CAIO Connect Podcast: Zscaler’s Dhawal Sharma Says AI Security Must Shift to Intent-Based Governance with Sanjay Puri

Zscaler EVP Dhaval Sharma told the Chief AI Officer Podcast that AI security must shift to intent-based governance as autonomous agents reshape enterprise risk.

CAIO Connect Podcast

LAS VEGAS, NV, UNITED STATES, June 15, 2026 /EINPresswire.com/ -- Speaking on the CAIO Connect Podcast at Zenith Live, Zscaler Executive Vice President of Product Strategy Dhawal Sharma outlined how enterprises must rethink cybersecurity in the age of AI agents, arguing that traditional security models are no longer sufficient for autonomous systems. In a conversation with CAIO Connect Podcast host Sanjay Puri, Sharma discussed the rapid evolution of AI-driven security challenges, the rise of agentic AI, and why organizations need to adopt intent-based governance frameworks to manage emerging risks. Sharma, who has spent more than 14 years at Zscaler and helped build several of the company's flagship products, including Zscaler Private Access, said AI is fundamentally changing how enterprises approach security. "Traditionally, we have done policies based on defined patterns and signatures," Sharma said on the CAIO Connect Podcast. "With AI, you need to do intent-based policy. You need to understand why an agent was created and whether it is performing the task it was designed to do."

> “The question today is not how to block AI. It's how to enable AI securely.”
>
> *Dhawal Sharma*

According to Sharma, one of the biggest challenges facing chief AI officers and CISOs is the emergence of autonomous AI agents that can operate independently of human users. Historically, governance frameworks have focused on human identities and user permissions. AI agents, however, can act autonomously, creating a need for new identity, access, and monitoring mechanisms. Speaking with Sanjay Puri, Sharma said organizations must establish clear guardrails around agent permissions, responsibilities, and access to corporate data. He also emphasized the growing importance of cost governance as enterprises scale AI deployments.

"You can burn through tokens in half a month for what used to be an annual budget," Sharma noted, urging organizations to match model size and complexity to specific business problems rather than defaulting to large frontier models.

Dhaval Sharma, Executive Vice President of Product Strategy at Zscaler with Sanjay Puri, President of CAIO Connect

A significant portion of the discussion focused on the rise of "shadow AI"—unauthorized AI tools and applications used across enterprises. Sharma said organizations are increasingly struggling to understand where AI systems are operating, what data they can access, and how they connect to internal infrastructure. "Security leaders need visibility not just into AI assets, but into everything those AI systems connect to," Sharma said. He warned that AI systems often extend deep into enterprise environments through SaaS platforms, cloud services, endpoints, and developer workflows, making visibility and inventory management critical. Among the recommended safeguards, Sharma highlighted AI-specific gateways, cloud traffic controls, and stronger governance over Model Context Protocol (MCP) connections that enable AI systems to interact with external tools and services.

The CAIO Connect Podcast discussion also explored Zscaler's work with frontier AI developers, including Anthropic and OpenAI, through cybersecurity evaluation programs. Sharma revealed that advanced AI models are already capable of identifying thousands of software vulnerabilities, significantly reducing the time required for security assessments. However, the same capabilities can benefit attackers. "The window between vulnerability discovery and exploitation is shrinking rapidly," Sharma said. Beyond identifying vulnerabilities, modern AI systems can chain multiple weaknesses together to create sophisticated attack paths in seconds a task that previously required highly skilled security researchers. To address this reality, Sharma argued that enterprises should shorten patching cycles and adopt Zero Trust architectures that hide vulnerable infrastructure from external attackers. "Attackers can't attack what they can't see," he said.

During the conversation, Sanjay Puri asked Sharma about the evolving relationship between chief AI officers and chief information security officers. Sharma said the two roles are becoming increasingly interconnected as organizations attempt to balance AI innovation with security and regulatory compliance. He noted that frameworks such as the European Union's AI Act and the U.S. National Institute of Standards and Technology (NIST) AI guidance are pushing enterprises toward more formal governance structures. Rather than acting as a "department of no," Sharma said modern CISOs are increasingly focused on enabling secure AI adoption. "The question today is not how to block AI," Sharma said. "It's how to enable AI securely." Appearing on the CAIO

Connect Podcast, Sharma concluded that while AI introduces new risks and attack surfaces, organizations that combine robust governance, continuous security testing, and Zero Trust principles will be best positioned to safely unlock AI's transformative potential.

Upasana Das
Knowledge Networks
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
