# Zscaler Innovation Chief Nathan Howe Warns of Machine-Speed Threats on CAIO Connect Podcast with Sanjay Puri

*Zscaler's Nathan Howe warns on the Chief AI Officer Podcast that AI threats move at machine speed, requiring immediate zero trust isolation over patching.*

CAIO Connect Podcast

WASHINGTON, DC, UNITED STATES, June 12, 2026 /EINPresswire.com/ -- The era of leisurely patch cycles and perimeter-focused cybersecurity is officially over, replaced by a landscape where vulnerabilities are weaponized at machine speed. Speaking with the host of the CAIO Connect Podcast, Sanjay Puri, at the Zenith Live conference at the Fontainebleau Resort, Nathan Howe, Zscaler's Global Vice President of Innovation, warned that artificial intelligence has radically altered the offensive cybersecurity landscape. The traditional methods of treating digital risks are failing because software engines can now orchestrate multi-layered attacks in mere seconds, forcing organizations to rethink how they defend their applications, users, and emerging AI technologies.

> The industry still hasn't answered a fundamental question: should an AI agent inherit your identity, or should it have an identity of its own? ”
>
> *Nathan Howe*

Howe highlighted this dramatic shift by pointing to Project Glasswing and the release of Mythos, an AI framework developed with Zscaler's involvement. While human security researchers traditionally take months to find and validate a few vulnerabilities, Mythos can uncover hundreds of flaws instantly. Remarkably, the AI does not just flag a bug; it automatically builds a duplicate copy of the target application, runs test exploits against the replica to gather intelligence, and then executes the final attack. Howe emphasized that this level of rapid automation means organizations can no longer rely on prioritizing only "critical" flaws while leaving lower-level risks unaddressed.

This compression of the exploit timeline leaves Chief Information Officers (CIOs) and Chief AI

Officers (CAIOs) facing an impossible hurdle: a severe lack of resources to patch vulnerabilities as fast as AI discovers them. Howe's advice to overwhelmed executives is to step back from the endless patching cycle and return to fundamental cybersecurity hygiene. He noted that businesses must first gain comprehensive visibility into their digital footprints because you cannot protect what you do not know. Once an inventory is established, organizations must immediately pull unnecessary assets offline and implement granular segmentation to limit lateral movement.

Nathan Howe, Zscaler's Global Vice President of Innovation with Sanjay Puri, President of CAIO Connect

This strategy is particularly vital for industries managing legacy systems that are impossible to patch, such as old Windows 98 machines still operating critical production lines in manufacturing plants. Rather than trying to update obsolete software, Howe stated that enterprises must isolate these systems entirely. This approach is the core tenet of zero trust architecture, a framework championed by Zscaler CEO Jay Chaudhry. Under a true zero trust model, the concept of a shared network is entirely eliminated. Instead, no application, user, or automated agent is permitted to communicate until it clears strict stages of contextual authorization and access control.

The explosive rise of autonomous AI agents introduces another complex layer to this governance challenge. As these short-lived, ephemeral agents continuously spin up and down to perform tasks, the tech industry is struggling to determine their digital identities. Howe argued that AI agents should possess distinct identities separate from their human creators to maintain proper auditability and accountability. However, managing these rapid identity cycles remains a massive computational hurdle. Furthermore, Howe noted that effective agent governance is severely hindered by the fact that most modern companies have still not successfully achieved full data classification across their corporate ecosystems.

Looking ahead, Howe expects the underlying architecture of software-as-a-service (SAS) and corporate applications to naturally adapt to these AI risks, much like the cloud did over the past two decades. While the cybersecurity industry continues to debate emerging protocols like the Model Context Protocol (MCP) for connecting AI systems, Howe urged leaders to remain focused on establishing a single, unified control platform. Ultimately, managing machine-speed risks requires organizations to transition away from fragmented, piecemeal security tools. Success will belong to enterprises that can successfully apply a centralized zero-trust policy across every asset, from corporate users and cloud workloads to autonomous robots and cellular-enabled

devices.

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

---