



ManageEngine
SecureAI

Every agent governed.
Every call secured.



www.manageengine.com/secure-ai/

The unseen risks weighing on your business

Unseen data exposure

Sensitive data can pass through AI interactions unprotected.

Agent privilege sprawl

Excessive agent access widens the potential blast radius.

Unmonitored tool access

Ungoverned tool calls can trigger unauthorized actions.

Orphaned agents

Agents without owners create gaps in oversight and accountability.

Misconfiguration exposure

Configuration gaps can weaken your overall AI security posture.

Why AI security can't wait

94%

expect AI to be the most significant driver of **cybersecurity change**.

87%

identified AI-related vulnerabilities as the **fastest-growing cyber risk**.

*Source: World Economic Forum, Global Cybersecurity Outlook 2026

Meet SecureAI

SecureAI governs your AI ecosystem, so every agent and its access stays in check.

Discover

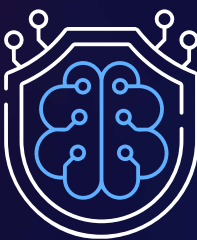
agents, models, and MCP servers.

Govern

ownership, access, and certifications.

Protect

every agent-to-MCP interaction.



What SecureAI delivers



Cross-platform AI discovery

Discover AI agents, models, and MCP servers across platforms.



AI risk assessment

Assess and identify AI platform configuration risks.



Agent ownership

Give every AI agent a human owner who's accountable for it.



MCP gateway

Route agent-to-MCP traffic through secure, centralized gateways.



Access graph

View agent access mapped across identities, roles, permissions, and more.



MCP access control

Define which MCP tools and servers agents can access.



Entitlement visibility

Govern agent entitlements and define review scope with access templates.



Sensitive data protection

Prevent sensitive data exposure in MCP traffic with DLP controls.



Access certification

Validate and revoke agent access through periodic reviews.



Runtime visibility

Track gateway activity, tool usage, policy decisions, and errors.

3 reasons to choose SecureAI

01 AI estate visibility

Understand where AI risk exists across your environment and prioritize what needs attention.

02 Accountable AI access

Keep agent access owned, reviewed, and aligned with evolving business needs.

03 Protected AI interactions

Reduce unauthorized access and sensitive data exposure during agent-to-MCP interactions.

Built for every stakeholder



CISO

Reduce AI-driven risk and strengthen security oversight as AI adoption scales across the business.



Admin

Utilize one console to discover agents, assign owners, and enforce policies across providers.



SecOps Team

Identify high-risk agents and gain visibility into policy violations and MCP activity.

Pricing

\$50 per agent/per year*

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



Scan to visit the website



Email: secureai-support@manageengine.com



Call: +1-840-200-1275