

CAIO Connect Podcast: Zscaler's Swamy Kocherlakota Tells Host Sanjay Puri That AI Security Must Focus on Intent

On the CAIO Connect Podcast, Zscaler's Swamy Kocherlakota told host Sanjay Poonen that AI security must evolve as agents reshape enterprise risk.

LAS VEGAS, NV, UNITED STATES, June 15, 2026 /EINPresswire.com/ --

Speaking with host [Sanjay Puri](#) on the [CAIO Connect Podcast](#) at Zenith Live in Las Vegas, [Dr. Swamy Kocherlakota](#), Executive Vice President of Agentic AI

Engineering at Zscaler, said organizations must rethink cybersecurity for the age of AI agents. He warned that traditional security practices are no longer enough as autonomous systems become a bigger part of enterprise operations.



“

Companies that allow the Chief AI Officer and CISO to work together will leapfrog others in the AI race.”

Swamy Kocherlakota

During the conversation on the CAIO Connect Podcast, Kocherlakota explained why he moved from leadership roles at major financial institutions to Zscaler. He said years of working with artificial intelligence showed him that security was often treated as an afterthought. At Zscaler, he now leads teams focused on using AI to defend against AI-powered threats. According to Kocherlakota,

customer conversations over the past few months have confirmed that CIOs, CISOs, and Chief AI Officers are struggling to roll out AI safely while maintaining innovation and business growth. One of the key themes discussed by host Sanjay Puri and guest Swamy Kocherlakota on the CAIO Connect Podcast was accountability in an AI-driven world. As companies deploy autonomous agents, questions are emerging about who is responsible when something goes wrong. Kocherlakota said the ultimate responsibility still rests with Chief Risk Officers and Chief Information Security Officers, who must create policies and enforce governance. However, he noted that AI introduces new challenges because agents can act independently, making it critical to build systems that understand intent and follow organizational policies.

Kocherlakota also addressed the growing impact of advanced AI tools such as Anthropic's Project Mythos, which can identify large numbers of software vulnerabilities. He said many organizations already struggle to fix known security weaknesses and that AI is making the challenge more urgent. While AI can help identify and repair vulnerabilities, it also enables attackers to find and connect weaknesses much faster than before. Rather than relying only on patching systems,

Kocherlakota argued that organizations

should adopt Zero Trust architectures that make applications and infrastructure invisible to unauthorized users. "Make yourself disappear, especially to the people you don't want to appear to," he said during the CAIO Connect Podcast discussion.

The interview also focused on the rise of shadow AI and shadow agents. Kocherlakota said employees are increasingly using AI tools whether companies approve them or not. Because AI services are easy to access through everyday web traffic, organizations need visibility into how employees and systems are using them. He advised Chief AI Officers and CIOs to establish clear controls while allowing responsible innovation. He also highlighted risks surrounding Model Context Protocol (MCP) technology, which allows AI agents to access tools and services. Without proper governance, unauthorized tools, prompts, and skills could expose organizations to new security threats.

Looking ahead, Kocherlakota told CAIO Connect Podcast host Sanjay Puri that the partnership between Chief AI Officers and CISOs will become one of the most important relationships inside modern enterprises. He believes future security leaders must understand applications, infrastructure, AI models, and business goals while remaining open-minded and collaborative. As AI becomes embedded across organizations, the mission of security teams is expanding from protecting networks to protecting both data and AI systems. According to Kocherlakota, companies that align their AI and security strategies will be best positioned to gain a competitive advantage while managing the risks that come with the next wave of enterprise AI adoption.

Upasana Das

Knowledge Networks

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[Facebook](#)

[YouTube](#)



This press release can be viewed online at: <https://www.einpresswire.com/article/919776511>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something 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.

© 1995-2026 Newsmatics Inc. All Right Reserved.