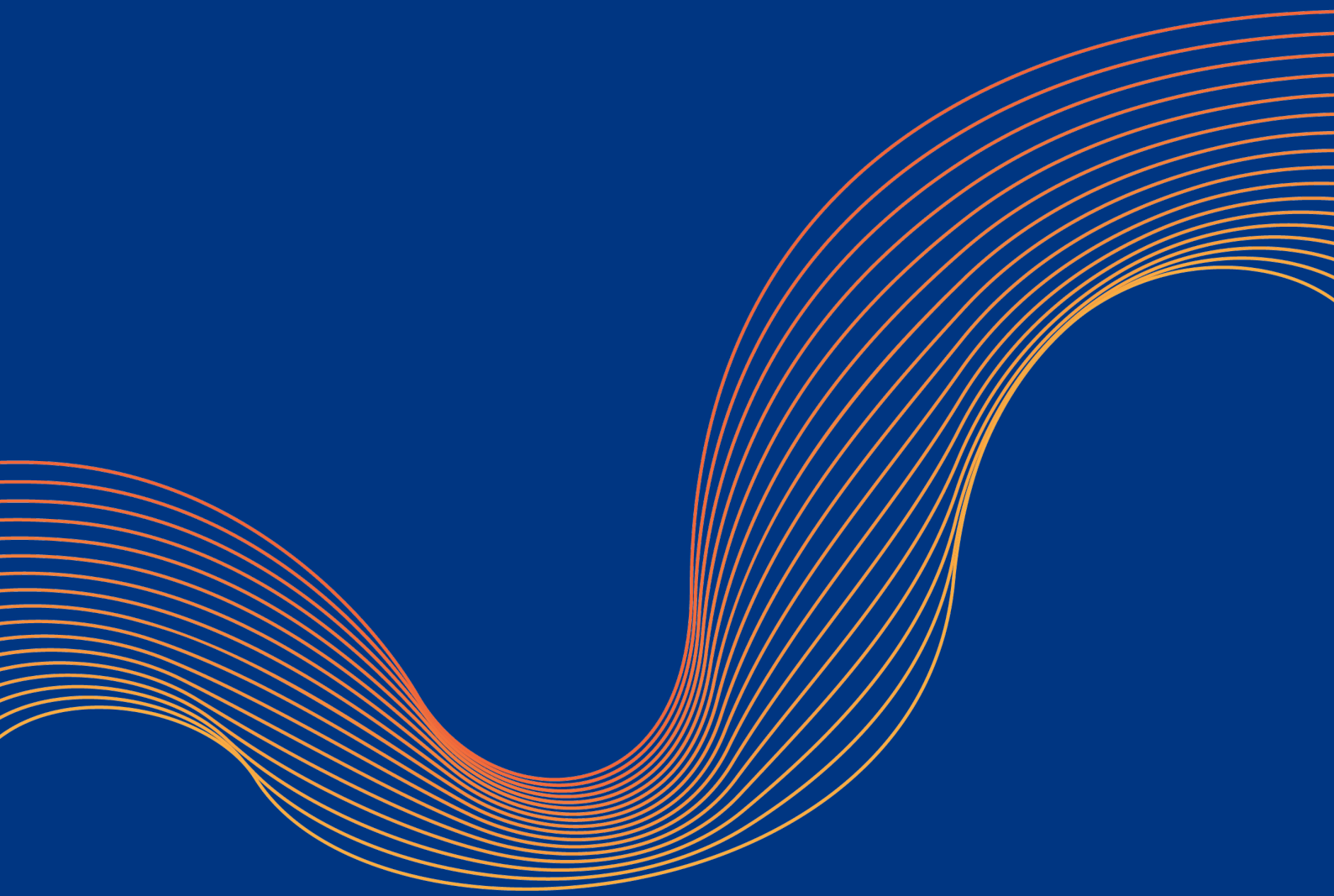
Comment Cloudflare régionalise les données au sein de l'Union européenne ?



+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

Introduction

Cloudflare s'engage à aider ses clients à respecter leurs obligations de confidentialité des données au sein de l'UE.

C'est la raison pour laquelle Cloudflare a créé la Data Localization Suite (suite d'outils de régionalisation des données), un ensemble de produits permettant à nos clients de garder le contrôle sur l'endroit où leurs données sont traitées et stockées. Ce document abordera les aspects techniques de la Data Localization Suite afin d'expliquer comment Cloudflare assure la gestion locale de ses données.

La Data Localization Suite aide nos clients dans trois domaines différents :

1. **Gestion des clés de chiffrement** (Geo Key Manager et SSL sans clé)
2. **Isolement géographique de l'inspection des charges utiles** (services régionaux)
3. **Isolement géographique des métadonnées du client**

Gestion des clés de chiffrement

Afin de s'assurer que leurs clés TLS ne quittent pas l'UE, les clients peuvent choisir entre deux fonctionnalités : SSL sans clé ou Geo Key Manager.

SSL sans clé

Avec le SSL sans clé, les entreprises peuvent tirer parti du réseau Cloudflare tout en conservant le contrôle des informations de leur clé. La fonctionnalité SSL sans clé conviendra bien aux clients qui souhaitent utiliser leur propre serveur de clé et un module de sécurité physique (HSM, Hardware Security Module). Le SSL sans clé n'est finalement « sans clé » que du point de vue de Cloudflare : Cloudflare ne voit jamais la clé privée du client, mais ce dernier en conserve néanmoins la possession et l'usage. Parallèlement, l'utilisation de la clé publique continue à s'effectuer de manière tout à fait habituelle côté client.

Également connu sous son nom plus exact de TLS, le protocole SSL permet d'authentifier et de chiffrer les communications sur un réseau. Ce protocole nécessite l'usage de ce que nous appelons une clé publique et une clé privée. Lorsqu'une entreprise passe par un prestataire comme Cloudflare, ce dernier dispose généralement d'un accès à la clé privée afin d'assurer différents services, comme le pare-feu WAF et la mise en cache. La fonctionnalité SSL sans clé permet à Cloudflare d'exercer ses prestations, tout en s'assurant que la clé privée demeure bien à l'abri, en possession du client.

Cette fonctionnalité repose sur le fait que la clé privée n'est utilisée qu'une seule fois au cours de la procédure de négociation TLS, c'est-à-dire au début d'une session de communication TLS. La fonctionnalité SSL sans clé agit en scindant les étapes de cette négociation. Elle déplace la partie du processus impliquant la clé privée vers un autre serveur, le plus souvent un serveur situé dans les locaux du client. Au lieu d'utiliser directement la clé privée pour générer des clés de session, Cloudflare obtient les clés de session du client par l'intermédiaire d'un canal sécurisé et s'en sert pour assurer le chiffrement. La procédure continue donc toujours à impliquer une clé privée, mais cette dernière n'est communiquée à personne en dehors du périmètre du client.

Imaginons, par exemple, que la société Lambda implémente le protocole SSL. Lambda conservera ainsi sa clé privée en sécurité sur un serveur qu'elle possède et contrôle. Si Lambda commence à utiliser les services de Cloudflare avec notre option SSL par défaut, nous disposerons alors de la clé privée. Toutefois, si Lambda commence à utiliser la fonctionnalité SSL sans clé, la clé privée pourra rester sur le serveur possédé et contrôlé par la société Lambda, comme dans l'implémentation SSL non cloud.

Pour plus de détails techniques, n'hésitez pas à vous rendre dans notre centre d'apprentissage.

Geo Key Manager

La solution Geo Key Manager (gestionnaire de clés géolocalisées) conviendra aux clients qui cherchent à s'assurer que leurs clés privées SSL restent au sein d'une région, mais ne souhaitent pas héberger leur propre serveur de clé.

Les rouages de la fonctionnalité Geo Key Manager reposent en définitive sur le SSL sans clé. Plutôt que de demander à un client d'héberger un serveur de clé au sein de sa propre infrastructure, Cloudflare peut garantir l'hébergement de ces serveurs de clé uniquement au sein de l'UE. Ce format permet de réduire la complexité liée au déploiement du SSL sans clé, tout en s'assurant que les clés privées ne quittent jamais l'UE.

Pour plus de détails sur le fonctionnement du Geo Key Manager, n'hésitez pas à consulter cet article.

Isolement géographique de l'inspection des charges utiles

Services régionaux

Les fonctionnalités SSL sans clé et Geo Key Manager permettent de s'assurer que les clés privées ne quittent pas l'Union européenne. Les services régionaux font en sorte que ces clés ne puissent être utilisées qu'au sein de l'UE. Grâce aux services régionaux, les connexions TLS ne peuvent avoir lieu que dans l'espace européen. Les services de Cloudflare peuvent ainsi uniquement déchiffrer et inspecter le contenu du trafic HTTP au sein de cet espace.

Lorsque les services régionaux sont utilisés, l'ensemble de nos « services pour applications » périphériques s'exécutent au sein de l'UE. Ces services comprennent :

- le stockage et la récupération de données à partir du cache ;
- le blocage de messages HTTP malveillants à l'aide du pare-feu d'applications web (WAF) ;
- la détection et le blocage d'activités suspectes à l'aide de la solution de gestion des bots ;
- l'exécution de scripts Workers ;
- l'équilibrage de charge du trafic vers les serveurs d'origine les plus disponibles.

Vous trouverez plus d'informations sur les services régionaux dans cet article.

Isolement géographique des métadonnées du client

Que sont les métadonnées du client ?

Cloudflare recueille des métadonnées sur l'utilisation de nos produits aux fins suivantes :

- l'établissement de résultats d'analyse via nos tableaux de bord et nos API ;
- le partage de journaux avec nos clients ;
- le blocage des menaces, comme les bots ou les attaques DDoS ;
- l'amélioration des performances de notre réseau ;
- la préservation de la fiabilité et de la résilience de notre réseau.

Le réseau périphérique de Cloudflare se compose de dizaines de services, parmi lesquels notre pare-feu, notre cache, notre résolveur DNS, nos systèmes de protection contre les attaques DDoS et l'environnement d'exécution Workers. Chacun de ces services émet des événements sous forme de journaux structurés contenant divers champs, comme l'horodatage, des informations sur les fonctionnalités Cloudflare utilisées et le client auquel le trafic appartient. Ces messages sont renvoyés vers l'un de nos datacenters centraux afin d'y être traités.

Ces messages ne renferment pas le contenu du trafic du client et ne contiennent donc pas de noms d'utilisateurs, de mots de passe, d'informations personnelles ni d'autres détails privés sur les utilisateurs finaux du client. Toutefois, ces journaux peuvent contenir les adresses IP des utilisateurs finaux, c'est-à-dire des informations considérées comme des données personnelles au sein de l'UE.

Isolement géographique des métadonnées du client

L'isolation géographique des métadonnées du client permet de s'assurer que l'ensemble des métadonnées du trafic susceptibles d'identifier un client restent dans l'UE. Ce cas de figure couvre toutes les données pour lesquelles Cloudflare est sous-traitant des données (tel que défini dans notre politique de confidentialité) et incluttous les journaux et résultats d'analyse visibles par un client.

L'ensemble des métadonnées du trafic susceptibles d'entraîner l'identification d'un client circulent à travers un composant nommé « logfwdr » (prononcé « log forwarder »), situé en périphérie de notre réseau. Les services qui s'exécutent à notre périphérie envoient des messages sous forme de journaux structurés au logfwdr, qui les regroupe en lots et les transfère (« forwarde ») à un datacenter principal.

Lorsque l'isolement géographique des métadonnées est activé pour un client, le logfwdr s'assure que les messages de log susceptibles d'identifier un client (c'est-à-dire, qui contiennent l'ID de compte de ce client) ne sont pas envoyés en dehors de l'UE. Ces messages seront uniquement envoyés à notre datacenter principal situé au Luxembourg et non à notre datacenter principal aux États-Unis.

Conclusion

Cloudflare contribue à bâtir un Internet meilleur et, à cet égard, nous considérons que la protection des données de nos clients et de leurs utilisateurs finaux constitue un élément fondamental de cette mission.

Grâce aux différents produits décrits dans ce document, la Data Localization Suite aide les entreprises à bénéficier des avantages de notre réseau mondial en termes de sécurité et de performances, tout en leur permettant de définir facilement des règles et des mesures de contrôle en périphérie concernant l'endroit où leurs données sont traitées et stockées.