Trust3 AI Appoints Anish Menon as Chief AI Security Officer

SAN FRANCISCO, CA, UNITED STATES, August 3, 2026 /EINPresswire.com/ -- Trust3 AI, the control plane for Agent and Data security, today announced the appointment of Anish Menon as Chief AI Security Officer (CAISO). Menon will lead Trust3 AI's AI security strategy, contribute to product direction, and work with enterprise security leaders to address the rapidly expanding risks created by autonomous AI agents.

> AI security means securing the entire agent system: code, identity, permissions, tools, data access, and runtime behavior, so enterprises can move agents into production without losing control."
> *Anish Menon, Chief AI Security Officer, Trust3 AI*

Menon brings more than 14 years of experience building security systems at Netflix, Apple, and Qualcomm. His expertise spans security architecture, authentication, authorization, cryptography, device trust, digital rights management, threat modeling, and secure software development.

At Netflix, Menon helped advance security architecture for large-scale consumer and content platforms, including initiatives supporting password-sharing controls and Netflix Preview Club. He also pioneered the use of generative AI to accelerate threat modeling and improve how security teams identify and remediate vulnerabilities. Menon presented this work at RSAC 2026 in a session titled "Accelerating Threat Modeling with GenAI: Netflix's Journey." RSAC Conference

Previously, Menon led security engineering efforts supporting the expansion of Apple TV+ across non-Apple devices. Earlier in his career at Qualcomm, he worked on foundational platform security technologies, including cryptographic software, Secure Boot, Image Authentication, disk encryption, and TrustZone.

"AI agents are becoming active participants in enterprise systems. They access sensitive data, invoke tools, write code, and execute business processes with growing autonomy," said Balaji Ganesan, CEO and Co-Founder of Trust3 AI. "Anish understands security from the silicon layer to large-scale cloud platforms and now AI systems. That combination is rare. His appointment strengthens our mission to give enterprises visibility and control over every agent action and data interaction."

As CAISO, Menon will work across Trust3 AI's product, engineering, research, and go-to-market organizations. His responsibilities will include:

- Defining Trust3 AI's enterprise Agent security strategy
- Advancing security across the AI lifecycle, from development through production
- Strengthening agent identity, authorization, observability, and threat-modeling capabilities
- Helping customers establish practical security architectures for autonomous agents
- Developing security research and reference architectures for AI agents, MCP servers, tools, and enterprise data
- Working directly with CISOs, CIOs, and security teams on production AI deployments
- Representing Trust3 AI in industry forums and security research initiatives

"AI security cannot be reduced to scanning a model or placing another filter around a prompt," said Menon. "The real challenge is securing the complete system: the agent's code, identity, permissions, tools, data access, and behavior at runtime. Trust3 AI is building the security architecture enterprises need to move AI agents from prototype to production without losing control."

Menon is an IEEE Senior Member and has served as a co-editor of the IEEE Silicon Valley FeedForward publication. He has also evaluated emerging technology as a judge for the Global Recognition Awards and Stanford TreeHacks. In 2025, he was recognized as an Indian Achievers' World 40 Under Forty honoree for his contributions to security architecture and innovation.
Indian Achievers' Forum

His appointment comes as Trust3 AI expands its platform across both build-time and runtime security. At build time, Trust3 AI helps identify exposed secrets, insecure configurations, vulnerable dependencies, and risks within agent and MCP development environments. At runtime, the platform continuously discovers agents, observes their behavior, traces identity and activity across systems, and enforces enterprise data authorization for every agent interaction.
"Security teams need more than a list of AI risks. They need a control plane that can discover what is running, understand what it is doing, and enforce what it is allowed to access, added Ganesan. "Anish will play an important role in turning that vision into practical security outcomes for our customers."

About Trust3 AI

Trust3 AI provides one control plane to secure AI from build time to runtime while enforcing enterprise data authorization across any AI platform. Built on more than a decade of enterprise authorization experience, Trust3 AI helps organizations discover every AI agent, observe its behavior, and control how it accesses sensitive data and tools.
Trust3 AI enables enterprises to accelerate AI adoption while maintaining security, accountability, and control across Snowflake, Databricks, Microsoft, AWS, Google Cloud, Salesforce, and other enterprise platforms.

To learn more, visit https://trust3.ai

Media Contact
Angela Chen

Angela Chen
Trust3 AI
+1 510-413-7300
email us here
Visit us on social media:
LinkedIn
