securiti

AI Security & Governance

With the emergence of generative AI (GenAI), unsanctioned AI use has proliferated within organizations, giving rise to a multitude of risks associated with shadow AI, data privacy, and data security. The lack of governance guardrails exposes organizations to severe legal penalties, irreversible reputational damage, and significant operational inefficiencies, underscoring an urgent need for comprehensive AI oversight.

Securiti's AI Security & Governance solution empowers organizations to discover AI and institute privacy, security, and governance guardrails to drive safe adoption of AI.

It is designed to assist organizations in effectively managing and aligning the usage of their AI systems with both business needs and regulatory requirements. The solution offers features such as model inventory, model risk assessment, data and AI system mapping, data privacy and security controls, and compliance reporting to meet regulatory standards such as NIST AI RMF and the EU AI Act, among over twenty other regulations.

> "By 2026, organizations that operationalize artificial intelligence (AI) transparency, trust and security will see their AI models achieve a 50% improvement in terms of adoption, business goals and user acceptance."
>
> Gartner

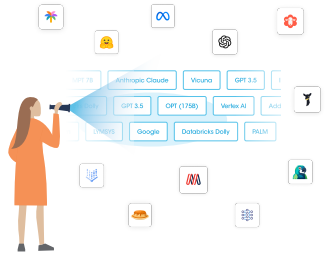
sales@securiti.ai

www.securiti.ai

5 Steps to AI Security & Governance

STEP 1

AI Model Discovery & Cataloging



Discover and catalog AI models in use, whether sanctioned or unsanctioned, across public clouds, private clouds, and SaaS applications.

STEP 2

AI Risk Management

Evaluate and classify AI models against regulatory standards and risks such as toxicity, bias, efficiency, copyright, and disinformation.

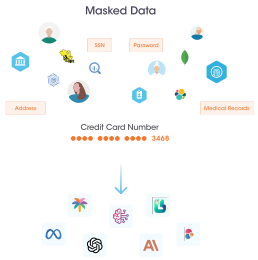
STEP 3

Data+AI Mapping

Map AI models to data sources, processes, and vendors to uncover associated privacy, security, and compliance obligations.

STEP 4

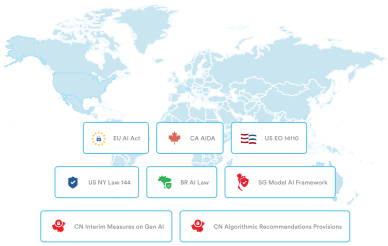
Data+AI Controls



Implement in-line data and AI controls, like LLM firewalls, to enforce security, privacy, and governance policies.

STEP 5

Regulatory Compliance



Automate compliance management and reporting for over twenty regulatory standards, such as NIST AI RMF and EU AI Act.

By adopting the outlined steps, organizations can ensure full transparency, increased risk awareness, and clarity in AI data processing, alongside robust protection for AI models and interactions. Embracing AI governance transforms regulatory obligations into growth opportunities, fostering financial gain, enhancing reputation, and facilitating informed decision-making.

Visit us online at Securiti.ai to learn more about how our platform can help you address all of your privacy compliance requirements and priorities.

sales@securiti.ai

www.securiti.ai