AI Terms Glossary

Enhanced Professional Edition

Generated with AI · 2025

AI (Artificial Intelligence)

Refers to systems capable of performing tasks that normally require human intelligence, such as reasoning, planning, perception, or decision-making. AI enables machines to adapt to new inputs and perform human-like activities in domains ranging from automation to predictive analytics.

LLM (Large Language Model)

A category of AI models trained on massive text datasets to process, understand, and generate human language. LLMs are the foundation of modern conversational AI, enabling natural interactions, summarization, translation, and code generation.

RAG (Retrieval Augmented Generation)

A hybrid approach in which an LLM retrieves information from external knowledge sources before generating responses. This method improves factual accuracy, reduces hallucinations, and is widely used in enterprise knowledge bases and secure AI assistants.

HITL (Human-in-the-Loop)

A governance model requiring explicit human validation before an AI system performs sensitive actions. HITL is critical for compliance-heavy industries such as healthcare, banking, and government, ensuring accountability and oversight.

Agentic AI

AI systems that operate autonomously or semi-autonomously, capable of making independent decisions and pursuing goals with minimal supervision. These agents adapt dynamically to changing environments, representing the future of enterprise automation.

AI Gateway

A middleware service that improves scalability, security, and performance for AI applications by providing rate limiting, caching, monitoring, and analytics. Gateways help enterprises safely integrate AI models into production environments.

NIST AI RMF

The National Institute of Standards and Technology ’ s Artificial Intelligence Risk Management Framework. It provides structured guidelines for organizations to identify, measure, and mitigate risks related to AI adoption.

OWASP Top 10 for LLMs

An industry-standard security list highlighting the ten most critical vulnerabilities specific to Large Language Model applications. It serves as a guideline for developers and enterprises to secure AI systems against threats like prompt injection and data leakage.

MAESTRO Framework

Cloud Security Alliance ’ s threat modeling framework for agentic AI systems. It defines adversarial tactics such as overriding safeguards, misusing tools, and evading monitoring to help security teams model and mitigate risks.

BYOA (Bring Your Own Agent)

A concept where individuals introduce and operate their own AI agents, typically on personal devices. BYOA raises governance and security considerations, especially in corporate and regulated environments.