aembit

Secure Agentic AI With Identity and Access Management

Aembit's Identity and Access Management (IAM) platform allows you to securely authenticate the agents and MCP Servers that access your sensitive data and systems.

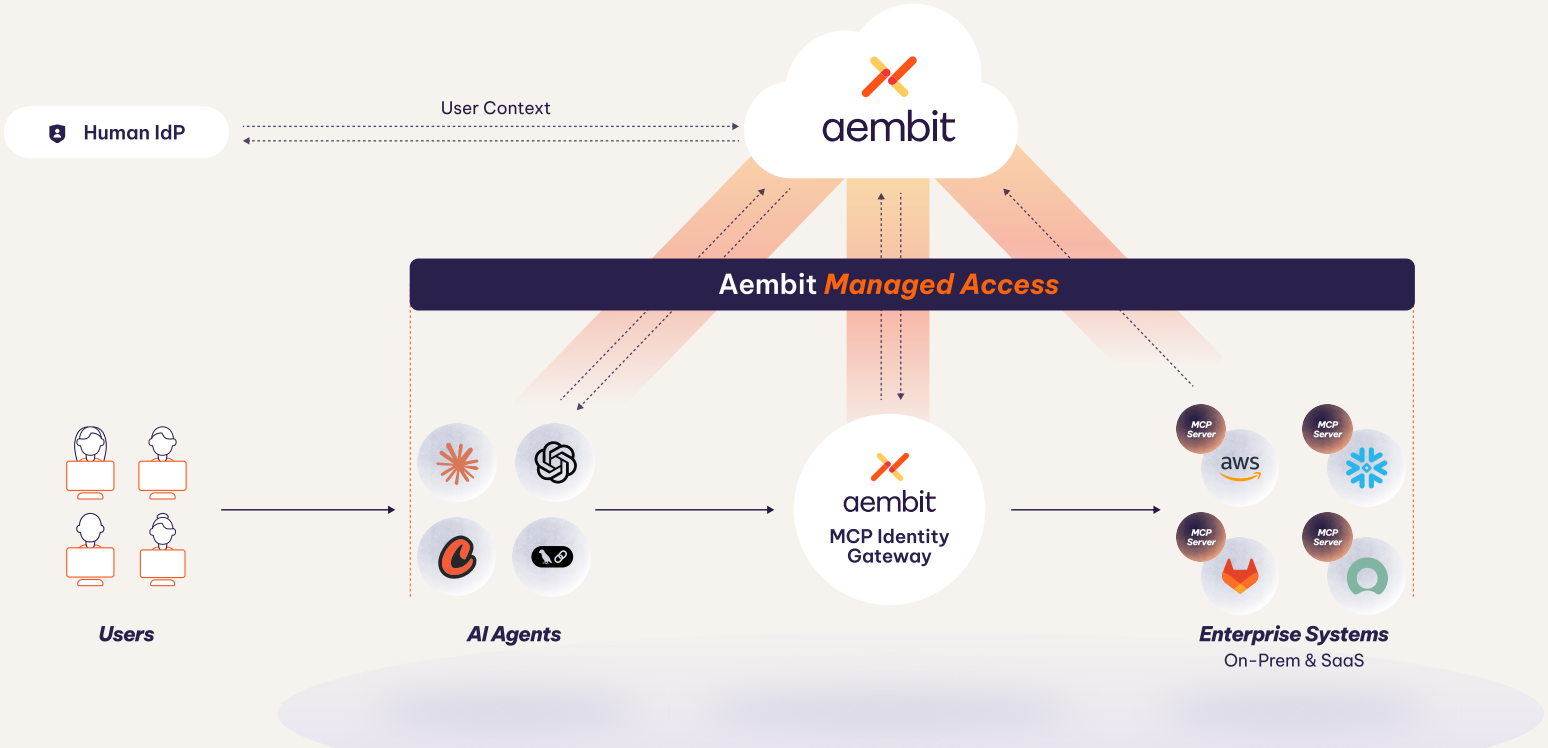
Aembit provides an independent identity control plane that provides secretless, just-in-time access to AI agents. We enable you to manage access, not secrets.

Agentic AI Access Risks

- Autonomous agents aren't always tied to a single human's actions.
- AI agents possess secrets to access resources.
- No enforcement of access to sensitive data.
- Unmanaged AI posture or behavior.
- Obscured audit trail for Agentic AI.

Agentic AI With Aembit

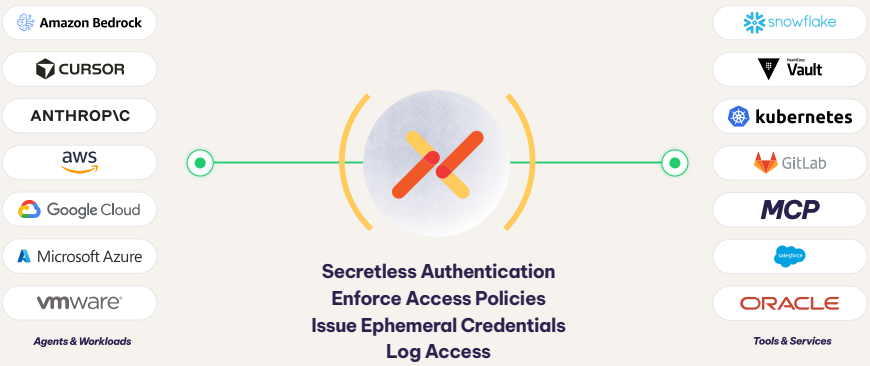
- Every AI agent gets its own identity, whether it operates autonomously or via delegated authority.
- AI agents use secretless access based on cryptographically verifiable machine identity.
- Run-time policy enforcement means every AI agent can only access the resources it is permitted to reach, seamlessly supporting MCP.
- Access gated by conditional access for agent security posture and permitted access behavior.
- Audit logging means that the access trail for an agent is fully visible, based on human user, identity, policy, and credentials.



Request a demo at www.aembit.io

Aembit IAM for *AI Agents*

Aembit IAM for Agentic AI provides an identity and authorization for AI agents and other non-human identities. This enforces access securely between any kind of workload and downstream sensitive data, applications, and resources.



Aembit integrates flexibly with modern software — like AI Agents using MCP — along with scripts, applications, serverless applications, containers, and more.

1. **Verify identity** - use blended identities for agents and the humans using them. Leverage SPIFFE, OIDC, Oauth, and your Workforce IAM to cryptographically attest to an agent's identity.
2. **Check policy and conditional access** - define tightly scoped acces policies that also enforce security posture, time-of-day, or geographic requirements.
3. **Issue just-in-time credential** - provide a short-lived credential only when access is granted.
4. **Log transaction** - create a centralized, auditable record of access from AI agents to sensitive resources.

Built for the *Enterprise*

1 Control AI Risk, While Driving Its Potential

You tightly control - and automate - the provisioning and enforcement of access policies, whether they are based on MCP or the next emerging protocol. You create a single point of visibility into AI-driven access to your data and services. Securing Agentic AI access goes from reactive to proactive.

2 Modern Innovation Meets Existing Infrastructure

You enable innovative AI-driven tools to interact securely with your existing and legacy systems. Aembit integrates cleanly with AI but also transparently works with earlier generations of technology whether they are on-premise virtual machines, SaaS applications, or cloud-native infrastructure, a range of identity providers, and credential types.

3 Machine-Scale IAM

You increase development speed without sacrificing security or auditability. Built for automation, Aembit already works across thousands of workloads and agents. Aembit is designed to work with Infrastructure as Code (IaC) to meet the scale and flexibility your developers require.

4 Standards-Based and Compliance Minded

You keep your systems compliant with Aembit-supported standards such as MCP, OAuth, SPIFFE, OIDC, and more, ensuring frictionless interoperability and no lock-in. Aembit meets industry standards such as SOC 2 Type 2 and ISO 27001.

snowflake

"Aembit gives us IAM for Agentic AI."

Gaurav Singodia, Senior Cloud Manager