

# Comment utiliser le cloud sans risque

Stocker films, photos, musique et données en ligne, c'est pratique. Mais ça peut aussi être imprudent. Nos conseils pour profiter du cloud, sans nuages.

**L**es chiffres donnent le vertige : fin 2014, il y avait environ 300 exabytes de données stockées dans le cloud au niveau mondial, soit 7% des données produites sur terre. L'équivalent de 450 milliards de DVD, de 90 000 milliards de photos ou de MP3 ou encore de 37 milliards de milliards de pages de texte ! On estime qu'un Européen sur cinq utilise déjà le cloud pour sauvegarder des fichiers et les partager.

Le cloud computing, c'est la possibilité d'accéder à distance et depuis n'importe quel appareil à des fichiers (mails, agenda, photos, musique, vidéos...), qui ne sont plus enregistrés dans la mémoire de votre ordinateur ou de votre smartphone, mais sur un puissant serveur central. Problème : il faut obligatoirement une connection Internet, et les données stockées en ligne sont potentiellement piratables. Ainsi, en septembre, des hackers sont parvenus à pénétrer dans les serveurs d'iCloud, le service d'Apple, pour y voler les photos dénudées que des célébrités y avaient placées. Des clichés très personnels de l'actrice Jennifer Lawrence ou de la chanteuse Rihanna se sont ainsi retrouvés sur les réseaux sociaux.

Côté entreprises, le cloud permet de recourir à des logiciels en ligne, sans avoir à les installer sur l'ensemble des postes des utilisateurs. Autre avantage : ne pas avoir à investir régulièrement pour augmenter les capacités de stockage, au risque de se retrouver en surcapacité par la

suite. Il n'y a qu'à adapter le forfait aux besoins. Ses ordinateurs ne tournant à plein régime qu'au moment des fêtes, Amazon a ainsi eu l'idée, dès 2002, de louer ses serveurs pendant les périodes creuses. Depuis, IBM, Google, Apple, Amazon et Microsoft ont lancé leurs solutions de cloud et plusieurs autres compagnies sont sur les rangs, comme Cisco, qui a annoncé un plan de 1 milliard de dollars pour créer un nouveau service de cloud. En 2020, le marché devrait représenter plus de 190 milliards de dollars. Nos conseils pour y voir plus clair.

Mathias Chaillot •

## 1. Est-ce que c'est sûr ?

Globalement, oui. Mais de la même façon que vous pouvez vous faire voler le mot de passe de votre messagerie, celui du cloud peut être forcé. Le meilleur moyen de se protéger est de bien choisir sa combinaison : elle doit être complexe et ne pas être utilisée pour d'autres services. «Un mot de passe fort, c'est au moins dix caractères, de trois types différents (chiffres, lettres, caractères spéciaux)», conseille Eric Filiol, directeur de recherche en sécurité à l'ESIEA (école d'ingénieurs en informatique). Essayez un mécanisme simple : les deux premières lettres du site, toujours les quatre mêmes chiffres, et les deux dernières lettres du site, en les reculant d'un cran dans l'alphabet. Et modifiez-le à chaque incident de sécurité (alerte de votre antivirus, comportement anormal de votre ordinateur).

## 2. Peut-on tout stocker dans le cloud ?

Le cloud n'étant pas infallible, toute donnée potentiellement sensible ne devrait pas s'y trouver. «Pour les particuliers, on est dans le subjectif, estime Gabriel Chadeau, spécialiste en sécurité pour Vision Solutions. La photo dénudée d'une star n'a pas le même intérêt que celle de madame Michu.» Demandez-vous si un document dans la nature pourrait vous nuire. Qu'un inconnu découvre votre fiche de salaire ne changera pas votre vie. S'il a votre RIB entre les mains, c'est plus gênant.

## 3. Où sont réellement stockées mes données ?

Dans d'immenses data centers répartis sur quatre continents. En Europe, Microsoft et Google en possèdent un à Dublin, mais rien ne dit que c'est là que vont les données européennes : elles peuvent très bien être stockées sur le territoire américain. Vos données peuvent également avoir été copiées dans plusieurs centres, pour éviter qu'elles soient perdues en cas d'incident. Cela ne va pas sans poser de problèmes : les lois sur la vie privée sont plus ou moins souples selon les pays, et rien ne garantit que des données confidentielles en France le soient ailleurs. Par exemple, le Patriot Act autorise le gouvernement américain à piocher dans les serveurs de ses sociétés en cas de menace terroriste. «Mais on a des informations qui nous disent que les Américains utilisent ce prétexte pour récupérer

d'autres données, prévient Eric Filiol. Ce n'est pas de la paranoïa, c'est une réalité.»

## 4. Tous les services de cloud sont-ils sécurisés de la même façon ?

Non, certains ont même démontré leur légèreté. «Tout en bas, vous pouvez mettre Sony et Apple, détaille Eric Filiol. Google est en revanche très sécurisé, mais c'est un cauchemar en termes de respect des données privées. Idem pour Dropbox.» Pour Gabriel Chadeau, «la première chose à faire est de bien lire les contrats, notamment sur les garanties, la localisation des données, les méthodes de cryptage». Si les services doivent au moins afficher la norme ISO 27001, «celle-ci est basée sur un audit, un jour J, explique Mohammed Boumediene, président d'HTTPCS, spécialiste de la sécurité sur Internet. Or les systèmes sont tellement complexes et si souvent mis à jour que ça n'a pas beaucoup de crédibilité. Dans l'idéal, il faut que les données soient chiffrées par une clé unique générée par un mot de passe et un identifiant». Google Drive le fait, pas iCloud.

## 5. Qu'est-ce qu'un coffre-fort numérique ?

La plupart des banques proposent des clouds sécurisés, pour stocker principalement des documents administratifs que l'on souhaite conserver. Vous pouvez faire envoyer certains documents directement par leur expéditeur (les factures EDF, vos fiches de paie, etc.) dans ce



## Les trois principaux services de stockage au banc d'essai



### Prix par mois et capacité de stockage

- Gratuit jusqu'à 2 Go, possibilité d'obtenir jusqu'à 16 Go en parrainant des amis (+ 500 Mo par contact inscrit).
- Formule pro à 99 euros/an pour 1 To d'espace.

### Pour un fichier de 100 Mo

- S'inscrire : **2 clics**
- Stocker : **2 clics**
- Télécharger : **18 secondes**
- Envoyer : **55 secondes**

### Partage en ligne

Oui, mais à la première demande de partage, obligation de valider son adresse mail. Possibilité de partage via un lien à envoyer aux personnes désirées avec, en option, le contrôle des droits des utilisateurs et la date d'expiration du lien.

### Notre avis

Pas le plus intuitif à utiliser, ni le plus rapide. Impossible de créer des documents en ligne avec la version gratuite. Pas de possibilité de transférer un dossier contenant plusieurs fichiers : obligation de les télécharger un par un.

### Prix par mois et capacité de stockage

- Gratuit jusqu'à 15 Go, possibilité d'obtenir jusqu'à 20 Go en parrainant des amis (+ 500 Mo par inscrit).
- De 1,99 euro/mois pour 100 Go à 10 euros/mois avec 1 To et accès à Office 365.

### Pour un fichier de 100 Mo

- S'inscrire : **5 clics**
- Stocker : **2 clics**
- Télécharger : **30 secondes**
- Envoyer : **68 secondes**

### Partage en ligne

Possibilité de partage via un lien avec, en option, un moyen de contrôle du fichier (avec ou sans modification). Mais pas d'option permettant de fixer une date d'expiration du lien.

### Notre avis

Gestion facile et complète des droits de partage. Téléchargement assez lent sur PC, plus rapide sur l'appli. Possibilité dès la version gratuite de créer en ligne des documents (Word, Excel, PowerPoint...) et de les partager. Possibilité de transférer d'un dossier complet.

### Prix par mois et capacité de stockage

- Gratuit jusqu'à 15 Go, à partager entre sa boîte Gmail, Google Drive et Google+ Photos.
- De 1,99 euro/mois pour 100 Go à 9,99 euros/mois pour 1 To, et 299,99 euros/mois pour 30 To.

### Pour un fichier de 100 Mo

- S'inscrire : **1 clic**
- Stocker : **2 clics**
- Télécharger : **22 secondes**
- Envoyer : **20 secondes**

### Partage en ligne

Possibilité de partage de fichiers via un lien, avec contrôle des actions sur le contenu (lecture seule, modification ou commentaire). Pas de possibilité de fixer une date d'expiration du lien.

### Notre avis

Rapide et intuitif. Utile, le mode hors connexion qui permet de travailler sur ses documents même sans accès à Internet. Dès la version gratuite, on peut créer en ligne et partager des documents (Word, Excel, PowerPoint...) avec des applications Google.

coffre-fort virtuel. Leur copie numérique aura alors la même valeur légale que l'original.

**6.** Est-il risqué de partager ses documents ? Si les pirates s'attaquent parfois aux serveurs, il y a très peu de risques qu'ils tentent d'intercepter vos données quand vous les partagez. Mais pour Eric Filiol, «le mieux est de crypter les documents sensibles avant de les stocker en ligne et de transmettre le mot de passe pour le décrypter par un autre canal, comme un SMS». Plusieurs logiciels permettent de le faire simplement, comme TrueCrypt, VeraCrypt ou Ghostscript.

**7.** Les clouds sont-ils compatibles entre eux ?

Non, mais ce n'est pas gênant : avoir un compte n'est nécessaire que pour l'envoi de fichier. Même s'il n'a pas de cloud, un internaute pourra ouvrir le lien et le document que vous lui avez envoyé. En revanche, si vous partagez un film stocké sur Google Drive avec un contact qui, lui, utilise iCloud, il pourra le lire, mais ne pourra pas l'enregistrer directement dans iCloud. Il devra d'abord le télécharger puis l'envoyer vers son cloud.

**8.** Comment faire sans connexion Web ?

Le cloud ne fonctionne qu'avec Internet. Toutefois, certains services comme Google Drive proposent un mode hors connexion pour travailler sur ses documents même sans accès au réseau (ils seront mis à jour à la connexion suivante).

**9.** Combien ça coûte ?

La plupart des services de cloud offrent 15 Go de mémoire gratuite (soit 20 films en DivX, par exemple). Ensuite, on paie selon l'espace de stockage utilisé.

**10.** Quel cloud choisir ?

Voir le test ci-contre. Le mieux est d'essayer d'abord les versions gratuites, puis de choisir en fonction de son utilisation.