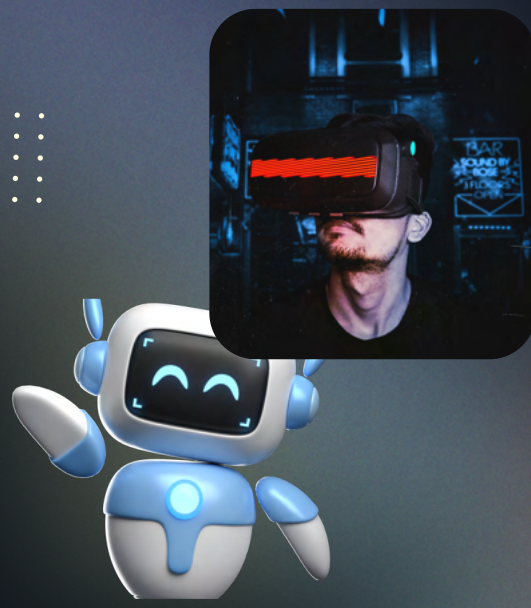
NESTRIA.AI

Securing Agentic AI Systems



Trust, Control, and Resilience for Next-Gen AI Agents

EMERGING RISKS LANDSCAPE

- Compromised tool use & unintended actions
- Chain-of-thought manipulation
- Untrusted knowledge retrieval
- Rogue agents & lateral movement
- Lack of policy traceability & visibility

As multi-agent AI systems become central to enterprise automation, they introduce new security risks:

NESTRIA.AI CORE SOLUTIONS

Multi-Agent Risk Orchestration Platform

A control tower for managing and enforcing safe AI behavior in enterprise systems.

AI Supply Chain Provenance & Integrity Scanner

Track agent logic, data & model provenance, and component versions.

Runtime Trace & Audit for AI Systems

Trace decision flows, detect manipulation, and respond in real-time.

Built for Builders. Trusted by Experts.

- Seamlessly integrates with LangChain, OpenAgents etc
- Optimized for NVIDIA, AWS, and on-prem environments
- Modular SDKs and APIs for effortless deployment
- Co-developed with leaders in Critical sectors

hello@nestria.ai
www.nestria.ai