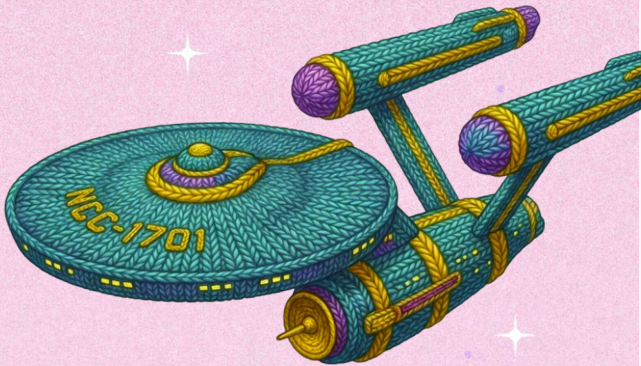


The Secure AI Control Plane



Accelerate secure AI adoption across your environment with Onyx, a single platform that enables security, governance, and infrastructure teams as they oversee AI agent use, ensure compliance, and measure effectiveness.

Onyx gives enterprises a unified platform to continuously discover AI agents, monitor their reasoning, and govern their actions in real time. Powered by proprietary supervisory agents and models, Onyx can block risky behavior, require human approval, or redirect decisions as needed, ensuring every agent operates within security and governance policies.

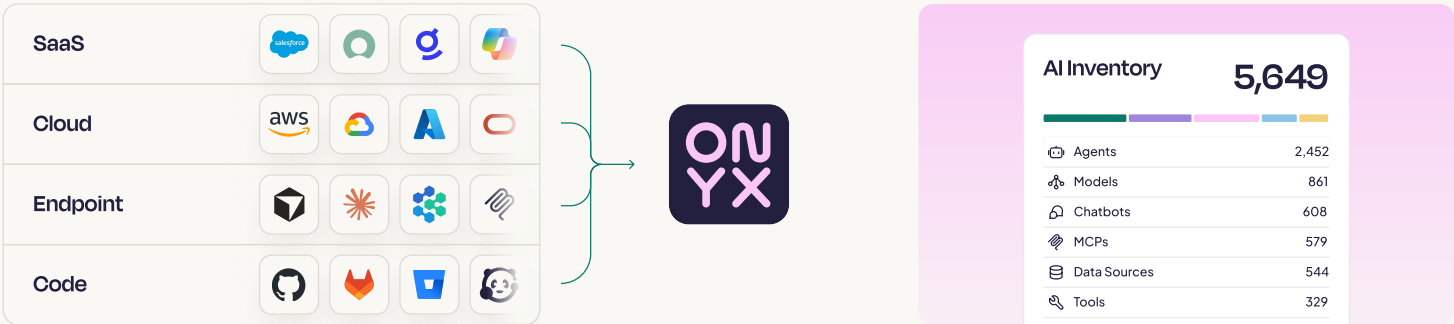
Platform Pillars

 AI Observability Discover all AI usage across the entire enterprise with comprehensive visibility into every prompt, response, and agent action.	 AI Governance Confidently meet AI security standards and regulatory requirements with built-in framework alignment and natural language policies.	 AI Security Protect AI agents and applications from threats, misuse, and vulnerabilities proactively and in real time.	 AI Orchestration Eliminate the friction of setting up AI agents and MCPs at scale, while optimizing for cost, accuracy, and latency.	 AI ROI Measure adoption, set goals, and track attainment for AI use across each department.
---	--	---	--	--

AI Observability

Full Inventory of Every AI Asset

Onyx continuously identifies all AI usage across your environment through any combination of integrations, the clientless Onyx Scanner, and the Onyx Browser Plugin, mapping ownership, access, tool usage, and risk.



AI Governance

Natural Language Policies, Automatic Enforcement

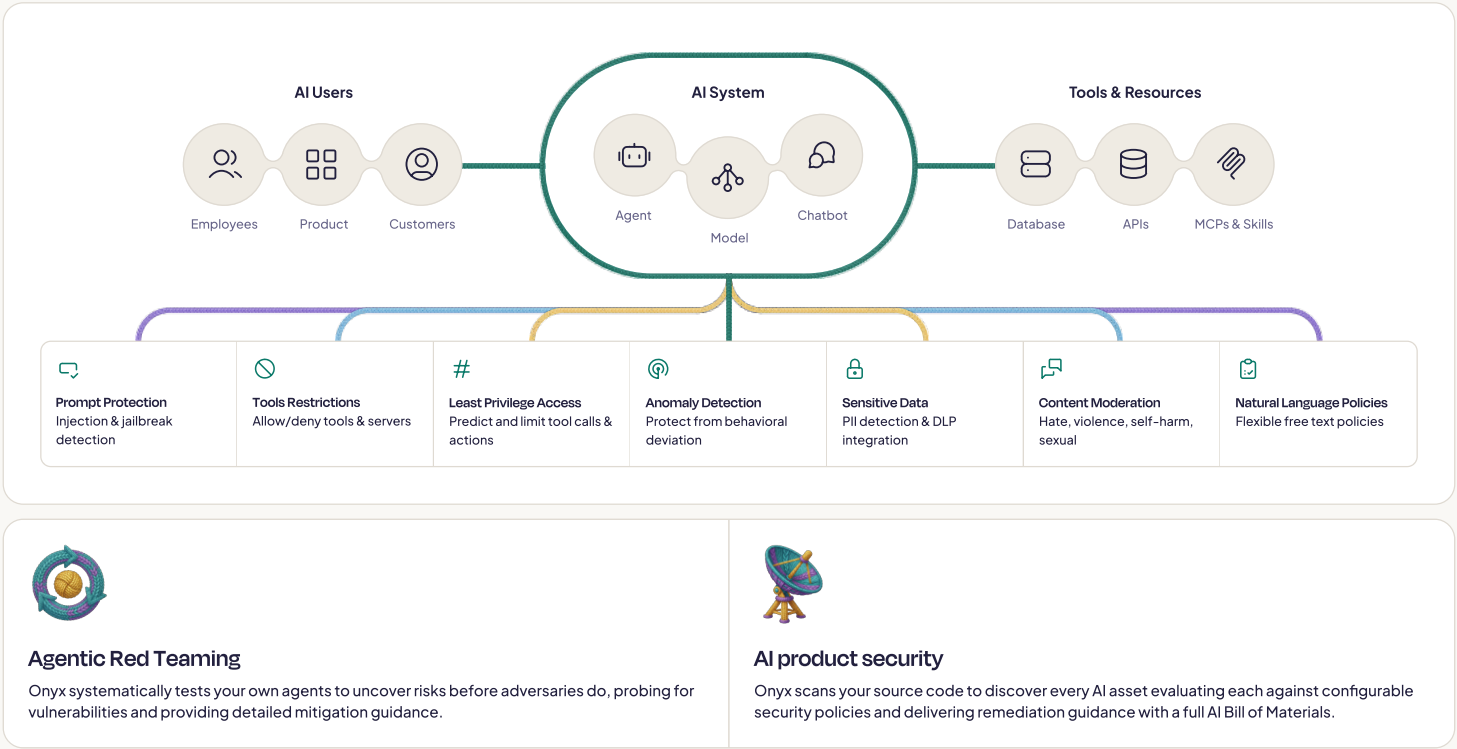
Define natural language policies that are automatically enforced for current and future AI assets, with built-in compliance framework mapping to streamline audit readiness.

 EU AI Act	 OWASP Top 10	 ISO/IEC 42001
 NIST AI RMF	 MITRE ATLAS	 Industry Specific

AI Security

Real-Time Protection for Every AI Interaction

Onyx secures your AI environment at every layer, combining real-time runtime protection with proactive defenses that surface and neutralize threats before they can be exploited.



AI Orchestration

Managed Infrastructure for AI Agents and MCPs

Reduce the friction of deploying AI agents and MCP servers with managed infrastructure and intelligent LLM routing that optimizes cost, accuracy, and latency without compromising quality.

AI ROI

Track Outcomes, Justify Investment

Track enterprise return on AI investment against measurable business outcomes with executive dashboards that make it easy to set goals, assess adoption, and track attainment for AI agent use across every department.

Get Started With Onyx

Securely adopt, manage, and govern AI agents at scale

Schedule a demo

www.onyx.security

Overview

Risk Score

Current health based on weighted signals.

4.5

Score

Medium Risk

Updated automatically from live risk metrics

Risk Over Time

Observe trends displayed over time.

Assets Over Time

Detection trends for agents, chatbots, and AI tools.

AI Autonomy Canvas

AI Agents map by autonomy and risk.

ONYX

www.onyx.security © 2026 Onyx Security