CLOUDFLARE

SOLUTION BRIEF

Protect your sensitive data

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

Unified protection for data everywhere

Data protection is not a new mandate, but the shift to hybrid cloud architectures alongside rapid AI adoption introduces new challenges:

- **93% of employees** admit to putting information into AI tools without approval [1]
- **79% of all countries** have data privacy legislations [2]

Cloudflare enforces consistent controls across your data's lifecycle:

- **Secure everywhere:** Enforce consistent controls across web, SaaS, email, and cloud traffic.
- **Block AI exfiltration:** Analyze GenAI prompts to block sensitive data and govern AI usage.
- **Govern data risks:** Discover and manage Shadow IT/AI, and scan SaaS/cloud apps with CASB.

"The rise of all these unauthorized AI tools makes us reconsider our security approach. We're looking into SASE now." - *Head of Infosec,* ***AllSaints***

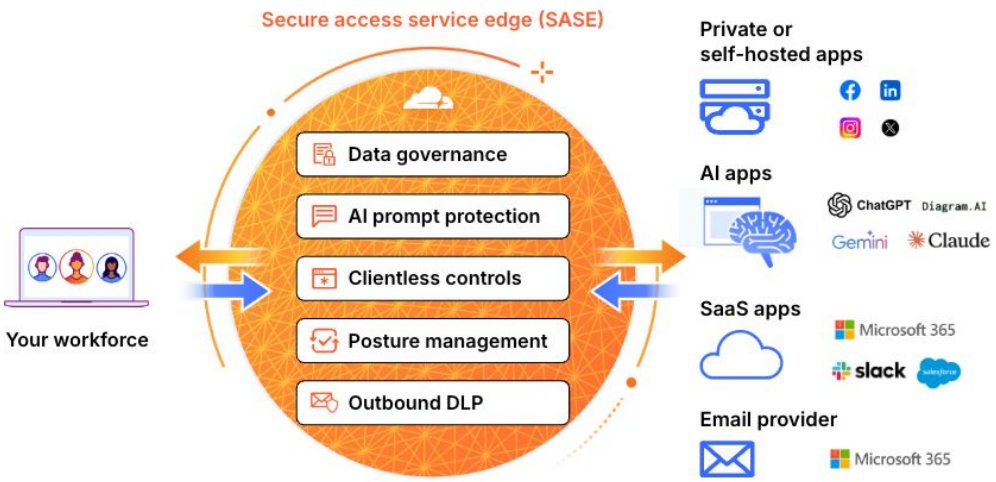
Why SASE over enterprise DLP?

Cloudflare's secure access service edge (SASE) platform is built to sit between your workforce and every application and data source. This makes SASE an ideal starting point for many to begin safely protecting data.

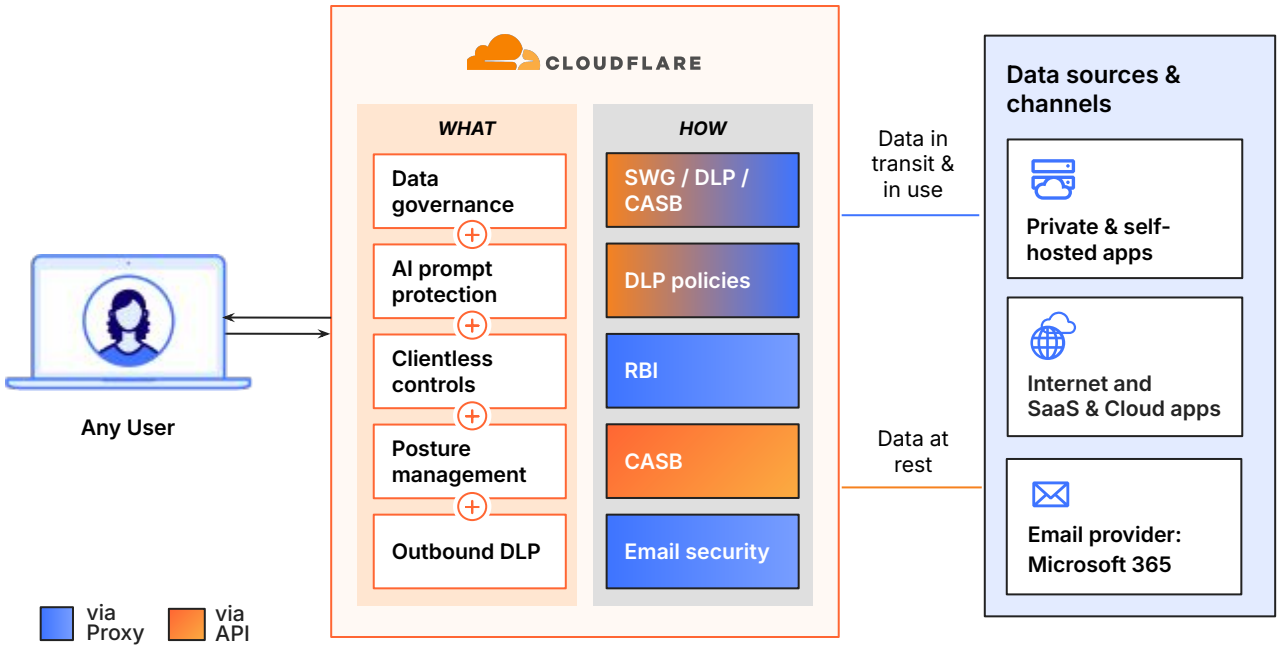
Whether employees are accessing data in SaaS apps, downloading sensitive files, or chatting with GenAI tools, Cloudflare's SASE platform enforces consistent security controls across all data interactions.

How it works

Cloudflare's SASE platform sits inline between your workforce and resources to unify data visibility and controls.



AI-powered data protection with Cloudflare's SASE platform
across web, SaaS, email, and cloud traffic



Real-time, inline data protection

- **Granular DLP:** Stop sensitive data exposure with context-aware detections for PII, source code, customer data, and more.
- **Outbound email DLP:** Automatically flag sensitive data in outgoing emails, preventing accidental data leaks.
- **Prompt protection:** Detect and block risky AI prompts and responses based on intent (e.g., jailbreak attempts, code abuse, PII requests).

Secure access and client controls

- **Secure app access:** Enforce zero trust network access (ZTNA) rules — such as granular DLP scanning for agentic AI connections — across all corporate applications.
- **Device posture checks:** Control access based on granular posture checks such as disk encryption and enabled endpoint DLP.
- **Clientless controls:** Apply browser-based data controls to safeguard third-party access and employee BYOD policies.

Shadow IT and posture risks

- **Shadow IT and AI discovery:** Discover and manage shadow IT/AI across your environment. Quantify risk with app confidence scores and data transfer metrics to quickly mitigate exposure.
- **Posture management:** Scan SaaS apps and cloud environments for posture risks. Take prescriptive steps to remediate security findings.
- **Tenant control:** Block personal tenants of SaaS apps to prevent data exfiltration.

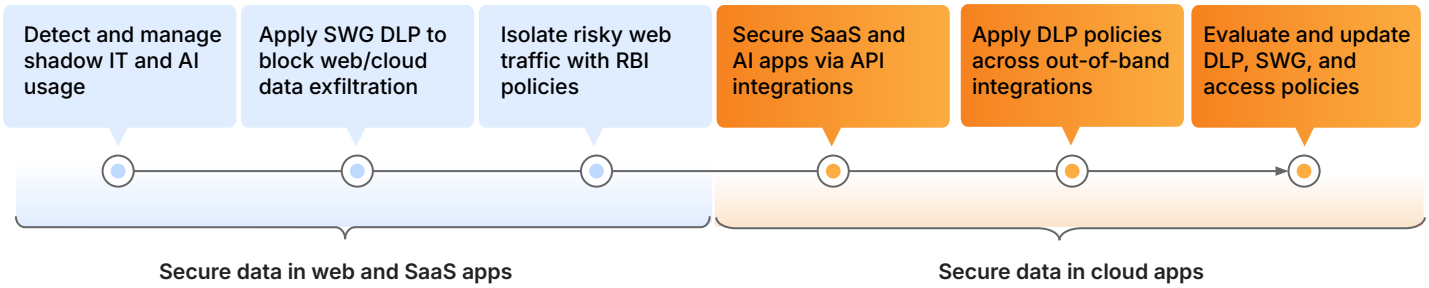
Integrations and reporting

- **CASB Integrations:** Seamlessly integrate with leading SaaS and AI platforms (including Microsoft 365, Google Workspace, and ChatGPT) for API-based CASB scans.
- **Microsoft MIP integration:** Sync continuously with Microsoft Information Protection (MIP) labels for consistent DLP policies.
- **Observability & forensics**: Securely log data to your preferred SIEM for audit, or analyze logs instantly via the dashboard or API.

Example data protection journey

Start with discovering shadow IT and AI usage for attack surface visibility. Configure foundational DLP policies on SWG to block high-risk data leakage from unmanaged cloud apps, and deploy RBI for unapproved web traffic.

Then, deploy CASB to secure sanctioned SaaS and AI apps by remediating misconfigurations and enforcing internal sharing policies. Refine and integrate granular DLP and access policies across the SWG, email, and CASB to achieve automated, unified prevention across all major data vectors.



Sample use cases to get started

- **Block real-time exfiltration of PII/PHI** across all unapproved communication and storage channels.
- **Protect source code and intellectual property (IP)** from insider theft and unauthorized distribution.
- **Enforce prompt protection policies** for GenAI apps to prevent sensitive data exposure and model contamination.
- **Prevent misconfigurations** and enforce granular access controls across all SaaS and AI apps.

Customer outcomes

EESTI RAUDTEE

Infrastructure provider
Read case study

Mitigate data loss and SaaS vulnerabilities

by identifying data leaks and misconfigurations.

APPLIED

Insurance technology
Read case study

Isolate public GenAI tools like ChatGPT

to block copy-paste of sensitive data.

Flo

Leading health app
Read case study

Protect patient data

and achieve compliance with email security and zero trust.

CREDIT SAISON INDIA

NBFC lender
Read case study

Protect PII and achieve compliance

to prevent unwanted data egress.

Ready to discuss your data protection needs?

Request a workshop

1. 2025 Manage Engine research: Source
2. 2025 United Nations Conference on Trade & Development: Source

 | 1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com