CLOUDFLARE

EBOOK

Simplifying data compliance during digital transformation

Three capabilities that make it easier to govern and protect your data

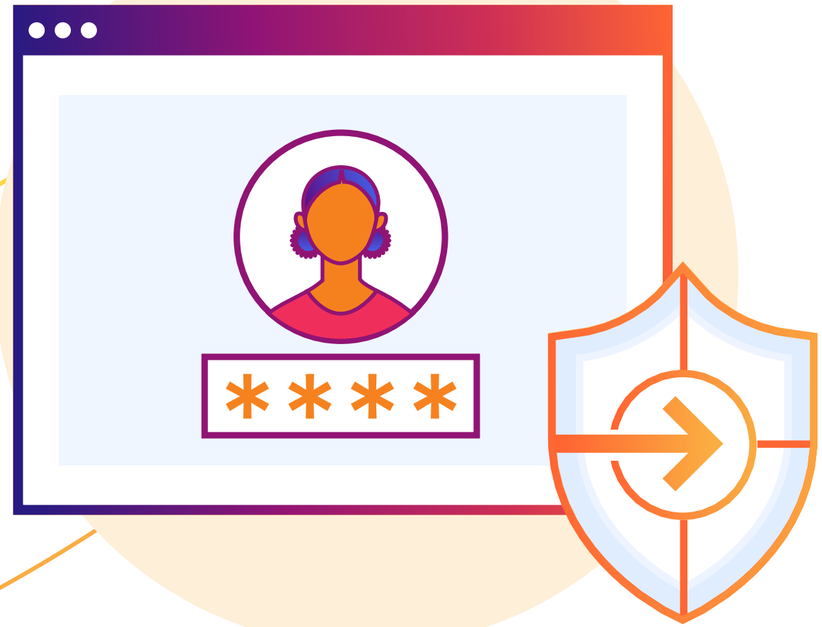
Table of contents

Introduction

Data compliance is a broad practice area, and projects may stem from a variety of motivations. Sometimes, new product lines or digital goals demand new forms of data governance. In other cases, the organization pursues a new certification in order to attract more demanding customers. The organization may also expand into new regions with new data privacy regulations. And of course those regulations can change quickly.

Unfortunately, data compliance obstacles stem from a variety of places, too. Cloud migration and multi-cloud adoption disperse data across more places. Hybrid work lets employees access data from more locations and devices. Modern web applications rely more on hard-to-track APIs, third-party code, and AI services. Small wonder that, in a recent survey of IT leaders, IDC found that **50%** of organizations only felt "somewhat prepared" to deal with regulatory compliance management.

Tracking and securing data will never be easy, and finding resources for compliance will always be a struggle. **But several technological capabilities can simplify a wide range of compliance tasks to some degree.** Read on to learn about those capabilities, or jump ahead to see how Cloudflare can help you attain them.



Digital challenges that slow down common data compliance goals.

Most organizations are constantly trying to stay abreast of the latest digital business trends. Unfortunately, most of these trends complicate data compliance. Common examples from the past few years include:

Changing regulations: US-EU data transfer frameworks have a history of sudden change. In the Asia-Pacific region, India, Indonesia, Japan, Singapore, South Korea, and others have introduced or significantly amended data privacy regulations. New regulations like DORA often impose resiliency requirements. Such changes make it hard for organizations to remain compliant globally.

Surging artificial intelligence adoption: The jury is still out on how well generative AI tools and AI agents protect data, and where on Earth they process and store it. In addition, widespread excitement around AI may make employees use it without permission, and keep security teams out of fast-moving AI adoption projects.

Complex app architectures: Many modern applications now rely on APIs, third-party code, and multi-cloud environments, each of which grows the organization's attack surface.

Hybrid workforces: Every new working location and employee device also represents a new attack surface, and thus a new compliance risk to manage.

Complex security and IT stacks: All of this change and new technology makes organizations grow their security stack. Cruelly, too many tools to manage can actually make an organization less secure and thus less compliant.

Several technological capabilities help organizations manage all of this change and stay on top of data compliance: **shadow API and IT detection, effective data localization, and security consolidation.** Read on to learn more about each one and see how a large enterprise is implementing it.

CAPABILITY 1

Shadow IT and API detection

Table of contents

Unknown third party software in your web application or workforce is one of the thorniest data governance obstacles. Compliance standards like PCI DSS call for tracking and monitoring of data access. Yet hybrid work, microservice-based app architectures, and AI adoption make 'shadow IT' harder to detect. **Organizations can mitigate these issues with the ability to detect shadow IT across their digital environment.**

Ways to strengthen shadow IT detection:

1. **Automated API discovery:** Find a way to scan your web applications for unknown API endpoints and their schemas. The latter is an especially important consideration, since a known API may still be vulnerable to data exfiltration. Some form of machine-learning powered automation will likely be necessary for this scanning, since manual scans can leave vulnerabilities open for too long. An API gateway is a good service to consider, since it can also close any vulnerabilities it discovers.

2. **Customer-facing AI controls:** Developers may also add unknown or unvetted AI services to an organization's web app. API discovery may uncover many of them But if the organization is building its own LLM, or incorporating a model more directly into the app's infrastructure, some web application firewalls will be able to surface the model's activity.

2. **Monitor employee Internet usage:** Employees access much shadow IT — particularly shadow AI tools — over the Internet rather than installing it on their corporate device. Security teams may use network firewall rules to block known risky sites altogether. But this won't work as well with remote workers, freelancers, or in-office employees using shadow AI the security team isn't aware of. Instead, use a service like a secure web gateway to monitor a wider range of Internet browsing and understand employee IT usage — as well as enforcing data loss prevention rules on that browsing.

Potential misstep to consider: Strict blocking of many risky applications is sometimes necessary. But remember that most employees using shadow IT are simply trying to be more productive, and may thus find creative workarounds you aren't aware of. Instead, consider security services that let you enforce more nuanced policies — like preventing copy/paste, or isolating risky sites on remote browsers to prevent malware infections.

Success story: How Indeed manages shadow AI

Organization:

Indeed, a leading job site with over 350 million customers and 15,000 employees across North America, Europe, and the Asia-Pacific region.

Challenge:

As an international job site, Indeed has a great deal of sensitive customer data to protect. Unfortunately, its existing perimeter-based security architecture gave employees excessive access to that data. In addition, the company didn't have a way to detect what AI tools employees used or monitor data those tools ingested.

Solution:

Indeed adopted Cloudflare SASE services to implement the beginnings of a Zero Trust security framework. The company uses Cloudflare's Secure Web Gateway to detect and block unsanctioned AI tools, and is rolling out more granular data loss prevention capabilities. In addition, the company uses Cloudflare's Zero Trust Network Access service to enforce least-privilege access policies for corporate applications. In addition to strengthening security, this switch has reduced outages which plagued the company's VPN.

indeed

“

Despite its many legitimate uses, AI presents major security and privacy concerns. Cloudflare helps us find what shadow AI risks exist and block unsanctioned AI apps and chatbots.”

Matthew Ortiz
Senior Manager,
Information Security

Learn more about Indeed's experience

Table of contents

Enforce data locality without app performance or availability tradeoffs

Data privacy and data sovereignty regulations like the GDPR limit where web applications can store and process customer data. This includes inspecting web requests and serving/caching web content containing such data. However, many modern applications depend heavily on the ability to do this processing and serving in a globally distributed way — in part because it reduces latency for distant customers, and also because global scale can help absorb volumetric attacks and legitimate traffic surges. **Finding a way around this tradeoff helps maintain compliance organizations remain compliant without hurting the customer experience.**

Ways to avoid these tradeoffs:

1. **Use a network that disaggregates security and app delivery services from physical locations.** Many such services are designed around specialized data centers in specific locations — e.g. large DDoS 'scrubbing centers.' Instead, use a network whose services are built to run anywhere in the network, and which thus lets organizations control which regions different services operate in.

2. **Use network and security providers with strong data privacy policies.** Organizations need to be sure their vendors will maintain data privacy under extraordinary circumstances. Ideally, the vendor should minimize risk by process and store as little customer data as possible. But organizations should also talk with potential vendors to understand how they respond to law enforcement requests for user requests, encryption keys, and more.

Potential misstep to consider:
To avoid performance and data locality tradeoffs, some organizations consider using different regional security and content delivery services to process requests. However, running too many redundant security services can increase management burdens and slow down incident response. Also, region-specific providers may not be able to handle large traffic volumes or volumetric attacks.

Success story: How Doctolib localizes data without tradeoffs

Organization:

Doctolib, an e-health platform serving over 390,000 healthcare providers and 90 million patients across France, Germany, and Italy.

Challenge:

Doctolib faced a difficult choice between web application performance and data compliance. The patient data they processed was subject to the GDPR's data locality requirements. However, usage of their web app was growing rapidly, including frequent traffic spikes as high as 10x. Doctolib worried European-based app delivery providers couldn't handle the load.

Solution:

Doctolib uses Cloudflare's Data Localisation Suite to limit security functionality like traffic decryption and inspection to data centers in the EU. DDoS prevention still happens on a global scale, helping ensure Doctolib's app availability. And because of Cloudflare's large network presence in Europe, even geo-limited functions like content caching and policy enforcement have more than enough network capacity to handle large traffic spikes.

Doctolib

"The Data Localisation Suite is invaluable for us because it allows us to use Cloudflare while remaining compliant. And no one else in Europe has Cloudflare's capabilities and ability to handle the massive amount of traffic we have."

Cédric Voisin
CISO

Learn more about Doctolib's experience

CAPABILITY 3

Ongoing security consolidation

Table of contents

Having data spread across too many applications and clouds makes compliance harder, but so does using too many security services to monitor and protect that data. Unsecured attack surfaces take more effort to discover, and teams spend more time learning how to use those different services. Logging and auditing takes more time, too. Many large enterprises won't want the mythical 'all-in-one' security platform vendors are fond of suggesting. **But most benefit from some degree of security service consolidation.**

Ways to pursue security consolidation:

1. **Make a consolidation tracker:** In larger enterprises, it can be easy for legacy security services to fly under the radar. Keeping a record of your services and when you last evaluated them is a simple but often overlooked way to surface the highest priorities. This also helps you treat consolidation as an ongoing process — an important mindset in organizations whose security stacks are always growing based on new business and compliance demands.

2. **Prioritize more mature areas of the business:** New customer-facing technologies or web applications tend to attract novel threats, and thus may have a legitimate need for separate security services. More mature applications are a better candidate for consolidation. In those cases, it's often easier to tell what is really necessary.

2. **Security automation:** When considering which providers to consolidate onto, don't just think about the threats they block. Consider also their ability to simplify your security and compliance operations via automation and more streamlined policy updates and maintenance.

Potential misstep to consider: Some security providers portray themselves as being strong platforms for consolidation, but actually run different services on different infrastructure around the world. Among other issues, this architectural model can complicate data locality by limiting your ability to run services in specific regions. Learn more about these architectural considerations here.

Success story: How Temple & Webster consolidated their security stack

Organization:

Temple & Webster, Australia's largest online marketplace for furniture and home goods.

Challenge:

The complexity of Temple & Webster's security stack made it difficult for them to perform seemingly simple tasks like changing web application firewall settings and updating employee access permissions. To reduce this complexity, and accelerate their ISO/IEC 27001 compliance, the company wanted to centralize their security on a single platform.

Solution:

Temple & Webster consolidated much of their Layer 7 and workforce security services on Cloudflare. Specific benefits included:

- **Replacing their VPN with Cloudflare's Zero Trust Network Access.** Since adopting Cloudflare's ZTNA, Temple & Webster's security and IT teams have spent 50% less time managing workforce application access. And getting more granular access control is an important step towards ISO/IEC 27001 certification
- **Adopting Cloudflare's WAF and Bot Management.** Both services give Temple & Webster's SecOps team easier access to more detailed information about unwanted web traffic — an important aspect of protecting customer payment data.

TEMPLE & WEBSTER

"We are on the path to compliance and, because Cloudflare Zero Trust has been so easy to implement and administer, we will achieve certification much earlier than we expected."

Mike Henriques
CIO

Learn more about Temple & Webster's experience

Cloudflare's compliance services streamlines and accelerates data compliance

Cloudflare's **connectivity cloud** can be a single point of control for data compliance. It's a unified platform of connectivity, security, and developer services powered by a global cloud network. Many of those services help organizations more easily comply with a wide range of regulations, frameworks, and standards:

Security

Enforce many of the data protections required by many regulations and certifications like PCI DSS, HIPAA, and others, with our:

- SASE and Workspace security services
- Web application and API security
- AI security

Learn more

Data locality

Comply with data locality requirements in regulations like the GDPR and NIS2. Cloudflare lets you limit a wide degree of functionality to the regions of your choice:

- Policy enforcement (e.g. caching, traffic inspection,
- Log storage
- Encryption key storage

Learn more

Logging and reporting

Store logs, detect security and performance issues, investigate root cause, and mitigate impact — all without adding complexity or cost.

- One-click ingestion and storage
- Unified visibility across all Cloudflare services

Learn more

Cloudflare simplifies and accelerates data compliance efforts

Organizations that use Cloudflare to meet data compliance needs achieve outcomes like:

35%
boost in security team efficiency

24%
reduction in breach risk

20%
license fee savings from service consolidation

These outcomes are possible because of Cloudflare's:

- **Unified management interface:** Manage every Cloudflare service via a single UI or API, and even pull in data from third-party logging services (e.g. SIEM). This makes it easier to manage risk and run audits and reporting
- **Global service availability with customizable data locality:** Cloudflare services are built to run on any server in any data center in our network, or can be limited to specific data centers and regions. This helps organizations use Cloudflare no matter their data localization needs.
- **Built-in privacy:** Cloudflare maintains security and privacy certifications like ISO 27001, 27018 and 27701, SOC 2 Type II, and PCI DSS. In addition, traffic and data transiting Cloudflare's network is encrypted by default, and much is protected against decryption by future quantum computers. These protections allow the most regulated organizations to use Cloudflare.
- **Peerless threat intelligence:** Cloudflare protects around 20% of all web properties, and uses AI to analyze all threats and automatically update policies across our security portfolio. This helps organizations protect their data with less effort.

Learn more about Cloudflare's data compliance services

Read solution brief

Talk with a member of our team

Schedule meeting