KubeCon CloudNativeCon North America 2026

#KubeCon #CloudNativeCon

From Vibe to Live

Building for the Real World



Who we are



David Biel

Director of Business Development,
Biel Dental Cabinets

Background	Former teacher and band director
Business	Makes cabinets for dentist offices
CLI Experience	Has never typed kubectl



Trey Caliva

Staff Cloud Architect & Security Engineer

Domain	Cloud Architecture, Infrastructure, Security
Focus	Multi-cloud, IaC, guardrails
Role	The engineer friend in this story

KubeCon CloudNativeCon
North America 2026

PART ONE

No engineers. Vibe-coded.





“I knew what I wanted to do. But at what cost?”

— David Biel, on past quotes for a website and lead generator



The lightbulb

KubeCon | CloudNativeCon
North America 2026

$10K

Quote for a website in 2015

vs

$200

Per month AI subscription

Plus [HOSTING $/MO] monthly hosting

A $10,000 problem became a $200 a month problem, and David was the one who could solve it.

What David set out to build

KubeCon | CloudNativeCon North America 2026

DAVID'S FIRST PROMPT (PARAPHRASED)

```
> I make cabinets for dentist offices. I need a
website that shows our work, lets a dentist request
a quote, and sends those requests to me. I've never
built anything like this. Where do we start?
```

THE GOAL

A website

Pages, forms, contact flow.

THE QUESTION

Can someone who has never typed kubectl get this to production?

KubeCon CloudNativeCon
North America 2026

PART TWO

From prompt to production



Two-pint sprints



Spare afternoons

Two months, 80 hours total.

An agentic coding tool

Sits in project, reads, writes, runs, asks.

The loop

Describe business need → **build** → **click around** → **repeat** ↺

The four edges of production

KubeCon CloudNativeCon North America 2026

GETTING LIVE

STAYING LIVE

Platform

Managed opinionated platform

Delivery

Ship through GitHub PR checks, not from a laptop.

Security

- Secrets in chat & code
- Open database rules
- Unauthenticated endpoints

Observability

Know it's down before a customer calls.

KubeCon | CloudNativeCon
North America 2026

● ○ ○ ○ EDGE 1 OF 4 · PLATFORM

✓ Running on localhost

“This is great.

Now how do I get this on the internet?”

— David Biel



What David's app runs on

FIREBASE HOSTING

Global CDN

The website, served from the edge.

CLOUD FUNCTIONS

Serverless compute

Containers that scale to zero.

FIRESTORE

Managed NoSQL

A document database with no servers to run.

FIREBASE AUTH

Sign-in

Who's logged in, handed over as a JWT.

No servers to patch. No cluster to run. Everything Trey suggested instead of a raw VM.

KubeCon CloudNativeCon
North America 2026

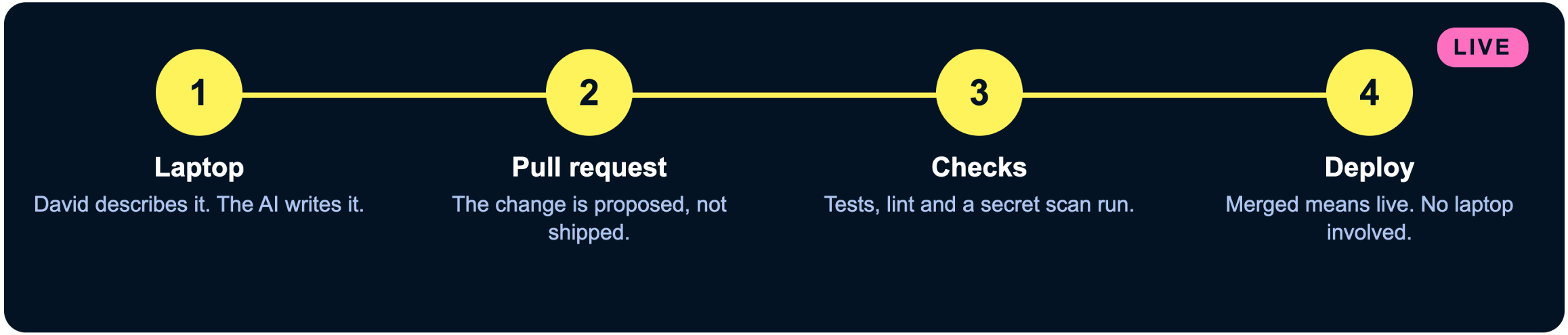
○ ● ○ ○ EDGE 2 OF 4 · DELIVERY

“What's a CI/CD?”

— David Biel



CI/CD, explained to a cabinet maker



BEFORE

Deploy from the laptop

Whatever is on the laptop goes live.

AFTER

Let GitHub deploy it

Every change is proposed, checked, then shipped.

Trey was the context window

TREY SAYS

“Put that behind auth. Let GitHub deploy it.”

DAVID TYPES

```
> Put that behind
auth. Let GitHub
deploy it.
```

Almost word for word.

THE AI BUILDS

- Auth
- Pipeline
- Managed platform

What first-time builders miss

Open database rules

THE MISS

```
allow read, write: if true;
```

Test-mode rules ship to prod. Anyone can read or wipe the data.

THE FIX

```
allow read: if request.auth.uid
== resource.data.owner;
```

Default deny. Users only touch their own records.

Unauthenticated endpoints

THE MISS

```
$ curl -X POST …/api/quotes
200 OK
```

No auth check on the function. Anyone can call it, or script it.

THE FIX

```
$ curl -X POST …/api/quotes
401 Unauthorized
```

Verify the caller on every request. Rate-limit what stays public.

Deep dive: secrets in chat

chat with the AI

```
> Here's the API key: sk_live_FAKE_DEMO_…
> Hook it up and deploy to prod
AI: Sure! I'll add that to the config and deploy.
```

More than once. Keys, a password or two.

A pasted secret has already leaked

History	Conversation logs on external servers
Git	Committed in source code forever

What would have caught it

Secret manager	Plus an AI instruction to use it
Scanning	Secret scanning in CI and pre-commit
Prompt hook	Blocks raw secrets in prompts



○ ○ ○ ● EDGE 4 OF 4 · OBSERVABILITY

“What about how we monitor that your site is up and running?”

— Trey, to David



One prompt, real monitoring

THE PROMPT (PARAPHRASED)

```
> Set up monitoring so I know when the site or the
quote form goes down. Alert me by email, and report any
errors from the functions.
✓ Uptime check: homepage
✓ Uptime check: quote form
✓ Alert policy: email
✓ Error reporting: functions
```

BEFORE

A customer would call.

Silent failure. Unasked by the AI.

AFTER (20 MINUTES)

Uptime check. Alerting.
Error reporting.

Monitoring is imposed by a platform team.

The AI could build it in 20 minutes. Nobody thought to ask.

HOLD THAT THOUGHT →

Why was a person the delivery mechanism?

Why didn't that advice live next to the AI?



KubeCon CloudNativeCon
North America 2026

PART THREE

Put your Platform in the context window



IF YOU'RE THINKING “THIS IS SHADOW IT”

Your users are already doing this

KubeCon | CloudNativeCon North America 2026

MARKETING	SALES	FINANCE	HR	OPERATIONS	SUPPORT
Internal campaign and content tool	Custom lead automation	Automated ERP script	Onboarding checklist app	Inventory tracker	Ticket triage bot
Social post scheduler	Quote calculator	Invoice reconciler	PTO tracker	Shipping label script	FAQ chatbot
Landing page builder	CRM sync script	Expense report bot	Interview scheduler	Vendor portal	Customer health dashboard
Brand asset finder	Commission tracker	Budget dashboard	Policy Q&A bot	Production scheduler	Refund approval flow

The question isn't how to stop it.
It's how to give them guardrails.

THE ANSWER

The guardrails live in the AI's context

KubeCon | CloudNativeCon North America 2026

START HERE

KNOW-HOW

Skills

Instructions the AI loads before it writes a line.

ENFORCEMENT

Hooks

Checks that run every time, like blocking a secret in a prompt.

ACCESS

MCP servers

Live connections to your cluster, CRM and data. Governed like secrets.

Whatever your tool calls them: skills, rules, instructions, AGENTS.md.

PUT TREY IN THE CONTEXT WINDOW

What a skill actually is

KubeCon | CloudNativeCon North America 2026

SKILL.md · EXCERPT

```
---
name: golden-path
description: Use whenever they want it "on the internet".
---
```

- ## Platform
  Deploy to the managed platform. Never a raw VM.
- ## Delivery
  Ship through a GitHub PR. Never deploy from a laptop.
- ## Security
  Never accept a secret in chat. Use the secret manager.
  Default-deny database rules. Auth on every endpoint.
- ## Observability Uptime check and alerting before "done".

Trey's advice, written down.

The AI loads it before it writes a line.

One Markdown file.

Same four edges, for every builder, every time.

Golden paths, delivered as AI context

KubeCon | CloudNativeCon North America 2026

Every org climbs the same three steps, whatever its size.

AD HOC · WHERE DAVID STARTED

Knowledgeable friend

Advice reaches code via builder prompts.

SHARED

Shared skill repo

Every builder's AI loads identical instructions.

GOVERNED

Governed catalog

Approved skills owned like base images.

SAME SKILL, DIFFERENT TARGETS

Same four edges, pointed at your platform

KubeCon | CloudNativeCon North America 2026

DAVID'S SKILL.md

```
## Platform
Managed serverless platform

## Delivery
GitHub + CI/CD pipeline

## Security
GCP Secret Manager


## Observability
Cloud Monitoring + Error Reporting
```

YOUR PLATFORM'S SKILL.md

```
## Platform
Internal platform · Backstage templates · Knative

## Delivery
GitOps: Argo CD or Flux

## Security
External Secrets Operator + Kyverno / Gatekeeper


## Observability
OpenTelemetry + Prometheus
```

Same four lessons. Different tools. **The skill is a Markdown file pointing the AI at your cluster.**

Skills advise. Hooks enforce. MCP connects.

KubeCon CloudNativeCon North America 2026

ENFORCEMENT

Hooks

A skill can be ignored. **A hook can't.**

```
CLAUDE CODE · .claude/settings.json
{ "hooks": {
  "UserPromptSubmit": [{ "hooks": [{
    "type": "command",
    "command": "…/secret-scan.sh" }] }],
  "SessionEnd": [ …same script… ] } }
# match → {"continue": false}: never sent
# on exit → transcript + history wiped
```

ACCESS

MCP servers

Live connections to real systems. **Grant them like secrets.**

```
CLAUDE CODE · .mcp.json + settings.json
"kubernetes": { "command": "npx", "args": [
  "-y", "kubernetes-mcp-server@latest",
  "--read-only" ] },
"firebase": { "command": "npx", "args": [
  "-y", "firebase-tools@latest", "mcp",
  "--tools", "firestore_query_collection,…" ] }
"deny": [ "Bash(firebase deploy:*)", … ]
# read-only tools · deploys only from CI
```

Own skills, hooks and MCP servers like base images: approved, versioned, kept current.

The hook stops the key

THE PROMPT · ILLUSTRATED

```
> We need a new webhook endpoint that forwards incoming quote
requests to our distributor's API. Here is our production API
key:
sk_live_FAKE_DEMO_KEY_9988776655
Wire it up and deploy it to prod!

● Operation stopped by hook: Blocked: this prompt looks like
it contains a secret. Rotate that key now, store the new one
in your secret manager, and reference it by name instead.
This session will be deleted from local history when you
exit, so exit now (/exit) and start a fresh session.
```

HOOK

Blocked before the AI sees it.

The prompt never leaves the laptop. Rotate the key, then put it in the secret manager. Then it tells you to exit, and the session is wiped from local history.

ILLUSTRATED DEMO · STEP 2 OF 3

The skill steers the build

KubeCon | CloudNativeCon North America 2026

THE AI'S PLAN · ILLUSTRATED

```
> Wire up the quote webhook to our distributor's API and
deploy it.
Loaded skill: golden-path
→ Cloud Function (2nd gen), not a VM
→ API key read from Secret Manager
→ New branch + pull request, CI checks run
```

SKILL

Loaded before the first line.

Approved platform, the secret manager and a pull request. Nobody asked for any of it. The skill did.

MCP checks the live project

TOOL CALLS · ILLUSTRATED

```
firebase › firebase_get_project ✓ read
firebase › firestore_query_collection ✓ read
bash › firebase deploy ✗ denied by permissions
→ ships through the pull request instead
→ Uptime check added for /api/quote-webhook
```

MCP

Read access, not deploy access.

A deny rule blocks the deploy command. The change ships through the PR, with an uptime check attached.

One prompt, four guardrails

Stops on the key
Blocked before the AI sees it.

HOOK

Approved platform
Managed functions, not a server.

SKILL

Ships through a PR
Not from the laptop.

SKILL

Adds an uptime check
Checks the live project. Nobody had to ask.

MCP

Every one of David's hard lessons, enforced in ninety seconds.

THE PAYOFF, SO FAR

Started with a website, ended up replacing a SaaS

KubeCon | CloudNativeCon North America 2026



Website

Pages, forms, contact flow.

Lead generation

Automated form follow-ups.

Replaced the SaaS

Dropped the paid subscription product.

NOW BUILDING

A full CRM

Bigger app. Same guardrails.

UNDER THE HOOD

Thank you, cloud native community

KubeCon | CloudNativeCon North America 2026

UNDER DAVID'S MANAGED SERVICES

Knative
Cloud Run functions implement the Knative Serving API.

Cloud Native Buildpacks
Turn his source into a container on every deploy.

CloudEvents
The format every event-driven function receives.

UNDER YOUR PLATFORM

- Kubernetes
- Knative
- Backstage
- Argo CD
- Flux
- External Secrets
- Kyverno
- OPA Gatekeeper
- Prometheus
- OpenTelemetry
- Cloud Native Buildpacks
- CloudEvents

The wrapper is opinionated. The primitives are yours.

Most vibe coders will never know you exist. You made this possible for every one of them.

KubeCon | CloudNativeCon
North America 2026

REMEMBER BEING A BEGINNER

DAVID ASKED

"Now how do I get this on the internet?"

"What's a CI/CD?"

HE DIDN'T KNOW TO ASK

Where should this key live?

Who can read my database?

How would I know it's down?

Every one of us asked these once.
Most of us forgot.

Your golden paths have to answer the questions a beginner doesn't know to ask.





NOW BUILDING: A FULL CRM

The next app is bigger. So the guardrails matter.

There are people like David in every one of your companies.



KubeCon | CloudNativeCon
North America 2026

#KubeCon #CloudNativeCon · Salt Lake City, UT

Thank you

`github.com/treycaliva/from-vibe-to-live-kubecon-2026`

Skills, hooks and MCP configs from the demo, plus how to test them.

Session feedback

Scan to rate this talk.

