

Thursday, August 20

11:00 AM - 11:20 AM

Securing AI where it executes: the rise of the endpoint agents

Jeff Worthington

Executive Strategist

CrowdStrike

Abstract:

Powerful, computer-use agents like Claude Code, OpenAI Codex, and OpenClaw have transformed the endpoint into a critical control plane for AI security. These agents can inherit full permissions of their users, autonomously act, and take high risk actions that never cross network boundaries, like running terminal commands and modifying local files. Attend this talk to learn how to assess and defend the agentic blast radius on the endpoint.