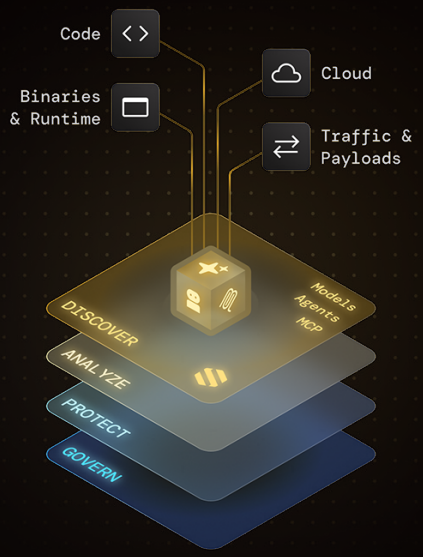
AQTIVE GUARD by SANDBOXAQ

AI-SPM

Secure AI from code to production

Inspect and secure code, cloud, and applications deep in your stack, from code to production.



The Problem

79% of organizations have AI in production, yet 72% lack a strategy to govern it. Legacy security silos fall short because they were not built for the AI stack.

Fragmented Tooling

AppSec tools see the code but miss runtime context. Cloud tools see the server but miss the AI logic inside the code.

Unchecked Risks

AI assets are being deployed with unmonitored access to sensitive data and critical tools, creating automated paths for data exfiltration.

Security Blind Spots

AI moves from code to production in a vacuum. Without a unified AI-BOM, shadow AI and unvetted agents live in your environment before security even knows they exist.

The Solution

AQtive Guard AI-SPM

Gain unified visibility to govern the AI you build and the AI you consume.

Discover Every Asset

Automatically generate a live AI-BOM. Inventory assets embedded in compiled code and files to uncover hidden models, agents, and MCP servers.

Contextualize Risk

Go beyond basic scanning. Instantly detect threats like model serialization attacks and distinguish safe models from critical liabilities.

Protect at Runtime

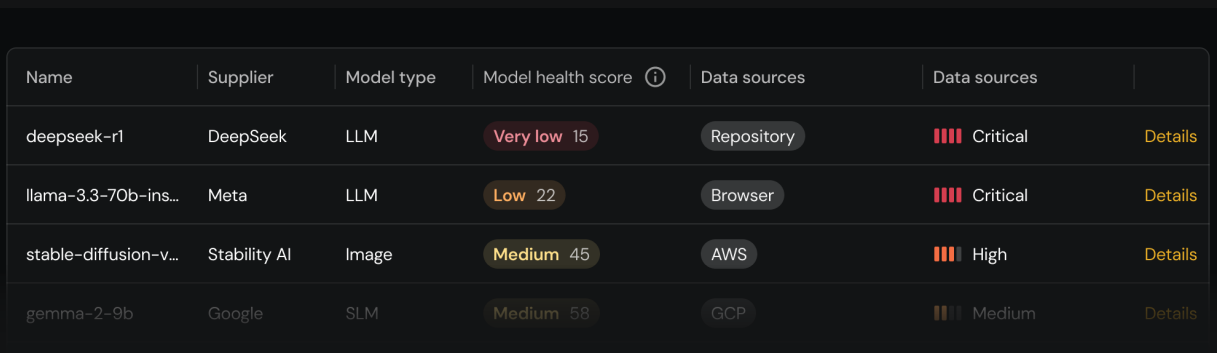
Prevent unsafe inputs and outputs in real-time. Enforce guardrails to block jailbreaks and sensitive data exposure.

Automated Governance & Compliance

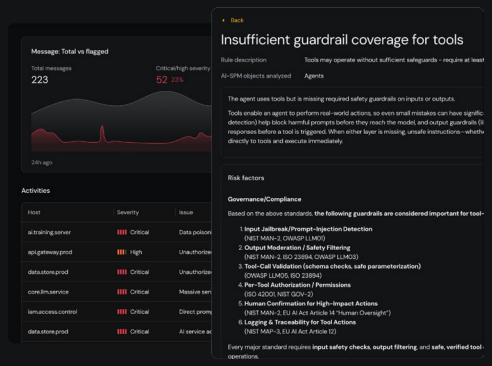
Continuously verify your AI posture aligns with internal mandates and frameworks like the EU AI Act and NIST.

AQTIVE GUARD by SANDBOXAQ

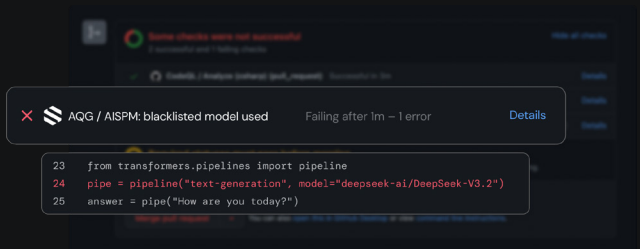
AQtive Guard AI-SPM In Action



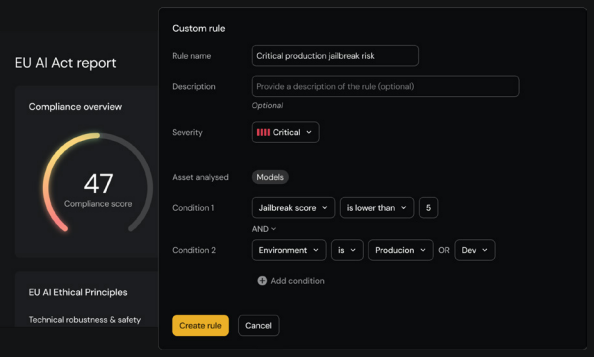
Instant AI-BOM. Automatically uncover unsanctioned models and agents that IT doesn't know about—giving you a complete inventory of your Shadow AI.



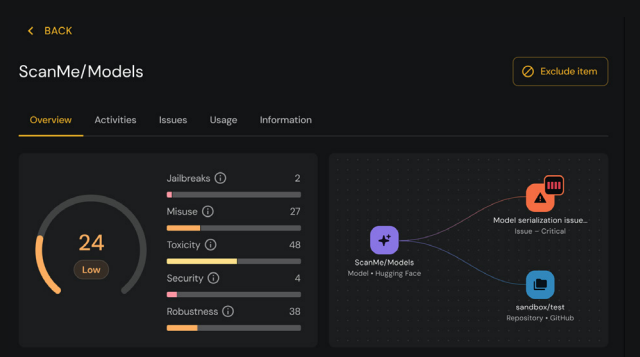
Active Runtime Protection. Proactively stop active attacks through detection of jailbreaks, sensitive data exposure, and unsafe AI responses.



Shift AI security left. Automatically scan pull requests and enforce security gates at the earliest stage of the development lifecycle.



Automated governance. Build custom rules to enforce internal policy and automatically map your security posture to major compliance frameworks.



Deep risk correlation. Don't just see the asset, see the impact. Correlate risk across data lineage, code implementation, and deployed assets to prioritize what matters.

Secure your AI assets and ship AI securely.
Request a Free AI Risk Assessment at aqtiveguard.com/demo