Protection de vos données dans le Cloud avec les mesures de sécurité et de chiffrement les plus complètes

Les atouts de MozyPro

Simple

Gère sans encombre les sauvegardes, les synchronisations et l'accès mobile pour les environnements multiutilisateurs et multi-serveurs à partir d'une console web unique.

Sécurisé

Vos données sont sécurisées avec un chiffrement de classe militaire, des centres de données de classe mondiale et avec EMC, une société créée pour durer.

Abordable

Maîtrisez vos coûts grâce à une solution qui ne requiert aucun achat de matériel et n'implique que des frais généraux très minimes.

Contacter MozyPro

emeasales@mozy.com
0800 91 71 34
www.mozy.fr/pro

Au-delà de la sauvegarde des données

Le développement des solutions de sauvegarde Cloud peut s'expliquer par leur capacité à fournir une protection des données et une continuité d'activité efficaces de manière plus fiable et plus cohérente, tout en réduisant considérablement les coûts IT et les efforts continus en matière de maintenance et de support. Cependant, avant de profiter de tout service de sauvegarde Cloud, les entreprises doivent examiner de près les méthodes de chiffrement et les mécanismes de sécurité employés par le Service Provider. L'un des principaux Service Providers du secteur de la sauvegarde Cloud, Mozy prend la protection de vos données dans le Cloud très au sérieux : il utilise les mesures de sécurité et de protection de la confidentialité les plus complètes.

Sécurité

Mozy chiffre vos données avant qu'elles ne quittent votre machine, pendant le transfert par câble et alors qu'elles sont au repos dans nos datacenters. Les datacenters EMC appliquent des pratiques de sécurité physiques et techniques et le cas échéant, respectent les principes de confidentialité du Safe Harbor de l'Union européenne. En outre, Mozy a été certifié conforme aux normes SOC 1 SSAE 16 Type 2 et ISO 27001. Ces vérifications indépendantes certifient que les processus et les procédures de Mozy respectent ou dépassent les objectifs de contrôles les plus stricts du secteur. En se soumettant volontairement à un audit SSAE 16 et en obtenant la certification ISO 27001, Mozy montre son engagement pour les informations de ses clients, ainsi que son niveau de préparation aux menaces actuelles qui pèsent sur les informations numériques. Non seulement beaucoup de services de sauvegarde Cloud ne respectent pas de telles normes de sécurité, mais certains ne chiffrent pas vos données de manière totalement sécurisée et d'autres encore négligent tout simplement le chiffrement. Plus loin dans ce document, nous détaillons les mesures et les options complètes que Mozy propose pour garantir la protection et le chiffrement corrects de vos données.

Normes et options de chiffrement de Mozy

Avant même que vos données de sauvegarde ne quittent votre ordinateur, Mozy les chiffre à l'aide d'une clé de chiffrement AES ou Blowfish. Blowfish est un algorithme du domaine public créé en 1993 par un cryptographe de renom, Bruce Schneier. Cet algorithme générique rapide utilise un code par blocs symétrique sécurisé à longueur de clé variable. Mozy utilise la longueur de clé maximale, soit 448 bits, lorsqu'il a recours à l'algorithme de chiffrement Blowfish.

AES est un algorithme de chiffrement 256 bits standard qui est devenu la norme de facto pour l'administration des États-Unis en matière de chiffrement des informations confidentielles et classées top secret. Il s'agit également de l'algorithme de chiffrement standard utilisé par la NSA (National Security Agency) et c'est devenu l'un des algorithmes les plus largement pris en charge et utilisés pour le chiffrement. Par ailleurs, l'algorithme AES est conforme à la norme FIPS (Federal Information Processing Standard) 140-2 pour la cryptographie. Par conséquent, l'utilisation du chiffrement AES assure à votre entreprise de respecter entièrement les normes de protection des données publiques, ce qui permet à toutes les administrations et filiales réglementées d'utiliser les options de chiffrement AES de Mozy pour protéger leurs données.

Même si AES est considéré comme un algorithme plus sécurisé ou plus robuste que Blowfish, ces deux algorithmes offrent un très haut niveau de sécurité. En outre, alors qu'AES peut atteindre des vitesses de chiffrement élevées, cet algorithme n'est pas aussi rapide que Blowfish.

Bien que Blowfish soit considéré comme un algorithme sécurisé, aucune analyse cryptographique de ce dernier n'est accessible au public. Cela n'indique en aucun cas que l'algorithme lui-même est défaillant, simplement que s'il a des points faibles, ils n'ont pas encore été identifiés. Cela suggère également que les autres algorithmes ayant reçu plus d'attention pourraient connaître une longévité supérieure en matière d'utilisation dans le secteur et d'étendue de la prise en charge. Par contre, AES a fait l'objet de nombreuses vérifications. Dans le cadre de son adoption en tant qu'Advanced Encryption Standard lui-même, il a été soumis à un processus d'examen de cinq ans. Depuis l'an 2000, un certain nombre d'analyses cryptographiques publiques ont été menées sur AES, ce qui a entraîné son approbation et sa distinction globales en tant que l'un des algorithmes de chiffrement les plus sécurisés disponibles.

Types de chiffrement

L'utilisation du chiffrement AES ou Blowfish avec le service MozyPro dépend de l'option de chiffrement Mozy choisie parmi les trois suivantes, chacune représentant des avantages spécifiques :

- **Clé de chiffrement par défaut de Mozy :** Mozy attribue une clé de chiffrement à vos utilisateurs. Cette dernière est stockée et gérée par Mozy pour une expérience la plus transparente possible. Cette option utilise le chiffrement Blowfish.
- **Clé de chiffrement personnelle :** l'utilisateur saisit une phrase de passe qui sert à créer la clé de chiffrement. Chaque utilisateur crée une clé de chiffrement personnelle unique. Cette option utilise le chiffrement AES.
- **Clé de chiffrement d'entreprise :** l'administrateur saisit une phrase de passe qui sert à créer la clé de chiffrement. Vous pouvez créer une clé pour tous les utilisateurs de l'entreprise ou une clé unique pour chaque groupe d'utilisateurs. On appelle parfois cette clé la c-key. Cette option utilise le chiffrement AES.

Indiquez le type de clé de chiffrement à utiliser pendant l'installation du logiciel Mozy : ce chiffrement sera systématiquement associé aux fichiers stockés dans le Cloud EMC. Les clients MozyPro peuvent configurer le type de chiffrement à l'aide d'une configuration client pour attribuer le type de clé aux utilisateurs. Vous pouvez modifier le type de chiffrement après l'installation du logiciel. Si vous le modifiez, le logiciel téléchargera de nouveau tous vos fichiers pour garantir que les fichiers stockés sont chiffrés avec la clé de chiffrement actuellement sélectionnée.

Indépendamment du type de clé de chiffrement utilisé, les fichiers sont chiffrés lors de la première étape de leur traitement, avant leur envoi vers le Cloud EMC. Cela garantit que les fichiers sont protégés avant même de quitter votre

ordinateur et qu'ils le restent pendant leur transfert et lorsqu'ils sont au repos dans le Cloud EMC. Si vous utilisez des clés de chiffrement personnelles, Mozy ne peut pas lire votre clé de chiffrement et ne l'entiercera pas. Par conséquent, les fichiers ne seront jamais déchiffrés avant leur restauration sur votre ordinateur.

En plus du chiffrement AES ou Blowfish, Mozy utilise au cours du transfert de vos données une connexion SSL certifiée avec vérification de certificat bidirectionnelle pour les communications entre vos ordinateurs et le service MozyPro. Il s'agit de la technologie utilisée par les banques pour sécuriser les transactions en ligne. De plus, tous les utilisateurs doivent s'authentifier à Mozy à l'aide d'un nom d'utilisateur et d'un mot de passe enregistrés.

Clé de chiffrement par défaut de Mozy

Ce type de clé utilise l'algorithme Blowfish pour chiffrer vos données. Outre l'utilisation d'un algorithme de chiffrement très sécurisé et très rapide, l'un des principaux avantages de la clé par défaut est que Mozy la gère pour vous. Vous n'avez pas besoin de mémoriser la phrase de passe pour chiffrer ou déchiffrer vos données. Mozy s'en occupe automatiquement, garantissant que vos données sont chiffrées en toute sécurité avant même leur transfert pendant le processus de sauvegarde.

Par ailleurs, les fonctions Web et de mobilité de Mozy bénéficient d'une prise en charge intégrée de la clé par défaut. En d'autres termes, vous pouvez afficher, rechercher ou télécharger les fichiers de sauvegarde de manière transparente à partir de votre périphérique mobile ou d'un navigateur Web. La clé par défaut permet un chiffrement simple et prêt à l'emploi de toutes vos sauvegardes. Même si ce type de clé offre un chiffrement facile et sécurisé, certaines entreprises préfèrent gérer leur propre phrase de passe de chiffrement plutôt que d'autoriser Mozy à la connaître. Comme son nom l'indique, la clé de chiffrement par défaut sera utilisée par défaut à moins que vous ne choisissiez l'une des autres options.

Clé de chiffrement personnelle

Ce type de clé constitue l'une des deux options Mozy destinées aux entreprises ou utilisateurs souhaitant profiter d'un chiffrement AES. Les clés de chiffrement personnelles permettent aux utilisateurs individuels de gérer leurs propres clés. Lors de l'utilisation d'une telle clé, chaque utilisateur indique une clé unique pour les données de son ordinateur. En plus de bénéficier du niveau de sécurité le plus élevé que l'algorithme AES propose, la protection est encore renforcée par le caractère unique de la clé, connue seulement de l'utilisateur. Le service Mozy ne gère pas cette clé et n'en a pas connaissance. Par conséquent, même en cas de demande légale, Mozy ne peut pas déchiffrer vos fichiers si vous choisissez la clé de chiffrement personnelle.

Pour créer leur clé de chiffrement personnelle unique, les utilisateurs sont invités à saisir une phrase de passe pouvant contenir des caractères, des symboles ou des chiffres. La longueur de cette phrase de passe n'est pas limitée. Pour sécuriser la clé, le logiciel client Mozy applique un hachage cryptographique sur la phrase de passe stockée sur la machine de l'utilisateur. Le service Mozy ne stocke pas votre clé de chiffrement personnelle et il ne peut pas la déchiffrer. Par conséquent, pour utiliser les fonctions Web et mobiles de Mozy pour afficher, rechercher ou directement télécharger les fichiers sauvegardés, vous devrez saisir la phrase de passe appropriée.

De plus, si vous êtes administrateur Mozy, vous devez connaître ou avoir accès aux clés de chiffrement personnelles des utilisateurs pour effectuer une restauration en leur nom ou pour restaurer les fichiers des utilisateurs ayant quitté l'entreprise.

De même, si des utilisateurs individuels oublient leur phrase de passe, ils ne pourront pas déchiffrer ou restaurer leurs données vers un poste de travail. Pour se prémunir contre tout oubli de phrase de passe, Mozy propose une option d'exportation. Elle permet à l'utilisateur d'enregistrer la phrase de passe de chiffrement sous forme de fichier de texte brut sur un partage réseau ou une clé USB. Cette phrase peut également être enregistrée sur le disque

dur de l'ordinateur local, mais cela n'est pas recommandé, car ce fichier ne sera pas accessible en cas de panne système. En cas d'utilisation de l'option d'exportation, nous recommandons aux entreprises d'établir une règle de sécurité concernant l'emplacement de stockage de tels fichiers de phrase de passe.

Pour les entreprises souhaitant profiter du chiffrement AES sans laisser leurs utilisateurs gérer leurs propres phrases de passe, Mozy propose l'option de clé de chiffrement d'entreprise.

Clé de chiffrement d'entreprise

Ce type de clé (parfois appelée c-key) permet aux entreprises de profiter de la puissance de l'algorithme AES pour chiffrer leurs données, tout en simplifiant et en renforçant considérablement la gestion des phrases de passe. Grâce à cette option, un individu crée la phrase de passe pour l'entreprise tout entière. Il peut s'agir de la personne de votre choix, par exemple un administrateur, un responsable ou un directeur IT ou de la sécurité.

Depuis la console d'administration de Mozy, vous pouvez définir la phrase de passe de la clé d'entreprise et son emplacement de stockage, comme un partage réseau, un serveur Web ou dans un package d'installation de Mozy sur les ordinateurs clients. Comme Mozy est utilisé sur différentes machines, chacune d'entre elles accédera à cet emplacement pour utiliser la clé de chiffrement pour chiffrer et déchiffrer les fichiers.

La phrase de passe de la clé de chiffrement d'entreprise sera certainement stockée sur un partage réseau ou un serveur Web. Par conséquent, pour se protéger contre tout accès non autorisé à cette clé, Mozy utilise une fonction de code secret partagé qui chiffre la phrase de passe. Lorsque vous installez Mozy sur vos machines clients, le chiffrement de cette phrase de passe est automatiquement programmé dans chaque client. Par conséquent, les postes de travail exécutant le client de sauvegarde Mozy peuvent utiliser la phrase de manière transparente pour chiffrer ou déchiffrer les fichiers selon les besoins.

Tout comme avec les clés de chiffrement personnelles, Mozy ne peut pas vous aider à déchiffrer les fichiers sauvegardés, car nous n'avons pas accès à votre clé de chiffrement d'entreprise. Ces clés sont partagées avec tous les utilisateurs de votre entreprise ou au sein d'un groupe d'utilisateurs, et elles peuvent être distribuées sur les ordinateurs locaux ou stockées sur un serveur réseau pour que les utilisateurs y aient accès.

Datacenters très avancés

Les datacenters ultraperformants d'EMC ont fait l'objet d'un audit SSAE 16 et sont certifiés ISO 27001. Ils utilisent les mesures de sécurité suivantes.

- **Sécurité et surveillance sur site :** tous nos datacenters se trouvent dans un périmètre sécurisé et des responsables opérationnels y travaillent 24x7x365. Ils y appliquent les normes les plus strictes en matière de protection des données. Deux types d'authentification sont requis pour entrer sur le site et accéder à la zone des serveurs Mozy : authentification par carte et sécurité biométrique.
- **Système de détection et d'extinction d'incendie :** Les datacenters gérés par EMC sont équipés d'un système d'extinction des incendies pour les éteindre en cas d'urgence sans nuire au fonctionnement des serveurs.
- **Alimentations et réseaux redondants :** l'alimentation de nos datacenters est conditionnée et protégée par des systèmes redondants. En outre, plusieurs opérateurs réseau gèrent chaque datacenter pour garantir leur fonctionnement en cas de panne de l'un des réseaux.
- **Contrôle de la température :** tous nos sites de datacenter sont équipés de systèmes de ventilation pour maintenir les serveurs à des températures de fonctionnement optimales.

Et comme Mozy possède plusieurs datacenters dans le monde, les données peuvent être stockées localement, au sein de communautés économiques. Par exemple, les données peuvent être conservées aux États-Unis ou dans l'Union européenne. Cela garantit ainsi le respect des lois et principes de gestion des données locaux.

Confidentialité

Pour protéger la confidentialité de vos données, Mozy intègre une combinaison de contrôles techniques, administratifs et physiques destinés à préserver vos données personnelles. Par ailleurs, Mozy a établi son propre engagement en matière de confidentialité, en conduisant nos activités en suivant ces principes :

- Vos informations sont les vôtres, pas les nôtres.
- Nous ne vendrons jamais vos données à quiconque, pas plus que nous ne vendrons des informations à votre sujet.
- Nous ne consulterons jamais vos informations pour créer votre profil ou pour de la publicité ciblée.
- Vous pourrez toujours récupérer vos informations. Nous n'avons aucun droit sur vos informations si vous quittez le service.

Protégez vos données, protégez votre entreprise

Lorsque vous sauvegardez des informations avec Mozy, vous gardez le contrôle des données pendant les processus d'authentification et de chiffrement que le système utilise. Chaque fichier stocké dans le Cloud Mozy est chiffré avant son transfert vers notre infrastructure. Autrement dit, toutes les informations confidentielles et sensibles restent privées pendant que nous les stockons pour vous. Nous ne compromettons par les contrôles de sécurité internes utilisés par nos clients pour respecter les diverses réglementations en vigueur. Mozy prend également des mesures proactives pour protéger les données contre les attaques, les risques ou tout accès non autorisé qui pourraient menacer la sécurité, la confidentialité et l'intégrité de vos données.

L'objectif de Mozy c'est de protéger à la fois vos données et votre entreprise. Vous pouvez compter sur ses règles de sécurité strictes, son chiffrement conforme aux normes de l'industrie et ses datacenters très avancés pour vous offrir la disponibilité, la sécurité et la confidentialité nécessaires pour la protection optimale de vos données métiers.

Une entreprise conçue pour durer

Mozy sauvegarde les données de plus de 100 000 entreprises et de 6 millions d'individus, et il stocke près de 90 pétaoctets de données. Faisant partie d'EMC, leader dans le domaine du stockage et entreprise du Fortune 200, Mozy est un élément essentiel dans la mission d'EMC de protéger vos données métiers critiques. EMC fournit les solutions et les technologies d'infrastructure qui permettent aux entreprises de renforcer leur avantage concurrentiel et de valoriser leurs informations. De par son héritage en tant que l'une des premières entreprises de Cloud computing et son partenariat avec EMC, Mozy possède l'expérience, l'infrastructure et la solidité financière pour garantir la sécurité et la disponibilité de vos données, quand vous en avez besoin. Des entreprises du Fortune 500 aux petites structures, Mozy by EMC est l'un des noms les plus fiables dans le domaine de la sauvegarde Cloud.