Google Workspace : les choses à savoir avant d'activer le chiffrement côté client

Gérer ses transferts de données hors de l'Union européenne sur Google Workspace ? Il y a les « contrôles souverains » pour ça. Derrière cette bannière, un chantier en cours depuis l'an dernier. Avec trois briques : le contrôle des accès, la gestion de la localisation des données et le chiffrement côté client (CSE ; Client-side Encryption).

Sous la bannière « contrôles souverains », Google donne une forme de nouvel élan à la démarche. Au menu, diverses fonctionnalités dont la mise en place doit démarrer « fin 2022 ». Et s'étaler, pour certaines, jusqu'à fin 2023. Mais qu'en est-il pour le moment ?

L'intégration du CSE est récente. Le déploiement a démarré fin mars, sur les deux éditions les plus avancées de la suite : Enterprise Plus et Education Plus. Il couvre pour le moment Drive, Docs, Sheets et Slides… plus ou moins exhaustivement. Il est par exemple encore en bêta sur l'application Drive pour ordinateur. Même chose, entre autres, sur Meet, où certains éléments restent même encore à développer. Comme la compatibilité avec les appareils mobiles et la gestion des clés par le client.

Qu'entend-on par « gestion des clés par le client » ? La possibilité, pour ce dernier, de connecter à Google Workspace son propre service externe, par API. L'autre option, c'est de s'appuyer sur un fournisseur partenaire : Flowcrypt, Fortanix, Futurex, Thales ou Virtru. Dans l'un ou l'autre cas, l'idée est de compléter le chiffrement par défaut de Google Workspace avec des clés sur lesquelles le groupe américain n'a pas la main (le chiffrement intervient dans le navigateur, avant transmission).

Le CSE peut s'activer au niveau des domaines, des unités organisationnelles et des groupes (pas des utilisateurs individuels). Après avoir associé Google Workspace au service de gestion de clés, il faut connecter un fournisseur d'identités qui authentifiera les utilisateurs avant qu'ils puissent chiffrer des fichiers et en consulter.

Google Workspace : les limites du CSE

Travailler avec des fichiers chiffrés implique un certain nombre de choses. En particulier, il n'y a **pas d'édition collaborative** : une seule personne à la fois peut modifier un fichier. **Pas non plus de travail hors connexion**.
L'enregistrement automatique fonctionne par ailleurs différemment : il s'enclenche toutes les 5 minutes. Le poids maximal est de 100 Mo par fichier et de 1 Mo par image. Jusqu'à 100 versions d'un document sont conservées, les « moins importantes » étant supprimées.

Autres actions que ne permet pas le chiffrement côté client :

– Accéder au mode éditeur Office et importer des fichiers Office
– Ajouter des commentaires
– Modifier des fichiers avec l'app mobile
– Utiliser des fonctions dans Sheets pour passer des appels externes

– Utiliser la vérification orthographique, la traduction, la saisie vocale et la comparaison de documents
– Imprimer depuis Sheets et Slides (possible depuis Docs)
– Afficher un aperçu et faire une recherche en texte intégral pour les fichiers chiffrés importés dans Drive
– Réaliser une analyse antiphishing ou une analyse de protection contre la perte des données (ou alors *a minima*, grâce aux métadonnées des fichiers)

On ne peut pas, pour le moment, rechiffrer des fichiers existants avec une autre clé. Ni remplacer le chiffrement côté client par celui de Google.

Pour afficher, modifier ou télécharger un fichier chiffré côté client, il faut utiliser Chrome ou Edge. Et surtout, il **faut une licence Google Workspace** (ou Cloud Identity). Cette exigence **vaut aussi pour les organisations externes** avec lesquelles on partagerait des documents.

Illustration © Google