Deploy AI with Confidence

Manage the Risk of Using Chat GPT, Claude, Copilot, or any other AI Vendor, in One Unified Platform

AI is becoming every employee's newest coworker, and every vendor is either using it or racing to adopt it. McKinsey reports that 88% of organizations now use AI regularly, with nearly 40% using five or more AI models.

But AI adoption has outpaced AI governance. Risk visibility is fragmented. Oversight is manual. Security teams are flying blind.

SAFE AI Security Posture Management changes this; giving organizations a continuous, unified view of AI vendor exposure so they can scale AI safely, securely, and confidently.

SAFE Reimagines AI Security Posture Management

SAFE AI Security Posture Management enables organizations to continuously discover, understand, and reduce the cyber risk introduced by AI vendors such as OpenAI ChatGPT, Anthropic Claude, and Microsoft Copilot among others - through **unified visibility, continuous AI risk intelligence, and instant time-to-value with autonomous AI risk management.**

Why Choose SAFE AI-SPM?

Built for Enterprise AI Adoption
Manage risk across OpenAI, Anthropic Claude, Microsoft Copilot, Google Gemini, and any key AI vendor in your ecosystem.

Unified AI Exposure Visibility
Gain a single, continuously updated view of all AI vendors, including shadow AI usage, AI data flows and access patterns, identity risks, and more.

Continuous AI Risk Intelligence
Get visibility across 5 key areas: live activity, configurations, outside-in monitoring, questionnaires, and contracts, along with conflicts across them.

Instant Time-To-Value
SAFE's Agentic Workflow Engine, powered by 100+ AI Agents, enables enterprises to design always-on workflows that continuously monitor AI risk

Defensible AI Governance
Support security, legal, compliance, and TPRM teams with evidence-backed oversight across critical AI vendors.

Five Dimensions of SAFE AI Security Posture Management

01 | Live Activity: See how AI vendors are used across projects, prompts, users, files, PII exposure, and policy violations.

02 | Configuration Exposure: Identify insecure settings, configuration drift, overexposed access, and AI BOM risks.

03 | Outside-In Monitoring: Continuously monitor vendors across assets, breaches, leaked credentials, news, and more.

04 | Questionnaires & Compliance Assessments: Map compliance and control gaps to globally accepted AI frameworks.

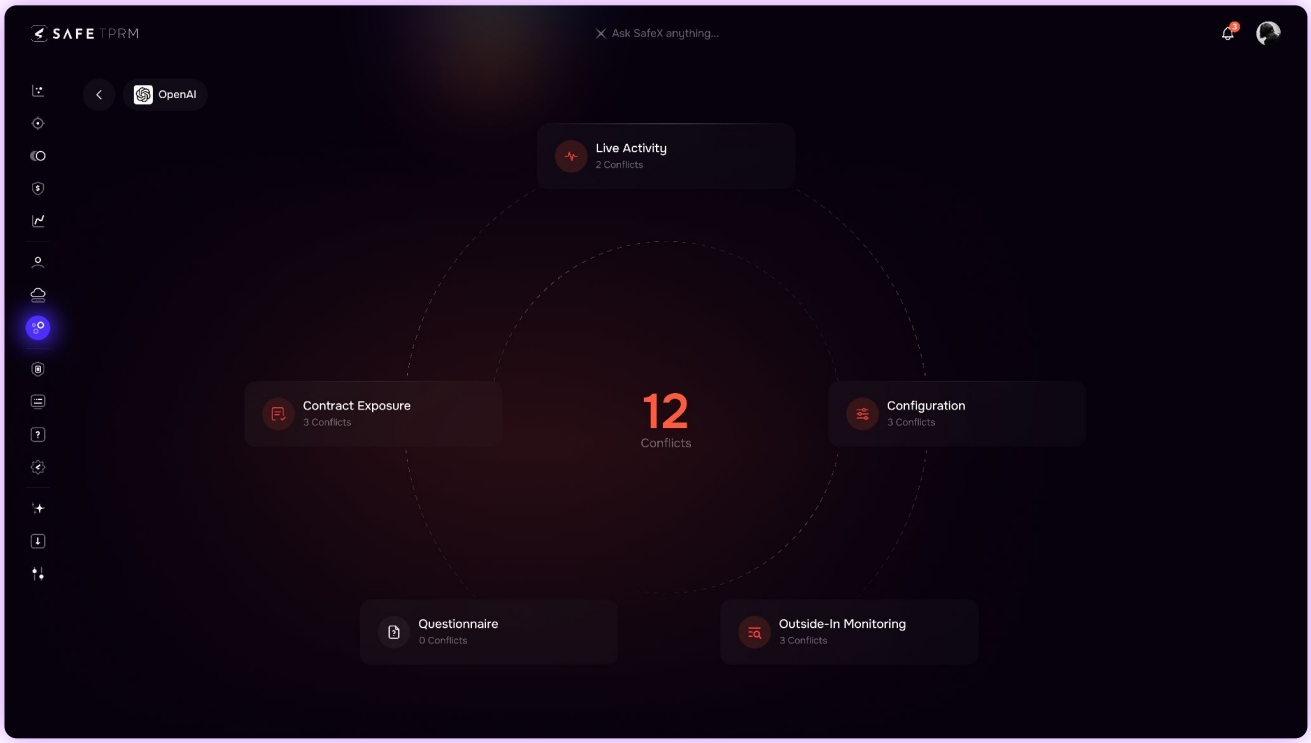
05 | Contracts: Analyze contracts for AI usage clauses, liability exposure, regulatory commitments, and governance gaps.

From Visibility to Conflict Resolution

SAFE AI Security Posture Management correlates data across all five dimensions to identify conflicts, prioritize risk, and guide teams toward action. SAFE helps teams:

- Detect contradictions across contracts, questionnaires, live activity, configurations, and outside-in exposure.
- Understand which gaps create the highest business and security risk.
- Recommend actions based on the nature and severity of the conflict.

The result: teams move from fragmented oversight to continuous AI Security Posture Management.



Want to see SAFE AI-SPM in Action? Schedule your 1:1 demo today.

SAFE is also available via AWS Marketplace.

VISIONARY IN EXPOSURE MANAGEMENT
GARTNER MAGIC QUADRANT, 2025

CATEGORY LEADER IN CRQ
FORRESTER CRQ WAVE Q2, 2025

LEADER IN THIRD PARTY RISK MANAGEMENT
LIMINAL LINK INDEX™ REPORT, 2025

RESEARCH SPONSOR
MITRE ATT&CK, TOP CONTRIBUTOR