PRODUCT BRIEF

Cloud Access Security Broker

Comprehensive visibility and control over SaaS, AI, and cloud environments — protecting data without slowing down innovation.

SaaS security built for the AI era

Secure your SaaS, AI, and cloud environments without slowing down productivity. Detect misconfigurations, shadow IT, and data risks instantly across your hybrid workforce using Cloudflare CASB.

- **Automate compliance:** Instantly detect and fix security gaps — like unauthorized file sharing or weak MFA — across Microsoft 365, Google Workspace, and GitHub.
- **Stop Shadow AI/IT:** Discover unauthorized applications and block access to unapproved cloud storage or file-sharing sites.
- **Secure AI usage:** Gain visibility into AI tool adoption and enforce tenant restrictions on platforms like ChatGPT and Gemini to ensure corporate-only access.
- **Manage third-party risk:** Identify and revoke risky third-party integrations that have access to your corporate data.

Built on our global network, API-driven and inline protection from Cloudflare CASB ensures fast and cost-efficient security at scale.

Infrastructure provider

Identified SaaS vulnerabilities — like sensitive SharePoint files being widely shared — to help mitigate data loss.

Read case study

Insurance software provider

Secured Gen AI adoption by blocking sensitive data inputs to tools like ChatGPT without hindering workforce productivity.

Read case study

Telehealth provider

Secured sensitive patient data (PHI/HIPAA) and accelerated access for a rapidly growing remote workforce using DLP and CASB.

The Cloudflare difference

Instant, clientless deployment

Connect to SaaS and AI apps like Microsoft 365, GitHub, Slack, and ChatGPT in minutes via API. Immediately scan for historical risks, misconfigurations, and data exposure without installing clients.

Continuous SaaS and cloud data posture management

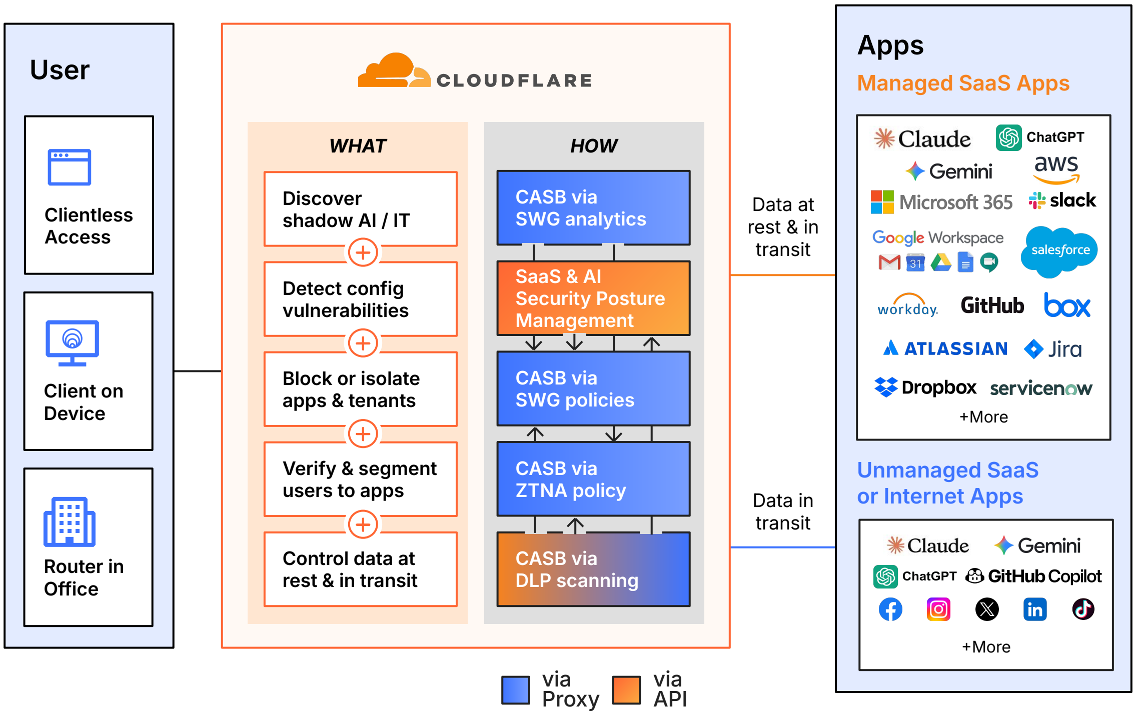
Identify security drifts and insecure settings across your SaaS and cloud storage. Detect and revert critical misconfigs—like public S3 buckets or open project permissions—before they lead to a breach.

Unified Shadow IT control

Stop hopping between consoles. Use CASB insights to detect unapproved apps, then instantly trigger Zero Trust policies to block or isolate that traffic via Cloudflare Gateway—managing everything from a single dashboard.

Want to go deeper on this product? Review our reference architecture or talk to an expert.

Comprehensive security for SaaS, AI, and shadow IT



User

Clientless Access

Client on Device

Router in Office

CLOUDFLARE

WHAT

Discover shadow AI / IT

Detect config vulnerabilities

Block or isolate apps & tenants

Verify & segment users to apps

Control data at rest & in transit

HOW

CASB via SWG analytics

SaaS & AI Security Posture Management

CASB via SWG policies

CASB via ZTNA policy

CASB via DLP scanning

Data at rest & in transit

Data in transit

Apps

Managed SaaS Apps

Claude, ChatGPT, Gemini, aws, Microsoft 365, slack, Google Workspace, salesforce, workday, GitHub, box, ATLASSIAN, Jira, Dropbox, servicenow

+More

Unmanaged SaaS or Internet Apps

Claude, Gemini, ChatGPT, GitHub Copilot

+More

🟦 via Proxy 🟧 via API

How it works

Cloudflare's multimode CASB helps deliver unified cloud security for SaaS apps. To secure data at rest, simple API integrations continuously scan your applications for vulnerabilities and potential risks.

Our Zero Trust access (ZTNA), gateway (SWG), and browser isolation (RBI) controls are seamlessly deployed as an inline CASB — combining easy configuration with robust security.

Out-of-band data protection and SaaS security posture (API-driven)	
SaaS Security Posture Management (SSPM)	Scan SaaS apps and cloud storage via API to detect misconfigurations and risky third-party integrations (e.g., public S3 buckets, unauthorized OAuth apps, or MFA violations).
SaaS data protection (DLP)	Detect sensitive files (PCI, PII, secrets) using data-at-rest scanning, and automatically remediate violations (e.g., remove publicly accessible files) to enforce compliance.
Inline data protection (Proxy-driven)	
Shadow AI and IT discovery	Instant visibility into unsanctioned app usage. Automatically categorize and block/isolate risky apps (e.g., unapproved PDF converters or AI tools) based on application confidence scores.
Inline DLP and OCR	Detect sensitive data in traffic using Exact Data Match (EDM) and advanced classifiers. Leverage Optical Character Recognition (OCR) to extend these protections to images, blocking data leakage.
GenAI prompt protection	Prevent sensitive data (source code, customer PII) from being pasted into public LLMs. Inspect HTTPS requests to tools like ChatGPT or Gemini to enforce safe AI usage.
Tenant control	Enforce corporate-only access for apps like Microsoft 365, Google Workspace, and Slack to prevent personal account logins on corporate devices.
Unified management	
Single client	No separate CASB client is required. The unified client handles ZTNA, SWG, and CASB with single-pass inspection.
User risk scoring	Detect compromised users by correlating CASB findings with behavioral anomalies to assign dynamic risk scores.
Logpush	Comprehensive logging captures all requests, users, and devices. Instantly export CASB logs to Splunk, Datadog, or S3 for SIEM analysis.