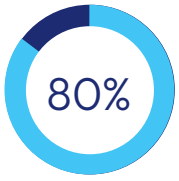
Securing the AI Revolution

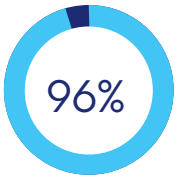
The Hidden Risks of AI

Awareness and adoption of AI solutions across organizations is skyrocketing in popularity, with generative AI (GenAI) capturing the imagination of the public. Enterprises are increasingly viewing AI as a competitive differentiator due to its potential to drive innovation, enhance customer experiences, and streamline operations, with first mover advantage being paramount. AI is being embedded into every business process, yet many enterprises remain uncertain about the security of their AI systems and lack the ability to show compliance with standards and forthcoming regulations.

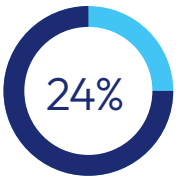
- Privacy Violations
- Data Manipulation and Bias
- Cyberattacks
- Safety Risks
- Loss of Trust
- Regulatory and Legal Consequences
- Economic Impact
- Ethical Concerns



of companies will leverage GenAI enabled systems in production by 2026



of executives say adopting AI will makes a security breach likely in their organization in the next three years



of AI projects will include a cybersecurity component in the next six months

Your Trusted AI Security Provider

Cranium is the leading enterprise AI security firm, ensuring visibility for organizations' AI and GenAI systems. With Cranium Enterprise, teams can map, monitor, and manage AI/ML environments against threats without disrupting model development and deployment.

Automatically map and visualize your AI pipelines

Increase AI regulatory awareness and alignment within your organization and with third parties

Enable secure LLM development and usage to reduce risk across your AI attack surface

Making AI Security a No-Brainer

Gain insight into the core of your AI systems, ensuring compliance, security, and trustworthiness while aligning with regulatory standards and enhancing vendor transparency. Stay ahead in the evolving compliance landscape and fortify the security and reliability of your AI systems.

Comprehensive, End-to-End Visibility

Using state-of-the-art AI, Cranium uncovers the use of AI libraries, models, and datasets to create your AI Bill of Materials (BoM). Unlike standard code analysis tools, Cranium understands the intricacies of machine learning within your code for more accuracy and understanding.

Governance & Compliance

The Cranium AI Card allows organizations to quickly gather and share information about the trustworthiness and compliance of their AI models internally as well as with supply chain, clients and regulators. Select from frameworks such as NIST AI RMF, EU AI Act, and ISO 42001 to stay on the cutting edge of the compliance landscape.

AI Attack Surface Exposure Management

Identify vulnerabilities in your AI infrastructure, ensuring the security and reliability of your machine learning applications. Supercharge red-teaming efforts to discover novel threats, inform protection strategies, and harden AI systems against known adversarial tactics and vulnerabilities to enable secure AI/LLM development and usage.

AI Risk Assessment

Cranium can help organizations build an AI system inventory and Bill of Materials (BoM) that will populate an AI Card for compliance monitoring, enable attack surface characterization and risk assessment resulting in comprehensive risk mitigation recommendations and best practices for an executive audience.

Global Financial Services Firm Case Study

Background: The CISO office at a leading global financial services firm needed more visibility into their AI processes and a more efficient way to manage the security and compliance risks associated with a new offering for their top clients.

Why Cranium? The enterprise organization deployed Cranium to identify open-source vulnerabilities, validate the data in tailoring, and continuously monitor for security threats to these AI models. Additionally, they utilized Cranium to create an AI Card, certifying the security and providing a compliance trustmark to reassure their clients that the AI in use was secure and compliant.

Get Serious About Securing Your AI

See a demo of Cranium to experience the power and peace of mind true AI security brings. **For inquiries, contact us: hello@cranium.ai**