Enkrypt AI Publishes AI Shared Responsibility Framework: 'Why CISOs Care About Outcomes, Not Layers'

The Shared Responsibility Framework helps CISOs bridge AI model provider and enterprise responsibilities, advancing governance, visibility, and protection.

Generative AI Security: The Shared Responsibility Framework

BOSTON, MA, UNITED STATES, October 29, 2025 /EINPresswire.com/ -- AI Shared Responsibility Framework: Why CISOs Care About Outcomes, Not Layers.

The framework redefines how enterprises and model providers share accountability in AI security—urging leaders to focus less on technical layers and more on measurable business outcomes.

"In cloud security, we learned that shared responsibility doesn't mean shared blame—it means shared vigilance. Now, AI is forcing us to extend that same discipline from infrastructure to behavior. The stakes are higher, the risks are faster, and the conversations have to center on outcomes," said Merritt Baer, Chief Security Officer at Enkrypt AI.

> The conversation can't stop at shared responsibility—it has to evolve toward shared outcomes. Because in AI, it's not about who failed, but whether we prevented a bad day"
>
> *Merritt Baer, Chief Security Officer, Enkrypt AI*

Why Outcomes Matter More Than Layers

The traditional Shared Responsibility Model divides duties between model providers—responsible for training, alignment, and infrastructure security—and enterprises—responsible for governance, compliance, and prompt hygiene.

Enkrypt AI's framework builds on this by emphasizing that **CISOs are ultimately accountable for outcomes**, not which "layer" technically failed.

Merritt Baer added, “Boards don’t ask whether an incident happened in Layer 2 or Layer 3. They ask how it impacted the business, the customer, and compliance. Our framework helps CISOs shift focus from blame assignment to operational resilience.”

From Shared Responsibility to Shared Outcomes

Enkrypt AI’s platform operationalizes this shift by:
- Providing unified visibility across both model-provider and enterprise environments.
- Enforcing real-time guardrails to stop hallucinations, prompt injections, or unsafe agentic actions.
- Instrumenting outcomes, not just layers, so enterprises can measure safety, compliance, and performance in production.

The framework highlights “bad day” scenarios—such as a chatbot leaking customer data or an AI agent triggering unintended transactions—and prescribes proactive controls to prevent them.

The Bigger Picture

The AI Shared Responsibility Framework offers a pragmatic blueprint for CISOs managing risk in the generative-AI era. It clarifies accountability, aligns technical controls with business impact, and strengthens enterprise readiness for emerging AI regulations.

Download the full framework at: https://www.enkryptai.com/shared-responsibility

Shared Responsibility Contributors

The AI Shared Responsibility Framework was developed collaboratively with insights from leaders across cybersecurity, AI, and enterprise risk management.

Contributors include **Rajendra Gangavarapu** (Chief Data & AI Officer, Artigen.AI), **Amanda Hartle** (Managing Director, FiddlersTech), **Inderpreet Kambo** (CEO, Improzo), **Jagadeesh Kunda** (Co-Founder & CPO, Oleria), **Rock Lambros** (CEO & Founder, RockCyber), **Sunil Mallik** (Head of CSAE, PayPal), **Sekhar Sarukkai** (Founder & CEO, Stealth Startup), **Nishil Shah** (Engineer, Notion), **Tara Steele** (Director, Safe AI for Children), **Aditya Thadani** (VP – AI Platforms, H&R Block), **Abhishek Trigunait** (Founder, Improzo), and **Dennis Xu** (Research VP, AI & Cloud Security, Gartner).

About Enkrypt AI

Enkrypt AI is a purpose built AI security and compliance platform that helps enterprises safely deploy agents by detecting, removing, and monitoring risks such as data leakage, jailbreaks, hallucinations, and compliance gaps. Its unified platform combines red teaming, guardrails, and

compliance automation to deliver end to end protection across the AI lifecycle. Trusted by Fortune 500 companies in finance, healthcare, and insurance, Enkrypt AI was founded in 2022 by Yale PhD experts and is backed by Boldcap, Berkeley SkyDeck, ARKA, and Kubera.

Sheetal Janala
Enkrypt AI
email us here
Visit us on social media:
LinkedIn
YouTube
X
