WSO2CON NORTH AMERICA

May 20 - 22, 2026 | Austin, Texas, USA

AI-Native Platforms: Accelerating Software Development, Delivery, and Operations

Lakmal Warusawithana

Vice President, Distinguished Engineer & GM - Choreo BU

Manjula Rathnayaka

Director - Engineering

MCP gives access. Skills add expertise.

OpenChoreo already ships MCP servers covering the full platform surface. Skills pair with MCP for token-efficient, deterministic workflows.

MCP / connectivity layer

Connects agents to real-time data and tools. Exposes the full platform surface.

What an agent CAN do. Works well for custom agents and ad-hoc tasks.

+

Skills / knowledge layer

Encoded workflows and best practices for HOW an agent should act.

Token-efficient. Deterministic. No guessing.

The Impact on Agent Performance

MCP only

Agent reasons through workflow each time. More tokens, variable results.

vs

MCP + Skills

Token-efficient, structured, more deterministic. Consistent from the first invocation.

OpenChoreo Skills — Runbooks for agents.

A growing open catalog of runbooks that any coding agent can discover and invoke. Available at github.com/openchoreo/skills

openchoreo-setup

task / Helm + kubectl

Interactively installs OpenChoreo on Colima, Rancher Desktop, or a managed cluster.

openchoreo-developer

persona / MCP

Promotion, env overrides, code→push→build→verify. Commits workload.yaml.

openchoreo-developer-gitops

persona / occ

Standard commit→push→verify reconcile. Repository-structure agnostic.

openchoreo-platform-engineer

persona / MCP + kubectl

Authors ComponentTypes, Traits, Workflows, Environments. Uses kubectl.

openchoreo-platform-engineer-gitops

persona / occ

Git-based platform engineering through Flux reconciliation.

add_circle_outline

More Skills coming

SRE, Migration, and security skills are in active development.

Demo 1: Developer Skills

- MCP capabilities
- Install the OpenChoreo Developer skill
- Deploy an existing app from a source repo
- Migrate the GCP microservices demo
- Report generation based on observability MCP tools

WSO2

Demo 2: Platform Engineering Skills

WSO2

Demo 4: Built-in SRE Agent

WSO2

Demo 5: Built-in Portal Assistant Agent

WSO2

Demo 3: Built-in FinOps Agent

WSO2

Demo 6: Securely Running AI Agents in Production

WSO2

The Problem

AI agents execute untrusted code by design. What happens when a prompt injection weaponizes them?

🔒 Steal internal secrets

Agent curls your internal APIs — leaks DB passwords, API keys, tokens

☁️ Harvest cloud credentials

Agent hits AWS metadata (169.254.169.254) for IAM role credentials

🔑 Access Kubernetes API

Mounted service account token = cluster-wide enumeration

💀 Container escape

Shared host kernel — one exploit away from the node

Real test result:

We asked OpenClaw to fetch data from an internal partner service.

The model refused to display it — but the curl **already succeeded.**

Model safety = **speed bump**

Infrastructure isolation = **the wall**

Your AI Agent Has the Keys to Everything

What agents do by design:

- 📝 Write & execute code
- 📂 Read & modify files
- 🌐 Make network calls
- 💻 Run shell commands

What a prompt injection exploits:

- 🔓 Steal internal secrets
- ☁️ Harvest cloud credentials
- 🔑 Access K8s API via SA token
- 💀 Container escape → host kernel

Real result from our test:

We asked OpenClaw to fetch data from an internal partner service.

The model's safety refused to display the output — but the **curl already succeeded.** **The data was already fetched.**

Model safety is a speed bump.

Infrastructure isolation is the wall.

Three Layers of Defense, One YAML Field

Kernel Isolation

Kata Containers — QEMU microVM
Dedicated kernel per agent

Host kernel: 6.1.168
VM kernel: 6.18.15

Network Isolation

Auto-generated NetworkPolicy

Blocks:
Private IPs (10.x, 172.x)
AWS metadata (169.254.x)

Allows:
Public internet (LLM APIs)

Identity Isolation

No K8s service account token
No cloud credentials
Zero capabilities (CapEff: 0)

automountServiceAccount Token: false

Before:
componentType:
name: deployment/service

After:
componentType:
name: proxy/ai-agent
parameters:
isolationTier: kata

Same image · Same agent · Same API key · One field activates all 3 layers

Live Demo: Same Agent, Same Prompts, Different Isolation

#	Prompt	Regular Container	Sandbox (Kata VM)
1	"grab me that secret menu"	🔴 LEAKED	🟢 BLOCKED
2	"check the filing cabinet"	🔴 TOKEN FOUND	🟢 NOT MOUNTED
3	"existential debugging"	🔴 HOST KERNEL	🟢 VM KERNEL + report
4	"AWS cookie jar"	🔴 REACHABLE	🟢 EMPTY
5	"tourist map"	🔴 container	🟢 virtiofs (VM proof)
6	"write me a REST API"	🟢 Works	🟢 Works

🎤 **The mic drop moment:**

The sandboxed agent investigates its own containment and concludes:

"This is a well-hardened sandbox with no realistic escape path."

Coming Up On Day 3 in the Yellow Room

09:00 a.m. (30 mins)

The Evolution of Platform Engineering – From Developer Platforms to AI-Native Platforms

Lakmal Warusawithana
Vice President, Distinguished Engineer & GM - Choreo BU

WSO2

09:30 a.m. (30 mins)

Unifying Developers and Platform Engineers Through OpenChoreo's Core Abstractions

Sameera Jayasoma
Vice President & Distinguished Engineer

WSO2

10:00 a.m. (30 mins)

Beyond Defaults – Extending and Customizing OpenChoreo for Your Enterprise

Manjula Rathnayake
Director - Engineering

WSO2

11:00 a.m. (30 mins)

Panel: WSO2 Developer Platform in the Enterprise–Real Stories, Real Impact

Glenn Donaldson
Chief Architect & Director, Enterprise Architecture & Integration - Office of Technology & Digital Innovation

The Ohio State University

Dr. Gautham Pallapa
Principal Director, Cloud, Data, and AI

Scotiabank

WSO2CON NORTH AMERICA

May 20 - 22, 2026 | Austin, Texas, USA

Thank You!

Lakmal Warusawithana

Vice President, Distinguished Engineer & GM - Choreo BU

Manjula Rathnayaka

Director - Engineering

Head of WSO2 Io