

Think Outside the Box, Deploy Inside It: AI Agent Control via Infrastructure

- **Speaker:** Priya Ananthasankar
 - * **Room:** CC 236
 - * **Time:** Sun 11:20 am – 11:50 am
- **Format:** Lecture (30 Min + Q&A)
 - * **Difficulty:** Introductory / Some experience required
 - * **Track:** Development & Dev Tools
 - * **Additional Tags:** DevOps, AI / ML, Creative
 - * **Presenter Location:** In-person
 - * **Experience:** several-th time speaking

Description:

What's the balance between giving AI agents enough autonomy to be useful and keeping them under control? This session explores that tension through a practical experiment: deploying the **same AI agent** across progressively more constrained environments and observing how its behavior changes.

Priya walks through three stages:

- **Unrestricted deployment** — watching how an unconstrained agent explores and behaves
 - * **Tightened constraints** — limiting environment, permissions, or resources and analyzing the impact
 - * **Minimal guardrails** — identifying the smallest set of controls needed to ensure safety, reproducibility, and reliability without killing creativity

Through concrete examples, attendees will discover:

- How much freedom an agent actually needs to stay useful
 - * How far you can lock things down before losing value
 - * Where the real control points live — and why control is about *channeling* creativity, not caging it

This talk blends infrastructure, DevOps, and AI agent design to show how deployment environments shape agent behavior as much as model architecture.

Target Audience:

- Cloud engineers
 - * DevOps engineers
 - * Infrastructure engineers
 - * AI practitioners

From:

<https://wiki.livingcartoon.org/> - **Living Cartoon Company**

Permanent link:

https://wiki.livingcartoon.org/events/lfnw_2026_ai_agent_control

Last update: **2026/04/20 21:42**

