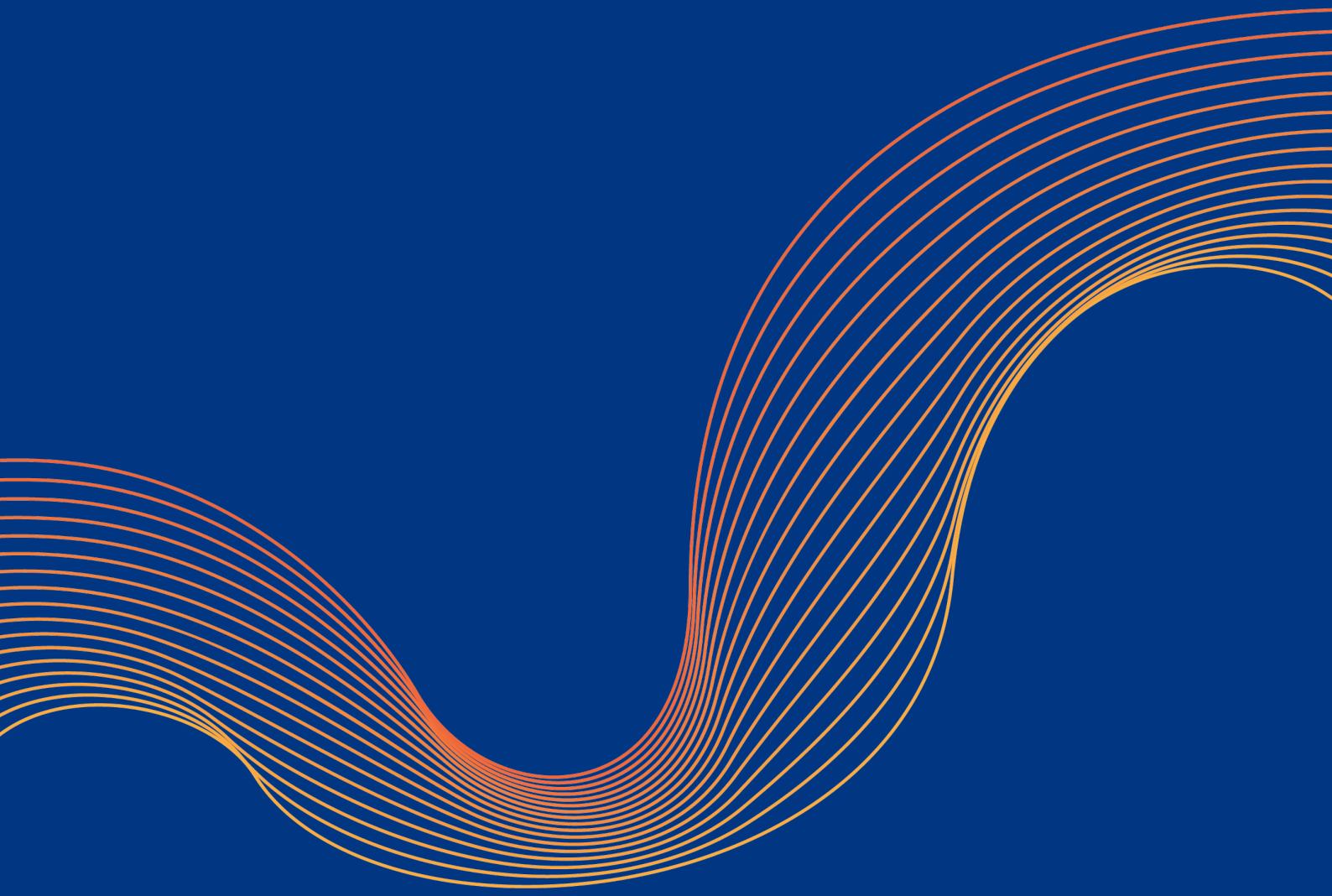
CLOUDFLARE

Cloudflare-Lösung zur Datenlokalisierung in der EU



+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

Einleitung

Cloudflare unterstützt Kunden bei der Einhaltung ihrer Verpflichtungen zur Aufbewahrung personenbezogener Daten in der EU.

Deshalb bieten wir unsere Data Localisation Suite an. Dabei handelt es sich um eine Reihe von Produkten, die den Kunden die Kontrolle darüber geben, wo ihre Daten geprüft und gespeichert werden. In diesem Beitrag werden wir die technischen Aspekte der Data Localisation Suite erörtern, um zu erklären, wie dafür gesorgt werden kann, dass Daten eine bestimmte Region nicht verlassen.

Die Data Localisation Suite unterstützt Kunden in drei verschiedenen Bereichen:

1. **Verwaltung von Kryptoschlüsseln** (Geo Key Manager und Keyless SSL)
2. **Grenze für Payload-Überprüfungen** (Regional Services)
3. **Grenze für Kunden-Metadaten** (Customer Metadata Boundary)

Verwaltung von Kryptoschlüsseln

Um sicherzustellen, dass ihre TLS-Schlüssel die Europäische Union nicht verlassen, können Kunden entweder Keyless SSL oder den Geo Key Manager verwenden.

Keyless SSL

Mit Keyless SSL sind Unternehmen in der Lage, Cloudflare zu nutzen und gleichzeitig ihr Schlüsselmaterial nicht aus ihrer Obhut zu entlassen. Keyless SSL eignet sich gut für Kunden, die einen eigenen Keyserver und ein Hardware-Sicherheitsmodul (HSM) verwenden möchten. Die Lösung ist nur aus der Perspektive von Cloudflare „schlüssellos“: Cloudflare sieht den privaten Schlüssel des Kunden nie, er existiert jedoch und wird vom Kunden benutzt. Der öffentliche Schlüssel wird unterdessen wie gewohnt auf Client-Seite verwendet.

Bei SSL – genauer gesagt TLS – handelt es sich um ein Protokoll zur Authentifizierung und Verschlüsselung der Kommunikation über ein Netzwerk. SSL/TLS erfordert die Verwendung eines öffentlichen und eines privaten Schlüssels. Wenn ein Unternehmen einen Anbieter wie Cloudflare nutzt, hat dieser in der Regel Zugriff auf den privaten Schlüssel, um Dienste wie WAF und Caching bereitzustellen. Mit Keyless SSL können wir unsere Aufgaben erfüllen und gleichzeitig gewährleisten, dass der private Schlüssel sicher im Besitz des Kunden bleibt.

Keyless SSL stützt sich auf die Tatsache, dass der private Schlüssel während des TLS-Handshakes nur einmal verwendet wird, und zwar zu Beginn einer TLS-Kommunikations-Sitzung. Bei Keyless SSL werden die Schritte des TLS-Handshakes aufgeteilt. Der Teil des Vorgangs, der den privaten Schlüssel betrifft, wird auf einen anderen Server verlagert, der sich in der Regel am Standort des Kunden befindet. Anstatt den privaten Schlüssel direkt zur Erzeugung von Sitzungsschlüsseln zu verwenden, erhält Cloudflare die Sitzungsschlüssel über einen sicheren Kanal vom Kunden. Diese werden dann zur Aufrechterhaltung der Verschlüsselung eingesetzt. Es wird also weiterhin ein privater Schlüssel genutzt, der jedoch nicht an Personen außerhalb des Kundenunternehmens weitergegeben wird.

Nehmen wir zum Beispiel an, dass die Acme Co. SSL implementiert. Die Firma speichert ihren privaten Schlüssel sicher auf einem eigenen Server, den sie kontrolliert. Wenn sie beginnt, Cloudflare mit unserer Standard-SSL-Option zu nutzen, wird Cloudflare über den privaten Schlüssel verfügen. Verwendet sie jedoch Keyless SSL, kann der private Schlüssel auf dem Server der Acme Co. verbleiben, wie bei einer SSL-Implementierung ohne Cloud.

Weitere technische Einzelheiten finden Sie in unserem Learning Center

Geo Key Manager

Der Geo Key Manager eignet sich gut für Kunden, die sicherstellen möchten, dass ihre SSL-Schlüssel in einer bestimmten Region verbleiben, aber keinen eigenen Schlüsselserver hosten möchten.

Bei dieser Lösung wird ebenfalls auf Keyless SSL zurückgegriffen. Cloudflare kann Schlüsselserver ausschließlich in der EU hosten, damit ein Kunde keinen Schlüsselserver in seiner eigenen Infrastruktur betreiben muss. Dies reduziert die Komplexität des Einsatzes von Keyless SSL und stellt gleichzeitig sicher, dass private Schlüssel die EU nicht verlassen.

Weitere Einzelheiten über die Funktionsweise des Geo Key Managers finden Sie in diesem Artikel.

Grenze für Payload-Überprüfungen

Regional Services

Keyless SSL und der Geo Key Manager sorgen dafür, dass privates Schlüsselmaterial die EU nicht verlässt. Regional Services stellen sicher, dass diese Schlüssel nur innerhalb der EU verwendet werden, indem TLS-Verbindungen nur in der EU beendet werden. Somit kann Cloudflare den Inhalt des HTTP-Traffics nur innerhalb der EU entschlüsseln und prüfen.

Wenn Regional Services genutzt werden, laufen alle unsere Edge-„Anwendungsdienste“ innerhalb der EU. Dazu gehören:

- Speichern und Abrufen von Inhalten aus dem Cache
- Blockieren bösartiger HTTP-Nutzdaten mit der Web Application Firewall (WAF)
- Erkennen und Blockieren verdächtiger Aktivitäten mit Bot-Management
- Ausführen von Workers-Skripten
- Verteilen des Traffics auf die besten Ursprungsserver mittels Load Balancing

Mehr über Regional Services erfahren Sie in diesem Artikel.

Grenze für Kunden-Metadaten

Was sind Kunden-Metadaten?

Cloudflare sammelt Metadaten über die Nutzung unserer Produkte für die folgenden Zwecke:

- Bereitstellung von Analysen über unsere Dashboards und APIs
- Weitergabe von Rohdatenprotokolle an Kunden
- Stoppen von Sicherheitsbedrohungen wie Bots oder DDoS-Angriffen
- Verbesserung der Performance unseres Netzwerks
- Aufrechterhaltung der Zuverlässigkeit und Ausfallsicherheit unseres Netzwerks

Das Edge-Netzwerk von Cloudflare besteht aus Dutzenden von Diensten, darunter unsere Firewall, der Cache, der DNS-Resolver, die DDoS-Abwehrsysteme und die Workers-Laufzeitumgebung. Jeder dieser Dienste gibt strukturierte Protokollnachrichten aus, die Felder wie Zeitstempel, Informationen über die verwendeten Cloudflare-Funktionen und den Kunden, zu dem der Datenverkehr gehört, enthalten. Diese Nachrichten werden zur Verarbeitung an eines unserer zentralen Rechenzentren zurückgeschickt.

Diese Nachrichten umfassen nicht den Inhalt des Kunden-Traffics und somit auch keine Nutzernamen, Kennwörter, persönlichen Informationen und anderen vertraulichen Einzelheiten zu den Endnutzern der Kunden. Allerdings können diese Protokolle die IP-Adressen der Endnutzer enthalten, die in der EU den personenbezogenen Daten zugerechnet werden.

Customer Metadata Boundary

Customer Metadata Boundary stellt einfach sicher, dass alle Traffic-Metadaten, die einen Kunden identifizieren können, in der EU bleiben. Dies umfasst alle Daten, für die Cloudflare als Auftragsverarbeiter (wie in unserer Datenschutzrichtlinie definiert) fungiert und beinhaltet alle Protokolle und Analysen, die ein Kunde sieht.

Alle Traffic-Metadaten, die einen Kunden identifizieren können, fließen durch eine Komponente namens „logfwdr“ (ausgesprochen: „log forwarder“) an unserer Edge. In unserer Edge betriebene Dienste senden strukturierte Protokollnachrichten an logfwdr, wo die Protokolle gebündelt und an ein zentrales Rechenzentrum weitergeleitet werden.

Ist Metadata Boundary für einen Kunden aktiviert, stellt logfwdr sicher, dass keine diesen Kunden identifizierende Protokollmeldung (d. h. eine Meldung, die die Konto-ID des Kunden enthält) in Nicht-EU-Länder gesendet wird. Die Daten werden nur an unser zentrales Rechenzentrum in Luxemburg und nicht an unser zentrales Rechenzentrum in den USA übertragen.

Fazit

Bei Cloudflare sehen wir es als unsere Aufgabe an, ein besseres Internet zu schaffen. Wir sind der Meinung, dass dem Schutz der Daten unserer Kunden und ihrer Endnutzer dabei eine wesentliche Bedeutung zukommt.

Die in diesem Beitrag beschriebenen Produkte der Data Localisation Suite helfen Unternehmen, die Performance- und Sicherheitsvorteile des globalen Netzwerks von Cloudflare zu nutzen. Gleichzeitig bieten sie eine einfache Möglichkeit, Regeln und Kontrollen dazu festzulegen, wo Daten gespeichert und geschützt werden.