CLOUDFLARE

SOLUTION BRIEF

Cloudflare One for Data Protection

Better network architecture for more effective, more productive, and more agile data protection.

Unified protection for data everywhere

Modern data risks demand modern security

Data is exploding in volume, variety, and velocity today, and organizations face escalating risks posed by:

Sprawling cloud & SaaS environments
↳ including opaque emerging AI tools like ChatGPT
↳ leading to the exposure of precious source code

Cloudflare One's data protection suite is built to stay at the forefront of these distinctly modern risks.

By unifying point solutions onto a single platform and network, Cloudflare delivers data protection that is:

- **More effective** by simplifying connectivity and policy management
- **More productive** by ensuring fast, reliable, and consistent user experiences everywhere
- **More agile** by innovating rapidly to meet your evolving security requirements

One Security Services Edge (SSE) to protect data across web, SaaS, and private apps

Progressively adopt Cloudflare on your SSE journey to:

1. Secure access to data with Zero Trust
2. Stop threats like phishing and ransomware
3. Detect and lock down your most sensitive info

Navigate escalating data risks...

Sprawling SaaS footprint

82%

of breaches involved data stored in cloud environments.[1]

And of course, data breach costs continue to rise – up 15% over the past 3 years. [1]

New, diverse regulations

71%

of all countries have legislation to protect data and privacy.[2]

In the U.S., **11 states** now have comprehensive data protection laws – up from 3 in 2021.[3]

Digital transformation

89%

of CISOs say that moving fast with digital transformation initiatives introduces unforeseen risks in securing company data[4]

Use case #1: Secure developer code

Problem

Code can be exposed or targeted for theft across many developer tools, including in plain sight locations like public repositories.

Solution

Scan for and remediate misconfigured public repositories like GitHub that risk code leaks. Detect source code in up/downloads and apply controls.

→ GitHub

→ GitLab

→ Bitbucket

Use case #2: Data exposure visibility and risk management

→ OpenAI

→ Bard

→ GitHub Copilot

Problem

Data spans diverse SaaS and cloud environments, unsanctioned shadow IT, and emerging AI tools like ChatGPT, creating more risk for leaks.

Solution

Scan SaaS suites for misconfigurations with integrated DLP detections for sensitive data. Gain visibility across unsanctioned app usage, then allow, block, isolate, or apply Zero Trust controls to access them.

Use case #3: Comply with regulations

Problem

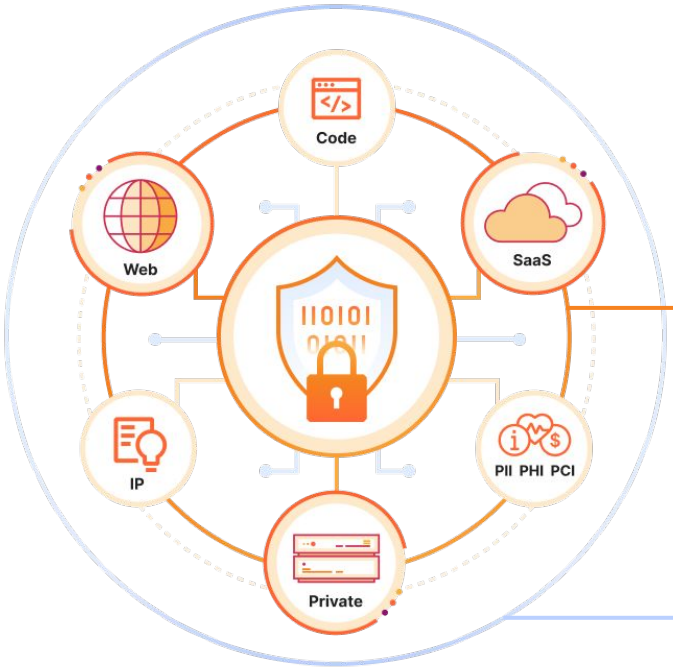
Stricter and more expansive legal requirements for companies to keep data safe and private, with rising fines for noncompliance.

Solution

Identify and apply controls to regulated data classes (PII, health, financial). Maintain detailed audit trails via logs and further SIEM analysis. Reduce attack surface with a comprehensive Zero Trust security posture.

- ✓ GDPR
- ✓ DPDP
- ✓ CCPA
- ✓ CPRA
- ✓ GLBA
- ✓ PCI DSS
- ✓ HIPAA
- ✓ ISO
- ✓ Many more!

How it works



One unified platform

Cloudflare converges visibility and controls across DLP, CASB, ZTNA, SWG, RBI, and email security services onto a single platform for simpler management.

One programmable network

One control plane with services built on our own developer platform to enforce controls for data in transit, in use, and at rest across all enforcement points — web, SaaS, or private app environments.

Example controls with composable services

Apply DLP for data in transit and secure access

- Scan for sensitive data in traffic and files, and configure block policies with DLP.
- Discover and manage shadow IT with CASB.
- Secure access to data in apps with ZTNA.
- Block personal tenants of SaaS apps to prevent data exfiltration.

Isolate apps to secure data in use

- Block copy/paste, up/download, printing, keyboard inputs – all without a device client.
- Clientless deployment is perfect for unmanaged devices, third party users, and AI tools like ChatGPT.
- Apply DLP policies within isolated apps.

Protect data at rest in SaaS apps

- Scan SaaS apps for suspicious activity, misconfigurations, and sensitive data.
- Take prescriptive steps to remediate risks via SWG policies.

Integrate to streamline compliance and controls

- Logpush to your preferred SIEM for correlation and audit.
- Integrate with 18 of the most popular SaaS suites for API-based CASB scans.
- Sync continuously with Microsoft Information Protection (MIP) labels for your DLP policies.

Better data protection with Cloudflare

More effective
by reducing complexity

Simplify connectivity with many flexible options to send traffic to Cloudflare for enforcement.

Use API-based scans for SaaS suites or clientless modes for ZTNA and RBI to secure app access. To forward proxy traffic, use one device client or wide area network on-ramps across security services.

More productive
by improving user experiences

Our network is everywhere, ensuring controls are enforced with single-pass inspection close to end users and data wherever they are.

Reliable and unintrusive, end-user experiences mean enforcing data controls never disrupts work. Proven faster than SSE peers.

More agile
by innovating with velocity

Our programmable network architecture enables us to build capabilities quickly, so you can adapt to new risks with agility.

We rapidly adopt adopt new security standards and protocols (like IPv6-only connections or HTTP/3 encryption) so data protection remains up-to-date.

What customers are saying

"Today, Cloudflare One helps prevent our users from sharing sensitive data and code with tools like ChatGPT and Bard, enabling us to take advantage of AI safely... Going forward, we are excited for Cloudflare's continued innovations to protect data, and in particular, their vision and roadmap for services like DLP and CASB."

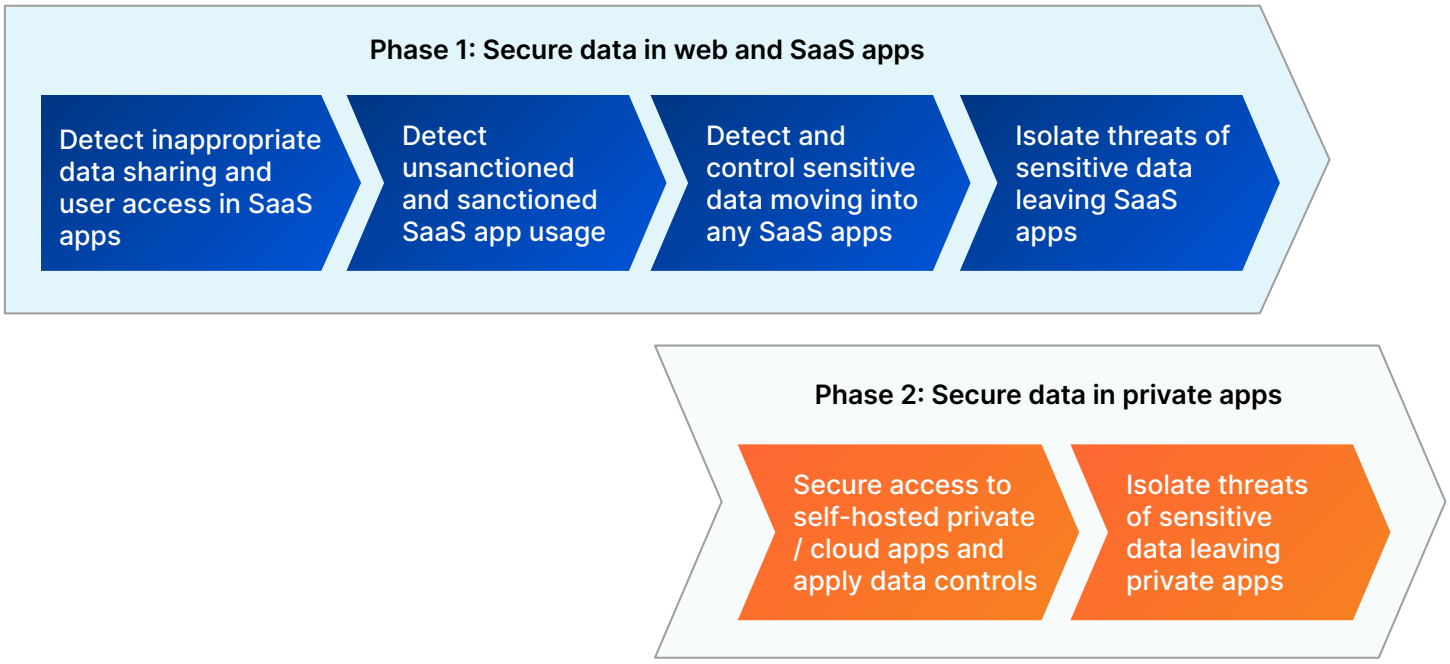
Tanner Randolph
Chief Information Security Officer (CISO)

Applied Systems
Read the case study

Other use cases

- **Fortune 500 natural gas company** to protect contractor access to data
- **Major US job site** to secure code and personal information
- **Regional US airline** to mitigate risks of exposing customer data
- **Australian healthcare company** to protect regulated medical data
- **US medical devices manufacturer** to streamline HIPAA compliance

Common adoption paths



Getting started

LEARN...

about escalating data risks in this infographic

ENGAGE...

with how the platform works in this demo

PROVE...

value by requesting a consultative workshop

1. Cost of a Data Breach Report 2023, IBM
2. United Nations Conference on Trade & Development
3. International Association of Privacy Professionals (IAPP)
4. 2023 "State of the CISO" report