowd à l'adresse : bugcrowd.com/dropbox.

Sécurité physique

Infrastructure

Dropbox limite l'accès physique aux installations de l'organisation de sous-services hébergeant nos systèmes de production aux seuls collaborateurs qui ont besoin de cet accès pour mener à bien leurs tâches. Toute personne supplémentaire ayant besoin de cet accès doit recevoir au préalable l'autorisation expresse des responsables concernés.

Ces derniers tiennent un registre des demandes, motifs et octrois d'accès, et l'accès est accordé par les personnes habilitées. Une fois l'approbation reçue, un membre autorisé de l'équipe chargée de l'infrastructure contacte l'organisation de sous-services afin de demander l'accès pour la personne concernée. L'organisation de sous-services saisit les informations relatives à l'utilisateur dans son propre système et accorde au collaborateur Dropbox autorisé un accès par badge et, si possible, un accès par dispositif biométrique. Une fois l'accès octroyé, c'est au datacenter de garantir que l'accès est limité aux seules personnes autorisées.

Installations physiques

- ***Sécurité physique***

  L'équipe Dropbox responsable de la sécurité physique est chargée de faire respecter les règles régissant l'accès physique et de contrôler la sécurité des bureaux.

- ***Règles d'accès applicables aux visiteurs***

  L'accès physique aux installations de l'entreprise, autres que les entrées publiques et les halls d'entrée, est limité aux employés Dropbox autorisés et aux visiteurs enregistrés accompagnés par un employé Dropbox. Un système d'accès par badge permet de n'autoriser l'accès aux zones réservées de ces installations qu'aux seules personnes habilitées.

- ***Accès aux serveurs***

  L'accès aux zones hébergeant les serveurs de l'entreprise et les équipements réseau est limité au personnel autorisé, via l'octroi de rôles adéquats par le système d'accès par badge. La liste des personnes habilitées à accéder physiquement aux environnements d'entreprise et de production est réexaminée au moins une fois par trimestre.

Gestion des incidents

Nous avons mis en place des stratégies et procédures de gestion des incidents afin de résoudre les problèmes de disponibilité, d'intégrité, de sécurité et de confidentialité. Nos procédures de gestion des incidents s'appuient sur des équipes dédiées et formées :

- Réaction rapide aux alertes (incident potentiel)
- Évaluation de la gravité de l'incident
- Exécution de mesures de correction et de confinement (si nécessaire)

- Communication avec les bonnes personnes, en interne et en externe, notamment via des notifications informant les clients concernés qu'ils doivent remplir leurs obligations contractuelles en matière de notification des incidents et des failles, et se conformer aux lois et réglementations en vigueur
- Collecte et archivage de preuves dans le cadre d'enquêtes
- Création de rapports d'incident et mise en place d'un système de tri permanent

Les stratégies et procédures de gestion des incidents sont auditées conformément aux normes de sécurité SOC 2 et ISO/IEC 27001, entre autres.

Sécurité de l'infrastructure

Sécurité du réseau

Dropbox accorde une grande importance à la sécurité de son réseau. Nos techniques de surveillance et de sécurité du réseau sont conçues pour fournir plusieurs niveaux de protection et de défense. Nous faisons appel à des techniques de protection conformes aux standards actuels pour que seul le trafic autorisé atteigne notre infrastructure : pare-feux, analyse des vulnérabilités, surveillance de la sécurité des réseaux, détection des intrusions, etc.

Notre réseau privé interne est segmenté en fonction de l'utilisation et du niveau de risque. Les principaux réseaux sont les suivants :

- Zone DMZ connectée à Internet
- Zone DMZ d'infrastructure prioritaire
- Réseau de production
- Réseau d'entreprise

L'accès à l'environnement de production est limité aux adresses IP autorisées et nécessite une authentification multifacteur sur tous les points de terminaison. Les adresses IP autorisées sont associées au réseau d'entreprise ou au personnel Dropbox habilité. Elles sont vérifiées chaque trimestre pour garantir la sécurité de l'environnement de production. Seules les personnes disposant des autorisations appropriées peuvent modifier la liste des adresses IP.

Le trafic Internet à destination du réseau de production est protégé par plusieurs niveaux de pare-feu et de services proxy.

Une séparation stricte est assurée entre le réseau interne de Dropbox et le réseau Internet public. Le trafic lié à Internet depuis et vers le réseau de production fait l'objet d'un contrôle strict au moyen d'un service proxy dédié, lui-même protégé par des règles de pare-feu extrêmement restrictives.

Dropbox met en place des outils sophistiqués pour surveiller les ordinateurs de bureau et les ordinateurs portables Mac et Windows ainsi que les systèmes de production, afin de détecter d'éventuels événements malveillants. Les journaux de sécurité sont centralisés afin de répondre aux incidents et aux demandes des autorités, conformément aux normes de rétention des données du secteur.

Dropbox identifie et limite les risques grâce à des tests et à des audits réguliers de la sécurité du réseau effectués par des équipes internes dédiées, ainsi que par des spécialistes externes.

Points de présence

Dans le but d'optimiser les performances du site Web pour les utilisateurs, Dropbox exploite des réseaux de diffusion de contenu (CDN) tiers, ainsi que des points de présence hébergés par Dropbox répartis sur 31 sites dans le monde. Aucune donnée d'utilisateur n'est mise en cache sur ces sites. De plus, toutes les données d'utilisateur transférées sont chiffrées à l'aide du protocole SSL/TLS. L'accès physique et logique aux points de présence hébergés par Dropbox est limité aux employés Dropbox autorisés. Dropbox continue à optimiser la couche de transport (TCP) et la couche applicative (HTTP).

Peering

Dropbox a mis en place une politique d'appairage ouvert (en anglais, "open peering") et invite tous ses clients à en profiter. Pour en savoir plus, rendez-vous sur dropbox.com/peering.

Fiabilité

Un système de stockage n'a de sens que s'il est fiable. C'est pourquoi nous avons développé Dropbox avec plusieurs niveaux de redondance pour éviter toute perte de données et garantir la disponibilité.

Métadonnées sur les fichiers

Les copies redondantes des métadonnées sont réparties sur différents appareils au sein d'un datacenter, selon un modèle de disponibilité d'au moins N+2. Des sauvegardes incrémentielles sont effectuées au minimum toutes les heures, en complément des sauvegardes complètes réalisées quant à elles toutes les 36 heures. Les métadonnées sont stockées sur des serveurs hébergés et gérés par Dropbox aux États-Unis.

Blocs de fichiers

Les copies redondantes des blocs de fichiers sont stockées séparément dans au moins deux zones géographiques distinctes et répliquées en toute fiabilité dans chacune d'elles. (**Remarque** : pour les clients qui choisissent de stocker leurs fichiers dans notre infrastructure en Allemagne, en Australie, au Japon ou au Royaume-Uni, les blocs de fichiers sont exclusivement répliqués dans ces régions respectives. Pour plus d'informations, consultez la section Datacenters et fournisseurs de services gérés ci-dessous.) Magic Pocket et AWS sont conçus pour assurer une durabilité annuelle des données d'au moins 99,999999999 %.

L'architecture, les applications et les mécanismes de synchronisation Dropbox fonctionnent de pair pour protéger les données des utilisateurs et garantir leur haute disponibilité. En cas d'indisponibilité du service, les utilisateurs Dropbox ont toujours accès aux dernières versions de leurs fichiers synchronisées dans le dossier Dropbox local sur leurs ordinateurs associés. Les copies des fichiers synchronisées dans le client de bureau ou dans le dossier Dropbox local restent accessibles sur le disque dur des utilisateurs lors des périodes d'interruption, des pannes ou lorsqu'ils sont hors ligne. Les modifications apportées aux fichiers et aux dossiers sont synchronisées avec Dropbox dès que le service ou la connectivité est restauré.

Documents Paper

Les copies redondantes des données de document Paper sont réparties sur différents systèmes au sein d'un datacenter, selon un modèle de disponibilité N+1. De plus, des sauvegardes complètes des données de document Paper sont effectuées quotidiennement. Pour le stockage des documents Paper, Dropbox utilise l'infrastructure AWS aux États-Unis, conçue pour assurer une durabilité annuelle des données d'au moins 99,999999999 %. En cas d'indisponibilité du service, les utilisateurs ont toujours accès aux dernières versions synchronisées de leurs documents Paper dans le mode "hors ligne" de leur application mobile.

Synchronisation des fichiers

Dropbox intègre la meilleure technologie de synchronisation de fichiers du marché. Nos dispositifs de synchronisation assurent un transfert rapide des fichiers et permettent aux utilisateurs d'accéder à leurs données partout et sur tous les appareils. La synchronisation Dropbox est également un service résilient. En cas d'échec de connexion au service Dropbox, le client renouvelle l'opération dès que la connexion est rétablie. Les fichiers sont mis à jour sur le client local uniquement s'ils ont été entièrement synchronisés et validés par le service Dropbox. L'équilibrage de charge entre les différents serveurs garantit la redondance et une expérience de synchronisation cohérente pour l'utilisateur final.

Synchronisation différentielle

Ce mode de synchronisation permet de télécharger/importer uniquement les parties modifiées d'un fichier (et non le fichier entier). Dropbox stocke chaque fichier importé dans des blocs chiffrés indépendants et met seulement à jour les blocs modifiés.

Synchronisation en flux continu

Plutôt que d'attendre que le transfert d'un fichier soit terminé, la synchronisation en flux continu démarre le téléchargement des blocs synchronisés sur un deuxième appareil avant la fin du transfert depuis le premier appareil. Ce processus se lance automatiquement lorsque des ordinateurs distincts sont associés au même compte Dropbox ou lorsque différents comptes Dropbox partagent le même dossier.

Économie d'espace disque

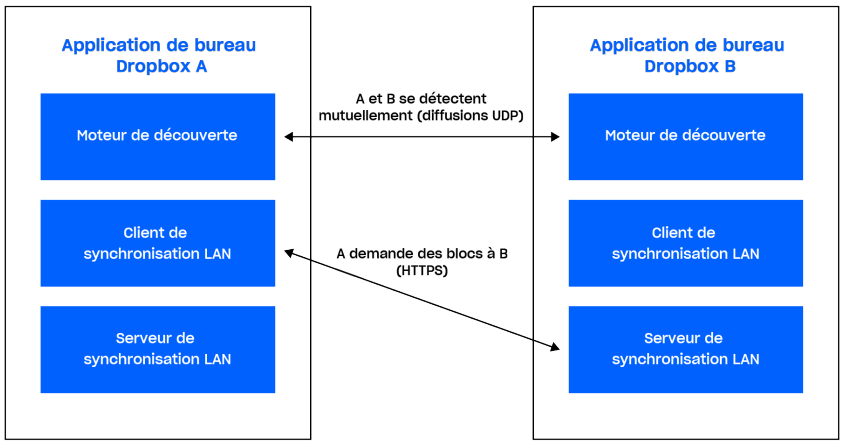
Les utilisateurs peuvent libérer de l'espace de stockage sur leur ordinateur en rendant accessibles hors ligne uniquement les fichiers qu'ils choisissent sur leur disque dur. Cette opération libère de l'espace sur l'ordinateur en conservant tout le reste en ligne sur dropbox.com.

Synchronisation LAN

Lorsqu'elle est activée, cette fonctionnalité télécharge les nouveaux fichiers et les fichiers mis à jour à partir des autres ordinateurs du réseau local (LAN ou Local Area Network). Le téléchargement est ainsi plus rapide et moins gourmand en bande passante qu'un téléchargement effectué depuis les serveurs Dropbox.

Architecture

Trois composants principaux du système de synchronisation LAN sont exécutés dans l'application de bureau : le moteur de découverte, le serveur et le client. Le moteur de découverte explore le réseau afin d'identifier les machines sur lesquelles la synchronisation doit avoir lieu. Ce procédé est limité aux machines disposant d'un accès autorisé aux mêmes dossiers Dropbox personnels ou partagés. Le serveur traite les demandes provenant des autres ordinateurs du réseau et distribue les blocs de fichier requis. Quant au client, il effectue les demandes de blocs de fichier à partir du réseau.



Moteur de découverte

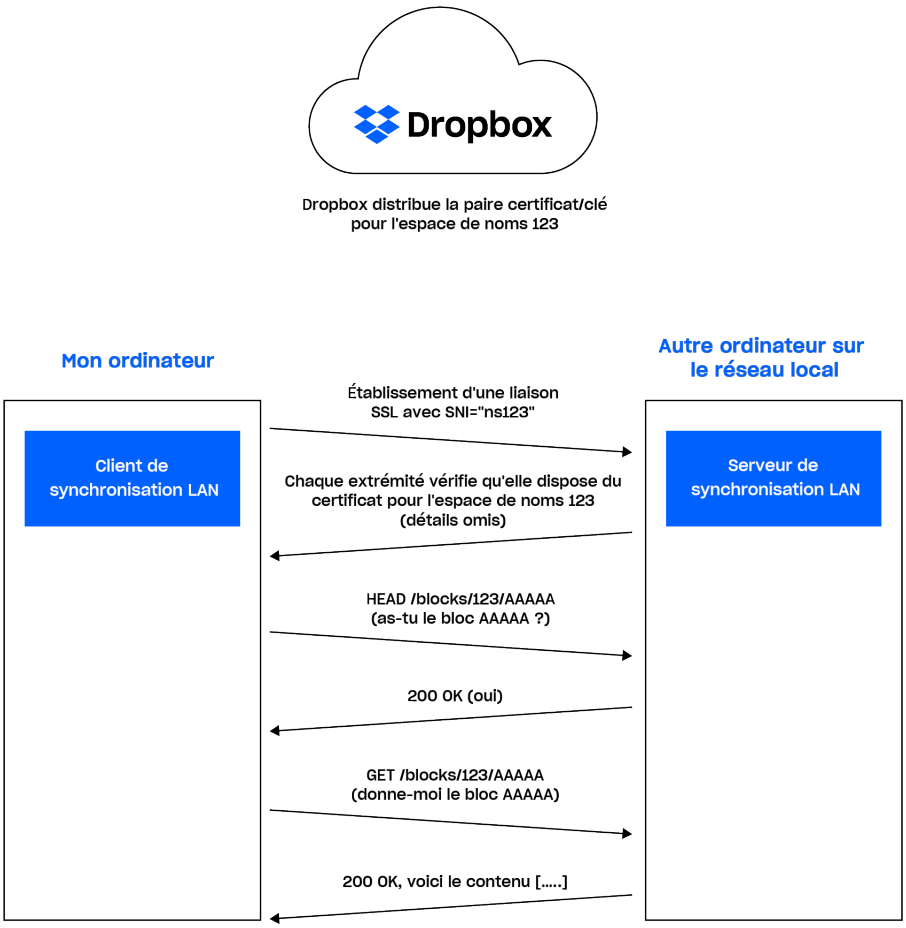
Chaque ordinateur du réseau local envoie et recherche régulièrement des paquets de diffusion UDP sur le port 17500 (réservé à la synchronisation LAN par l'Internet Assigned Numbers Authority, ou IANA). Ces paquets incluent la version du protocole utilisé par cet ordinateur, les dossiers Dropbox personnels et partagés, le port TCP utilisé pour exécuter le serveur (s'il diffère du port 17500), ainsi qu'un identifiant aléatoire pour l'ordinateur. Lorsqu'un paquet est détecté, l'adresse IP de la machine est ajoutée à une liste pour chaque dossier personnel ou partagé, indiquant ainsi une cible potentielle.

Protocole

Le transfert des blocs de données s'effectue via le protocole HTTPS. Chaque ordinateur exécute un serveur HTTPS associé à des points de terminaison. Le client interroge plusieurs systèmes homologues afin de déterminer s'ils possèdent les blocs à transférer, mais télécharge ces derniers à partir d'un seul serveur.

Pour protéger vos données, nous veillons à ce que seuls les clients authentifiés pour un dossier spécifique puissent demander des blocs de données. Nous veillons également à ce que les ordinateurs ne soient pas utilisés en tant que serveurs pour des dossiers qu'ils ne contrôlent pas. Pour ce faire, nous générons des paires clé/certificat SSL pour chaque dossier Dropbox personnel ou partagé. Les serveurs Dropbox distribuent ces paires clé/certificat aux ordinateurs des utilisateurs ayant accès à ces dossiers. Les paires clé/certificat sont modifiées à chaque changement de statut d'un membre (lorsque l'accès d'un utilisateur à un dossier partagé est révoqué, par exemple). L'authentification doit s'effectuer avec le même certificat (certificat du compte Dropbox ou du dossier partagé) aux deux extrémités de la connexion HTTPS. Cette approche permet de garantir que les deux extrémités sont bien authentifiées.

Lors de l'établissement d'une connexion, nous indiquons au serveur la Dropbox personnelle ou le dossier auquel nous essayons de nous connecter via l'extension SNI (Server Name Indication). Le serveur utilise ainsi le certificat approprié.



Serveur/client

Avec le protocole décrit ci-dessus, le serveur n'a qu'à déterminer les blocs présents et leur emplacement.

En fonction des résultats du moteur de découverte, le client met à jour une liste de clients homologues pour chaque dossier Dropbox personnel et partagé. Lorsque le service de synchronisation LAN reçoit une demande de téléchargement d'un bloc de fichiers, il sonde un échantillon aléatoire de clients qu'il a identifiés pour le dossier Dropbox personnel ou partagé, et demande le bloc au client qui répond en premier.

Pour éviter toute latence, des pools de connexion permettent de réutiliser les connexions déjà lancées. Nous n'établissons pas de nouvelle connexion tant que cela n'est pas nécessaire, et une fois une connexion établie, nous ne la fermons pas au cas où nous en aurions besoin à nouveau. Nous limitons également le nombre de connexions vers chaque client.

Si un bloc est introuvable, si son téléchargement échoue ou si la connexion s'avère trop lente, le système revient à l'étape d'obtention du bloc auprès des serveurs Dropbox.

Datacenters et fournisseurs de services gérés

Les systèmes de gestion et de production Dropbox sont hébergés dans des datacenters gérés par des organisations de sous-services tierces et des fournisseurs de services gérés situés aux États-Unis. Tous les rapports SOC (Service Organization Controls) relatifs aux datacenters gérés par des organisations de sous-services et/ou questionnaires de sécurité et obligations contractuelles des fournisseurs sont examinés au moins une fois par an pour vérifier que les contrôles de sécurité sont suffisants. Ces fournisseurs de services tiers sont responsables des contrôles de sécurité physiques, environnementaux et opérationnels à la périphérie de l'infrastructure Dropbox. Dropbox est responsable de la sécurité logique, de la sécurité du réseau et de la sécurité des applications de son infrastructure hébergée au sein de datacenters tiers.

Amazon Web Services (AWS), le fournisseur de services gérés de Dropbox actuellement chargé du traitement et du stockage, est responsable de la sécurité logique et de la sécurité réseau des services Dropbox fournis par le biais de son infrastructure. Les connexions sont protégées par le pare-feu du fournisseur de services gérés, qui est configuré pour refuser par défaut toutes les connexions. Dropbox restreint l'accès à l'environnement à un nombre limité d'adresses IP et de collaborateurs.

Infrastructure en Allemagne, en Australie, au Japon et au Royaume-Uni

Nos clients éligibles peuvent demander à ce que leurs blocs de fichiers soient stockés en dehors des États-Unis. Notre infrastructure est hébergée par AWS en Allemagne, en Australie, au Japon et au Royaume-Uni, et répliquée dans la région respective pour garantir la redondance et la protection contre la perte de données. Les métadonnées des fichiers sont stockées sur les serveurs propriétaires de Dropbox aux États-Unis. Les aperçus et les documents Paper sont actuellement stockés aux États-Unis pour tous les clients.

Continuité d'activité

Dropbox a mis en place un système de gestion de la continuité d'activité afin de définir comment assurer la continuité des services aux utilisateurs (et comment continuer à fonctionner en tant qu'entreprise) et les rétablir en cas d'interruption des processus métiers stratégiques. Nous utilisons un processus cyclique qui se déroule en plusieurs phases :

- ***Évaluation des risques et de l'impact sur l'entreprise***

  Au moins une fois par an, nous procédons à une évaluation de l'impact sur l'entreprise afin d'identifier les processus stratégiques de Dropbox, d'évaluer l'impact potentiel des interruptions de service, de définir un calendrier pour les opérations de récupération prioritaires et d'identifier les fournisseurs et acteurs essentiels au bon fonctionnement de Dropbox. Nous effectuons également, au moins une fois par an, une évaluation des risques à l'échelle de l'entreprise pour identifier, analyser et évaluer de manière systématique les risques associés aux interruptions de service au sein de Dropbox. Ces deux processus d'évaluation nous permettent d'établir nos priorités en matière de continuité d'activité et d'adapter nos stratégies de correction et de récupération dans le cadre de nos plans de continuité d'activité.

- ***Plans de continuité d'activité***

  Les équipes dont les processus ont été identifiés comme essentiels à la continuité d'activité de Dropbox lors de l'évaluation de l'impact sur l'entreprise s'appuient sur l'ensemble des données collectées pour développer des plans de continuité d'activité pour leurs processus. Grâce à ces plans, les équipes savent qui est en charge de rétablir les processus en cas d'urgence, qui peut prendre le relais dans un autre bureau ou une autre région en cas d'interruption de service, et quels modes de communication doivent être utilisés en cas d'incident affectant la continuité d'activité. Ces plans préparent également les équipes à faire face à une interruption de service en centralisant les plans de récupération et d'autres informations importantes, notamment sur l'application des plans (où et comment), les

coordonnées des équipes et détails des réunions, les applications critiques et les stratégies de récupération. Les plans de continuité d'activité de Dropbox sont liés à notre plan de gestion de crise global qui identifie les équipes chargées de la gestion de crise et de la gestion des incidents au sein de Dropbox.

- ***Test et mise en application des plans***

  Au moins une fois par an, Dropbox teste un certain nombre d'éléments de ses plans de continuité d'activité. Ces tests, conformes à la portée et aux objectifs de notre système de gestion de la continuité d'activité (BCMS), reposent sur des scénarios pertinents et bien conçus avec des objectifs clairs. Ils peuvent inclure aussi bien des exercices de simulation de petite envergure que des simulations à grande échelle d'incidents en conditions réelles. Les équipes utilisent ensuite les résultats de ces tests, ainsi que leur propre expérience suite à des incidents réels, pour mettre à jour et améliorer leurs plans afin de résoudre les problèmes et de renforcer leurs capacités de réponse aux incidents.

- ***Examen et approbation du système de gestion de la continuité d'activité***

  Au moins une fois par an, l'équipe dirigeante de Dropbox examine le système de gestion de la continuité d'activité dans le cadre de la réévaluation du programme de confiance Dropbox.

Reprise d'activité

Pour satisfaire aux exigences relatives à la sécurité des informations en cas de crise ou d'incident majeur affectant le fonctionnement de Dropbox Business, nous disposons d'un plan de reprise d'activité. L'équipe Dropbox chargée de l'ingénierie le revoit chaque année et teste certains éléments au moins une fois par an. Les résultats sont documentés et font l'objet d'un suivi jusqu'à leur résolution.

Notre plan de reprise d'activité concerne à la fois les incidents ayant un impact sur la durabilité et la disponibilité, tels que décrits ci-dessous :

- Les incidents de durabilité se caractérisent par un ou plusieurs des éléments suivants :
  - Perte complète ou permanente d'un datacenter principal stockant des métadonnées, ou de plusieurs datacenters stockant des blocs de fichiers.
  - Impossibilité de communiquer ou de distribuer des données à partir d'un datacenter stockant des métadonnées, ou de plusieurs datacenters stockant des données.
- Les incidents de disponibilité se caractérisent par un ou plusieurs des éléments suivants :
  - Panne dont la durée dépasse dix jours.
  - Impossibilité de communiquer ou de distribuer des données à partir d'un service de stockage/datacenter stockant des métadonnées, ou de plusieurs services de stockage/datacenters stockant des blocs de fichiers.

Nous définissons un objectif de délai de récupération (RTO), à savoir la durée après laquelle le processus ou le service métier doit être restauré après un sinistre et son niveau de service. Nous définissons aussi un objectif de point de récupération (RPO), à savoir la durée maximale autorisée pendant laquelle des données pourraient être perdues suite à une interruption du service. Nous mesurons également le délai de reprise réel (RTA) lors de tests de reprise d'activité, réalisés au moins une fois par an.

Les plans de gestion des incidents, de continuité d'activité et de reprise d'activité sont testés à intervalles réguliers et lors de changements importants dans l'entreprise ou l'environnement.

Sécurité des applications

Interfaces utilisateur Dropbox

Le service Dropbox est accessible via plusieurs interfaces. Chacune d'elles dispose de fonctionnalités et de paramètres de sécurité qui traitent et protègent les données des utilisateurs tout en offrant un accès simple.

- ***Site 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.

- ***Application de bureau***

  L'application de bureau Dropbox est un client de synchronisation ultraperformant qui stocke les fichiers localement afin de permettre aux utilisateurs d'y accéder hors ligne. Compatible avec les systèmes d'exploitation Windows et Mac, elle leur offre un accès complet à leurs comptes Dropbox. Les fichiers peuvent être consultés et partagés directement depuis le gestionnaire de fichiers du 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.

- ***API***

  Les API Dropbox offrent un moyen flexible de lire et d'écrire des données dans Dropbox, ainsi qu'un accès à des fonctionnalités avancées telles que la recherche, les versions de fichiers et la restauration des fichiers. Les API permettent de gérer le cycle de vie utilisateur d'un compte Dropbox Business, d'appliquer des actions à tous les membres d'une équipe et d'accéder aux fonctionnalités d'administration de Dropbox Business.

Interfaces utilisateur Paper

Le service Paper est accessible via plusieurs interfaces. Chacune d'elles dispose de fonctionnalités et de paramètres de sécurité qui traitent et protègent les données des utilisateurs tout en offrant un accès simple.

- ***Site Web***

  Tous les navigateurs Web récents permettent d'accéder à cette interface, qui offre aux utilisateurs la possibilité de créer, modifier, télécharger et partager leurs documents Paper.

- ***Application mobile***

  Disponible sur les appareils mobiles et tablettes iOS et Android, l'application mobile Paper permet aux utilisateurs d'accéder à tous leurs documents Paper lors de leurs déplacements. Cette application mobile hybride s'appuie sur un code natif (iOS ou Android) encapsulant un navigateur Web interne.

- ***API***

  L'API Dropbox décrite ci-dessus contient des points de terminaison et des types de données pour la gestion des documents et des dossiers dans Dropbox Paper, y compris la prise en charge des fonctionnalités telles que la gestion des autorisations, l'archivage et la suppression définitive.

Chiffrement

Données en transit

Pour protéger les données en transit entre les applications Dropbox et nos 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 (le client de bureau, les applications mobiles, l'API ou le site Web) et le service hébergé sont chiffrées au moyen de ces protocoles. De même, les données Paper en transit entre un client Paper (mobile, API ou Web) et les services hébergés sont chiffrées au moyen des protocoles SSL/TLS. En ce qui concerne les points de terminaison que nous contrôlons (applications de bureau et mobiles) et les navigateurs récents, nous utilisons un algorithme renforcé, et prenons en charge l'épinglage des certificats et la technologie PFS (Perfect Forward Secrecy). En outre, sur le Web, nous marquons tous les cookies d'authentification comme sécurisés et utilisons le dispositif de sécurité HSTS (HTTP Strict Transport Security) avec l'attribut includeSubDomains.

Remarque : en raison de vulnérabilités connues, Dropbox n'utilise plus SSLv3 mais uniquement TLS. Toutefois, nous avons choisi de continuer à utiliser le terme "SSL/TLS" dans ce document, car celui-ci reste fréquemment utilisé pour faire référence à TLS.

Pour empêcher les attaques de type "attacker-in-the-middle attacks", l'authentification des serveurs frontaux Dropbox s'effectue via des certificats publics détenus par le client. Une connexion chiffrée est négociée avant le transfert des fichiers ou documents Paper afin de garantir leur distribution sécurisée aux serveurs frontaux Dropbox.

Données au repos

Les fichiers Dropbox importés par des utilisateurs sont chiffrés au repos via un chiffrement AES (Advanced Encryption Standard) de 256 bits. Les fichiers sont stockés dans des blocs de fichiers distincts au sein de plusieurs datacenters. Chaque bloc est fragmenté et chiffré à l'aide d'un algorithme renforcé. Seuls les blocs modifiés d'une révision à une autre sont synchronisés. Les documents Paper au repos sont également protégés par un chiffrement AES (Advanced Encryption Standard) de 256 bits. Les documents Paper sont stockés dans plusieurs zones de disponibilité via des systèmes tiers.

Gestion des clés

L'infrastructure Dropbox de gestion des clés a été conçue pour mettre en œuvre des contrôles de sécurité opérationnels, techniques et procéduraux, avec un accès direct aux clés extrêmement limité. Les opérations de génération, d'échange et de stockage des clés de chiffrement sont réparties sur différents systèmes afin de décentraliser le traitement.

- ***Clés de chiffrement des fichiers***

  Dropbox gère les clés de chiffrement des fichiers à la place des utilisateurs afin de réduire la complexité, de mettre à sa disposition des fonctionnalités avancées et d'assurer un contrôle renforcé du chiffrement. Les clés de chiffrement des fichiers sont créées, stockées et protégées par les contrôles et les règles de sécurité de l'infrastructure du système de production.

- ***Clés SSH internes***

  L'accès aux systèmes de production est restreint par des paires de clés SSH uniques. Les règles et procédures de sécurité exigent la protection de ces clés. Un système interne gère le processus d'échange sécurisé des clés, et les clés privées sont stockées en lieu sûr. Les clés SSH internes ne peuvent pas être utilisées pour accéder aux systèmes de production sans l'utilisation d'un second facteur d'authentification.

- ***Distribution des clés***

  Dropbox automatise la gestion et la distribution des clés particulièrement sensibles aux systèmes requis pour mener à bien les opérations.

Épinglage des certificats

Dropbox fournit l'épinglage des certificats sur les navigateurs récents compatibles avec la norme HTTP Public Key Pinning, ainsi que sur nos clients de bureau et mobiles. L'épinglage des certificats est une vérification supplémentaire qui garantit que le service auquel vous vous connectez est bien celui qu'il prétend être. Cette mesure de sécurité vous protège contre toute tentative d'espionnage par des pirates informatiques expérimentés.

Protection des données d'authentification

Dropbox utilise une technique de hachage avancée afin de protéger les identifiants de connexion des utilisateurs. Conformément aux bonnes pratiques du secteur, chaque mot de passe est salé, c'est-à-dire qu'on lui attribue une chaîne de caractère (ou "sel") unique et aléatoire. Nous utilisons en complément une fonction de hachage itérative qui complique le déchiffrement des mots de passe. Ces pratiques permettent de protéger les données des attaques par force brute, par dictionnaire et par table arc-en-ciel (ou "rainbow table"). Pour renforcer encore davantage la sécurité, nous chiffrons les valeurs de hachage à l'aide d'une clé stockée dans un endroit distinct de la base de données et qui permet de protéger l'intégrité des mots de passe en cas d'attaque ciblant uniquement la base de données.

Analyse des programmes malveillants

Nous avons mis au point un système automatisé qui recherche les logiciels malveillants au moment où un contenu est partagé en dehors du compte de l'utilisateur d'origine. Le système repose à la fois sur notre technologie propriétaire et sur des moteurs de détection répondant aux normes du secteur. Il est conçu pour stopper la propagation des programmes malveillants.

Sécurité des produits

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 centralise tout ce qui est nécessaire à votre travail : outils, contenu et collaborateurs. Dropbox est bien plus qu'un système de stockage sécurisé. C'est un moyen intelligent et transparent d'optimiser votre workflow existant.

Vous découvrirez ci-dessous quelques-unes des fonctionnalités proposées aux administrateurs et aux utilisateurs, ainsi que les intégrations tierces permettant de gérer les principaux processus informatiques.

Remarque : la disponibilité des fonctionnalités varie selon le forfait choisi. Rendez-vous sur dropbox.com/business/plans pour en savoir plus.

Contrôle du contenu

La protection des contenus confidentiels, comme la propriété intellectuelle et les informations personnelles, est cruciale pour les équipes informatiques et celles chargées de la sécurité des données. Des autorisations d'accès granulaires aux conservations légales, en passant par les politiques de rétention des données, Dropbox fournit des solutions de pointe pour gérer, surveiller et protéger votre contenu. Les principaux produits et fonctionnalités Dropbox qui assurent le contrôle du contenu sont répertoriés ci-dessous.

Autorisations granulaires d'accès au contenu et autorisations relatives aux dossiers et fichiers partagés

- ***Autorisations relatives aux fichiers partagés***

  Les membres de l'équipe qui sont propriétaires d'un fichier partagé peuvent supprimer l'accès de certains utilisateurs et désactiver la fonctionnalité d'ajout de commentaires pour le fichier.

- ***Autorisations relatives aux dossiers partagés***

  Les membres de l'équipe qui sont propriétaires d'un dossier partagé peuvent supprimer l'accès de certains utilisateurs, modifier les autorisations de lecture et de modification de certains utilisateurs et transférer la propriété d'un dossier. En fonction des autorisations de partage de l'équipe, les propriétaires des dossiers partagés peuvent également définir si leurs dossiers peuvent être partagés avec des personnes extérieures à l'équipe, si les liens peuvent être partagés avec des utilisateurs n'ayant pas accès à ces dossiers et si d'autres utilisateurs autorisés à apporter des modifications peuvent en gérer les membres.

- ***Mots de passe pour les liens partagés***

  Tout lien partagé peut être protégé à l'aide d'un mot de passe défini par son propriétaire. Dans ce cas, avant la transmission des données, un niveau de contrôle d'accès vérifie que le bon mot de passe a été fourni et que toutes les autres conditions sont remplies (notamment les listes de contrôle d'accès de l'équipe, du groupe ou du dossier). Un cookie sécurisé est alors stocké dans le navigateur de l'utilisateur pour mémoriser le fait que le mot de passe a déjà été vérifié. Grâce aux contrôles de partage, les administrateurs peuvent également définir des mots de passe par défaut, au lieu de les rendre facultatifs, afin de mieux protéger le contenu de leur équipe.

- ***Délais de validité des liens partagés***

  Les utilisateurs peuvent définir un délai de validité pour tous les liens qu'ils partagent afin de fournir un accès temporaire aux fichiers et dossiers correspondants. Grâce aux contrôles de partage, les administrateurs peuvent également définir des délais de validité par défaut, au lieu de les rendre facultatifs, afin de mieux protéger le contenu de leur équipe.

Autorisations relatives aux documents Paper et aux dossiers Paper partagés

- ***Autorisations relatives aux documents Paper et aux dossiers Paper partagés***

  Les membres de l'équipe qui sont propriétaires d'un document Paper ou d'un dossier Paper partagé peuvent supprimer l'accès de certains utilisateurs et désactiver leur autorisation de modification.

- ***Autorisations relatives aux documents Paper***

  Les membres de l'équipe qui sont propriétaires d'un document Paper peuvent supprimer l'accès de certains utilisateurs explicitement répertoriés dans le panneau de partage. Le propriétaire du document Paper et les membres disposant d'un droit de modification peuvent modifier les autorisations de consultation/modification de certains utilisateurs, ainsi que les paramètres de partage du document. Les paramètres de partage déterminent quels utilisateurs peuvent ouvrir le document et leur niveau d'autorisation. L'administrateur d'équipe peut définir des règles de partage des liens et des documents pour l'ensemble de l'équipe.

- ***Autorisations relatives aux dossiers Paper***

  Les membres de l'équipe qui sont membres du dossier peuvent modifier les paramètres de partage du dossier et en supprimer l'accès à certains utilisateurs explicitement ajoutés au dossier.

Actions sur les fichiers et dossiers

- ***Dossiers d'équipe pour les fichiers***

  Les administrateurs peuvent créer des dossiers d'équipe donnant automatiquement aux groupes et aux autres collaborateurs le niveau d'accès approprié aux contenus dont ils ont besoin (lecture seule ou modification).

- ***Contrôles de partage et d'accès granulaires***

  Les contrôles de partage permettent aux administrateurs de gérer les membres et les autorisations à la racine ou au niveau du sous-dossier afin de limiter l'accès de certains groupes ou utilisateurs internes ou externes à certains dossiers seulement.

- ***Gestionnaire de dossiers d'équipe***

  Les administrateurs peuvent voir tous leurs dossiers d'équipe et personnaliser les règles de partage de façon centralisée afin d'éviter le partage involontaire de contenus confidentiels.

- ***Dossiers partagés pour les documents Paper***

  Les administrateurs peuvent créer des dossiers Paper partagés donnant automatiquement aux autres collaborateurs le niveau d'accès approprié aux contenus dont ils ont besoin (commentaire ou modification).

- ***Effacement à distance***

  En cas de départ d'un membre de l'équipe ou de perte d'un appareil, les administrateurs peuvent supprimer à distance les données Dropbox et la copie locale des fichiers. Les fichiers sont alors supprimés des ordinateurs et des appareils mobiles lors de la prochaine connexion à Internet et de l'exécution de l'application Dropbox.

- ***Transfert de compte***

  Lors de la suppression d'un compte utilisateur (manuellement ou via les services d'annuaire), les administrateurs peuvent transférer les fichiers associés à ce compte et la propriété des documents Paper créés par l'ancien membre de l'équipe à un autre membre de l'équipe. La fonctionnalité de transfert de compte peut être utilisée lors de la suppression d'un utilisateur ou à tout moment après la suppression du compte de l'utilisateur.

Les fonctionnalités suivantes sont disponibles sous forme d'options (contactez le service commercial pour plus d'informations).

- ***Analyse du contenu***

  Grâce à l'option de contrôle avancé des équipes et du contenu, les clients Dropbox Business Advanced et Enterprise peuvent analyser le contenu nouveau et existant dans Dropbox pour identifier et éviter les vulnérabilités des données.

- ***Configuration et déclenchement de workflows personnalisés***

  Grâce à l'option de contrôle avancé des équipes et du contenu, les administrateurs peuvent prendre des mesures personnalisées contre les fichiers qui enfreignent les règles de l'entreprise.

- ***Configuration d'alertes***

  Les administrateurs peuvent recevoir des alertes lorsque des fichiers sont partagés en externe ou lorsque des données sensibles ont été identifiées. Ils peuvent ainsi surveiller les problèmes de sécurité en temps réel et éviter toute vulnérabilité.

Visibilité du contenu

Notifications et alertes de sécurité

Les administrateurs Dropbox Enterprise peuvent recevoir des notifications en temps réel en cas d'activités abusives, d'activités à risque ou de fuites de données potentielles dans leur compte. Les événements suivants peuvent faire l'objet d'une surveillance :

- Suppression en masse
- Déplacement massif de données
- Partage externe de contenu sensible
- Programme malveillant partagé à l'extérieur de votre équipe
- Programme malveillant partagé à l'intérieur de votre équipe
- Trop de tentatives de connexion échouées
- Connexion à partir d'un pays à haut risque
- Détection de ransomware

Dropbox permet de définir des seuils d'alerte, des destinataires et des systèmes de signalement automatique en cas de partage de fichiers sensibles avec des utilisateurs externes. Les administrateurs peuvent également marquer les alertes comme étant en cours d'examen, résolues ou ignorées. En outre, un widget de tableau de bord affiche des informations générales sur les alertes d'équipe et les tendances de la semaine passée.

Rapport et page de partage à l'extérieur de l'équipe

Dropbox offre une visibilité supplémentaire grâce à un rapport et une page sur les partages externes. Les administrateurs peuvent créer un rapport à partir du tableau de bord ou de la page des partages externes. Le rapport répertorie tous les fichiers et dossiers de l'équipe qui sont partagés à l'extérieur de leur équipe et tous les liens partagés. La page sur les partages externes est une page supplémentaire de l'interface d'administration qui permet aux administrateurs de voir et de filtrer (type de fichier, auteur du partage, paramètres de lien, etc.) les fichiers et dossiers partagés à l'extérieur de l'équipe et les liens partagés.

Contrôles de partage

Les paramètres de partage permettent aux administrateurs de mieux contrôler le partage et l'accès au contenu de leur équipe. Ils peuvent définir des délais de validité par défaut au niveau de l'équipe, des mots de passe, ou les deux. Ces restrictions réduisent le risque de perte de données en déchargeant les utilisateurs de cette responsabilité.

Classification des données

Les équipes Dropbox Enterprise peuvent ajouter automatiquement un libellé à leurs données personnelles et sensibles pour mieux les protéger. Les administrateurs reçoivent des alertes de protection contre la perte de données (DLP) par e-mail et dans l'interface d'administration lorsque des fichiers ou des dossiers contenant des informations sensibles et enregistrés dans des dossiers d'équipe sont partagés à l'extérieur de leur équipe. Les administrateurs ont la possibilité d'identifier et de classer automatiquement les données sensibles stockées dans les dossiers partagés et les dossiers personnels des membres de l'équipe. Les administrateurs Dropbox Enterprise peuvent activer la classification automatique des données dans l'interface d'administration.

Option de gouvernance des données

La gouvernance des données désigne l'ensemble des processus, des technologies et des équipes qui gèrent et protègent les données d'une entreprise. Cela inclut la possibilité de stocker, d'identifier, de découvrir et de récupérer les données de l'entreprise.

L'option de gouvernance des données Dropbox regroupe un ensemble de fonctionnalités qui permettent aux entreprises de mieux contrôler et sécuriser leurs données, tout en réduisant les risques et les coûts liés au respect des exigences réglementaires et de conformité. Cette option comprend actuellement quatre fonctionnalités clés pour les administrateurs d'équipe et les administrateurs de conformité.

- ***Historique étendu des versions***

  La durée par défaut de l'historique des versions des fichiers dépend du forfait Dropbox souscrit. Avec Dropbox Business, vous pouvez toutefois disposer d'un historique étendu des versions (séparément ou dans le cadre de l'option de gouvernance des données) qui permet de récupérer les fichiers supprimés ou modifiés pendant dix ans.

- ***Conservations légales***

  En activant la conservation légale pour un membre de l'équipe, les administrateurs d'équipe et de conformité peuvent afficher et exporter tout le contenu qui a été créé ou modifié par ce membre. Les membres concernés par une conservation légale n'en sont pas informés et auront toujours la possibilité de créer, modifier et supprimer des fichiers.

- ***Rétention des données***

  La rétention des données permet aux équipes et aux administrateurs de conformité d'éviter la suppression accidentelle du contenu qu'ils sont juridiquement tenus de conserver pendant un certain délai. Cette fonctionnalité permet aux clients de conserver les données pendant dix ans à partir de la date de la dernière "version".

- ***Destruction des données***

  La destruction des données permet aux administrateurs d'équipe et de conformité de supprimer définitivement les données à une date précise dans le respect des exigences de rétention et de destruction des données. Les administrateurs peuvent surveiller les opérations grâce à des rapports les informant des suppressions de fichiers à venir.

Récupération et historique des versions

Les utilisateurs Dropbox Business ont la possibilité de récupérer des fichiers et des documents Paper supprimés et de restaurer la version précédente d'un fichier ou d'un document Paper. Ils peuvent ainsi suivre et rétablir les modifications apportées aux données importantes.

Sécurité des données sur les appareils mobiles

- ***Effacement des données***

  Pour renforcer la sécurité, les utilisateurs peuvent activer la suppression de toutes les données Dropbox de leur appareil après dix tentatives de connexion infructueuses.

- ***Espace de stockage interne et fichiers hors ligne***

  Par défaut, les fichiers ne sont pas stockés dans l'espace de stockage interne des appareils mobiles. L'application mobile Dropbox permet toutefois d'enregistrer les fichiers et les dossiers sur l'appareil pour une consultation hors ligne. Lorsqu'un appareil est dissocié d'un compte Dropbox, via l'interface mobile ou Web, ces fichiers et dossiers sont automatiquement supprimés de son espace de stockage interne.

- ***Documents Paper hors ligne***

  Lorsqu'un appareil est dissocié de Paper, via la page de sécurité du compte Dropbox, l'utilisateur est déconnecté et les documents Paper accessibles hors ligne sont automatiquement supprimés de son espace de stockage interne.

Contrôle des équipes

Chaque entreprise étant différente, nous avons développé plusieurs outils permettant aux administrateurs de personnaliser Dropbox Business en fonction des besoins spécifiques de leurs équipes. Dropbox Business intègre des outils permettant aux utilisateurs de renforcer la protection de leur compte et de leurs données. L'authentification, la récupération, la journalisation et les autres fonctionnalités de sécurité ci-dessous sont disponibles dans les différentes interfaces utilisateur de Dropbox.

Vous trouverez ci-dessous une liste des fonctionnalités de contrôle et de visibilité disponibles dans l'interface d'administration de Dropbox Business.

Autorisations granulaires d'accès au contenu

- ***Différents types d'administrateur***

  Dropbox propose différents rôles d'administrateur pour gérer plus efficacement les équipes. Les administrateurs de compte peuvent se voir attribuer l'un des trois niveaux d'accès suivants. Une équipe peut compter un nombre illimité d'administrateurs, et tous les membres de l'équipe peuvent se voir attribuer ce rôle.

- ***Administrateur d'équipe***

  Il peut définir les autorisations de sécurité et de partage de l'équipe, gérer ses membres et attribuer des rôles d'administrateur. L'administrateur d'équipe dispose de l'intégralité des autorisations d'administration disponibles. Il est le seul à pouvoir attribuer le rôle d'administrateur à d'autres membres de l'équipe et à modifier ce rôle. Chaque compte Dropbox Business nécessite au moins un administrateur d'équipe.

- ***Administrateur des utilisateurs***

  L'administrateur des utilisateurs peut accomplir la plupart des tâches de gestion des équipes, notamment ajouter et supprimer des membres, gérer des groupes, ou encore consulter le flux d'activité de l'équipe.

- ***Administrateur d'assistance***

  Il peut répondre aux demandes d'assistance courantes des membres de l'équipe : restauration de fichiers supprimés, résolution des problèmes de validation en deux étapes, etc. L'administrateur d'assistance peut également réinitialiser les mots de passe d'utilisateurs non administrateurs et exporter un journal d'activité pour un membre spécifique de l'équipe.

- ***Administrateur de facturation***

  Il peut accéder aux pages **Facturation** de l'interface d'administration.

- ***Administrateur de contenu***

  Il peut créer et gérer des dossiers d'équipe dans le gestionnaire de contenu.

- ***Administrateur des rapports***

  Il peut créer des rapports dans l'interface d'administration et a accès à la page **Activité**.

- ***Administrateur de sécurité***

  Il peut gérer les alertes de sécurité, le partage externe et les risques de sécurité.

- ***Administrateur de conformité (uniquement disponible pour les équipes ayant souscrit l'option de gouvernance des données)***

  Il peut gérer les pages de gouvernance des données (conservations légales, rétention des données et destruction des données) et a accès au gestionnaire de contenu.

- ***Groupes***

  Les équipes peuvent créer et gérer des groupes pour que leurs membres puissent facilement accéder à certains dossiers. Dropbox peut également synchroniser des groupes Active Directory à l'aide du connecteur Active Directory.

- ***Groupes gérés par l'entreprise***

  Seuls les administrateurs peuvent créer, supprimer et gérer des membres pour ce type de groupe. Les utilisateurs ne peuvent pas demander à rejoindre ou à quitter un groupe géré par l'entreprise.

- ***Groupes gérés par les utilisateurs***

  Les administrateurs choisissent si les utilisateurs peuvent créer et gérer leurs propres groupes. À tout moment, les administrateurs peuvent également transformer un groupe géré par les utilisateurs en groupe géré par l'entreprise afin d'en prendre le contrôle.

- ***Compte unique par ordinateur***

  Les administrateurs peuvent interdire aux membres de l'équipe d'associer un deuxième compte Dropbox à un ordinateur déjà associé à leur compte Dropbox professionnel.

- ***Suspension des comptes***

  Les administrateurs peuvent désactiver l'accès d'un utilisateur à son compte tout en conservant ses données et opérations de partage afin de protéger les données de l'entreprise. Ils peuvent ensuite réactiver le compte ou le supprimer.

- ***Connexion en tant qu'utilisateur***

  Les administrateurs d'équipe peuvent se connecter en tant que membre de leur équipe et accéder ainsi directement aux fichiers, aux dossiers et aux documents Paper de ce membre pour y apporter des modifications, les partager en leur nom et effectuer des audits sur les événements au niveau des fichiers. Les événements de connexion en tant qu'utilisateur sont consignés dans le journal d'activité de l'équipe et signalés ou non aux membres de l'équipe selon les paramètres définis par les administrateurs.

- ***Autorisations de partage***

  Les administrateurs d'équipe sont les seuls à pouvoir gérer les autorisations de partage des membres de leur équipe. Ils peuvent notamment :

  - autoriser ou non les membres de l'équipe à partager des fichiers et des dossiers avec des personnes extérieures à l'équipe ;
  - autoriser ou non les membres de l'équipe à modifier des dossiers appartenant à des personnes extérieures à l'équipe ;
  - activer ou non les liens partagés créés par les membres de l'équipe pour les personnes extérieures à l'équipe ;
  - autoriser ou non les membres de l'équipe à créer des demandes de fichiers et à récupérer des fichiers auprès des membres de l'équipe et/ou de personnes extérieures à l'équipe ;
  - autoriser ou non les utilisateurs à afficher et à ajouter des commentaires sur les fichiers appartenant à l'équipe ;
  - autoriser ou non les membres de l'équipe à partager des documents et des dossiers Paper avec des personnes extérieures à l'équipe ;
  - accorder ou non des autorisations de suppression définitive.

L'administrateur d'équipe d'un compte Dropbox Business peut choisir d'autoriser uniquement les administrateurs d'équipe à supprimer définitivement des fichiers et des documents Paper.

Ajout de nouveaux utilisateurs

Méthodes d'ajout de nouveaux utilisateurs et de gestion des identités

- ***Invitations par e-mail***

  L'interface d'administration de Dropbox Business permet aux administrateurs de générer manuellement des invitations par e-mail.

- ***Active Directory***

  Les administrateurs de Dropbox Business peuvent automatiser la création et la suppression de comptes à partir d'un système Active Directory via notre connecteur Active Directory ou un fournisseur d'identité tiers. Une fois intégré, Active Directory peut être utilisé pour gérer les membres de l'équipe.

- ***Authentification unique***

Vous pouvez configurer Dropbox Business pour que les membres de l'équipe accèdent à leur compte via un fournisseur d'identité centralisé. Notre implémentation de l'authentification unique, qui repose sur le standard SAML 2.0 (Security Assertion Markup Language 2.0), simplifie et sécurise le provisionnement en le déléguant à un fournisseur d'identité fiable et en permettant aux membres de l'équipe d'accéder à Dropbox sans avoir à gérer un mot de passe supplémentaire. Dropbox a également mis en place des partenariats avec les principaux fournisseurs de gestion des identités du marché afin d'automatiser les processus d'ajout de nouveaux utilisateurs et de leur suppression. Pour en savoir plus, consultez la section Intégrations via l'API Dropbox Business ci-dessous.

- ***API***

  L'API Dropbox Business permet aux clients de créer des solutions personnalisées de gestion des identités et d'ajout de nouveaux utilisateurs. Pour en savoir plus, consultez la section Intégrations via l'API Dropbox Business ci-dessous.

Validation en deux étapes

Cette fonctionnalité de sécurité, que nous vous recommandons vivement d'utiliser, ajoute un niveau de protection supplémentaire au compte Dropbox des utilisateurs. Lorsque la validation en deux étapes est activée, Dropbox exige un code de sécurité à six chiffres, en plus du mot de passe, lors de la connexion ou de l'association d'un nouvel ordinateur, d'un nouveau téléphone ou d'une nouvelle tablette.

- Les administrateurs peuvent choisir d'activer la validation en deux étapes pour tous les membres ou seulement certains membres de l'équipe.
- Les administrateurs de compte peuvent identifier les membres de l'équipe pour lesquels la validation en deux étapes est activée.
- Les codes de validation en deux étapes Dropbox sont envoyés par SMS ou via des applications conformes à l'algorithme TOTP (Time-based One-Time Password).
- Si un utilisateur ne peut pas recevoir de code de sécurité via ces méthodes, il peut choisir d'utiliser un code de secours à 16 chiffres à usage unique ou recevoir un code de secours par SMS sur un numéro de téléphone secondaire.
- Dropbox prend également en charge la norme ouverte FIDO Universal 2nd Factor (U2F) qui permet aux utilisateurs de ne plus s'authentifier à l'aide d'un code à six chiffres, mais avec une clé de sécurité USB qu'ils auront configurée.

Programme d'installation pour les entreprises

Les administrateurs qui doivent déployer Dropbox à grande échelle peuvent utiliser notre programme d'installation pour Windows afin d'installer le client de bureau Dropbox à distance et en toute discrétion via des solutions logicielles gérées et des mécanismes de déploiement.

Appareils gérés et connexion

- ***Gestion de la mobilité en entreprise (EMM)***

  Dropbox s'intègre avec des fournisseurs EMM tiers pour permettre aux administrateurs de Dropbox Business avec un forfait Enterprise de mieux contrôler l'utilisation de Dropbox sur les appareils mobiles des membres de l'équipe. Les administrateurs peuvent décider de limiter l'utilisation de l'application mobile Dropbox Enterprise aux appareils gérés (personnels ou fournis par l'entreprise), bénéficier d'une meilleure visibilité sur l'utilisation de l'application (notamment sur le stockage disponible et les emplacements d'accès) et effacer à distance un appareil perdu ou volé. Notez qu'il n'est pas possible de gérer l'application mobile Paper avec une solution EMM.

- ***Approbation des appareils***

  Les administrateurs de Dropbox Education et Dropbox Business avec forfaits Advanced et Enterprise peuvent définir un nombre maximum d'appareils pouvant être synchronisés avec Dropbox et choisir si ces approbations sont gérées par les utilisateurs ou par les administrateurs. Ils peuvent également créer une liste d'exceptions répertoriant les utilisateurs qui ne sont pas limités à un certain nombre d'appareils. Notez que l'application mobile Paper n'est pas incluse dans la fonction d'approbation des appareils.

- ***Validation en deux étapes***

  Les administrateurs peuvent choisir d'activer la validation en deux étapes pour tous les membres ou seulement certains membres de l'équipe. L'implémentation de l'authentification unique pour l'équipe permet également d'appliquer d'autres méthodes d'authentification multifacteur.

- ***Contrôle des mots de passe***

  Les administrateurs de comptes Dropbox Education, Advanced et Enterprise peuvent obliger les membres de leur équipe à définir et gérer des mots de passe longs et complexes. Lorsque cette fonctionnalité est activée, les membres de l'équipe sont déconnectés de toutes leurs sessions Web et ils doivent créer un nouveau mot de passe pour se reconnecter. Un outil intégré analyse le niveau de sécurité des mots de passe en les comparant à une base de données de mots de passe, noms, schémas et numéros couramment utilisés. Si un utilisateur définit un mot de passe trop commun, il est invité à en saisir un plus complexe et plus difficile à deviner. Les administrateurs peuvent également réinitialiser les mots de passe, soit pour l'ensemble de l'équipe, soit au cas par cas.

- ***Gestion de domaines***

  Dropbox fournit aux entreprises un certain nombre d'outils pour simplifier et accélérer les opérations d'ajout d'utilisateurs et de contrôle de l'utilisation de Dropbox.

  - **Validation du domaine**
    Les entreprises peuvent revendiquer la priorité de leurs domaines et accéder à d'autres outils de gestion des noms de domaine.

  - **Obligation à rejoindre l'équipe**
    Cette fonctionnalité permet aux administrateurs de s'assurer que les détenteurs d'un compte Dropbox personnel invités à rejoindre l'équipe Dropbox de l'entreprise migrent vers la Dropbox d'équipe ou modifient l'adresse e-mail associée à leur compte personnel.

  - **Visibilité sur le domaine**
    Cette fonctionnalité fournit des informations clés aux administrateurs, telles que le nombre de comptes Dropbox personnels qui utilisent des adresses e-mail de l'entreprise.

  - **Capture de compte**
    Cette fonctionnalité permet aux administrateurs d'obliger les utilisateurs Dropbox qui utilisent une adresse e-mail d'entreprise à rejoindre l'équipe Dropbox de l'entreprise ou à modifier l'adresse e-mail de leur compte personnel.

- ***Contrôle des sessions Web***

  Les administrateurs peuvent contrôler la durée de connexion des membres de l'équipe à dropbox.com. Ils peuvent limiter la durée de toutes les sessions Web et/ou des sessions inactives. Lorsqu'une session atteint le délai fixé, l'utilisateur est automatiquement déconnecté. Les administrateurs peuvent également suivre et mettre fin aux sessions Web de chaque utilisateur.

- ***Accès aux applications***

  Les administrateurs peuvent savoir quelles applications tierces ont accès aux comptes des utilisateurs et révoquer cet accès.

- ***Dissociation d'appareils***

  L'administrateur peut dissocier des ordinateurs ou appareils mobiles connectés à des comptes utilisateur depuis l'interface d'administration. Les utilisateurs peuvent également effectuer cette opération

depuis les paramètres de sécurité de leur compte. Sur un ordinateur, la dissociation efface les données d'authentification et permet de supprimer la copie locale des fichiers dès la prochaine connexion de l'ordinateur à Internet (voir la section **Effacement à distance** ci-dessous). Sur les appareils mobiles, la dissociation élimine les fichiers accessibles hors ligne, les données mises en cache et les informations de connexion. Elle supprime également les documents Paper de l'application mobile Paper. Lorsque la validation en deux étapes est activée, les utilisateurs doivent procéder à une nouvelle authentification de leur appareil s'ils souhaitent l'associer de nouveau à Dropbox. Enfin, les utilisateurs peuvent également configurer leurs paramètres afin de recevoir automatiquement un e-mail de notification en cas d'association d'un appareil à leur compte Dropbox.

- ***Contrôle réseau***

  Les administrateurs de Dropbox Business avec un forfait Enterprise peuvent restreindre l'utilisation de Dropbox sur le réseau de l'entreprise pour uniquement autoriser les comptes d'équipe Enterprise. Cette fonctionnalité s'intègre avec la solution de sécurité réseau de l'entreprise afin de bloquer tout trafic hors du compte approuvé sur les ordinateurs. Notez qu'il n'est pour le moment pas possible de gérer Paper via le contrôle réseau.

Sécurité mobile

- ***Lecteur d'empreintes digitales***

  Les utilisateurs peuvent activer Touch ID ou Face ID sur les appareils iOS et le déverrouillage par empreinte digitale sur les appareils Android compatibles pour déverrouiller l'application mobile Dropbox.

Visibilité sur les accès

- ***Vérification d'identité à des fins d'assistance technique***

  Avant toute tentative de dépannage ou tout envoi d'informations sur un compte par le service d'assistance Dropbox, l'administrateur du compte doit fournir un code de sécurité aléatoire à usage unique pour confirmer son identité. Ce code PIN n'est disponible que via l'interface d'administration.

Activité relative aux comptes des utilisateurs

Pour obtenir des informations actualisées sur l'activité relative à leur compte, les utilisateurs ont accès aux pages suivantes à partir des paramètres de leur compte.

- ***Page Partagé***

  Cette page affiche les dossiers partagés disponibles dans la Dropbox de l'utilisateur, ainsi que ceux que l'utilisateur peut ajouter. Un utilisateur peut annuler le partage de certains dossiers et fichiers, et définir des autorisations de partage.

- ***Page Fichiers***

  Cette page affiche les fichiers partagés avec l'utilisateur et indique à quelle date ce partage a eu lieu. L'utilisateur peut supprimer l'accès à ces fichiers. Pour afficher les documents Paper partagés avec lui, l'utilisateur peut cliquer sur **Partagés avec moi** depuis l'onglet **Documents** de l'interface Web Paper.

- ***Page Liens***

  Cette page affiche tous les liens partagés créés par l'utilisateur avec leur date de création. Elle répertorie également tous les liens que d'autres membres ont partagés avec l'utilisateur. L'utilisateur peut désactiver des liens ou modifier les autorisations.

- ***Notifications par e-mail***

  Les utilisateurs peuvent choisir de recevoir une notification par e-mail immédiate en cas d'association d'un nouvel appareil ou d'une nouvelle application à leur compte Dropbox.

Autorisations relatives aux comptes utilisateur

- ***Appareils associés***

  La section **Appareils**, accessible depuis les paramètres de sécurité d'un compte utilisateur, affiche tous les ordinateurs et appareils mobiles associés à ce compte. Pour chaque ordinateur, l'adresse IP, le pays et l'heure approximative de l'activité la plus récente sont indiqués. Les utilisateurs ont la possibilité de dissocier n'importe quel appareil et de supprimer, par la même occasion, tous les fichiers qui y sont stockés lors de sa prochaine connexion à Internet.

- ***Sessions Web actives***

  La section **Sessions** affiche tous les navigateurs Web actuellement connectés au compte Dropbox de l'utilisateur. Pour chacun d'eux, l'adresse IP, le pays, l'heure d'ouverture de la dernière session et l'heure approximative de l'activité la plus récente sont indiqués. Les utilisateurs peuvent fermer n'importe quelle session à distance à partir des paramètres de sécurité de leur compte.

- ***Applications associées***

  La section **Applications connectées** dresse la liste de toutes les applications tierces ayant accès au compte de l'utilisateur, ainsi que le type d'accès de chacune d'elles. Les utilisateurs peuvent révoquer l'accès d'une application à leur compte Dropbox.

Flux d'activité

Dropbox Business enregistre les actions liées aux fichiers dans le flux d'activité de l'équipe, consultable depuis l'interface d'administration. Ce flux d'activité 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. Le flux d'activité peut être exporté sous forme de rapport téléchargeable au format CSV 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. Les événements de contenu suivants sont enregistrés dans le flux d'activité :

- ***Partage de fichiers, dossiers et liens***

  Le cas échéant, les rapports indiquent si ces événements impliquent des personnes extérieures à l'équipe.

  Fichiers partagés

  - Ajout ou suppression d'un membre de l'équipe ou d'un membre extérieur à l'équipe
  - Modification des autorisations d'un membre de l'équipe ou d'un membre extérieur à l'équipe
  - Ajout ou suppression d'un groupe
  - Ajout d'un fichier partagé dans la Dropbox d'un utilisateur
  - Affichage du contenu d'un fichier ayant été partagé par le biais d'une invitation à rejoindre un fichier ou un dossier
  - Copie du contenu partagé dans la Dropbox d'un utilisateur
  - Téléchargement du contenu partagé
  - Ajout de commentaires dans un fichier

- Résolution ou annulation de la résolution d'un commentaire
- Suppression d'un commentaire
- Abonnement ou désabonnement aux notifications de commentaires
- Invitation à rejoindre un fichier appartenant à l'équipe
- Demande d'accès à un fichier appartenant à l'équipe
- Annulation du partage d'un fichier

Dossiers partagés

- Création d'un nouveau dossier partagé
- Ajout ou suppression d'un membre de l'équipe, d'un membre extérieur à l'équipe ou d'un groupe
- Ajout d'un dossier partagé dans la Dropbox d'un utilisateur ou suppression de l'accès à un dossier partagé par l'utilisateur lui-même
- Ajout d'un dossier partagé à partir d'un lien
- Modification des autorisations d'un membre de l'équipe ou d'un membre extérieur à l'équipe
- Transfert de la propriété d'un dossier à un autre utilisateur
- Annulation du partage d'un dossier
- Demande d'ajout comme membre d'un dossier partagé
- Demande d'accès à un dossier partagé
- Ajout d'un utilisateur qui en fait la demande à un dossier partagé
- Autorisation ou interdiction pour les membres extérieurs à l'équipe de rejoindre un dossier
- Autorisation pour tous les membres de l'équipe ou pour le propriétaire seulement d'ajouter des personnes à un dossier
- Modification de l'accès d'un groupe à un dossier partagé

Liens partagés

- Création ou suppression d'un lien
- Autorisation pour tous ou seulement certains membres de l'équipe de voir le contenu associé à un lien
- Protection par mot de passe du contenu d'un lien
- Configuration ou suppression du délai de validité d'un lien
- Consultation d'un lien
- Téléchargement du contenu associé à un lien
- Copie du contenu associé à un lien dans la Dropbox d'un utilisateur
- Création d'un lien vers un fichier via une API
- Partage d'un lien avec un membre de l'équipe, un membre extérieur à l'équipe ou un groupe
- Autorisation ou interdiction pour les personnes extérieures à l'équipe de voir des liens vers des fichiers se trouvant dans un dossier partagé
- Partage d'un album

Demandes de fichiers

- Création, modification, clôture ou suppression d'une demande de fichiers
- Ajout d'utilisateurs à une demande de fichiers
- Ajout ou suppression de la date d'expiration d'une demande de fichiers
- Modification du dossier d'une demande de fichiers
- Réception de fichiers via une demande de fichiers
- Réception de fichiers via Email to Dropbox

Événements relatifs à des fichiers ou à des dossiers individuels

- Ajout d'un fichier à Dropbox
- Création d'un dossier
- Consultation d'un fichier
- Modification d'un fichier
- Téléchargement d'un fichier
- Copie d'un fichier ou d'un dossier
- Déplacement d'un fichier ou d'un dossier
- Modification du nom d'un fichier ou d'un dossier
- Rétablissement d'une version précédente d'un fichier
- Annulation des modifications apportées aux fichiers
- Restauration d'un fichier supprimé
- Suppression d'un fichier ou d'un dossier
- Suppression définitive d'un fichier ou d'un dossier

Réussite ou échec de connexion

- Tentative de connexion réussie ou non
- Échec de la tentative de connexion ou erreur via l'authentification unique
- Échec de la tentative de connexion ou erreur via EMM
- Déconnexion
- Modification de l'adresse IP pour la session Web

Mots de passe

Modification des paramètres de mot de passe ou de validation en deux étapes. Les administrateurs ne peuvent pas voir le mot de passe des utilisateurs.

- Modification ou réinitialisation de mot de passe
- Activation, réinitialisation ou désactivation de la validation en deux étapes
- Configuration ou modification de la validation en deux étapes pour utiliser des SMS ou une application mobile

- Ajout, modification ou suppression d'un numéro de téléphone secondaire pour la validation en deux étapes
- Ajout ou suppression d'une clé de sécurité pour la validation en deux étapes

Gestion des membres

Ajout et suppression de membres d'équipe

- Invitation d'un membre à rejoindre l'équipe
- Ajout d'un membre à l'équipe
- Suppression d'un membre de l'équipe
- Suspension ou annulation de la suspension d'un membre de l'équipe
- Restauration d'un membre de l'équipe ayant été supprimé
- Demande d'ajout à l'équipe en fonction du domaine du compte
- Approbation ou refus d'une demande d'ajout à l'équipe en fonction du domaine du compte
- Envoi d'une invitation à rejoindre un domaine à des comptes de domaine existants
- Ajout d'un utilisateur à l'équipe dans le cadre de la capture de compte
- Suppression d'un utilisateur du domaine dans le cadre de la capture de compte
- Autorisation ou interdiction pour les membres de l'équipe de suggérer de nouveaux membres à ajouter à l'équipe
- Suggestion d'ajout d'un membre à l'équipe

Applications

Opérations d'association d'applications tierces aux comptes Dropbox

- Ajout ou suppression d'une application
- Ajout ou suppression d'une application d'équipe

Appareils

Association d'ordinateurs ou d'appareils mobiles aux comptes Dropbox

- Association ou dissociation d'un appareil
- Utilisation de la fonctionnalité d'effacement à distance et suppression réussie de tous les fichiers ou échec de la suppression de certains fichiers
- Modification de l'adresse IP pour l'ordinateur de bureau ou l'appareil mobile

Actions d'administration

Modifications apportées aux paramètres de l'interface d'administration (autorisations d'accès aux dossiers partagés, par exemple)

- ***Authentification classique et authentification unique***
  - Réinitialisation du mot de passe d'un membre de l'équipe
  - Réinitialisation du mot de passe de tous les membres de l'équipe
  - Autorisation ou interdiction pour les membres de l'équipe de désactiver la validation en deux étapes

- Activation ou désactivation de l'authentification unique
- Activation de la connexion obligatoire via l'authentification unique
- Modification ou suppression de l'URL d'authentification unique
- Mise à jour du certificat d'authentification unique
- Modification du mode d'identité de l'authentification unique

- ***Gestion des membres***
  - Autorisation ou interdiction pour les utilisateurs de demander à être ajoutés à l'équipe en fonction du domaine du compte
  - Approbation automatique des demandes d'adhésion à l'équipe ou demande d'approbation manuelle par un administrateur

- ***Gestion des comptes utilisateur***
  - Modification du nom d'un membre de l'équipe
  - Modification de l'adresse e-mail d'un membre de l'équipe
  - Attribution ou suppression de droits d'administrateur, ou modification du rôle d'administrateur
  - Connexion ou déconnexion en tant que membre de l'équipe
  - Transfert ou suppression du contenu d'un compte utilisateur supprimé
  - Suppression définitive du contenu d'un compte utilisateur supprimé

- ***Paramètres de partage généraux***
  - Autorisation ou interdiction pour les membres de l'équipe d'ajouter des dossiers partagés appartenant à des membres extérieurs à l'équipe
  - Autorisation ou interdiction pour les membres de l'équipe de partager des dossiers avec des personnes extérieures à l'équipe
  - Affichage d'avertissements pour les utilisateurs qui s'apprêtent à partager des dossiers avec des membres extérieurs à l'équipe
  - Autorisation ou interdiction pour les membres extérieurs à l'équipe de voir les liens partagés
  - Configuration des liens partagés afin de les rendre accessibles uniquement aux membres de l'équipe par défaut
  - Autorisation ou interdiction pour les utilisateurs de commenter les fichiers
  - Autorisation ou interdiction pour les membres de l'équipe de créer des demandes de fichiers
  - Ajout, modification ou suppression d'un logo pour les pages de liens partagés
  - Autorisation ou interdiction pour les membres de l'équipe de partager des documents et des dossiers Paper avec des personnes extérieures à l'équipe

- ***Gestion des dossiers d'équipe pour les fichiers***
  - Création d'un dossier d'équipe
  - Modification du nom d'un dossier d'équipe
  - Archivage ou annulation de l'archivage d'un dossier d'équipe
  - Suppression définitive d'un dossier d'équipe
  - Transformation d'un dossier d'équipe en dossier partagé

- ***Gestion de domaines***
  - Tentative de validation ou validation réussie d'un domaine, ou suppression d'un domaine
  - Validation ou suppression d'un domaine par l'assistance Dropbox
  - Activation ou désactivation de l'envoi d'invitations à rejoindre un domaine
  - Activation ou désactivation de la fonctionnalité d'invitation automatique des nouveaux utilisateurs
  - Modification du mode de capture de compte
  - Approbation ou révocation de la capture de compte par l'assistance Dropbox
- ***Gestion de la mobilité en entreprise (EMM)***
  - Activation d'EMM en mode test (facultatif) ou déploiement (obligatoire)
  - Actualisation du jeton EMM
  - Ajout ou suppression de membres de l'équipe dans la liste des utilisateurs non éligibles au programme EMM
  - Désactivation d'EMM
  - Création d'un rapport de liste des exceptions EMM
  - Création d'un rapport d'utilisation de l'application mobile EMM
- ***Modification d'autres paramètres d'équipe***
  - Fusion d'équipes
  - Passage de l'équipe à Dropbox Business ou à une équipe gratuite
  - Modification du nom de l'équipe
  - Création d'un rapport d'activité d'équipe
  - Autorisation ou interdiction pour les membres de l'équipe d'avoir plusieurs comptes associés à un ordinateur
  - Autorisation pour tous les membres de l'équipe ou les administrateurs seulement de créer des groupes
  - Autorisation ou interdiction pour les membres de l'équipe de supprimer définitivement des fichiers
  - Démarrage ou arrêt d'une session d'assistance Dropbox pour un revendeur

Groupes

Informations relatives à la création, à la suppression et à la gestion des membres de groupes

- Création, suppression, déplacement d'un groupe ou changement de son nom
- Ajout ou suppression d'un membre
- Modification du type d'accès d'un membre du groupe
- Attribution de la gestion d'un groupe à l'équipe ou à l'administrateur
- Changement de l'identifiant externe d'un groupe

Journal d'activité Paper

Les administrateurs peuvent sélectionner un type d'activité Paper dans le flux d'activité ou télécharger un rapport d'activité complet. Les événements Paper consignés sont les suivants :

- Activation ou désactivation de Paper
- Création, modification, exportation, archivage, suppression définitive et restauration d'un document Paper
- Commentaires et résolution de commentaires dans un document Paper
- Partage et annulation du partage d'un document Paper avec des membres de l'équipe et des membres extérieurs à l'équipe
- Demande d'accès à un document Paper de la part de membres de l'équipe et de membres extérieurs à l'équipe
- Mentions de membres de l'équipe et de membres extérieurs à l'équipe dans un document Paper
- Consultation d'un document Paper par des membres de l'équipe et des membres extérieurs à l'équipe
- Suivi d'un document Paper
- Modification des autorisations d'accès à un document Paper (modification, commentaire ou lecture seule)
- Modification des règles de partage externe d'un document Paper
- Création, archivage et suppression définitive d'un dossier Paper
- Ajout ou suppression d'un document Paper dans un dossier
- Modification du nom d'un dossier Paper
- Transfert d'un document ou d'un dossier Paper

Dropbox Passwords

Dropbox Passwords est un moyen simple et sécurisé de stocker, synchroniser et renseigner automatiquement les noms d'utilisateur, les mots de passe et les cartes bancaires sur tous les appareils pour protéger vos identifiants en ligne. Dropbox Passwords protège les données sensibles de votre compte en ligne à l'aide du chiffrement à divulgation nulle de connaissance dans le cloud comme sur vos appareils. Nos produits sont conçus pour une utilisation quotidienne et sont sécurisés dès la conception.

Chiffrement à divulgation nulle de connaissance

Dropbox Passwords stocke vos données chiffrées dans le cloud, mais les clés permettant de les déchiffrer sont stockées sur vos appareils uniquement. **Dropbox n'y a jamais accès.** Ces clés sont longues, aléatoires et générées sur votre appareil. Elles ne quittent jamais votre appareil, sauf lorsque vous décidez d'associer ou d'enregistrer un nouvel appareil. Ce transfert utilise le chiffrement à clé publique pour signer et protéger les clés pendant le transfert, de sorte que vous pouvez être certain que personne d'autre ne peut les déchiffrer tout en vérifiant qu'elles sont authentiques. Cette propriété est souvent appelée chiffrement à divulgation nulle de connaissance, car les données chiffrées sont inutilisables pour quiconque ne possède pas les clés, y compris Dropbox. Cela signifie que **vous seul pouvez consulter vos informations** et que dans le cas improbable où Dropbox serait piraté, vos informations seraient toujours en sécurité. Les données chiffrées sont séparées des dossiers Dropbox visibles et ne peuvent pas être consultées à l'aide des clients ou des API Dropbox.

Détails du chiffrement

Dropbox chiffre vos données en utilisant XChaCha20-Poly1305 en mode combiné pour une authentification implicite. Nos extensions de navigateur et nos applications mobiles utilisent toutes des implémentations de chiffrement reposant sur libsodium, qui est une branche vérifiée et largement distribuée de la bibliothèque NaCl.

Chaque opération de chiffrement génère un nonce aléatoire de 192 bits, qui est stocké avec la charge utile chiffrée en vue d'un déchiffrement ultérieur. Contrairement à AES-GCM, XChaCha20-Poly1305 prend en charge les nonces aléatoires. Lors du déchiffrement, le nonce de 192 bits est lu dans la charge utile et utilisé pour déchiffrer la charge utile chiffrée. Tout chiffrement ultérieur génère un nonce aléatoire de 192 bits indépendant du nonce précédent. Dropbox Passwords génère des nombres aléatoires à l'aide de libsodium, qui utilise par défaut un générateur de nombres aléatoires sécurisé par chiffrement sur chacune des plateformes que nous prenons en charge.

Clés et mots de récupération

Nous générons une clé symétrique de 256 bits (la clé de chiffrement) à partir de 128 bits d'entropie (la clé d'utilisateur) via le hachage Blake2. Cette clé de chiffrement reste uniquement sur les appareils de son propriétaire et, dans la mesure du possible, dans le stockage le plus sûr auquel nous avons accès sur ces appareils. Par exemple, sur les iPhone, nous stockons la clé de chiffrement dans le trousseau iOS.

Nous utilisons 128 bits d'entropie comme source parce qu'elle offre une sécurité suffisante tout en ne nécessitant que 12 mots de récupération avec la norme BIP-39 pour la sauvegarde. La phrase mnémonique BIP-39 offre un moyen convivial de représenter des clés aléatoires de grande taille en les transformant en une liste de 12 mots. Chaque clé de 128 bits correspond à une liste de mots et chaque liste de 12 mots identifie de manière unique les 128 bits. La seule réserve est que les 12 mots correspondent en fait à 132 bits, de sorte que les quatre bits supplémentaires sont utilisés comme somme de contrôle pour identifier les erreurs. Les mots de récupération vous permettent de récupérer votre clé de chiffrement en cas de perte ou de vol de votre appareil. Nous vous recommandons de les imprimer et de les conserver en lieu sûr. Vous pouvez également les confier à un ami ou à un membre de la famille en qui vous avez confiance ou les stocker sur une clé USB.

Enregistrement d'un appareil

Lorsqu'un utilisateur se connecte à Dropbox Passwords sur un nouvel appareil, ce dernier doit suivre une procédure d'enregistrement sécurisée pour accéder aux données Passwords de l'utilisateur. Cette procédure permet de s'assurer que la clé secrète et les données Passwords d'un utilisateur ne sont accessibles que sur les appareils enregistrés de l'utilisateur. Elle permet également de s'assurer qu'un utilisateur ne peut enregistrer d'appareils supplémentaires que s'il a accès à un appareil déjà enregistré ou à ses mots de passe de récupération. La procédure d'enregistrement de l'appareil se déroule comme suit.

L'appareil en cours d'enregistrement génère aléatoirement une paire de clés publiques/privées de 256 bits et importe la clé publique sur le serveur Dropbox. Ensuite, le scénario **A**, **B** ou **C** se produit.

A : si l'utilisateur n'a pas encore enregistré d'appareil, l'appareil en cours d'enregistrement génère aléatoirement une clé d'utilisateur secrète de 128 bits. La paire de clés de l'utilisateur et la paire de clés de l'appareil sont toutes les deux stockées dans un emplacement sécurisé du système d'exploitation, comme le décrit la section Stockage des clés suivante. L'appareil initialise les données Passwords de l'utilisateur, les chiffre et importe la charge utile chiffrée sur le serveur Dropbox.

B : si l'utilisateur possède un ou plusieurs appareils déjà enregistrés, une demande d'approbation de l'enregistrement est envoyée à chacun de ces appareils. La clé publique de l'appareil en cours d'enregistrement est jointe à la demande. L'utilisateur doit alors approuver la demande sur l'un de ses appareils enregistrés. En cas d'approbation, l'appareil enregistré chiffre la clé d'utilisateur à l'aide de sa clé privée et de la clé publique de l'appareil en cours d'enregistrement via X25519 ECDH avec XSalsa20-Poly1305. L'appareil enregistré importe la clé d'utilisateur chiffrée sur le serveur Dropbox pour l'envoyer à l'appareil en cours d'enregistrement. Ce dernier télécharge et déchiffre la clé d'utilisateur à l'aide de sa clé privée et de la clé publique de l'appareil enregistré. L'appareil en cours d'enregistrement télécharge ensuite les données de la charge utile Passwords chiffrée et la déchiffre à l'aide de la clé d'utilisateur.

C : si l'utilisateur a déjà enregistré un appareil, mais qu'il ne peut plus y accéder, il peut saisir ses 12 mots de récupération pour reconstruire en local la clé d'utilisateur. L'appareil en cours d'enregistrement télécharge ensuite les données de la charge utile Passwords chiffrée et la déchiffre à l'aide de la clé d'utilisateur.

Stockage des clés

Extensions de navigateur

Sur les navigateurs Web, la clé d'utilisateur est stockée dans la zone de stockage local de l'extension du navigateur. Les valeurs de stockage local de l'extension du navigateur ne sont accessibles qu'à partir de l'extension. Le code exécuté dans les sites Web consultés par l'utilisateur ne peut pas être lu depuis la zone de stockage local de l'extension du navigateur. En outre, les extensions de navigateur interdisent l'exécution de tout code qui n'est pas inclus dans le package d'extension signé, ce qui élimine le risque d'une vulnérabilité XSS qui permettrait d'accéder aux valeurs de stockage local.

Un pirate disposant d'un accès illimité à l'appareil de l'utilisateur peut accéder à la clé de l'utilisateur en lisant le fichier de stockage local sur le disque. Parmi les exemples de menaces, on peut citer : un pirate ayant un accès physique à l'appareil ou un pirate qui exécute un programme malveillant sur l'appareil. Pour se protéger, l'utilisateur peut configurer une phrase secrète locale sur son appareil.

Lorsqu'une phrase secrète est configurée, la clé d'utilisateur est chiffrée au repos dans le stockage local de l'extension du navigateur. La clé de chiffrement est déduite de la phrase secrète via le hachage de mots de passe Argon2, et la méthode de chiffrement utilisée est XChaCha20-Poly1305. Chaque fois que l'extension du navigateur redémarre, l'utilisateur doit fournir sa phrase secrète pour déchiffrer la clé d'utilisateur et déverrouiller ses données. Par conséquent, un pirate qui ne dispose pas de la phrase secrète n'est pas en mesure de déchiffrer la clé d'utilisateur stockée dans le fichier de stockage local sur le disque.

iOS

Sur iOS, la clé d'utilisateur est stockée dans le trousseau iOS, qui est un fichier de base de données chiffré sur le disque. Ce fichier est chiffré à l'aide d'une clé secrète stockée dans le module matériel Secure Enclave, en utilisant la méthode de chiffrement AES256-GCM. Seule l'application iOS Dropbox Passwords signée peut accéder aux éléments qu'elle a stockés dans le trousseau. Cela permet d'éviter que d'autres codes exécutés sur l'appareil de l'utilisateur n'accèdent à la clé d'utilisateur.

Android

Sur Android, la clé d'utilisateur est stockée dans un objet EncryptedSharedPreferences, qui est un fichier de préférences chiffré sur le disque. Ce fichier est chiffré à l'aide d'une clé principale stockée dans le matériel sécurisé du magasin de clés Android, en utilisant la méthode de chiffrement AES256-GCM. Seule l'application Android Dropbox Passwords signée peut accéder à la clé principale utilisée pour déchiffrer le fichier de préférences.

Authentification locale

Dropbox Passwords propose des mesures d'authentification locale facultatives pour restreindre davantage l'accès aux données Passwords d'un utilisateur sur son appareil physique. Pour les applications mobiles, le geste d'authentification du système d'exploitation local peut être réutilisé (c'est-à-dire un code secret avec une authentification biométrique supplémentaire). Pour les extensions de navigateur, vous pouvez également configurer une phrase secrète. Ces méthodes offrent un niveau de sécurité supplémentaire pour les applications lorsque le système d'exploitation de l'appareil de l'utilisateur est déverrouillé. Cela permet à l'utilisateur de sécuriser ses données Passwords lorsqu'un autre utilisateur peut accéder à son appareil, un membre de sa famille ou un collègue de travail, par exemple.

Suggestion de mots de passe sécurisés

Dropbox a développé l'outil open source zxcvbn qui est utilisé par plusieurs gestionnaires de mots de passe pour estimer le niveau de sécurité des mots de passe. Cet outil compare les mots de passe à une base de données de 30 000 mots de passe courants, de noms et prénoms courants d'après les données du recensement américain, de mots anglais populaires tirés de Wikipédia, de la télévision et des films américains, et d'autres modèles courants tels que les dates, les répétitions (aaa), les séquences (abcd), les modèles de clavier (qwertyuiop) et le Leet (1337) Speak. Si le mot de passe qu'un utilisateur tente de saisir est considéré comme courant, l'outil l'invite à saisir un mot de passe plus unique et plus difficile à deviner. L'utilisation du paramètre **Très fort** permet de garantir aux utilisateurs le niveau de sécurité le plus élevé pour leur compte.

Sécurité des données, confidentialité et transparence

Chaque jour, les particuliers et les entreprises confient à Dropbox leur travail le plus important. Il relève de notre responsabilité de protéger ces informations et de veiller au respect de leur confidentialité.

Politique de confidentialité

Notre politique de confidentialité est disponible à l'adresse dropbox.com/privacy. La politique de confidentialité, le contrat de service, les conditions d'utilisation et la politique d'utilisation acceptable de Dropbox stipulent les informations suivantes :

- Les types de données que nous collectons et pourquoi nous les collectons.
- Les entités avec lesquelles nous sommes susceptibles de partager ces informations.

- Les méthodes de protection de ces données et leur durée de rétention.
- Les emplacements où les données sont hébergées et transférées.
- La marche à suivre en cas de question ou de modification des règles.

Transparence

Nous nous engageons à faire preuve de la plus grande transparence possible concernant les demandes d'informations émanant des autorités chargées de l'application des lois, et concernant la fréquence et la nature de ces demandes. Nous examinons toutes les demandes d'informations afin de nous assurer qu'elles respectent la loi et informons les utilisateurs, dans les limites autorisées par la loi, lorsque l'accès aux informations de leur compte est requis par les autorités compétentes.

Ces efforts soulignent notre engagement en faveur de la confidentialité des utilisateurs et de leurs données. C'est pourquoi nous tenons à jour un rapport de transparence et avons défini un ensemble de principes relatifs aux demandes émanant des autorités. Les principes ci-dessous régissent nos actions lorsque nous recevons, examinons et répondons aux demandes d'accès aux données de nos utilisateurs émanant des autorités.

- ***Faire preuve de transparence***

  Nous pensons que les services en ligne devraient pouvoir publier le nombre et le type de demandes reçues de la part des autorités, et notifier les individus concernés par ces demandes. Ce type de transparence permet aux utilisateurs de mieux comprendre les demandes abusives de certaines administrations. Nous continuerons à publier des informations détaillées sur ces demandes et à plaider pour le droit à fournir davantage de ces informations importantes.

- ***Lutter contre les demandes trop vagues***

  Les demandes de données émanant des autorités devraient être limitées à des personnes spécifiques et à des enquêtes justifiées. Nous lutterons contre les demandes non ciblées et trop vagues.

- ***Protéger tous les utilisateurs***

  Les lois accordant différentes protections aux individus en fonction de leur pays de résidence ou de leur citoyenneté sont obsolètes et ne reflètent pas la nature internationale des services en ligne. Nous continuerons de plaider pour la réforme de ces lois.

- ***Fournir des services de confiance***

  Les gouvernements ne devraient jamais être autorisés à installer des portes dérobées sur les services en ligne ni compromettre l'infrastructure pour obtenir des données sur les utilisateurs. Nous continuerons à faire tout notre possible pour protéger nos systèmes et faire modifier la législation afin d'établir clairement que ce type d'activité est illégal.

Nos rapports de transparence sont disponibles à l'adresse dropbox.com/transparency.

Certifications de confidentialité, attestation et conformité réglementaire

Chaque jour, les particuliers et les entreprises confient à Dropbox leurs fichiers professionnels les plus importants. Il relève donc de notre responsabilité de les protéger et de veiller au respect de leur confidentialité. Notre engagement en faveur de la confidentialité est au cœur de chacune de nos décisions.

Code de pratique ISO/IEC 27018 pour la protection des données personnelles dans le cloud et norme ISO/IEC 27701 (extension des normes de sécurité de l'information ISO/IEC 27001 et ISO/IEC 27002) pour le management de la protection de la vie privée

Dropbox Business est l'un des premiers grands fournisseurs de services cloud à avoir obtenu la certification ISO/IEC 27018 et ISO/IEC 27701.

ISO/IEC 27018 est une norme mondiale relative à la confidentialité et à la protection des données dans le cloud. Publiée en août 2014, elle a été conçue spécifiquement pour garantir le respect de la confidentialité des données des utilisateurs.

Première norme internationale certifiable pour le management de la protection de la vie privée, ISO/IEC 27701 a été publiée en 2019 pour fournir un cadre pour compléter le système de gestion de la sécurité de l'information (ISMS - Information security management system) de la norme ISO/IEC 27001 et créer ainsi un système de gestion des informations de confidentialité (PIMS - Privacy information management system) incluant des considérations relatives à la confidentialité des données.

Ces normes imposent de nombreuses obligations que Dropbox doit suivre en matière d'utilisation des données d'entreprise :

- ***Votre organisation garde le contrôle de ses données***

  Nous utilisons les informations personnelles que vous nous transmettez uniquement dans le but de vous fournir les services que vous avez souscrits. Vous pouvez à tout moment ajouter, modifier ou supprimer des fichiers et des documents Paper dans votre Dropbox.

- ***Nous garantissons la transparence de vos données***

  Vous pouvez à tout moment connaître l'endroit où vos données sont hébergées sur nos serveurs, ainsi que les partenaires de confiance avec lesquels nous travaillons. Nous vous expliquons clairement toutes les implications liées à la clôture d'un compte ou à la suppression d'un fichier ou d'un document Paper. Enfin, nous vous tenons informé si l'un de ces éléments change.

- ***Vos données sont en sécurité***

  Les normes ISO/IEC 27018 et ISO/IEC 27701 complètent et améliorent la norme ISO/IEC 27001, l'une des normes de sécurité des données les plus reconnues au niveau international. Nous avons reçu le renouvellement de la certification ISO/IEC 27001 en octobre 2021.

- ***Nos pratiques sont régulièrement examinées***

  Afin de conserver les certifications ISO/IEC 27018, ISO/IEC 27701 et ISO/IEC 27001, nous ferons l'objet d'audits annuels réalisés par un organisme tiers indépendant. Pour consulter tous nos certificats ISO, cliquez ici.

Transfert de données

Lors du transfert de données depuis l'Union européenne, l'espace économique européen, le Royaume-Uni et la Suisse, Dropbox utilise plusieurs dispositifs juridiques tels que les contrats nous liant à nos clients et à nos filiales, les clauses contractuelles types et les décisions d'adéquation de la Commission européenne concernant certains pays, le cas échéant.

Dropbox respecte les cadres Privacy Shield établis entre l'Union européenne et les États-Unis et entre la Suisse et les États-Unis. Ces cadres ont été établis par le ministère du Commerce des États-Unis relativement à la collecte, l'utilisation et la rétention des données personnelles transférées aux États-Unis à partir de l'Union

européenne, de l'espace économique européen, du Royaume-Uni et de la Suisse, bien que Dropbox n'utilise pas les cadres Privacy Shield établis entre l'Union européenne et les États-Unis et entre la Suisse et les États-Unis comme base légale pour les transferts de données personnelles. Dropbox a certifié auprès du ministère du Commerce qu'elle adhère aux principes du Privacy Shield en ce qui concerne ces données. Pour en savoir plus sur le Privacy Shield, vous pouvez également consulter le site https://www.privacyshield.gov.

Toute réclamation ou tout litige ayant trait à notre conformité avec le programme Privacy Shield fait l'objet d'un examen mené à bien par un prestataire tiers indépendant, JAMS. Pour en savoir plus, consultez notre politique de confidentialité (dropbox.com/privacy).

Règlement général sur la protection des données (RGPD) européen

Le RGPD (Règlement général sur la protection des données) est une réglementation instaurée par l'Union européenne en 2018 qui définit un cadre juridique complet pour le traitement et la protection des données personnelles.

Dropbox s'engage à assurer la sécurité et la protection des données de ses utilisateurs dans le respect de la législation et des bonnes pratiques, et ce en permanence. Dans cette optique, nous avons tout mis en œuvre pour que Dropbox soit conforme au RGPD, notamment en désignant un délégué à la protection des données, en repensant notre programme relatif à la confidentialité pour s'assurer que les utilisateurs peuvent exercer leurs droits sur leurs données, en documentant nos mécanismes de traitement des données et en renforçant nos processus internes pour faire face à une éventuelle faille de sécurité. Nous continuons à adapter nos processus et pratiques afin qu'ils soient toujours conformes aux nouvelles règles édictées par les autorités chargées de la protection des données.

Code de conduite de l'UE pour le cloud

Le code de conduite de l'UE pour le cloud est un outil dont l'utilisation est basée sur le volontariat. Il permet aux fournisseurs de services cloud tels que Dropbox de démontrer qu'ils s'engagent à assurer leur conformité avec le RGPD. Dropbox Business, qui comprend les forfaits Standard, Advanced, Enterprise et Education pour les équipes, a été déclaré conforme au code de conduite de l'UE pour le cloud et a reçu une note de conformité de niveau 2, ce qui signifie que ces services ont mis en œuvre des mesures techniques, organisationnelles et contractuelles conformes aux exigences du code. Pour en savoir plus sur le code de conduite de l'UE pour le cloud et le niveau de conformité de Dropbox, veuillez consulter le site Web officiel du code.

Pour plus d'informations sur nos pratiques et notre politique de confidentialité, consultez notre livre blanc sur la confidentialité et la protection des données.

Conformité

Il existe différentes normes et réglementations de conformité que votre entreprise peut être amenée à respecter. Notre approche consiste à combiner les normes les plus reconnues avec des mesures de conformité correspondant aux besoins spécifiques de l'activité ou du secteur de nos clients.

ISO

L'organisation internationale de normalisation (ISO) a développé une série de normes reconnues sur le plan mondial qui concernent la sécurité des informations et la sécurité sociétale, et aident les organisations à concevoir des produits et des services innovants et fiables. Chez Dropbox, les datacenters, les systèmes, les applications, les personnes et les processus ont tous été certifiés conformes par un organisme indépendant, EY CertifyPoint, qui est basé aux Pays-Bas. Cet organisme est accrédité ISO par le Raad voor Accreditatie (Conseil d'accréditation néerlandais).

ISO/IEC 27001 (sécurité des informations)

ISO/IEC 27001 est l'une des normes de système de gestion de la sécurité de l'information (ISMS) les plus reconnues sur le plan international. Elle s'appuie sur les bonnes pratiques de la norme ISO/IEC 27002 en matière de sécurité. Afin de mériter votre confiance, nous examinons régulièrement nos systèmes de contrôle physiques, techniques et juridiques.

Consulter le certificat ISO/IEC 27001 pour Dropbox Business et Dropbox Education

ISO/IEC 27017 (sécurité dans le cloud)

ISO/IEC 27017 est une norme internationale relative à la sécurité dans le cloud qui fournit des recommandations sur les contrôles de sécurité applicables au provisionnement et à l'utilisation de services cloud. Les exigences en matière de sécurité, de confidentialité et de conformité auxquelles Dropbox et ses clients peuvent répondre ensemble sont expliquées dans le guide de la responsabilité partagée.

Consulter le certificat ISO/IEC 27017 pour Dropbox Business et Dropbox Education

ISO/IEC 27018 (confidentialité et protection des données dans le cloud)

ISO/IEC 27018 est une norme internationale relative à la protection et à la confidentialité des données. Elle s'applique aux fournisseurs de services cloud comme Dropbox qui gèrent des informations personnelles pour le compte de leurs clients, et sert de référence à nos clients pour comprendre les exigences contractuelles et réglementaires générales, et pour répondre à leurs questions en la matière.

Consulter le certificat ISO/IEC 27018 pour Dropbox Business et Dropbox Education

ISO/IEC 22301 (continuité de l'activité)

ISO/IEC 22301 est une norme internationale relative à la continuité de l'activité qui aide les entreprises à réduire les risques d'incidents ou à répondre à ces incidents de façon appropriée en minimisant leur impact potentiel. Le système de gestion de la continuité de Dropbox Business fait partie de notre stratégie de gestion du risque global pour protéger les personnes et les opérations en cas de crise.

Consulter le certificat ISO/IEC 22301 pour Dropbox Business et Dropbox Education

ISO/IEC 27701 (management de la protection de la vie privée)

ISO 27701 est une norme internationale concernant le management de la protection de la vie privée. La norme fournit un cadre pour améliorer et compléter le système de gestion de la sécurité de l'information de la norme ISO 27001 et créer ainsi un système de gestion des informations de confidentialité (PIMS - Privacy information management system). Les solutions Dropbox Business et Dropbox Education ont reçu cette certification en tant que sous-traitant de données personnelles.

Consulter le certificat ISO 27701 pour Dropbox Business et Dropbox Education

SOC

Les rapports SOC (Service Organization Controls), appelés SOC 1, SOC 2 et SOC 3, sont des cadres de référence établis par l'AICPA (American Institute of Certified Public Accountants) pour rendre compte des dispositifs de contrôle internes mis en œuvre au sein d'une entreprise. Les systèmes, applications, employés et processus de Dropbox ont été certifiés par une série d'audits réalisés par l'auditeur tiers indépendant Ernst & Young LLP.

SOC 3 pour la sécurité, la confidentialité, l'intégrité, la disponibilité et le respect de la vie privée

Le rapport d'attestation SOC 3 couvre les cinq grands critères des services de confiance portant sur la sécurité, la confidentialité, l'intégrité, la disponibilité et le respect de la vie privée (TSP, section 100). Le rapport Dropbox à usage général constitue une synthèse du rapport SOC 2. Il inclut l'opinion de l'auditeur tiers indépendant concernant l'efficacité de nos dispositifs de contrôle, tant en termes de conception que de fonctionnement.

Consulter l'évaluation SOC/IEC 3 pour Dropbox Business et Dropbox Education

SOC 2 pour la sécurité, la confidentialité, l'intégrité, la disponibilité et le respect de la vie privée

Le rapport SOC 2 permet à nos clients de bénéficier d'une analyse approfondie de l'efficacité de nos contrôles et couvre les cinq critères des services de confiance portant sur la sécurité, la disponibilité du système, l'intégrité de traitement, la confidentialité et le respect de la vie privée (TSP, section 100). Il offre une description détaillée des processus de Dropbox ainsi que de la centaine de contrôles mis en place pour protéger vos fichiers. Outre l'avis de notre auditeur tiers indépendant sur l'efficacité de ces contrôles, tant du point de vue de leur conception que de leur fonctionnement, ce rapport porte également sur les procédures de test de cet auditeur et leurs résultats pour chaque contrôle. Le rapport SOC 2 (également appelé rapport SOC 2+) inclut également une évaluation de nos contrôles par rapport aux normes ISO mentionnées ci-dessus, ce qui fournit une transparence supplémentaire à nos clients. L'évaluation SOC 2 pour Dropbox Business et Dropbox Education est disponible sur demande.

SOC 1/SSAE 18/ISAE 3402 (anciennement SSAE 16 ou SAS 70)

Le rapport SOC 1 détaille les exigences d'assurance qualité spécifiques pour les clients qui considèrent que Dropbox Business et Dropbox Education sont des éléments clés de leur programme ICFR (Internal Controls Over Financial Reporting). Ces exigences d'assurance qualité sont principalement utilisées par nos clients pour se mettre en conformité avec la loi Sarbanes-Oxley (SOX). Un organisme tiers indépendant procède à un audit conformément aux normes SSAE 18 (Standards for Attestation Engagements n° 18) et ISAE 3402 (International Standard on Assurance Engagements n° 3402). Ces normes ont remplacé les normes SSAE 16 (Standards for Attestation Engagements n° 16) et SAS 70 (Statement on Auditing Standards n° 70) devenues obsolètes. L'audit SOC 1 concernant Dropbox Business et Dropbox Education est disponible sur demande.

CSA

Cloud Security Alliance : Security, Trust, and Assurance Registry (CSA STAR)

Le registre STAR (Security, Trust & Assurance Registry) de la Cloud Security Alliance (CSA) est un registre gratuit et en accès libre. Il propose un programme de garantie de la sécurité pour les services cloud, dans le but d'aider les utilisateurs à évaluer la sécurité des fournisseurs de services cloud qu'ils utilisent ou envisagent d'utiliser.

Dropbox Business et Dropbox Education ont reçu la certification CSA STAR de niveau 2 et l'attestation CSA STAR de niveau 2. Elles requièrent une évaluation de nos dispositifs de contrôle de sécurité par des organismes tiers indépendants, EY CertifyPoint (pour la certification) et Ernst & Young LLP (pour l'attestation), établie à partir des exigences de la norme ISO/IEC 27001, des critères de service de confiance SOC 2 et de la matrice CCM (Cloud Controls Matrix) v4.0.2 de la CSA.

Consulter notre certificat et attestation CSA STAR de niveau 2 sur le site Web de la CSA

HIPAA/HITECH

Dropbox signera des accords de partenariat (BAA, ou Business Associate Agreement) avec les clients Dropbox Business ou Dropbox Education qui en ont besoin pour garantir la conformité avec les lois américaines HIPAA (Health Insurance Portability and Accountability Act) et HITECH (Health Information Technology for Economic and Clinical Health Act. Consultez l'article Dropbox et HIPAA/HITECH pour plus d'informations.

Dropbox met également à disposition un rapport d'attestation tiers évaluant ses contrôles en termes de sécurité, de confidentialité et de notification en cas de faille HIPAA/HITECH, ainsi qu'une évaluation de ses pratiques internes et recommandations pour les clients qui souhaitent utiliser Dropbox Business ou Dropbox Education conformément aux exigences de sécurité et de confidentialité HIPAA/HITECH.

Pour obtenir ces documents ou en savoir plus sur les modalités d'achat de Dropbox Business ou Dropbox Education, contactez le service commercial. Les administrateurs d'équipe Dropbox Business ou Dropbox Education peuvent signer un accord de partenariat par voie électronique depuis la page Compte de l'interface d'administration.

Notez que seuls les clients basés aux États-Unis peuvent signer un accord de partenariat par voie électronique via l'interface d'administration.

NIST 800-171

Aux États-Unis, le National Institute of Standards and Technology (NIST) promeut et maintient des normes et des lignes directrices pour aider à protéger les systèmes d'information. La publication spéciale du NIST 800171 Révision 2 (R2) fournit des lignes directrices sur la protection des informations non classifiées contrôlées (CUI - Controlled Unclassified Information) dans les organisations et systèmes d'information non fédéraux. Toute entité qui traite ou stocke des CUI du gouvernement américain, comme les institutions de recherche et le secteur de l'éducation, doit se conformer à la Publication spéciale du NIST SP 800-171 R2. Les systèmes, processus et contrôles CUI de Dropbox ont été validés par l'auditeur tiers indépendant Ernst & Young LLP.

Le rapport NIST SP 800-171 R2 concernant Dropbox Business et Dropbox Education est disponible sur demande auprès de notre équipe commerciale ou de notre équipe d'assistance (pour les clients Dropbox Business existants).

Notez que Dropbox Paper n'est pas inclus dans le rapport NIST SP 800-171 R2.

FERPA et COPPA (étudiants et enfants)

Dropbox Business et Dropbox Education permettent à leurs clients d'utiliser leurs services en respectant les obligations du fournisseur imposées par la loi FERPA (Family Education Rights and Privacy Act) relative à l'éducation et à la confidentialité. Les établissements d'enseignement dont les élèves ont moins de 13 ans peuvent également utiliser Dropbox Business ou Dropbox Education en respectant la loi COPPA (Children's Online Privacy Protection Act) relative à la protection des enfants sur Internet, à condition d'accepter certaines dispositions contractuelles spécifiques obligeant les établissements concernés à obtenir l'accord des parents pour l'utilisation de nos services.

FDA 21 CFR partie 11

Le Titre 21 du Code of Federal Regulations (CFR - Code des réglementations fédérales) régit les denrées alimentaires et les médicaments aux États-Unis pour la Food and Drug Administration (FDA - Agence américaine des produits alimentaires et médicamenteux), la Drug Enforcement Administration (Agence antidrogue américaine) et l'Office of National Drug Control Policy (Bureau de contrôles des drogues aux États-Unis). La Partie 11 du Titre 21 énonce les critères en vertu desquels la FDA considère les documents et les signatures électroniques comme fiables et généralement équivalents aux documents papier et aux signatures manuscrites effectuées sur support papier.

Pour plus d'informations sur la manière dont Dropbox peut vous aider à vous conformer aux directives du titre 21 CFR Part 11, veuillez consulter notre livre blanc (en anglais) et cet article du centre d'assistance.

PCI DSS

En tant que fournisseur de services, Dropbox respecte la norme PCI DSS (Payment Card Industry Data Security Standard). Toutefois, Dropbox Business, Dropbox Education et Dropbox Paper ne sont pas voués à traiter ni à stocker des transactions de carte de crédit. Notre attestation de conformité PCI est disponible sur demande.

Pour en savoir plus sur la conformité de Dropbox Business et de Dropbox Education, consultez dropbox.com/business/trust/compliance.

Applications pour Dropbox

DBX Platform repose sur un solide écosystème de développeurs qui utilisent nos API (Application Programming Interfaces) flexibles pour créer des applications. Ils sont plus de 750 000 à avoir conçu des applications et des services de productivité, collaboration, sécurité et administration sur cette plateforme.

Composants existants

Les modules Chooser, Saver et Embedder sont des composants Web et mobiles conçus pour faciliter l'accès à Dropbox depuis des applications et sites tiers en quelques lignes de code.

- Le module Chooser permet de sélectionner des fichiers dans Dropbox.
- Le module Saver permet d'enregistrer des fichiers directement dans Dropbox.
- Le module Embedder permet d'afficher des fichiers et des dossiers dans Dropbox.

L'autorisation d'accès à ces composants s'effectue intégralement via Dropbox. Les applications ont accès aux fichiers sélectionnés via des liens partagés Dropbox ou des liens de téléchargement de courte durée. Ces composants existants peuvent être utilisés indépendamment ou en conjonction avec l'API, décrite ci-dessous.

Intégrations via l'API Dropbox Business

L'API Dropbox publique permet aux développeurs tiers d'accéder à Dropbox et d'interagir avec la solution directement depuis leurs applications. Cela inclut les interactions liées aux fichiers et métadonnées, le partage et les fonctionnalités d'équipe.

Autorisation

Dropbox utilise le protocole d'autorisation standard OAuth pour permettre aux utilisateurs d'accorder aux applications des droits d'accès à leur compte sans pour autant divulguer leurs identifiants. Nous prenons en charge le protocole OAuth 2.0 pour authentifier les demandes d'API via le site Web ou l'application mobile Dropbox. Dropbox prend en charge les bonnes pratiques OAuth, notamment les jetons d'accès de courte durée et la clé de vérification pour les échanges de code (PKCE) pour les applications distribuées.

Autorisations relatives aux utilisateurs

Les applications qui reposent sur l'API Dropbox peuvent bénéficier d'un des niveaux d'accès suivants aux contenus Dropbox des utilisateurs :

- ***Accès au dossier de l'application***

  Un dossier dédié qui porte le nom de l'application est créé dans le dossier **Applications** de la Dropbox d'un utilisateur. L'application reçoit un accès en lecture et en écriture à ce dossier uniquement. Les utilisateurs peuvent y transférer des fichiers s'ils souhaitent ajouter du contenu à l'application. L'application peut également demander l'accès à un fichier ou à un dossier via le module Dropbox Chooser ou Dropbox Saver.

- ***Accès complet***

  L'application bénéficie d'un accès complet à tous les fichiers/dossiers de la Dropbox d'un utilisateur. Elle peut également demander l'accès à un fichier ou à un dossier via le module Dropbox Chooser ou Dropbox Saver.

Les applications peuvent aussi demander des accès spécifiques et limiter leurs comportements en accédant à des sous-ensembles de points de terminaison de l'API. Elles peuvent par exemple se limiter à accéder aux fichiers en lecture seule ou à importer du contenu, mais pas à créer des partages.

Autorisations de l'équipe

Les administrateurs Dropbox Business peuvent autoriser des applications à réaliser les fonctionnalités d'administration qui se trouvent dans l'interface d'administration de l'équipe. Les actions que les applications liées à l'équipe sont capables d'effectuer sont définies par des ensembles d'autorisations qui régissent à quels paramètres d'équipe l'application a accès en lecture seule ou en écriture.

Les ensembles d'autorisations suivants sont couramment utilisés :

- ***Informations sur l'équipe***

  Accès en lecture seule à des informations générales relatives à l'équipe et l'utilisation.

- ***Audit de l'équipe***

  Accès en lecture seule aux informations relatives à l'équipe et au journal détaillé des événements.

- ***Accès aux fichiers des membres de l'équipe***

  Possibilité d'effectuer des opérations au nom des utilisateurs de l'équipe, par exemple gérer leurs fichiers et dossiers.

- ***Gestion des membres de l'équipe***

  Ajout et suppression de membres dans l'équipe.

Webhooks

Les webhooks permettent aux applications Web de recevoir des notifications en temps réel sur les modifications apportées dans le compte Dropbox d'un utilisateur. Lorsqu'un URI est enregistré pour recevoir des webhooks, une requête HTTP lui est envoyée à chaque modification dans les comptes d'utilisateur de l'application. Avec l'API Dropbox Business, les webhooks peuvent également être utilisés pour générer des notifications relatives aux modifications apportées à la liste de membres d'une équipe. De nombreuses applications de sécurité utilisent les webhooks pour aider les administrateurs à suivre et à gérer les activités au sein des équipes.

Dropbox Extensions

Des URI d'extension peuvent être ajoutés à des applications afin d'afficher des actions dans les menus **Partager** et **Ouvrir** de l'interface utilisateur Dropbox. Les extensions permettent aux utilisateurs de lancer des workflows tiers personnalisés directement à partir d'un fichier dans un espace Dropbox. Au déclenchement d'une action, Dropbox redirige les utilisateurs vers l'URI spécifié, en transmettant un identifiant de fichier qui peut être utilisé avec l'API pour réaliser n'importe quelle opération sur le fichier. Les applications doivent être autorisées pour que l'utilisateur puisse voir les extensions. Nous pouvons promouvoir un ensemble d'extensions dans les menus **Partager** et **Ouvrir** même si ces applications n'auront pas accès au contenu tant que l'utilisateur ne l'aura pas autorisé.

Recommandations pour les développeurs Dropbox

Nous fournissons plusieurs recommandations et bonnes pratiques pour aider les développeurs à créer des applications basées sur l'API qui respectent et protègent la confidentialité des utilisateurs tout en optimisant l'expérience utilisateur de Dropbox.

- ***Clés d'application***

  Une clé d'application Dropbox unique est nécessaire pour chaque application créée par un développeur. En outre, si une application fournit des services ou des logiciels qui exigent des autres développeurs qu'ils utilisent DBX Platform, chacun d'eux doit également demander sa propre clé d'application Dropbox.

- ***Autorisations accordées aux applications***

  Les développeurs doivent appliquer un droit d'accès minimal à leurs applications. Lorsqu'un développeur nous envoie une application pour que nous approuvions son statut de production, nous vérifions que l'application ne nécessite pas d'autorisation superflue au regard des fonctionnalités fournies par l'application.

- ***Processus d'examen des applications***

  - **Statut de développement**

    Au moment de la création d'une application basée sur l'API Dropbox, un statut lui est attribué pour indiquer qu'elle est en cours de développement. Le statut de développement est similaire au statut de production, sauf que l'application ne peut être associée qu'à 500 comptes Dropbox maximum. Dès lors que l'application est associée à 50 comptes Dropbox, le développeur dispose d'un délai de deux semaines pour faire approuver le statut de production de l'application. Sans ce statut, aucun autre compte Dropbox ne pourra être associé à l'application.

  - **Statut de production et validation**

    Pour que le statut de production soit approuvé, toutes les applications basées sur l'API doivent respecter la charte graphique et éditoriale de marque pour les développeurs, ainsi que les conditions d'utilisation, notamment celles relatives aux utilisations non autorisées de DBX Platform (incitation au non-respect de la propriété intellectuelle ou du copyright, création de réseaux de partage de fichiers ou téléchargement illégal de contenu, etc.). Avant l'examen de leur application, les développeurs doivent fournir des informations supplémentaires sur ses fonctionnalités. Ils doivent également décrire comment elle utilise l'API Dropbox. Une fois que le statut de production est accordé, n'importe quel utilisateur Dropbox peut associer son compte à l'application.

Administration des applications d'équipe

Dans l'interface d'administration de l'équipe, les administrateurs d'équipes Dropbox Business peuvent gérer les intégrations et applications connectées.

Partenariats relatifs aux API

Dropbox a travaillé en étroite collaboration avec ses partenaires technologiques pour leur permettre d'intégrer leurs applications à Dropbox. Pour ce faire, ces partenaires utilisent les API Dropbox et suivent les conseils avisés d'architectes Dropbox en matière de sécurité et d'expérience utilisateur. Ces intégrations incluent des outils de productivité ou de gestion et de sécurité, tels que :

- ***Outils SIEM et d'analyse***

  Vous pouvez intégrer des outils SIEM et d'analyse à votre compte Dropbox Business pour surveiller et évaluer le partage de contenu entre les utilisateurs, les tentatives de connexion, les actions d'administration, et plus encore. Utilisez votre outil centralisé de gestion des journaux pour consulter et gérer les journaux d'activité des employés, ainsi que les données relatives à la sécurité.

- ***Protection contre la perte de données***

  Analysez automatiquement les métadonnées et le contenu des fichiers afin de déclencher des alertes, des rapports et des actions lorsque votre compte Dropbox Business fait l'objet de modifications majeures. Déployez Dropbox Business conformément aux règles de votre entreprise pour respecter les exigences réglementaires.

- ***eDiscovery et obligation de rétention des données***

  Vous pouvez utiliser les données de votre compte Dropbox Business pour répondre aux litiges, arbitrages et enquêtes réglementaires. Pour faire gagner du temps et de l'argent à votre entreprise, recherchez et recueillez les informations pertinentes stockées par voie électronique, et conservez vos données à l'aide du processus eDiscovery.

- ***Gestion des droits numériques (DRM)***

  Intégrez un système tiers de protection de contenu pour les données sensibles ou protégées par copyright stockées dans les comptes des employés. Profitez de puissantes fonctionnalités de gestion des droits numériques, y compris le chiffrement côté client, l'ajout de filigranes, les journaux d'audit, la révocation de l'accès et le blocage des utilisateurs ou des appareils.

- ***Migration des données et sauvegarde on-premise***

  La migration des données sur Dropbox à partir de serveurs existants ou d'autres solutions cloud permet d'économiser du temps et de l'argent. Vous pouvez également automatiser les sauvegardes de votre compte Dropbox Business sur des serveurs on-premise.

- ***Gestion des identités et authentification unique***

  Automatisez le processus d'ajout et de suppression d'utilisateurs, et accélérez la création des comptes. Intégrez Dropbox Business à un système de gestion des identités existant afin de simplifier la gestion et d'optimiser la sécurité.

- ***Workflows personnalisés***

  Créez des applications internes qui intègrent Dropbox aux processus existants de l'entreprise afin d'optimiser les workflows internes.

Vous trouverez la liste de ces partenaires technologiques sur la page Intégrations. Les utilisateurs découvriront également certaines applications et intégrations propriétaires et tierces dans l'App Center.

Intégrations Dropbox

Nous avons également collaboré avec certains de nos principaux partenaires pour développer des intégrations disponibles directement depuis les interfaces Dropbox. Ces intégrations plus étroites sont développées par Dropbox et par le partenaire. Les voici :

Dropbox Extensions

Grâce à ces intégrations, les utilisateurs peuvent recourir à différents types d'extensions qui permettent par exemple de publier une vidéo, d'ajouter des fichiers dans des e-mails et discussions, ou d'envoyer un document pour signature électronique directement depuis Dropbox. Ces applications sont conçues par le partenaire. Le rôle de Dropbox consiste à faciliter la découverte de certains partenaires via les menus **Ouvrir** et **Partager**.

Slack, Zoom et Trello

Ces intégrations sont conçues par Dropbox. Elles permettent aux utilisateurs de démarrer des conversations Slack, d'organiser des réunions et de créer des tâches directement dans Dropbox. Les utilisateurs peuvent utiliser l'authentification OAuth sur ces outils.

Microsoft Office pour version mobile et Web

Nos intégrations avec Microsoft Office permettent aux utilisateurs d'ouvrir les fichiers Word, Excel et PowerPoint stockés dans leur Dropbox, d'y apporter des modifications dans les applications Office mobiles ou Web et d'enregistrer directement ces modifications dans Dropbox. Les utilisateurs doivent autoriser chaque application Office (mobile ou Web) à accéder à Dropbox lors de la première tentative d'ouverture d'un fichier depuis Dropbox. Cette opération n'est pas nécessaire par la suite. En outre, le Badge Dropbox vous permet de collaborer directement à partir des applications de bureau Office. Il vous permet de voir les utilisateurs qui consultent ou modifient un fichier Office et vous informe lorsque des personnes accèdent au fichier, le modifient et le mettent à jour.

Adobe Acrobat et Acrobat Reader

Nos intégrations avec les versions de bureau et mobiles (Android et iOS) de ces applications permettent aux utilisateurs de consulter, de modifier et de partager des PDF stockés dans leur Dropbox. Les utilisateurs doivent autoriser chaque application à accéder à Dropbox lors de la première tentative d'ouverture d'un fichier. Les modifications apportées aux PDF sont automatiquement enregistrées dans Dropbox.

Résumé

Dropbox Business offre des outils simples d'utilisation qui permettent aux équipes de collaborer efficacement tout en répondant aux exigences de sécurité et de conformité des entreprises. Grâce à une approche multiniveau qui associe une infrastructure solide à un ensemble de règles personnalisables, nous proposons aux entreprises une solution performante capable de s'adapter à leurs besoins. Pour en savoir plus sur Dropbox Business, contactez-nous à l'adresse sales@dropbox.com.