

Secure AI with Cloudflare

One platform to secure every AI app, agent, and user and defend against evolving threats.

Secure the AI lifecycle from development to production

Your organization is asked to do two things at once: move fast on AI, and stay in control while you do it. But every AI tool and agentic workload you adopt expands your risk beyond what the security stack you built for humans was designed to govern.

Cloudflare delivers complete AI security to keep your business moving at full speed. One unified platform unifies visibility, policy, and cost control across AI apps, agents, and human users:

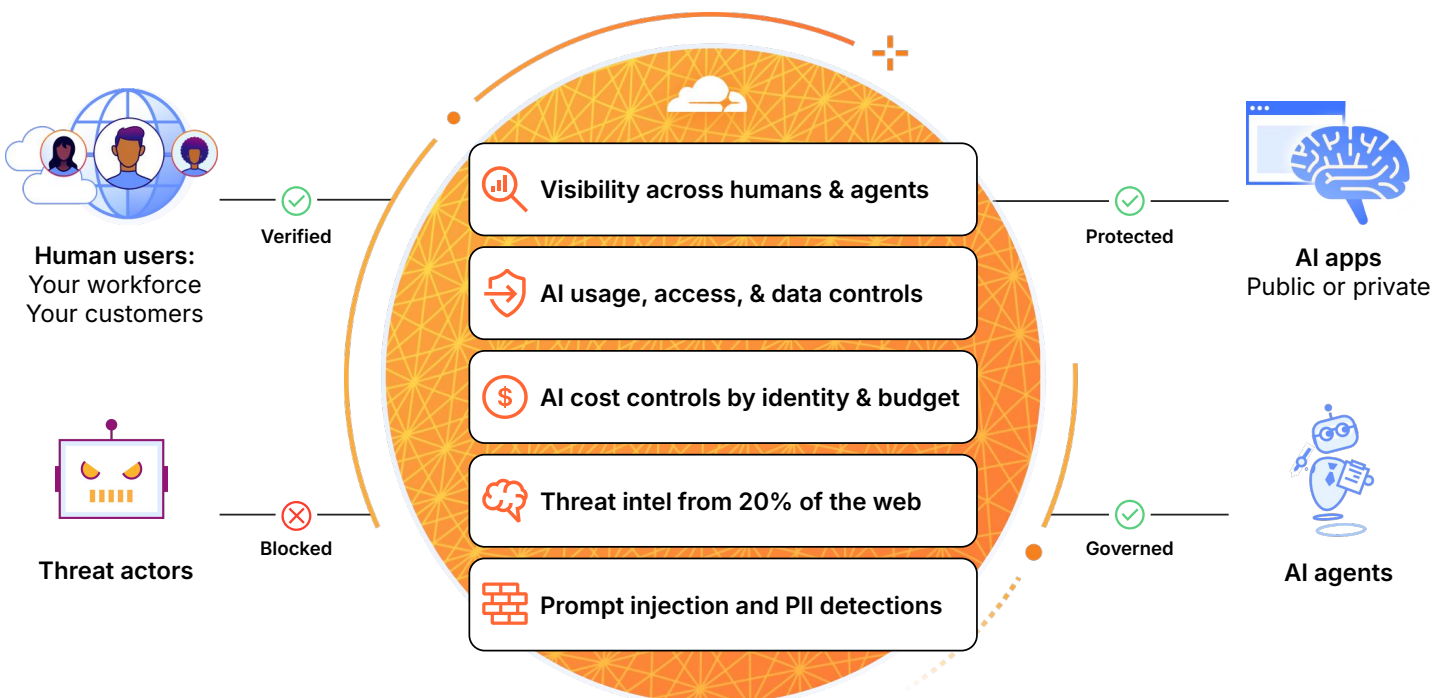
- Detect and prevent shadow AI and data loss
- Govern AI agents with centralized access rules
- Regain control over runaway AI costs
- Stop and contain AI-accelerated threats
- Protect customer-facing AI apps and models



Build and secure AI on the same platform

Cloudflare is both a developer platform for building AI and a security platform for protecting it. Workloads are secure by design, not through separate scanning or post-deployment fixes. Protections like Zero Trust verification and AI prompt guardrails are built-in from development through runtime.

One platform, one control plane



Every AI security need. One platform, no integrations.

	CLOUDFLARE			
Use case	Secure workforce use of AI	Govern AI agents	Protect AI-powered applications	Build AI securely
Cloudflare services	Cloudflare One (SASE) AI Gateway	Remote MCP servers, Cloudflare Access (ZTNA) with MCP Server Portals	Application Security (inc. AI Security for Apps)	Workers AI, AI Search, AI Gateway, Agents SDK, Dynamic Workers, Containers, Artifacts
Other major vendors	SASE / SSE	Developer-focused	App Security / WAAP	Hyperscalers
	 	 Hyperscalers 		
Specialized startups				

Cloudflare advantages

Complete AI security
across apps, agents, & users

See and control your entire AI attack surface from one platform: AI tools and models you use, AI agents you deploy, and your public-facing AI apps and web experiences. Unlike vendors that specialize in one domain, Cloudflare secures them all.

Security integrated by architecture
not by invoice

Cloudflare services share one global infrastructure across 335+ cities, enforcing security in a single pass. Unlike vendors with point solutions integrated by invoice, Cloudflare's architecture is unified for consistent protection without service chaining.

Global threat intelligence
that learns from 20% of the Internet

Cloudflare's unmatched visibility into global web, network, and DNS traffic helps us spot AI-accelerated threats faster. That intelligence powers all of our security services, so you're already protected from the latest threats before they reach you.

Post-quantum (PQ) encryption
on by default and free

Hybrid PQ key agreement has been deployed across our network by default and at no extra cost since 2022 to protect against harvest-now-decrypt-later attacks. PQ authentication is rolling out against a published, dated roadmap.