ARTIFICIAL INTELLIGENCE

AI Security

How We Can Help

Sayers Architects will take the time to understand your requirements and objectives to provide solution options for the following AI challenges. Sayers collaborates with top AI security vendors, offering services to overcome AI security challenges. **Contact Sayers' AI security experts today!**

AI FIREWALLS

Protect AI from malicious inputs, data, and unexpected outputs.

Prompt injection attacks are considered the most critical AI security risk.

DATA EMPOWERMENT

Prepare internal data to be utilized by AI-powered applications and identify security risks.

Data related tasks consume roughly 70% of AI Project's total time.

SHADOW AI DEFENSE

Discover and protect against unauthorized AI usage.

Cyber leaders are ranking "Shadow AI" as one of the biggest emerging threats.

DEEPFAKE DETECTION

Detect AI generated content and manipulated media.

The amount of online deep fakes is doubling every 6 months.

AI GOVERNANCE

Manage, monitor and enforce policies across diverse systems and geo-locations.

AI governance will be a mandatory requirement under all sovereign AI laws and regulations worldwide by 2027 – Gartner Predicts

AI DEVELOPMENT OPERATIONS

Streamline and secure AI development and AI fine-tuning.

74% of C-suite executives plan to customize models with proprietary data.

PEN TEST & RED TEAMING

Test the guardrails, behavior and security of AI applications/agents.

Over 10% of organizations reported breaches involving AI models or applications.

AGENT ORCHESTRATING

Create AI-powered automation and applications specialized for the client.

47% of AI using organizations develop custom internal AI tools.

sayers

sayers.com 800.323.5357

SCAN TO LEARN MORE