

Trust Assurance for the Agentic Era: Rethinking Security, Safety, Governance and Audit.

AI is no longer just answering questions. It is beginning to act. As systems gain greater autonomy, connect to more data, use tools, make decisions and operate across business processes, the question of trust becomes far more complex. The risks are no longer limited to incorrect outputs or isolated technical failures. They increasingly involve how AI behaves, what it is allowed to do, and how organizations maintain control when these systems operate at speed and scale. This keynote explores what this shift means for the way organizations think about trust in AI. It will examine how emerging AI capabilities are challenging traditional boundaries between security, safety, governance and assurance and why these disciplines can no longer be treated in isolation. Through real-world examples and practical perspectives, the session will look at how the risk landscape is changing, where existing approaches may fall short, and what a more integrated model of trust will require. Most importantly, it will challenge organizations to rethink assurance itself. In an era where AI systems can continuously change, adapt and act, trust cannot be established through a policy, a one-time assessment or a periodic audit alone. It must be continuously demonstrated through how these systems are designed, governed, tested, monitored and ultimately held accountable. The question for leaders is no longer simply whether AI can be trusted. It is whether their organizations are prepared to continuously assure that trust.



Rani Kumar Rajah

Founder & CEO SecuraAI

Rani is a Global CIO Award-winning innovator and Founder of SecuraAI, a platform focused on the security, safety, governance, risk, and compliance of enterprise AI assets. She brings more than 20 years of experience across AI, cloud, and cybersecurity, including over 14 years at EY, where she led large-scale security, risk, and transformation programs for Fortune 500 clients across financial services, healthcare, life sciences, and government.

At SecuraAI, Rani has built an AI trust assurance suite spanning AI discovery, security assessments, red teaming, and safety evaluations for RAG, agentic AI, and multimodal AI systems. She also leads Project Feral, an open security research initiative focused on production-grade agentic AI systems. Its initial research examined OpenClaw to identify control gaps, remediation priorities, and emerging risks in autonomous AI.

Rani has trained more than 600 professionals in AI security and governance. She is the author of an AI architecture eBook and the creator of the OWASP Top 10 Dangers of LLMs and Agentic AI Top 10 digital comics. She is also an active contributor to OWASP and Cloud Security Alliance working groups focused on AI red teaming and controls, and a frequent speaker at ISC2 and ISACA events.

Personal Portfolio Website: <https://raniportfolio.safeeval.ai/>

LinkedIn Profile: <https://www.linkedin.com/in/ranikumarrajah/>