

Building a Bank from scratch*

CLOUD NATIVE COPENHAGEN, JANUARY 2020

HANS KRISTIAN FLAATTEN

Hans Kristian Flaatten

- From Norway 
- Married, two boys (0b011 && 0b101)
- DevOps Practice Lead @ TietoEVRY
- Node.js Foundation Member
- Open Source Contributor ❤️





```
$ go get github.com/bulderbank/ndc-2019  
$ go run agenda.go
```

- Bulder, what?!
- Architecture
- Build and Deploy
- Runtime
- Operations





BULDER BANK

BULDER BANK



Awesome mobile experience



Competitive mortgages with
automatic rent adjustments



Value adds and integrations



Minimum Viable Product



Onboarding



My Cards



Subscriptions



Transactions



Push notifications



Transactions 2.0



Payments

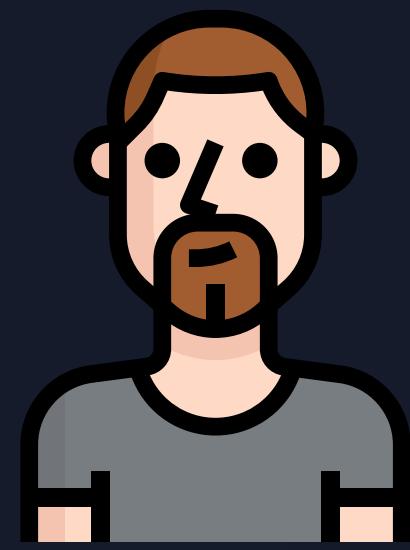


Invoice scanning



My Economy

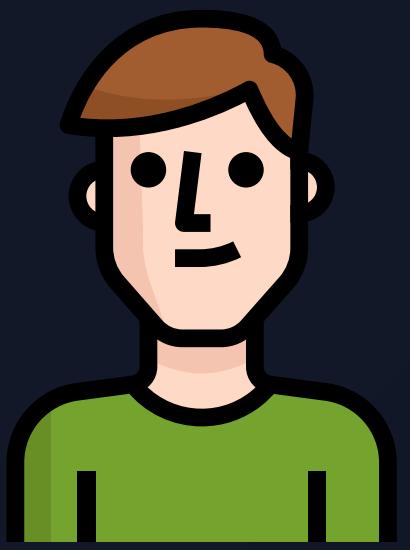
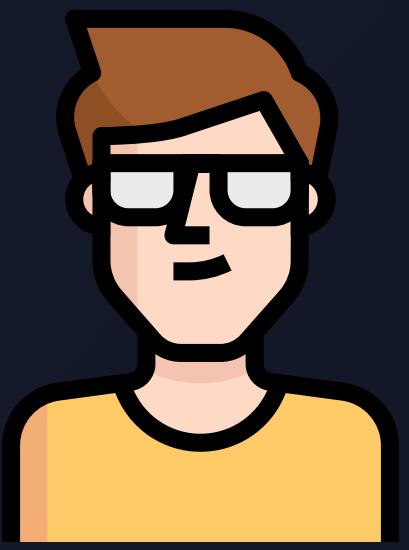
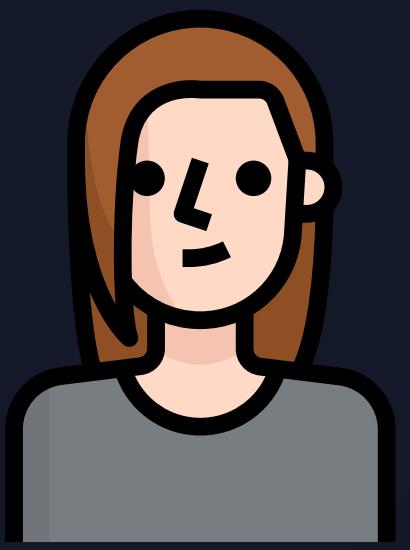
The Team



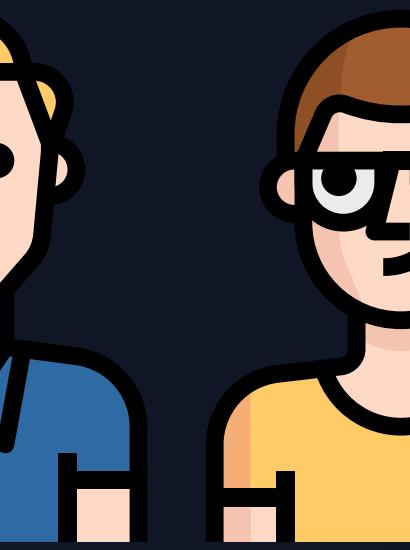
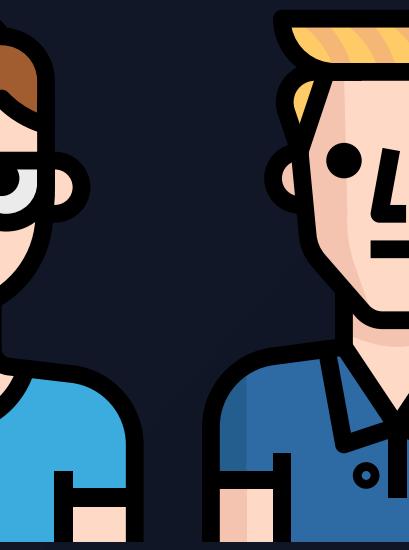
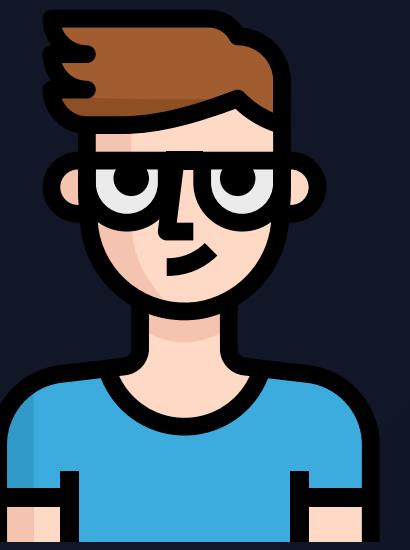
CTO



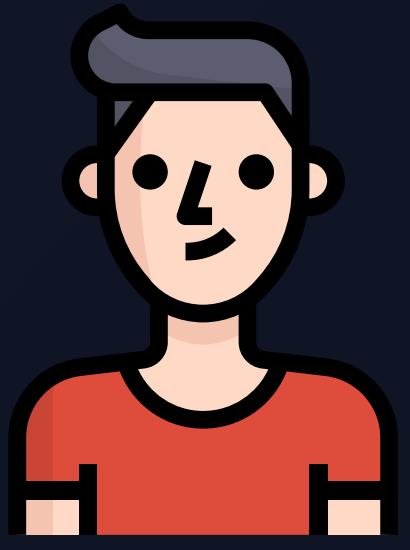
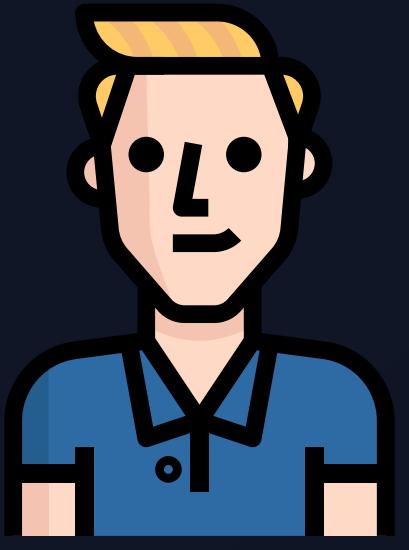
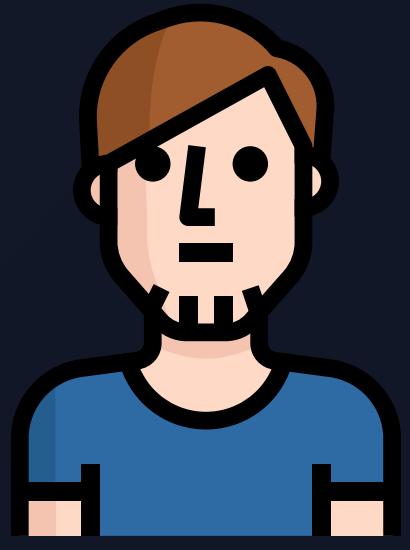
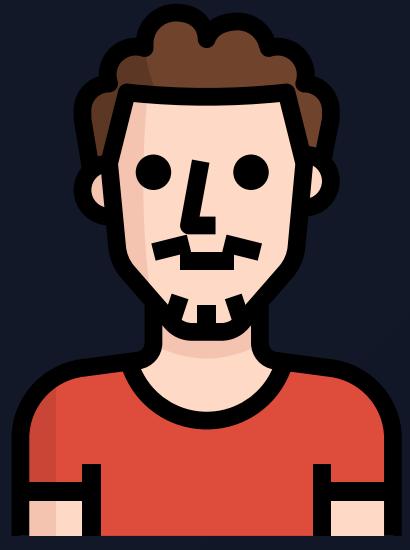
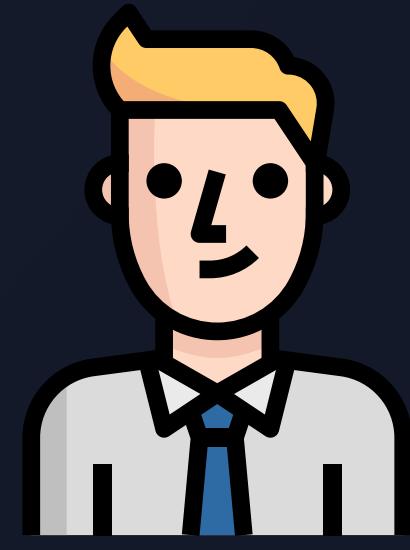
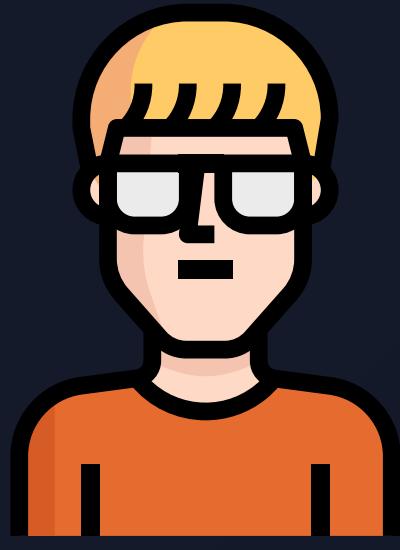
Frontend



Backend



Cloud Engineers



Design / UX

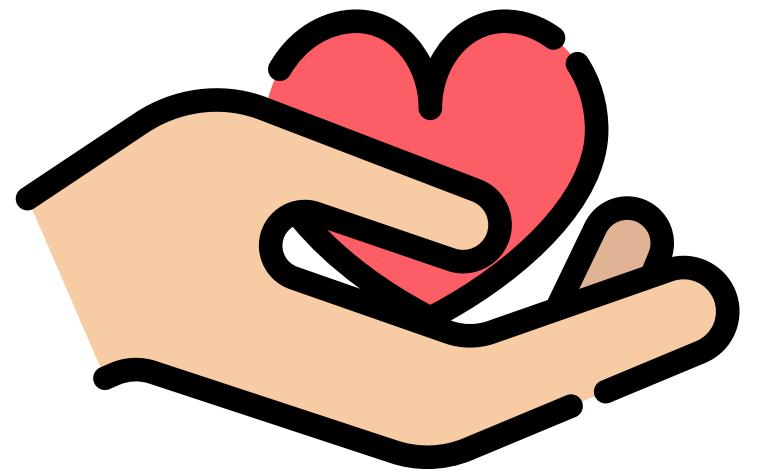
Android

iOS



Open Banking @ Sparebanken Vest

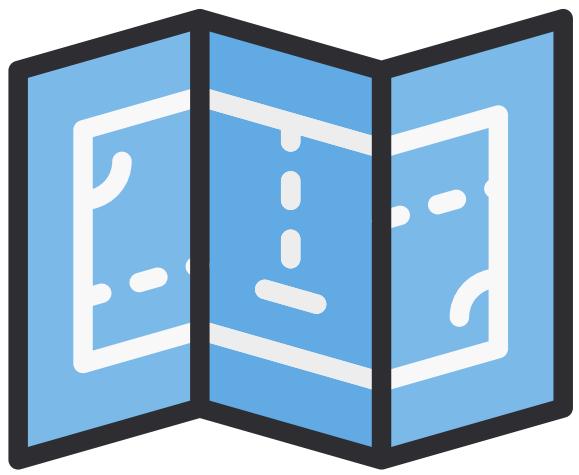
Key Principles



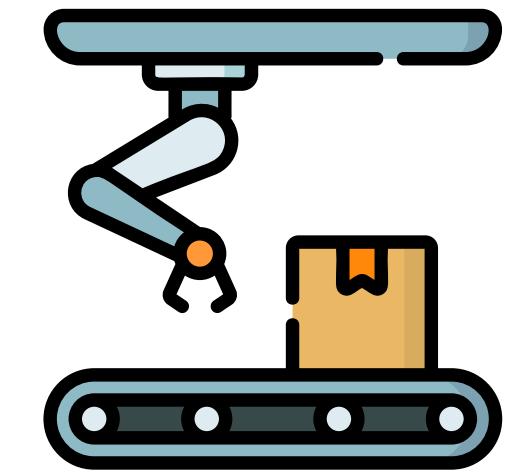
Make People
Awesome



Make Safety
a Prerequisite



Experiment &
Learn Rapidly



Deliver Value
Continuously

Timeline



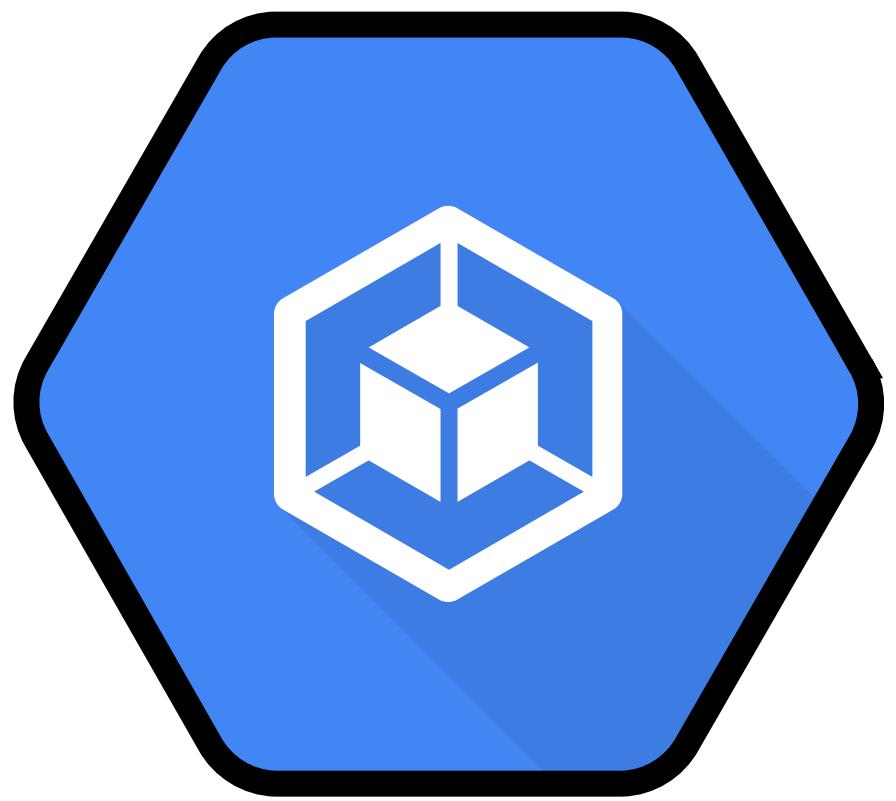
Timeline

10

MONTHS



Google Cloud

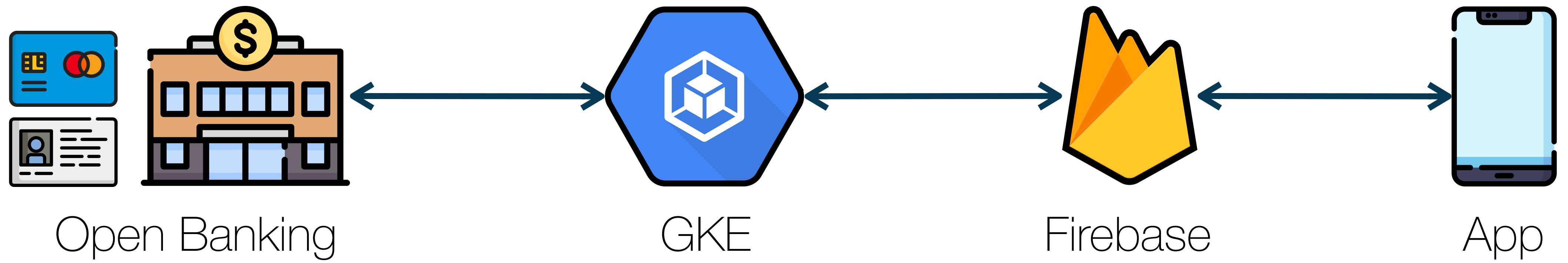


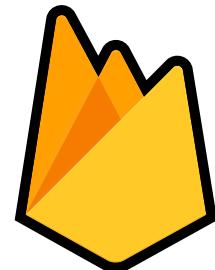
GKE



Firebase

Bulder Bank

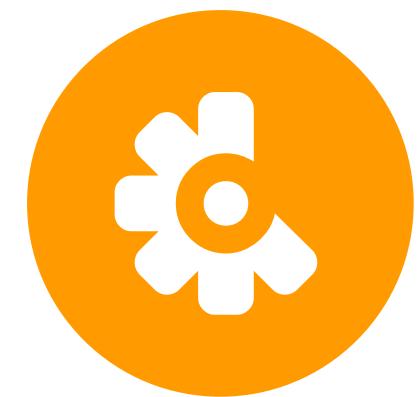




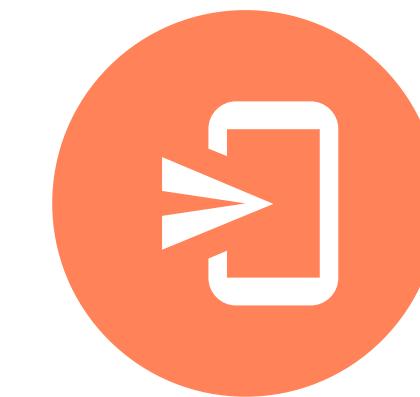
Firebase



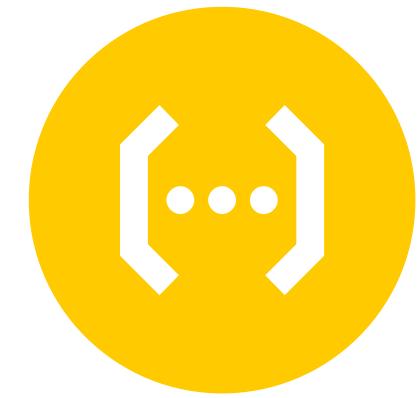
Firestore



Crashlytics



Messaging



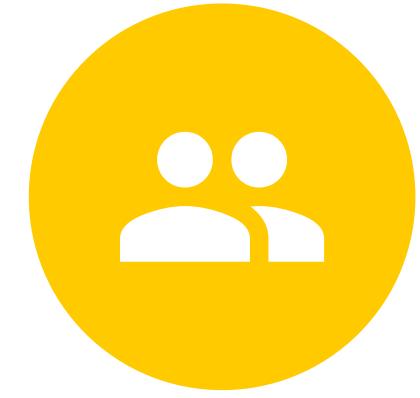
Functions



Performance
Monitoring



Analytics



Authentication

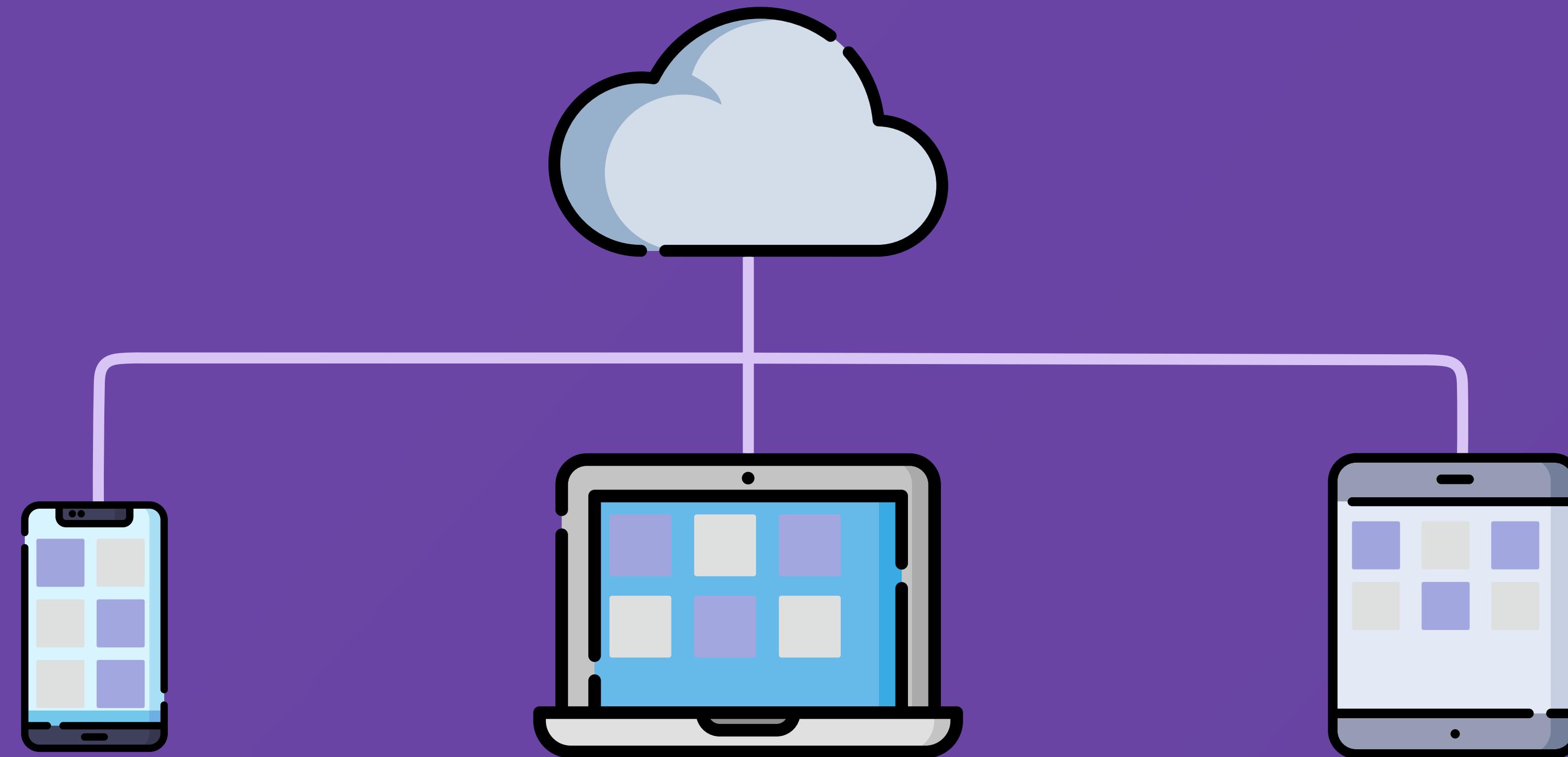


Test Lab

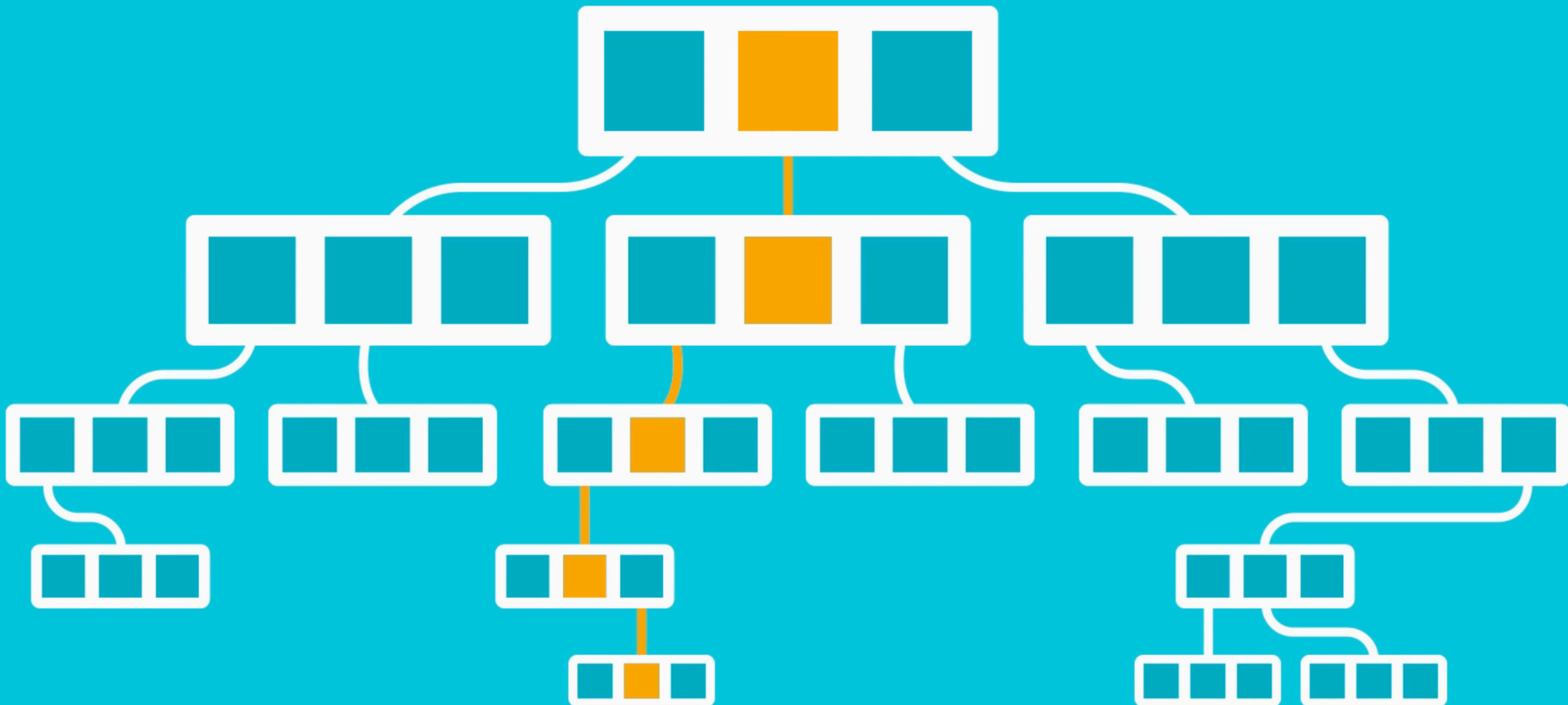


Remote
Config

Firebase



Firebase



No Schema – No Problems?

No Schema – ~~new~~ Problems

OpenAPI

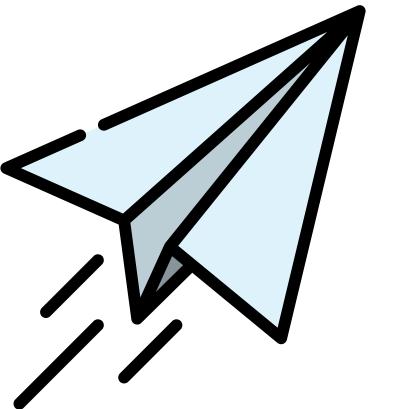
```
● ● ●  
definitions:  
  user:  
    type: object  
    properties:  
      created:  
        type: string  
        format: date  
      ...  
  
  userInfo:  
    $ref: '#/definitions/contact'  
  
  contact:  
    type: object  
    properties:  
    ...
```



Write



Verify



Deploy

OpenAPI



```
definitions:  
  user:  
    type: object  
    properties:  
      created:  
        type: string  
        format: date  
      ...  
  
  userInfo:  
    $ref: '#/definitions/contact'  
  
contact:  
  type: object  
  properties:  
  ...
```



Account **v1**

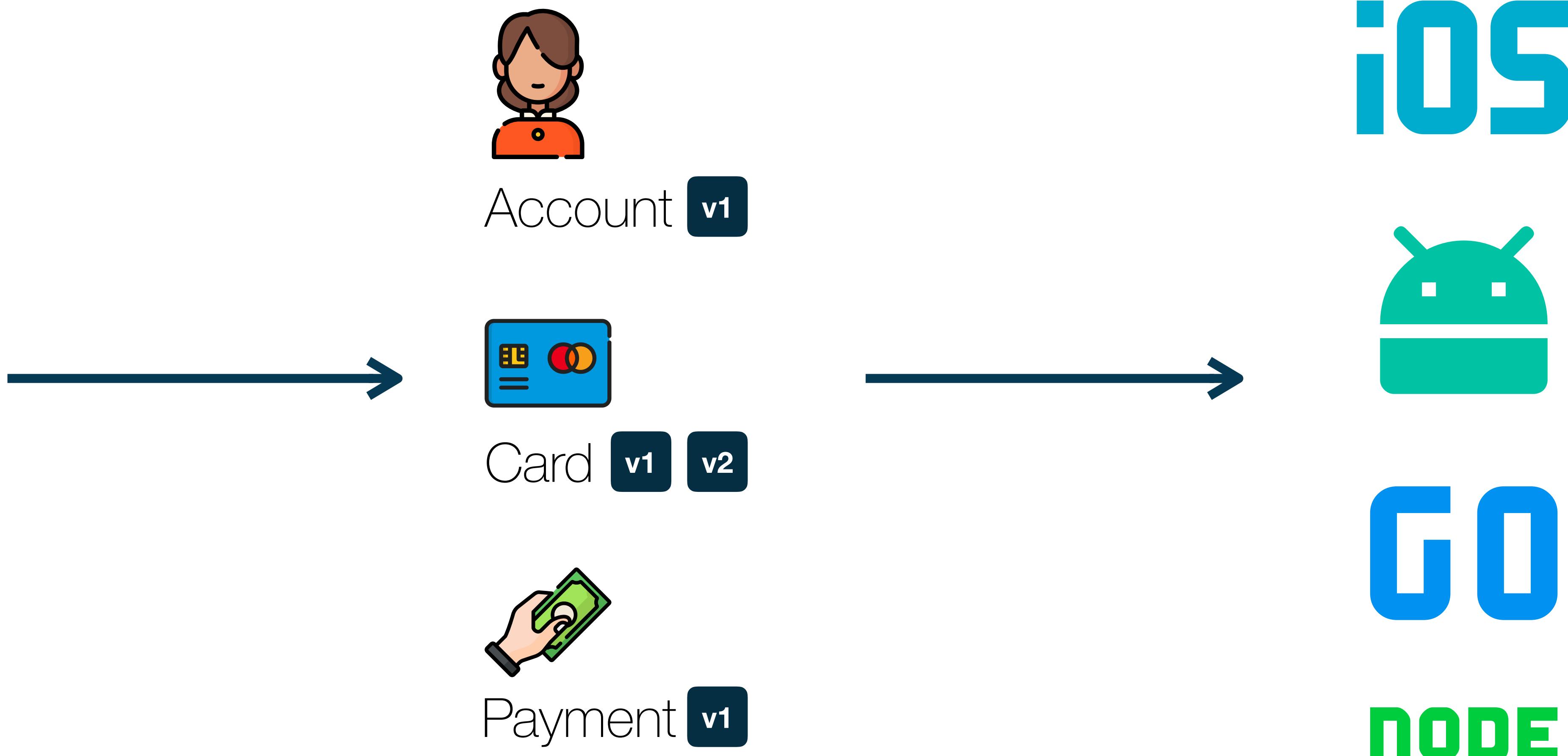


Card **v1** **v2**



Payment **v1**

OpenAPI

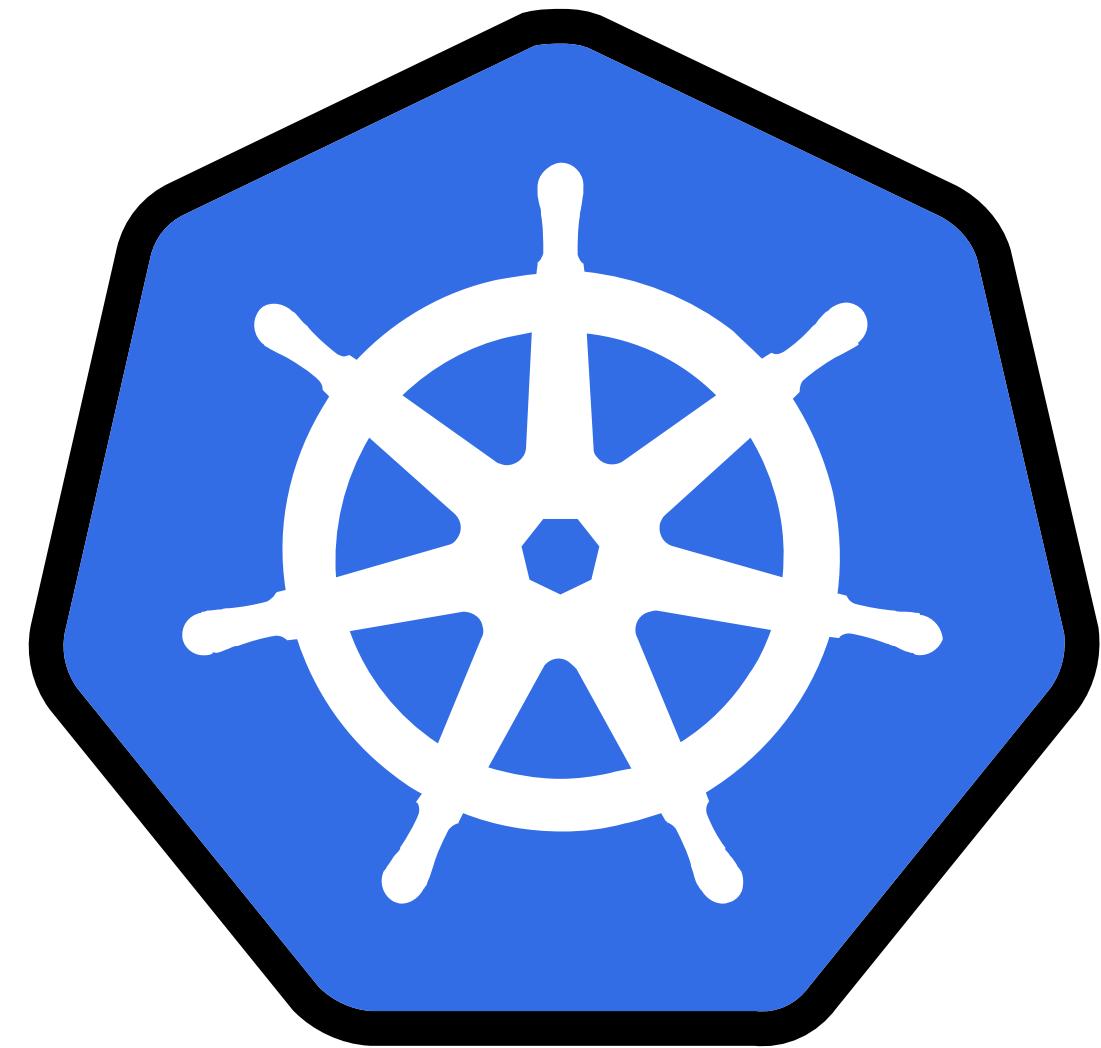




ios

- Native app written in Kotlin
- Gradle for dependencies
- Android JetPack (AndroidX)
- Coroutines
- CircleCI → Fastlane → Google Play
- Native app written in Swift 5
- CocoaPods for dependencies
- Model–view–viewmodel (MVVМ)
- Storyboard-reference
- CircleCI → Fastlane → TestFlight

Kubernetes

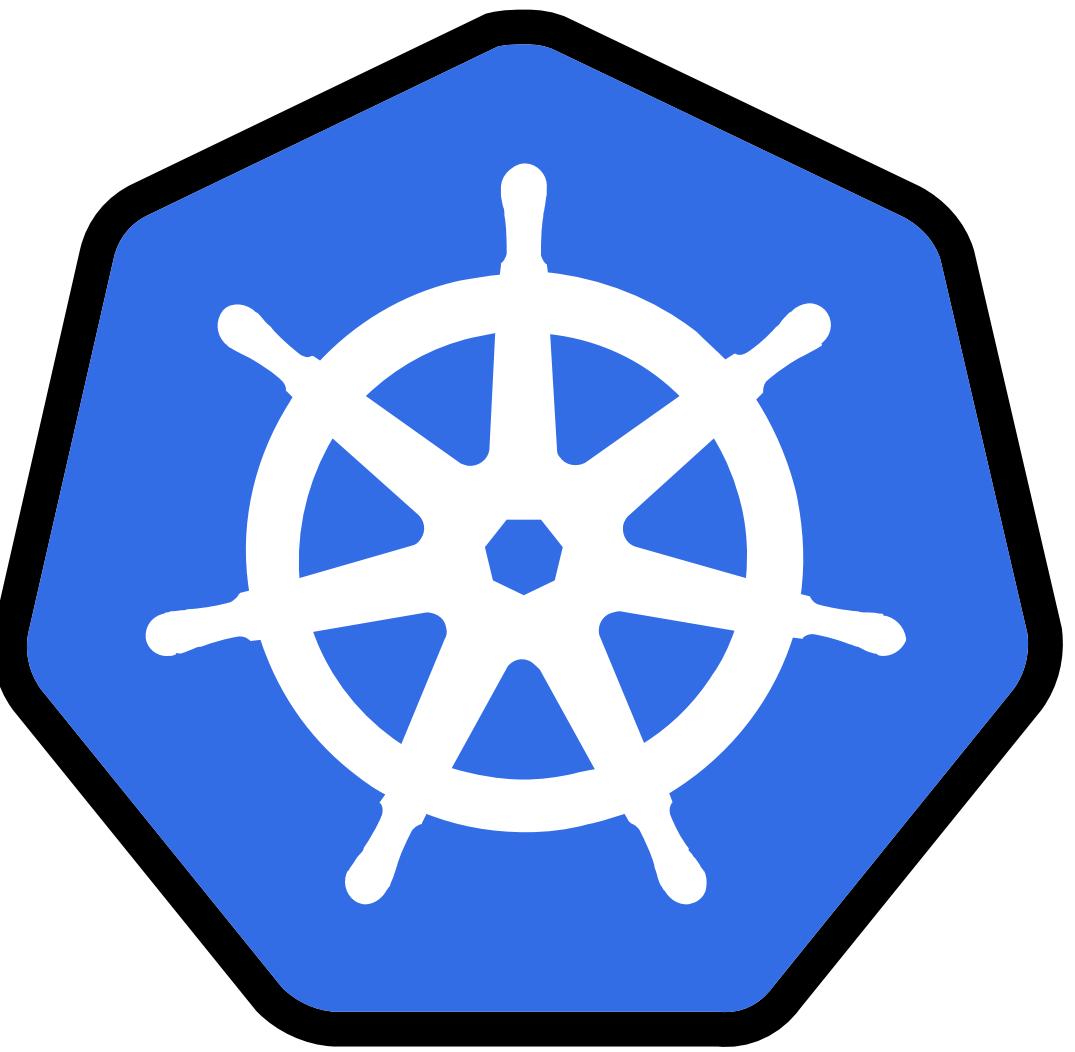


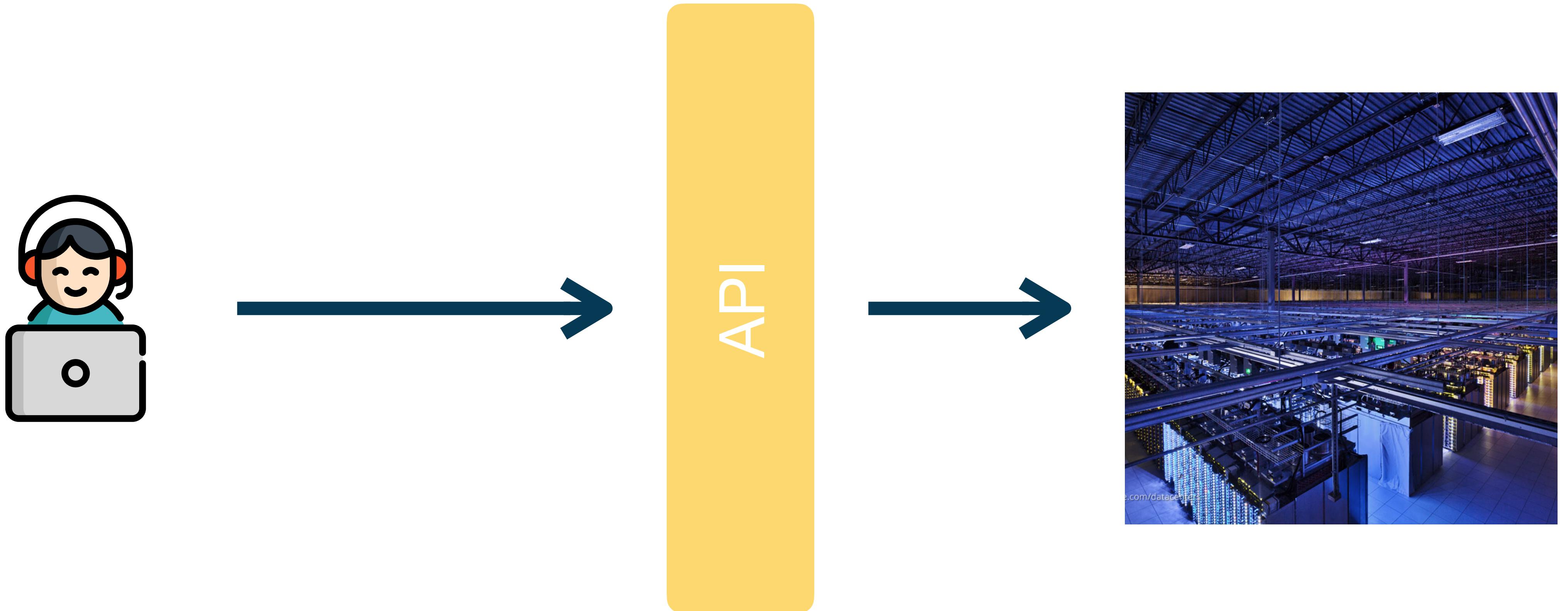
kubernetes

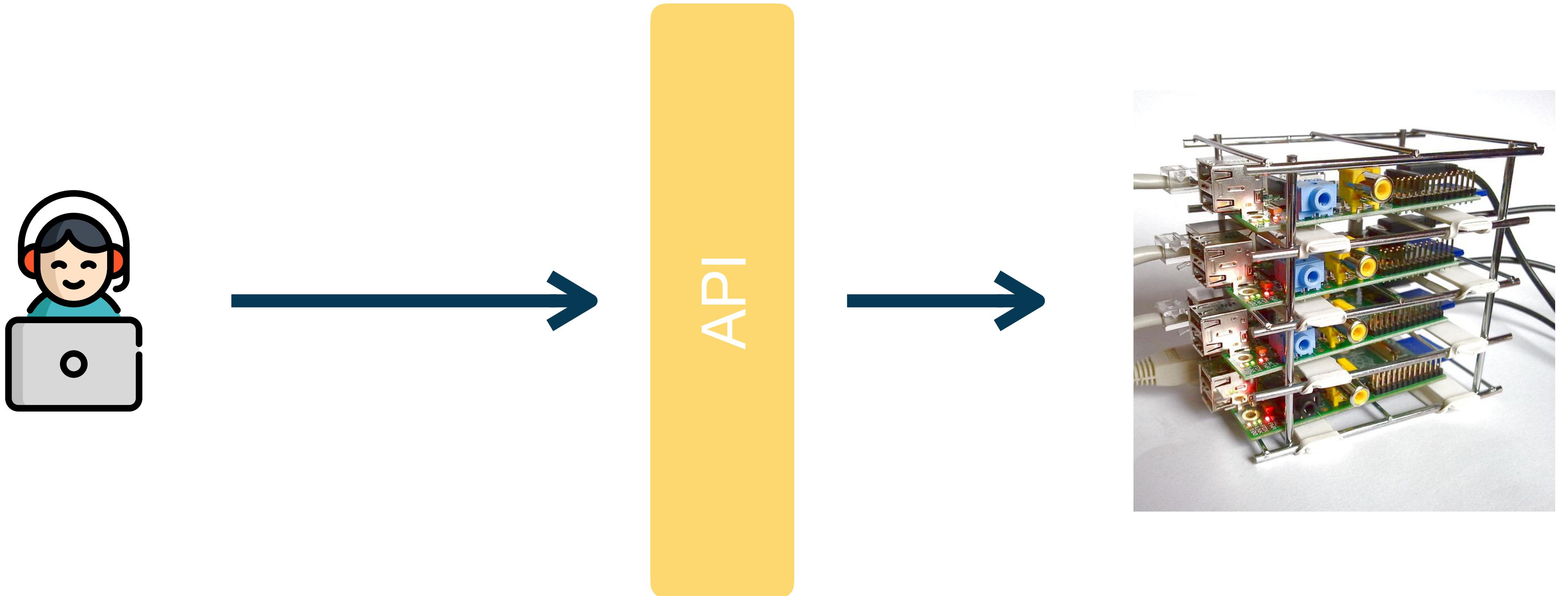
Kubernetes

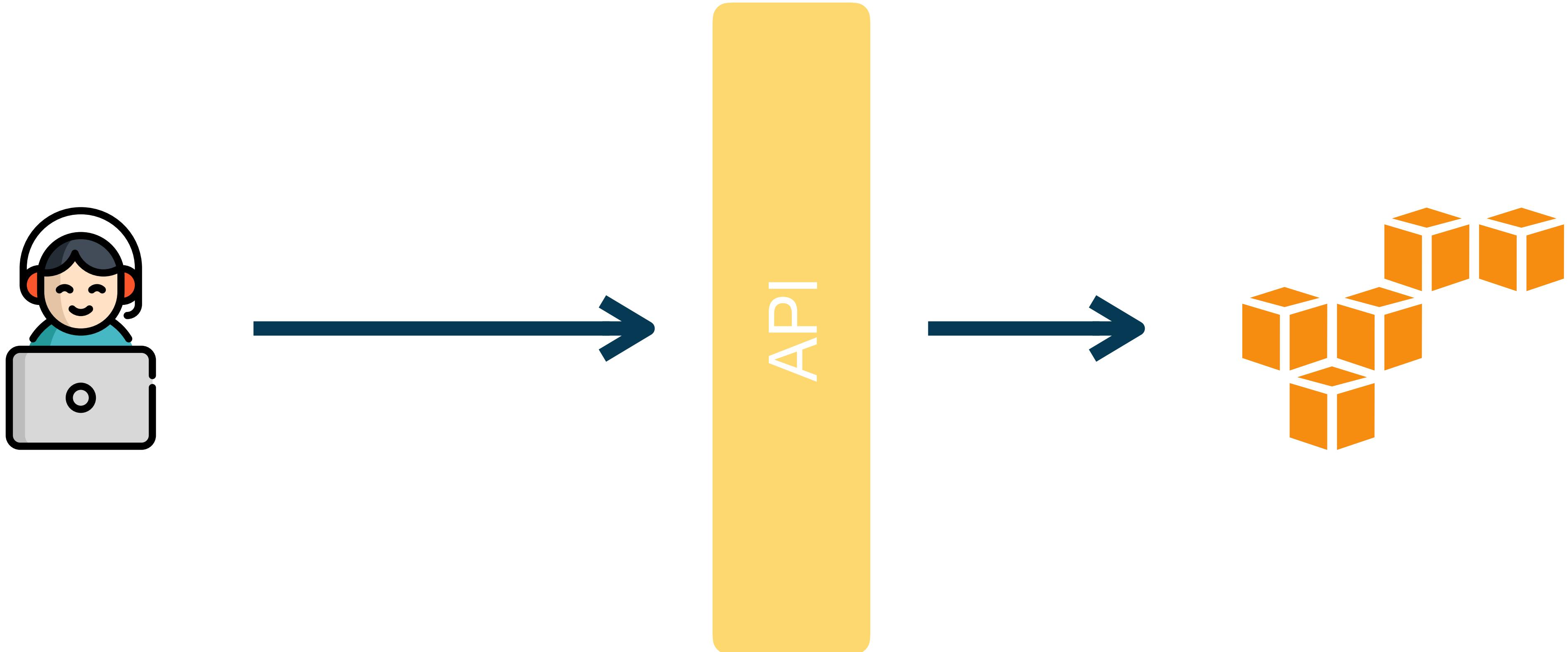
Greek for "Helmsman"

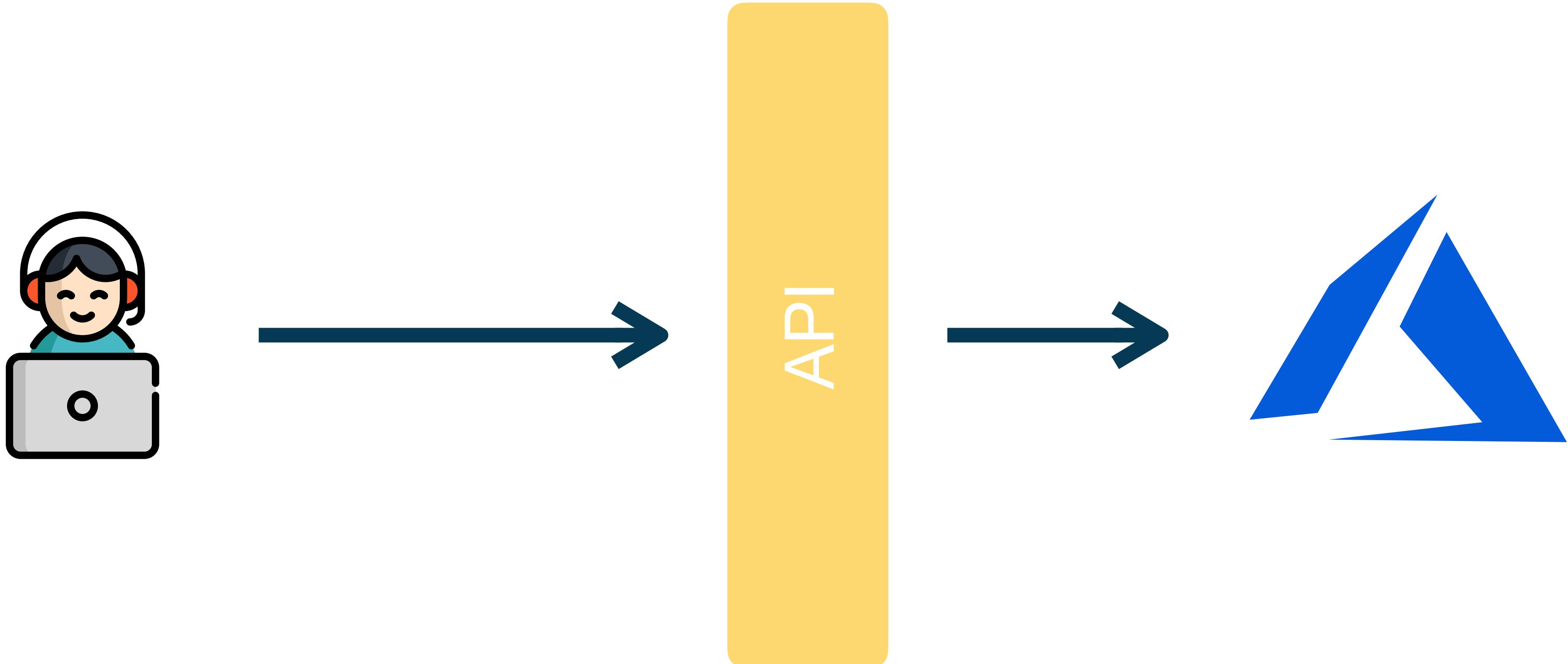
- Container orchestrator
- Based on Google's internal systems
- Runs on cloud or bare-metal
- Supports multiple container runtimes

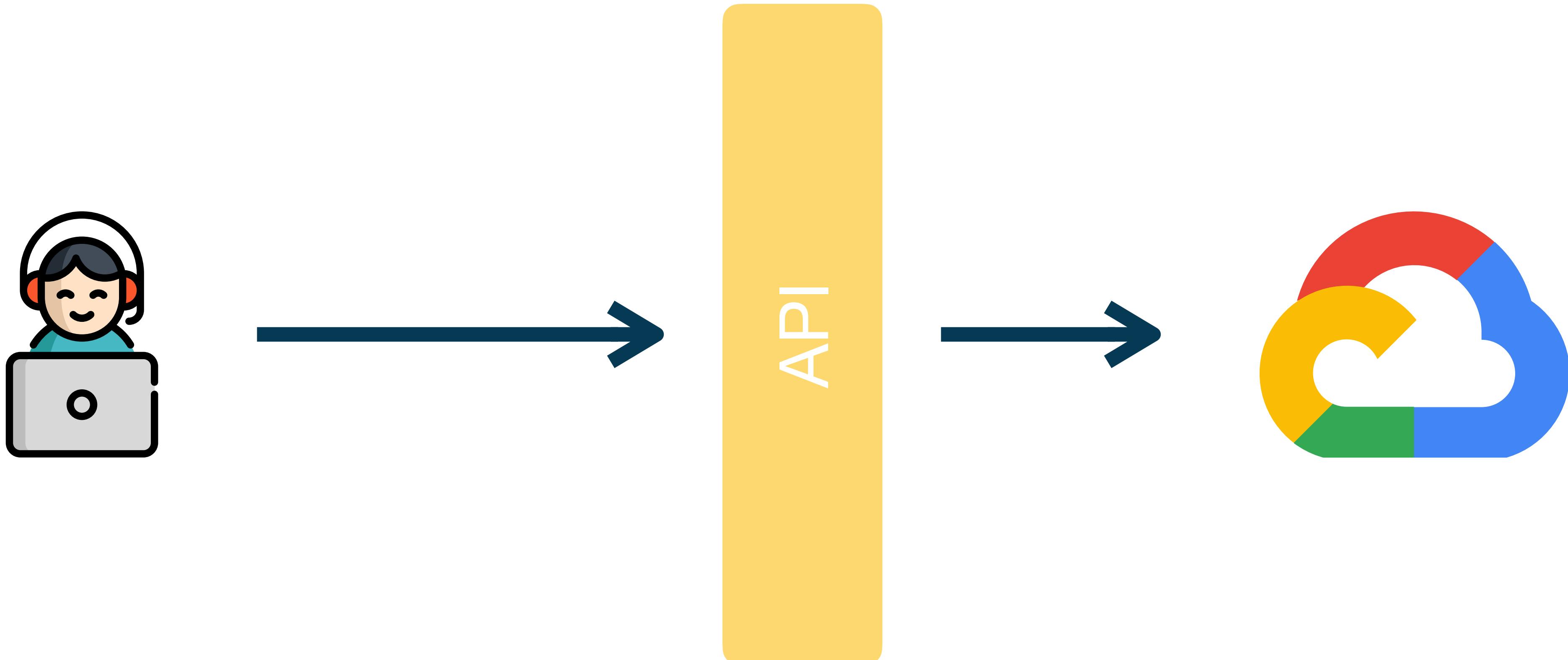




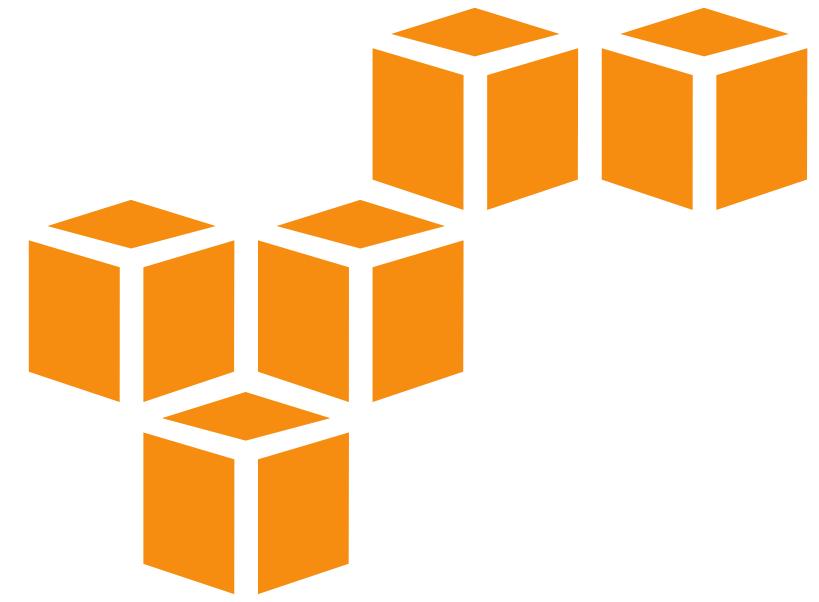




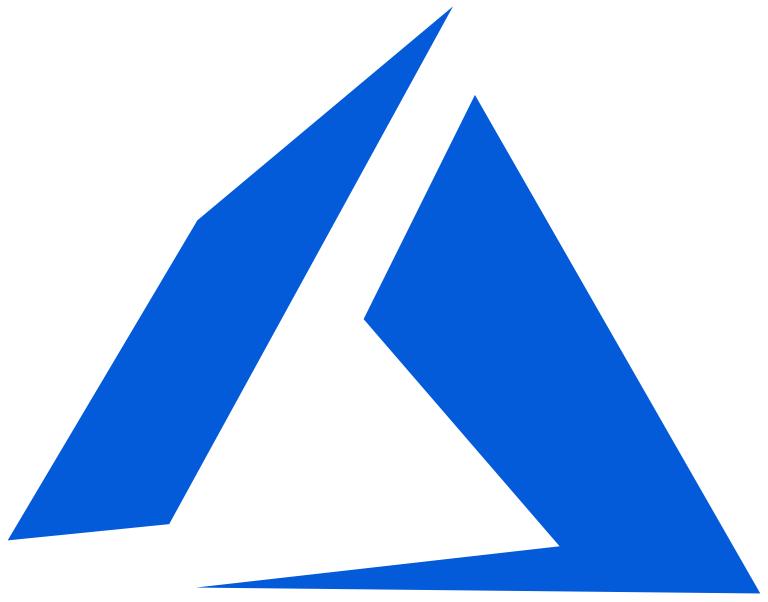




One-Click Managed Kubernetes



Amazon EKS

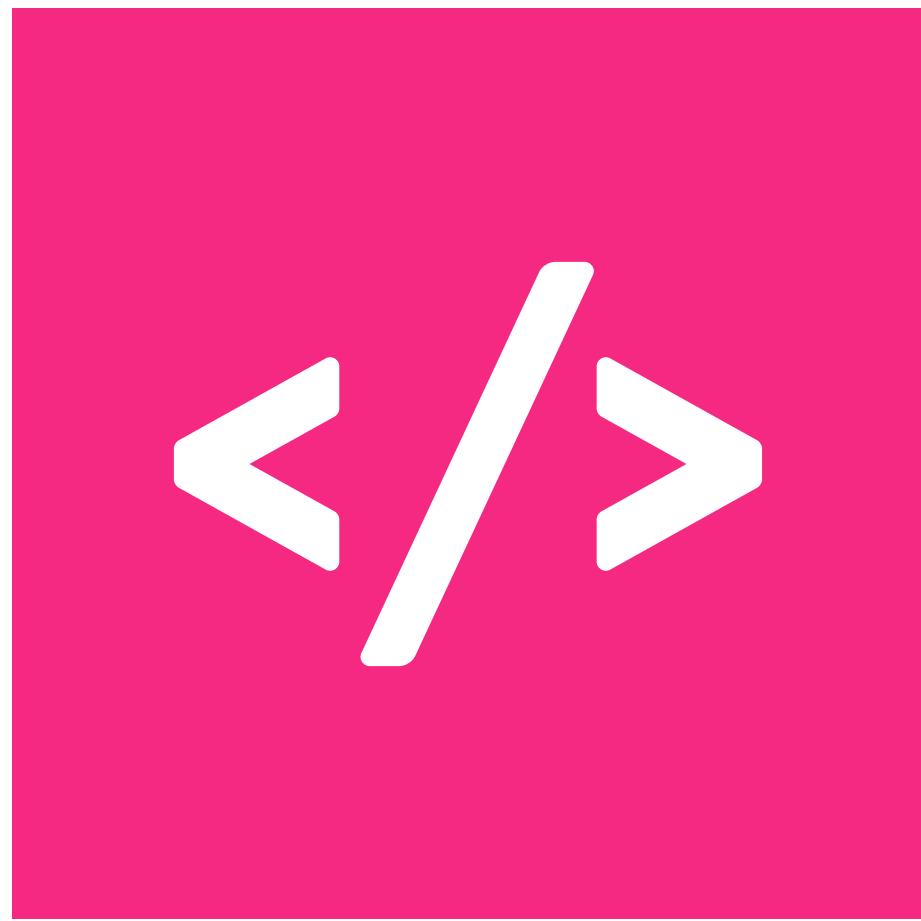


Microsoft AKS



Google GKE

Kubernetes in a Nutshell



API First

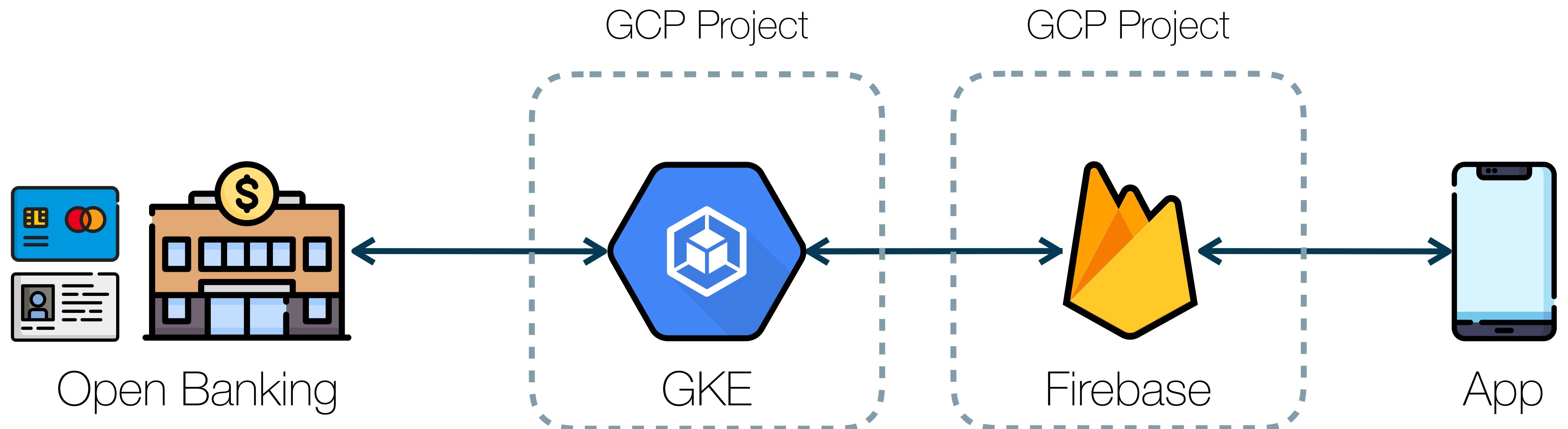


Modular

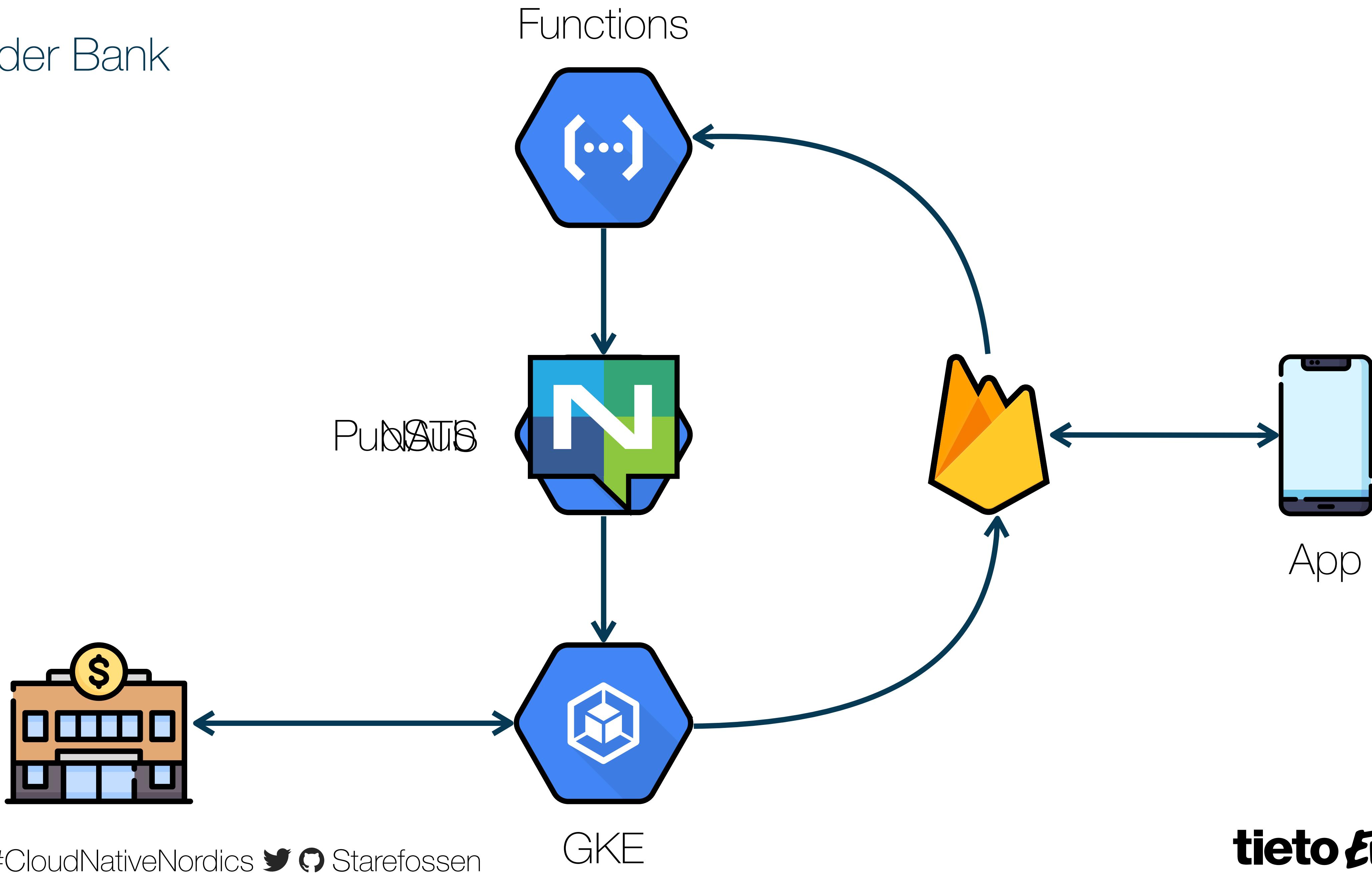


Self Healing

Bulder Bank



Bulder Bank



NATS

- High performance messaging system
 - Publish-subscribe
 - Atleast once-delivery
- Static binary written in Go
- First release in 2013
- Official CNCF Project



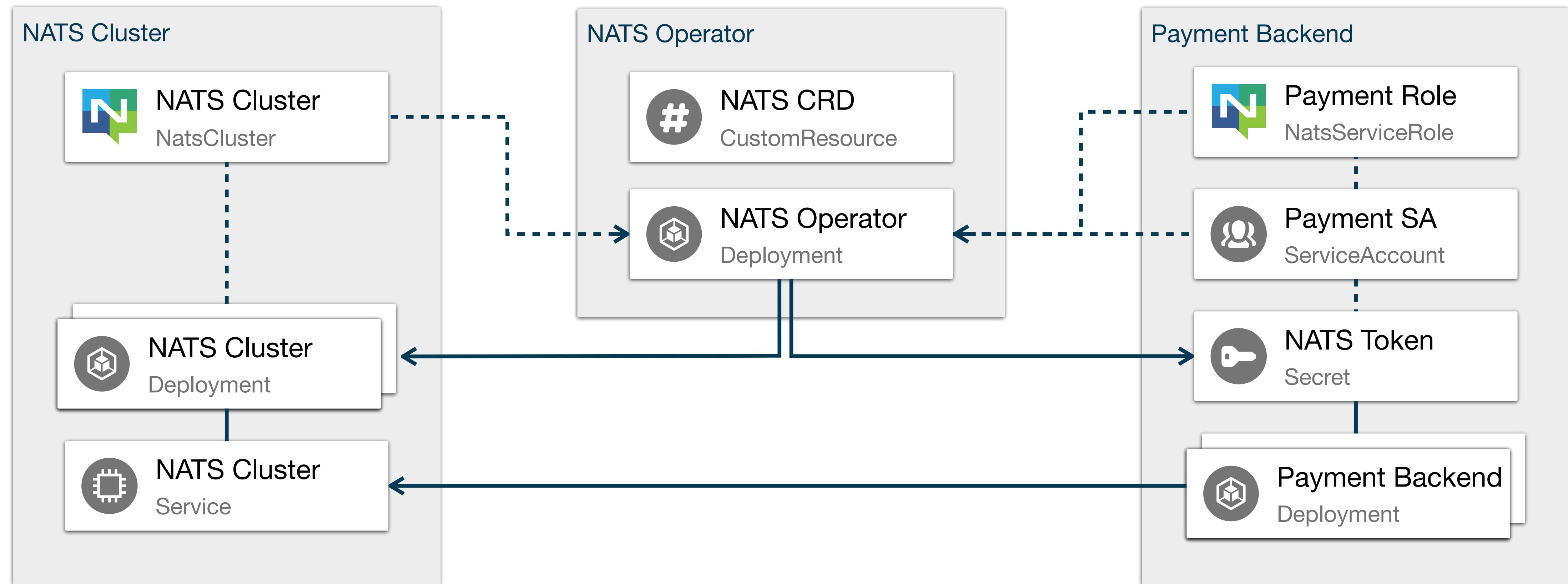
Kubernetes Operators

- Building Kubernetes native applications
 - Extends the Kubernetes API
 - Runs inside Kubernetes
 - Built for a specific application
 - Runs inside Kubernetes
 - Lifecycle; scaling, upgrading, and recovery
 - Well suited for complex applications

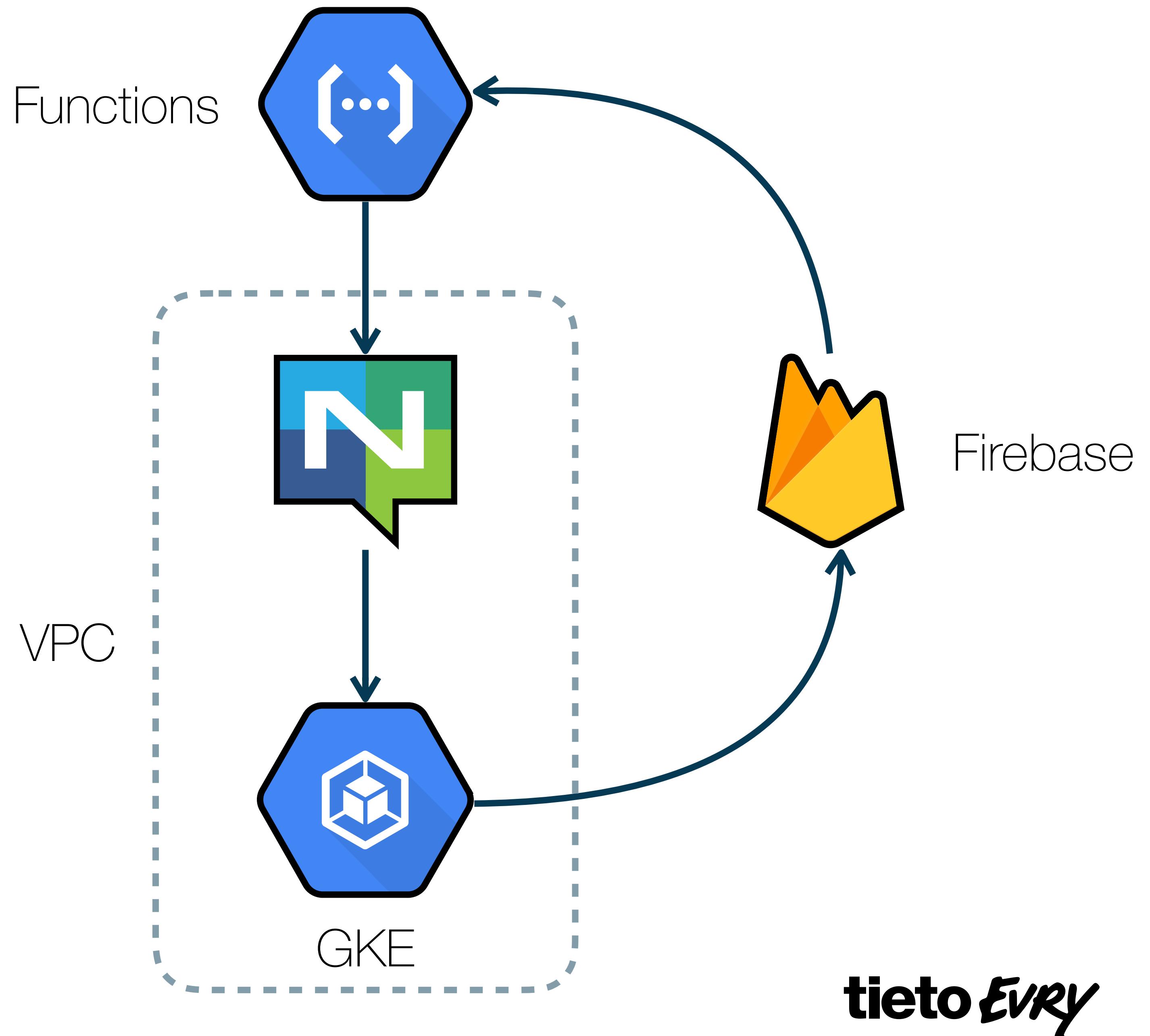


```
apiVersion: monitoring.coreos.com/v1
kind: Prometheus
metadata:
  name: prometheus
spec:
  serviceAccountName: prometheus
  serviceMonitorSelector:
    matchLabels:
      team: frontend
  resources:
    requests:
      memory: 400Mi
  enableAdminAPI: false
```

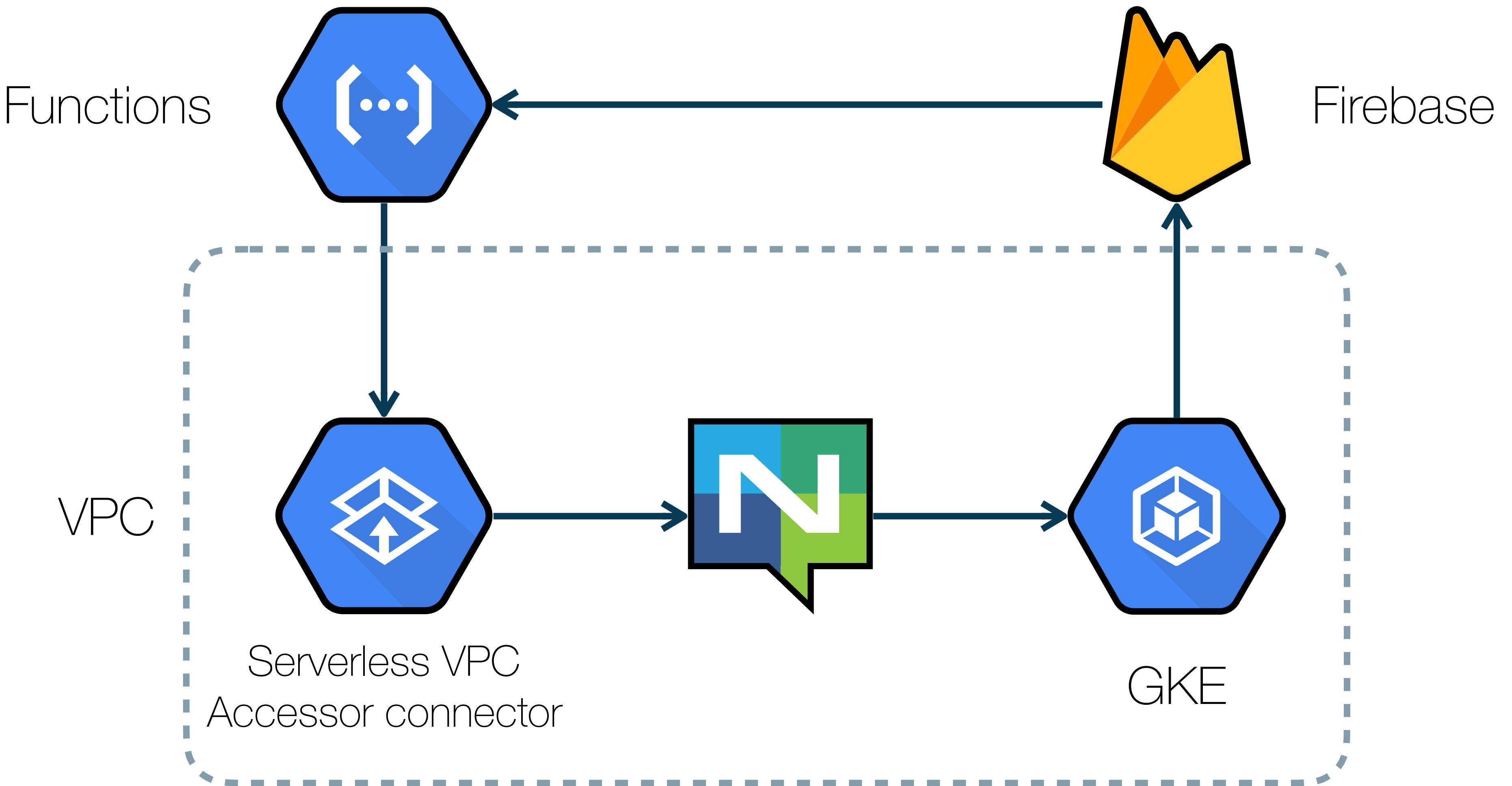
NATS Operator



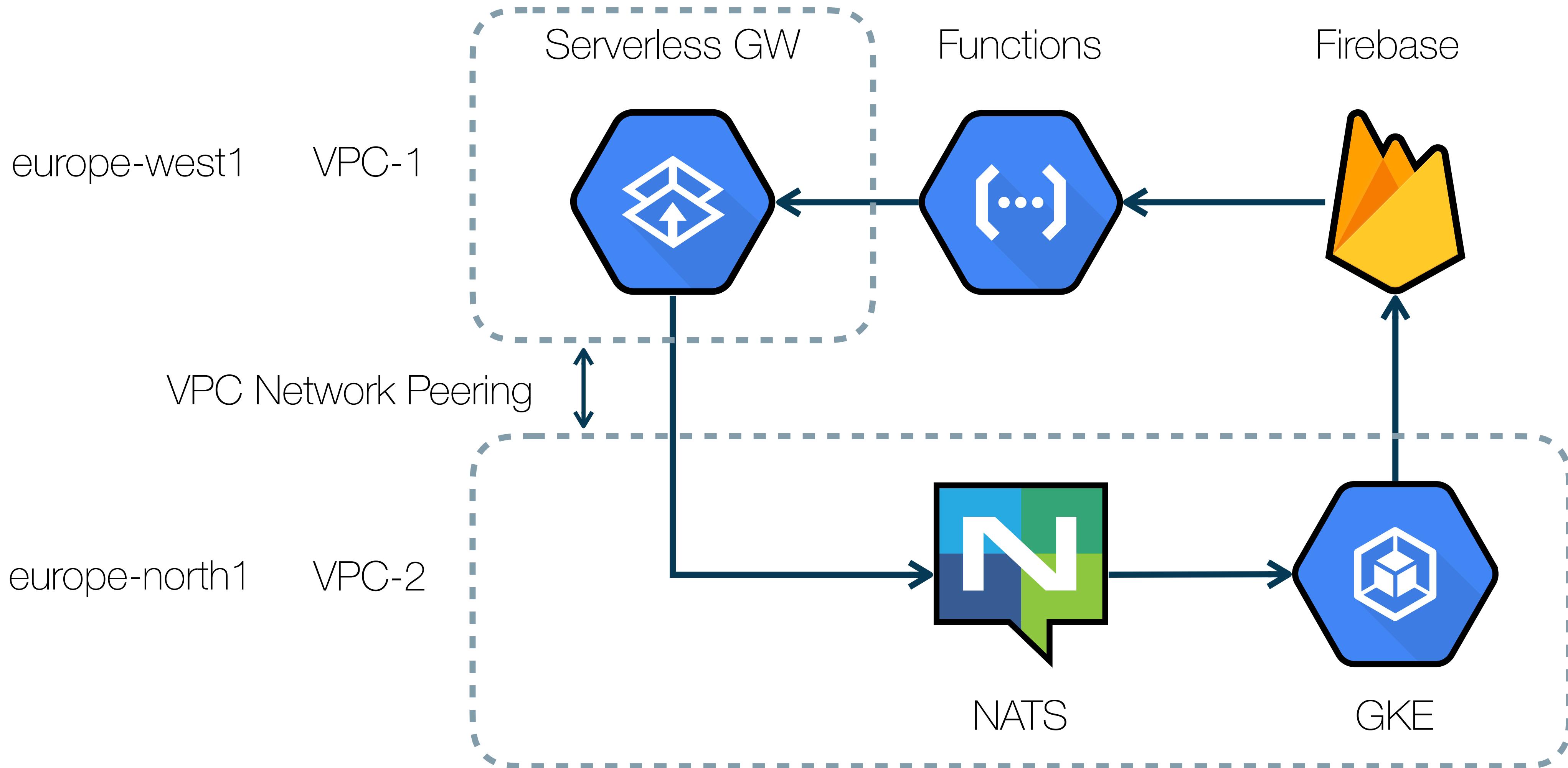
Cloud Functions → NATS



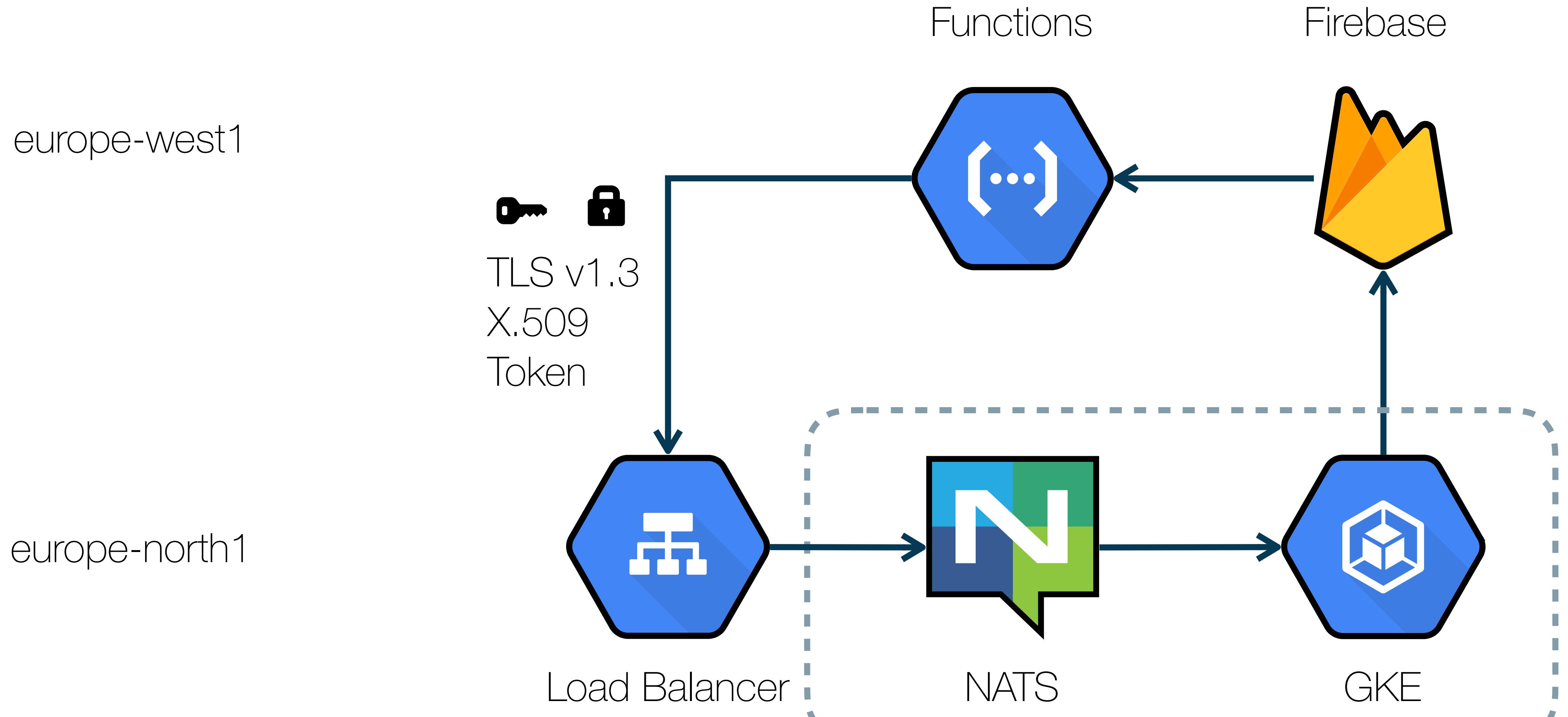
Cloud Functions → NATS



Cloud Functions → NATS



Cloud Functions → NATS



What if we could run Serverless Functions inside Kubernetes?

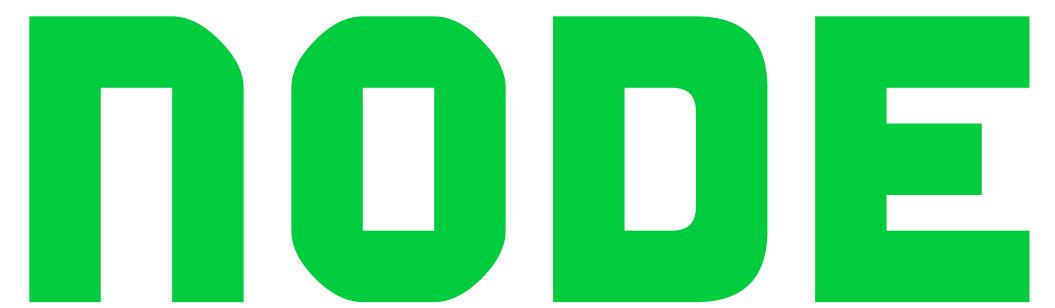
Knative

- Serverless Containers on Kubernetes
- Built by Google, IBM, RedHat++
- Runs on top of Istio
 - Build – source-to-container
 - Serving – run serverless containers
 - Eventing – universal subscriptions
- Managed Knative with Google Cloud Run

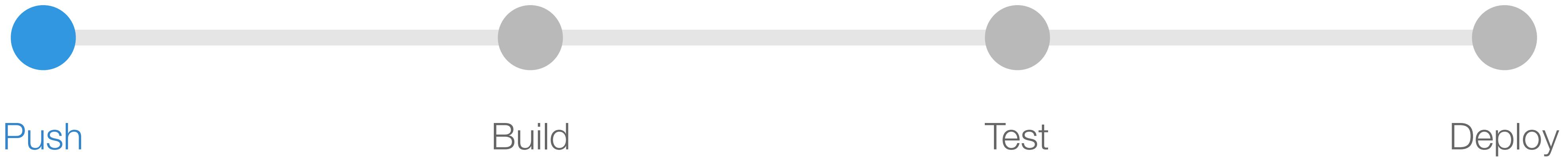


Backend Services

- Go v1.12
 - APIs and functions
 - gRPC (and some REST)
- No framework!
- Node.js v10 LTS
 - BulderBank.no
 - Administration

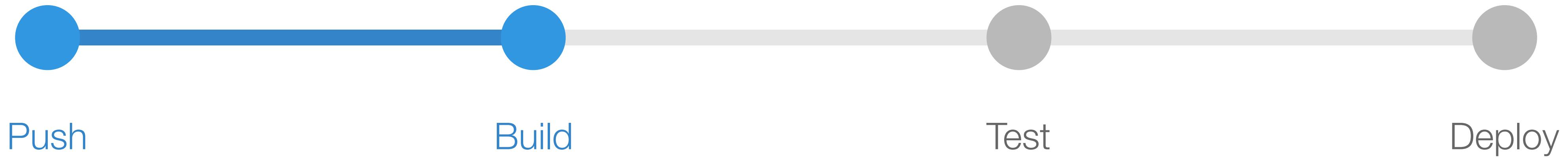


Software Delivery Pipeline



- All changes must go through Git!
- CircleCI automatically starts on push
- Audit and traceability for all changes

Software Delivery Pipeline



- Fetch and install dependencies
- Automated and reproducible!

Software Delivery Pipeline

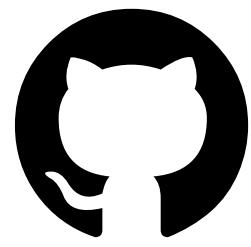


- Syntax linting (go fmt)
- Unit testing, integration testing
- Source code scanning (SonarCloud)
- Dependency scanning (Snyk)

Software Delivery Pipeline



- Build and sign images
 - Deploy and promote (Helm)
- dev → test → prod
- No cuts, No bugs, No coconuts 🍹



Add new features #123

Open

Developer Dave wants to merge 1 commit into master from new-feature

Conversation 4

Commits 3

Files changed 5

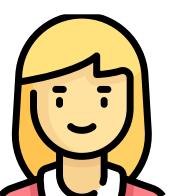


Developer Dave commented 23 minutes ago

This pull request adds all the new features to our awesome application 😊 Now we are ready to rock our competitors 🎉

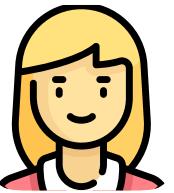
Add new backend functionality af231ce

Add new security roles de0230f



Security Sarha requested changes 17 minutes ago

Update roles based on feedback from Sarha ad77b09



Security Sarha approved these changes 6 minutes ago

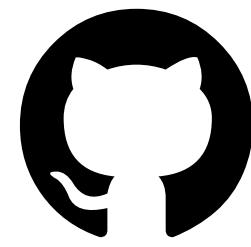


Teamlead Tom approved these changes 4 minutes ago

Reviewers

Security Sarha

Teamlead Tom



Add new features #123

Open

Developer Dave wants to merge 1 commit into master from new-feature

Conversation 4

Commits 3

Files changed 5

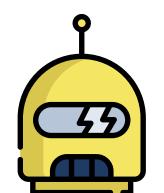


Developer Dave commented 23 minutes ago

This Pull Request adds all the new features to our awesome application 😃 Now we are ready to rock our competitors 🎉

Add new backend functionality af231ce

Add new security roles de0230f



Security Bot requested changes 22 minutes ago

Update roles based on feedback from Security Bot ad77b09



Security Bot approved these changes 6 minutes ago



Teamlead Tom approved these changes 4 minutes ago

Reviewers

Security Bot ✓

Teamlead Tom ✓



255

Build Hours Month

iOS

Android

Go

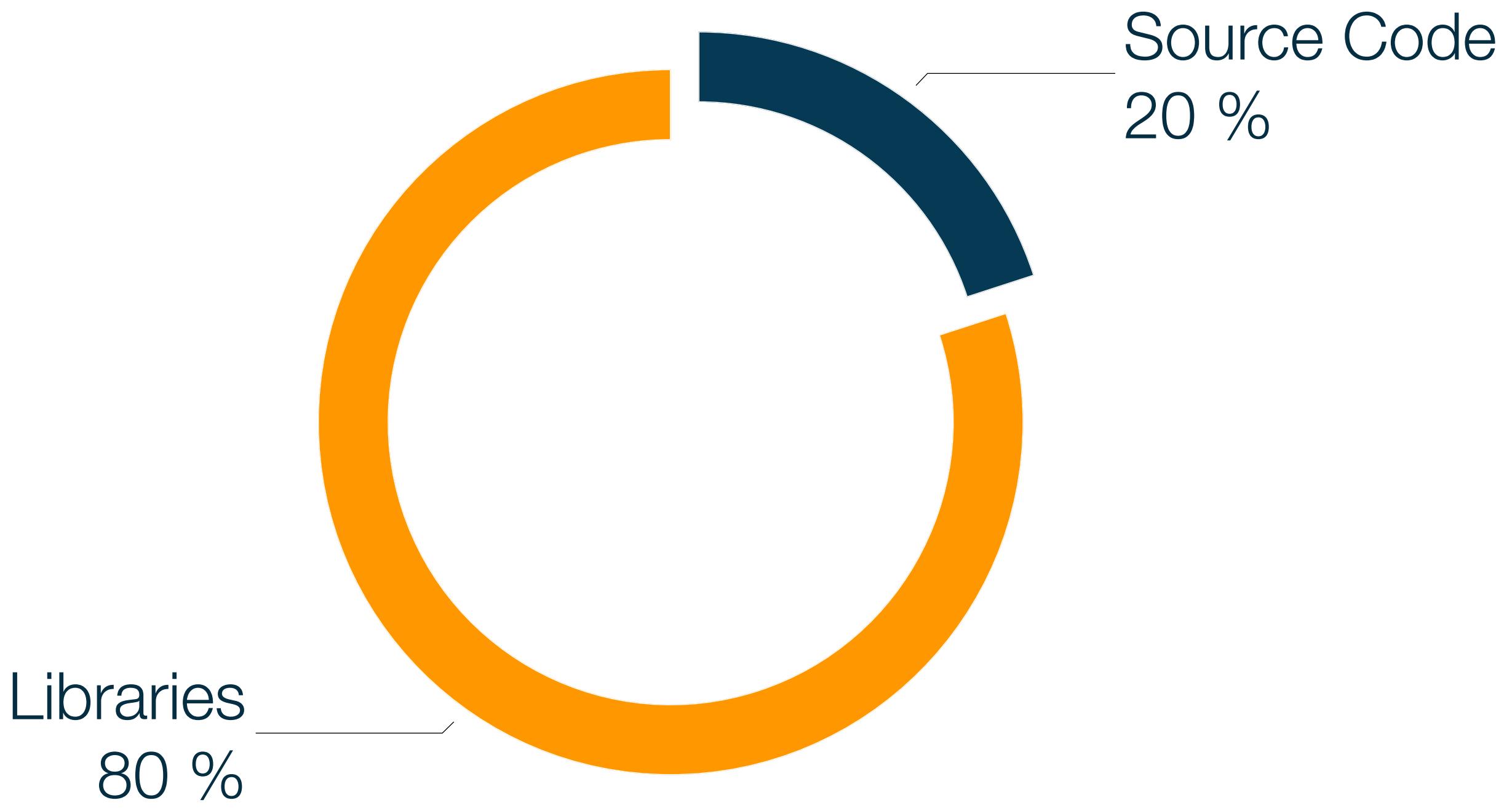
Functions

Web

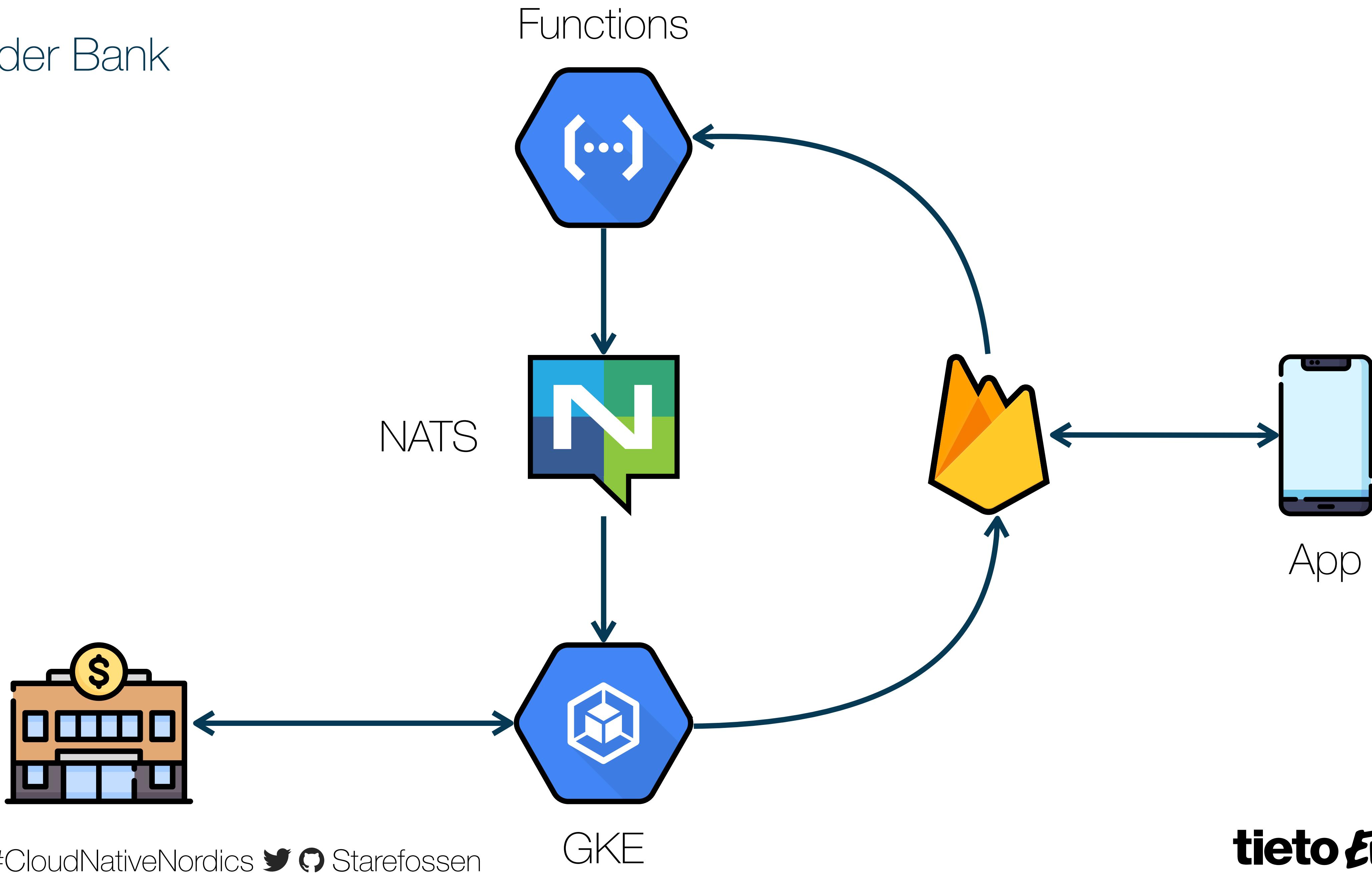
TF

Applications are 'assembled'

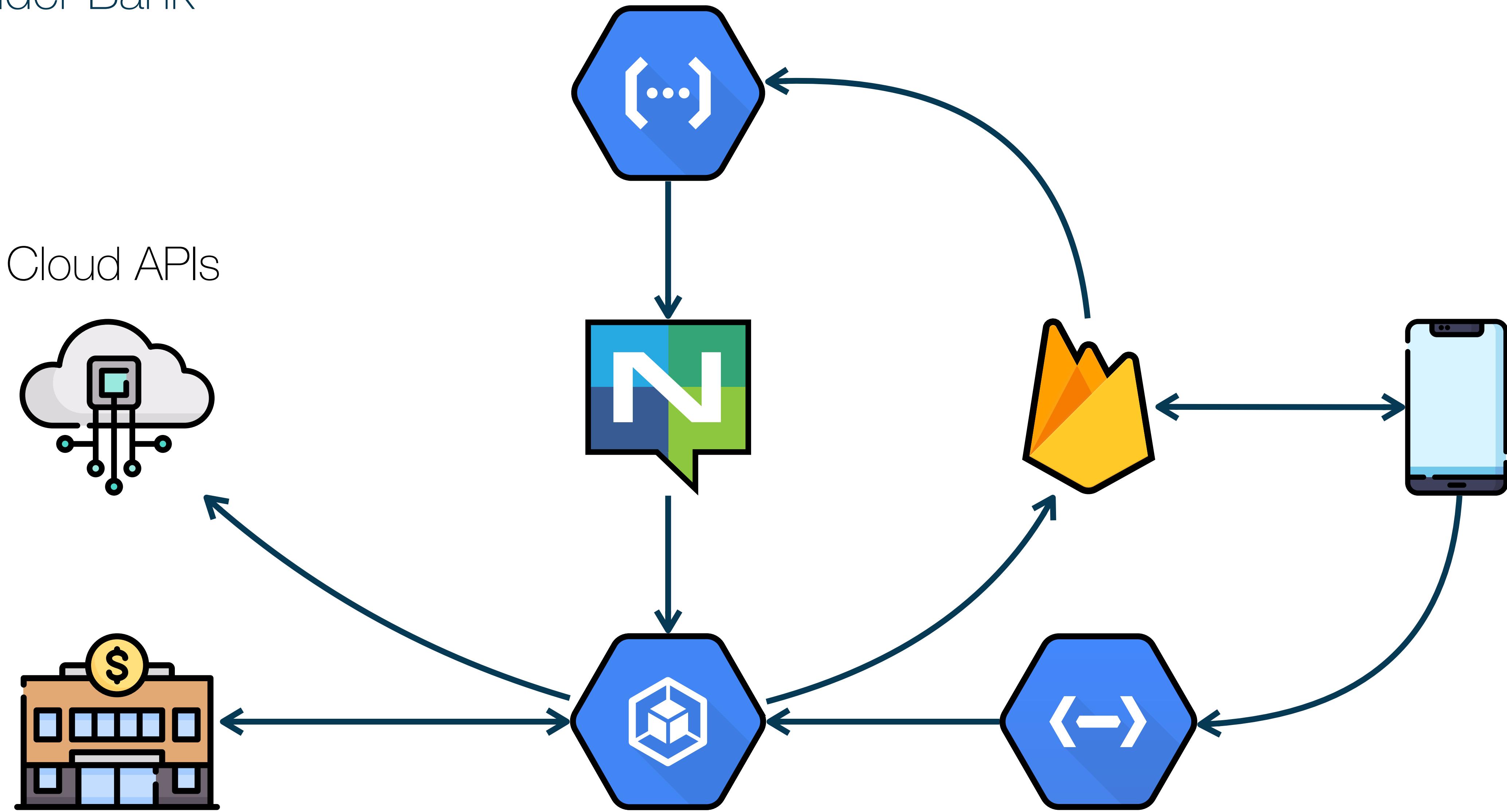
- Not all are created equal, some are healthy and some are not
- All go bad over time, they age like milk, not like wine
- Enterprises consumes on average 229.000 software components annually, of which 17.000 had a known security vulnerability.



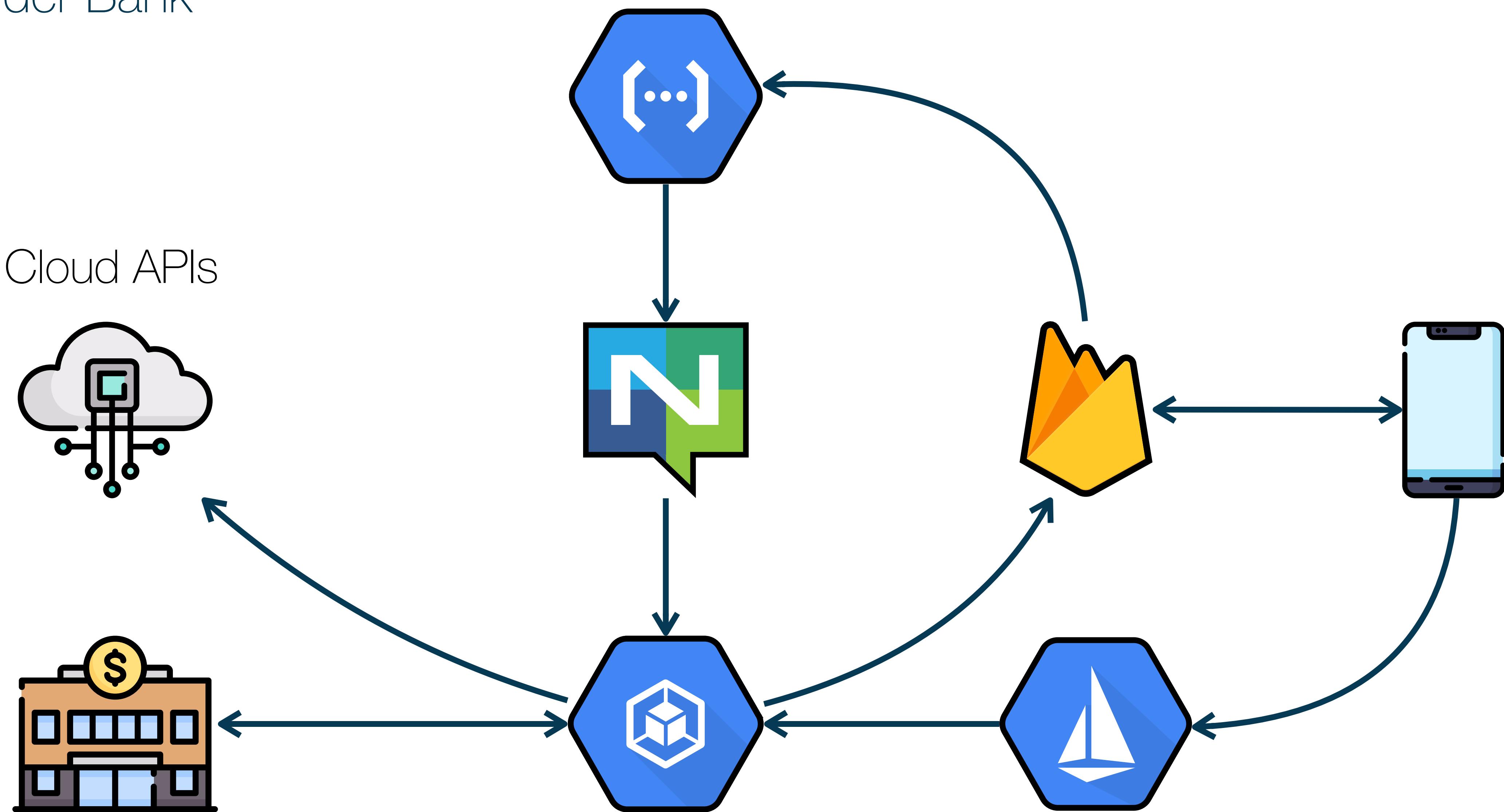
Bulder Bank



Bulder Bank



Bulder Bank



Istio

- Service mesh control plane
- Kubernetes native
- Builds on top of Envoy proxy
- Created by Google, IBM, RedHat, Lyft
- Managed version in GKE



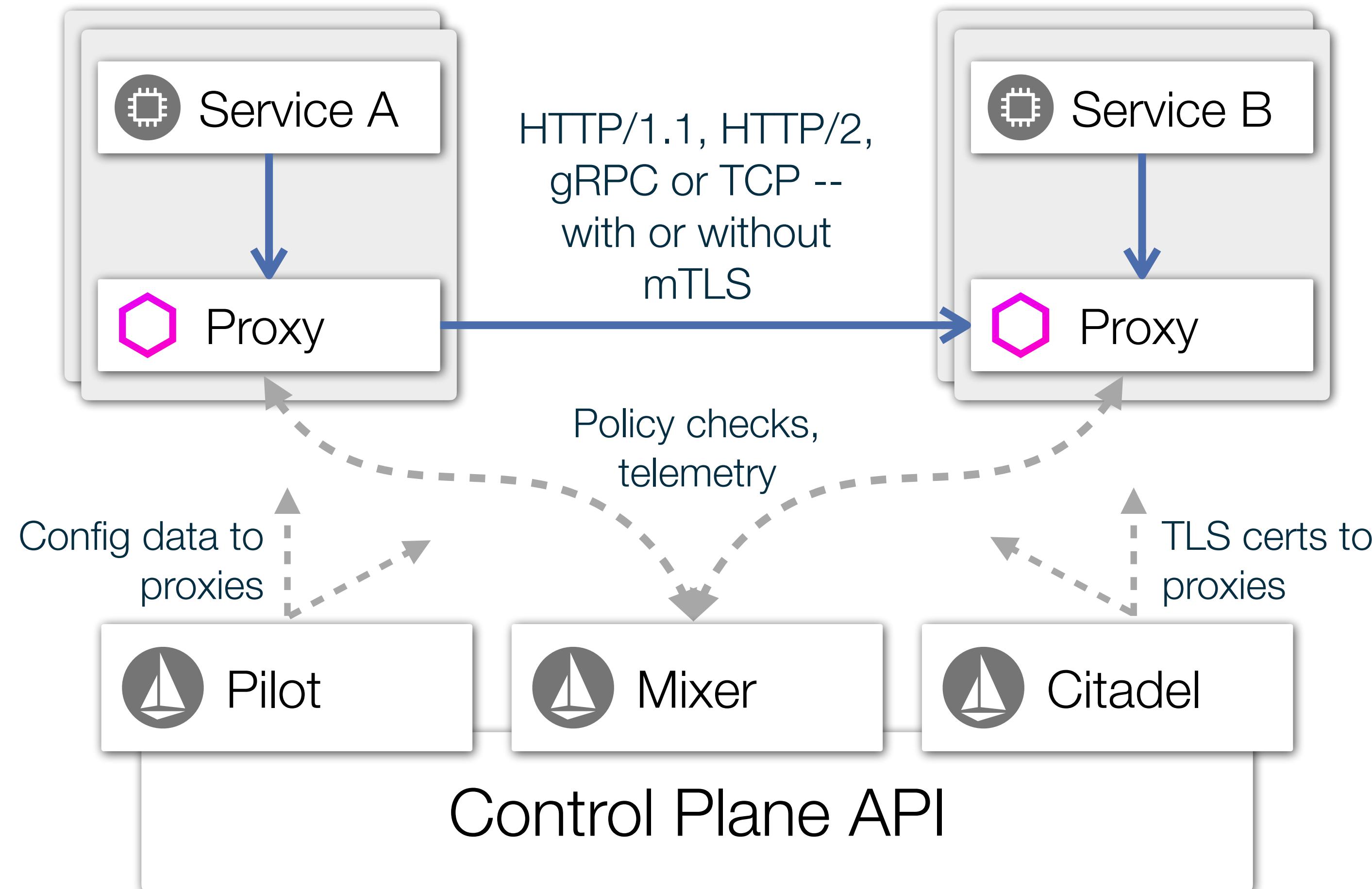
Why Istio?

Microservices must deal with

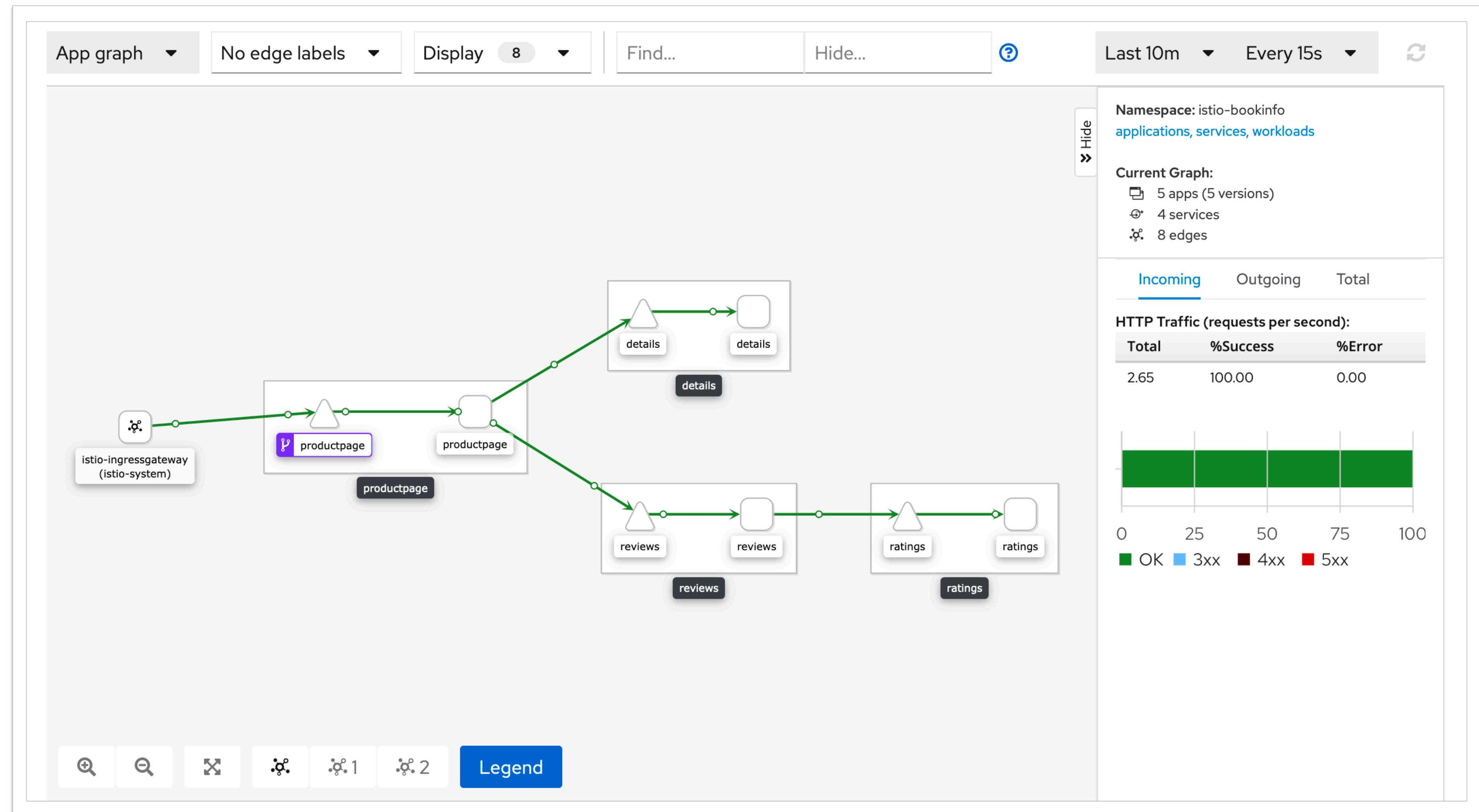
- Client side load balancing
- Timeouts and retries
- Monitoring and tracing
- Traffic encryption
- Traffic policies



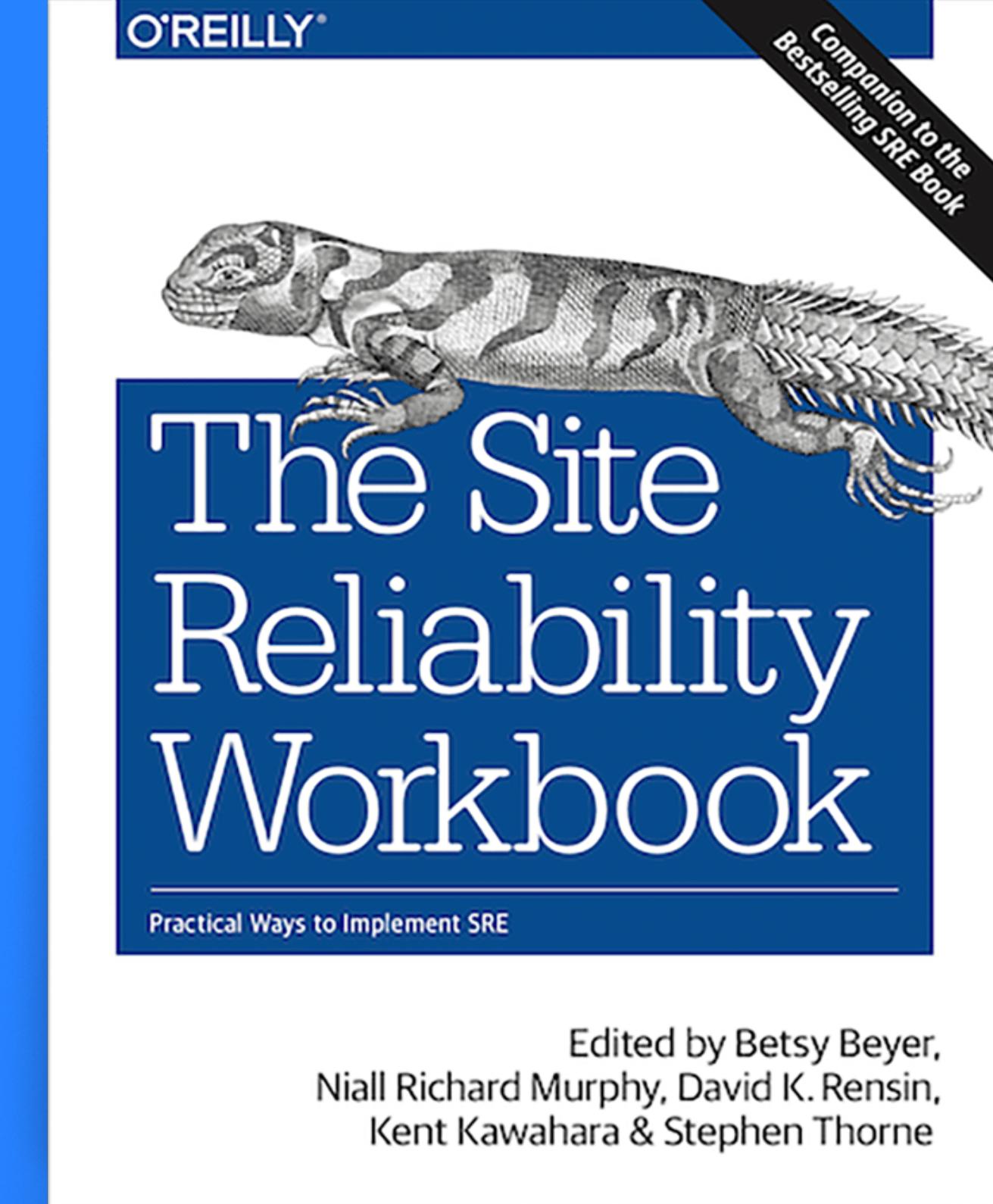
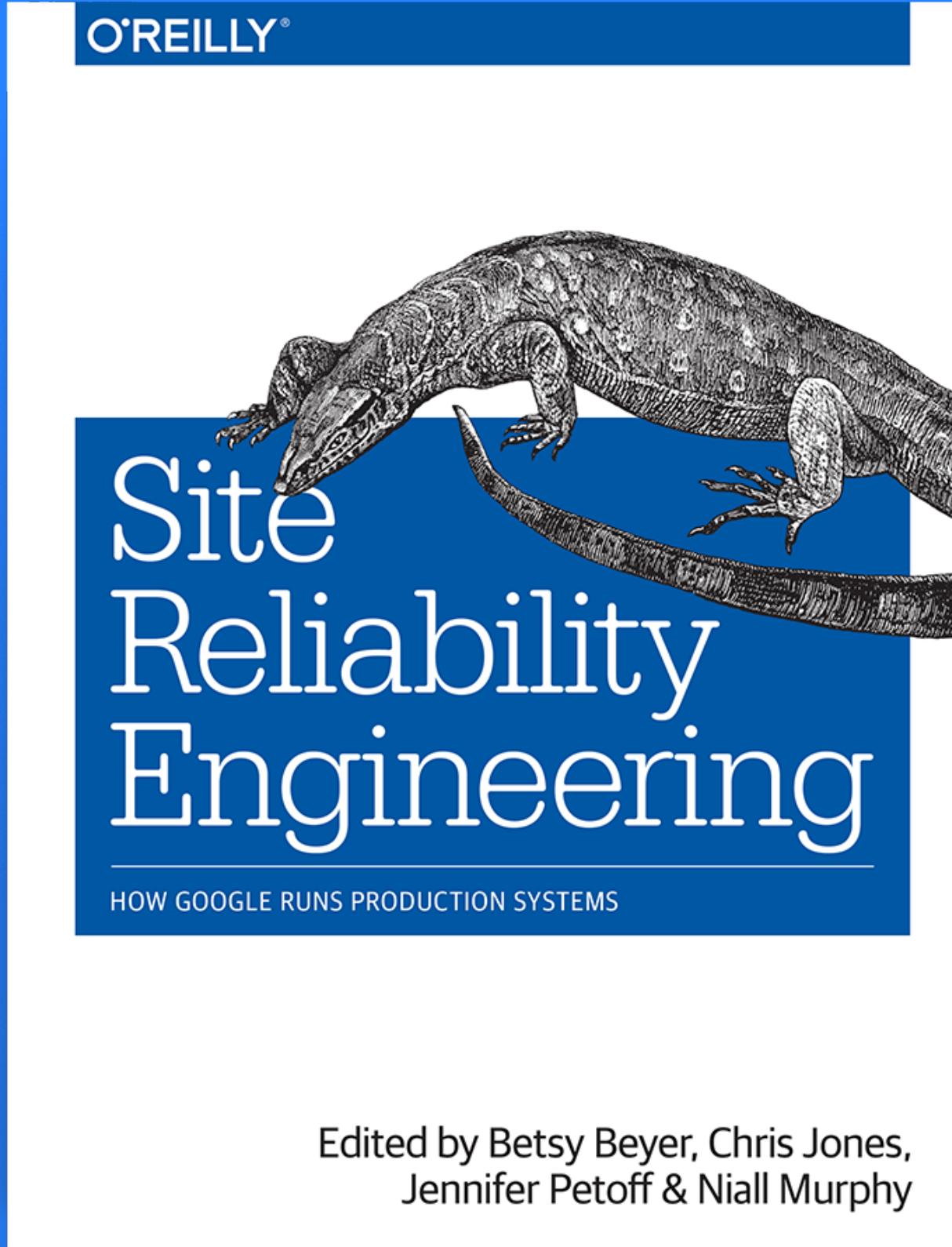
What is a service mesh?



Istio Observability



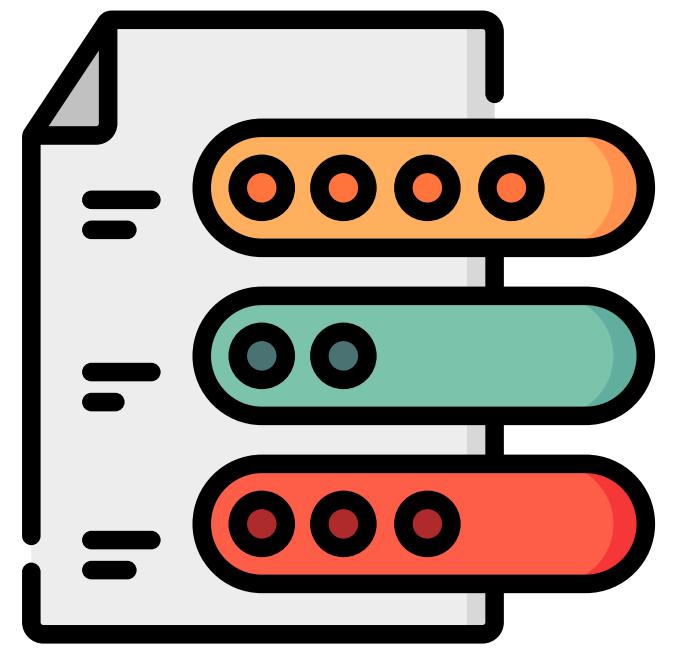
Site Reliability Engineering



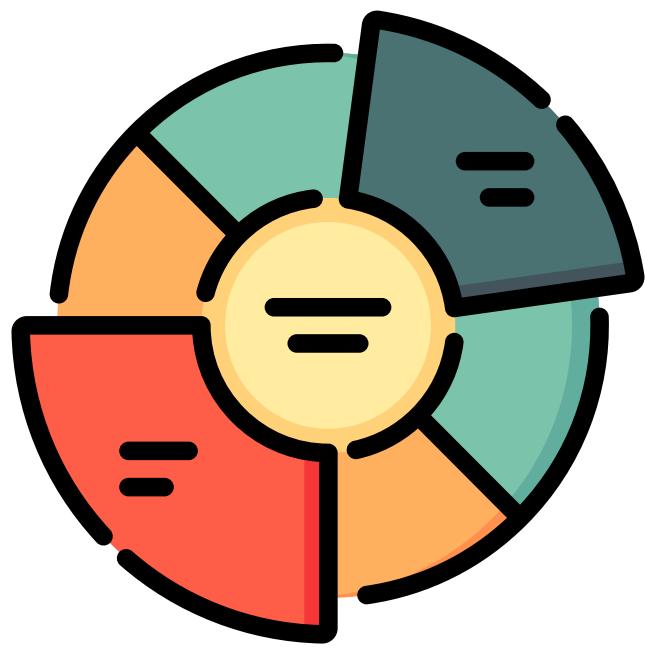
Ben Treynor – Founder of Google's SRE Team

“SRE is what happens when a software engineer is tasked with what used to be called operations”

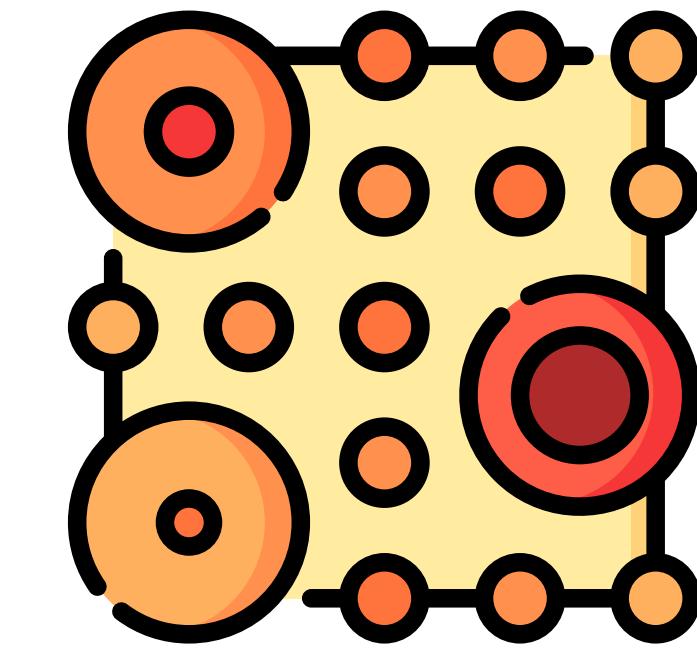
Observability



Logs



Metrics



Tracing

Observability



Prometheus



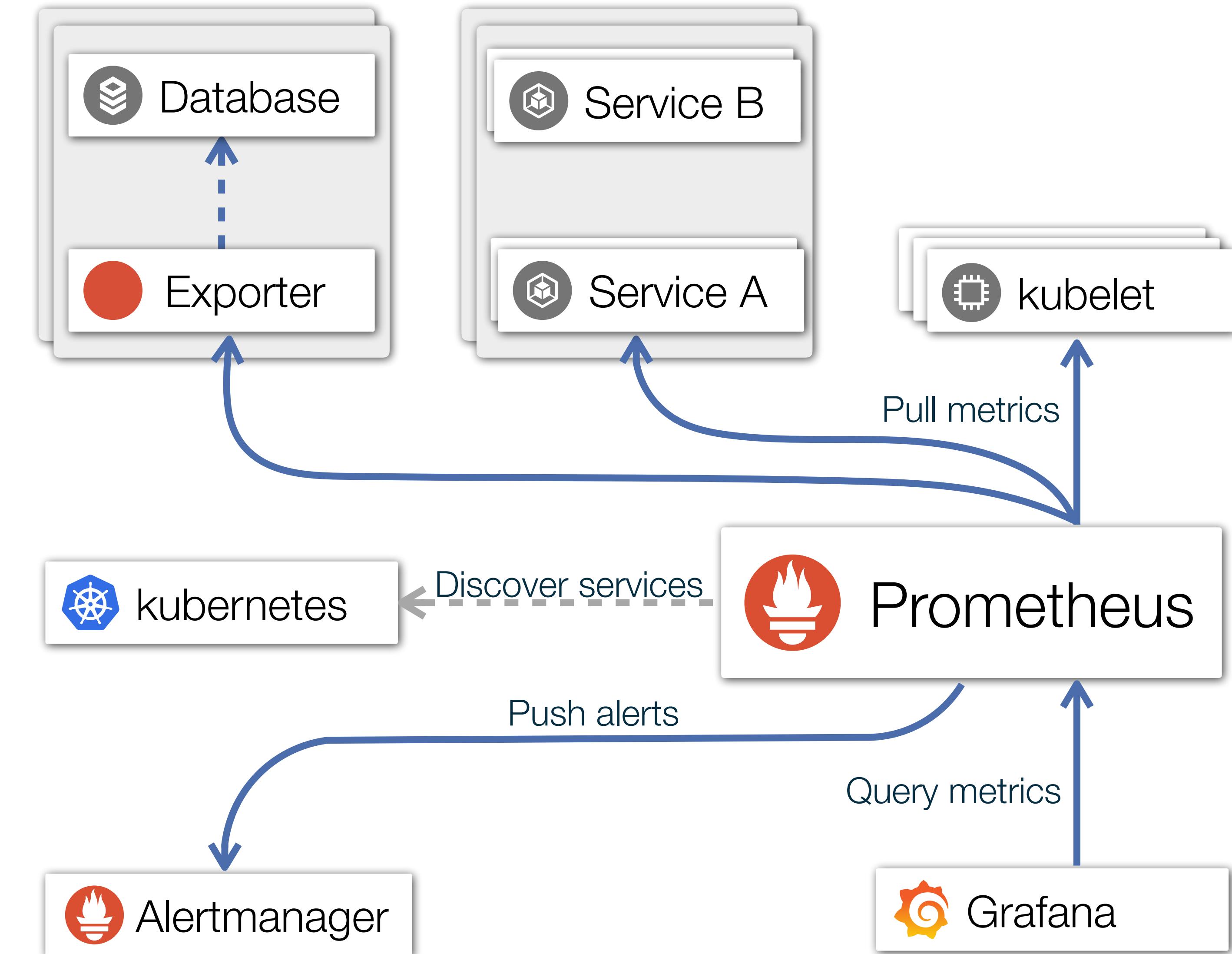
Grafana

Prometheus

Monitoring system and TSDB:

- **Instrumentation**
- **Metrics collection and storage**
- **Querying, alerting, dashboarding**
- **For all levels of the stack**

Auto discovery of new applications





Observability



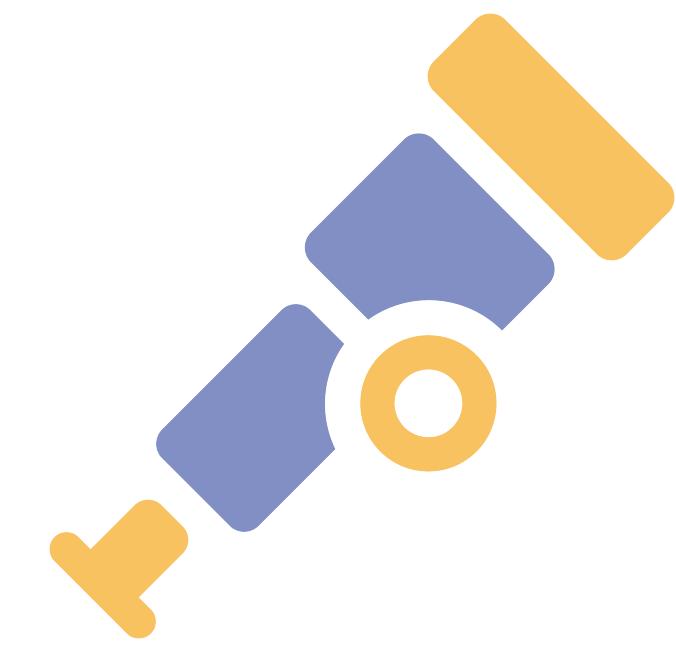
Prometheus



Grafana



Stackdriver



OpenTelemetry

Trace list

+ ANALYZE RESULTS

UNDO ZOOM

▶ AUTO RELOAD

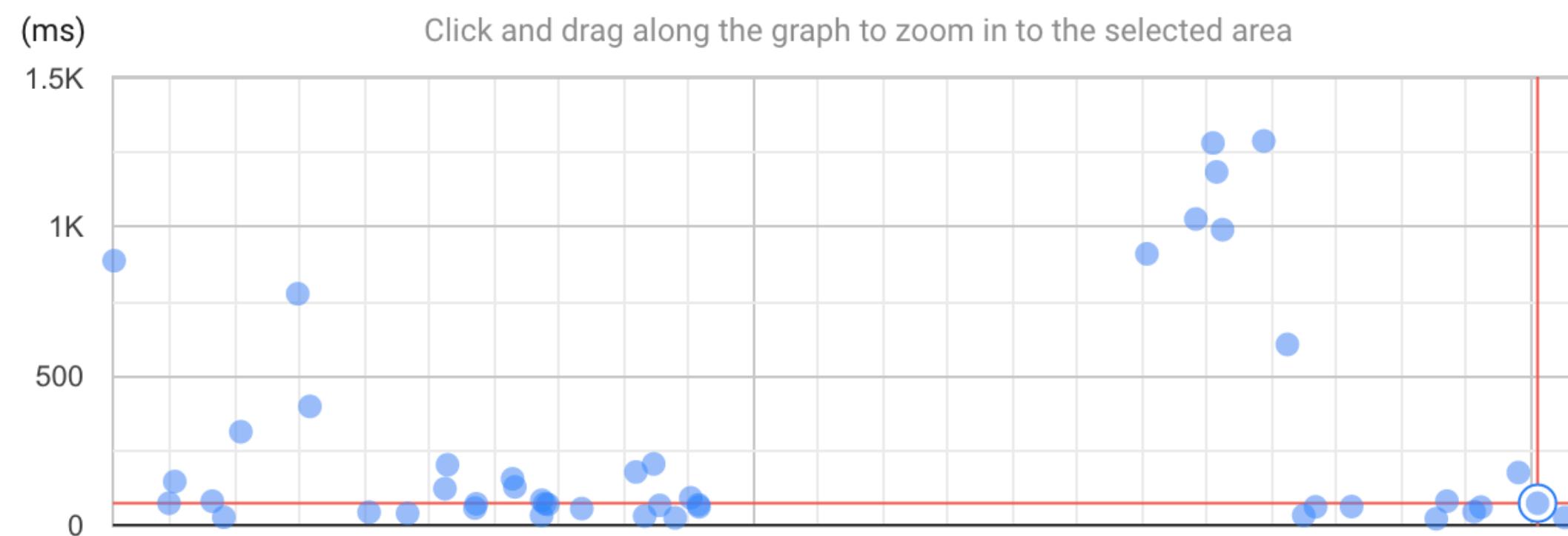
1 hour 4 hours 12 hours 1 day 3 days 1 week 1 month Custom

Request filter

productpage.istio-bookinfo.svc.cluster.local

HTTP method All

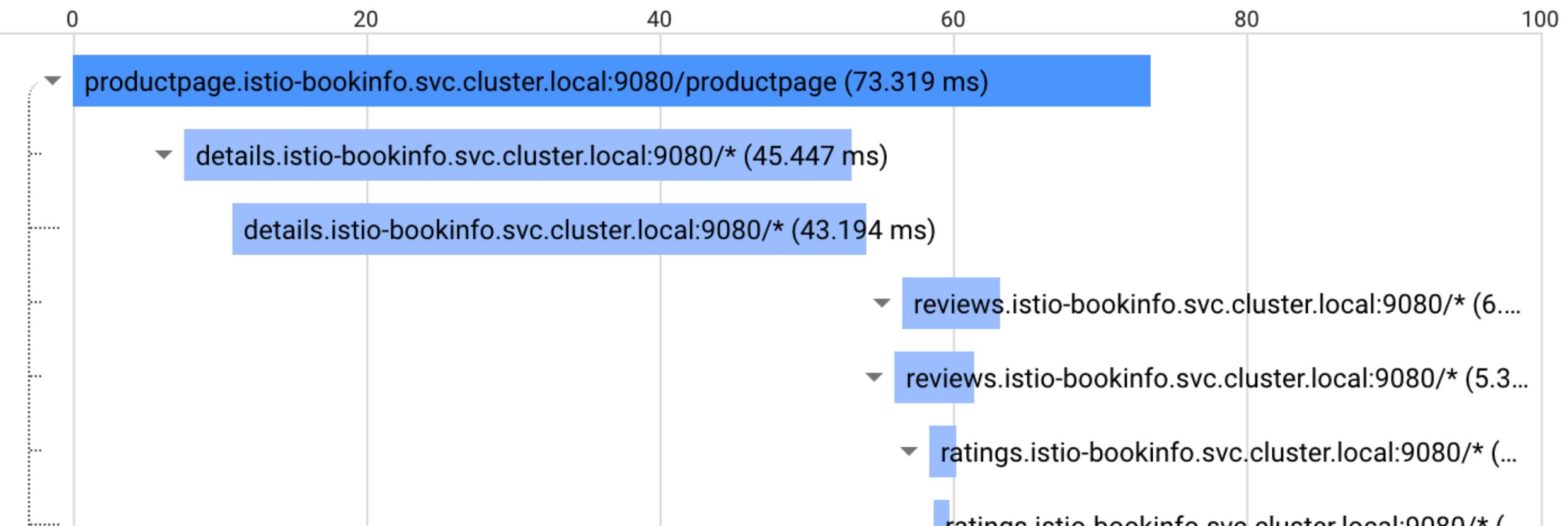
HTTP status All



Latency	HTTP Method	URI	Analysis Report	Time
70 ms		productpage.istio-bookinfo.svc.cluster.local:9		9:18 PM (Just now)
25 ms		productpage.istio-bookinfo.svc.cluster.local:9		9:18 PM (Just now)
73 ms		productpage.istio-bookinfo.svc.cluster.local:9	productpage.istio-bookinfo.svc.cluster.local:9	9:18 PM (Just now)
176 ms		productpage.istio-bookinfo.svc.cluster.local:9		9:17 PM (Just now)
60 ms		productpage.istio-bookinfo.svc.cluster.local:9		9:17 PM (Just now)

Rows per page: 5 1 - 5 of 47 ⏪ ⏩

Timeline



@0 ms

productpage.istio-bookinfo.svc.cluster.local:9080/productpage

Summary

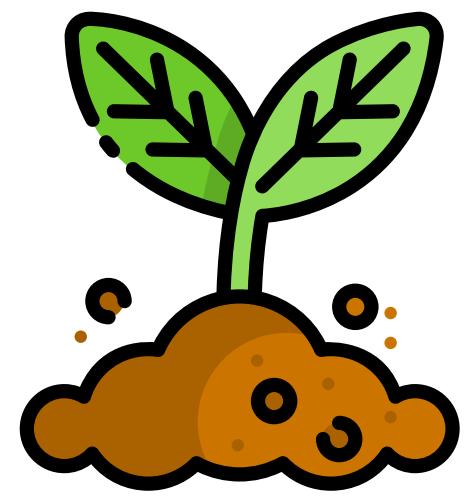
Name	RPCs	Total Duration (ms)
details.istio-bookinfo.svc.cluster.local:9080/*	2	89
productpage.istio-bookinfo.svc.cluster.local:9080/productpage	1	73
ratings.istio-bookinfo.svc.cluster.local:9080/*	2	3
reviews.istio-bookinfo.svc.cluster.local:9080/*	2	12

Details

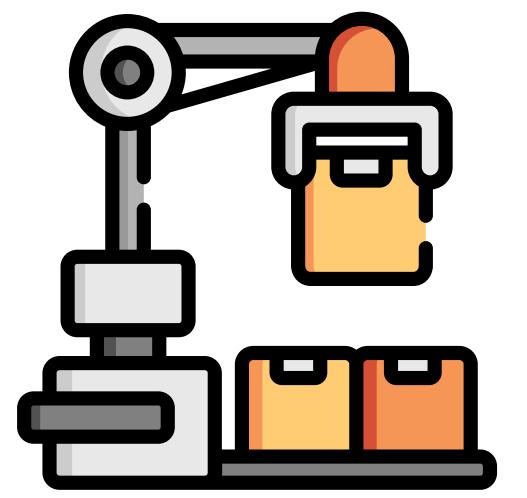
Timestamp 2019-11-26 (21:18:00.523)

Traced time ? 52.094 ms

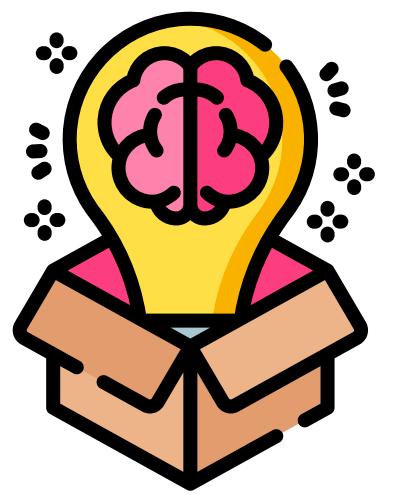
CALMS



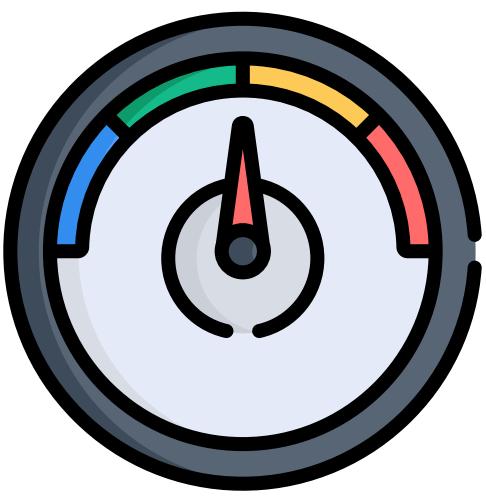
Culture



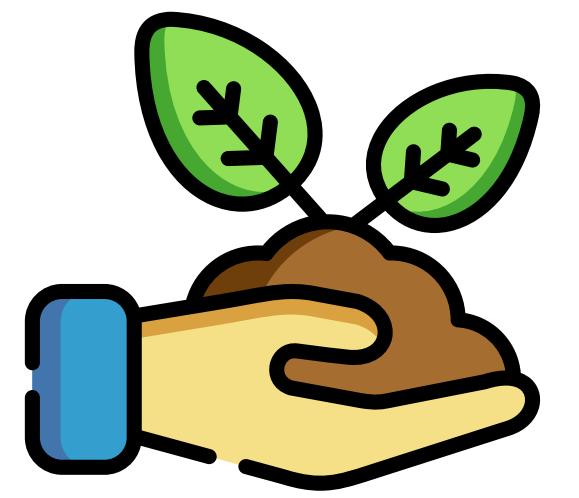
Automation



Lean



Metrics

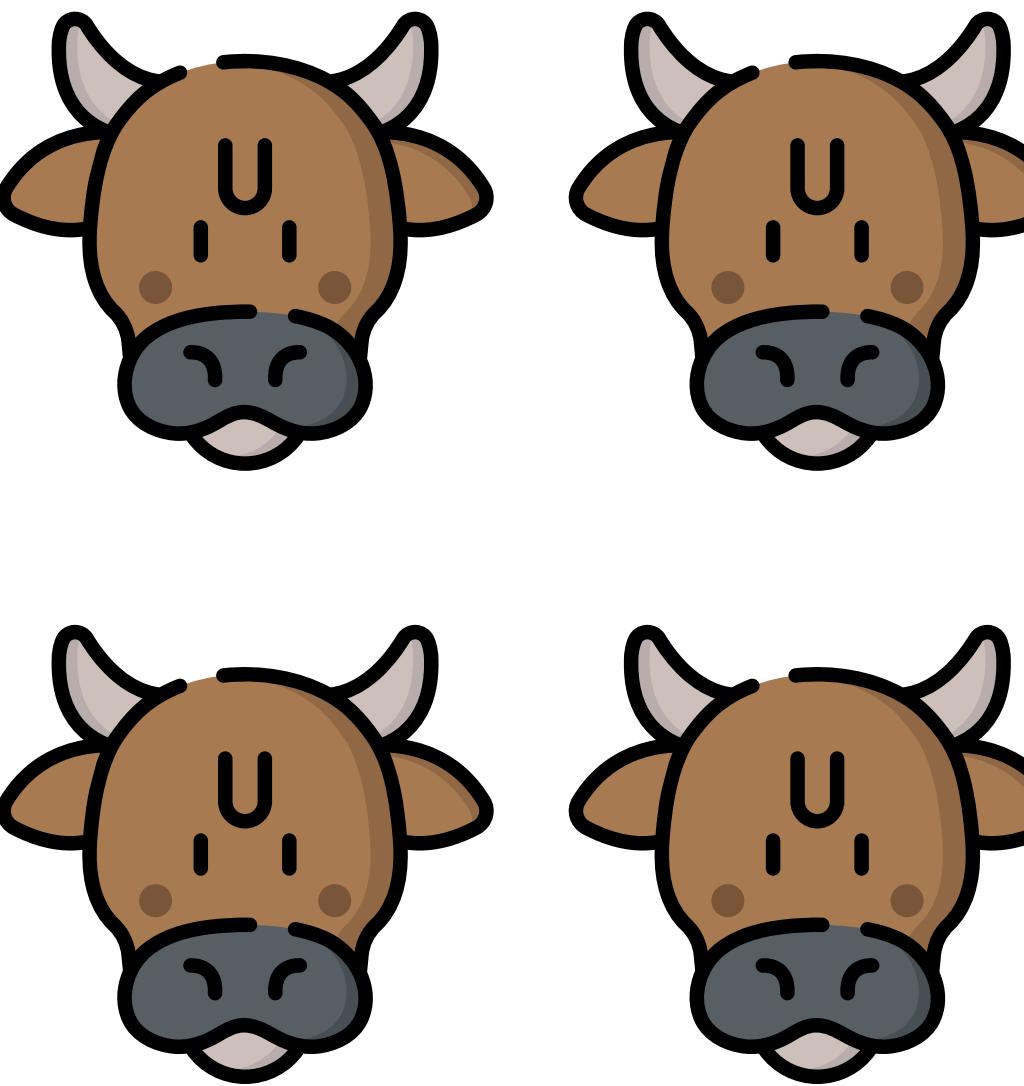


Sharing

Pets vs. Cattle



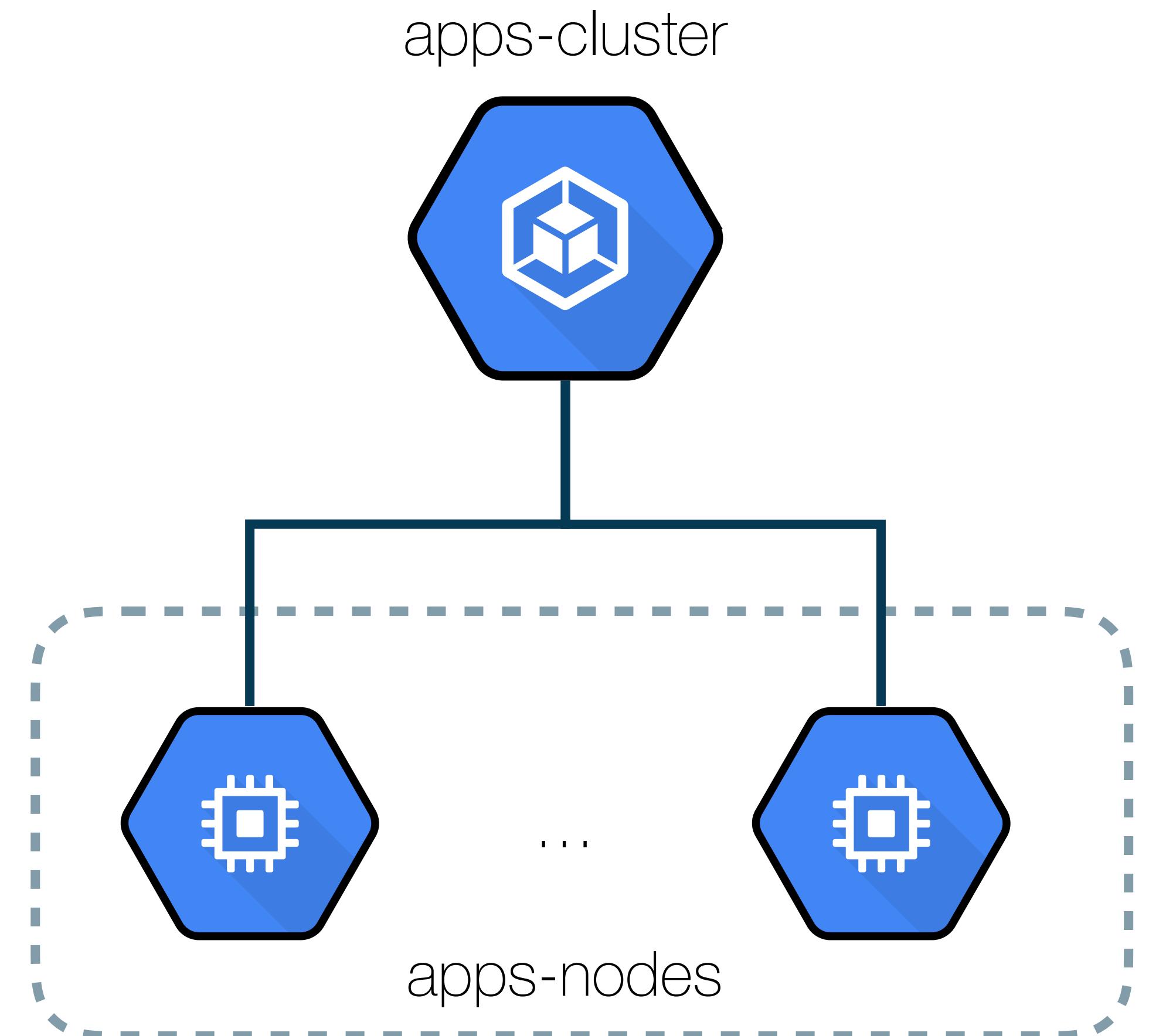
vs.



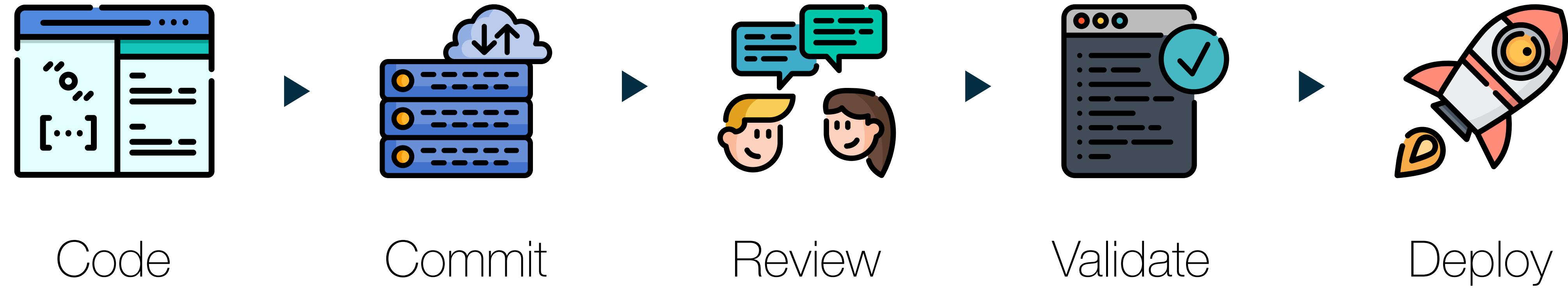
Infrastructure as Code



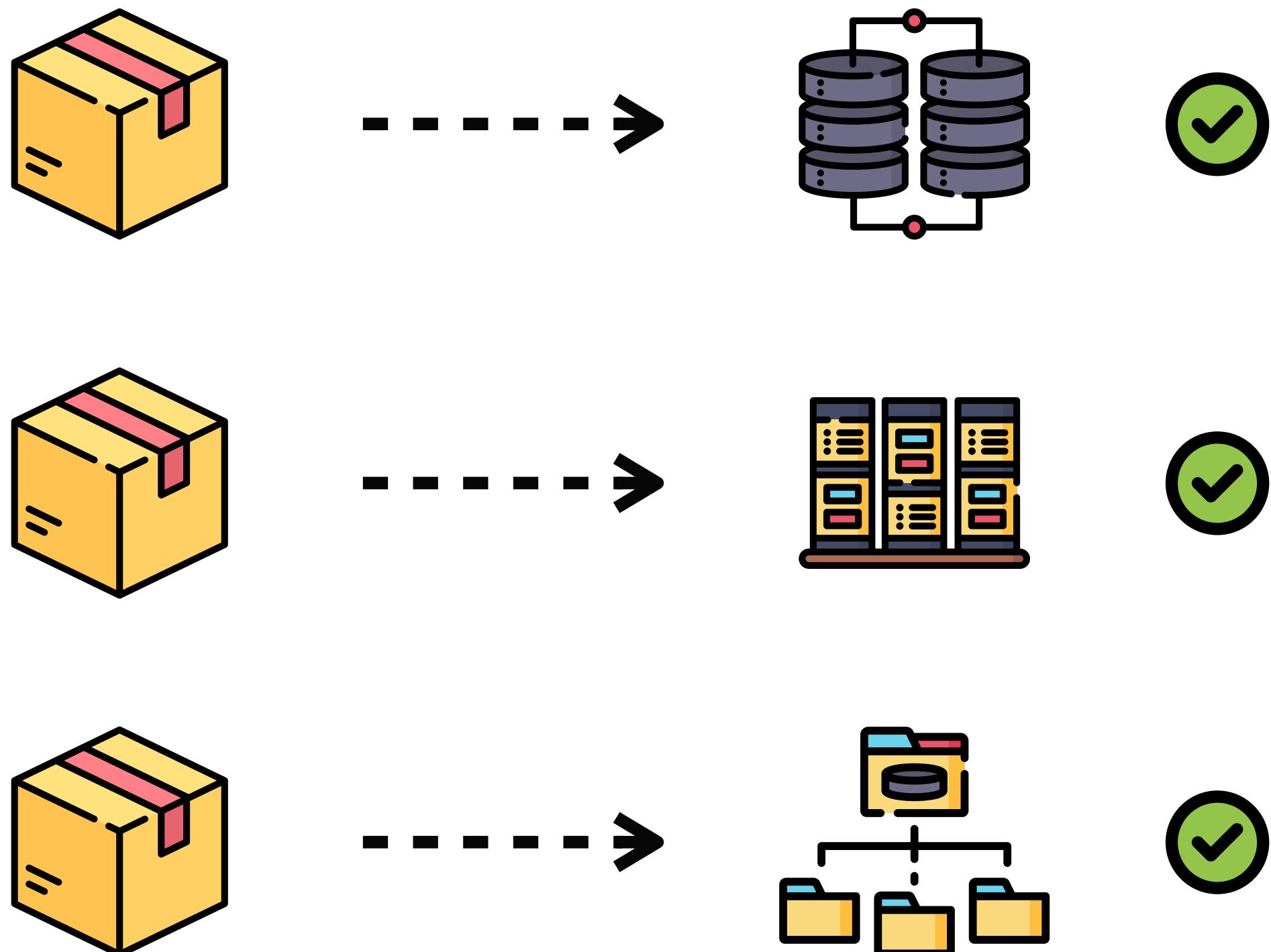
```
resource "container_cluster" "apps" {  
  name = "apps-cluster"  
  location = "europe1-north"  
  
  initial_node_count = 1  
}  
  
resource "container_node_pool" "nodes" {  
  name = "apps-nodes"  
  location = "europe1-north"  
  cluster = "${container_cluster.apps.name}"  
  
  node_config {  
    machine_type = "n1-standard-1"  
  }  
}
```



Infrastructure as Code Workflow



Infrastructure Templates

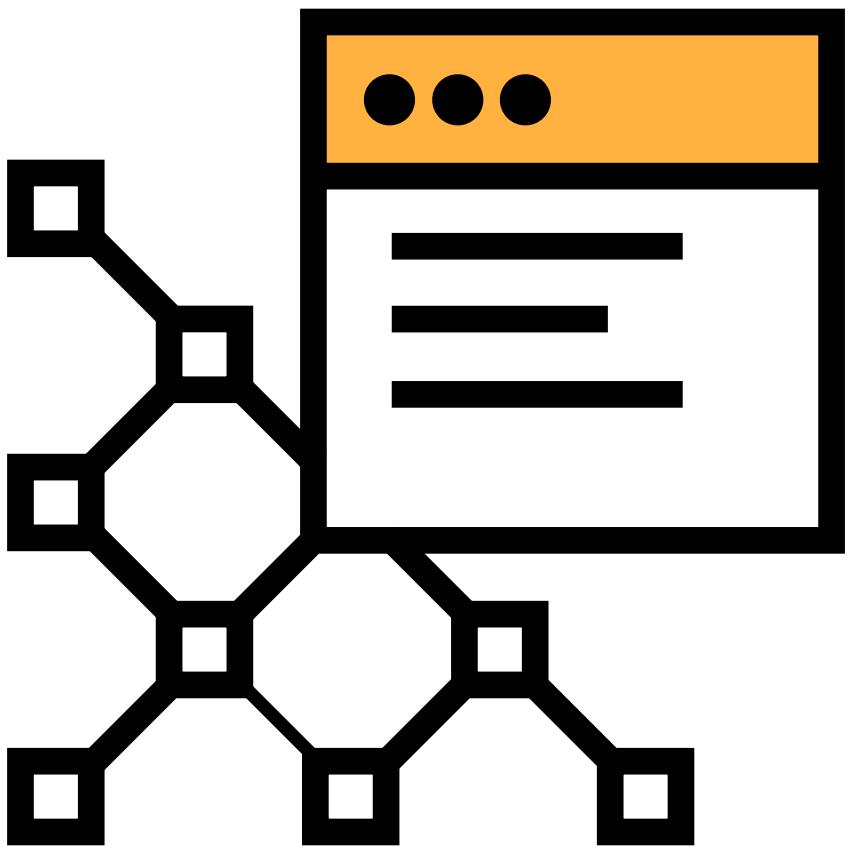


Make the right way the easy way!

- Shared templates
- Shared knowledge
- Best practices
- Conventions
- Security

Security Benefits of IaC

- Change history and audit trail
- Review and collaborate
- Statical security analysis
- Inventory tracking
- Security knowledge sharing by transparency
- Consistency and reproducibility





```
$ go get github.com/bulderbank/ndc-2019  
$ go run summary.go
```

- From idea to production in 10 months
- Building on the shoulders of giants
- Kubernetes and Firebase

\$



Questions?

Thank you!

Hans Kristian Flaatten
hans.flattent@evry.com
@Starefossen





tieto *EVRY*