Integrated DLP & CASB

Cloudflare One improves data visibility and reduces risk of exfiltration as data moves across all web, SaaS, and self-hosted/private apps.

Protect data everywhere

~81% of breaches now involve data stored in cloud environments.

Today, organizations are processing more data than ever. Customers entrust businesses with their personal information. Modern knowledge workers need to leverage and share data to across cloud and SaaS environments to do their jobs. And code is now a company's crowned jewel, growing rapidly in volume everyday. Sensitive data now essentially lives everywhere.

Integrated Data Loss Prevention (DLP)
+ Multimode Cloud Access Security Broker (CASB)

Built into one composable SSE platform, Cloudflare DLP and CASB easily extends visibility and unifies data protection controls across all apps, users, and devices. Deployment simplicity and flexibility for administrators, ensures that policies are functional, not shelfware.

75% Reduced costs (or less) associated with using multiple point solutions [1]

69% Minimized time spent on low value tasks (i.e. setup & configuration of threat defense policies [1]

20% Decreased likelihood and related costs of a data breach [2]

Embrace SaaS apps and the cloud securely

Avoid regulatory fines

Mitigate financial and reputational damages caused by data compliance violations with more streamlined policy enforcement for regulated data.

Simplify SaaS security

Empower your business to safely and confidently adopt new SaaS apps. Eliminate blind spots with continuous detection and control over SaaS risks.

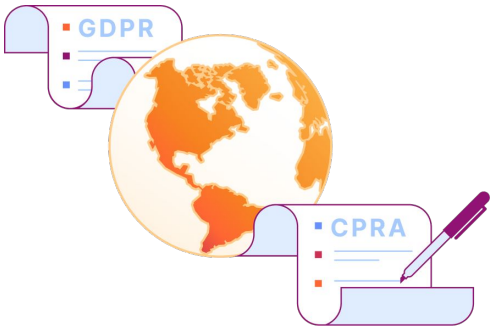
Scale at your own pace

Layer on data security without disrupting day-to-day operations. Configuration is simple and end user experiences are seamless.

Top use cases for DLP & CASB

Simplify regulatory compliance

Reduce the risk of compliance violations caused by data breach with a comprehensive Zero Trust security posture. DLP identifies and apply controls to regulated data classes (PII, health, financial). Additionally, maintain detailed data audit trails via logs and further SIEM analysis for ease compliance efforts.

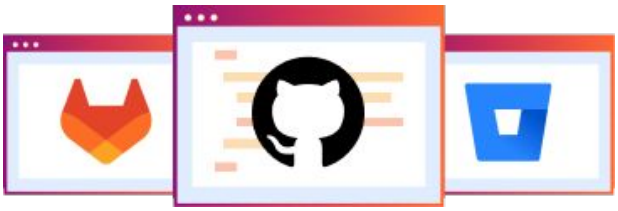


Increase visibility of data and misconfiguration risks

You can't protect what you don't know. Cloudflare CASB scans SaaS suites for misconfigurations and data threats with integrated DLP detections for sensitive data. Quickly gain visibility across unsanctioned app usage, such as emerging AI tools like ChatGPT and Bard. Then reduce risks with allow, block, isolate, or apply Zero Trust controls to access them.

Safeguard valuable IP and developer code

CASB detects and remediates misconfigured public repositories like GitHub that risk code leaks. For source code in transit, apply granular DLP controls to block users from up/downloading to any apps or device.



Getting started with unified data protection

Be more proactive with your data protection with a Zero Trust approach. Determine how corporate users are using SaaS, web, & private apps and granularly identify which ones they are using. Then accordingly, apply data controls and identity/device-driven policies to shrink your attack surface.

Gain visibility over data movement

- Detect inappropriate sensitive data sharing in SaaS apps
- Detect unsanctioned and sanctioned SaaS apps
- Integrate logs with SIEM providers for auditing*

Reduce risk of data exfiltration

- Apply DLP controls to what/where data moves into any app
- Isolate threats of data leaving SaaS and private apps*
- Secure access to SaaS and self-hosted private/cloud apps*

**using ZTNA, SWG, and/or RBI capabilities in the SSE & SASE platform*

How DLP Works

The migration to the cloud has made tracking and controlling sensitive information more difficult than ever. Employees are using an ever-growing list of tools to manipulate a vast amount of data. Meanwhile, IT and security managers struggle to identify who should have access to sensitive data, how that data is stored, and where that data is allowed to go.

Data Loss Prevention enables you to protect your data based on its characteristics, such as keywords or patterns. As traffic moves into and out of corporate infrastructure, the traffic is inspected for indicators of sensitive data. If the indicators are found, the traffic is allowed or blocked based on the customers' rules.

Easy, quick controls over regulated data classes

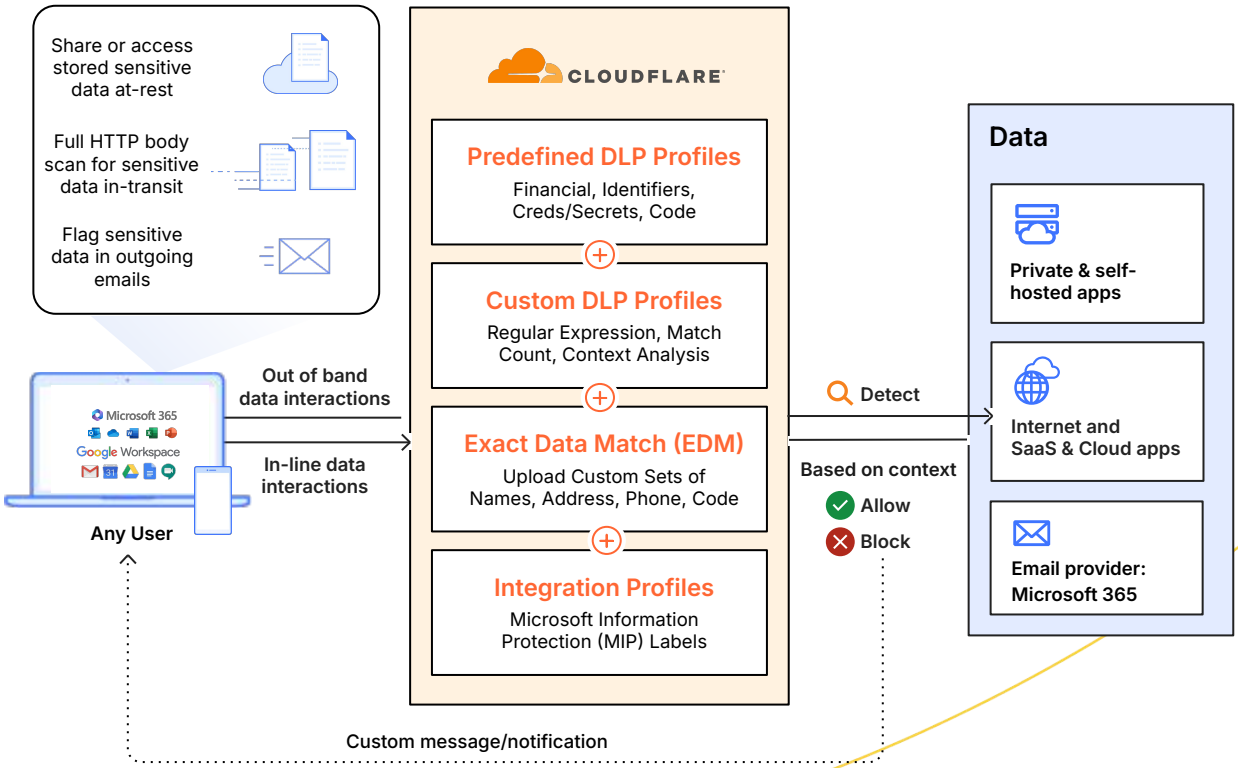
Compliance requirements are getting stricter and more expansive. Quickly enable predefined DLP profiles to parse employee network traffic and block sharing of regulated data, such as PII, PHI, and other financial information (e.g., banking / credit card numbers).

Advanced customization for constant changing data needs

The definition of sensitive data can vary drastically across organizations depending on industry and operating locations. Apply granular controls to other data types, such as secrets, code, credentials, and IP, by creating custom DLP profiles with context analysis and Exact Data Match.

Seamless integration with existing data classification tools

Maintaining a thorough inventory of sensitive data is a massive lift for security teams and therefore require data classification tools like MIP. Increase agility, not complexity with our integrations that automatically retrieve sensitivity labels and populate into a DLP profile.



How CASB Works

Natively built SSE delivers inline CASB for consistent data control across all apps and devices

Each SaaS app requires different security considerations, and operate outside the safeguards of the traditional perimeter. As organizations adopt dozens SaaS apps, it becomes increasingly challenging to maintain consistent security, visibility, and performance.

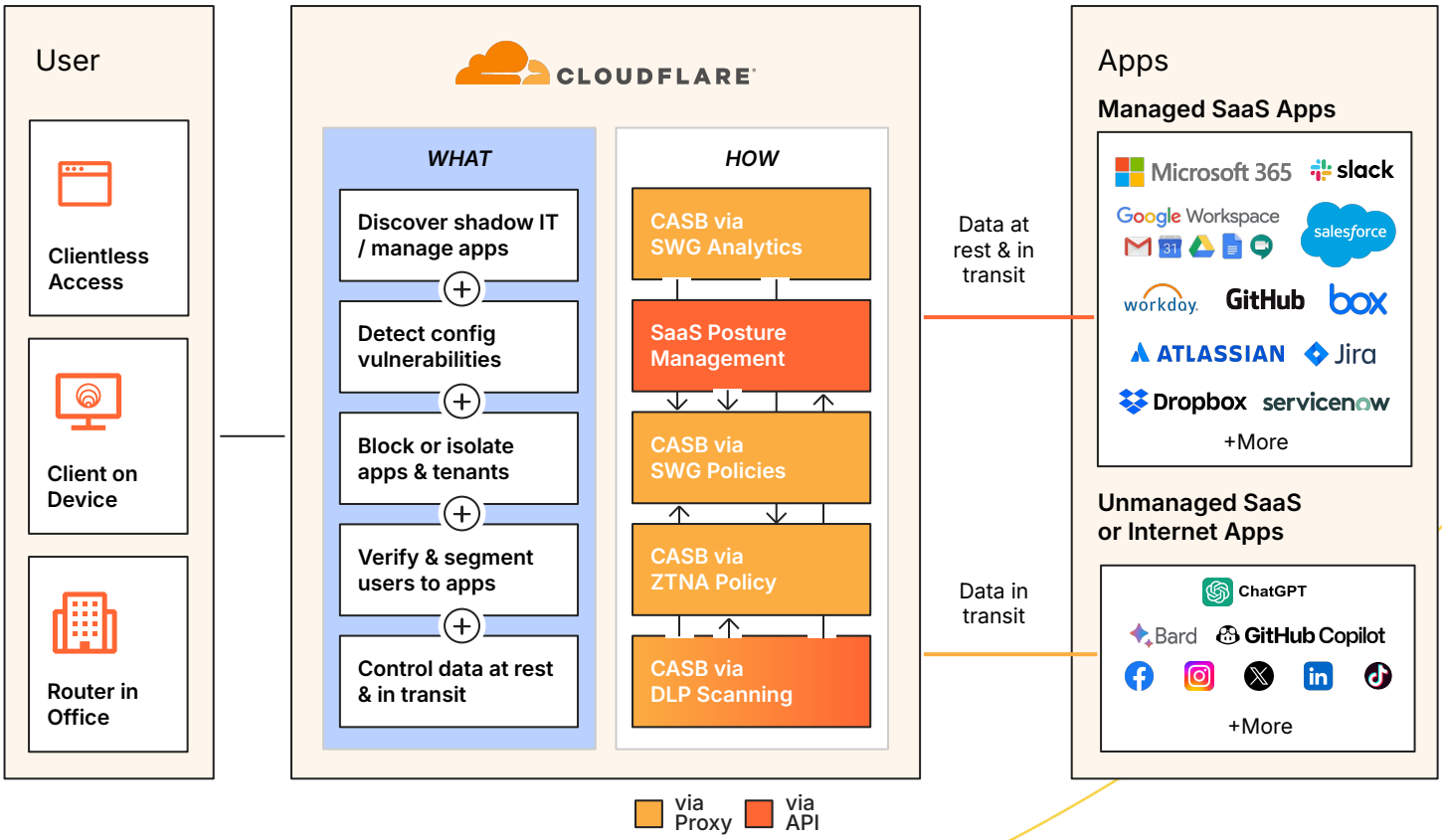
To protect data in transit, our inline CASB places ZTNA, SWG, and RBI controls in front of your apps.

- Log every HTTP request to reveal Shadow IT
- Block/isolate threats and risky data sharing
- Secure access to any SaaS app

Easy API CASB integrations provides quick risk visibility across your managed SaaS apps

Connect to popular SaaS apps (Google Workspace, Microsoft 365, etc.) in just a few minutes with quick API read-only integrations.

Maintain strong SaaS security posture and empower your IT and security teams with visibility into permissions, misconfigurations, improper access, and control issues that could leave their data and employees at risk. Then, quickly remediate CASB surfaced threats with easy click SWG policies and integrated DLP scanning.



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."

— **Applied Systems**, Tanner Randolph, CISO

APPLIED

Cloudflare replaced point solutions Zscaler ZIA and Cisco AnyConnect VPN.

More broadly helped Applied Systems consolidate security across employees, applications, and networks.

Read the case study

What analysts are saying

FORRESTER

Cloudflare named a Strong Performer in The Forrester Wave™: Zero Trust Platforms, Q3 2023

Cloudflare cites continued disruptive momentum in SSE market demonstrated via analyst recognition, receiving the highest scores possible, 5.0/5.0, in the innovation, roadmap, pricing flexibility & transparency, and hybrid workforce enablement & protection criteria.

According to the report, *"Cloudflare's various network, DLP, and access control policies are managed from a single console, allowing customers to quickly deploy and protect against Internet-born threats."*

Read full report

Gartner®

Cloudflare is the only new vendor in the 2023 Gartner® Magic Quadrant™ for SSE

Cloudflare has been recognized in the 2023 Gartner® Magic Quadrant™ for Security Service Edge (SSE) report. We believe our recognition validates our commitment to continue advancing our Zero Trust platform to help secure hybrid work.

Read full report

Integrated DLP Capabilities

DLP Profiles	Define the data patterns you want to detect. • **Predefined DLP Profiles:** Financial information (e.g.. credit card numbers), national identifiers (PII), Health Information (PHI), credentials & secrets (e.g. GCP/AWS keys), and source code • **Custom Profiles**: Build custom detections to identify unique types of sensitive data (e.g. internal project names, unreleased product names)
Data classification	Integrate DLP with third-party data classification providers like Microsoft Information Protection (MIP) sensitivity labels. Retrieve classification information from provider, populate into Cloudflare DLP Profile, and enable policy to allow or block matching data.
Match count	Set custom match counts for number of times that any enabled entry in the profile can be detected before an action is triggered, such as blocking or logging.
Context analysis	Context analysis to restricts DLP detections based on proximity keywords (~1000 bytes distance).
Custom datasets	Parse web traffic and SaaS apps for specific data defined in a custom dataset. For sensitivity, can redact/hash data in logs. • **Exact Data Match:** Specify most important sets of PII like such as customer names, addresses, phone numbers, and credit card numbers. All data encrypted before reaching Cloudflare. • **Custom Wordlists:** Protect non-sensitive data, such as IP and SKU numbers.

Multimode CASB Capabilities

Risk Visibility and Compliance	
API-based scanning	Integrate a third-party SaaS apps to scan data-at rest for security findings like misconfigurations, unauthorized user activity, shadow IT, and data security issues that can occur after a user has successfully logged in. 18+ integrations available (e.g. Microsoft 365, Google Workspace).
Shadow IT discovery	Shadow IT visibility into the SaaS apps and private network origins your end users are visiting. Review discovered apps and adjust approval status—Approved, Unapproved, In Review, and Unreviewed. Set granular identity and device-driven policies* accordingly.
Audit logging	Comprehensive logging* for all requests, users, and devices. Use logpush* or API to integrate with existing third-party storage or SIEM tools for compliance auditing.
Data Security and Threat Prevention	
Zero Trust access*	Set least-privilege policies per app via ZTNA to limit user access to data
File sharing controls*	Allow or block file upload/downloads based on MIME type via HTTP SWG policies
App controls*	Allow or block traffic to specific apps or app types via HTTP SWG policies
Tenant controls*	Control traffic SaaS app tenants via SWG to prevent data loss
Browser controls*	Protect data-in-use in a browser by restricting download, upload, copy/paste, keyboard input, and printing actions within isolated web pages and applications via RBI. Prevent data leakage onto local devices, and control user inputs on suspicious websites.
DLP scanning*	Scan HTTP traffic via SWG for sensitive data through strings matching the keywords or RegEx specified in configure DLP profile. Enable DLP profiles in a CASB integration and discover if files stored in your SaaS apps contain sensitive data. Extend DLP to private apps via clientless RBI which inherits all HTTP based policies.

**using ZTNA, SWG, and/or RBI capabilities in the SSE & SASE platform*

Why Cloudflare?

One unified platform

Secure access
by verifying and segmenting any user to any resource

Threat defense
by covering all channels with network-powered AI/ML & threat intel

Data protection
by increasing visibility and control of data in transit, at rest and in use

One programmable network

More effective
by simplifying connectivity and policy management

More productive
by ensuring fast, reliable, and consistent UX everywhere

More agile
by innovating rapidly to meet your evolving security requirements

Ready to discuss your data protection needs?

Request Workshop

Not quite ready for a live conversation?

Keep learning more in our SASE reference architecture, or see how it works in an interactive tour of our Zero Trust platform.

1. 2023 survey: techvalidate.com/product-research/cloudflare/charts
2. IBM Cost of Breach Report: https://www.ibm.com/reports/data-breach