Enkrypt AI Launches Ground-Breaking AI Agent Security Solution to Mitigate Risk and Non-Compliance

Innovative solution empowers organizations to build trust, ensure reliability, and drive responsible AI adoption

Enkrypt AI

BOSTON, MA, UNITED STATES, April 16, 2025 /EINPresswire.com/ -- Enkrypt AI, a pioneer in next-generation AI security, has unveiled a groundbreaking security solution that's purpose-built to safeguard autonomous AI agents. As businesses increasingly deploy AI agents to automate complex decision-making and operational tasks, Enkrypt AI offers the industry's most advanced protection against novel threats, compliance risks, and performance disruptions associated with these intelligent systems.

> Securing AI agents is complex due to their autonomy and risk amplification. Enkrypt AI ensures secure, compliant interactions—safeguarding our brand, data, and customers at every touchpoint."
>
> *Enterprise Executive at Salesforce.com*

AI agents are rapidly transforming business operations by autonomously perceiving environments, interpreting natural language commands, making decisions, and executing actions across tools and systems. Unlike traditional AI models, these agents operate with minimal oversight and exhibit dynamic, evolving behaviors—which introduces a radically different set of security challenges.

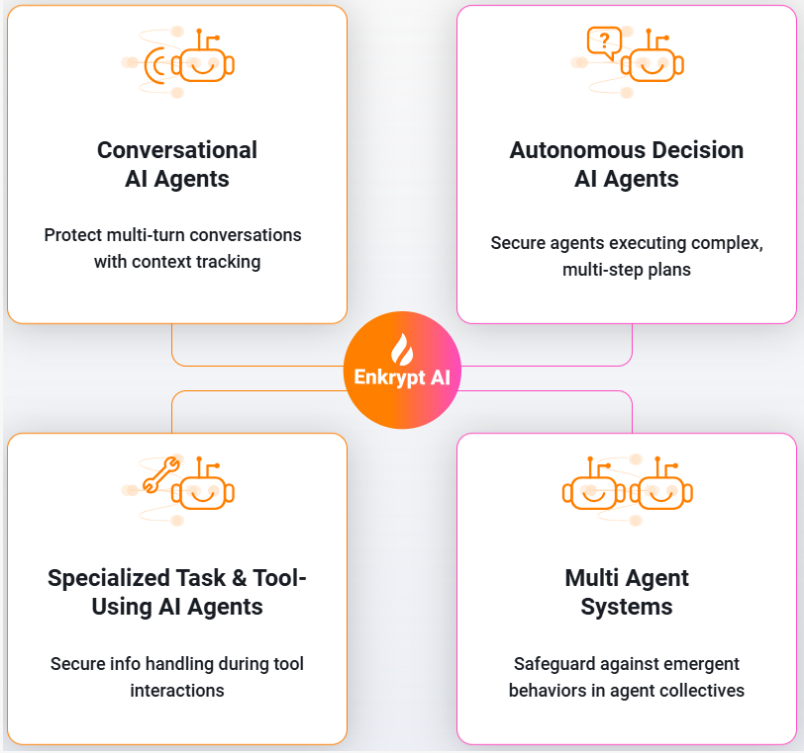
Addressing the Unique Security Risks of Agentic AI

Enkrypt AI's solution addresses the critical vulnerabilities that conventional AI security tools fail to secure:

- Prompt Injection & Tool Misuse – Agents can be manipulated via malicious language inputs or misdirected in their use of connected tools.
- Semantic Interpretation Risks – AI agents interpret intent, not just syntax, creating new attack

vectors.

- Dynamic Decision-Making – Fluid reasoning boundaries make static security controls ineffective.
- Opaque Reasoning Paths – The inability to audit agent decisions increases the risk of undetected compromises.
- Cross-System Vulnerabilities – Agents often operate across diverse environments, requiring cohesive protection strategies.



Enkrypt AI provides specialized security for all AI agent types

Purpose-Built Security for the AI Agent Era

The Enkrypt AI platform addresses the challenges above with its integrated capabilities, including:

- AI Agent Red Teaming: Simulates real-world attacks to uncover vulnerabilities in agent reasoning, tool access, and decision pathways before deployment.
- AI Agent Guardrails: Provides real-time oversight of active agents, monitoring memory manipulation, tool usage, and reasoning anomalies.
- AI Agent Monitoring: Enables post-incident recovery through forensic decision tracing, vulnerability patching, and behavior tuning to prevent future threats.

Together, these capabilities offer complete AI agent lifecycle protection—from design and deployment to runtime and recovery.

Tangible Business Benefits

Organizations deploying Enkrypt AI's agent security solution gain critical advantages, including:

- Improved Customer Confidence: Deliver trusted, secure, and responsible AI experiences that protect brand reputation.
- Automated Compliance Readiness: Meet evolving AI regulations and reduce liability exposure.
- Accelerated AI Adoption: Safely roll out secure and operational AI agents across the enterprise without costly project delays and business interruptions.

Why Enkrypt AI is Different

Unlike generic AI security or traditional IT-focused solutions, Enkrypt AI is engineered for the semantic, adaptive, and tool-integrated nature of today's agent systems. The platform secures all agent types with purpose-built defenses tailored to the threat landscape of agents and LLMs.

Differentiators include:

- AI-Native Security – Tailored security for agentic and LLM-driven systems.
- Minimal Performance Impact – Lightweight security layers that preserve agent speed and responsiveness.
- Comprehensive Ecosystem Coverage –Protects the full AI agent ecosystem, from core models to external tool integrations.
- Intent-Based Threat Detection – Understands semantic meaning to block attacks that bypass pattern-based systems.
- Advanced Behavior Modeling – Detects deviations from normal agent behavior.
- Cryptographic Agent Identity Framework – Ensures authenticity in multi-agent systems.
- Cross-Agent Communication Security – Protects inter-agent data exchange.

As one enterprise executive at Salesforce put it:
"Securing AI agents is complex due to their autonomy and risk amplification. Enkrypt AI ensures secure, compliant interactions—safeguarding our brand, data, and customers at every touchpoint."

The Future of Secure AI Agents

As enterprises accelerate their adoption of AI agents, robust security and compliance are no longer optional—they are mission-critical. Enkrypt AI's security-first approach empowers organizations to harness the full potential of autonomous AI while preserving trust, meeting regulatory demands, and ensuring safe, responsible innovation.

Learn More

Website
https://www.enkryptai.com/solutions/AI-agents

Blog
https://www.enkryptai.com/blog/securing-ai-agents-with-enkryptai

Video: Safeguarding Microsoft Pilot
https://www.youtube.com/watch?v=RyadTaVFOMM

Video: How to Secure AI travel agents
https://www.youtube.com/watch?v=7LtGnTI3Kcc

For media inquiries or more information, please contact:
Erin Swanson
Enkrypt AI
Erin@Enkryptai.com

About Enkrypt AI
Enkrypt AI is an AI security and compliance platform. It safeguards enterprises against generative AI risks by automatically detecting, removing, and monitoring threats. The unique approach ensures AI applications, systems, and agents are safe, secure, and trustworthy. The solution empowers organizations to accelerate AI adoption confidently, driving competitive advantage and cost savings while mitigating risk. Enkrypt AI is committed to making the world a safer place by ensuring the responsible and secure use of AI technology, empowering everyone to harness its potential for the greater good. Founded by Yale Ph.D. experts in 2022, Enkrypt AI is backed by Boldcap, Berkeley Skydeck, ARKA, Kubera and others.

Erin Swanson
Enkrypt AI
+1 858-472-5228
email us here
Visit us on social media:
X
LinkedIn
YouTube
