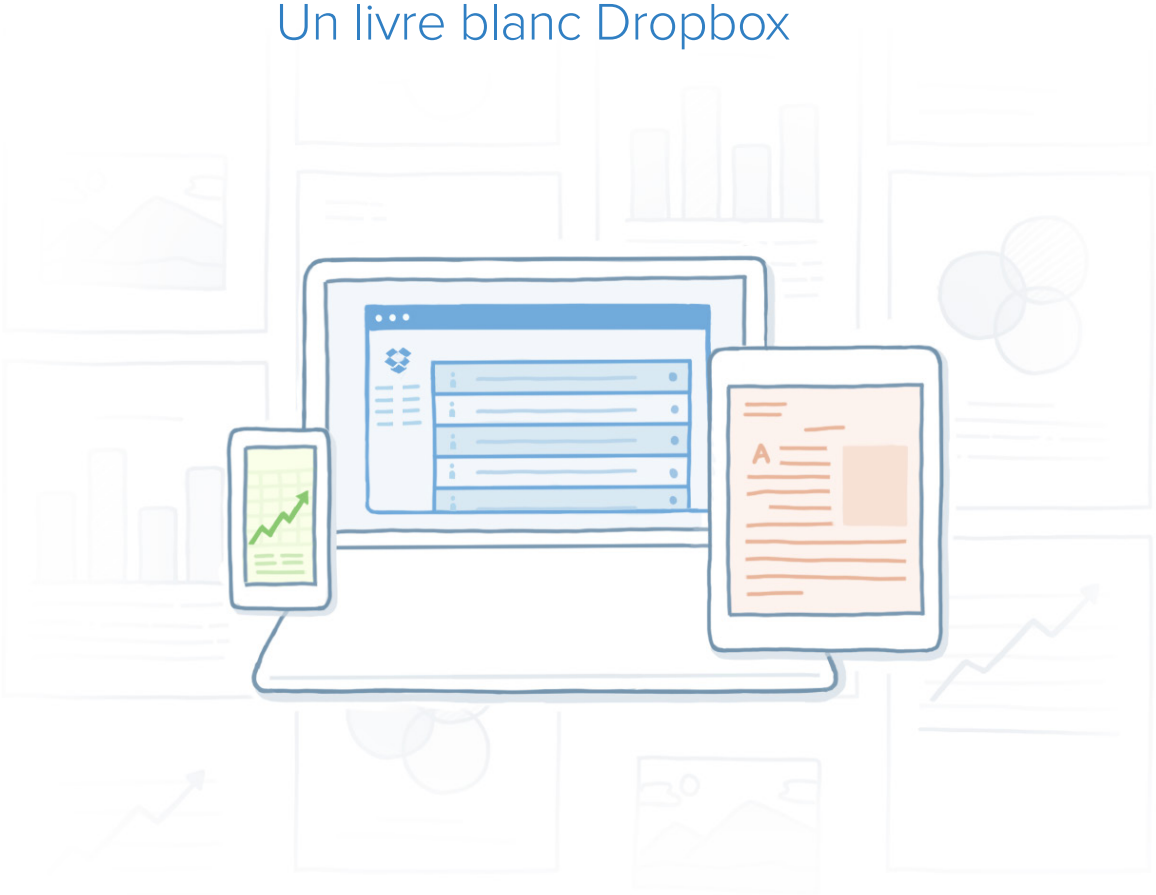
Sécurité de Dropbox Entreprises

Un livre blanc Dropbox



Dropbox

Sommaire

Introduction

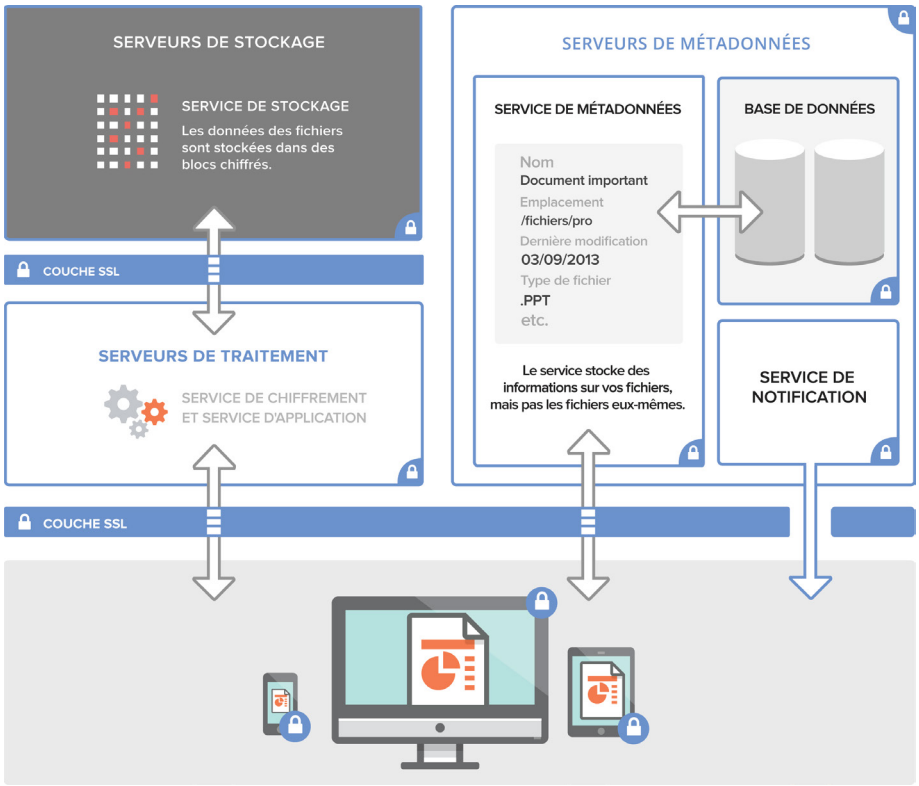
Des millions d'utilisateurs font confiance à Dropbox pour stocker, synchroniser et partager de façon simple et fiable des photos, des documents, des vidéos et d'autres contenus sur différents appareils et différentes plates-formes. Avec Dropbox Entreprises, il est maintenant possible de profiter de la même simplicité d'utilisation dans un contexte professionnel. Grâce aux fonctionnalités avancées, les équipes peuvent partager instantanément des fichiers dans l'ensemble de l'organisation. De leur côté, les administrateurs disposent de toute la visibilité et des possibilités de contrôle dont ils ont besoin. Mais Dropbox n'est pas qu'un simple outil de stockage et de partage : c'est aussi une solution qui vous permet de protéger vos fichiers professionnels. À ce titre, nous avons créé une infrastructure sophistiquée dans laquelle les administrateurs de comptes peuvent ajouter des niveaux de sécurité supplémentaires et personnaliser leurs propres règles. Ce document détaille les règles que nous avons mises en place ainsi que les options proposées aux administrateurs. Ensemble, ces règles et ces options font de Dropbox un outil parfaitement sécurisé qui vous permet de gagner en productivité.

Sous le capot

Extrêmement simples d'utilisation, les interfaces de Dropbox s'appuient sur une infrastructure d'arrière-plan qui assure des transferts et des téléchargements fiables, rapides et entièrement automatisés, ne nécessitant que très peu d'intervention de la part des utilisateurs. Pour parvenir à ce résultat, nous faisons évoluer nos produits et notre architecture en permanence, afin d'accélérer les transferts, d'améliorer la fiabilité et de nous adapter à l'évolution de l'environnement informatique. Dans cette section, nous vous expliquons comment les données sont transférées, stockées et traitées en toute sécurité.

Architecture

De par sa conception, Dropbox intègre plusieurs niveaux de protection répartis sur une infrastructure évolutive et sécurisée, couvrant à la fois les transferts de données, le chiffrement, la configuration du réseau et les contrôles au niveau des applications.



Les utilisateurs de Dropbox peuvent à tout moment accéder aux fichiers et aux dossiers à partir des applications de bureau, de l'interface Web et des clients mobiles, mais également par l'intermédiaire des applications connectées à Dropbox. Tous

ces clients se connectent à des serveurs sécurisés pour permettre l'accès aux fichiers et leur partage, et pour mettre à jour les appareils associés lorsque des fichiers sont ajoutés, modifiés ou supprimés.

Notre architecture se compose des services suivants :

- **Service de chiffrement et d'application.** Pour protéger les données des utilisateurs, Dropbox intègre de par sa conception un dispositif de sécurité unique en son genre qui va bien plus loin que les systèmes de chiffrement classiques. Les services de chiffrement et d'application traitent les données issues des applications Dropbox en scindant chaque fichier en plusieurs blocs, en chiffrant chacun de ces blocs à l'aide d'un algorithme renforcé, et en synchronisant uniquement les blocs modifiés entre chaque révision. Lorsqu'une application Dropbox détecte la présence d'un nouveau fichier ou la modification d'un fichier existant, elle signale la modification aux services de chiffrement et d'application. Les blocs de fichier nouveaux ou modifiés sont alors traités et transférés au service de stockage. Pour découvrir plus en détail le mécanisme de chiffrement utilisé par ces services pour les données dormantes et les données en cours de transfert, consultez la section Chiffrement ci-après.
- **Service de stockage.** Ce service stocke le contenu des fichiers des utilisateurs dans des blocs chiffrés. Avant l'envoi des données, le client Dropbox scinde les fichiers en plusieurs blocs afin de les préparer pour le service de stockage en mode bloc. Le service de stockage fonctionne comme un système de stockage dédié aux contenus fixes (Content-Addressable Storage ou CAS), chaque bloc de fichier chiffré étant récupéré à partir de sa valeur de hachage. Un niveau de chiffrement supplémentaire assure la protection des données dormantes au moyen d'un algorithme renforcé.
- **Service de métadonnées.** Certaines informations de base sur les données des utilisateurs (noms des fichiers, types des fichiers, etc.), qu'on appelle "métadonnées", sont stockées dans leur propre service de stockage indépendant. Ce service joue le rôle d'index pour les données stockées dans les comptes des utilisateurs. Toutes les métadonnées Dropbox sont stockées dans un service de base de données MySQL. Elles sont partagées et répliquées autant de fois que nécessaire pour atteindre les performances et les niveaux de disponibilité attendus.
- **Service de notification.** Ce service indépendant surveille si des modifications ont été apportées aux comptes Dropbox. Il ne stocke et ne transfère aucun fichier ni aucune métadonnée, et les connexions à ce service ne sont donc pas chiffrées. Chaque client établit une connexion d'interrogation longue avec le service de notification, puis se met en attente. Lorsqu'une modification est apportée à un fichier stocké dans une Dropbox, le service de notification signale la modification aux clients concernés en interrompant la connexion d'interrogation longue. L'interruption de la connexion signale au client qu'il doit se connecter au service de métadonnées de façon sécurisée afin de synchroniser les modifications.

En répartissant ainsi les différents niveaux d'informations sur l'ensemble de ces services, la rapidité et la fiabilité de la synchronisation sont améliorées, et la sécurité est renforcée. En raison de l'architecture même de Dropbox, il est impossible de reconstruire les fichiers en accédant à l'un ou l'autre de ces services. Pour en savoir plus sur les modes de chiffrement utilisés par les différents services, consultez la section Chiffrement ci-après.

Interfaces utilisateur Dropbox

Le service Dropbox est utilisable et accessible par le biais de plusieurs interfaces. Chacune d'entre elles offre des paramètres et des fonctionnalités de sécurité permettant de traiter et de protéger les données des utilisateurs, tout en garantissant un accès aisé.

- **Interface Web.** Tous les navigateurs Web récents permettent d'accéder à cette interface, qui offre aux utilisateurs la possibilité de transférer, de télécharger, de consulter et de partager leurs fichiers.
- **Application de bureau.** L'application de bureau Dropbox est un client de synchronisation performant qui stocke les fichiers localement, pour un accès hors connexion. Elle permet aux utilisateurs d'accéder à l'intégralité de leurs comptes Dropbox, et elle est compatible avec les systèmes d'exploitation Windows, Mac et Linux. Les fichiers sont consultables directement dans l'explorateur de fichiers du système d'exploitation et peuvent également être partagés via cet explorateur.
- **Applications mobiles.** L'application Dropbox est disponible sur les appareils mobiles et les tablettes iOS, Android et BlackBerry. Elle permet aux utilisateurs d'accéder à tous leurs fichiers, où qu'ils se trouvent. Grâce à son gestionnaire de favoris, les documents peuvent également être accessibles hors connexion.

Notre équipe de sécurité effectue régulièrement des tests automatisés et manuels pour contrôler la sécurité des applications, et corriger ainsi les vulnérabilités de sécurité potentielles et les bugs. Pour préserver la sécurité de nos applications, nous collaborons également avec des experts en sécurité indépendants, mais aussi avec les services de sécurité d'autres entreprises informatiques et la communauté des experts en sécurité informatique.

Fiabilité

Pour être efficace, un système de stockage doit être fiable. Aussi, nous intégrons à Dropbox plusieurs niveaux de redondance empêchant les pertes de données et garantissant la disponibilité. Des copies redondantes des métadonnées sont distribuées sur des systèmes indépendants au sein d'un datacenter, en suivant une approche "N+2" pour la disponibilité. Les métadonnées font l'objet d'une sauvegarde incrémentielle toutes les heures et d'une sauvegarde complète tous les jours. Le stockage de fichiers en mode bloc de Dropbox utilise des systèmes qui font appel à des fournisseurs tiers garantissant une durabilité de 99,9999999999 %.

En plus de protéger les données des utilisateurs, cette fonctionnalité assure la haute disponibilité du service Dropbox. En cas d'échec de connexion avec le service Dropbox, un client ou un serveur frontal reprend l'opération en douceur dès le rétablissement de la connexion. Les fichiers ne sont mis à jour sur le client local que s'ils ont été entièrement synchronisés et correctement validés auprès du service Dropbox. L'équilibrage de charge entre les différents serveurs assure une redondance et permet à l'utilisateur de profiter d'une expérience de synchronisation cohérente.

Chiffrement

Données en cours de transfert

Pour protéger les données en cours de transfert, Dropbox utilise le protocole SSL/TLS (Secure Sockets Layer/Transport Layer Security) pour le transfert de données, créant ainsi un tunnel sécurisé protégé par un chiffrement AES (Advanced Encryption Standard) sur au moins 128 bits. Les données en cours de transfert entre un client Dropbox (c'est-à-dire actuellement l'application de bureau, l'application mobile, l'API ou l'interface Web) et le service hébergé sont systématiquement chiffrées au moyen des protocoles SSL/TLS. Dans le cas des terminaux que nous contrôlons (application de bureau et application mobile) et des navigateurs récents, nous utilisons un algorithme renforcé et nous prenons en charge la confidentialité persistante parfaite (PFS). Au niveau de l'interface Web, tous les cookies d'authentification sont signalés comme sécurisés, et nous utilisons le mécanisme HSTS (HTTP Strict Transport Security).

Pour empêcher les attaques de type MITM (Man-in-the-middle), l'authentification des serveurs frontaux Dropbox est réalisée par le biais de certificats publics détenus par le client. La connexion chiffrée est négociée avant le transfert des données de l'utilisateur et garantit une transmission sécurisée des données vers les serveurs frontaux Dropbox, aussi bien pour le stockage des fichiers en mode bloc que pour le stockage des métadonnées.

> "Je préfère largement stocker mes données sur un système sécurisé, chiffré et redondant tel que celui de Dropbox, plutôt que dans mes locaux où je risquerais de les perdre."
>
> Richard Wetzel, associé, Centric Projects

Données dormantes

Les données dormantes stockées dans Dropbox par les utilisateurs sont chiffrées au moyen du standard AES (Advanced Encryption Standard). Le stockage primaire des données Dropbox des utilisateurs est réparti dans plusieurs datacenters, sous forme de blocs de fichiers indépendants. Chaque bloc est fragmenté et chiffré au moyen du standard AES. Seuls les blocs qui ont été modifiés entre les révisions sont synchronisés.

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. Dropbox gère

intentionnellement les clés à la place de l'utilisateur afin de réduire la complexité, de mettre à sa disposition des fonctionnalités produit avancées et d'assurer un chiffrement au moyen d'un algorithme renforcé.

Datacenters

Les systèmes de gestion et de production de Dropbox sont hébergés au sein de datacenters appartenant à une organisation de sous-services tierce, ainsi qu'auprès de fournisseurs de services gérés situés aux États-Unis. Tous les rapports SOC relatifs aux datacenters de l'organisation de sous-services 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 aux frontières de l'infrastructure Dropbox. Dropbox est responsable de la sécurité logique, de la sécurité réseau et de la sécurité des applications de son infrastructure hébergée au sein de datacenters tiers.

Le fournisseur de services gérés actuel de Dropbox, 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 des fournisseurs 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.

Fonctionnalités du produit

Fonctionnalités d'administration

Chaque entreprise étant différente, nous avons mis au point plusieurs outils permettant aux administrateurs de personnaliser Dropbox Entreprises en fonction des besoins de leurs utilisateurs. Le paragraphe ci-après détaille les fonctionnalités de contrôle et de surveillance disponibles dans l'interface d'administration de Dropbox Entreprises.

Contrôles

- Méthodes de provisionnement des utilisateurs
  - Invitations par e-mail. Un outil accessible dans l'interface d'administration de Dropbox Entreprises permet aux administrateurs de générer manuellement une invitation par e-mail.
  - Active Directory. Les administrateurs Dropbox Entreprises peuvent automatiser la création et la suppression des comptes à partir d'un système Active Directory existant. Une fois intégré à Dropbox, il est possible d'utiliser Active Directory pour gérer les membres.
  - Authentification unique (SSO). Dropbox Entreprises peut être configuré pour autoriser les membres de l'équipe à accéder au compte en se connectant à un fournisseur d'identité central. Notre implémentation SSO, qui utilise le standard SAML (Security Assertion Markup Language), simplifie et sécurise l'authentification en la confiant à un fournisseur d'identité fiable et en offrant aux membres de l'équipe la possibilité d'accéder à Dropbox sans devoir gérer un mot de passe supplémentaire.
- Autorisations de partage. Les administrateurs de compte Dropbox Entreprise peuvent autoriser ou non les membres de l'équipe à partager des contenus avec des personnes extérieures à l'équipe, et définir des règles différentes pour les dossiers partagés et les liens partagés. Si le partage à l'extérieur de l'équipe est activé, les membres peuvent quand même décider de restreindre l'accès à certains dossiers ou liens aux membres de l'équipe.
- Réinitialisation des mots de passe. Pour plus de sécurité, les administrateurs peuvent réinitialiser de façon proactive les mots de passe, soit pour l'ensemble de l'équipe, soit au cas par cas.
- Sessions Web. Les sessions actives dans les navigateurs Web peuvent faire l'objet d'un suivi et être arrêtées, soit à partir de l'interface d'administration, soit à partir des paramètres de compte de chaque utilisateur.
- Accès des applications. Les administrateurs peuvent voir quelles applications tierces ont accès aux comptes des utilisateurs et révoquer les autorisations correspondantes.
- Dissociation d'appareils. Les ordinateurs et les appareils mobiles connectés aux comptes des utilisateurs peuvent être dissociés par l'administrateur, dans l'interface d'administration, ou par l'utilisateur, dans les paramètres de sécurité de son compte. Sur les ordinateurs, la dissociation provoque la suppression des données d'authentification et offre la possibilité de supprimer les copies locales des fichiers dès la prochaine connexion de l'ordinateur à Internet (voir Effacement à distance).

Sur les appareils mobiles, la dissociation provoque la suppression des fichiers ajoutés aux favoris, des données mises en cache et des informations de connexion. Si la validation en deux étapes est activée, les utilisateurs doivent de nouveau authentifier l'appareil avant de le réassocier. En outre, les paramètres de compte des utilisateurs offrent la possibilité d'envoyer automatiquement un e-mail de notification lorsque des appareils sont associés à Dropbox.

- Couplage des comptes. Les utilisateurs peuvent associer leurs Dropbox professionnelle et personnelle sur l'ensemble de leurs appareils pour permettre une séparation stricte de leurs données professionnelles et personnelles. Les administrateurs peuvent choisir d'autoriser ou non le client de bureau à accéder à cette fonctionnalité, pour chaque membre de l'équipe.
- Effacement à distance. Lorsqu'un collaborateur quitte l'équipe ou perd un appareil, les administrateurs peuvent effacer à distance les données Dropbox et les copies locales des fichiers, aussi bien sur les ordinateurs que sur les appareils mobiles.

> "En permettant à nos collaborateurs de passer à Dropbox Entreprises, nous avons pu reprendre une gestion centralisée. Nos équipes informatiques peuvent ainsi répondre à nos besoins en matière de sécurité, tout en offrant à nos utilisateurs la solution qu'ils attendaient. C'est pour nous un choix gagnant sur toute la ligne."
>
> Karl Ma, sécurité globale et conformité, BCBG MAXAZRIA Group

- Transfert de comptes. Après avoir déprovisionné un utilisateur (soit manuellement, soit par le biais des services d'annuaire), les administrateurs peuvent transférer les fichiers de ce compte à un autre utilisateur appartenant à l'équipe.

Visibilité

- Rapports sur les activités des utilisateurs. Les administrateurs Dropbox Entreprises peuvent à tout moment générer des rapports sur les activités pour différents types d'événement, filtrés par période. Les rapports peuvent porter sur des utilisateurs individuels ou sur l'ensemble des comptes d'une équipe. Ils peuvent être téléchargés au format CSV (valeurs séparées par des virgules) en vue d'une analyse à l'aide d'outils SIM/SEM de gestion des incidents de sécurité et des événements. Grâce aux rapports sur les activités des utilisateurs, les administrateurs ont accès aux informations suivantes :
  - Mots de passe. Modifications apportées aux mots de passe et aux paramètres de validation en deux étapes. Les administrateurs n'ont pas directement accès aux mots de passe des utilisateurs.
  - Connexions. Connexions et échecs de connexion au site Web Dropbox.
  - Actions d'administration. Modifications apportées aux paramètres de l'interface d'administration (autorisations d'accès aux dossiers partagés, par exemple).
  - Applications. Opérations d'association d'applications tierces aux comptes Dropbox.
  - Appareils. Opérations d'association d'ordinateurs ou d'appareils mobiles aux comptes Dropbox.
  - Partage. Événements relatifs aux dossiers partagés et aux liens partagés : création et accès à des dossiers partagés, envoi et ouverture de liens partagés permettant d'accéder à des documents, etc. Bien souvent, les rapports indiquent si les actions impliquent ou non des membres extérieurs à l'équipe.
  - Gestion des membres. Opérations d'ajout et de suppression de membres.

  Par ailleurs, les événements relatifs aux différents fichiers et dossiers (modifications, suppressions et gestion des personnes ayant accès à un dossier partagé) sont visibles dans la page Événements de chaque utilisateur.
- Vérification d'identité pour l'accès à l'assistance technique. Avant l'envoi de conseils de résolution des problèmes ou d'informations sur le 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 secret n'est disponible que dans l'interface d'administration.

Fonctionnalités de gestion des utilisateurs

Dropbox Entreprises intègre également des outils permettant aux utilisateurs de renforcer la protection de leur compte et de leurs données. Les fonctionnalités d'authentification, de restauration et de consignation, ainsi que les autres fonctionnalités de sécurité décrites ci-après sont disponibles par le biais des différentes interfaces utilisateur Dropbox.

- Restauration et contrôle des versions. Tous les clients Dropbox Entreprises ont la possibilité de restaurer des fichiers perdus et les versions précédentes de leurs fichiers, sans limite de durée. Ils peuvent ainsi effectuer un suivi des modifications apportées aux données importantes et rétablir d'anciennes versions.
- Validation en deux étapes. Cette fonctionnalité facultative mais vivement recommandée ajoute un niveau supplémentaire de protection au compte Dropbox des utilisateurs. Lorsqu'elle est activée, Dropbox exige un code de sécurité à six chiffres en plus du mot de passe lors de la connexion à Dropbox ou de l'association d'un nouvel appareil (ordinateur, téléphone ou tablette).
  - Les administrateurs de compte peuvent voir quels membres de l'équipe ont activé la validation en deux étapes.
  - Les codes Dropbox de validation en deux étapes peuvent être reçus par SMS ou par le biais d'applications respectant le standard d'algorithme TOTP (Time-based One-Time Password). Si un utilisateur ne peut pas recevoir les codes de sécurité au moyen de ces méthodes, il peut choisir d'utiliser un code de secours à 16 chiffres, à usage unique. Il peut également utiliser un numéro de téléphone secondaire pour recevoir un code de secours par SMS.
  - Dès lors qu'un utilisateur a activé la validation en deux étapes, les administrateurs peuvent l'obliger à laisser le service activé sur son compte. Par ailleurs, les administrateurs peuvent générer un e-mail de rappel incitant les utilisateurs qui n'ont pas encore activé le service à le faire.
- Indicateur de niveau de sécurité du mot de passe. Visible par tous les utilisateurs lorsqu'ils créent un compte ou modifient leur mot de passe, l'indicateur de niveau de sécurité les aide à générer un mot de passe suffisamment sécurisé et à protéger ainsi leur propre compte.
- Activité du compte utilisateur. Chaque utilisateur peut consulter les pages suivantes dans les paramètres du compte afin d'obtenir des informations actualisées sur l'activité de son propre compte :
  - Page Partage. Cette page permet à l'utilisateur de voir la liste des dossiers dont il est membre, ainsi que les dossiers partagés qu'il a quittés (et qu'il peut de nouveau rejoindre, s'il le souhaite). À partir de cette page, un utilisateur propriétaire d'un dossier partagé peut afficher la liste des membres du dossier, révoquer l'accès au dossier pour certains utilisateurs et transférer la propriété du dossier.
  - Page Liens. Cette page permet à l'utilisateur de voir tous les liens de partage actifs et leur date de création. Il peut également afficher la liste des liens partagés par d'autres utilisateurs et désactiver des liens actifs.
  - Page Événements. Cette page contient un journal actualisé en permanence, indiquant les modifications apportées aux fichiers et aux dossiers, ainsi que les ajouts et les suppressions. L'activité des dossiers partagés (gestion des membres, modifications apportées par d'autres membres du dossier) peut également être surveillée sur cette page.
  - Notifications par e-mail. Un utilisateur peut demander à recevoir immédiatement une notification par e-mail lors de l'association d'un nouvel appareil ou d'une nouvelle application à son compte Dropbox.
- Autorisations des comptes utilisateur
  - Appareils associés. La rubrique Appareils des paramètres de sécurité d'un compte utilisateur contient la liste de tous les ordinateurs et appareils mobiles associés au compte. Pour chaque ordinateur, différentes informations sont disponibles : adresse IP, pays et heure approximative de l'activité la plus récente. L'utilisateur peut dissocier les appareils de son compte et choisir de supprimer ou non les fichiers présents sur l'ordinateur correspondant lors de sa prochaine connexion à Internet.
  - Sessions Web actives. La rubrique Sessions contient la liste des navigateurs Web actuellement connectés au compte de l'utilisateur. Pour chaque navigateur, différentes informations sont disponibles : adresse IP, pays et heure d'ouverture de la session. L'utilisateur peut arrêter à distance une session à partir des paramètres de sécurité de son compte.
  - Applications associées. La rubrique Applications associées contient la liste des applications tierces qui ont accès au compte de l'utilisateur, ainsi que le type d'accès accordé à chacune d'entre elles. L'utilisateur peut révoquer l'autorisation de chaque application pour l'empêcher d'accéder à sa Dropbox.

- Sécurité des appareils mobiles
  - **Verrouillage par code secret.** Pour ajouter un niveau de protection supplémentaire à l'application mobile Dropbox, les utilisateurs peuvent exiger la saisie d'un code secret à quatre chiffres à chaque lancement ou sortie de veille de l'application. L'utilisateur est alors invité à saisir le code secret dès qu'il ouvre ou réaffiche l'application Dropbox.
  - **Effacement des données.** Pour plus de sécurité, les utilisateurs peuvent activer une option provoquant l'effacement de toutes les données Dropbox présentes sur l'appareil au bout de dix échecs de saisie du code secret.
  - **Stockage interne et fichiers favoris.** Par défaut, les fichiers ne sont stockés dans un cache temporaire sur l'appareil mobile qu'au moment de leur consultation. Les clients mobiles Dropbox offrent la possibilité d'ajouter des fichiers individuels aux favoris et de les enregistrer sur l'appareil pour les consulter hors connexion. Lorsqu'un appareil est dissocié d'un compte Dropbox, soit par le biais de l'appareil lui-même, soit par le biais de l'interface Web, les favoris sont supprimés automatiquement du dispositif de stockage interne de l'appareil.

Applications pour Dropbox

La plate-forme Dropbox comprend un solide écosystème de développeurs s'appuyant sur notre API (Application Programming Interface) polyvalente. Il existe actuellement plus de 100 000 applications actives, conçues pour la communication professionnelle, la gestion de documents, la productivité, la gestion de projets ou la gestion des identités.

L'API Dropbox

Il existe trois types d'API Dropbox :

- **API Sync.** Cette API permet aux applications mobiles de stocker et de synchroniser des fichiers avec Dropbox de façon efficace.
- **API Datastore.** Cette API assure la synchronisation des données structurées.
- **API Core.** Cette API prend en charge des fonctionnalités avancées : recherche, révisions, restauration de fichiers, etc. Elle est adaptée aux applications exécutées sur des serveurs.

> "Avec Dropbox Entreprises, nous disposons d'un espace sécurisé et centralisé pour le stockage de tous nos documents, et nous évitons les soucis liés à la gestion de plusieurs centaines d'ordinateurs au sein d'une même entreprise."
>
> Bill O'Donnell, architecte principal et vice-président sénior des produits mobiles, Kayak

Autorisations accordées aux applications

- **Outils Drop-ins.** Les outils Drop-ins Chooser et Saver permettent respectivement de transférer des données vers le compte Dropbox d'un utilisateur et de télécharger des données à partir d'un compte. Ils jouent essentiellement le même rôle que les boîtes de dialogue classiques de type Ouvrir et Enregistrer, et limitent l'accès d'une application aux fichiers et/ou dossiers que l'utilisateur sélectionne au cas par cas.
- **Datastores uniquement.** Les applications qui n'ont accès qu'aux datastores peuvent accéder aux données par le biais de l'API Datastore ou en demandant l'accès au fichier ou dossier concerné par le biais des drop-ins. Les datastores sont des structures de données spécifiques stockées indépendamment du système de fichiers. Avec cette autorisation, l'application n'a pas accès aux fichiers présents dans la Dropbox de l'utilisateur (en dehors des fichiers pour lesquels celui-ci a explicitement accordé une autorisation par le biais des drop-ins).
- **Dossier de l'application.** Un dossier spécifique portant le nom de l'application est créé dans le dossier des applications de la Dropbox de l'utilisateur. L'application dispose d'un accès en lecture et en écriture uniquement pour ce dossier, et les utilisateurs peuvent transmettre des contenus à l'application en plaçant des fichiers dans ce dossier. En outre, l'application peut également créer son propre datastore et/ou demander l'accès à un fichier ou dossier par le biais des outils Drop-ins.
- **Type de fichier.** L'autorisation Type de fichier autorise les applications à accéder à tous les fichiers d'un type donné (fichier texte, images, etc.) présents dans la Dropbox d'un utilisateur. En outre, l'application peut également créer son propre datastore et/ou demander l'accès à un fichier ou dossier par le biais des outils Drop-ins.

- **Intégralité de la Dropbox.** L'application peut accéder en lecture et en écriture à tous les fichiers et dossiers de la Dropbox d'un utilisateur, ainsi qu'aux datastores via l'API Datastore. Elle peut également demander l'accès à un fichier ou dossier par le biais des outils Drop-ins.

Dropbox utilise le protocole d'autorisation standard OAuth pour permettre aux utilisateurs d'autoriser les applications à accéder à leur compte sans pour autant divulguer leurs identifiants. Nous prenons en charge OAuth 2.0 et 1.0 pour l'authentification des demandes envoyées aux API.

Développeurs Dropbox

Nous avons établi un certain nombre de consignes et de bonnes pratiques pour aider les développeurs à créer des applications basées sur nos API, qui respectent et protègent la confidentialité des utilisateurs tout en améliorant le confort d'utilisation de Dropbox.

- **Clés d'application.** Pour chaque application créée par un développeur, une clé d'application Dropbox unique doit être utilisée. En outre, si une application fournit des services ou des logiciels qui incluent la plate-forme Dropbox dans un wrapper en vue de permettre à d'autres développeurs de l'utiliser, chaque développeur doit également demander sa propre clé d'application Dropbox.
- Processus d'examen des applications
  - **État "En développement".** Lorsqu'une application utilisant l'API Dropbox est créée, son état est "En développement". L'application fonctionne alors comme n'importe quelle autre application en production, à ceci près qu'elle ne peut être utilisée que par 100 utilisateurs maximum. Pour que l'application devienne accessible au grand public, les développeurs doivent demander à la faire passer à l'état "En production".
  - **État "En production" et validation.** Pour qu'une application utilisant l'API puisse être validée et accéder à l'état "En production", elle doit respecter notre charte éditoriale de marque ainsi que nos conditions d'utilisation, et donc ne pas utiliser la plate-forme Dropbox de façon illicite. Les usages suivants, entre autres, sont interdits : incitation à la violation de la propriété intellectuelle ou de copyrights, création de réseaux de partage de fichiers, téléchargement illégal de contenus. Avant de faire examiner leur application, les développeurs doivent fournir des informations complémentaires concernant les fonctionnalités de leur application et la manière dont elle utilise l'API Dropbox. Une fois que l'application est validée et passe à l'état "En production", le nombre d'utilisateurs pouvant associer leur compte Dropbox à l'application n'est plus limité.

Informations sur la sécurité de Dropbox

Dropbox a mis en place un cadre régissant la sécurité des informations. À ce titre, nous vérifions et mettons à jour régulièrement nos règles de sécurité, nous formons nos collaborateurs aux questions de sécurité, nous testons la sécurité de nos applications et de notre réseau, nous surveillons la conformité aux règles de sécurité, et nous réalisons des évaluations internes et externes des risques.

Nos règles

Nous avons établi un ensemble complet de règles de sécurité couvrant différents domaines : sécurité des informations, sécurité physique, réponse en cas d'incident, accès logique, accès physique à l'infrastructure de production, gestion des changements et assistance. Ces règles sont examinées et validées au moins une fois par an. Nos collaborateurs, stagiaires et sous-traitants sont informés des modifications apportées à ces règles et sont formés en continu aux questions de sécurité, par e-mail et/ou par le biais de notre page intranet consacrée aux règles de sécurité.

- **Sécurité des informations.** Règles applicables aux informations relatives aux utilisateurs et à Dropbox : sécurité des appareils, exigences en matière d'authentification, sécurité des données et des systèmes, utilisation par les collaborateurs des consignes relatives aux ressources, gestion des problèmes potentiels, etc.
- **Sécurité physique.** Règles nous permettant de maintenir un environnement sûr et sécurisé pour les collaborateurs et les installations de Dropbox (consultez la section Sécurité physique ci-après).
- **Réponse en cas d'incident.** Exigences que nous nous sommes fixées pour répondre aux incidents de sécurité potentiels, notamment en matière d'évaluation, de communication et de procédures d'enquêtes.

- **Accès logique.** Règles permettant de sécuriser les systèmes Dropbox, les informations des utilisateurs et les informations de Dropbox. Elles couvrent le contrôle d'accès aux environnements de gestion et de production.
- **Accès physique à l'infrastructure de production.** Procédures de restriction d'accès au réseau de l'infrastructure physique de production : examen du personnel par la direction, annulation des autorisations accordées aux collaborateurs qui quittent l'entreprise, etc.
- **Gestion des changements.** Règles relatives à la vérification du code et à la gestion par les développeurs autorisés des modifications apportées au code source des applications, à la configuration des systèmes et aux mises en production, qui sont susceptibles d'influer sur la sécurité.
- **Assistance.** Règles régissant l'accès aux métadonnées des utilisateurs par notre équipe d'assistance, à des fins de consultation, d'assistance ou d'exécution d'actions sur les comptes.

Règles applicables aux collaborateurs et accès

L'accès de nos collaborateurs à l'environnement de Dropbox est géré par un annuaire central, et authentifié en associant des mots de passe sécurisés, des clés SSH protégées par un code secret et des jetons à usage unique. 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.

L'accès entre les réseaux est limité au strict minimum en termes de nombre de collaborateurs et de services. Par exemple, l'accès au réseau de production est protégé par une clé SSH et limité aux équipes techniques qui doivent pouvoir y accéder 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 collaborateurs qui accèdent aux environnements de gestion et de production à respecter les bonnes pratiques en matière de création et de stockage des clés SSH privées.

Les règles d'intégration et de retrait des collaborateurs impliquent une vérification des antécédents, l'acceptation des règles de sécurité, la diffusion des mises à jour apportées aux règles de sécurité et la signature d'accords de non-divulgation. Les accès des collaborateurs sont révoqués au plus vite lorsqu'ils quittent l'entreprise.

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 des utilisateurs. 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.

À l'heure où Dropbox devient le véritable prolongement de l'infrastructure des clients, ces derniers ont la certitude que nous nous comportons en véritable garant de leurs données. Pour en savoir plus, consultez la section Confidentialité ci-après.

Sécurité du réseau

Dropbox apporte un soin tout particulier à la sécurisation de son réseau dorsal. Dropbox identifie et atténue les risques en testant régulièrement les applications et le réseau, et en pratiquant d'autres tests et audits de sécurité, réalisés aussi bien par des équipes internes spécialisées en sécurité que par des spécialistes externes.

Nos techniques de sécurité et de surveillance des réseaux sont conçues pour fournir plusieurs niveaux de protection et de défense. Nous faisons appel à des techniques de protection standard pour faire en sorte que seul le trafic légitime puisse atteindre notre infrastructure : pare-feu, surveillance de la sécurité du réseau, systèmes de détection d'intrusion, etc.

Le réseau privé interne de Dropbox est scindé en plusieurs parties, selon l'usage et le niveau de risque.
Nos réseaux principaux sont les suivants :

- Zone démilitarisée connectée à Internet
- Zone démilitarisée avec VPN frontal
- Réseau de production
- Réseau de gestion

L'accès à l'environnement de production est limité aux adresses IP autorisées. Les adresses IP bénéficiant d'un accès sont

associées au réseau de l'entreprise ou au personnel Dropbox autorisé. Ces adresses IP sont vérifiées chaque trimestre pour garantir la sécurité de l'environnement de production. L'accès permettant de modifier la liste des adresses IP est limité aux personnes autorisées.

Une séparation stricte est maintenue entre le réseau interne de Dropbox et l'Internet public. L'intégralité du 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.

Gestion des changements

Une règle formelle de gestion des changements a été définie par l'équipe technique de Dropbox de façon à ce que l'ensemble des changements liés aux applications soient autorisés avant leur implémentation dans les environnements de production. Les modifications du code source sont initiées par les développeurs qui souhaitent apporter une amélioration à l'application ou au service Dropbox. Toutes les modifications doivent faire l'objet de tests d'assurance qualité permettant de vérifier que toutes les exigences de sécurité sont respectées. Une fois que les procédures d'assurance qualité sont terminées, la modification est implémentée. Toutes les modifications approuvées par une procédure d'assurance qualité sont automatiquement implémentées dans l'environnement de production. Les problèmes de sécurité potentiels sont analysés à chaque modification du code, par le biais de nos procédures d'assurance qualité et d'un examen manuel de la sécurité du code.

Toutes les modifications qui passent en production sont consignées et archivées, et des alertes sont envoyées automatiquement à la direction de l'équipe technique 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 mise à jour de ce serveur, du pare-feu et des autres configurations de sécurité, conformément aux 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'un examen régulier.

Conformité

Dropbox a passé l'examen SOC 2 (Service Organization Control) de type 2 mené par un vérificateur indépendant. Le rapport établi dans le cadre de cet audit détaille la conception et l'efficacité de nos contrôles de sécurité, et il peut être utilisé par les clients Dropbox Entreprises dans le cadre de leurs propres stratégies de conformité. Notre document d'audit SOC 2 de type 2 est disponible sur demande. Nous continuerons à participer régulièrement à des audits SOC 2, et les rapports actuels seront disponibles au fur et à mesure de leur rédaction.

Dropbox vérifie également les rapports SOC de toutes les organisations de sous-services. En l'absence de rapport SOC, nous effectuons des visites sur site pour contrôler la sécurité des nouvelles installations afin de vérifier que les contrôles de sécurité physiques, environnementaux et opérationnels respectent nos critères en la matière ainsi que les exigences mentionnées dans nos contrats. Les procédures d'identification et de résolution des violations de sécurité font également l'objet d'un examen. Nous évaluerons les autres certifications et standards de conformité, et nous communiquerons les informations les concernant lorsque nous les aurons.

Sécurité physique

Infrastructure

L'accès physique aux installations de l'organisation de sous-services hébergeant nos systèmes de production est limité aux collaborateurs autorisés par Dropbox qui ont besoin d'un tel accès pour mener à bien leurs tâches. Toutes les personnes qui ont besoin d'accéder aux installations de l'environnement de production ne bénéficient d'un accès qu'après autorisation explicitement accordée par le responsable concerné.

Les responsables tiennent un registre des demandes d'accès, des motifs d'accès et des approbations, et l'accès n'est accordé qu'aux seules personnes appropriées. Une fois l'approbation reçue, un membre responsable de l'équipe chargée de l'infrastructure contacte l'organisation de sous-services adéquate afin de demander un accès au nom de 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 accordé aux individus autorisés, le datacenter doit limiter l'accès aux seules personnes autorisées et est entièrement responsable de ce contrôle d'accès.

Bureaux

- **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 est limité aux collaborateurs Dropbox autorisés. Un système d'accès par badge permet de n'autoriser l'accès à ces installations qu'aux seules personnes autorisées.
- **Accès aux serveurs.** L'accès aux zones où se trouvent les serveurs de l'entreprise est limité au personnel autorisé, par le biais de rôles bénéficiant d'une élévation de privilèges accordée par le système d'accès par badge. La liste des personnes autorisées à accéder physiquement aux environnements de gestion et de production est réexaminée au moins chaque trimestre.

Confidentialité

Nous accordons une grande importance à la protection de la confidentialité de nos utilisateurs et de leurs données professionnelles. Aussi, nous nous efforçons d'empêcher tout accès non autorisé aux informations concernant nos utilisateurs. Nos règles de confidentialité sont consultables à l'adresse suivante : www.dropbox.com/privacy.

Dropbox respecte le cadre juridique du Safe Harbor, qui établit une sphère de sécurité entre l'UE et les États-Unis ainsi qu'entre la Suisse et les États-Unis. En respectant les sept principes du Safe Harbor, une organisation atteste qu'elle protège convenablement la confidentialité des utilisateurs conformément à la directive de l'UE relative à la protection des données.

Les plaintes et les litiges relatifs au respect par Dropbox des principes du Safe Harbor doivent être examinés et résolus par le biais de TRUSTe, un organisme tiers indépendant.

Dropbox s'engage à faire preuve de transparence au sujet du traitement des demandes d'informations sur les utilisateurs transmises par la police et la justice, notamment en ce qui concerne le nombre et les types de demandes. Nous examinons toutes les demandes de données pour vérifier qu'elles sont conformes au droit, et nous nous engageons à informer les utilisateurs, comme la loi nous y autorise, lorsque leur compte est cité dans une demande émanant des autorités.

Ces efforts soulignent notre engagement vis-à-vis de la protection de la confidentialité des utilisateurs et de leurs données. Nous étudions en permanence de nouvelles approches pour poursuivre nos efforts en la matière, notamment en défendant et en protégeant la confidentialité des utilisateurs auprès des tribunaux. Notre dernier rapport de transparence est disponible à l'adresse suivante : www.dropbox.com/transparency.

Résumé

Dropbox Entreprises offre des outils simples d'utilisation conçus pour aider les équipes à collaborer efficacement sans mettre à mal la sécurité exigée par les entreprises. Avec notre approche multiniveau qui associe une solide infrastructure dorsale à un ensemble de règles personnalisable, nous proposons aux entreprises une solution performante capable de s'adapter à leurs besoins. Pour en savoir plus sur Dropbox Entreprises, contactez notre équipe commerciale à l'adresse sales@dropbox.com.

À propos de Dropbox

Dropbox vous permet d'avoir toujours à portée de main vos documents, photos et vidéos, et de les partager facilement. Vos fichiers sont à jour sur tous vos appareils et restent synchronisés de façon extrêmement simple avec les autres membres de l'équipe. Avec Dropbox Entreprises, vous bénéficiez d'outils d'administration, d'une assistance téléphonique et de tout l'espace dont vous avez besoin.