



Know every agent. Control every call.



What an AI security and governance layer must do

- ✓ Discover every agent, model, and MCP server
- ✓ Establish clear ownership for AI agents
- ✓ Review and certify agent access regularly
- ✓ Enforce access at runtime, on every call
- ✓ Keep sensitive data out of agent traffic
- ✓ Prove which agent accessed what

What organizations are up against



AI agent
sprawl



Ownerless
AI agents



Over-privileged
agents and
identities



Uncontrolled
agent-to-MCP
access



Sensitive data
exposure

Introducing SecureAI

ManageEngine SecureAI is an AI agent security and governance platform for enterprises that brings visibility, accountability, and control to your growing AI ecosystem. Discover AI agents, models, and MCP servers across various platforms, establish ownership, and govern their access with built-in certifications and risk assessments. Secure every agent-to-MCP-server interaction through MCP gateways that enforce access and DLP policies in real time, so your teams can embrace AI while keeping every agent accountable, appropriately scoped, and auditable.

◆ THE CHALLENGE

◆ HOW SECUREAI SOLVES IT

◆ VALUE DELIVERED



**Fragmented
AI visibility**

AI agent discovery identifies AI agents, models, and MCP servers across connected providers.

Eliminate AI blind spots and gain control over your growing AI estate



**Unowned
AI agents**

Agent ownership policy ensures every AI agent has a named owner, establishing clear accountability

Strengthen accountability by ensuring every AI agent has a responsible owner



**Agent privilege
sprawl**

Access Graph reveals agent access paths by mapping identities, roles, permissions, policies, and accessible resources.

Identify over-privileged agents before they put critical resources at risk



**Stale agent
access**

Access certification requests and campaigns enable reviewers to approve or revoke access and periodically reconfirm existing agent access.

Ensure appropriate AI access and promptly revoke outdated permissions.



**Risky AI
configurations**

AI Risk Assessment determines the risk posture of enterprise AI platforms such as Anthropic Claude, GitHub Copilot, and Gemini based on misconfigurations.

Reduce AI risk by identifying security gaps before they lead to security incidents



**Ungoverned
MCP access**

MCP Gateways mediate every agent-to-MCP-server interaction, enforcing access policies to tools and servers

Prevent unauthorized agent activity from reaching enterprise tools and resources



**Sensitive data
exposure**

DLP Policies redact or block sensitive data passing through MCP gateways.

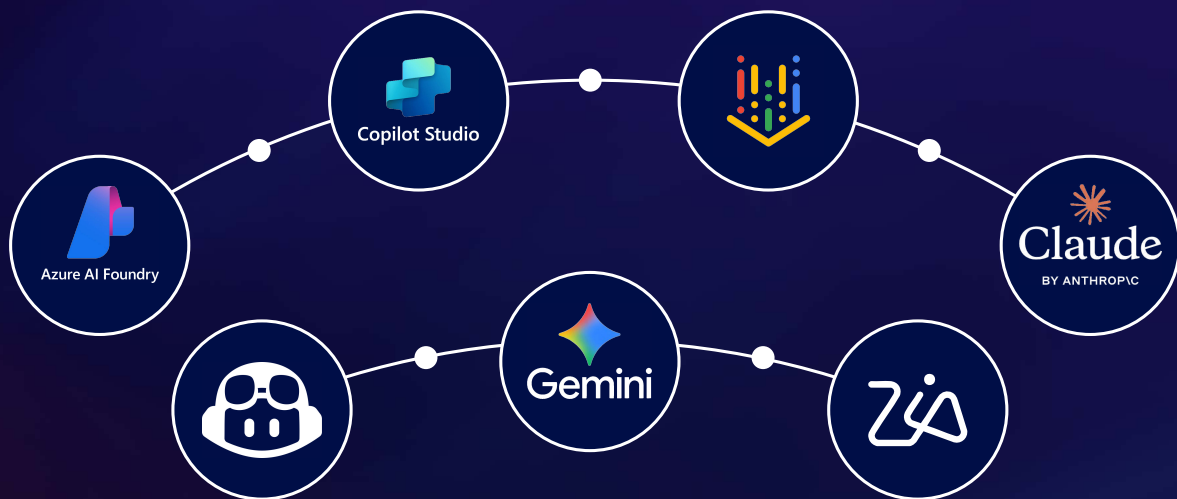
Keep sensitive information protected as agents interact with enterprise tools



**AI activity
blind spots**

Agent, Gateway activity and Insight reports provide visibility into agent usage, MCP tool usage, server latency, inactive servers, errors, and policy decisions.

Improve oversight and accountability with a clear record of AI activity and policy decisions



Built to fit your environment

Discover

Agents, models, and
MCP servers

Govern

Ownership, access, and
certifications

Protect

Every agent-to-MCP
interaction

Pricing and licensing

\$50

per agent/per year*

**Pricing based on a contract for 100 agents.
Volume-based discounts are available.*

We'll shape a plan around your AI stack.

Receive a custom quote.

Specifications



Supported device platforms:

Windows Server 2008 and
above, Windows 7 and
above, and Windows Vista



Supported browsers:

Mozilla Firefox,
Google Chrome,
and Microsoft Edge

 <https://www.manageengine.com/secure-ai/>

 secureai-support@manageengine.com

 +1-840-200-1275

 [Get Quote](#)

 [Download](#)