Zscaler Founder Jay Chaudhry Tells CAIO Connect Podcast Host Sanjay Puri Why AI Demands a New Security Playbook

On the CAIO Connect Podcast, Jay Chaudhry told host Sanjay Puri that AI is reshaping cybersecurity, making zero trust and proactive defense essential.

CAIO Connect Podcast

Jay Chaudhry, Founder and CEO of Zscaler with Sanjay Puri, President of CAIO Connect

WASHINGTON, DC, UNITED STATES, June 22, 2026 /EINPresswire.com/ -- During a recent episode of the CAIO Connect Podcast, host Sanjay Puri spoke with Jay Chaudhry, Founder and CEO of Zscaler, about the rapid rise of artificial intelligence and its impact on cybersecurity. The discussion focused on AI-powered threats, the growing challenge of software vulnerabilities, and the security strategies organizations need to adopt. Speaking on the CAIO Connect Podcast platform, Chaudhry described AI as a transformational force that is moving faster than any previous technology wave and forcing businesses to rethink how they protect their digital environments.

Chaudhry compared the AI revolution to major technological shifts such as the internet, cloud computing, and mobile technology. However, he argued that AI is even more significant. He called it a “giga wave” because it is changing applications, business processes, and security at an unprecedented pace. While earlier technology revolutions unfolded over years or even decades, AI continues to evolve every week. According to Chaudhry, this rapid innovation creates pressure on CEOs, CIOs, CISOs, and Chief AI Officers to move faster and stay informed about new developments.

One of the key topics discussed on the CAIO Connect Podcast was Project Mythos, an advanced AI system designed to uncover software vulnerabilities. Chaudhry explained that Zscaler gained

> AI is not even a megawave; it's a gigawave."
>
> *Jay Chaudhry*

early access to the technology through the Glasswing program and used it to test its own infrastructure. The results revealed a large number of vulnerabilities hidden in applications, operating systems, and open-source software. While he praised Mythos for its capabilities, Chaudhry warned that organizations already struggle to fix existing security issues. AI-powered tools can identify many more weaknesses, but security teams often lack the resources to patch everything. As a result, companies must focus not only on finding vulnerabilities but also on reducing the likelihood and impact of breaches.

To address these challenges, Chaudhry outlined several practical security measures. First, he urged organizations to hide critical applications behind a zero-trust architecture rather than exposing them directly to the internet. He argued that traditional firewalls create attack surfaces because they remain visible to attackers. Zscaler's approach places applications behind a secure exchange that verifies users before granting access. "If they can't reach you, they can't breach you," Chaudhry said. He also emphasized the importance of limiting lateral movement within networks so attackers cannot easily access sensitive systems after compromising a device or user account.

Chaudhry also highlighted the growing value of deception technology. These systems create decoy assets, often called honeypots, that attract attackers and immediately alert security teams when someone interacts with them. Zscaler offers this capability through its deception platform, which can even create fake AI models to lure threat actors. According to Chaudhry, organizations can deploy these defenses quickly and at relatively low cost. He believes deception technology provides an effective way to detect intruders before they reach mission-critical applications or sensitive corporate data.

The conversation concluded with a look at the future of AI agents. Chaudhry predicted that employees could soon work alongside dozens or even hundreds of AI agents. While these digital workers can improve productivity, they also introduce new security risks. He warned that compromised agents could operate at machine speed and cause significant damage. To address this challenge, Zscaler is extending its zero-trust exchange model to AI agents, enabling organizations to enforce policies, monitor communications, and control access between agents, applications, and data sources. In his closing remarks on the CAIO Connect Podcast with Sanjay Puri, Chaudhry encouraged Chief AI Officers to drive change aggressively, launch focused AI projects, and help their organizations adapt to a rapidly evolving technological landscape.

Upasana Das
Knowledge Networks
email us here
Visit us on social media:
LinkedIn

Instagram
Facebook
YouTube
X
