Chick-fil-A®

weaveworks

Managing Fleets of Kubernetes Clusters w/GitOps

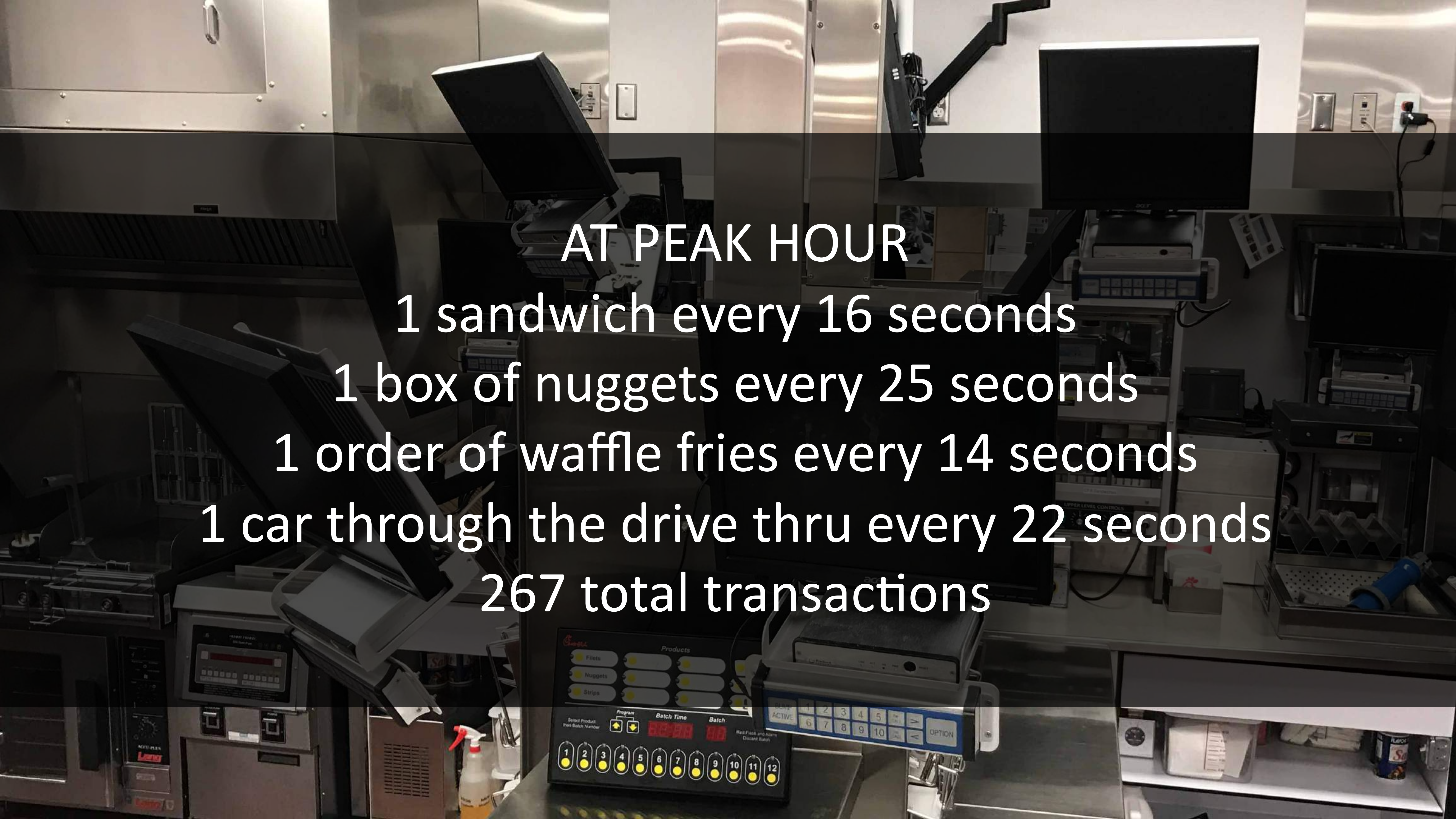
GitOps

weaveworks
GitOps for Kubernetes
Deploy, monitor and manage
cloud native infrastructure and apps
Prometheus
HELM

GitOps with Chickens

weaveworks
GitOps for Kubernetes
Deploy, monitor and manage
cloud native infrastructure and apps
Prometheus
HELM

Why IoT?



AT PEAK HOUR

1 sandwich every 16 seconds

1 box of nuggets every 25 seconds

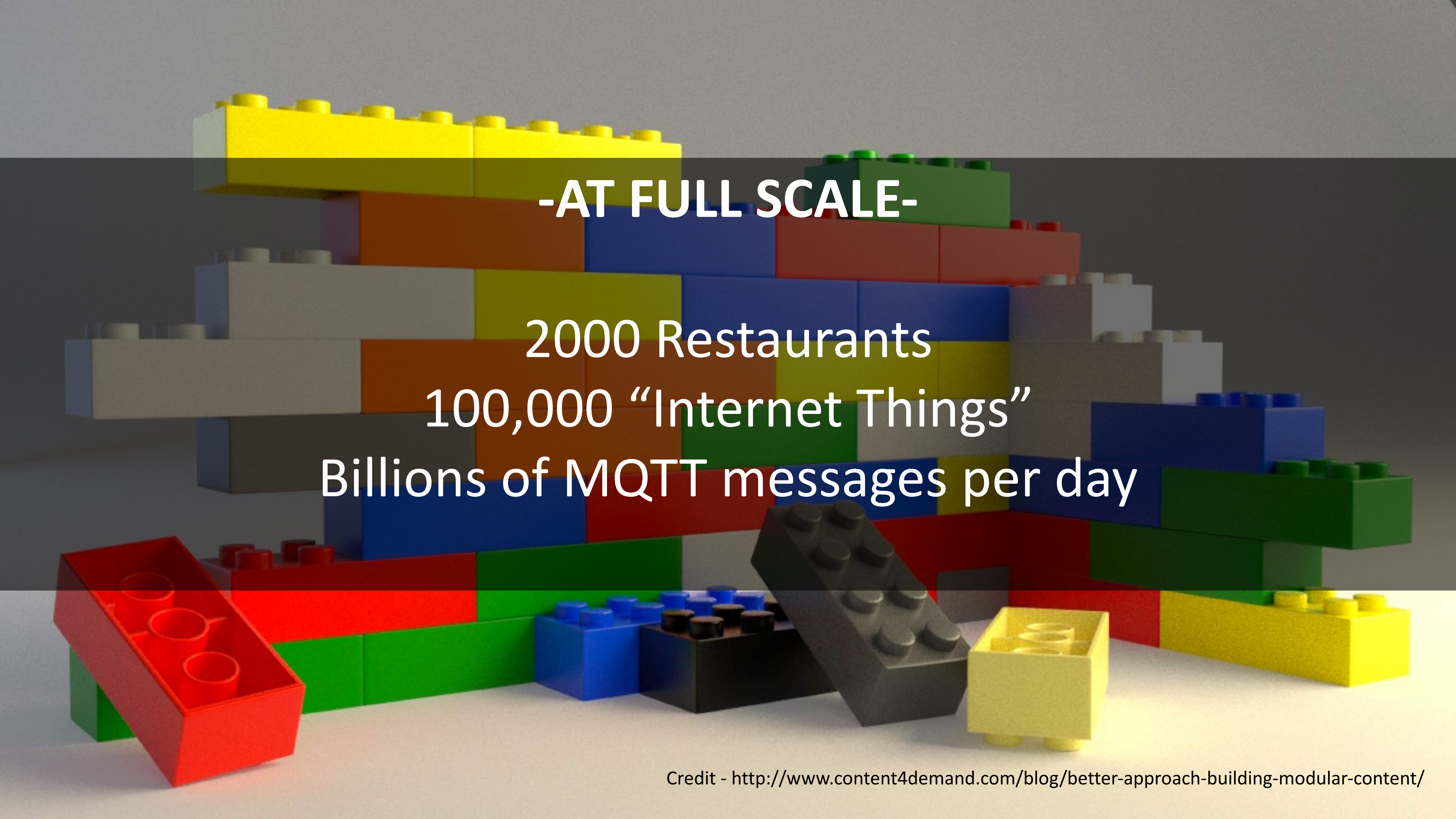
1 order of waffle fries every 14 seconds

1 car through the drive thru every 22 seconds

267 total transactions

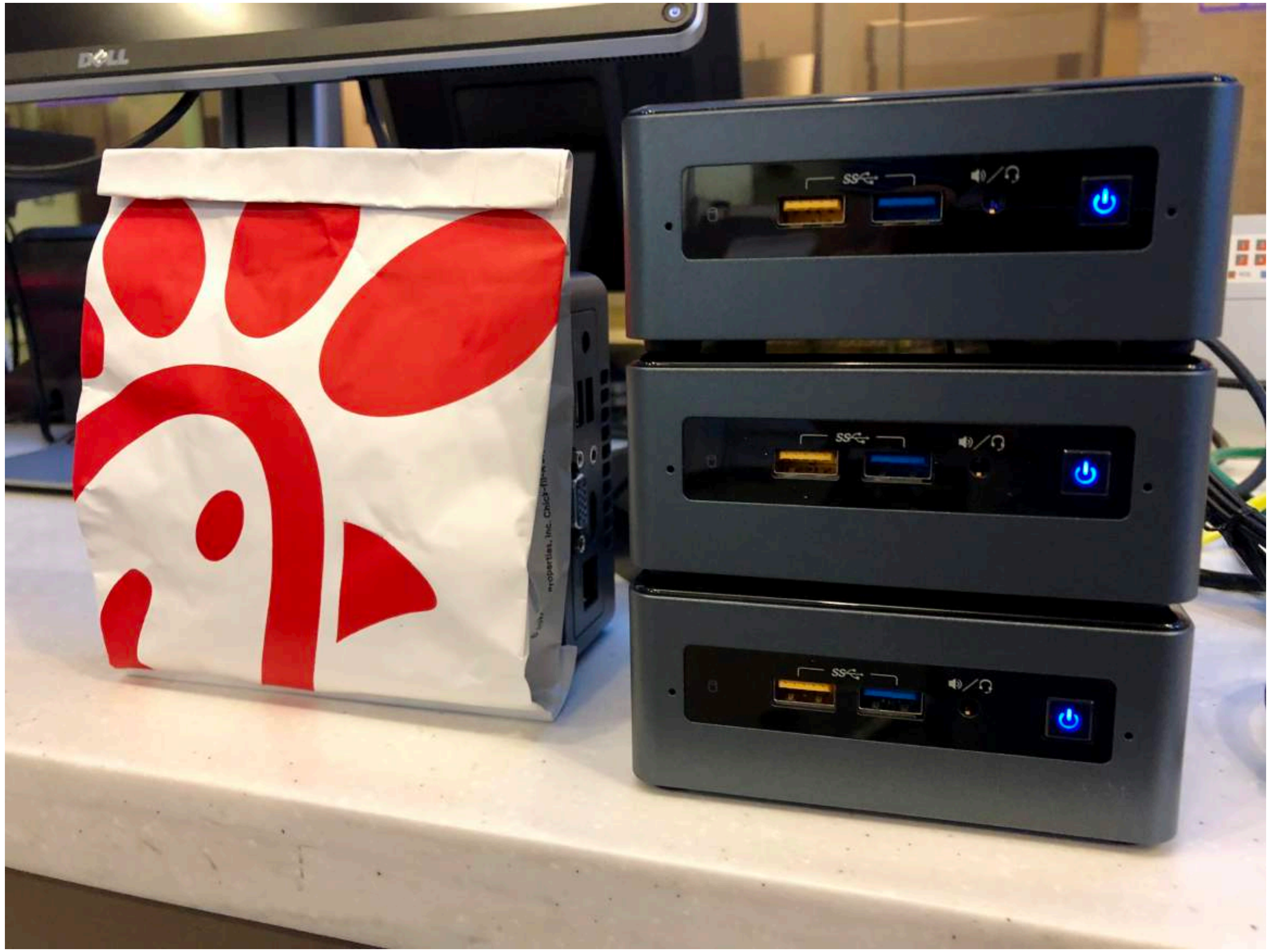
-AT FULL SCALE-

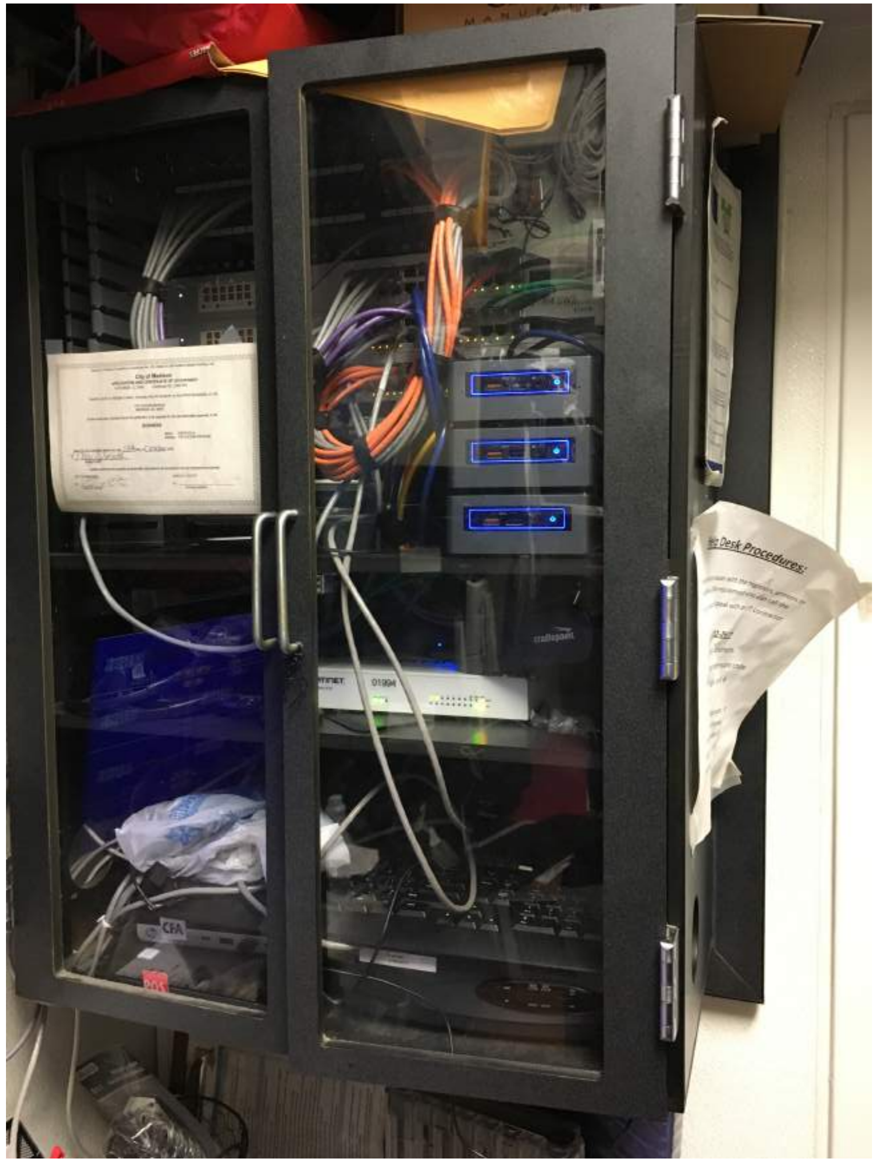
2000 Restaurants
100,000 “Internet Things”
Billions of MQTT messages per day



Credit - http://www.content4demand.com/blog/better-approach-building-modular-content/

Restaurant "Data Centers"





Intel: Quadcore processor, 8 GB RAM, SSD

Wait, what just happened?

…

Problems solved!

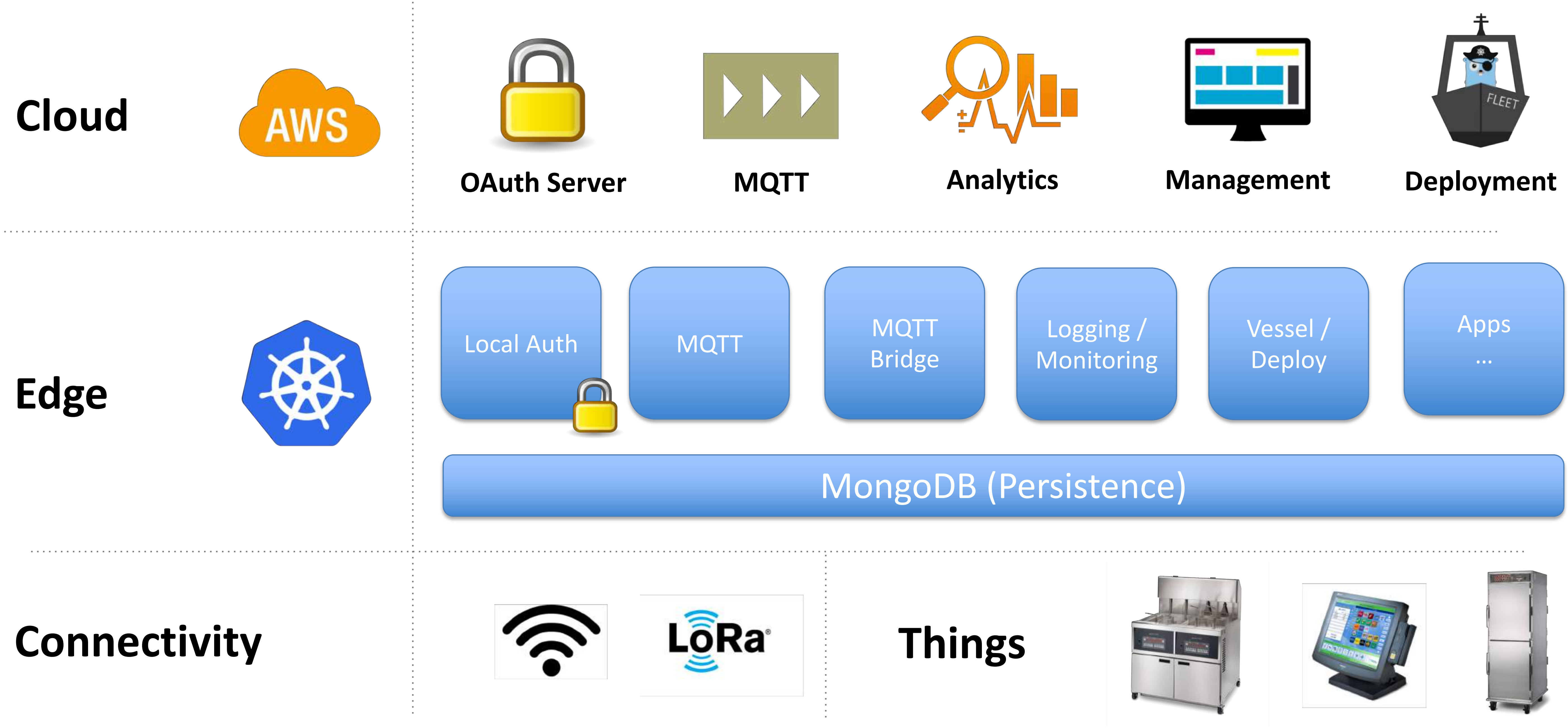
- Scale
- Availability
- Throughput

New problems caused!

- Communication
- Consistency
- Deployment

…

Chick-fil-A IoT Architecture



Cloud

OAuth Server

MQTT

Analytics

Management

Deployment

Edge

Local Auth

MQTT

MQTT Bridge

Logging / Monitoring

Vessel / Deploy

Apps
…

MongoDB (Persistence)

Connectivity

Things

New ways of working

cloud led us to devops

cloud native leads us to **gitops**

automation for cloud native
or “operations by pull request”

GitOps is...

An operating model for managing Kubernetes & Apps

A way to do continuous delivery

Derived from SRE best practices and CompSci foundations

A set of tech agnostic principles (Why instead of How)

A way to speed up your team

> *To me, [GitOps is] the holy grail of software and infrastructure management. I make this change, I push it, and off it goes*
>
> Chris Short, THENEWSTACK, May 2018

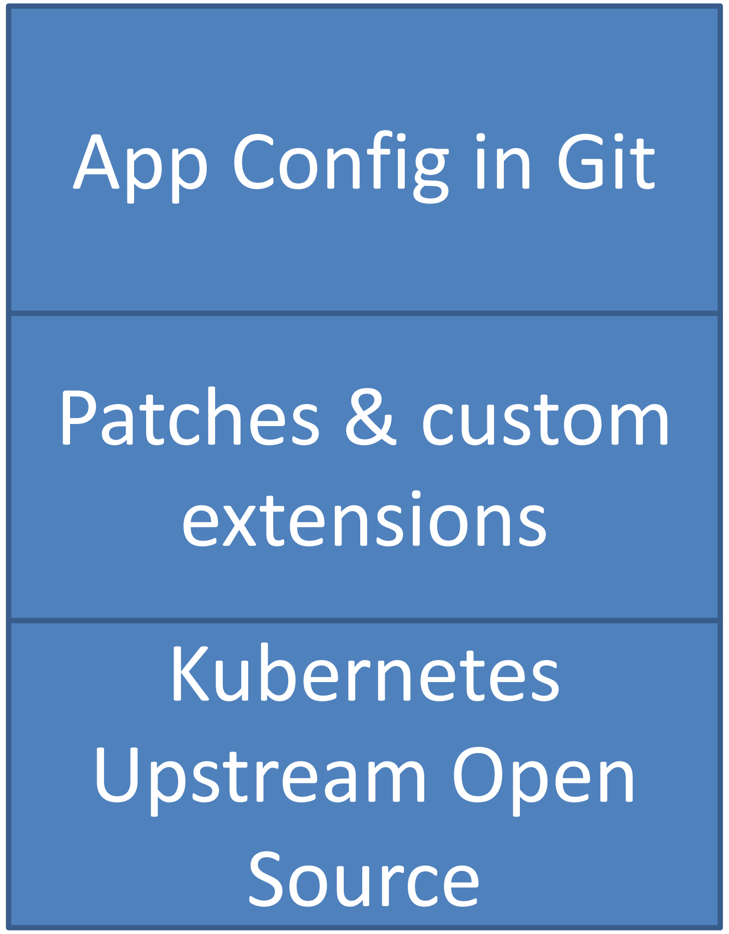
Kubernetes ❤️ GitOps

“The world is envisioned as a repo and not as a kubernetes installation"

- Kelsey Hightower

© pinar@pinarozger.com

We want to map from this

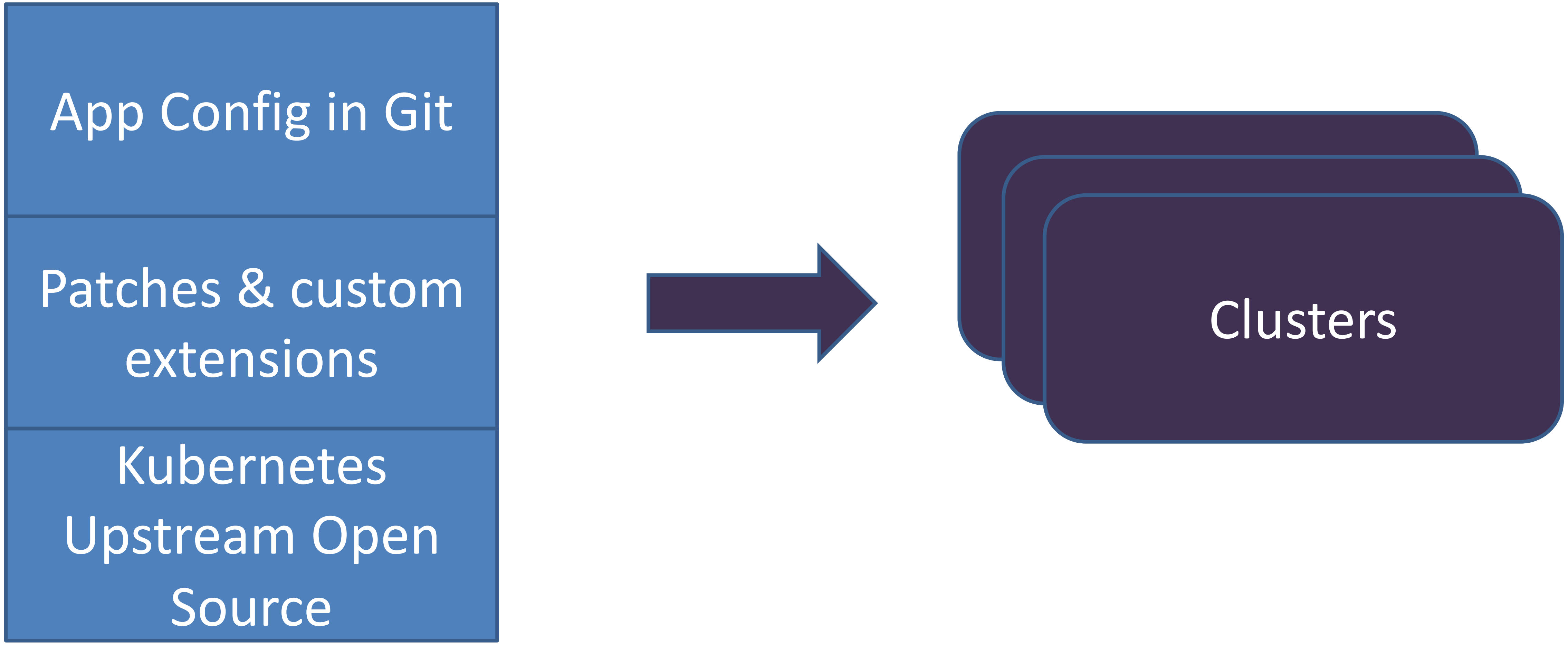


App Config in Git

Patches & custom extensions

Kubernetes Upstream Open Source

We want to map from this… to this



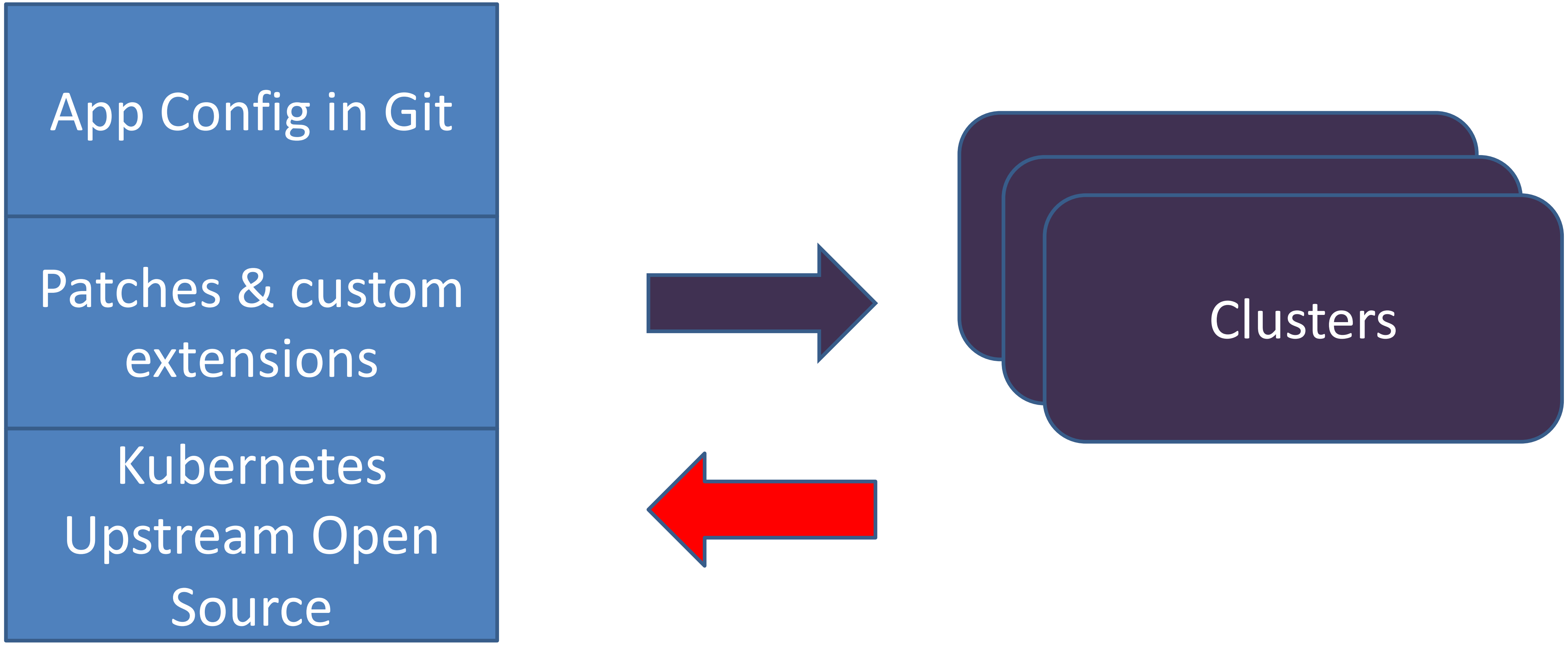
App Config in Git

Patches & custom extensions

Kubernetes Upstream Open Source

Clusters

We want to map from this… to this & alert on drift



App Config in Git

Patches & custom extensions

Kubernetes Upstream Open Source

Clusters

1. The entire system is described declaratively.
2. The canonical desired system state is versioned (with Git, so changes are also Git workflows)
3. Approved changes to the desired state are then applied to the system autonomically
4. Software agents ensure correctness (convergence) and alert on divergence

1 The entire system is described declaratively.

Beyond code, config and data ⇒

- Implementation independent
- Easy to abstract in simple ways
- Easy to validate for correctness
- Easy to generate & manipulate from code

2 The canonical desired system state is versioned (with Git)

Canonical Source of Truth (DRY)

With declarative definition, trivialises rollbacks

Excellent security guarantees for auditing

Sophisticated approval processes (& existing workflows)

Great Software ⟷ Human collaboration point

3 Approved changes to the desired state are autonomically applied to the system

Significant velocity gains

Privileged operators don’t cross security boundaries

Separates **What** and **How**.

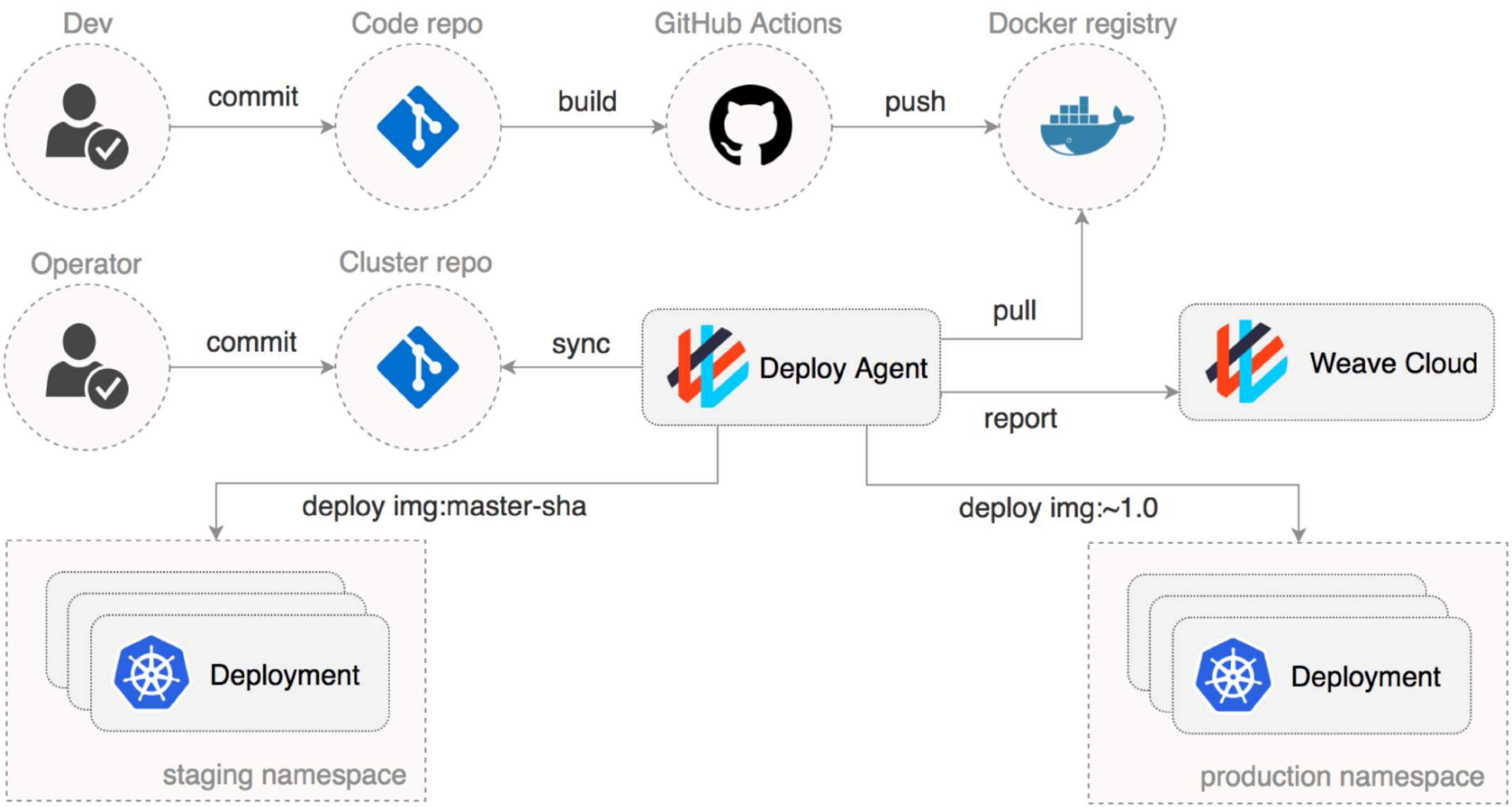
4 Software agents ensure correctness (convergence) and alert on divergence

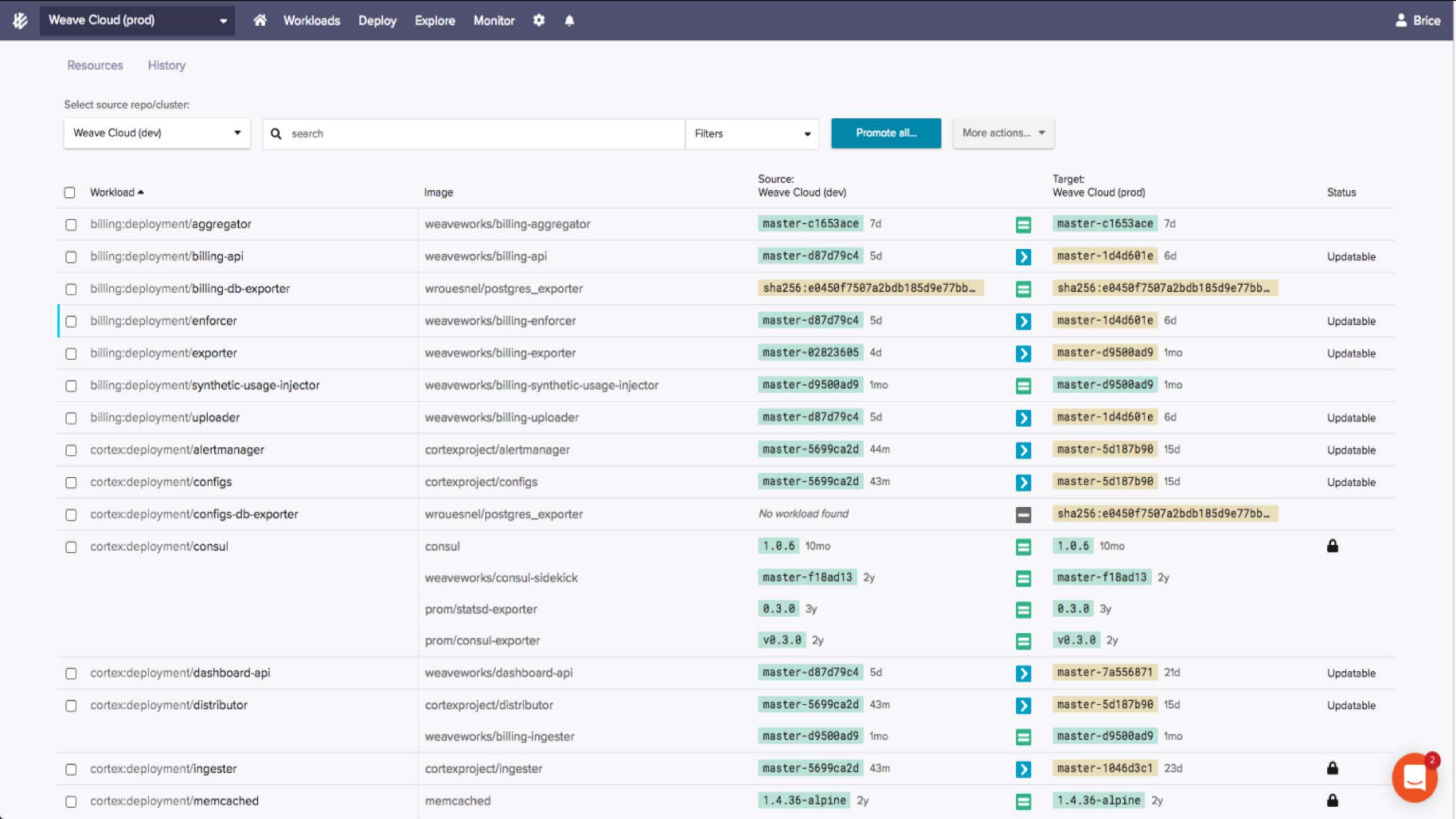
Continuously checking that desired state is met

System can self heal

Recovers from errors without intervention (PEBKAC)

It’s the control loop for your operations


Dev
commit
Code repo
build
GitHub Actions
push
Docker registry
Operator
commit
Cluster repo
sync
Deploy Agent
pull
Weave Cloud
report
deploy img:master-sha
deploy img:~1.0
Deployment
staging namespace
Deployment
production namespace



Resources History

Select source repo/cluster:

Weave Cloud (dev) ▾ | search | Filters ▾ | Promote all... | More actions... ▾

☐	Workload ▲	Image	Source: Weave Cloud (dev)		Target: Weave Cloud (prod)	Status
☐	billing:deployment/aggregator	weaveworks/billing-aggregator	master-c1653ace 7d	=	master-c1653ace 7d	
☐	billing:deployment/billing-api	weaveworks/billing-api	master-d87d79c4 5d	›	master-1d4d601e 6d	Updatable
☐	billing:deployment/billing-db-exporter	wrouesnel/postgres_exporter	sha256:e0450f7507a2bdb185d9e77bb…	=	sha256:e0450f7507a2bdb185d9e77bb…	
☐	billing:deployment/enforcer	weaveworks/billing-enforcer	master-d87d79c4 5d	›	master-1d4d601e 6d	Updatable
☐	billing:deployment/exporter	weaveworks/billing-exporter	master-02823605 4d	›	master-d9500ad9 1mo	Updatable
☐	billing:deployment/synthetic-usage-injector	weaveworks/billing-synthetic-usage-injector	master-d9500ad9 1mo	=	master-d9500ad9 1mo	
☐	billing:deployment/uploader	weaveworks/billing-uploader	master-d87d79c4 5d	›	master-1d4d601e 6d	Updatable
☐	cortex:deployment/alertmanager	cortexproject/alertmanager	master-5699ca2d 44m	›	master-5d187b90 15d	Updatable
☐	cortex:deployment/configs	cortexproject/configs	master-5699ca2d 43m	›	master-5d187b90 15d	Updatable
☐	cortex:deployment/configs-db-exporter	wrouesnel/postgres_exporter	*No workload found*	−	sha256:e0450f7507a2bdb185d9e77bb…	
☐	cortex:deployment/consul	consul	1.0.6 10mo	=	1.0.6 10mo	🔒
		weaveworks/consul-sidekick	master-f18ad13 2y	=	master-f18ad13 2y	
		prom/statsd-exporter	0.3.0 3y	=	0.3.0 3y	
		prom/consul-exporter	v0.3.0 2y	=	v0.3.0 2y	
☐	cortex:deployment/dashboard-api	weaveworks/dashboard-api	master-d87d79c4 5d	›	master-7a556871 21d	Updatable
☐	cortex:deployment/distributor	cortexproject/distributor	master-5699ca2d 43m	›	master-5d187b90 15d	Updatable
		weaveworks/billing-ingester	master-d9500ad9 1mo	=	master-d9500ad9 1mo	
☐	cortex:deployment/ingester	cortexproject/ingester	master-5699ca2d 43m	›	master-1046d3c1 23d	🔒
☐	cortex:deployment/memcached	memcached	1.4.36-alpine 2y	=	1.4.36-alpine 2y	🔒

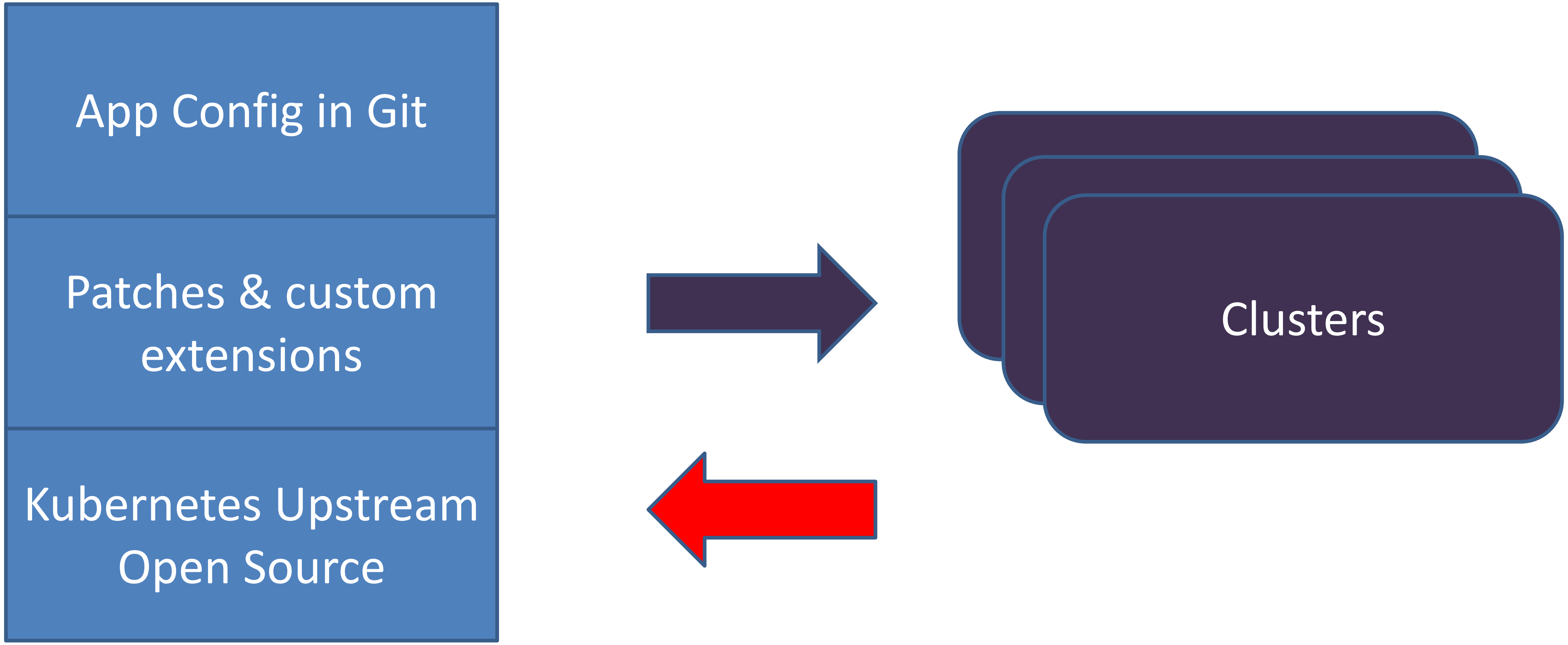
What this gets us

- Management based on continuous deployment from config & image repos.
- Monitoring as a control loop
- Policy & audit “built in”
- All using standard upstream OSS K8s and friends

When does this matter most?

- When your developers don’t want to learn k8s
- When you want secure changes, not kubectl
- When you scale to many apps, services, configs

What about GitOps for Edge compute?



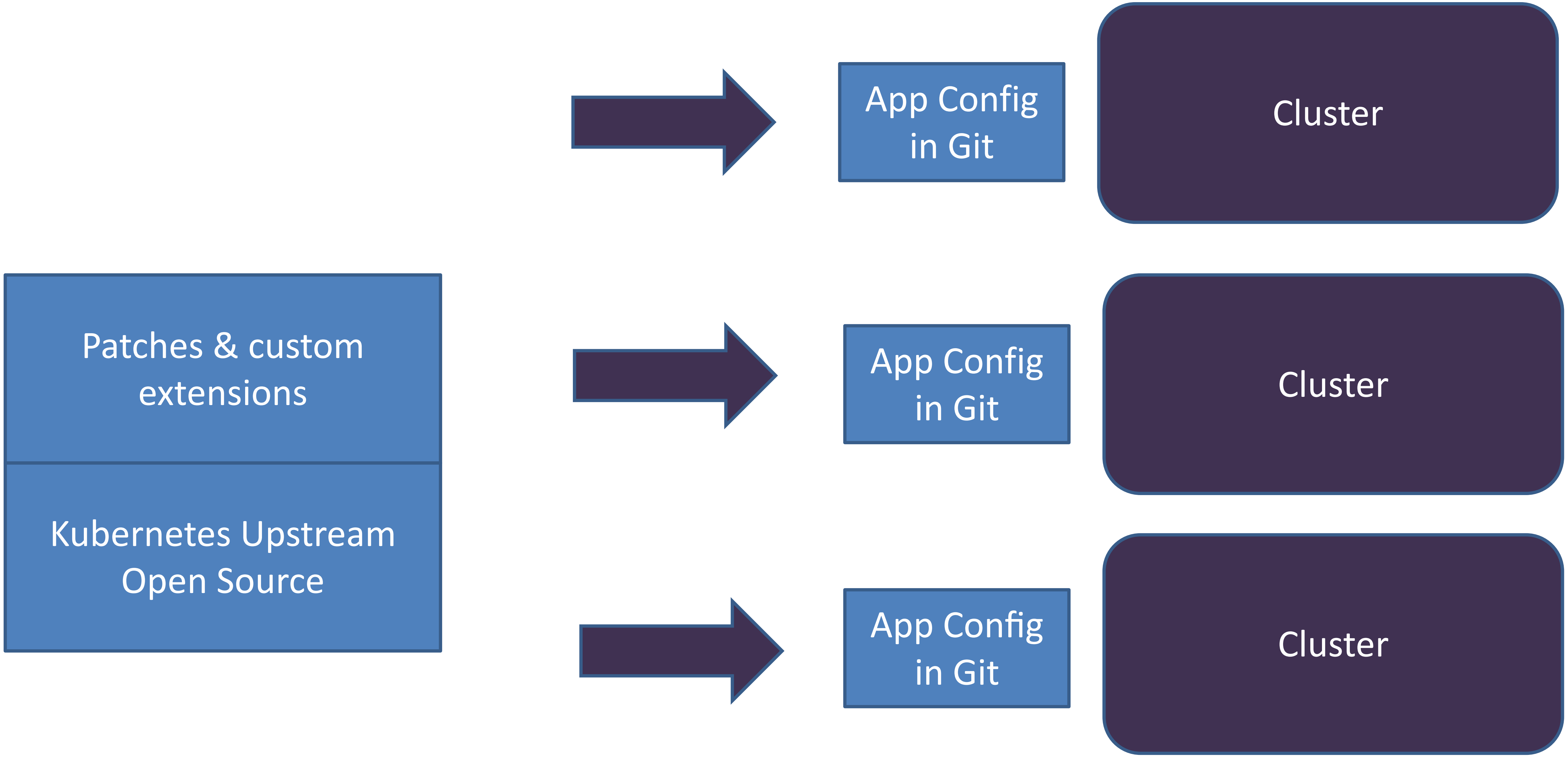
App Config in Git

Patches & custom extensions

Kubernetes Upstream Open Source

Clusters

One solution…



DEMO

Find out more

www.linkedin.com/in/seandrucker
www.linkedin.com/in/brian-chambers

Medium

https://medium.com/@cfatechblog

https://github.com/chick-fil-a

@brianchambers21

Team

- Berlin
- London
- San Francisco
- **Remote**