

Secure workforce use of generative and agentic AI

Empower your teams to use any AI tool safely and cost effectively with protections enforced by Cloudflare's SASE platform.

Regain control, unlock productivity

The rush to adopt AI is leaving a trail of mounting risks, including data leaks, regulatory violations, unpredictable expenses, and an expanding attack surface.

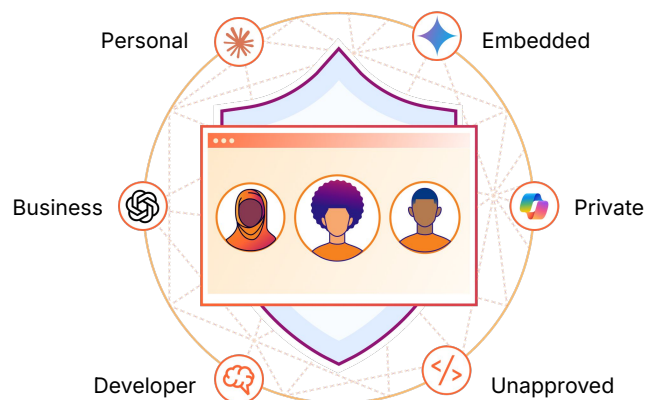
Cloudflare safeguards your organization's use of AI by extending visibility, mitigating risks, and protecting data holistically across AI environments, all while keeping AI costs under control:

- **Discover shadow AI** and manage policies for all sanctioned and unsanctioned AI tools.
- **Strengthen AI governance** with identity-based access controls and posture management.
- **Stop data loss** by blocking sensitive information in user prompts and enforcing topical guardrails
- **Manage costs** by enforcing individual or team budgets and intelligent model routing

Extend Cloudflare to safely adopt AI, whether your AI strategy involves limiting use to specific applications or experimenting with a wider range of diverse tools.

Secure generative and agentic AI communication

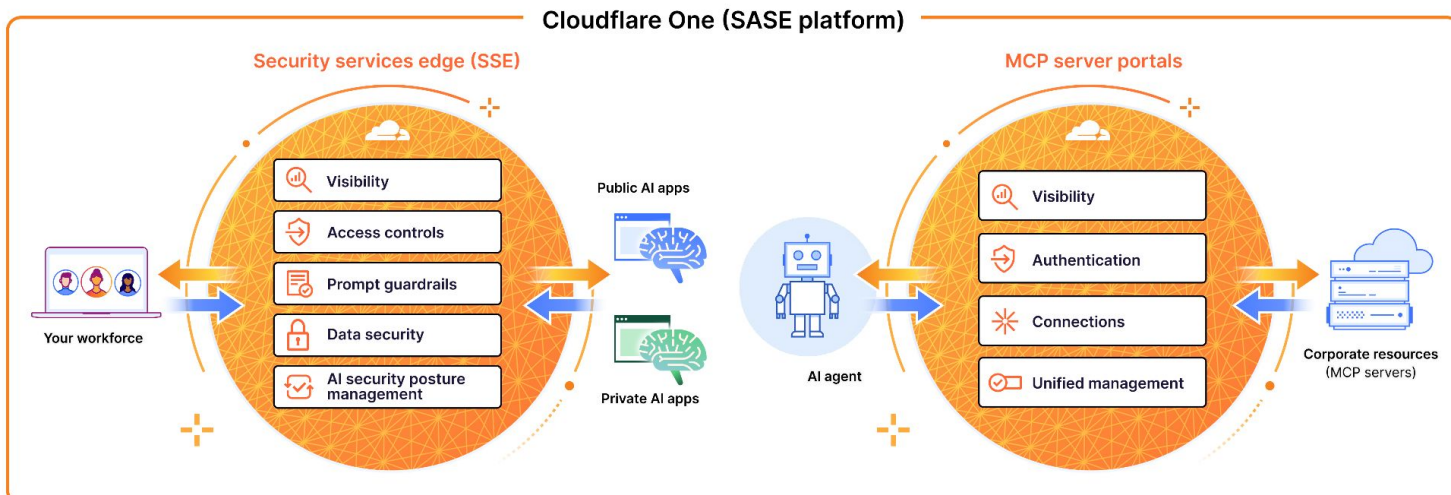
Cloudflare's SASE platform provides one unified dashboard and control plane to manage both human-to-AI and machine-to-machine interactions throughout your organization.



Why SASE?

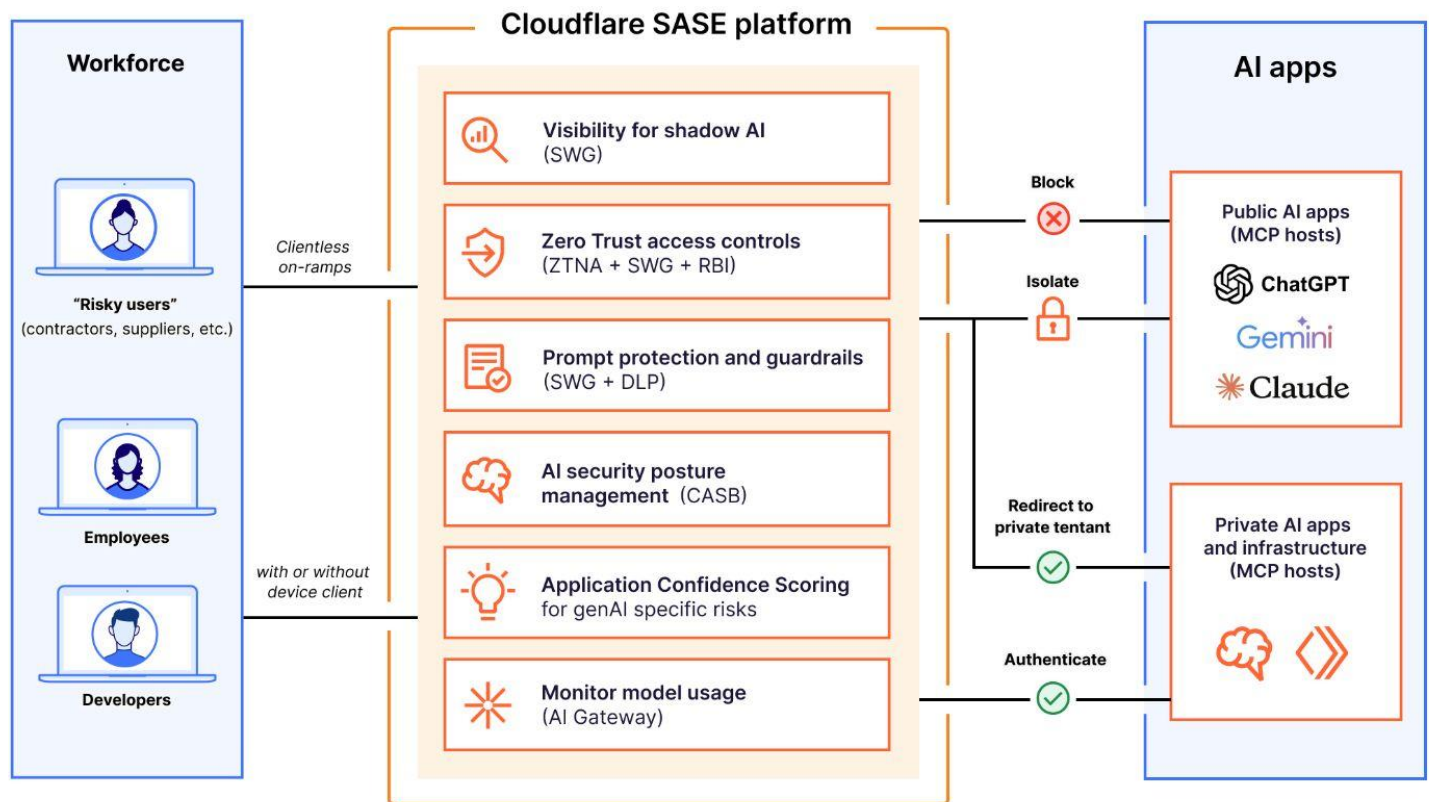
Cloudflare's secure access service edge (SASE) platform sits in between your workforce and AI tools. This makes SASE an ideal starting point for many to begin safely using AI.

Whether employees are chatting with ChatGPT or AI agents are gathering information across corporate resources, Cloudflare's SASE platform enforces consistent security controls.



Unlike other SASE vendors, Cloudflare also helps connect and protect public-facing AI-enabled apps and workloads (like your website's AI chatbot or recommendation engines).

Protect user communication with generative AI apps with AI usage controls on Cloudflare's SASE platform



- **Visibility:** Discover and analyze [shadow AI](#) use via in-line traffic inspection. Evaluate risks posed by those AI apps with [transparent scoring](#).
- **Access controls:** Block, isolate, redirect, or allow user connections. Enforce identity-based zero trust rules per app.
- **Prompt protection and guardrails:** Detect and block user prompts based on [intent](#) (e.g., jailbreak attempts, code abuse, PII requests).
- **Data security:** Stop sensitive data exposure with AI-powered [data loss prevention \(DLP\)](#) detections for PII, source code, and more.
- **AI security posture management:** Integrate with GenAI tools via API (Copilot, ChatGPT, Claude, Gemini) to scan for misconfigurations using our [cloud access security broker \(CASB\)](#).

Customer outcomes

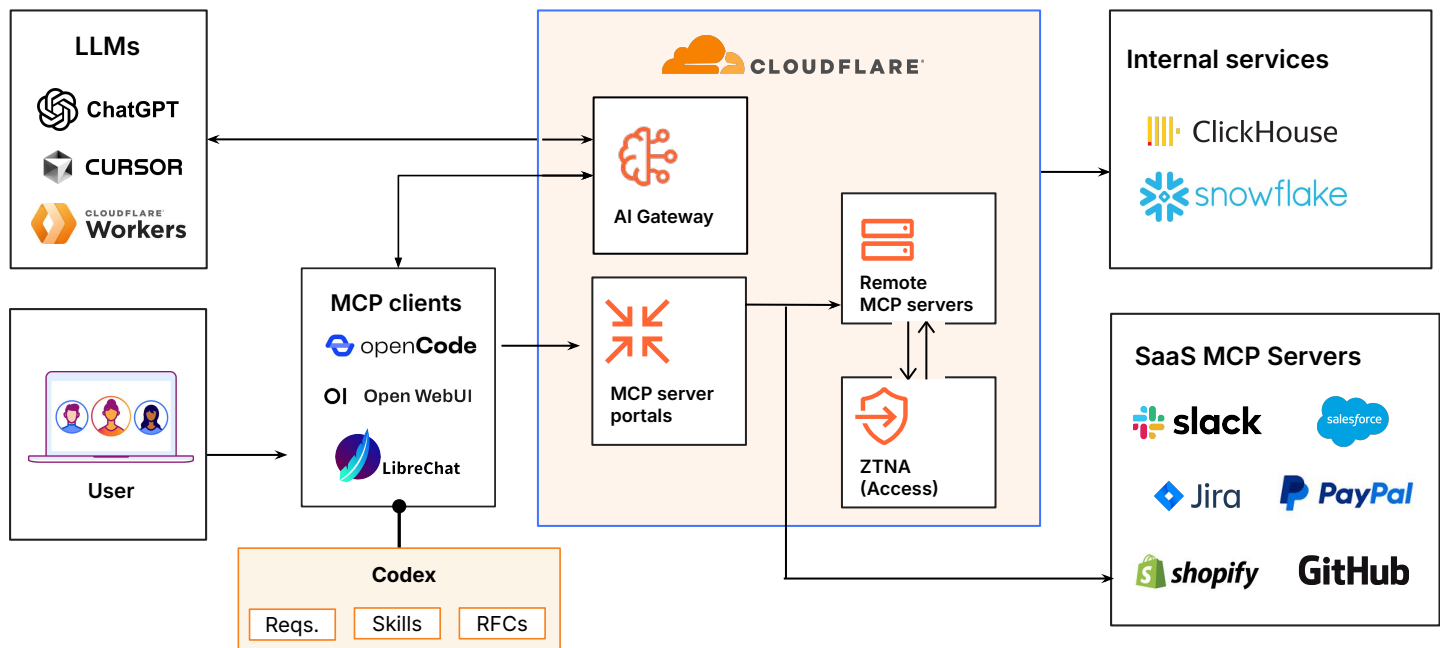


Identify and control shadow AI in parallel with VPN replacement project.



Isolate public GenAI tools like ChatGPT to block copy-paste of sensitive data.

Govern agentic AI communication (AI-to-resource) with MCP server portals on Cloudflare's SASE platform



- **Visibility:** Aggregate all MCP request logs for audit and analysis. Review and approve each MCP server before adding to portal.
- **Authentication:** Authenticate user access to portal based on identity. Scope access to MCP servers based on least privilege.
- **Connections:** Connect all accessible MCP servers with a single URL, instead of individually configuring each MCP server.
- **Unified management:** Enforce the same granular access policies for AI connections as you do for human users.

- **Customize tools per portal:** Choose the specific tools and prompt templates made available per user.
- **Enforce cost controls:** Set identity-based budgets and intelligently route models to more effectively manage frontier model usage.

Note: Cloudflare's [MCP server portals](#) support any MCP server, including (but not limited to) any [remote MCP server built or deployed](#) on Cloudflare. This capability is available as a [zero trust network access \(ZTNA\)](#) control.

Learn more about our implementation in this [blog](#).

Ready to explore how Cloudflare can
secure your use of AI?

Request a workshop