Dropbox Business

Responsabilité partagée : travaillons ensemble pour mieux sécuriser vos données

Dropbox collabore avec ses clients Business et Education pour mieux sécuriser leurs données. Nous mettons tout en œuvre pour protéger notre infrastructure, nos réseaux et nos applications, mais aussi pour former nos employés aux pratiques de sécurité et de confidentialité, bâtir une culture centrée sur notre volonté d'être dignes de confiance et soumettre nos systèmes et nos pratiques aux tests et audits externes les plus rigoureux.

Certes, Dropbox est garant de la sécurité à tous les niveaux de service relevant de son contrôle, mais nos clients jouent un rôle essentiel dans la protection et la sécurisation de leurs équipes et de leurs données. En tant qu'administrateur d'une équipe Dropbox Business ou Education, vous êtes en mesure de configurer, d'utiliser et de surveiller votre compte dans des conditions qui vous permettent de répondre aux besoins de sécurité, de confidentialité et de conformité de votre organisation.

Nous avons créé ce guide pour vous aider à comprendre les mesures mises en place par Dropbox pour sécuriser votre compte, mais aussi ce que vous pouvez faire pour garder une visibilité sur les données de votre équipe et les contrôler.

Les responsabilités de Dropbox

Intégrer la sécurité à notre architecture

Des milliers d'entreprises du monde entier nous confient leurs fichiers les plus importants. Pour nous montrer dignes de cette confiance, nous mettons tout en œuvre pour développer des produits sécurisés sur lesquels les administrateurs comme vous peuvent compter. Voici quelques-unes des méthodes que nous employons pour sécuriser notre architecture et nos réseaux.

Architecture distribuée

L'architecture de Dropbox prévoit la répartition des différents niveaux d'information sur plusieurs services. En plus de rendre les synchronisations plus rapides et plus fiables, ce principe améliore également la sécurité. En raison de sa nature, l'architecture de Dropbox ne permet pas d'accéder à chaque service pour recréer des fichiers ou des documents Paper.

Réseaux sécurisés

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. L'accès à l'environnement de production est limité aux adresses IP autorisées et nécessite une authentification multifacteur sur tous les points de terminaison.

Chiffrer les données des utilisateurs

Les clients Dropbox Business et Education interagissent avec nos systèmes via le client de bureau, le site Web et les applications mobiles, ainsi qu'au moyen d'API. Quelle que soit l'application utilisée, nous protégeons vos fichiers en transit comme au repos.

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.

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. 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 au repos sont protégés par un chiffrement AES (Advanced Encryption Standard) de 256 bits. Les fichiers sont stockés dans des blocs de fichier 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.

Assurer un service fiable

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. 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 toutes les heures, en complément des sauvegardes complètes quotidiennes. Les métadonnées sont stockées sur des serveurs hébergés et gérés par Dropbox. Pour le stockage des blocs de fichiers, Dropbox utilise des systèmes internes et externes conçus pour assurer une durabilité annuelle des données d'au moins 99,999999999 %.

En cas d'indisponibilité du service, les utilisateurs Dropbox ont toujours accès aux dernières versions synchronisées de leurs fichiers dans le dossier Dropbox local de 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.

De même, des copies redondantes des données Paper sont réparties sur différents appareils au sein d'un datacenter, selon un modèle de disponibilité N+1. De plus, des sauvegardes complètes des données Paper sont effectuées quotidiennement. Pour le stockage des documents Paper, Dropbox fait appel à des systèmes tiers conçus 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 en mode hors ligne dans l'application mobile.

Limiter l'accès des employés aux systèmes backend

Que vous soyez un client Dropbox Business ou Education, nous savons que lorsque vous stockez des fichiers et des documents Paper dans Dropbox, vous comptez sur nous pour veiller dessus de façon responsable. Pour cette raison, nous contrôlons très strictement l'accès de nos collaborateurs à nos systèmes internes. Les échanges entre nos réseaux de production et d'entreprise font l'objet de limitations très strictes. 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. 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.

S'assurer que nos employés restent sensibilisés aux questions de sécurité et de confidentialité

Pour garantir la sécurité de son service, Dropbox sait qu'il est important d'employer des collaborateurs sensibilisés aux questions de sécurité et capables de reconnaître toute activité suspecte. Les employés de Dropbox doivent ainsi prendre connaissance des règles de sécurité avant de se voir accorder un accès aux systèmes. Ils doivent également suivre une formation sur la sécurité et la confidentialité lors de leur embauche, ainsi que des formations complémentaires tous les ans. Des e-mails d'information, des présentations, ainsi que les ressources disponibles sur notre intranet contribuent à assurer cette sensibilisation.

Valider nos pratiques

Pour nous assurer que nos pratiques de sécurité fonctionnent correctement, nous faisons évaluer leur efficacité par des organismes indépendants. Des spécialistes effectuent régulièrement des tests d'intrusion et de vulnérabilité sur nos environnements d'entreprise et de production. Les problèmes identifiés sont résolus de façon prioritaire par notre équipe d'ingénieurs en charge de la sécurité. En outre, des auditeurs tiers comparent nos pratiques de sécurité aux normes en vigueur dans le secteur informatique à travers le monde. Pour vous aider à découvrir les pratiques de Dropbox et à les évaluer, nous mettons notre rapport SOC 3, et nos certificats ISO 27001, ISO 27017, ISO 27018 et ISO 22301 à votre disposition en ligne. Vous pouvez également obtenir notre rapport SOC 2, un rapport contenant le mappage des critères HIPAA et son évaluation, une évaluation et un rapport BSI C5 (disponibles en anglais et en allemand) ou encore des synthèses des résultats de nos tests d'intrusion, si vous en faites la demande et acceptez de signer un accord de non-divulgation.

Vous alerter en cas de problème

État du service

Dropbox vous permet de bénéficier d'un site indépendant qui vous indique l'état de notre service pour les clients Dropbox Business et Education. Si vous êtes un client, vous pouvez vous rendre sur status.dropbox.com à tout moment pour connaître l'état actuel du site, ainsi que les interruptions passées et les informations concernant la maintenance.

Notifications en cas de faille de sécurité

Dropbox vous notifiera de toute violation de données, conformément aux dispositions légales en vigueur. Nous observons des règles et des procédures de réponses aux incidents, en particulier un processus dédié aux notifications des failles de sécurité, qui nous permettent d'avertir les clients touchés lorsque c'est nécessaire. Si vous avez conclu un accord de partenariat conforme aux normes HIPAA ou un accord de traitement des données répondant aux lois de l'Union européenne, vous serez averti selon les modalités énoncées dans ces accords.

Vous donner les outils pour sécuriser vos données

Nous tenons à ce que vous disposiez, au même titre que tous les administrateurs Dropbox Business ou Education, des outils nécessaires pour prendre des décisions informées et responsables concernant la sécurité de votre équipe. Afin de vous aider à configurer, à utiliser et à surveiller votre compte comme vous l'entendez, nous avons intégré à votre interface d'administration des fonctionnalités de sécurité à activer au nom de votre équipe. Grâce à des guides tels que le présent document, notre livre blanc Dropbox Business et la sécurité, le centre d'assistance et notre équipe d'assistance, nous mettons à votre disposition toutes les informations nécessaires pour comprendre comment ces paramètres peuvent vous aider à configurer votre compte de façon responsable.

Les responsabilités des clients

Découvrir nos pratiques

Décider si Dropbox Business ou Education offrent une solution adaptée aux besoins de votre entreprise est un processus important. Nous vous conseillons de prendre le temps d'évaluer nos pratiques, comme vous le feriez pour toute autre application. À cette fin, vous pouvez notamment consulter nos certificats ISO 27001, ISO 27017, ISO 27018 et ISO 22301 ; notre rapport de conformité à la norme SOC 3 et notre auto-évaluation de niveau 1 et certificat CSA STAR de niveau 2, qui sont disponibles en ligne. Nous pouvons également vous donner accès à des documents supplémentaires pour vous aider à prendre une décision en connaissance de cause si vous acceptez de signer un accord de non-divulgation. Ces documents comprennent nos rapports d'évaluation SOC 1 et SOC 2, notre rapport d'évaluation C5 (disponible en anglais et en allemand), un mappage de nos pratiques internes, des recommandations si vous souhaitez vous conformer aux règles HIPAA/HITECH relatives à la sécurité, à la confidentialité et à la notification des violations de sécurité, et enfin des synthèses de nos derniers tests d'intrusion dans les applications. Nos Conditions d'utilisation, notre Politique d'utilisation acceptable et notre Contrat Entreprises sont disponibles en ligne. En les examinant, vous pourrez vous assurer que Dropbox Business ou Education constituent bien une solution adaptée à votre équipe.

Configurer les autorisations de partage et de consultation

La flexibilité offerte par Dropbox Business et Education vous permet de configurer votre compte en fonction de vos besoins de sécurité, de collaboration et de confidentialité. Les administrateurs peuvent examiner et modifier ces paramètres dans l'interface d'administration pour les adapter à leur environnement de partage ou à la réglementation en vigueur. Par exemple, il est possible de configurer des comptes de sorte que certains dossiers, liens et documents Paper ne puissent pas être partagés avec des personnes ne faisant pas partie de votre équipe. Lorsque des membres de votre équipe partagent des dossiers de fichiers Dropbox, ils peuvent personnaliser leurs paramètres et sélectionner le niveau d'accès souhaité, avec autorisation de modification ou en lecture seule.

Renforcer l'authentification

Des pratiques d'authentification sérieuses contribuent à assurer la sécurité des données de votre équipe. Les administrateurs doivent examiner les paramètres d'authentification disponibles et activer ceux qui conviennent le mieux à la protection des comptes dont ils sont responsables. Les comptes Dropbox Business et Education comprennent les options suivantes :

Validation en deux étapes

Les administrateurs peuvent exiger que tous les membres d'une équipe utilisent la validation en deux étapes pour se connecter à leurs comptes. Cette fonctionnalité de sécurité, que nous vous recommandons vivement d'utiliser, ajoute un niveau de protection supplémentaire aux comptes Dropbox des utilisateurs. Lorsqu'elle est activée, Dropbox exige un code de sécurité à six chiffres ou une clé de sécurité, 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.

Authentification unique

Si votre entreprise fait déjà appel à un fournisseur d'identité pour la gestion des règles de mots de passe et l'authentification, il peut être préférable de configurer une authentification unique pour votre équipe Dropbox Business ou Education. Mais surtout, l'accès à Dropbox sera géré selon les mêmes règles de mots de passe que les autres services au sein de votre entreprise. Mais surtout, l'accès à Dropbox sera géré selon les mêmes règles de mots de passe que les autres services au sein de votre entreprise.

Effectuer des bilans d'accès réguliers

L'accès au compte de votre équipe évoluera au fil des changements d'effectifs, de rôles et d'appareils. Procédez à des vérifications régulières afin de vous assurer que l'accès à votre compte est bien limité aux personnes, appareils et applications souhaités, et pour vous aider à conserver l'entière maîtrise de vos informations. Les droits d'accès peuvent être modifiés ou supprimés très simplement à l'aide de l'interface d'administration.

Membres d'équipe

L'interface d'administration permet d'ajouter, de supprimer ou de contrôler des membres d'une équipe très facilement. Pour vous assurer que les données sensibles de votre compte Dropbox Business ou Education ne sont accessibles que par les personnes souhaitées, nous vous conseillons de contrôler régulièrement cette liste. Vous pourrez ainsi supprimer l'accès des personnes quittant votre organisation ou des employés qui n'ont plus besoin d'un droit d'accès à la suite d'un changement de poste. De façon similaire, vous pouvez modifier les droits d'accès dans l'interface d'administration afin que chaque compte utilisateur dispose d'un niveau d'accès approprié.

Appareils

Avec les membres de votre équipe, vérifiez fréquemment la liste des appareils associés à votre compte afin de supprimer ceux qui ne sont plus utilisés ou autorisés. Les appareils peuvent être dissociés par les membres de l'équipe comme par ses administrateurs. Dans un cas comme dans l'autre, vous et les membres de votre équipe avez également la possibilité d'effacer les contenus Dropbox de l'appareil à distance quand vous le dissociez. La dissociation et l'effacement d'appareils contribuent à la sécurité de vos données si un employé quitte votre équipe, voire en cas de perte ou de vol.

Applications tierces

Il existe un écosystème très fiable d'applications tierces que vous pouvez associer à votre compte Dropbox Business ou Education pour bénéficier de fonctionnalités supplémentaires. Les intégrations qui proposent des fonctionnalités de gestion des informations et des événements de sécurité, de protection contre la perte de données, et de gestion des identités peuvent vous aider à renforcer les pratiques de sécurité que vous avez déjà mises en place. Or s'il est vrai que ces applications tierces peuvent jouer un rôle important dans votre compte, il ne faut pas oublier qu'elles ne sont pas comprises dans nos services. À ce titre, elles ne sont couvertes ni par les Conditions d'utilisation de Dropbox ni par nos accords professionnels, tels que les accords de partenariat ou les accords de traitement de données que vous pouvez avoir conclus avec Dropbox. Les applications peuvent vous demander divers niveaux d'accès à vos informations selon leurs fonctionnalités. En tant qu'administrateur, vous pouvez associer ou supprimer des applications au niveau de l'équipe, c'est-à-dire pour l'ensemble de votre compte, ou supprimer des applications spécifiques ajoutées par les membres de l'équipe à leur propre compte. Les applications tierces et leurs accès peuvent être vérifiés et modifiés depuis la console d'administration.

Assurer la détection de toute activité suspecte

En tant qu'administrateur d'équipe, vous pouvez consulter et exporter des rapports détaillant les événements liés aux fichiers de votre équipe, ainsi que toutes les activités de partage, d'authentification et d'administration. Les administrateurs doivent régulièrement inspecter ces rapports de façon à détecter toute activité inhabituelle et contribuer à la sécurité de leur équipe. Il peut être intéressant de faire appel à une application tierce assurant la gestion des informations et des événements de sécurité ou à d'autres solutions de surveillance pour renforcer vos capacités.

Déterminer vos besoins de chiffrement

Par défaut, Dropbox stocke une copie locale de vos fichiers sur votre ordinateur pour vous permettre d'accéder en un clin d'œil aux fichiers dont vous avez besoin. Les copies locales de vos fichiers bénéficient du même niveau de protection que tous les autres fichiers se trouvant sur votre ordinateur. Pour plus de sécurité, nous vous conseillons d'activer le chiffrement des disques durs de tous vos appareils lorsque cela est possible et de définir un mot de passe sécurisé et unique pour votre ordinateur portable, votre téléphone, vos tablettes ou tout appareil permettant d'accéder à votre compte Dropbox. L'utilisation de mots de passe sécurisés et uniques sur vos appareils protégera également l'accès à vos documents Paper.

Dropbox protège les fichiers transférés vers votre compte en les scindant en blocs indépendants et en soumettant chacun de ces blocs à un chiffrement AES (Advanced Encryption Standard) de 256 bits. De même, Dropbox protège les documents Paper au repos en les chiffrant dans des systèmes de stockage persistant avec le même algorithme AES (Advanced Encryption Standard) de 256 bits. Dropbox gère les clés de chiffrement pour le compte de ses clients afin de leur simplifier le processus et de leur offrir certaines fonctionnalités.

Les membres Dropbox Business et Education peuvent également chiffrer leurs fichiers avant de les transférer vers Dropbox à leur propre initiative ou à l'aide d'une application intégrée tierce. Toutefois, les utilisateurs chiffrant des données avant de les transférer vers leur compte Dropbox sont responsables de la gestion de leurs clés de chiffrement. Le fait de chiffrer des fichiers avant de les transférer vers Dropbox peut également entraîner la désactivation de certaines fonctionnalités.

Dropbox Business

Nous invitons les clients souhaitant en savoir plus sur la façon dont Dropbox envisage la sécurité à lire notre livre blanc sur la sécurité ou à consulter notre site : dropbox.com/business/trust.
Pour en savoir plus sur Dropbox Business ou Education et demander l'envoi de rapports d'audits indépendants, remis contre signature d'un accord de non-divulgation, veuillez envoyer un e-mail à l'adresse sales@dropbox.com.