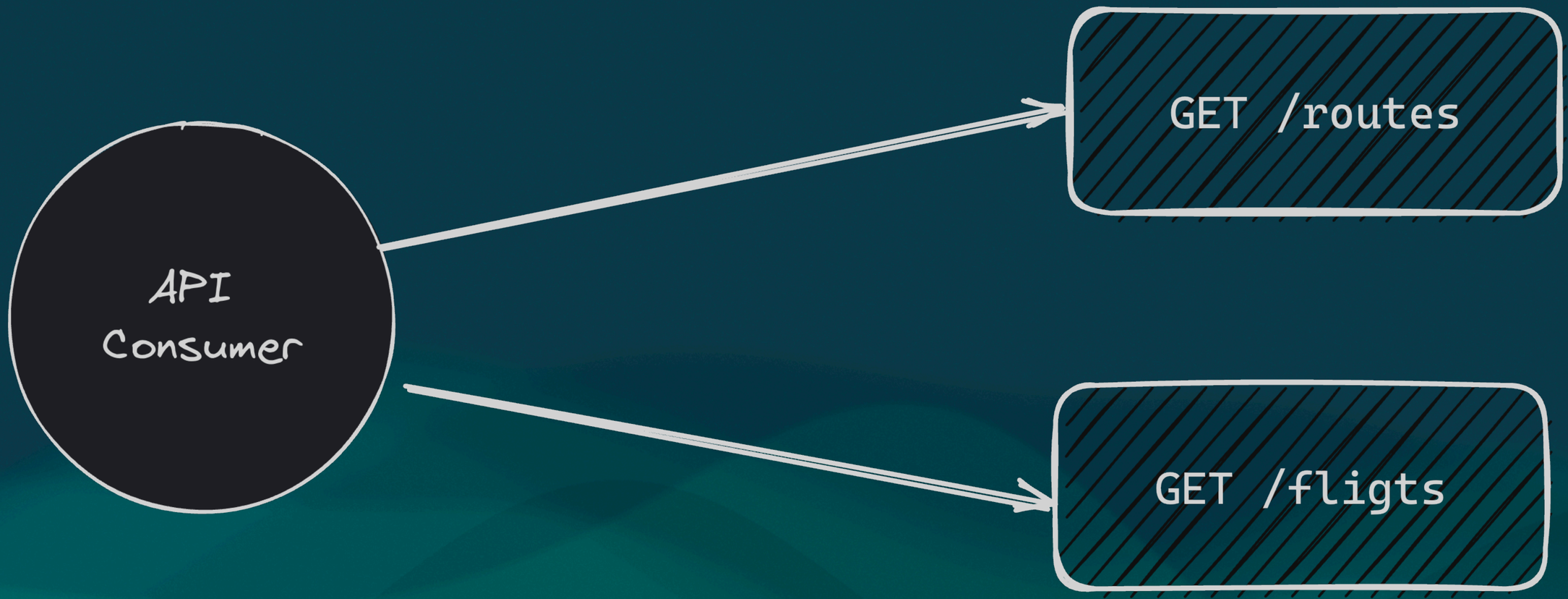
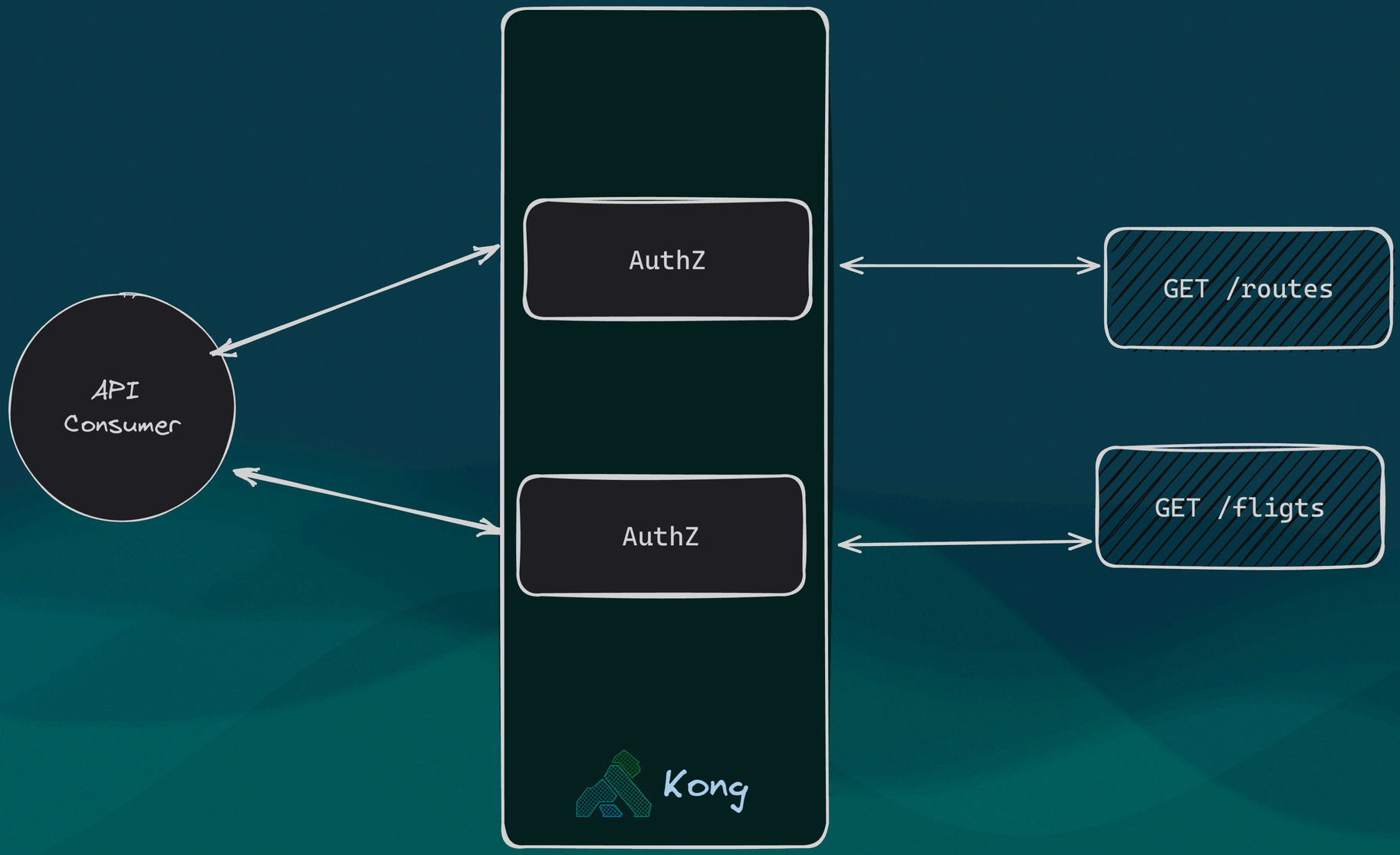
Guarding GraphQL
Strategies for Robust API Authorization

Viktor Gamov, October 24th, Santa Clara, California

X: @gamussa @thekonginc


API
Consumer
GET /routes
GET /fligts

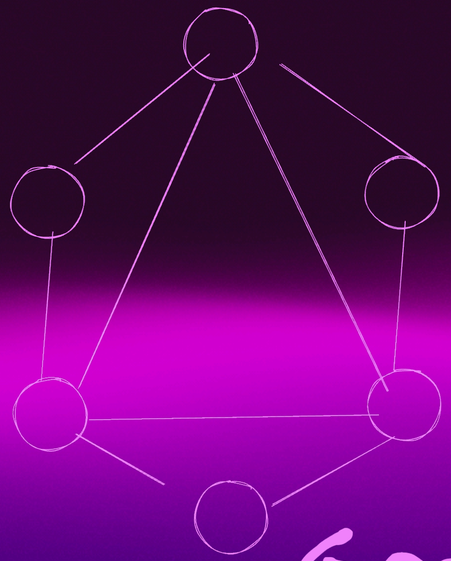
API Gateway



API Consumer Query

```
query {
  flights(date: "2024-03-20") {
    number
    route {
      origin
      destination
    }
    scheduled_departure
  }
}
```

KongAir GraphQL



GraphQL

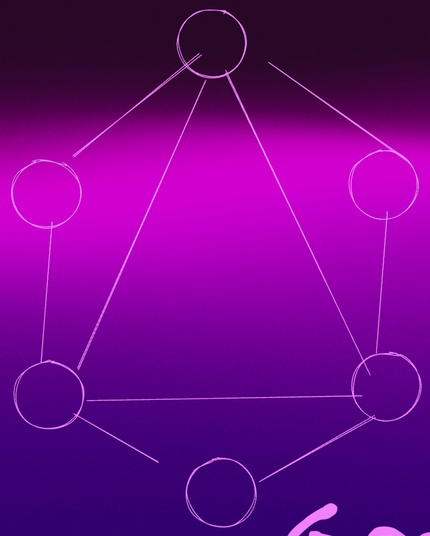
AuthZ

nested
conditional data

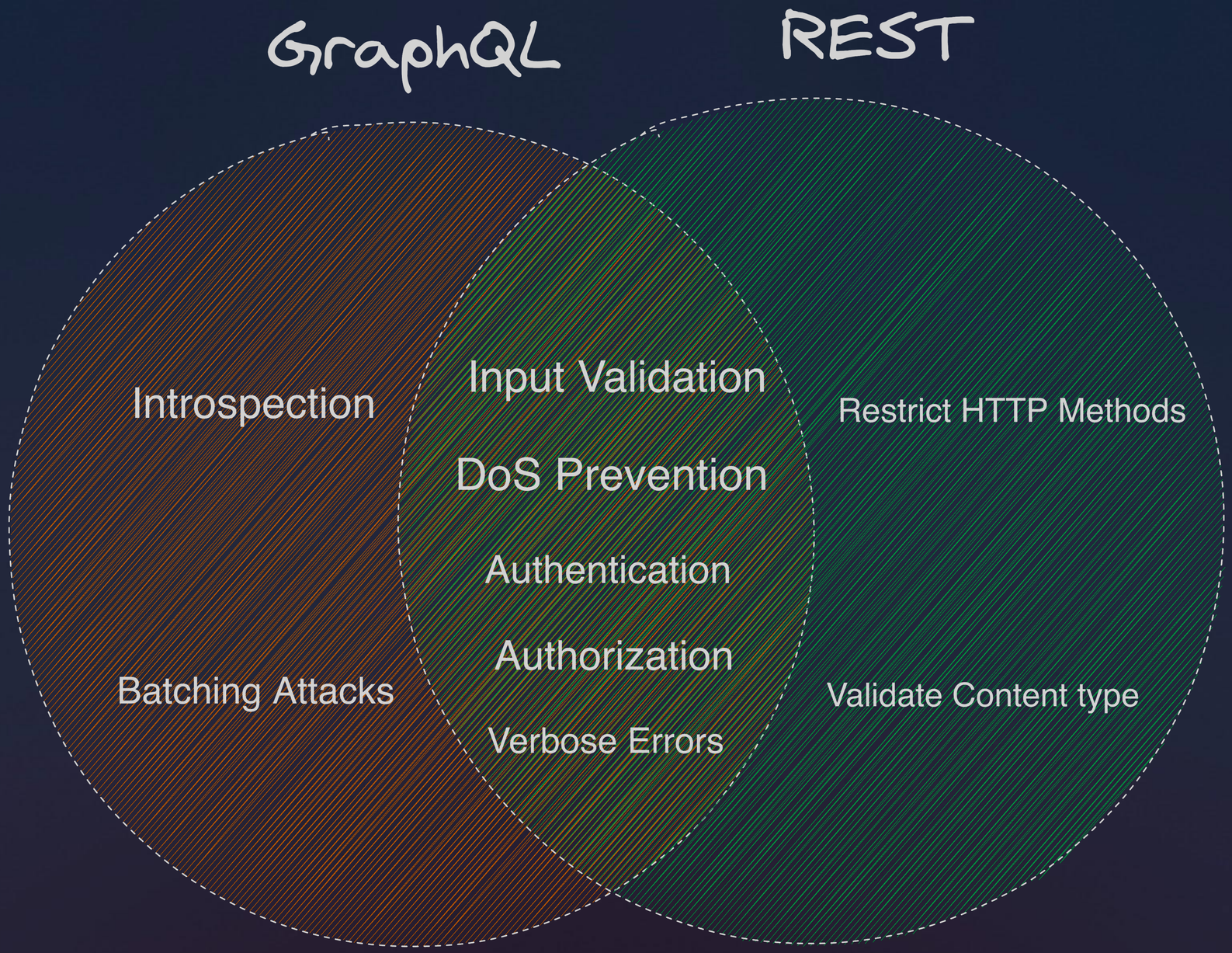
API Consumer Query

```
query {
  flights(date: "2024-03-20") {
    number
    route {
      origin
      destination
    }
    scheduled_departure
  }
}
```

KongAir GraphQL



GraphQL


GraphQL
REST
Introspection
Input Validation
Restrict HTTP Methods
DoS Prevention
Authentication
Authorization
Batching Attacks
Validate Content type
Verbose Errors

Viktor

G A M O V

Principal Developer Advocate | Kong

~~Twitter~~ X: @gamussa

Danny

FREESE

Partner Solutions Engineer | Kong

X: @thekonginc

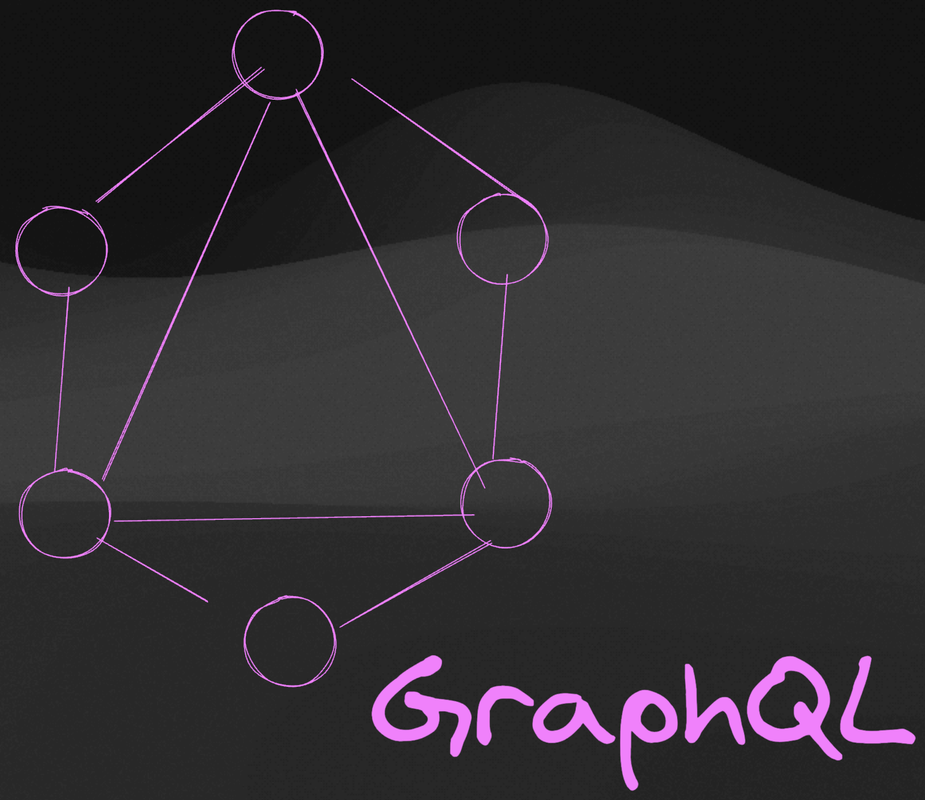
Agenda

- Start from the beginning - REST or GraphQL
- Why is Authorization with GraphQL Hard to Tackle?
  - REST example
  - GraphQL example
- Tackling AuthZ with API Gateway

GraphQL

Nuts and Bolts

- Schema
- Queries
- Mutations
- Subscriptions



Schema

Define your API

```
type Route {
    origin: String!
    destination: String!
}

type Flight {
    number: String!
    route: Route!
    scheduled_departure: String!
    scheduled_arrival: String!
}

type Booking {
    ticket_number: String!
    flight: Flight!
    seat: String!
}
```

Queries

Get what you need

```
type Query {
    routes(origin: [String!]): [Route!]!
    flights(date: String!): [Flight!]!
    bookings(customer_id: ID!): [Booking!]!
}
```

Queries

Get what you need

```
type Query {
    routes(origin: [String!]): [Route!]!
    flights(date: String!): [Flight!]!
    bookings(customer_id: ID!): [Booking!]!
}
```

```
query {
    flights(date: "2024-03-20") {
        number
        route {
            origin
            destination
        }
        scheduled_departure
    }
}
```

Mutations

Modify data

```
input BookingInput {
…
}

input CustomerInformationInput {
…
}

type Mutation {
    bookFlight(
        booking: BookingInput!
        customerInformation:
CustomerInformationInput
    ): BookingResponse!
}
```

Mutations

Modify data

```
input BookingInput {
…
}

input CustomerInformationInput {
…
}

type Mutation {
    bookFlight(
        booking: BookingInput!
        customerInformation:
CustomerInformationInput
    ): BookingResponse!
}
```

```
mutation {
    bookFlight(
        booking: {
            flight_number: "KA924"
            seat: "32A"
        }
        customerInformation {
            frequentFlierNumber: "ABC123"
        }
    )
    {
        ticket_number
    }
}
```

Subscription

Real-time updates

```
type Subscription {
    newFlight: Flight!
}
```

Subscription

Real-time updates

```
type Subscription {
    newFlight: Flight!
}
```

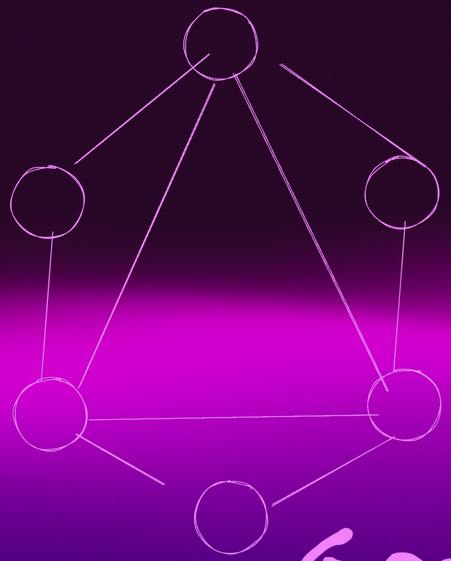
```
subscription {
    newFlight {
        number
        route {
            origin
            destination
        }
        scheduled_departure
        scheduled_arrival
    }
}
```

Why is Authorization with GraphQL Hard to Tackle?

API Consumer Query

```
query {
  flights(date: "2024-03-20") {
    number
    route {
      origin
      destination
    }
    scheduled_departure
  }
}
```

KongAir GraphQL



GraphQL

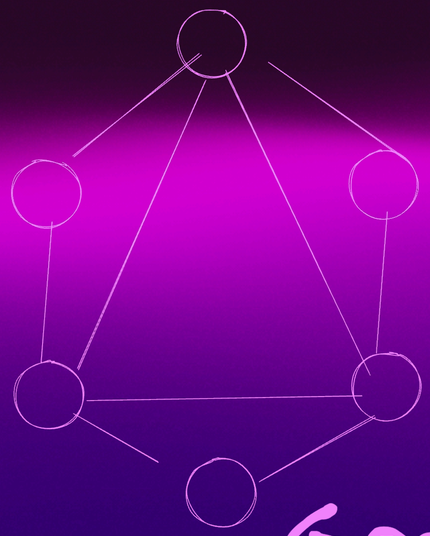
AuthZ

nested
conditional data

API Consumer Query

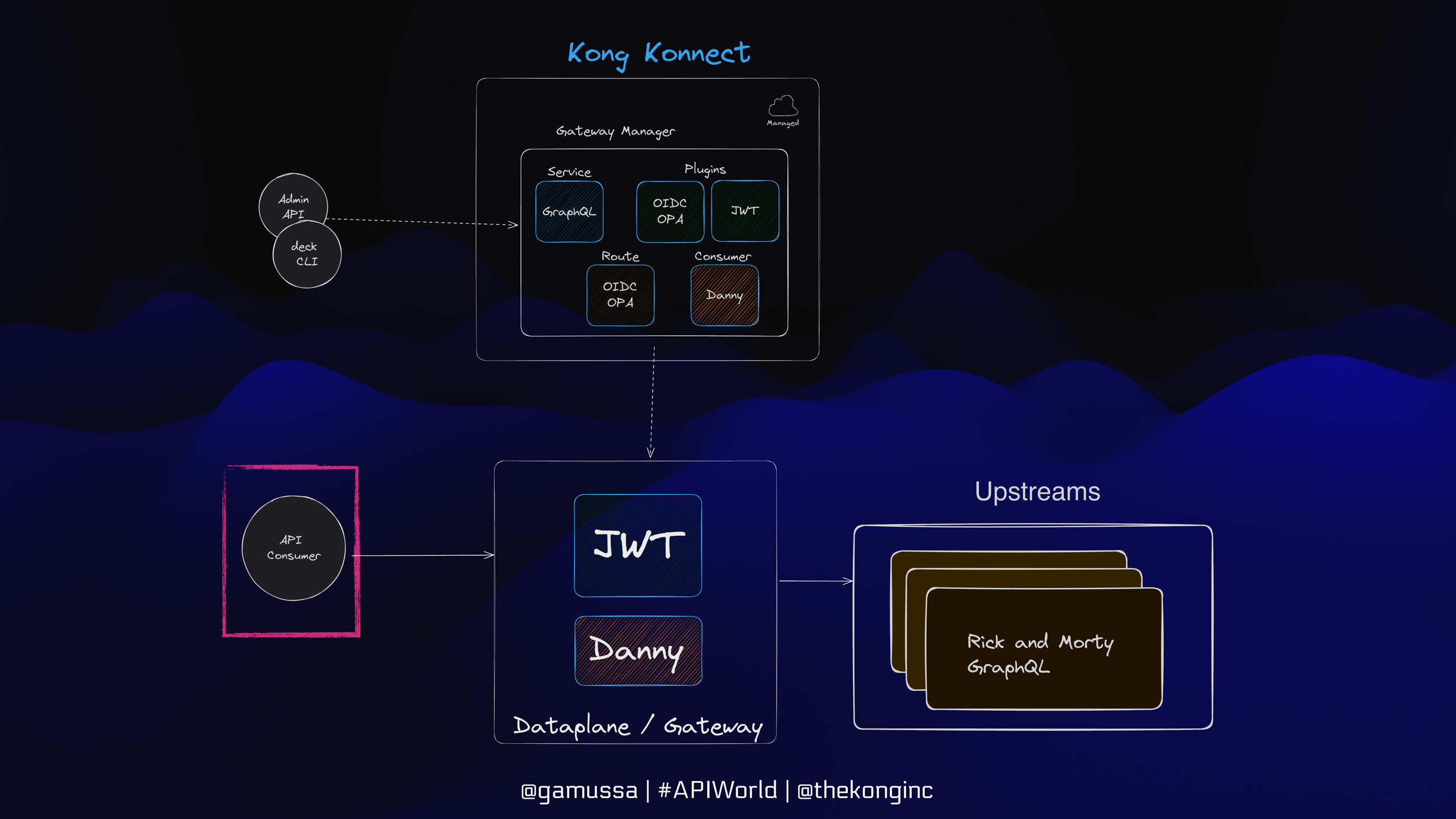
```
query {
  flights(date: "2024-03-20") {
    number
    route {
      origin
      destination
    }
    scheduled_departure
  }
}
```

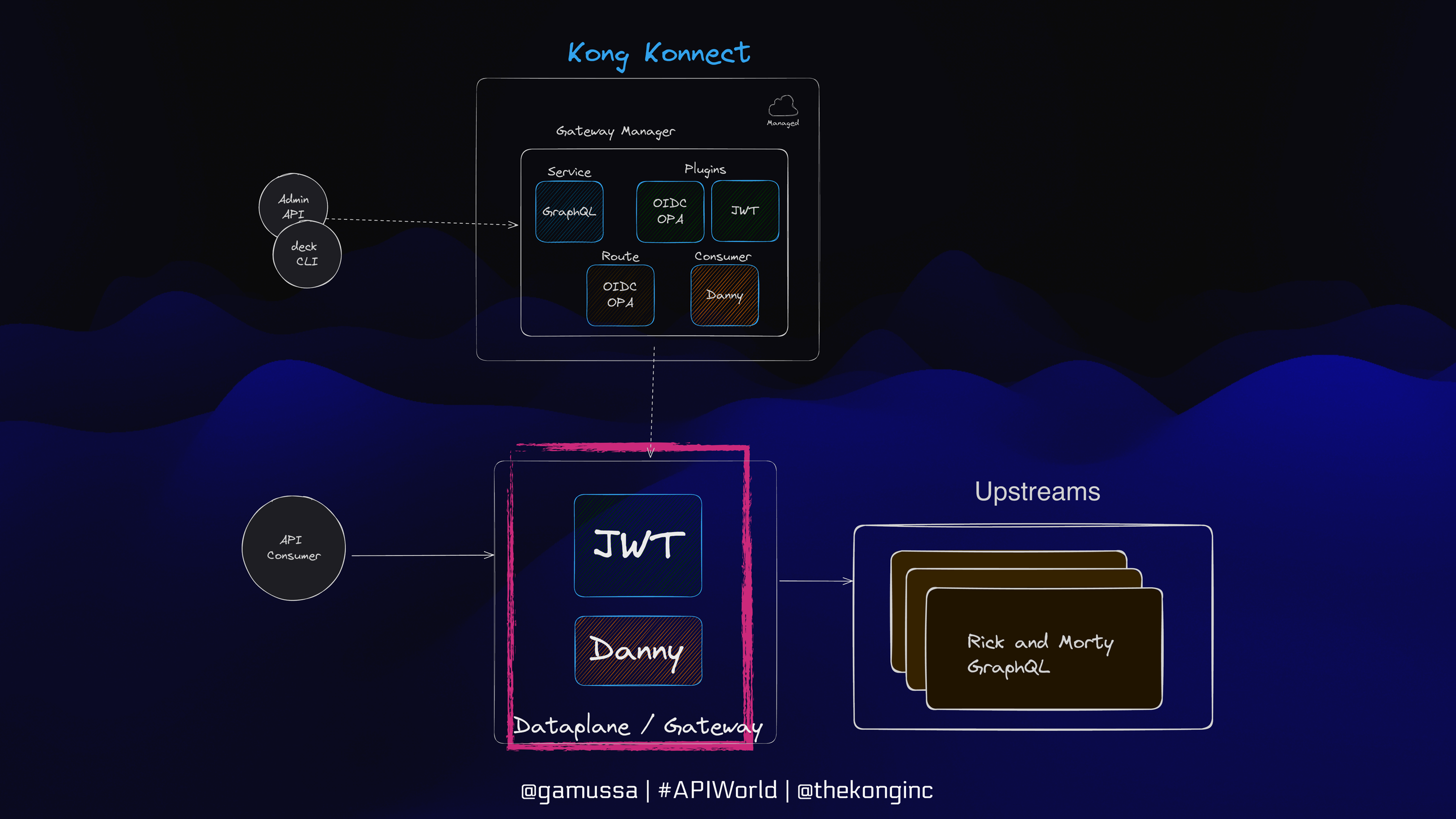
KongAir GraphQL

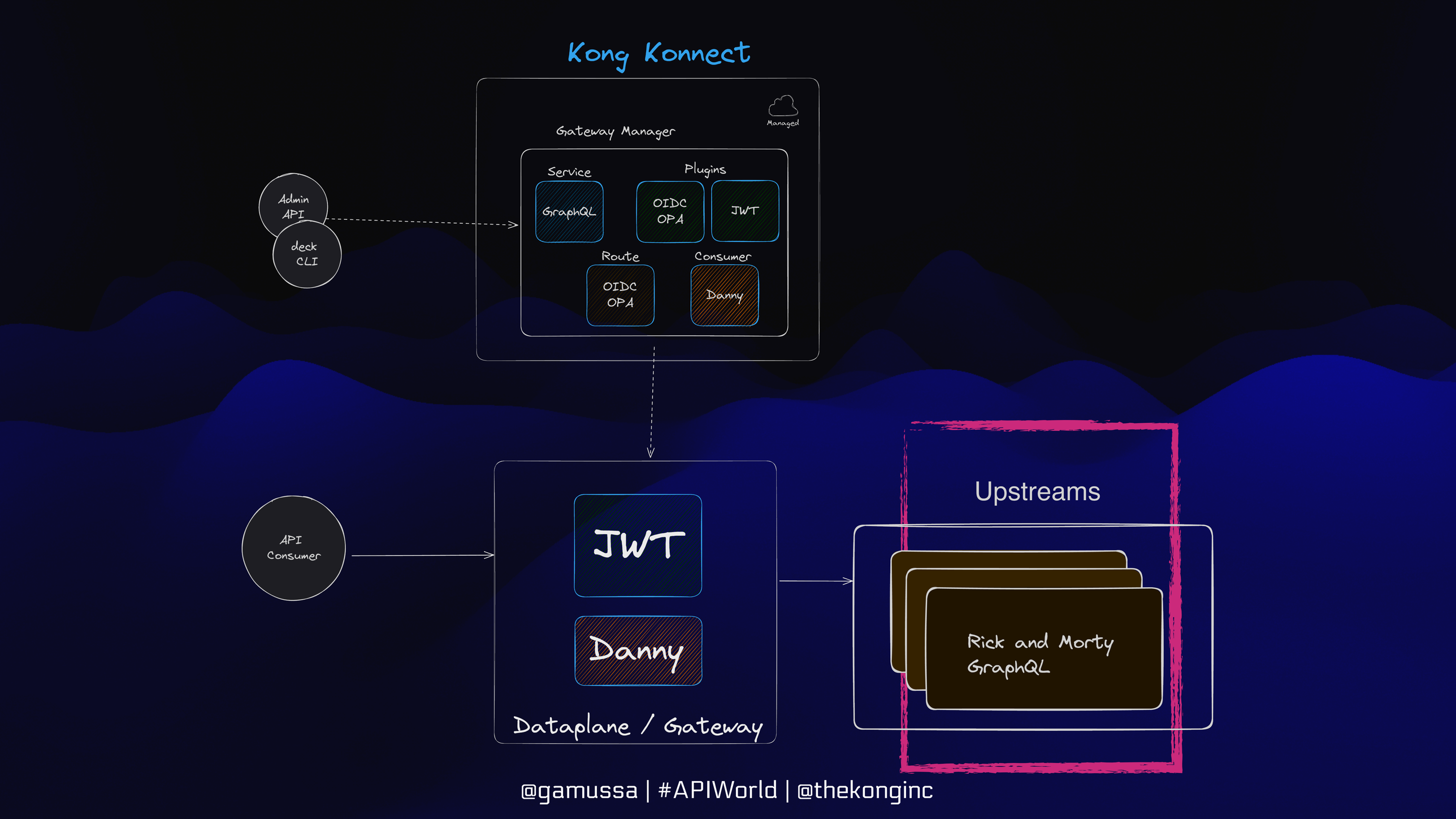


GraphQL

Protect Endpoints with JWT

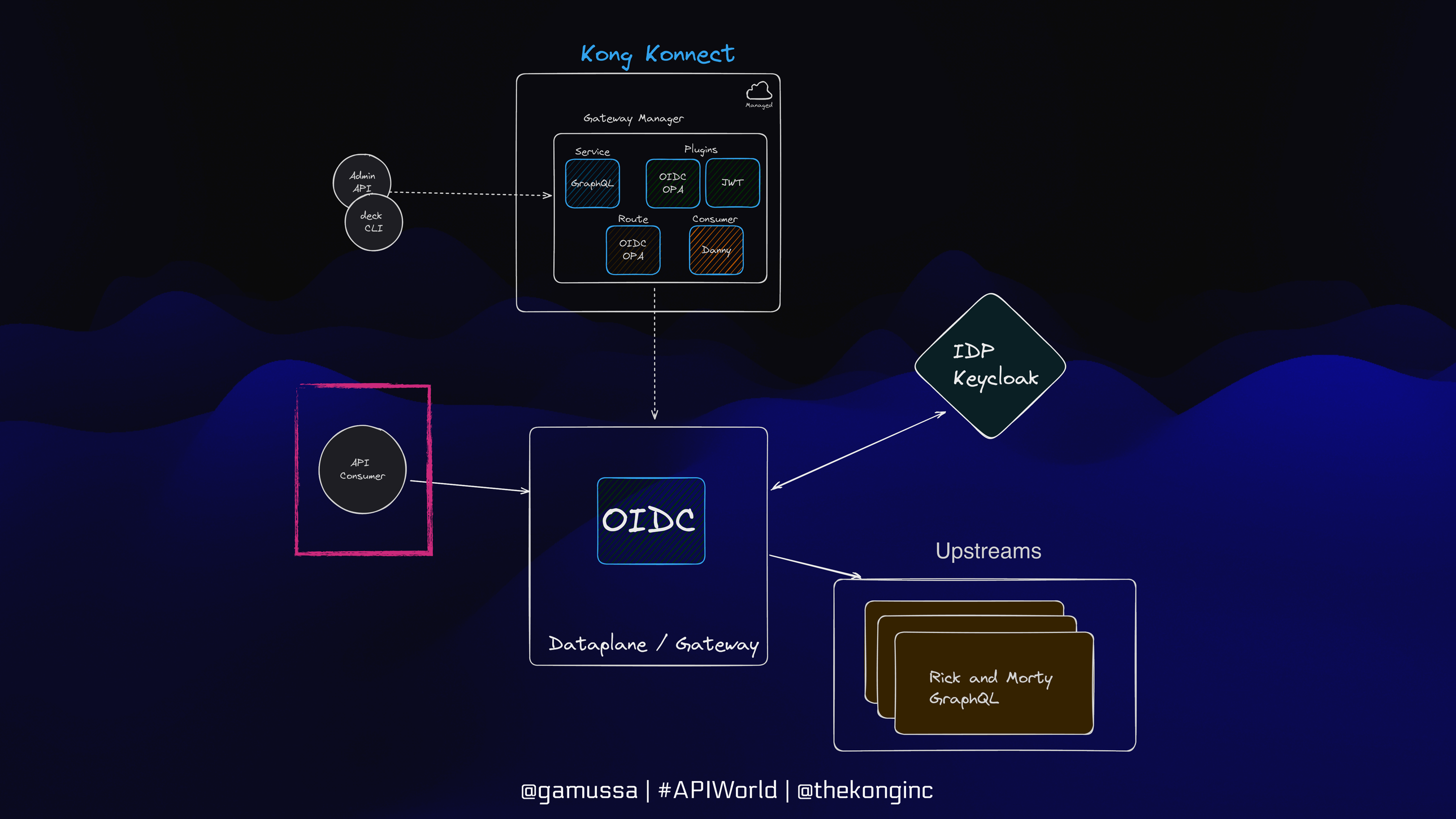

Kong Konnect
Gateway Manager
Managed
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
API
Consumer
JWT
Danny
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL

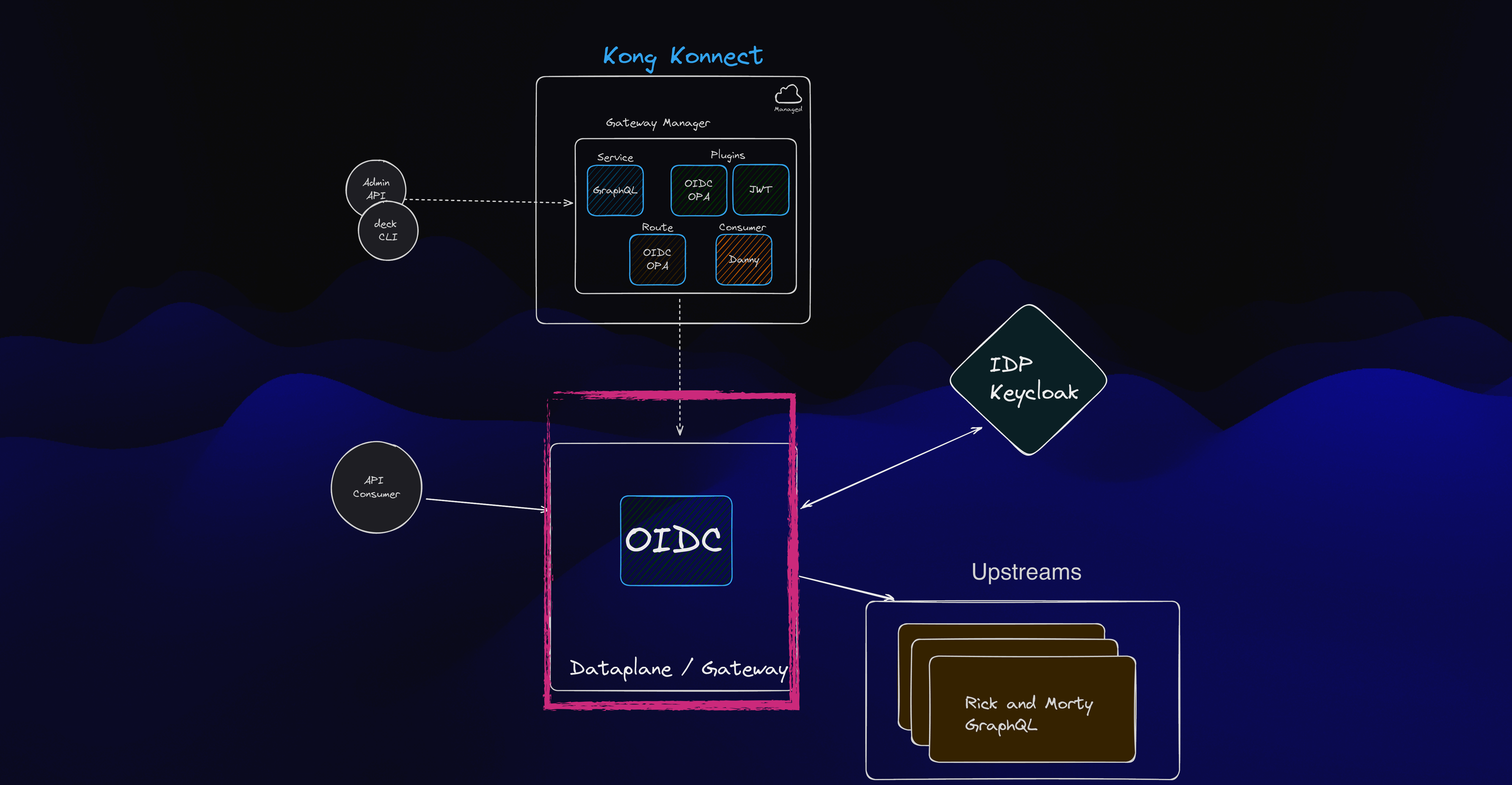

Kong Konnect
Gateway Manager
Managed
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
API
Consumer
JWT
Danny
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL

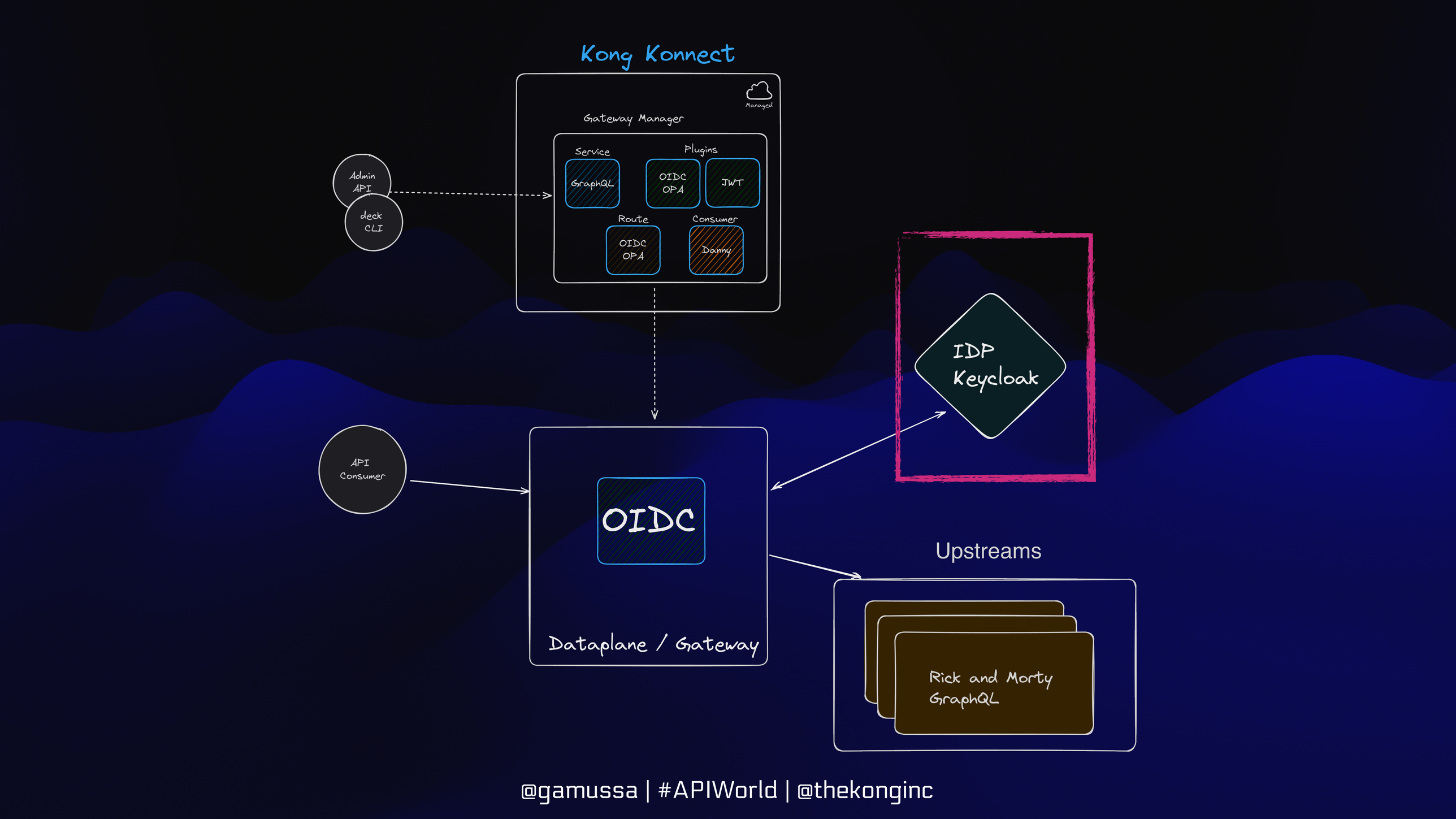

Kong Konnect
Gateway Manager
Managed
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
API
Consumer
JWT
Danny
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL

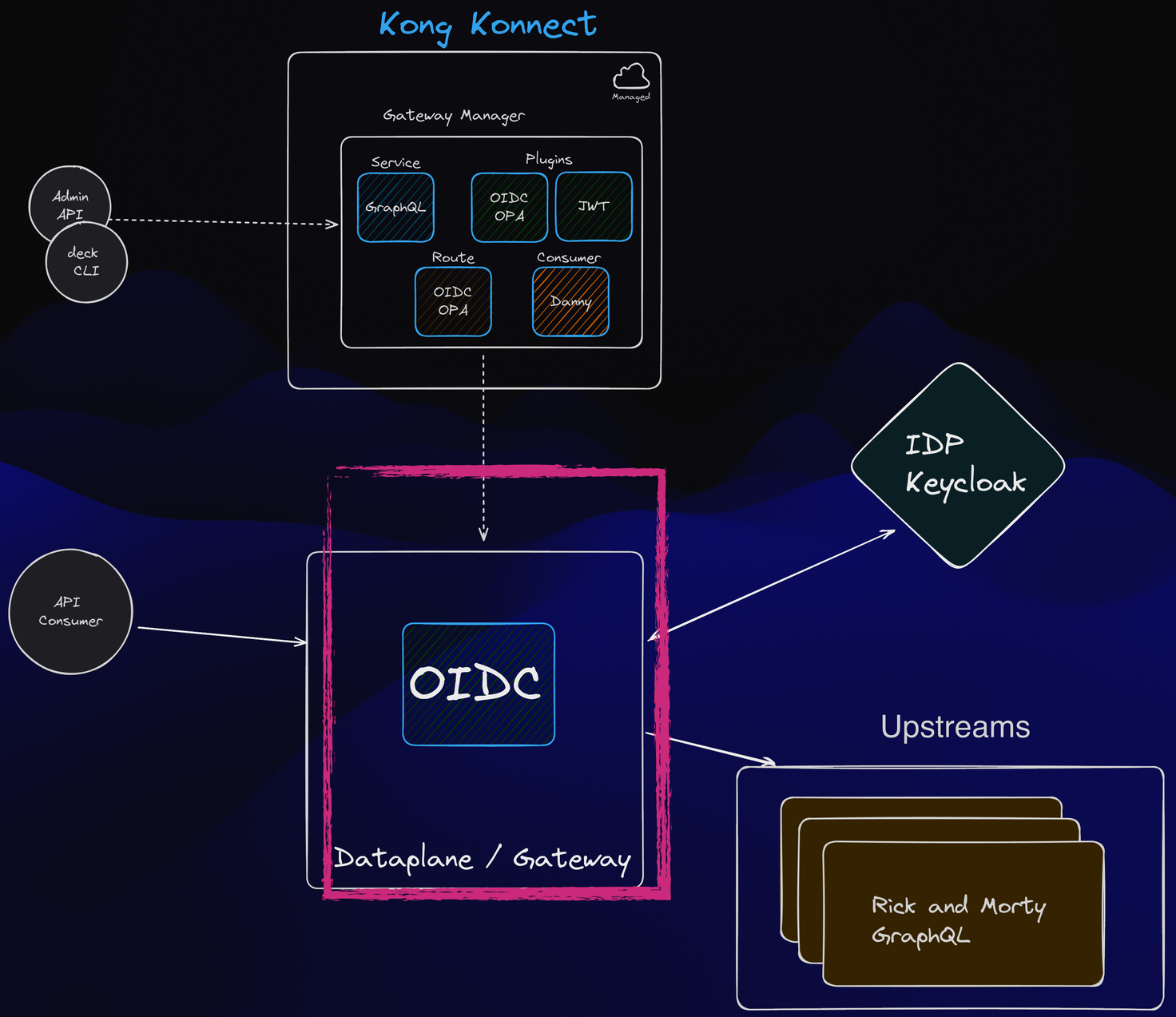
DEMO

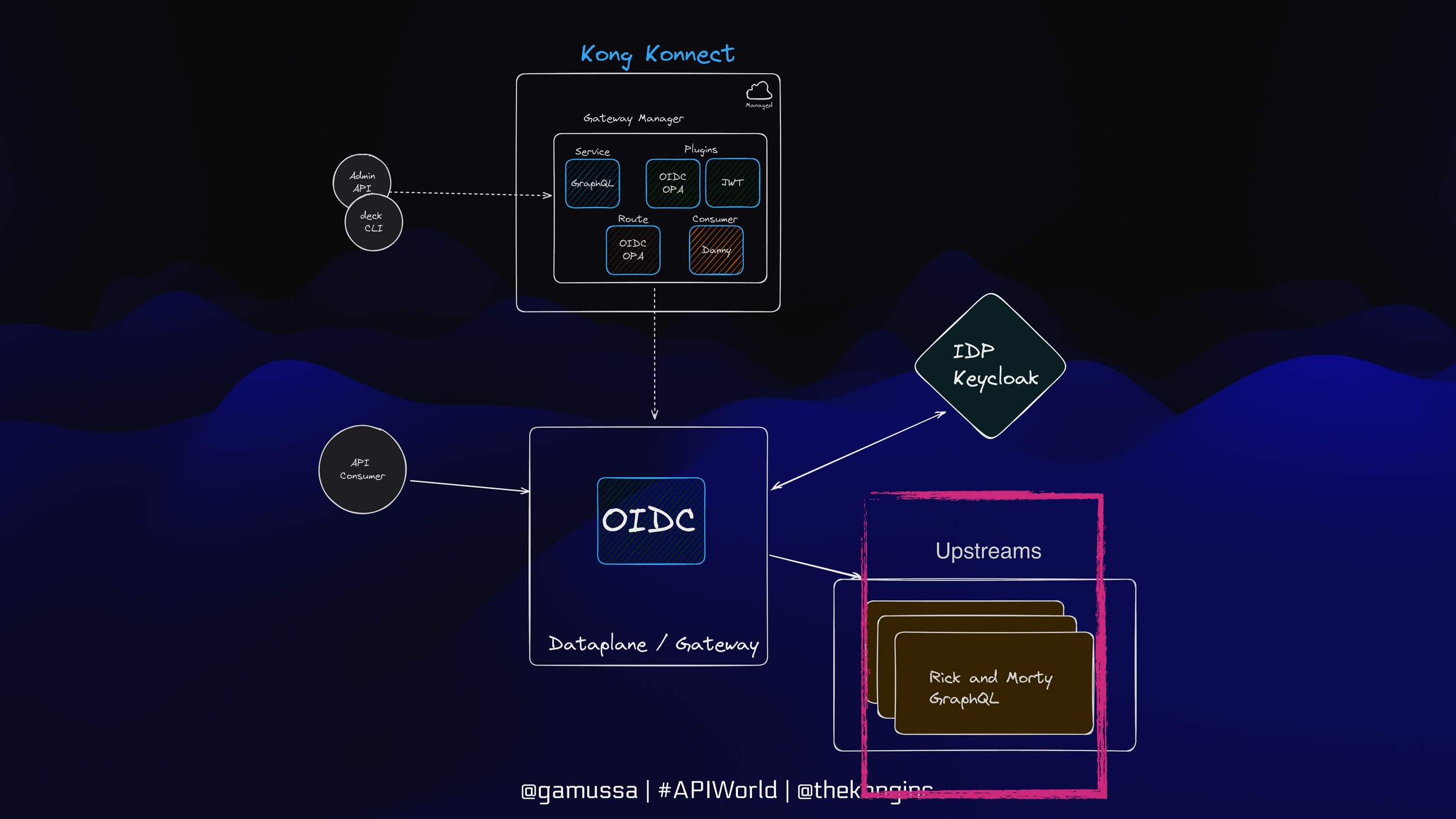
Integrate with IDP


Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL


Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL

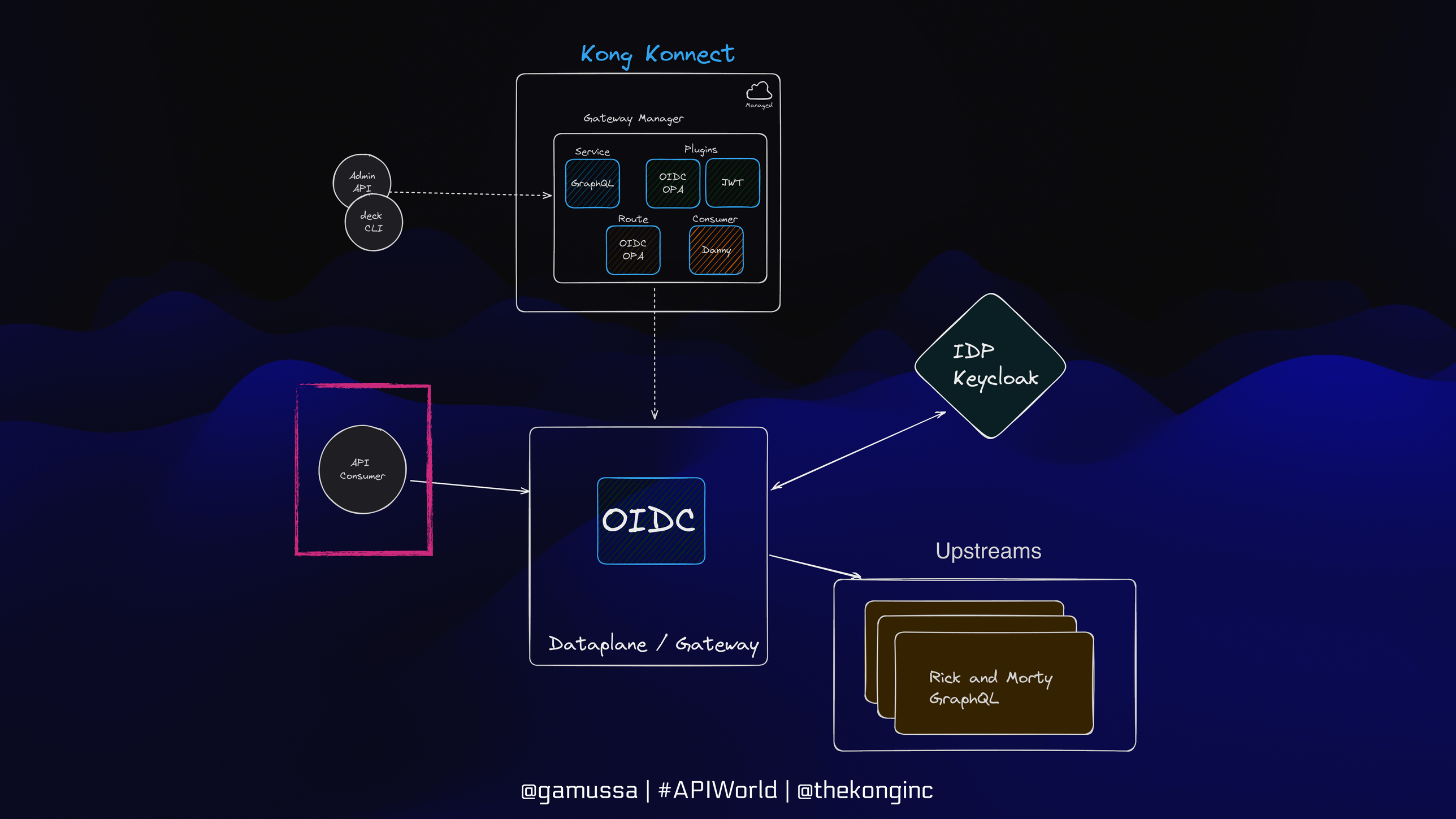

Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL

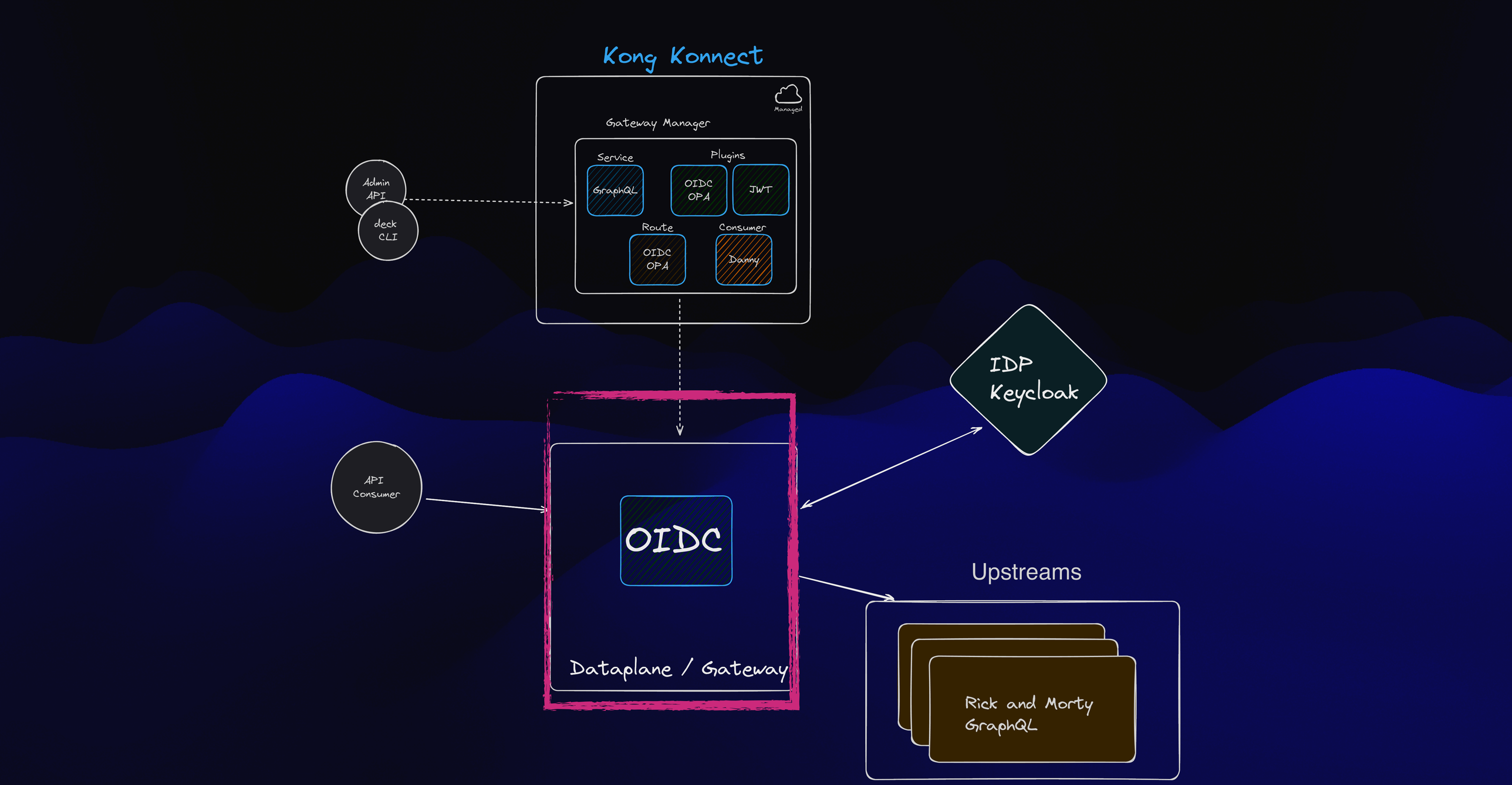

Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL

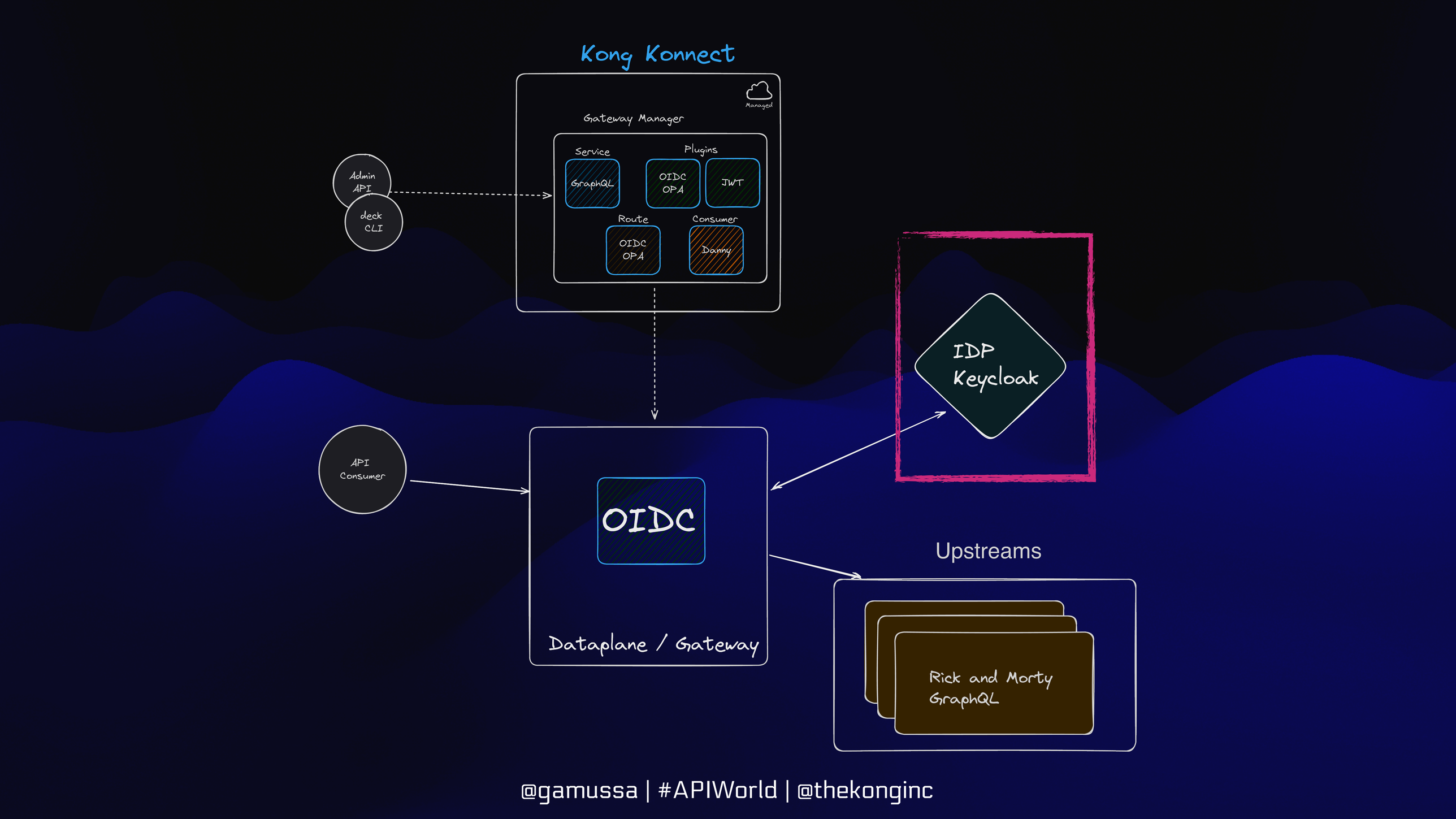

Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL

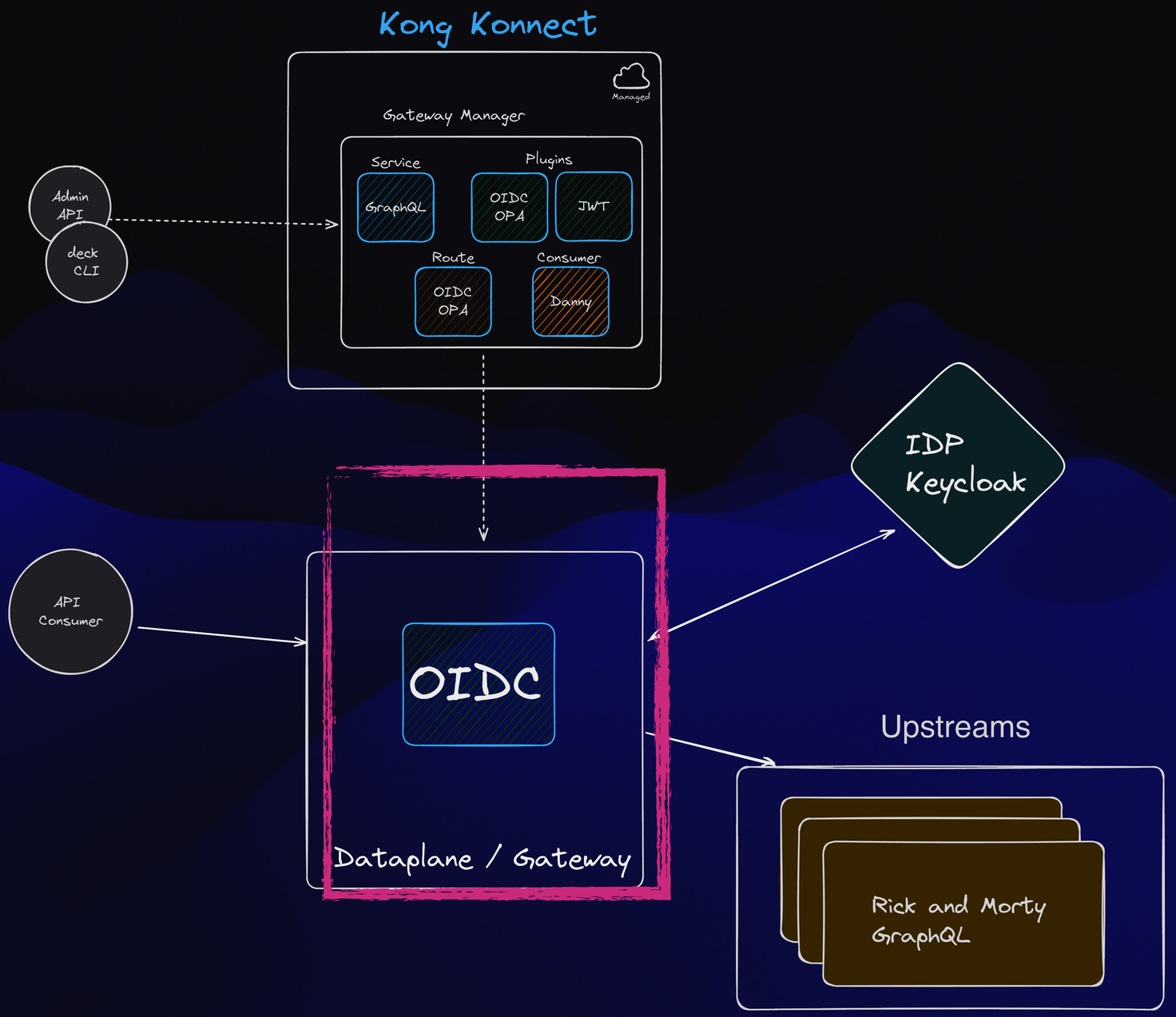
DEMO

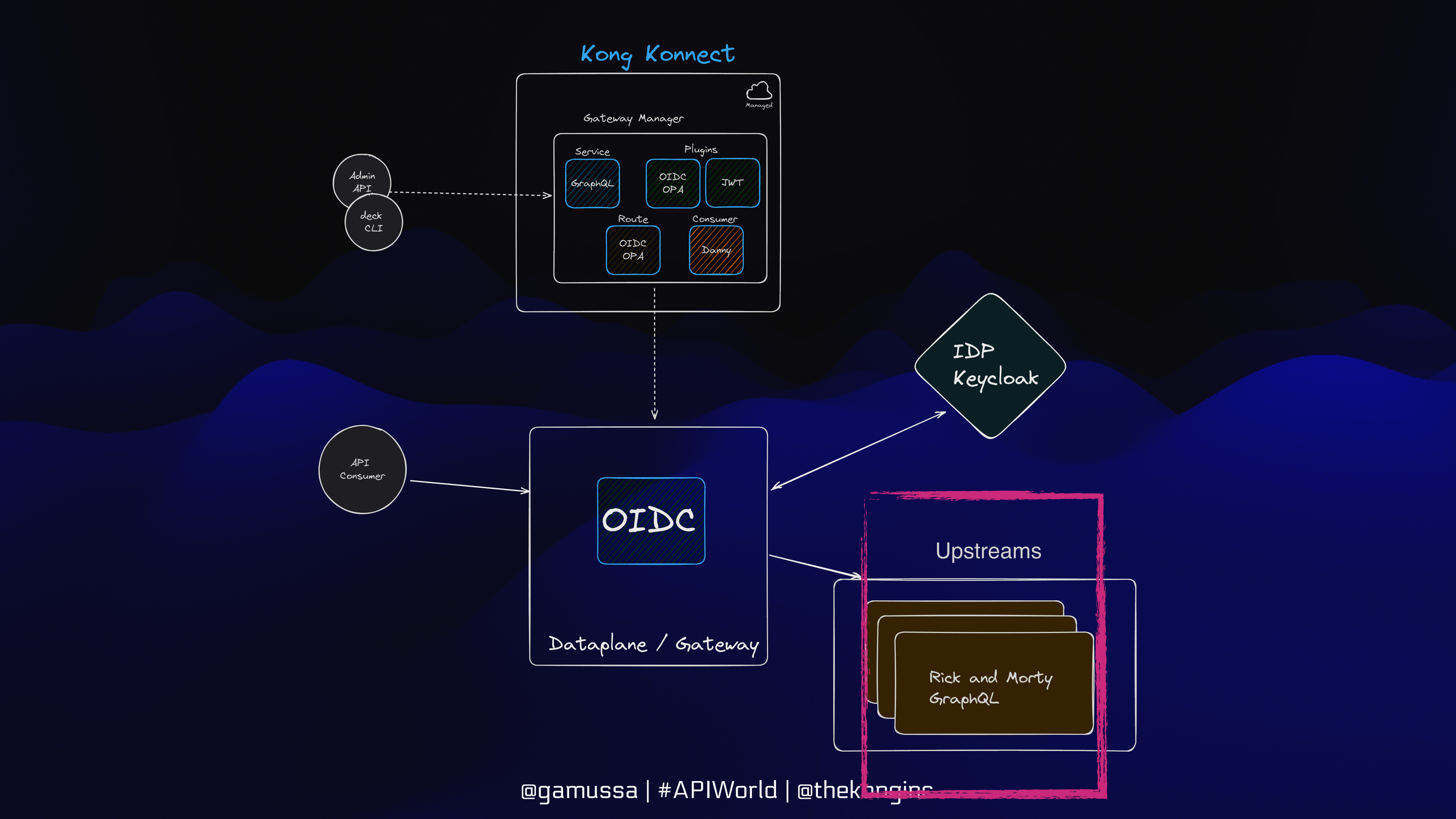
Granular Access Control with OPA


Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL


Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL


Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL


Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL


Kong Konnect
Managed
Gateway Manager
Service
Plugins
GraphQL
OIDC
OPA
JWT
Route
Consumer
OIDC
OPA
Danny
Admin
API
deck
CLI
IDP
Keycloak
API
Consumer
OIDC
Dataplane / Gateway
Upstreams
Rick and Morty
GraphQL

DEMO

https://gamov.dev/try-konnect

https://gamov.dev/api-world-graphql

Please, subscribe to my YouTube channel ™

Premium NL

Search

6

Home

Shorts

Subscriptions

Originals

YouTube Mu...

Library

Downloads

Kong's Kubernetes Ingress Controller

Kong

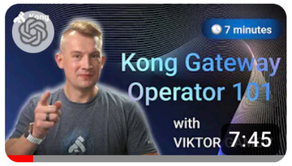
14 videos 1,202 views Last updated on Mar 31, 2023

Play all Shuffle

1 

What's new in Kong Ingress Controller 2.9 - GRPCRoute #gatewayapi #kubernetes #ingress #grpc

Kong • 108 views • 12 days ago

2 

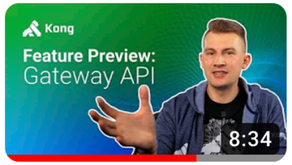
Introducing Kong Gateway Operator

Kong • 3.4K views • 5 months ago

3 

Kong Builders - Kubernetes Ingress Controller: Expose TCP services with Kong

Kong • 1.3K views • Streamed 11 months ago

4 

Kong Ingress Controller Feature Preview: Gateway API

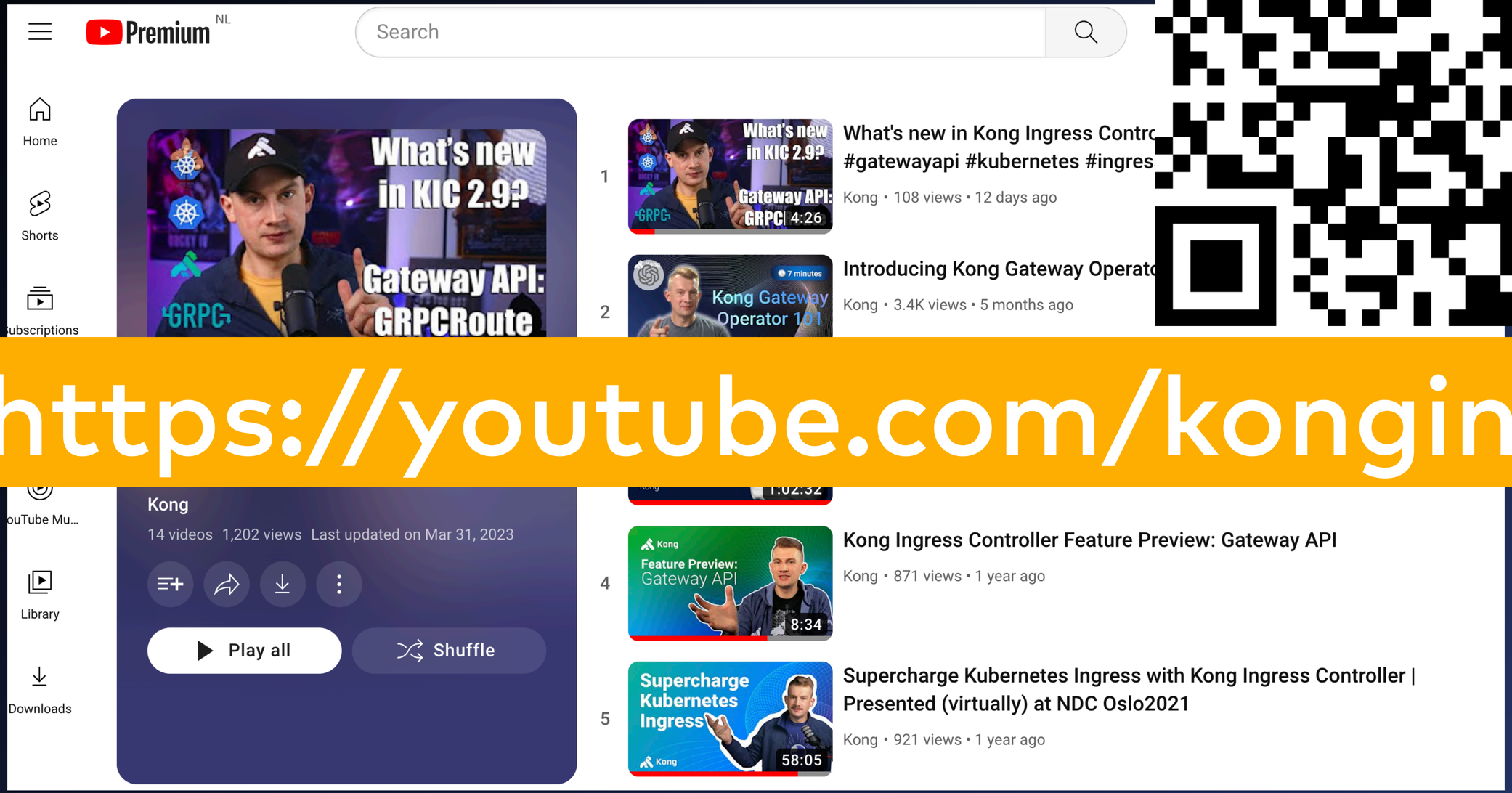
Kong • 871 views • 1 year ago

5 

Supercharge Kubernetes Ingress with Kong Ingress Controller | Presented (virtually) at NDC Oslo2021

Kong • 921 views • 1 year ago

Please, subscribe to my YouTube channel ™



https://youtube.com/konginc

@gamussa | #APIWorld | @thekonginc