

# Full Visibility and Control for Enterprise AI

Most organizations cannot see all the models, agents, datasets, and third-party systems operating across their environments. This creates shadow AI, untested risks, and growing compliance pressure. Cranium's AI Governance & Security platform is built for the speed, complexity, and scale of enterprise AI ecosystems, helping you to ensure that as your AI systems grow smarter, your AI guardrails grow stronger.

## The Problem

**AI is growing faster than your ability to govern it**

- Shadow AI across teams and vendors
- Models deployed without security testing
- New regulations that require ongoing proof of compliance
- Limited transparency from third-party AI suppliers

## The Solution

**One platform to discover, test, secure and verify every AI system**

- **Discover** → Detects all AI models, agents, and datasets across your enterprise and vendor ecosystem.

- **Inventory** → Auto-generate AI Bills of Materials that document ownership, purpose, and dependencies.
- **Test** → Run real-world adversarial simulations with Cranium Arena to identify vulnerabilities.
- **Remediate** → Apply and verify fixes automatically through Cranium's remediation engine.
- **Verify** → Produce AI Cards and attestations aligned with EU AI Act, NIST AI RMF, and ISO standards.
- **Share** → Create secure Trust Hubs to exchange risk and compliance data with partners.

## Why Cranium

- Built by experts behind MITRE ATLAS
- Recognized by Gartner as a Cool Vendor in AI Cybersecurity Governance
- Creator of the EU AI Act Trust and Safety Hub with KPMG and Microsoft
- Proven solution across some of the largest global enterprises in Financial Services, Life Sciences, and Telecommunications

## Business Value

- Reduce AI and supply chain risk
- Accelerate compliant AI deployment
- Improve vendor transparency
- Replace manual governance with automation
- Support safe AI adoption across all teams

 Awards and Accolades

Gartner

COOL  
VENDOR  
2025

Cranium Named in the Gartner® Cool Vendors™ for AI Cybersecurity Governance Report



Cranium was recognized by Fortune and Evolution Equity Partners as one of the Top 50 cybersecurity companies of 2025 for its leadership in digital protection and innovation.



Cranium named to CRN's 2025 Stellar Startups list, recognizing fast-rising innovators driving the future of AI security.



Recognized by TAG Infosphere as a Top Five AI Security Vendor for 2025. Trusted by enterprises to protect, monitor, and govern AI implementations across the entire AI supply chain.



Cranium Connect was named to CRN's 2025 Partner Program Guide for providing exceptional support to solution providers across the IT channel.

Gartner

Cranium was recognized by Gartner in 2025 for its leadership in AI governance, inclusion in 11 Hype Cycle reports, and contributions to transparency and oversight in embedded AI.

 See what's inside your AI.  
 Secure what matters. Scale with confidence.

Cranium HQ  
1200 Morris Tpke, Suite 3005  
Short Hills, NJ 07078  
hello@cranium.ai

