Aurascape AI Security At a Glance

Key Benefits

Discover AI Use

Gain full visibility into all AI applications, copilots, agents, and embedded AI —across known and emerging tools, with zero-day application support.

Control AI Use

Set risk-aware policies that account for user identity, intent, and the context of the conversation—enabling safe AI use without stifling productivity.

Safeguard AI Activity

Protect sensitive data and prevent AI-driven threats with real-time data classification plus threat detection for both prompts and responses, with user coaching for risky activity.

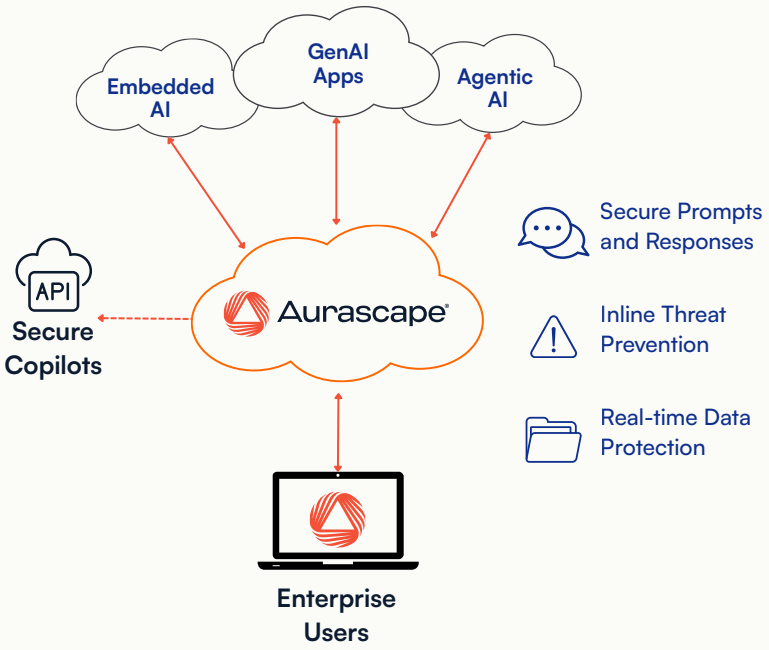
Streamline Operations

Role-based natural language investigation, automated reporting, and user coaching provide distributed, comprehensive human-in-the-loop AI security.

From Shadow AI to Secure AI

Firewalls and Secure Web Gateways were built for a pre-AI world—when apps used standard protocols and data exposures followed predictable patterns. Today's AI tools operate differently. They use opaque, custom protocols, stream data continuously, and are rapidly embedding themselves into existing trusted applications—making them invisible to traditional security solutions.

Aurascape closes that visibility and control gap. As an AI-native security layer, Aurascape gives you real-time visibility and control over AI access and usage across your entire organization. It empowers teams to adopt AI responsibly—by discovering, classifying, and securing AI activity without disrupting productivity or innovation.



Aurascape automatically discovers and maps thousands of AI applications—providing full visibility and granular control for both known and emerging tools. It goes beyond prompt monitoring to deliver full-context insight into entire AI conversations, identifying user intent and risk in real time. Intelligent data classification, fingerprinting, and threat inspection enable precise controls to prevent data loss and block AI-driven threats without disrupting productivity.

Key Solutions

AI Data Protection

Protect sensitive data and ensure compliance with real-time data categorization and intent-aware data protection policy enforcement—driven by full conversational context.

"Considering AI is now in almost every tool that our employees use, we wanted to further strengthen our security posture. Aurascape provided that for us."

Vineet Arora | CTO

WinWire

Control Shadow AI

Enable safe AI adoption by blocking unsanctioned tools, allowing approved apps with guardrails, and ensuring only enterprise accounts—not personal ones—can share sensitive data with AI tools.

Guardrails for Coding

Let developers use AI in their workflows without leaking critical code to untrusted systems. Enforce intention-based policies in browsers and IDEs to block or nudge users away from unsafe apps and actions.

Secure AI Copilots

Detect and tag sensitive information before it can be learned by AI copilots. If exposure has already occurred, flagged content is automatically unlearned—ensuring your data stays protected.

Secure Agentic AI

Agentic AI and protocols like MCP and A2A introduce new risk pathways —often invisibly. Aurascape delivers real-time visibility and context-driven policy control, helping you responsibly adopt agentic AI.

Prompt & Response Risk Analysis

Intent & Identity-Based Controls

User Coaching & Behavior Change

Automated Reporting & Compliance

Aurascape®