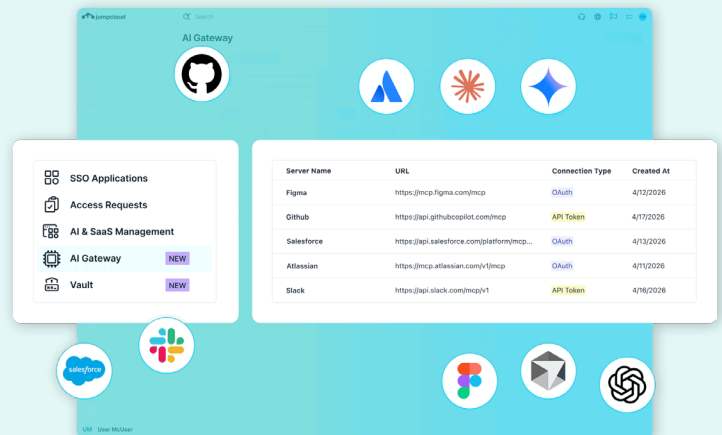


JumpCloud Agentic IAM

See every agent. Govern every identity. JumpCloud manages the full lifecycle of humans, devices, and agents, from discovery to deprovisioning. By connecting user logins and extending privileged access to agents, JumpCloud turns shadow AI into a safe value accelerator for Intelligent, Secure IT.



See, Control, Accelerate



Reveal Every Agent

Discover and manage AI tools and MCP configurations to prevent data leakage and ensure compliance. Identify and register agents with lifecycle controls, remove rogue agents, and secure local MCP integrations via the AI Gateway. Empower your workforce by managing and delivering IT-approved AI tools through a trusted catalog, ensuring safe, compliant innovation.



Govern and Scale At the Speed of AI

Establish agents as primary identities and extend Privileged Access Management (PAM) with temporary, minimal permissions. Unify workforce and workload governance across the entire identity chain while applying Zero Trust principles at the machine layer. Maintain continuous audit logging for compliance to ensure full accountability across legacy and modern systems.



Innovate with Agentic Control

Accelerate innovation by operating at the speed of AI within hardened security guardrails. Replace manual, reactive processes with high-velocity governance to achieve compliance goals ahead of schedule. Automatically enforce the principle of least privilege to eliminate identity debt, streamline your path to production, and drive down Total Cost of Ownership (TCO).

Interested in learning more?

Contact your JumpCloud Account Executive or Account Manager.

Strategic Use Cases

1. Eliminate Shadow AI

Discover all AI usage across browsers and managed devices, from GenAI to agentic browsers, to eliminate blind spots and reduce risk. By turning shadow usage into an inventoried, governed catalog, you empower teams to innovate safely and accelerate productivity, transforming IT from a barrier into an accelerator for AI-driven work.

2. Onboard and Govern Autonomous Agents Safely

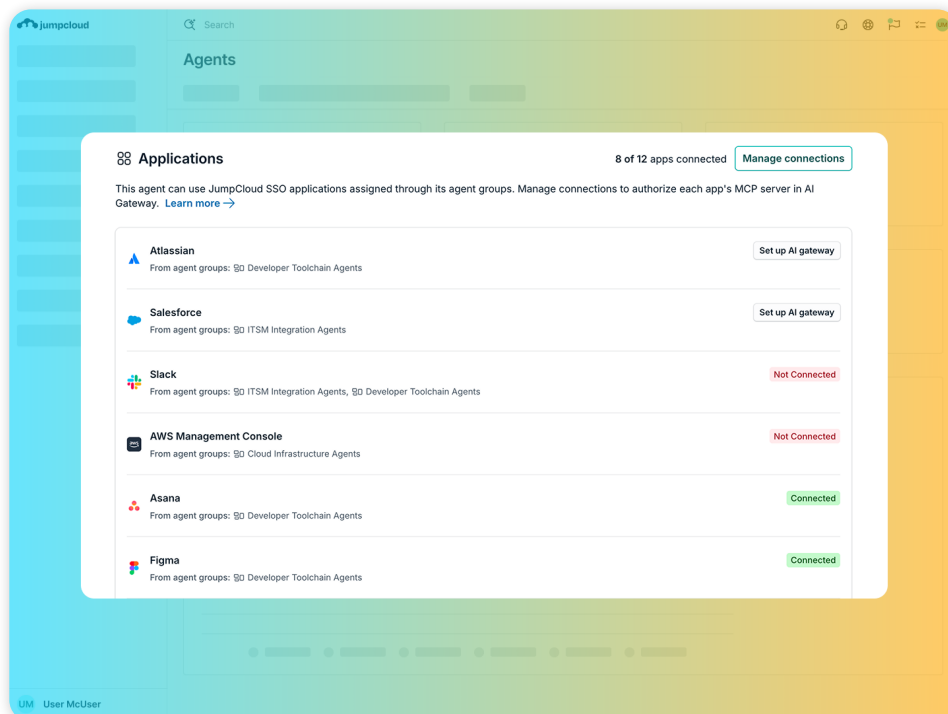
Lacking identity models for autonomous bots, teams default to unsafe shortcuts like shared credentials, fake users, and unmanaged API keys. JumpCloud treats agents as primary identities bound to human owners, enabling Agent Group application access and independent lifecycle controls to disable an agent without impacting the human owner.

3. Trusted Employee AI with MCP Governance

Connecting employee AI tools via Model Context Protocol (MCP) introduces shadow MCP, credential sprawl, and missing runtime attribution. JumpCloud uses device MCP Discovery to surface unvetted connections and routes traffic through AI Gateway for tool authorization, volume tracking, and user activity logging.

4. Extend Privileged Access Management (PAM) to AI Agents

Infrastructure agents requiring elevated access often rely on standing privileged credentials and static root passwords. JumpCloud extends PAM directly to agent workflows, providing scoped, temporary access to production databases and servers with explicit audit trails.



Key Features

- **AI Agent Identity & Access:**
Register, authenticate, group, and manage agents independently, while providing policy-governed access to approved AI tools.
- **Managed AI Gateway:**
Create a secure control layer between agents and resources to centrally provision, govern, and revoke AI connectors and tokens used across approved tools.
- **Audit and Visibility:**
Provide centralized logging and reporting of AI access and activity correlated directly to user identity and device context.
- **Shadow AI to Secure MCP Connection:**
Discover MCP configurations on devices and connect them directly to JumpCloud AI Gateway for secure access, eliminating shadow AI and manual MCP hunting.
- **Dashboard & Analytics:**
View usage and trend details related to AI traffic to trace security anomalies and automatically generate executive reporting.
- **PAM MCP Server:**
Deploy a secure, per-tenant PAM agent with zero setup required to enable safe administrative automation without static credentials or complex wiring.

Need Help Getting Started?

JumpCloud's Professional Services Team is here to support you along the way. Whether you need implementation assistance or hands-on engineering support, there's a service package for you.

[Learn more and find the right service level for your business today.](#)