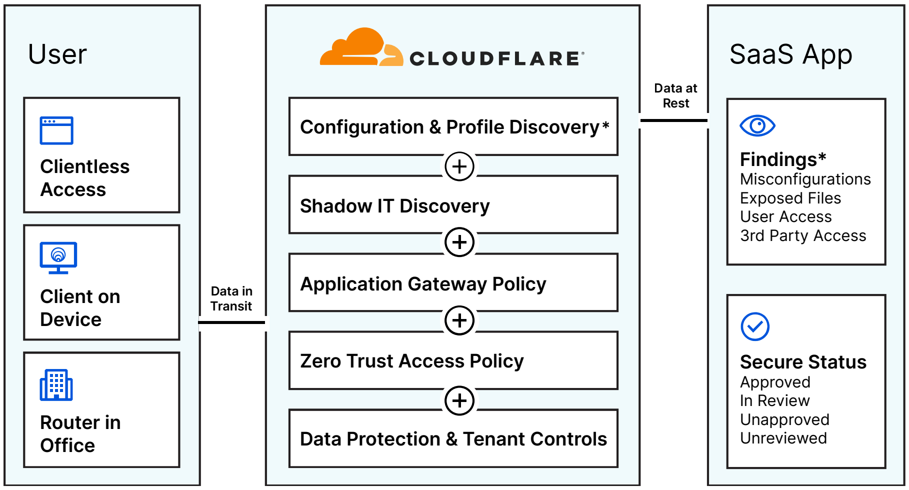
SOLUTION BRIEF

CLOUDFLARE

Zero Trust visibility and control of every SaaS application

SaaS applications empower your teams to do more than ever before, but the flexibility and freedom they afford your workforce also introduces security risks, visibility challenges, and access control hurdles for your organization.

Cloudflare gives you the tools you need to protect your data and workforce while still allowing your employees to use the tools that help them get the job done.



Mitigate risks and control Shadow IT

Without visibility into which applications your employees are using and how, you can't control how sensitive data is stored, shared, or exposed. Cloudflare helps you uncover misconfigurations in your SaaS application setup, risky file sharing behaviors, unauthorized users, and Shadow IT instances.* With greater threat intel, you can categorize and control all approved and unapproved applications within your organization, while logging every connection and request in one centralized location.

Apply Zero Trust access policy

SaaS applications are hosted outside of the corporate network, leaving your security teams with limited ability to control how users access those applications and move data in and out of them. Cloudflare layers Zero Trust security measures in front of your SaaS applications, authenticating legitimate users and preventing unauthorized users or risky devices from accessing your files and data.

Apply tenant and data protection controls

When employees access the wrong instance of applications, they can share and store your data in the wrong places — opening the door to potential data leaks and other security risks. Cloudflare helps you control the sharing and storage of your data, whether it is in transit over our network or in-use within our remote browser. Now, you can build and deploy Zero Trust browsing policies to protect the data that lives within any SaaS tenant, while keeping your employees from accessing the wrong applications or the wrong tenants of approved applications.

*Certain stated features are in Closed Beta for the announced API-driven CASB

Mitigate risks and control Shadow IT

Evaluate the applications your employees use

When your IT team can’t see the applications your employees are using, they can’t control what happens to the data within those applications. Cloudflare aggregates and automatically categorizes all HTTP requests in our activity log by application type. From there, you can set the status and track the usage of both approved and unapproved apps across your organization.

Log every connection and request

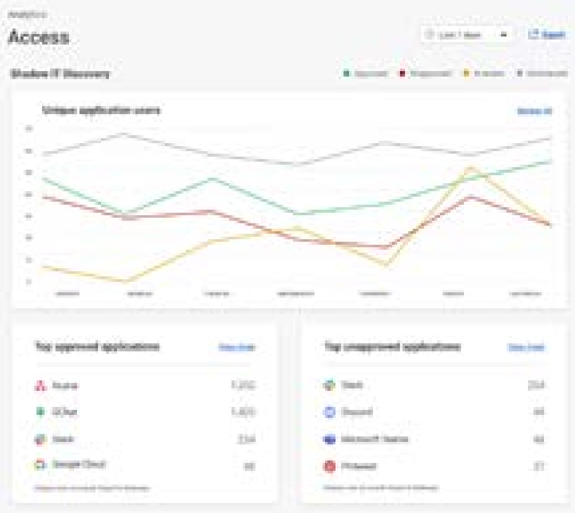
Cloudflare helps minimize the risks introduced to your organization when employees access unsanctioned applications or use unmanaged devices to access sensitive information. Every connection and request is logged in one central location, so you can see which applications are in use and what actions users are taking within them. Administrators also have the ability to block and allow requests to SaaS applications, preventing users from bypassing important security controls and gaining unauthorized access.

Continuously monitor SaaS applications for vulnerabilities*

To protect the sensitive data within your managed applications, your IT team needs expanded visibility into how those applications are set up and used by each employee. Through API integrations, Cloudflare scans your SaaS applications to detect misconfigurations, exposed files, and suspicious activities. By continously analyzing data at rest in the cloud, you can mitgate data exfiltration and be more compliant with security best practices.

Key Features

- Automatically track which applications have already been secured by Cloudflare
- Retain logs for up to 6 months in Cloudflare’s network
- Push logs to one or more of your cloud log storage and SIEM services
- Detect application misconfigurations within minutes*
- Continously monitor for exposed files and suspicious activity*



*Certain stated features are in Closed Beta for the announced API-driven CASB

Apply Zero Trust access policy to your SaaS applications

Provide secure SaaS access through Cloudflare’s identity proxy

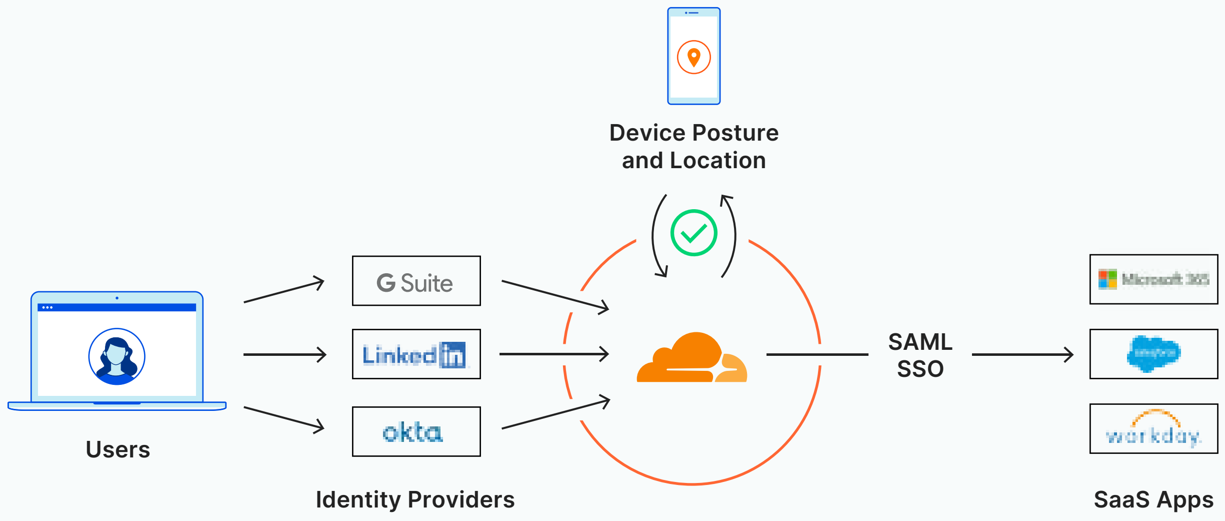
SaaS applications are hosted by third parties and often managed by business units, which means your IT team often has little say over how users access those applications. Cloudflare sits between your identity provider and your SaaS applications, enabling you to build and apply identity-aware, context-driven Zero Trust rules to the login process — all without disrupting the end-user experience.

Determine application permissions for user devices

Your IT department needs granular control over the way corporate-managed devices log in to SaaS applications. Cloudflare inserts Zero Trust rules into the single sign-on process for all applications that support SAML authentication. Users first authenticate with their identity provider; then, Cloudflare checks the request against device posture and location before authorizing access to any SaaS app -- with flexible session management for continuous verification. Co

Key Features

- Integrate multiple identity providers or multiple instances of the same provider
- Verify user identity with per-app rules (e.g. MFA requires hard key)
- Verify device posture with per-app rules (e.g. SWG policy enforced, EPP installed, mTLS certificate, disk encryption enabled) and location
- Cloudflare’s app launcher portal allows users to see and access all of their approved SaaS applications



Apply tenant and data protection controls to any SaaS application

Restrict access to non-corporate instances of applications

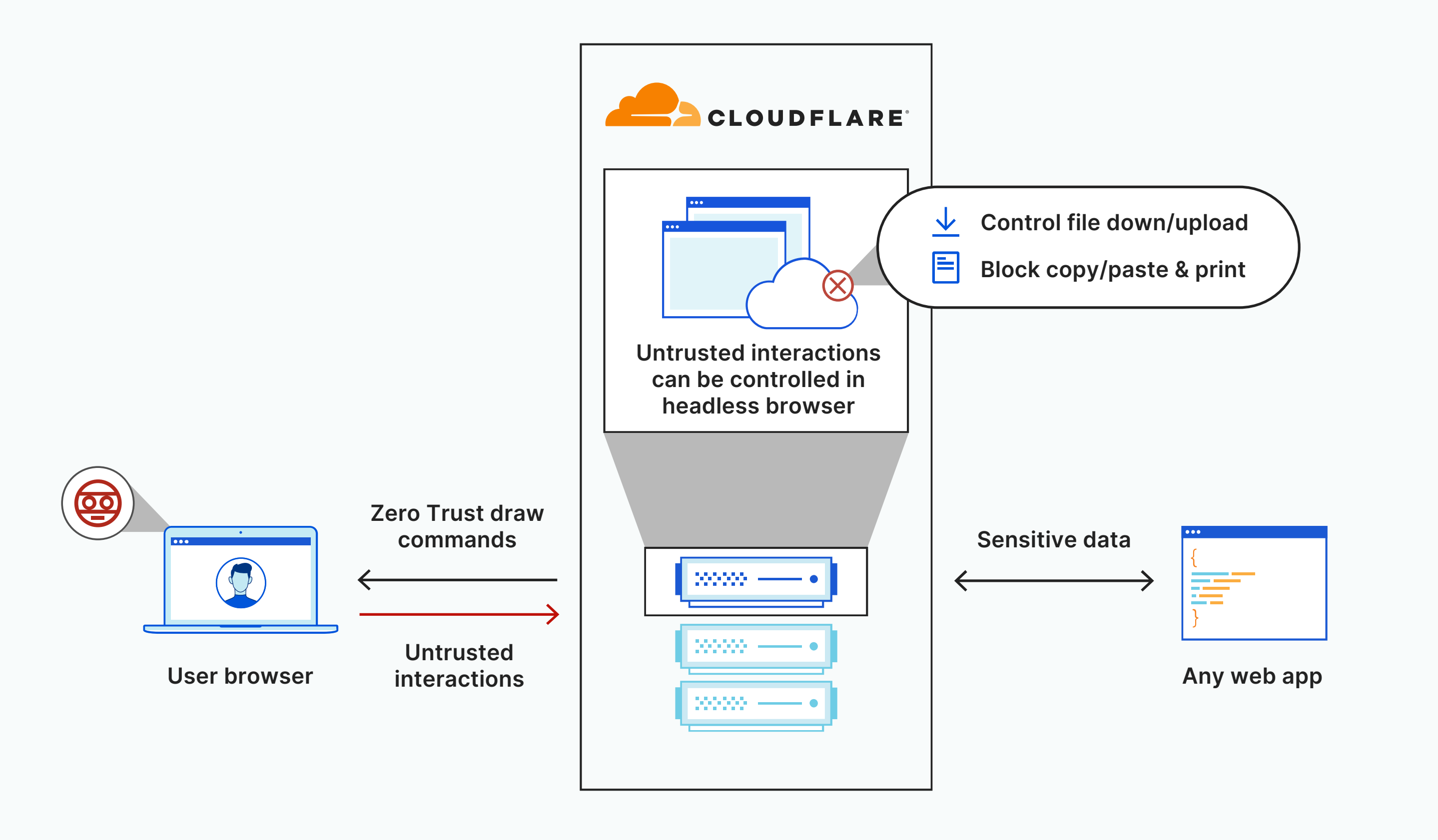
Cloudflare enables tenant control through HTTP gateway policies, which can be configured to prevent users from accessing consumer versions of applications. Instead of enforcing these policies using on-premise proxy servers via corporate VPNs, Cloudflare filters and inspects all traffic and requests through a vast global network of data centers — so your users never experience increased latency or degraded performance.

Prevent corporate data from leaving your tenants

Cloudflare makes it easy to build and deploy Zero Trust browsing policies to control and protect the data that lives within your web-based applications. All application code is executed in a secure headless browser running remotely across our massive global network, rather than endpoint devices, so sensitive data is shielded from compromised or untrusted devices and zero-day threats. And administrators retain control over how users access and share that data, so you can minimize the risk of accidental data loss or more significant data breaches.

Key Features

- Allow or block browser behaviors based on multiple criteria, including application, application type, hostname, user identity, and security risk
- Control user actions within the browser: download, upload, copy-paste, keyboard input, and printing functionalities



The Cloudflare difference

Breadth of our platform

Cloudflare places Zero Trust access (ZTNA), gateway (SWG), and browser (RBI) controls in front of your SaaS applications — without requiring your IT team to configure and operate a dedicated inline CASB product.

Built from scratch

Cloudflare's CASB capabilities work seamlessly with our ZTNA, SWG, and RBI services because all are built from scratch — eliminating the need to juggle multiple point products to protect your applications and teams.

Single control pane

Cloudflare allows organizations to set policies and manage application access and usage from a single dashboard — so you can monitor all requests and permissions at a glance.

Cloudflare helps teams monitor, protect, and control SaaS applications via a natively integrated suite of Zero Trust security capabilities.

Learn more now