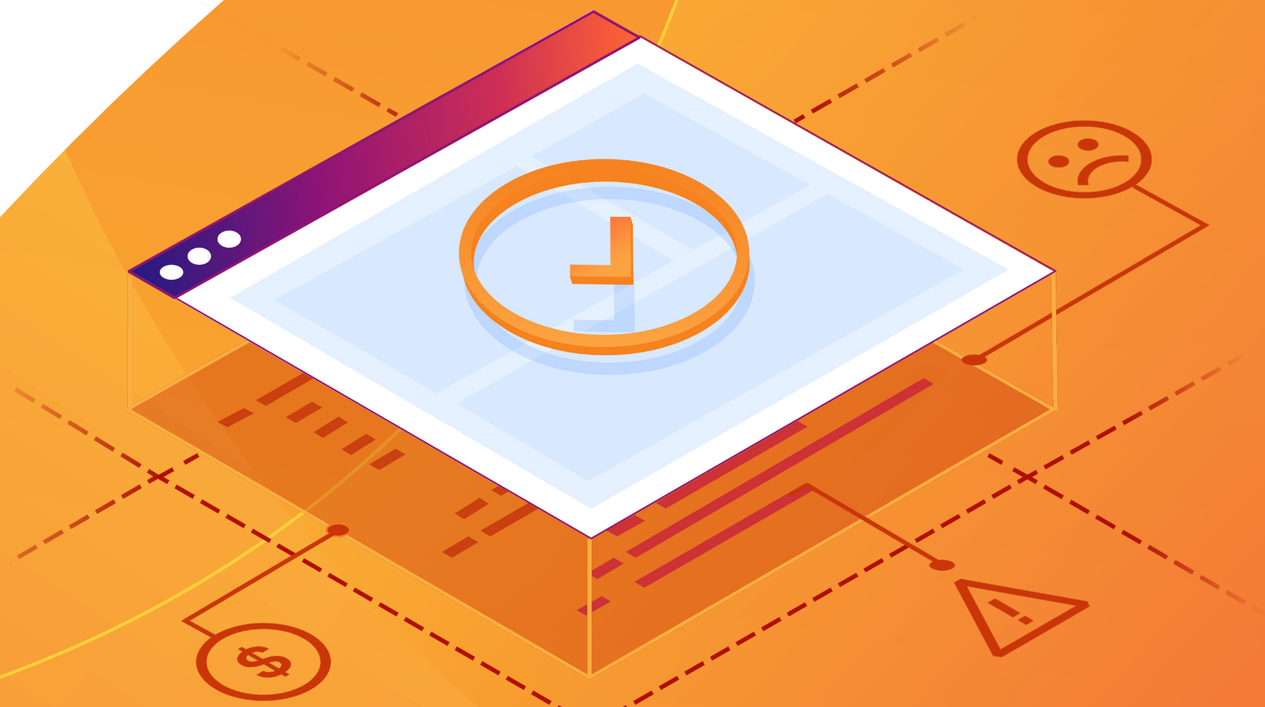
CLOUDFLARE

E-BOOK

# Drei Compliance-Hürden von Sicherheitstools überwinden

Wie die Connectivity Cloud Compliance-Risiken senkt



# Inhalt

# **Compliance heute:** Weniger Ressourcen, sich verändernde Vorschriften



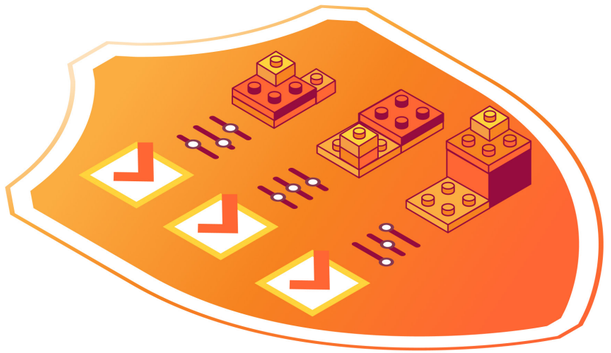
**Die digitale Bedrohungslandschaft verändert sich ständig, die Aufsichtsbehörden prüfen immer strenger: Für viele Unternehmen wird die Einhaltung des Datenschutzes und Vorschriften zur Informationssicherheit zur Herausforderung. Das Zusammenspiel aus technologischer Veränderung, global geteilten Daten und sich wandelnden regulatorischen Bedingungen belasten Unternehmen, die für Datenkonformität sorgen möchten.**

Doch in vielen Fällen stehen den Compliance-Verantwortlichen weniger Ressourcen denn je zur Verfügung:

- **Geringere Budgets**
- **Weniger Mitarbeitende**
- **Steigende Kosten**

Die Compliance-Teams wollen sicherstellen, dass ihre Unternehmen die Anforderungen von gesetzlichen Rahmenbedingungen wie der Datenschutzgrundverordnung (DSGVO), dem Payment Card Industry Data Security Standard (PCI DSS) und anderen erfüllen.  Doch heute tun sie dies in einer digitalen Umgebung, in der die IT-Teams die Kontrolle verloren haben.

Die digitale Modernisierung, das Aufkommen von Remote- und Hybridarbeit und das Experimentieren mit künstlicher Intelligenz (KI) führen zu einer größeren Angriffsfläche, sodass IT-Verantwortliche Mühe haben, Schritt zu halten. Gleichzeitig werden alte Compliance-Lösungen und -Ansätze bis zur Belastungsgrenze strapaziert.



**53 %**

der Unternehmen sagen, dass die technischen Datenschutzfunktionen unterbesetzt sind

# Die 3 größten Compliance-Hürden bestehender Sicherheitsansätze

Da sich ihre digitalen Umgebungen verändert haben, waren Sicherheits- und Compliance-Verantwortliche gezwungen, einen Flickenteppich aus alten Tools und Einzellösungen zusammenzuschustern, die durch manuelle Prozesse ergänzt wurden, um unterschiedliche Nachverfolgungs- und Auditsysteme zu kombinieren. Dieser Ansatz führt sie jedoch direkt zu diesen drei Herausforderungen:

### 1. Ausufernde Kosten

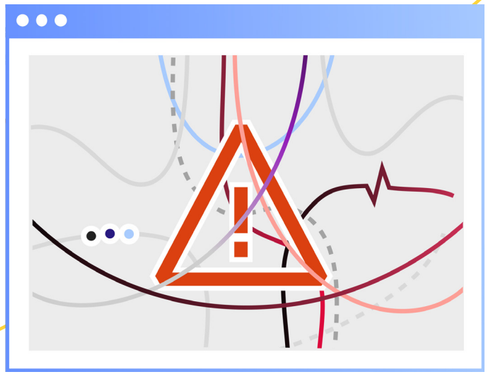
Compliance-Teams müssen für mehrere isolierte Tools für Datensicherheit, -souveränität und -datenschutz bezahlen und diese pflegen (die möglicherweise nicht integriert sind), was die Kosten in die Höhe treibt.

### 2. Hohes Risiko

Bei so vielen unterschiedlichen Tools sind manuelle Prozesse erforderlich, um Protokolle zu kombinieren, damit sie den Audit-Anforderungen entsprechen. Dies verlangsamt die Prozesse, führt zu Fehlern und verschwendet viel Zeit und Mühe.

### 3. Schlechte Nutzererfahrung

Veraltete lokale Sicherheitslösungen führen zu Engpässen im Netzwerk, die die Anwendungsperformance beeinträchtigen. Dieses Problem wird durch die Einschränkungen bei der Datenlokalisierung noch verschärft.



# Mit welchen Fähigkeiten kann man diese Compliance-Hürden bewältigen?



1. **Erstellung optimierter Regeln von** einer einzigen Kontrollebene aus, die als einheitliche Richtlinien-Engine fungiert und einheitliche Datenschutz- und Sicherheitsrichtlinien für lokale, Cloud- und Web-Umgebungen bietet.

2. **Anwendung, Konfiguration und Erweiterung einheitlicher Kontrollen** über Standorte, Benutzer, Daten, Anwendungen (Web, SaaS und private Anwendungen) und Infrastruktur – wo immer Sie sie benötigen. Erfüllen Sie regulatorische Anforderungen, sobald sie festgelegt sind, mit erweiterbaren Kontrollen, einschließlich präziser Zugriffskontrollen für SaaS und geschäftskritische Anwendungen, Überprüfung des HTTP-Traffics auf personenbezogene Daten, um Datenexfiltration zu verhindern, Schutz des Endbenutzer-Browsers vor Angriffen auf die Lieferkette und mehr.

3. **Lokalisierung von Daten zur Einhaltung regionaler Vorschriften** ohne Performance-Einbußen. Stellen Sie sicher, dass Ihre Datenlokalisierungsanforderungen Ihre geschäftliche Agilität nicht beeinträchtigen – mit einem Netzwerk, das Lokalisierungsanforderungen gerecht wird.

4. **Durchführung erfolgreicher Audits** mit Sicherheitseffizienz, Datentransparenz, Analysen und Berichten in Ihrem gesamten Netzwerk und in Multi-Cloud-Umgebungen mit einem einheitlichen Satz von Erkennungs- und Präventionsrichtlinien, um die Kontrolle über Daten zwischen Quelle und Ziel zu gewährleisten und die Einhaltung von Compliance-Anforderungen zu unterstützen.

# Ein neuer Ansatz: Optimierte Compliance mit einer Connectivity Cloud

Eine Connectivity Cloud ist ein neues Modell für die sichere Verbindung von Nutzern, Daten, Infrastruktur und Anwendungen, egal wo sie sich befinden. Dieses Modell gibt Unternehmen nicht nur die Kontrolle über ihre Netzwerke und ihre Sicherheit zurück, sondern geht auch die größten Herausforderungen an, mit denen Sicherheits- und Compliance-Teams konfrontiert sind.

### 1. Gesamtbetriebskosten (TCO) senken

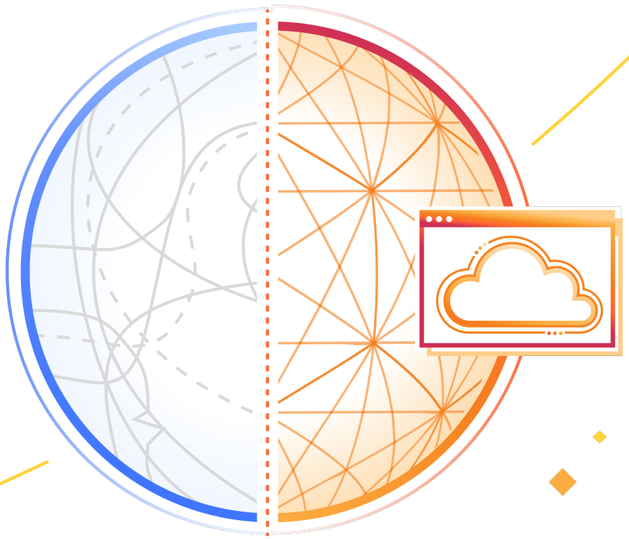
Eine Connectivity Cloud integriert alle Dienste in einer Plattform, die nach Bedarf skaliert.

### 2. Risiken abwehren

Eine Connectivity Cloud bietet zusammensetzbare Kontrollen für Authentifizierung, Sicherheit, Netzwerke und Protokollierung – alles in einem einzigen Dashboard.

### 3. Verbesserung der Nutzererfahrung

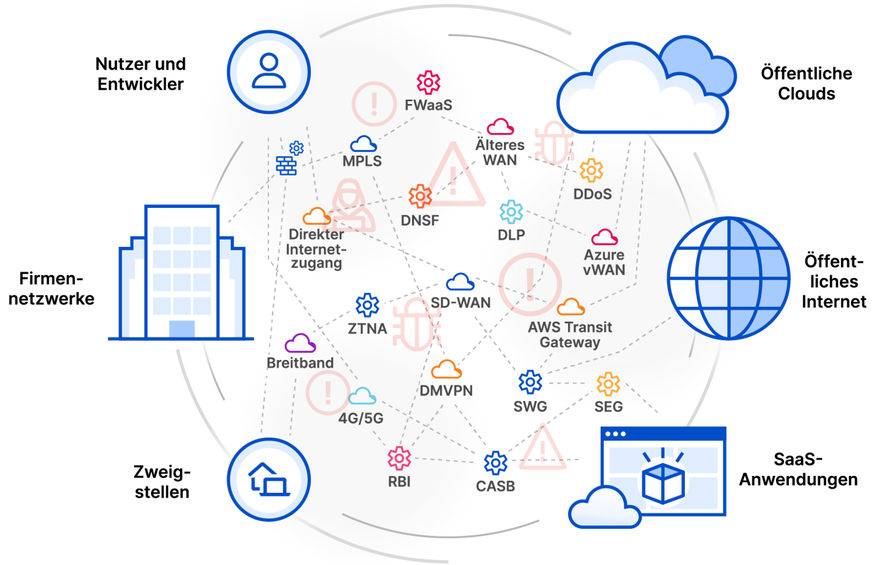
Eine Connectivity Cloud ist standortunabhängig und kann Nutzer unabhängig von ihrem Aufenthaltsort auf der Welt effizient verbinden.



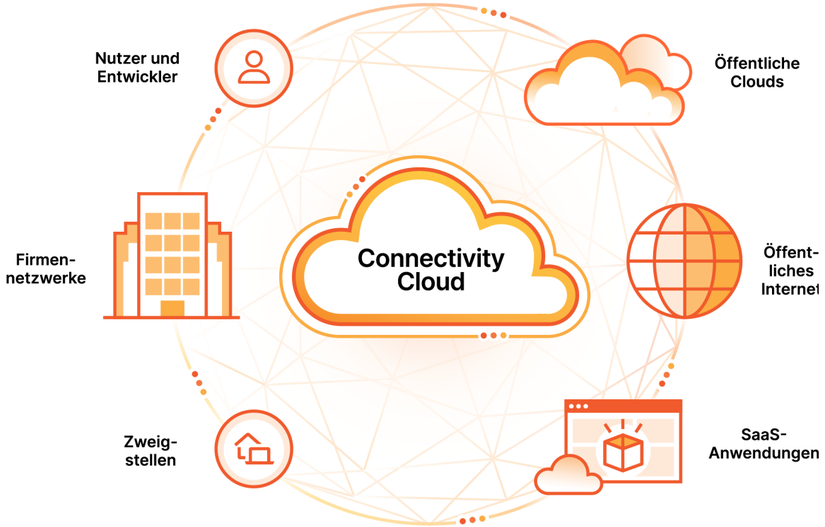
# Ein neuer Ansatz: So funktioniert er

Die Bereiche Cloud, SaaS, Internet und On-Premises sind von Grund auf verschieden und nicht miteinander verbunden. Transparenz und Kontrolle sind schwieriger geworden, und die Werkzeuge, die eingesetzt werden, um die Komplexität in den Griff zu bekommen, machen die Sache nur noch komplizierter. Eine Connectivity Cloud überbrückt Silos, anstatt neue zu schaffen, und bringt eine Organisation…

## Von dieser Situation:




## Zu dieser Situation:

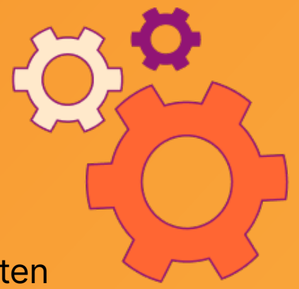


# 4 Must Haves für eine optimierte Compliance

## 1. Für Datenkonformität konzipierte Architektur:

Cloudflare verfügt über das größte und stärkste Netzwerk aller Connectivity Cloud-Anbieter, mit Standorten in Hunderten von Städten weltweit. So können Compliance-Teams einheitliche Sicherheitskontrollen für Standorte, Benutzer, Anwendungen, Daten und die Infrastruktur auf der ganzen Welt anwenden, konfigurieren und erweitern.

## 2. Einheitliche Richtlinien-Engine:



Das Cloudflare-Netzwerk bietet an allen Standorten die gleichen Dienste an. Compliance-Teams können Regeln einmalig von einer einzigen Kontrollebene aus erstellen, die als einheitliche Richtlinien-Engine fungiert, und sie in der gesamten Umgebung anwenden. Wenden Sie Regeln für Zero Trust-Zugriff, Datenschutz, Anwendungssicherheit und mehr an.

## 3. Datensouveränität und Lokalisierung ohne Performance-Einbußen:

Cloudflare ist so konzipiert, dass eine Datenlokalisierung möglich ist. Senden Sie den gesamten Datenverkehr an das nächstgelegene Rechenzentrum, um eine optimale Performance zu erzielen; in der Zwischenzeit werden die Protokolle sicher über ein privates Netzwerk-Backbone an eine beliebige Region gesendet.

## 4. Erfüllung von Audits mit intelligenten Berichten

Die Berichterstattung von Cloudflare bietet detaillierte Prüfprotokolle. Die enorme Größe von Cloudflare ermöglicht einen Einblick in die neuesten Bedrohungen aus dem gesamten Internet und erlaubt eine intelligente automatische Erkennung neuer Angriffe.

# Ein neuer Ansatz: Die Resultate

Die Connectivity Cloud von Cloudflare optimiert die Einhaltung von Vorschriften und minimiert gleichzeitig das Risiko:

**50 %** weniger Richtlinien- und Compliance-Risiken*

**24 %** Einsparung bei den jährlichen Cyberversicherungsprämien*

**59 %** weniger Zeitaufwand für die Verwaltung von Systemen/Prozessen*

Das Ergebnis: ein einfacher, anpassbarer Ansatz für Compliance und Daten, der über ein einziges Dashboard verwaltet wird.

Darüber hinaus können die Compliance-Verantwortlichen sicher sein, dass die Daten im Cloudflare-Netzwerk geschützt sind. Cloudflare erfüllt von Haus aus die Compliance-Anforderungen für:

- PCI
- DSGVO
- SOC 2 Typ II
- FedRAMP

**Für eine vollständige Liste siehe:** https://www.cloudflare.com/de-de/trust-hub/

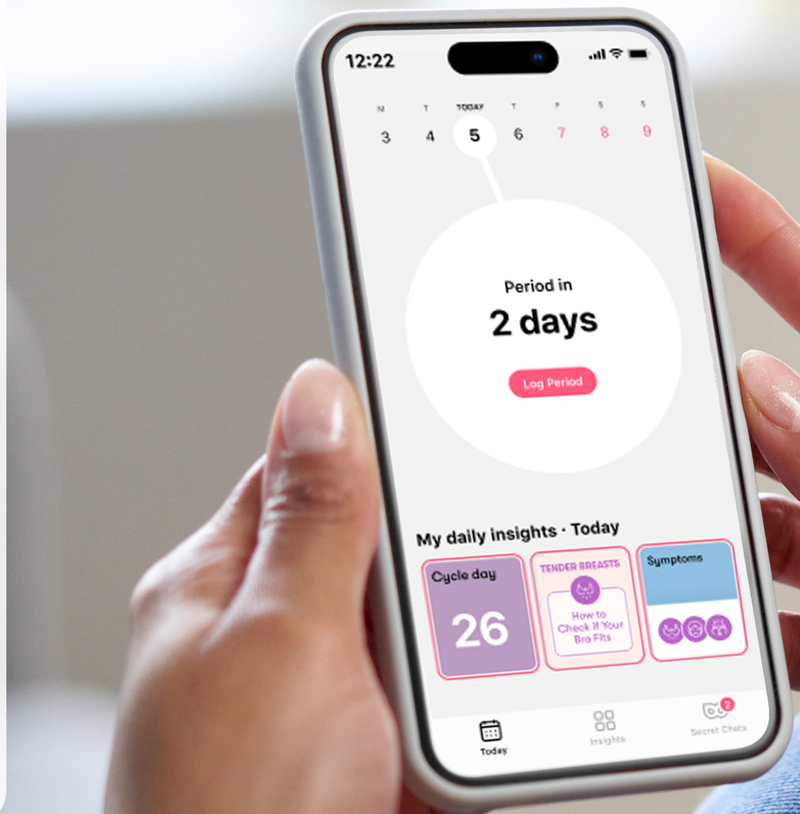
* 50 % Statistik: Cloudflare 2023 Connectivity Cloud-Umfrage

* 24 % Statistik: Cloudflare TechValidate-Umfrage 2023 unter Kunden des Cloudflare-Anwendungsdienstes.

* 59 % Statistik: Cloudflare TechValidate-Umfrage 2023 unter Kunden des Cloudflare-Anwendungsdienstes.

„Wir bei Flo sind der festen Überzeugung, dass jede Frau das Recht verdient, ihre Gesundheit ohne Bedenken im Auge behalten zu können..., und dank der Produktpalette von Cloudflare können wir die Daten unserer Nutzenden noch besser schützen.“

**—Roman Bugaev, Chief Technology Officer, Flo Health**

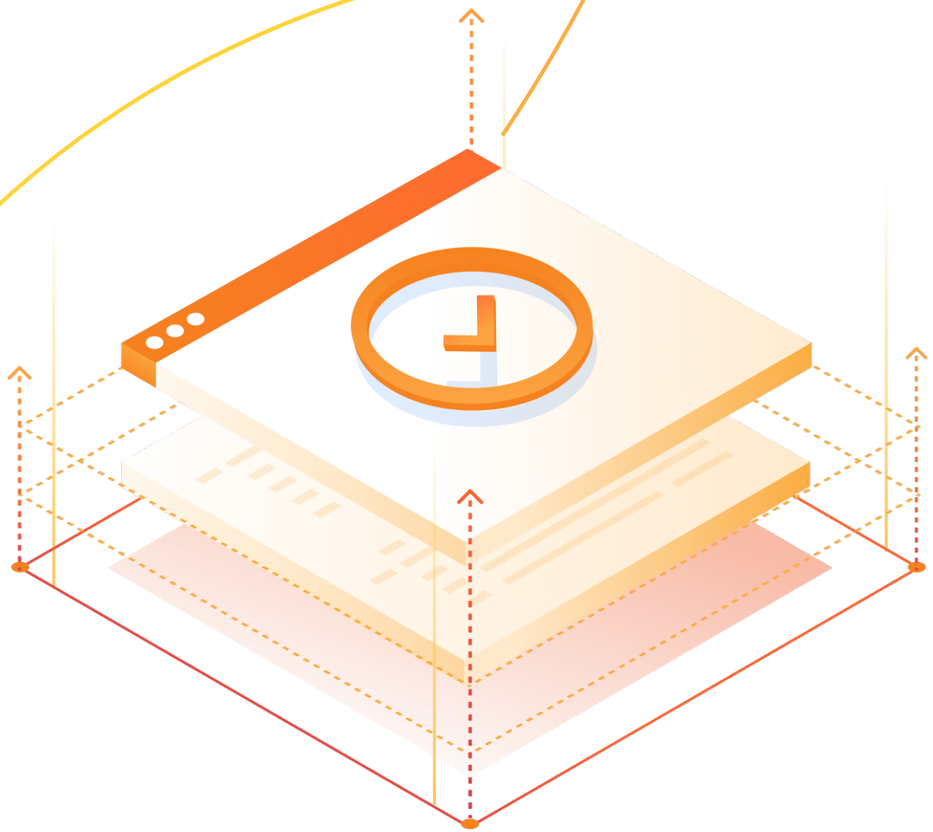


# Zusammenfassung

**Compliance-Verantwortliche brauchen einen neuen Ansatz, um die heutigen Herausforderungen bei der Einhaltung gesetzlicher Vorschriften zu meistern.**

**Veraltete Sicherheitslösungen zur Einhaltung von Vorschriften sind teuer, ineffizient und langsam. Der Einsatz einer vollständigen Compliance-Plattform, die unabhängig vom Speicherort der Daten ist – eine Connectivity Cloud – kann den Compliance-Verantwortlichen helfen, diese Herausforderungen zu überwinden und zu beseitigen.**

**Die Connectivity Cloud von Cloudflare unterstützt Unternehmen bei der Optimierung der Compliance mit zusammensetzbaren Kontrollen zur Durchsetzung von Richtlinien und Lokalisierung von Daten. Cloudflare ermöglicht es Compliance-Teams, die Einhaltung von Daten zu gewährleisten, ohne die Innovation oder Performance zu beeinträchtigen und gleichzeitig die Gesamtbetriebskosten (TCO) zu senken.**



# Mehr erfahren

## darüber, wie Sie die Connectivity Cloud nutzen können, um Ihre Anforderungen an die Datenkonformität zu erfüllen



Telefon: +49 89 2555 2276
E-Mail: enterprise@cloudflare.com
Web: www.cloudflare.com/de-de/

REV:BDES-5701.2024APR29