CLOUDFLARE

SOLUTION BRIEF

Boost data compliance with Cloudflare's connectivity cloud

A unified platform for managing data security and locality across complex environments

Challenge

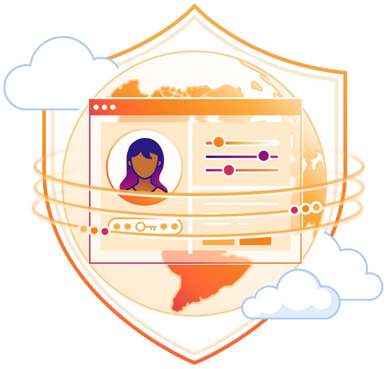
In data compliance, many organizations struggle to keep up with two flavors of increasing difficulty. The regulatory landscape is always changing, and hybrid networks and modern application infrastructures send and store data in more and more places.

Already, only 50% of organizations feel completely prepared to manage regulatory compliance. With AI adoption further complicating data protection, organizations need more efficient ways to implement compliance policies.

Solution

Protecting data, analyzing its usage, and managing where it lives needn't rely on a complex tech stack. Ideally, an organization should be able to do all of this from a single place, regardless of where data sits across apps and APIs, networks and workforces, and AI services.

Cloudflare's **connectivity cloud** can be that single point of control. It's a unified platform of connectivity, security, and developer services powered by a global cloud network. The platform helps organizations more efficiently comply with a wide range of regulations, frameworks, and standards via its:



Unified management interface

Built-in data privacy

Global service availability

Peerless threat intelligence

Cloudflare services help you maintain regulatory requirements across your hybrid environment

Compliance means different things to different organizations. Cloudflare products can help meet data localization requirements, strengthen compliance, build resilient infrastructure, and more — across applications, corporate networks, and hybrid- or multi-cloud environments.

Security services

Use Cloudflare to enforce many of the data protections required by many regulations and certifications like PCI DSS, HIPAA, and others, thanks to our unified platform of security services.

- **SASE & Workspace security:** Apply Zero Trust access policies to applications; monitor and manage how and where employees use data; and prevent phishing, shadow IT, network vulnerabilities, and other types of intrusion
- **Apps & APIs:** Block code injection and other vulnerabilities, discover and lock down APIs, secure other third-party code, and more
- **AI services:** Extend visibility, mitigate risk, and protect data across their entire AI attack surface — workforce AI apps, AI-enabled public applications, and the AI you build yourself

Logging and reporting services

Cloudflare's **Log Explorer** helps you store logs, detect security and performance issues, investigate root cause, and mitigate impact — all without adding complexity or cost.

Data locality services

Comply with data locality requirements in regulations like the GDPR and NIS2, thanks to Cloudflare's global scale and granular customization.

- **Policy enforcement:** Set rules about where data is cached and requests are inspected, without compromising on performance
- **Logs:** Cloudflare's Customer Metadata Boundary ensures that logs don't leave specific regions
- **Encryption:** Choose where encryption keys are stored, or store them on your own infrastructure, while the Cloudflare network for SSL/TLS

zendesk

"Because Cloudflare operates in so many countries, we can easily localize data on the global network, keeping it in the data center nearest the customer without making compromises in security or performance."

- ***Nan Guo***
  SVP of Engineering

A network and platform build to simplify data compliance

Our connectivity cloud's security, connectivity, and developer services live on a single global network spanning over 330 cities in more than 125 countries. The network offers a unified management interface, built-in privacy, global service availability, and peerless threat intelligence, all of which help organizations achieve a variety of data compliance goals:

1. Unified management interface

You can manage every Cloudflare service via a single UI or API, automate policy enforcement via our Terraform integration, and even pull in data from third-party logging services (e.g. SIEM).

This unified interface makes it more efficient for organizations to understand and manage risk, and serves a single point for auditing and reporting across the entire digital environment.

2. Built-in privacy

Cloudflare maintains security and privacy certifications like ISO 27001, 27018 and 27701, SOC 2 Type II, and PCI DSS.
In addition, all traffic and data transiting Cloudflare's network is encrypted by default, and much is quantum-resistant, meaning it's protected against decryption by future quantum computers.

These protections allow even the most regulated organizations to use Cloudflare.

3. Global service availability

Cloudflare services are built to run in any server in any data center in our network.

This distributed architecture ensures service continuity during infrastructure disruptions, cyber attacks, or regional outages. It also lets organization use Cloudflare no matter their data localization needs.

4. Peerless threat intelligence

Cloudflare protects around 20% of all web properties, and blocks an average of 234 billion cyber threats daily. We use AI to analyze these threats and automatically update policies across our security portfolio.

This visibility and automation helps organizations protect their data from the latest threats with minimal effort.

Benefits and outcomes

When organizations use Cloudflare's connectivity cloud to secure their digital environment and enforce data locality, and meet other compliance needs, they achieve outcomes like:

Easier compliance

Cloudflare's unified management and customizable data locality helps boost security team efficiency by **35%**

Reduced risk

Cloudflare's threat intelligence and unified visibility help reduce breach risk by **24%**

Flexibility and innovation

Cloudflare helps organizations use the technology and cloud services of their choice while remaining compliant

Learn more

Learn more about Cloudflare's connectivity cloud

See how the European e-health company Doctolib uses Cloudflare to meet compliance requirements