



Secure Your Entire AI Ecosystem

AI adoption is moving faster than security can keep up. Ovalix bridges this gap by delivering visibility and control through a single AI security platform – enabling organizations to innovate with confidence.



Public GenAI Apps

Eliminate shadow AI & data leakage, enforcing compliant AI usage.



Homegrown AI Apps

Protect custom AI apps from manipulation and adversarial attacks.



Employee Endpoints

Control AI tool usage and activity on employee devices.



Coding Agents

Secure coding agents to prevent risky actions and policy violations.



Key Benefits



Enterprise AI security in one platform



Full visibility across all AI tools



Data leakage prevention



Proactive risk mitigation



Centralized AI governance

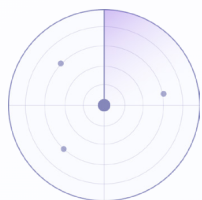


Real-time guidance for employees

How Ovalix Works

Secure your complete AI environment – from discovery to prevention.

1



Discover

Gain visibility into all AI applications and interactions, identifying shadow AI, agentic workflows, and risks.

2



Detect

Continuously monitor AI usage for suspicious activities, malicious inputs, and unauthorized access in real time.

3



Govern

Establish policies and controls to ensure compliance with regulatory and organizational requirements.

4



Prevent

Proactively mitigate risks and remediate vulnerabilities with built-in safeguards to protect AI assets from exploitation.

About Ovalix

Ovalix provides a holistic platform for organizations to safely adopt AI technology. The platform eliminates critical risks including data leakage, shadow AI, malicious prompts, and compliance failures across a wide range of AI applications – from basic GenAI applications to advanced agentic AI systems.