PARTICIPATION BUSINESS CASE · TO FORWARD TO YOUR TEAM LEAD

DevOpsCon New York 2026

Why we shouldn't skip this edition

September 28 – October 2, 2026 · New York City · DevOps · Platform Engineering · AI

In Short

This is the edition where agentic AI stops being a side experiment and becomes part of the platform. DevOpsCon New York 2026 debuts a dedicated **AI Platform Engineering Day** — at exactly the moment when we're deciding how AI agents should interact with our pipelines, our internal platform, and our production clusters.

For me: After DevOpsCon, I'll come back with a concrete, governed playbook for integrating AI agents into our delivery pipeline and platform safely.

For the team: We'll be able to adopt agentic DevOps deliberately, capturing the speed gains without the risks in security, cloud-cost and "DevOps debt" that hit teams who bolt agents onto unfinished automation.

The ask: I'd like to attend, and I'm asking for approval of the ticket, travel and accommodation.

Topics: Besides the AI Platform Engineering Day, the Conference will cover the following topics:

- Agents as new users and what to consider
- Agents as security risks and the guardrails required to control them
- How to properly introduce AI to the delivery pipeline
- Embedded governance and how it can speed up delivery

Five themes run through the program — each addressing a pressing question in DevOps right now. The summary below shows why each theme is relevant this year and the sessions that help answer the questions..

What the Team Gets from It

The value doesn't stay at the conference — it comes back into the team:

- A prioritized recap mapped to our pipelines, platform and clusters.
- An internal tech talk that passes the agent-safety, governance, and observability patterns to the whole team.
- A shared "agentic DevOps" adoption plan: sandbox → shadow → gated.
- **Session recordings:** available for months afterward, so we can reference them whenever a project needs them.

1 Finish the Platform Before You Agentify it — the AI Platform Engineering Day

This year's hard lesson: a platform needs to be deterministic and observable *before* you add a non-deterministic AI agent. Otherwise, teams risk ending up "moonwalking"— looking like they advance while fragility quietly piles up. DevOpsCon's first-ever **AI Platform Engineering Day** is built around exactly that shift: from "adding AI features" to running platforms where humans and agents are first-class participants.

After the day's Opening, we'll dive into *The Leader's Role in Orchestrating AI-Native Platforms* and a practitioner Roundtable on responsible scaling. *Moonwalking the DevOps* names the antipattern directly, while *Every Eng a CTO* shows how engineers can gain leverage by orchestrating agents instead of doing the routine work by hand.

> **Bottom line:** *Finish the fundamentals first. Teams that agentify an unfinished platform risk having every apparent step forward slide them back.*

2 An Internal Platform that's Safe for Agents

Our IDP was built for humans who pause at confirmation steps. Agents don't: they act on "success-shaped" responses and can skip the safeguards. That means that a platform that's fine today can be driven into runaway provisioning tomorrow. The fix is machine-checkable contracts: explicit state machines, intent tokens, and full lineage.

Your IDP Has a New User. It Wasn't Designed for Them walks through the failure modes and their fixes. *The End of Documentation* shows an MCP-based "living" platform where agents query machine-readable context instead of guessing, with an intent-trace on every action.

> **Bottom line:** *Agents are a new class of user: give them explicit contracts and full lineage, or a single misconfiguration can propagate across every tenant at machine speed.*

3 The new AI Attack Surfaces

Every AI agent and MCP server introduces a new attack surface, and self-adapting "rogue" agents can widen the blast radius. These sessions treat agents as first-class security risks and focus on the zero-trust controls needed to contain them.

Session	What it shows
Agents and MCP Servers: Are the Electric Sheep Safe?	MCP endpoints as a supply-chain pivot; mTLS, isolation and provenance checks at the boundary.
When AI Loses Context: A Zero Trust Blueprint for AI Agents in Kubernetes	Just-in-time ephemeral credentials and a "Two-Brain" pattern that routes every destructive write through human approval.
AI Broke AppSec — Rethinking Security in the Mythos Era	Risk-based triage for AI-amplified code churn; provenance metadata on every generated artifact.
Zero to AI-Ready in One Day: Securing Citizen Development & Agentic AI	Tiered profiles, sandboxing and prompt-injection prevention for low-code and citizen developers.

> **Bottom line:** *One agent with a long-lived credential and no write gate can cause damage at machine speed. The guardrails are cheap; the incident is not.*

4 AI in the Delivery Pipeline: Velocity Without the Debt

AI generates more changes, faster shifting the bottleneck to validation and release risk, while the promises of AIOps outrun reality. These sessions show the controlled path: measurable risk-scoring, validation that keeps pace with delivery, and provenance controls that prevent speed from turning into rollbacks.

Session	What it shows
What 105 Research Papers Got Wrong About AIOps	A five-level maturity model and vendor-vetting checklist; run auto-remediation in shadow mode before trusting it.
AI-Accelerated Delivery: Predicting Release Risk Before Production	Score every release from commit, churn and test signals; gate risky ones into canary rollout and human review.

Session	What it shows
The Bottleneck in AI-Driven Delivery: Scaling Validation	Masked production data, synthetic data and agentic testing to keep validation inside the sprint.
Don't Let AI Become Your Next Source of DevOps Debt	Shift software-composition and provenance checks left, onto AI-generated code as it is written.

> **Bottom line:** *Faster code only pays off if validation and risk-scoring keep pace. Otherwise, "velocity" just means more rollbacks.*

5 Govern It and See It: Compliance, Supply Chain & Observability

Regulated delivery, agentic pipelines and agent-driven change all require built-in governance and visibility from the start. one right, those embedded controls speed up delivery:

Session	What it shows
Governed by Design	Embedded CI/CD controls and observability cut release time by 55% and compute cost by 40% in a regulated Microsoft data platform.
Compliance-Driven CI/CD Pipelines	Policy-as-code gates, artifact lineage and content-addressable storage make compliance intrinsic.
Endless Runner — Agentic Pipelines for an OS Supply Chain	Sigstore signing and SLSA Level 3 verification, with human-in-the-loop escape hatches.
Seeing the Invisible — Microservices Observability:	OpenTelemetry and Linkerd tracing so agent-driven changes stay debuggable and reversible.

> **Bottom line:** *Embedded governance isn't a tax on delivery. One team cut its release time in more than half while gaining control instead of losing it.*

Also on the program: Hands-on Kubernetes, Open-Source-AI bootcamps and DevOps/DevSecOps workshops. There is room to go deeper where it counts.

Sources

All sessions are from the DevOpsCon New York 2026 program (September 28 – October 2, 2026, New York City):

- Welcome & Opening Keynote of DevOpsCon New York 2026
- Opening of the AI Platform Engineering Day
- The Leader's Role in Orchestrating AI-Native Platforms
- Roundtable at the AI Platform Engineering Day
- Moonwalking the DevOps: When Every Step Forward Slides You Back
- AI Broke AppSec — Rethinking Security in the Mythos Era
- Zero to AI-Ready in One Day: Securing Citizen Development & Agentic AI
- What 105 Research Papers Got Wrong About AIOps
- AI-Accelerated Delivery: Predicting Release Risk Before Production
- The Bottleneck in AI-Driven Delivery: Scaling Validation

- Every Eng a CTO: Technical Leverage in the Agentic Organization
- Your IDP Has a New User. It Wasn't Designed for Them
- The End of Documentation: An MCP-Based "Living" Platform
- Agents and MCP Servers: Are the Electric Sheep Safe?
- When AI Loses Context: A Zero Trust Blueprint for AI Agents in Kubernetes
- Don't Let AI Become Your Next Source of DevOps Debt
- Governed by Design: Embedded CI/CD Controls (55% Release-Time Cut)
- Compliance-Driven CI/CD Pipelines for Cloud-Native Delivery
- Endless Runner: Agentic Pipelines for an OS Supply Chain
- Seeing the Invisible: Microservices Observability

Program: devopscon.io/new-york