EINPRESSWIRE

Enkrypt AI Launches New Multimodal AI Security Solution to Safeguard Text, Image, and Voice AI Systems

Innovative solution secures multimodal AI systems from emerging security, bias, and compliance risks

Enkrypt AI

BOSTON, MA, UNITED STATES, March 25, 2025 /EINPresswire.com/ -- [Enkrypt AI](), a leader in AI security and compliance – is proud to announce the launch of its latest [Multimodal AI Security Solution](). As multimodal AI adoption accelerates across industries, organizations must address growing security threats and compliance challenges.

“Multimodal AI enables AI systems to process and integrate multiple data types—text, images, voice, sensor data, and video—to enhance user experience and improve decision-making,” says Sahil Agarwal, CEO and cofounder of Enkrypt AI. “However, these systems are inherently more vulnerable than traditional AI models, as they are susceptible to attacks leveraging blended input methods such as text-to-image or voice-to-text exploitation.”

> We chose Enkrypt AI to secure our multimodal AI application that turns text commands into image creatives for ads and e-commerce listings. Their expertise in safeguarding such content is exceptional.”
>
> *Akshit Raja, Co-founder & Head of AI, Phot.AI*

Why Securing Multimodal AI Matters
As multimodal AI becomes a critical component of customer support, marketing, medical diagnostics, and intelligent virtual assistants, organizations face new risks, including:

• Expanded attack surfaces – Malicious actors can manipulate chatbots with embedded voice or image-based commands, bypassing security safeguards.

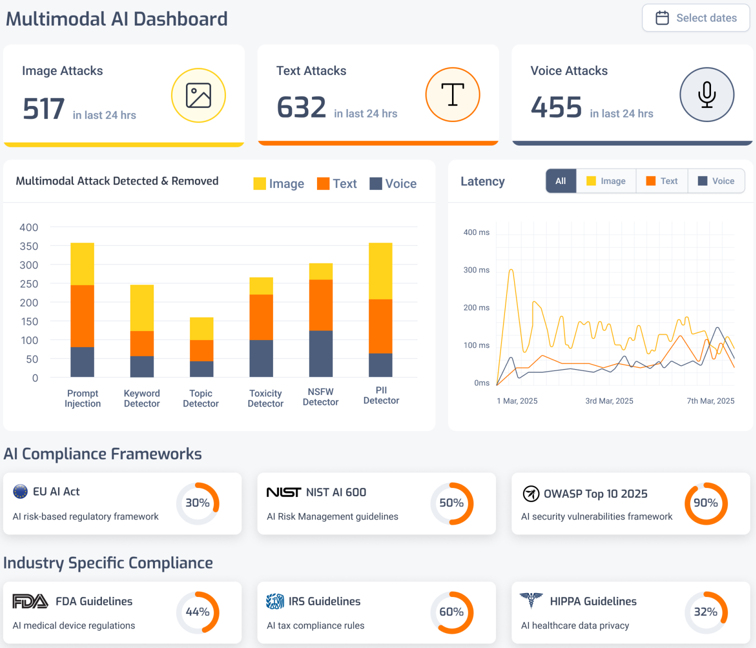
• Compounded AI bias – Bias in voice, text, and image recognition can reinforce discrimination in job recruitment, financial services, and healthcare.

• Privacy violations & data leakage – Multimodal AI applications that process voice and images risk exposing sensitive personal information.

Enkrypt AI's Multimodal AI Security: A Two-Pronged Approach
To combat these challenges, Enkrypt AI introduces a dual approach to detect and remove multimodal AI threats:

1. Multimodal Red Teaming (AI threat detection in pre-production)
o Detects malicious text, image, and voice prompts that attempt to manipulate AI responses.
o Identifies adversarial input attacks, hallucinations, and bias issues before deployment.
o Provides compliance readiness for global regulations (NIST, OWASP, EU AI Act) and industry-specific regulations (FDA, HIPAA, IRS, etc.)

2. Multimodal Guardrails (AI threat removal in production)
o Blocks harmful text, image, and voice inputs in real time.
o Provides high-accuracy, low-latency protection against security threats, bias, privacy violations, and hallucinations.
o Ensures continuous compliance with regulatory requirements and internal policies.



Multimodal AI Dashboard

Select dates

Image Attacks 517 in last 24 hrs

Text Attacks 632 in last 24 hrs

Voice Attacks 455 in last 24 hrs

AI Compliance Frameworks

EU AI Act – AI risk-based regulatory framework – 30%

NIST AI 600 – AI Risk Management guidelines – 50%

OWASP Top 10 2025 – AI security vulnerabilities framework – 90%

Industry Specific Compliance

FDA Guidelines – AI medical device regulations – 44%

IRS Guidelines – AI tax compliance rules – 60%

HIPPA Guidelines – AI healthcare data privacy – 32%

Enkrypt AI dashboard view of all multimodal AI system threats detected and removed. Breakdowns of text, image, and voice exploits are shown as well as readiness for AI compliance frameworks.

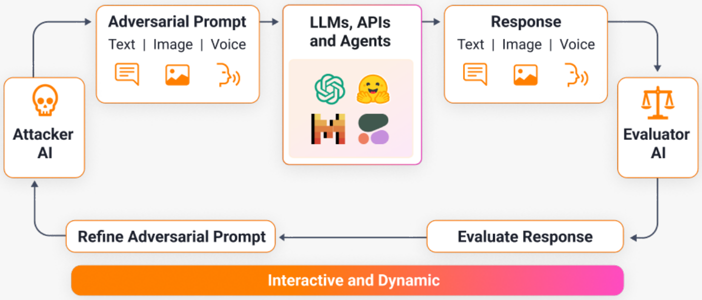


Figure 2: How Enkrypt AI Red Teaming safeguard multimodal AI systems in pre-production.

How Enkrypt AI Red Teaming safeguards multimodal AI systems in pre-production.

Enterprise Visibility into Multimodal AI Risks
Enkrypt AI offers a centralized dashboard that provides enterprises with real-time insights into detected and neutralized threats across all multimodal AI systems. Organizations can monitor security breaches, compliance violations, and AI bias issues across text, image, and voice modalities.

Proven Multimodal AI Security in Action
Companies like Phot.AI have already leveraged Enkrypt AI to safeguard their text-to-image AI applications, ensuring that AI-generated content remains secure, unbiased, and compliant.

"We chose Enkrypt AI to secure our multimodal AI application—transforming text commands into image creatives for ads and e-commerce listings. Their capability in safeguarding AI-generated text and creatives is exceptional."

— Akshit Raja, Co-founder & Head of AI, Phot.AI

The Future of Secure Multimodal AI
With increasing adoption of multimodal AI in enterprises, ensuring robust security and compliance measures is no longer optional—it is a necessity. Enkrypt AI’s security-first approach allows businesses to confidently deploy multimodal AI technologies without compromising on trust, compliance, or safety.

Learn More
- Webpage: Visit the new Multimodal AI Solutions page: https://www.enkryptai.com/solutions/multimodal-ai
- Blog: Read our latest blog post on multimodal AI security: https://www.enkryptai.com/blog/the-dual-approach-to-securing-multimodal-ai
- Videos: Watch how Enkrypt AI safeguards multimodal AI attacks on Google Gemini and IBM Granite:
  - Google Gemini: https://youtu.be/nKJn5QyIRZA
  - IBM Granite: https://youtu.be/4k9sOaa7z2U

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
Erin@EnkryptAI.com

---

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.