By Dr. Mahadi Harris Murshidi CAIO ® MHM2026

Understanding AI Agents and Agentic AI

The Role of Obiguard

Artificial intelligence is evolving rapidly, and with it, the terminology and concepts around autonomous systems are becoming more nuanced. Two key terms often discussed are AI agents and agentic AI. While related, they represent different levels of autonomy and complexity in AI systems. Understanding this distinction is crucial for effectively governing and securing these technologies, a role that solutions like Obiguard are uniquely positioned to fulfill.

AI Agents vs. Agentic AI: Defining the Difference

AI Agents

An AI agent is a software entity designed to perceive its environment, make decisions, and act to achieve specific goals. These agents can range from simple rule-based systems to more complex autonomous programs capable of handling multi-step tasks with minimal human intervention. However, AI agents typically operate within predefined boundaries and objectives set by their developers.

Key characteristics of AI agents include goal-oriented behavior within defined parameters, reactive or deliberative decision-making, and limited or no ability to redefine their own goals or policies.

Examples of AI Agents include chatbots and virtual assistants that answer queries and guide users within scripted flows; recommendation systems like those used by Netflix or Amazon that suggest content or products based on user data; automated trading bots in financial markets executing trades based on programmed strategies and risk limits; robotic process automation (RPA) systems automating repetitive business tasks such as data entry or invoice processing; smart home devices like thermostats or lighting systems adjusting settings based on user preferences and sensors; and game AI such as non-player characters (NPCs) in video games reacting to player actions within scripted behaviors.

These AI agents excel in automating specific, well-defined tasks with predictable outcomes, improving efficiency and scalability but lacking higher-level autonomy.

Agentic AI

Agentic AI refers to AI systems that possess agency — the capacity to act independently with intentionality, self-direction, and adaptability.

To possess agency means that the AI system can make decisions and take actions on its own, rather than just following pre-programmed instructions. It can set or modify its own goals, proactively plan actions, and adapt its behavior based on experience or changing circumstances. It can evaluate its environment, anticipate future states, and make autonomous decisions aligned with broader objectives, often in complex or uncertain situations. In essence, it acts as an autonomous "agent" capable of intentional, goal-driven behavior rather than simply executing fixed commands.

Agentic AI represents a more advanced form of autonomy, often involving complex reasoning and long-term decision-making.

Key traits of agentic AI include high-level autonomy with self-directed behavior, proactive and adaptive decision-making, and the ability to operate beyond rigid, predefined rules.

Agentic AI is often found in advanced autonomous agents and multi-agent systems that interact dynamically with their environment and other agents.

A prominent example of agentic AI in action is in autonomous vehicles. Companies like Tesla and Waymo deploy agentic AI systems that use computer vision, sensor fusion, and real-time decision-making to navigate complex road conditions, recognize traffic signals and pedestrians, and plan safe driving routes without constant human oversight. Unlike earlier autonomous systems that relied on rigid mapping and predefined parameters, these agentic AI-powered vehicles continuously learn and adapt to new scenarios, demonstrating high degrees of autonomy and proactive behavior.

The Role of Obiguard: Governing Autonomy and Ensuring Safety

As AI systems become more agentic, their capacity for independent action introduces new risks, including the potential for rogue behavior — actions that deviate from intended policies, ethical standards, or regulatory requirements. This is where Obiguard plays a critical role.

Obiguard acts as a real-time policy enforcement firewall designed to govern both AI agents and agentic AI systems by monitoring and intercepting all agent actions before execution to ensure compliance with enterprise policies and regulations. It embeds adaptive guardrails that prevent unauthorized or unsafe behaviors, especially in systems capable of self-directed decision-making. It continuously assesses contextual risks and detects anomalies that may indicate rogue or malicious activity. Obiguard maintains transparent audit logs for accountability and regulatory compliance and dynamically updates policies to respond to evolving threats and operational contexts.

By embedding these layered controls, Obiguard enables organizations to harness the power of agentic AI while maintaining control, safety, and trust.

Summary

AI agents operate with limited autonomy, following predefined goals and reactive or rule-based decision-making. Agentic AI exhibits high autonomy with self-directed, proactive, and adaptive decision-making. Obiguard governs and enforces safe autonomy by intercepting and validating decisions, mitigating risks of rogue behavior, and providing real-time policy enforcement and audit.

References

Bernard Marr, "The Important Difference Between Agentic AI And AI Agents," Forbes, February 25, 2025.

MoveWorks, "Agentic AI Vs AI Agents: 5 Differences and Why They Matter," February 12, 2025.

ISACA, "AI Agents and Agentic AI: Understanding the Difference That Matters for Your Organization," August 8, 2025.

Medium, "AI Agent vs Agentic AI: Understand The Actual Difference," 2025.