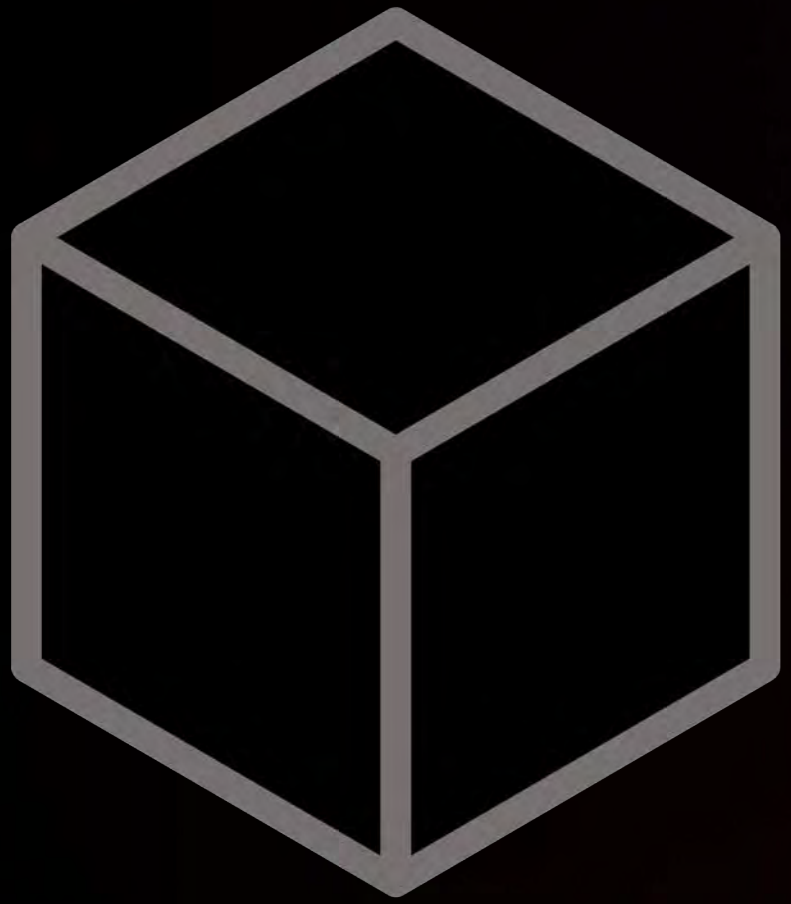
Application Networking on Kubernetes

Where are we now?

Federica Ciuffo

Sr Containers Specialist Solutions Architect



MONOLITH

INTERNAL CALLS

Loopback Interfaces

CLIENT TRAFFIC

Load Balancer

KUBERNETES

SERVICE TO SERVICE

CNI

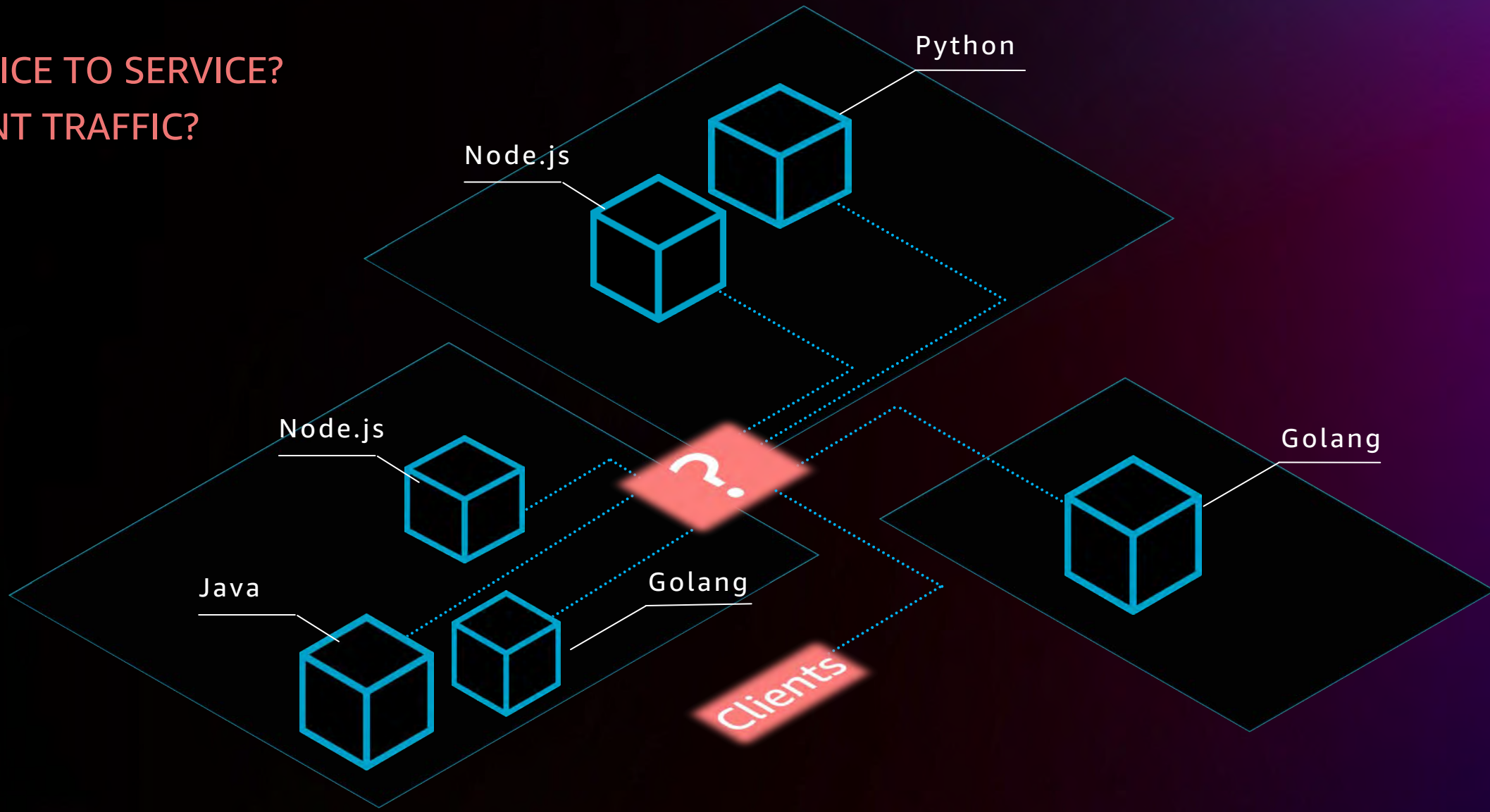
CLIENT TRAFFIC

Load Balancer

Ingress and
Ingress controllers

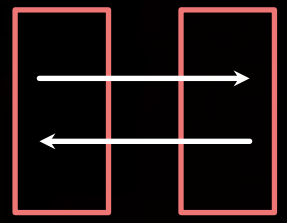
SERVICE TO SERVICE?

CLIENT TRAFFIC?



MICROSERVICES

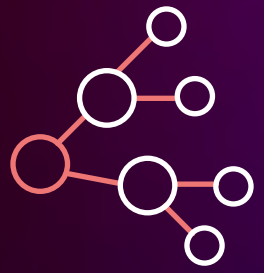
What is needed



CONSISTENT COMMUNICATIONS MANAGEMENT

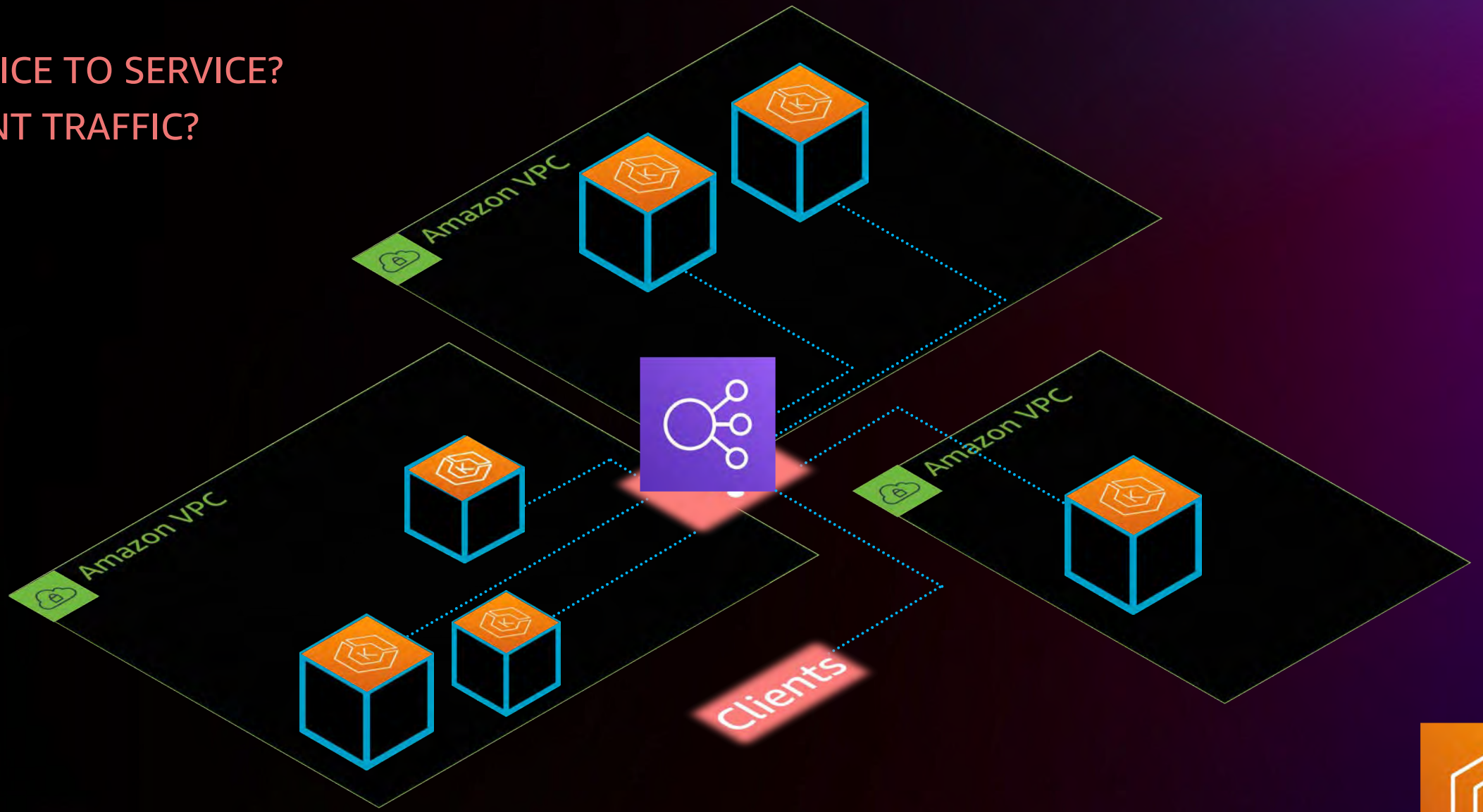
COMPLETE VISIBILITY

FAILURE ISOLATION AND PROTECTION



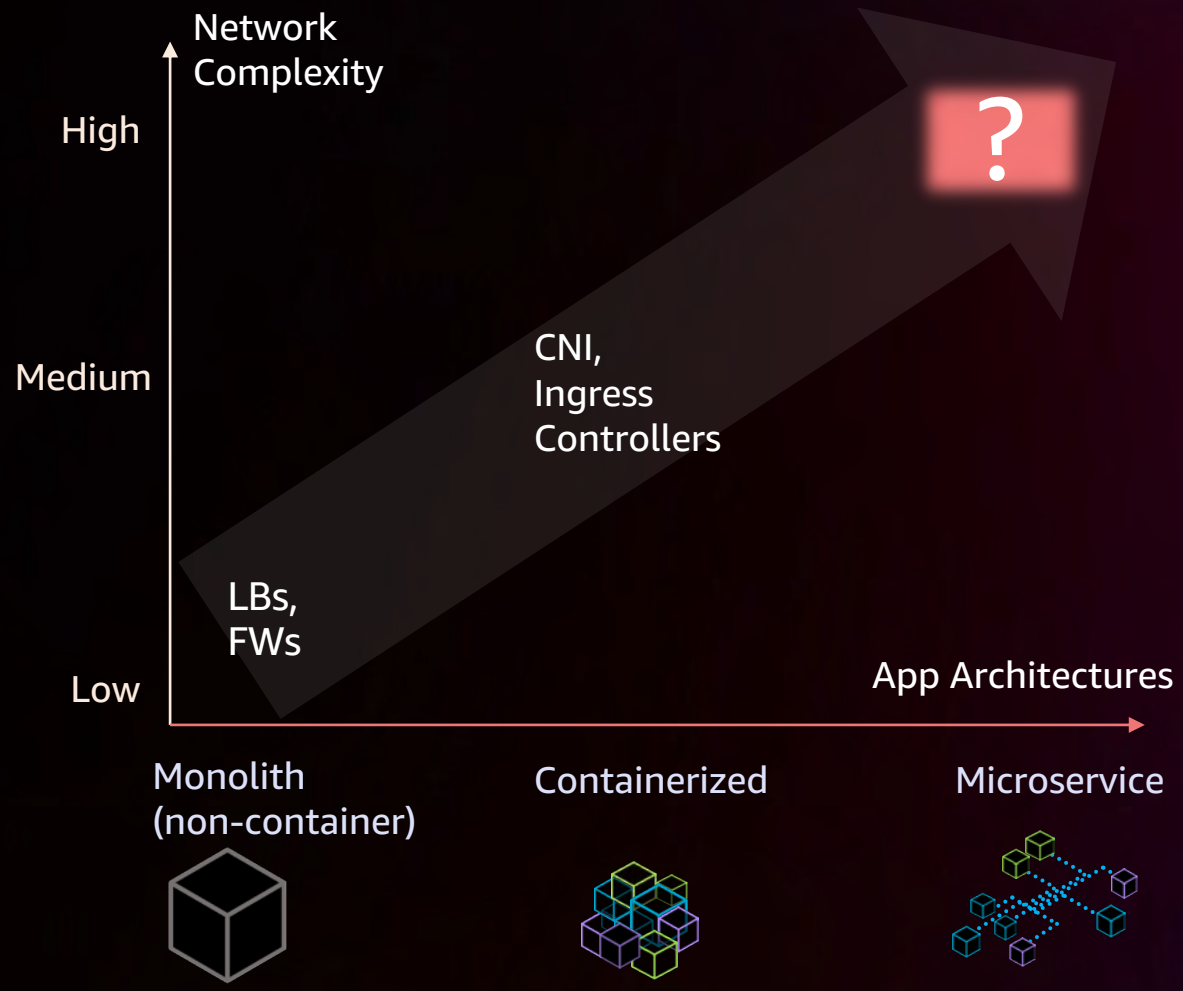
FINE-GRAINED DEPLOYMENT CONTROLS

SERVICE TO SERVICE?
CLIENT TRAFFIC?

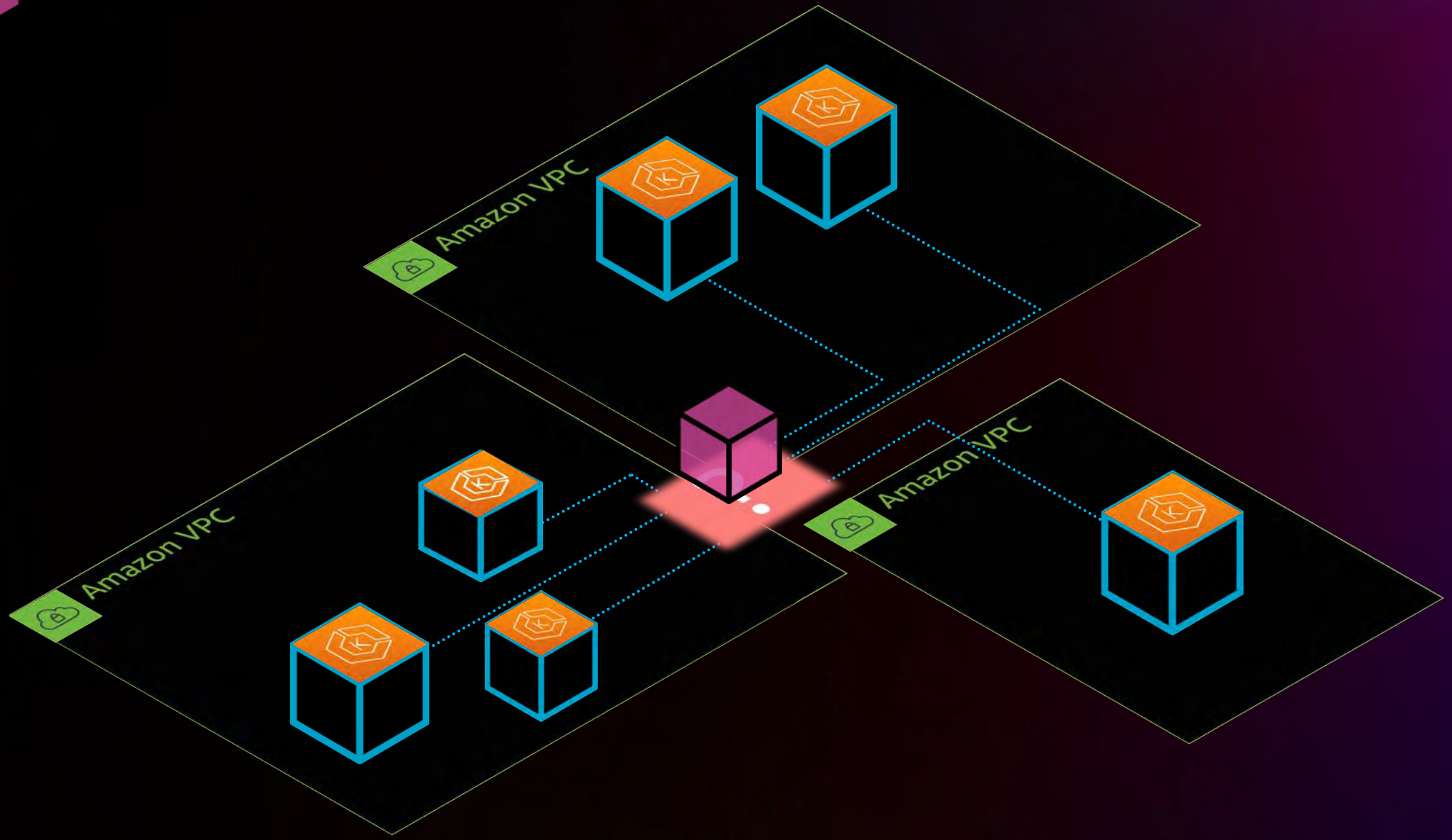


Amazon EKS

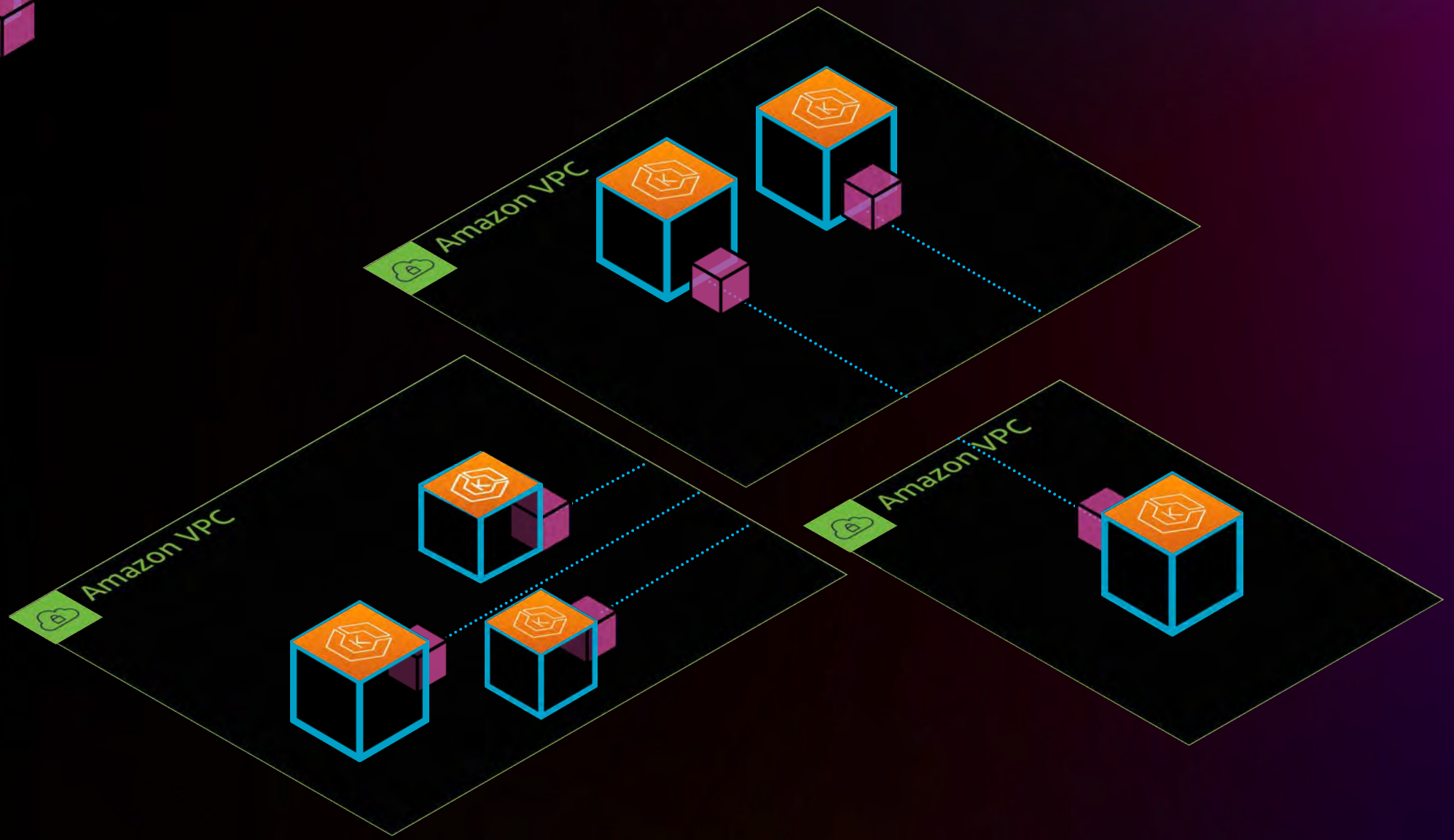
Higher Network complexity



PROXY

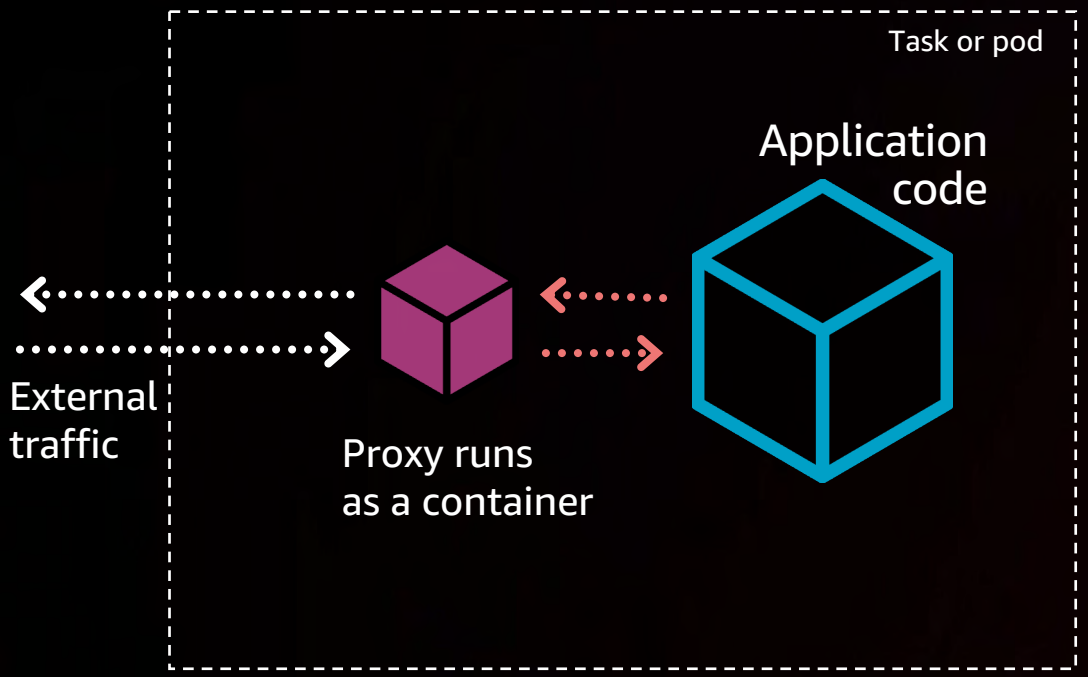


SIDECAR PROXY



Sidecar Proxy Pattern

DECOUPLE THE NETWORKING AND APPLICATION LAYERS



- Decouples install/upgrade
- Configurable: Separates business logic from operations
- Minimizes inconsistencies

Managing sidecars at scale

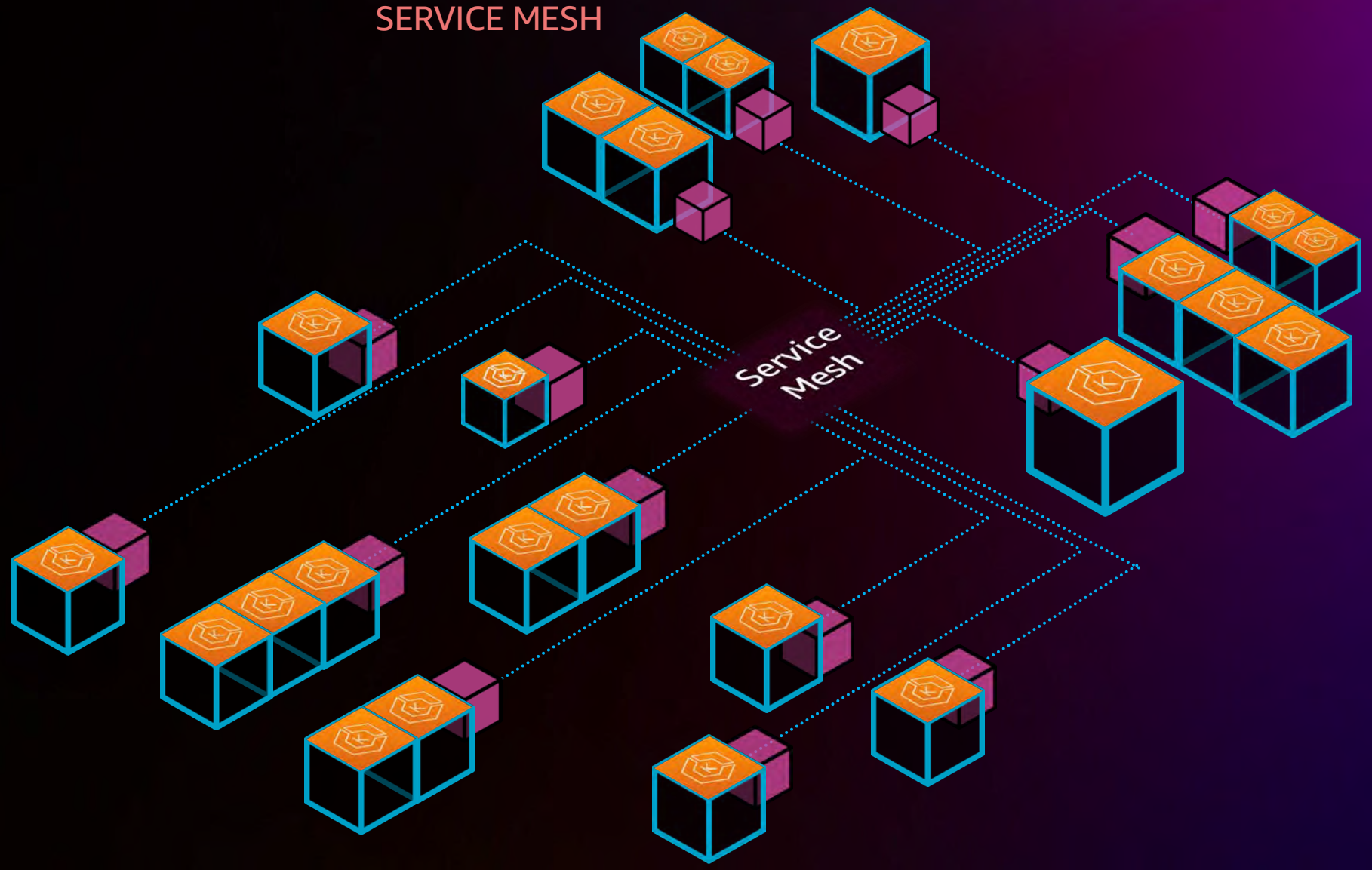
AWS App Mesh

Istio

Consul

Linkerd

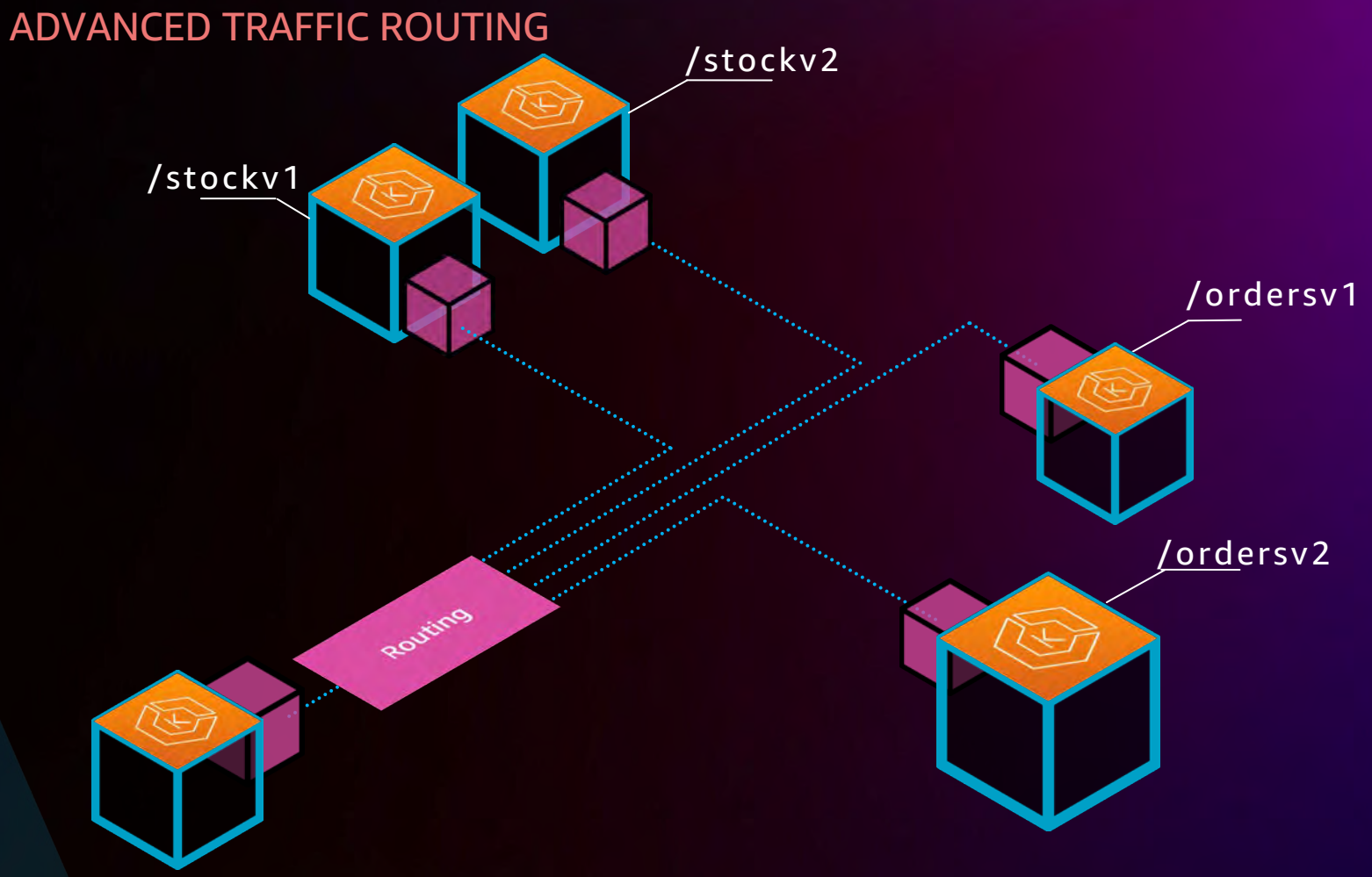
Kong



Use Cases for a Service Mesh

Use case:

As part of Blue / Green or Canary releases I want to do granular traffic routing and weighting.

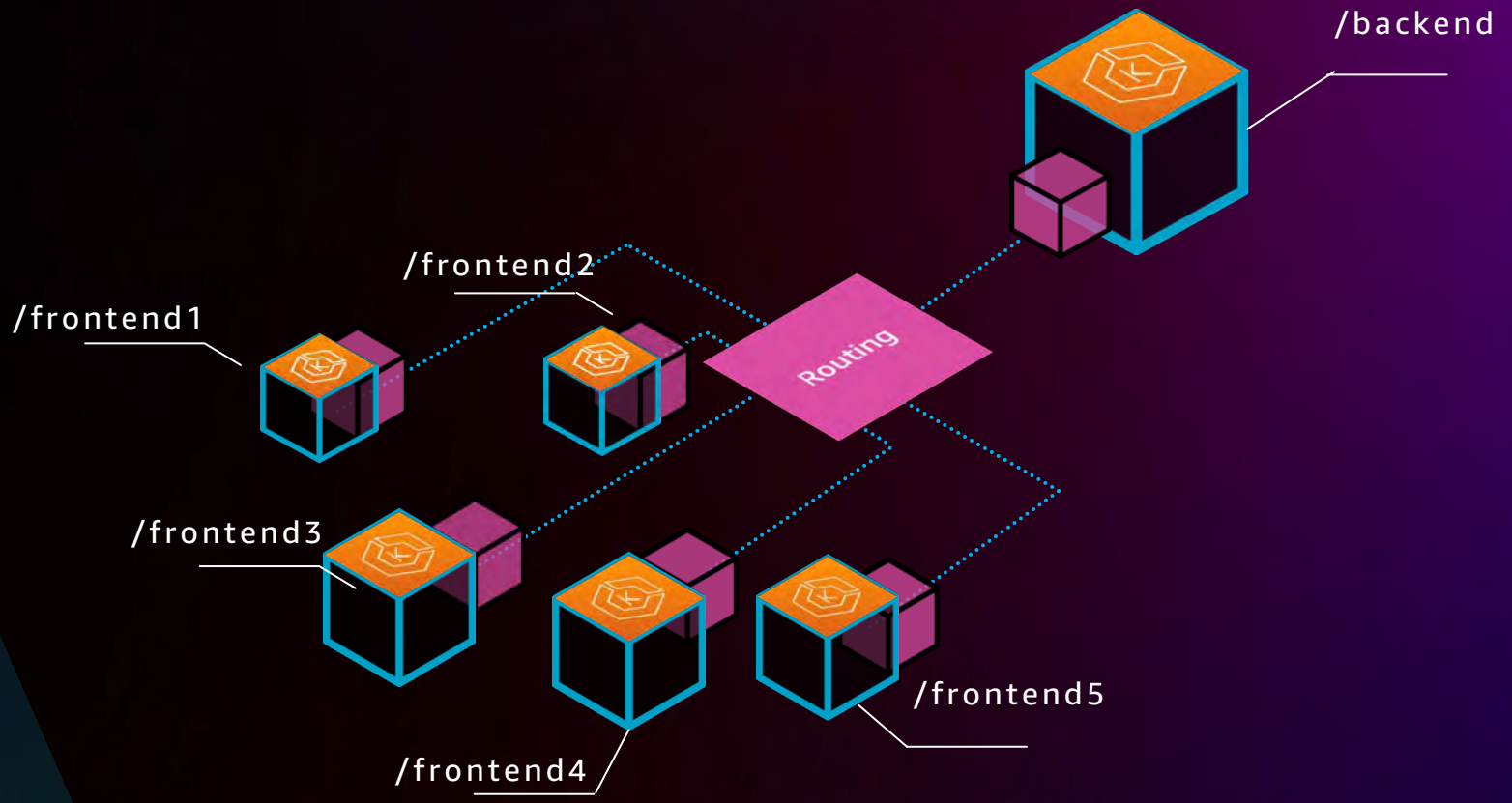


Use Cases for a Service Mesh

INCREASED NETWORK RELIABILITY

Use case:

I need to protect my application from large spikes in traffic to ensure a good level of service.

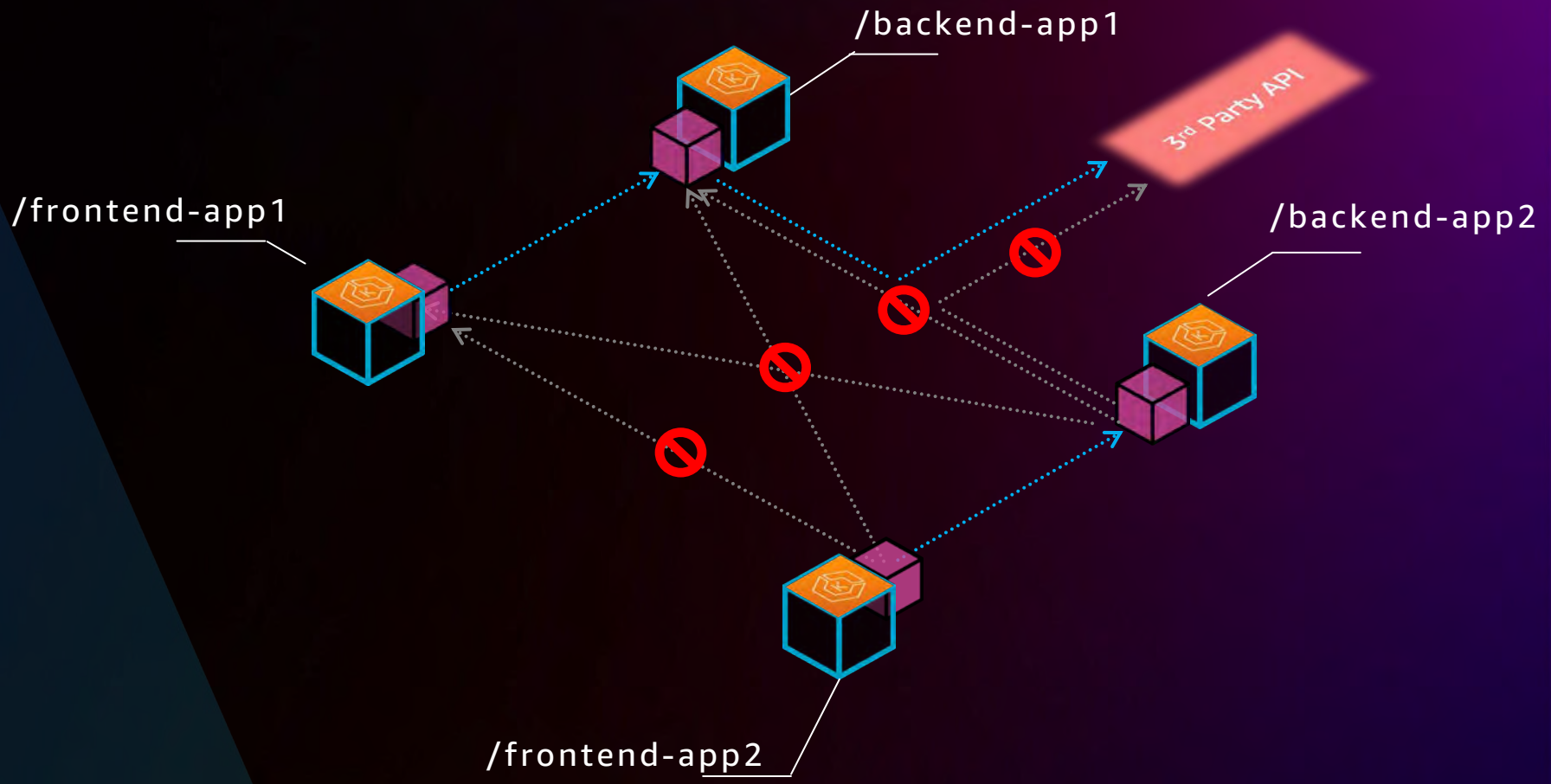


Use Cases for a Service Mesh

SECURITY – TRAFFIC ROUTING

Use case:

I want to create an allow list for my service for both internal and external services.

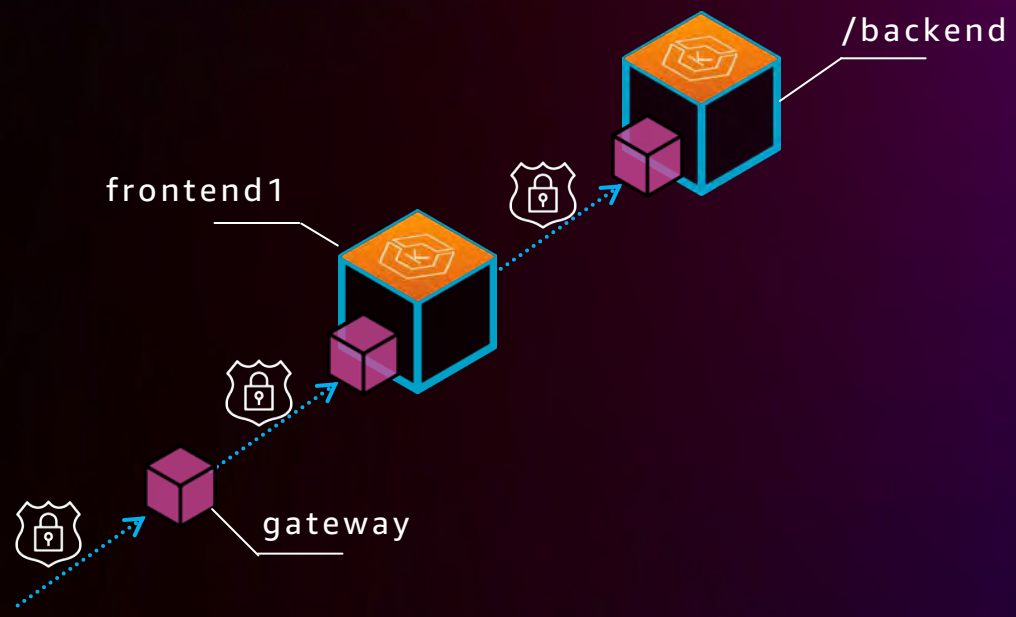


Use Cases for a Service Mesh

SECURITY – ENCRYPTED COMMUNICATION

Use case:

We have to ensure all communication is encrypted but do not want to put the burden on to the application teams.

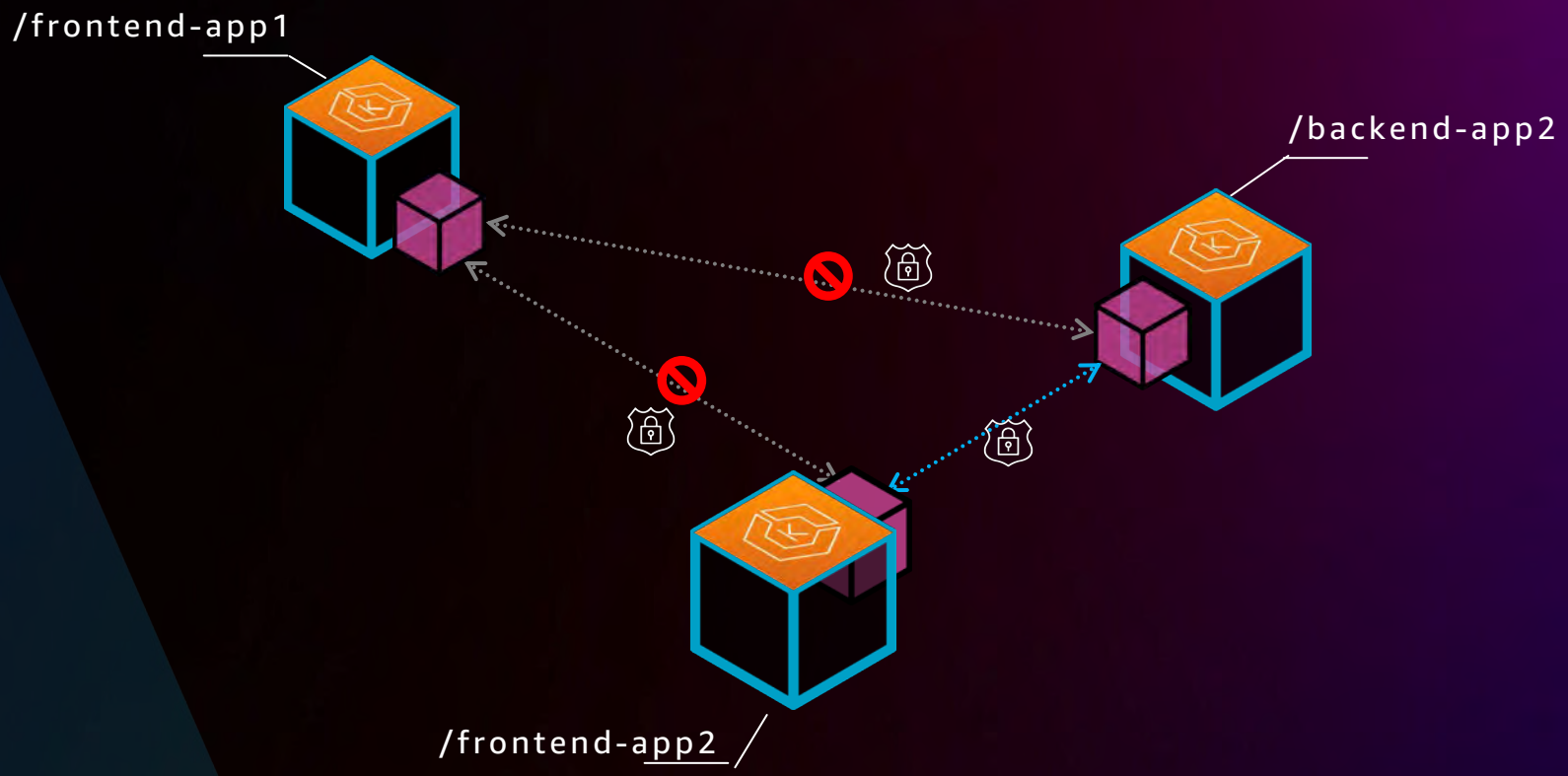


Use Cases for a Service Mesh

SECURITY – AUTHENTICATION

Use case:

All services need to have some form of identity, and that identity will be used to provide access to another service.

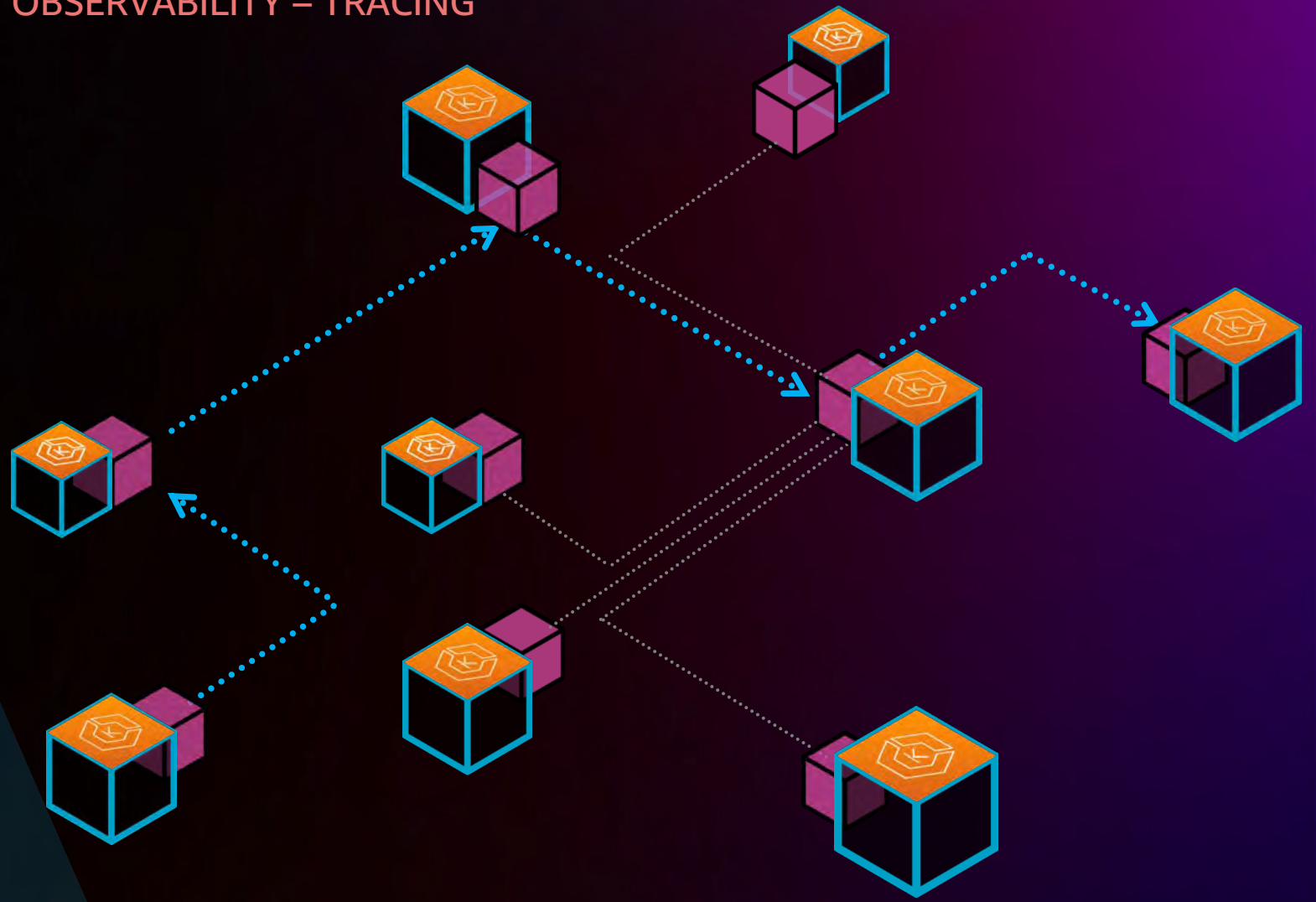


Use Cases for a Service Mesh

OBSERVABILITY – TRACING

Use case:

We would like to understand end to end traffic flows without touching the application code.

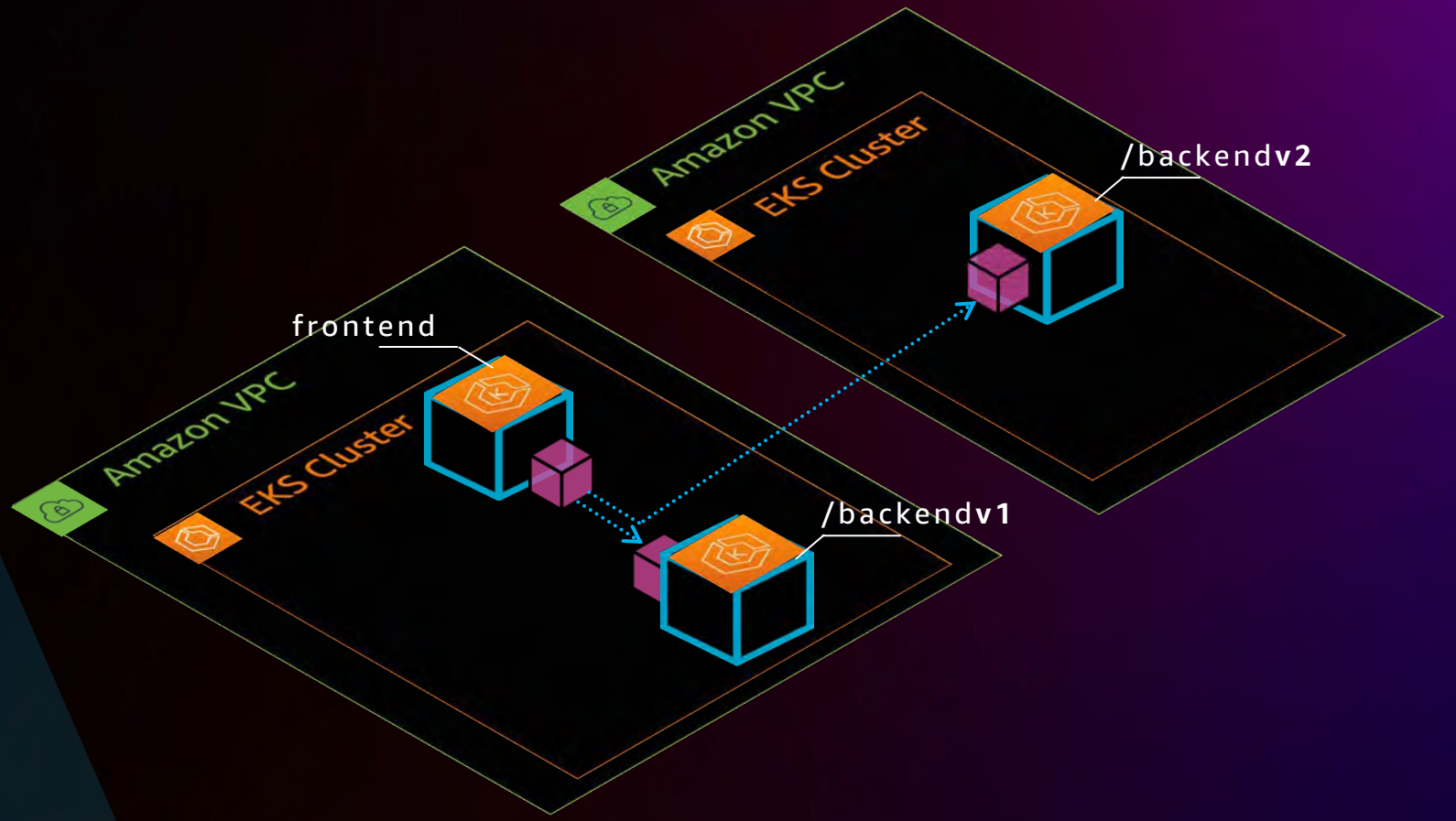


Use Cases for a Service Mesh

MULTI CLUSTER (OR ACCOUNT) NETWORKING

Use case:

I need to operate 2 active / active environments, how do I make services in Environment A aware of services in Environment B.



Envoy Proxy

- OSS project
- Wide community support, numerous integrations
- Stable and production-proven
- Graduated Project in Cloud Native Computing Foundation
- Started at Lyft in 2016

Istio

FUNDAMENTALS

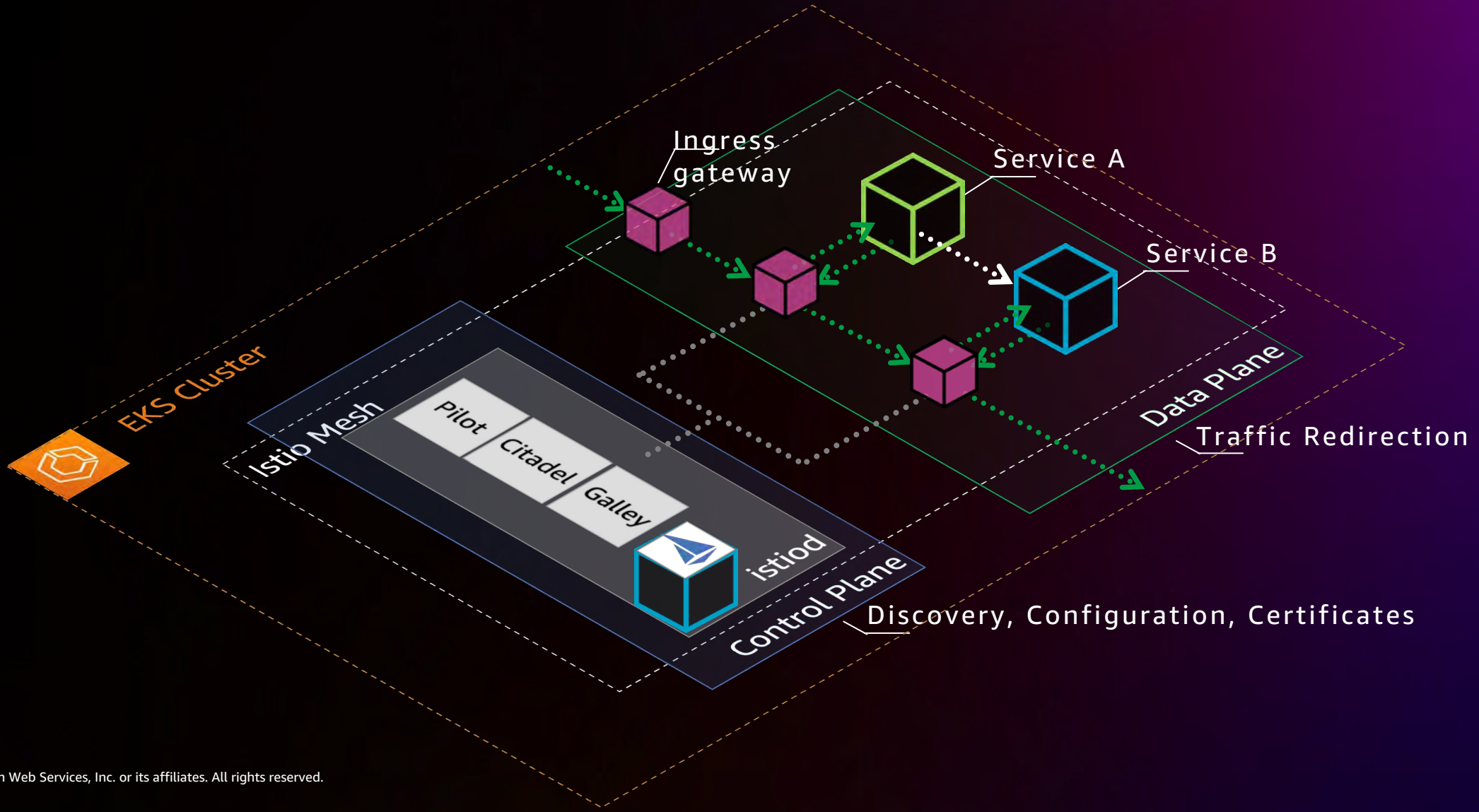
Mesh
Virtual Service
Virtual Gateways
Routing and Destination Rules
Service Discovery

Compatible
AWS Services

Observability

Istio

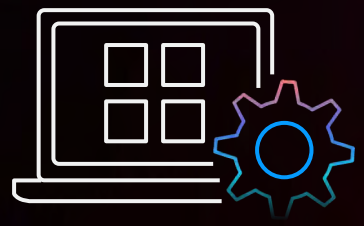
UNDER THE HOOD



Service mesh challenges

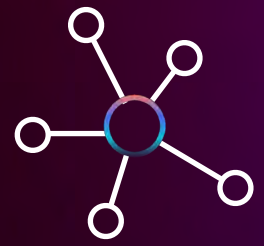
SIDECARS/PROXIES REQUIRED

Deploying and maintaining proxies at scale can be difficult



ONLY FOR CONTAINER-BASED WORKLOADS

Does not work for other workloads such as serverless and Amazon EC2



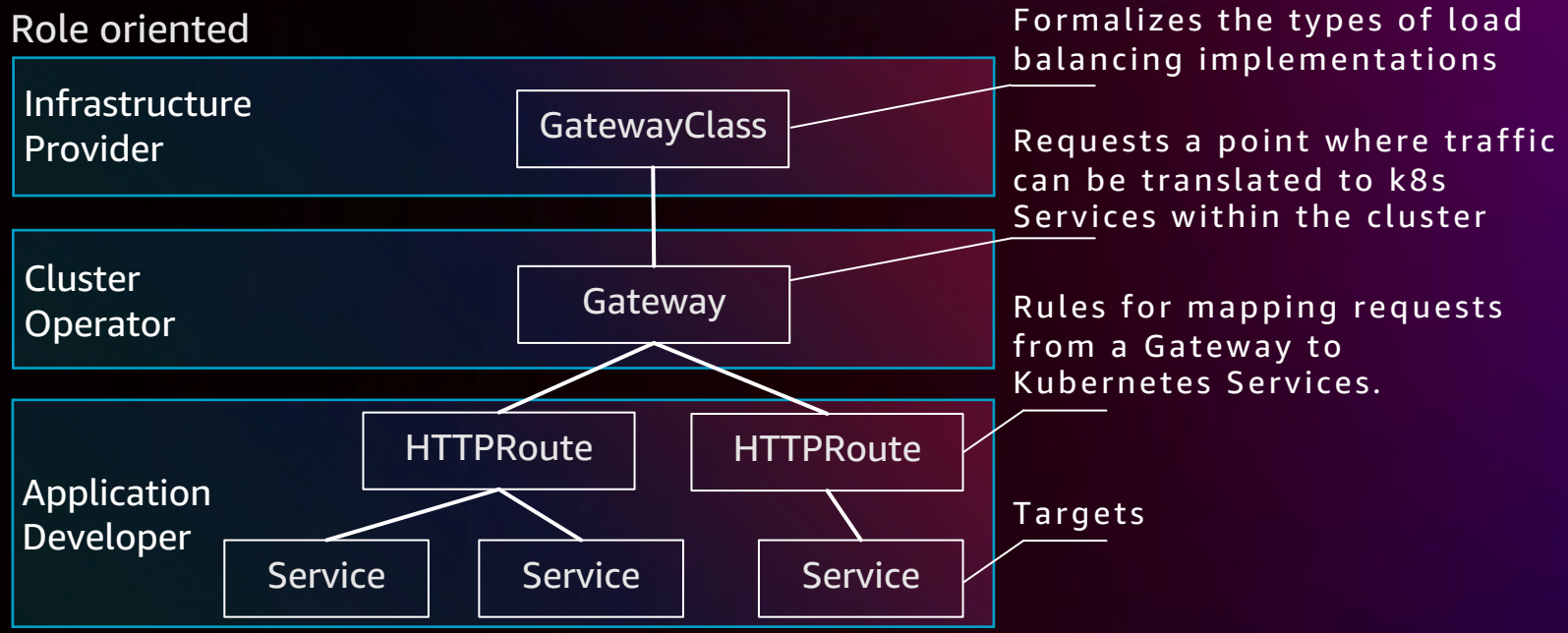
NETWORK CONNECTIVITY REQUIRED

Inter-VPC networking is not mapped to application and security needs

Kubernetes Gateway API

FUNDAMENTALS

SIG-Network project built to improve and standardize service networking in Kubernetes.



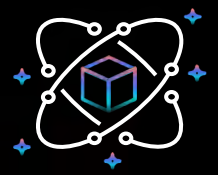
Implementations

PREVIEW

Amazon VPC Lattice

NO SIDECARS/PROXIES REQUIRED

Fully managed control and data plane, proxies to deploy and maintain



WORKS ACROSS ALL COMPUTE OPTIONS

Works across Amazon EC2, Amazon EKS, Amazon ECS, and AWS Lambda

TRAFFIC AND ACCESS CONTROLS

Improved security posture and rich traffic controls and segmentation

NO NETWORKING EXPERTISE REQUIRED

Simplified connectivity and security across VPCs and accounts

Amazon VPC Lattice

Components

Service network

A logical grouping mechanism to simplify how users enable connectivity and apply common policies.

Service

A unit of application running on instances, containers, and serverless and consisting of listeners, rules, and target groups.

Service directory

A centralized registry of all services that have been associated with Amazon VPC Lattice.

Security policies

IAM resource policy that can be associated with a Service Network and individual Services to support request level authentication and context specific authorization

Amazon EKS supports VPC Lattice

Kubernetes

K8S GATEWAY API

- Gateway Class
- Gateway
- HTTPRoute
- Service

Amazon EKS

KUBERNETES LATTICE CONTROLLER

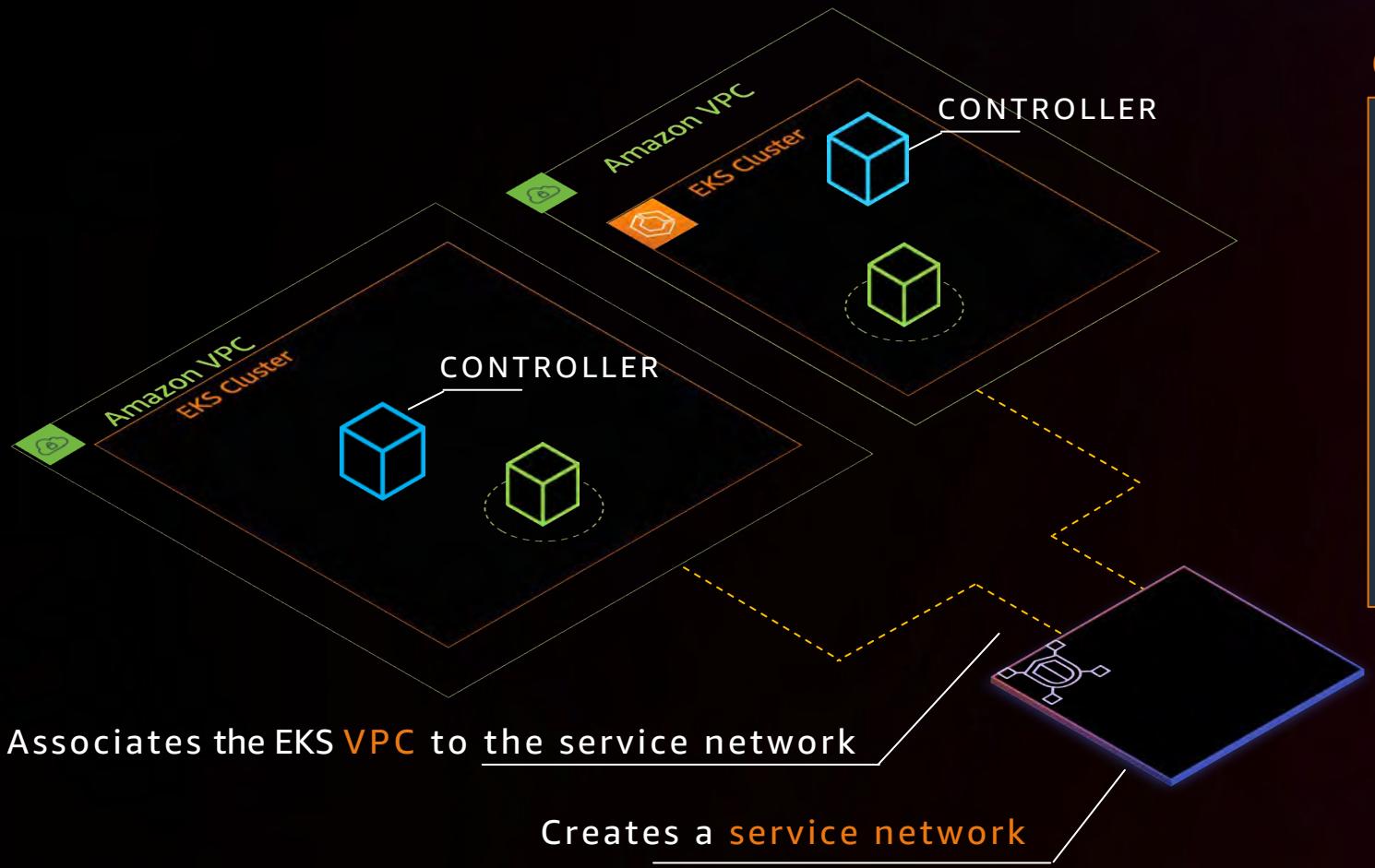
Amazon VPC Lattice

LATTICE RESOURCES

Service network
Service
Service directory
Security policies

Kubernetes Lattice Controller

HOW IT WORKS



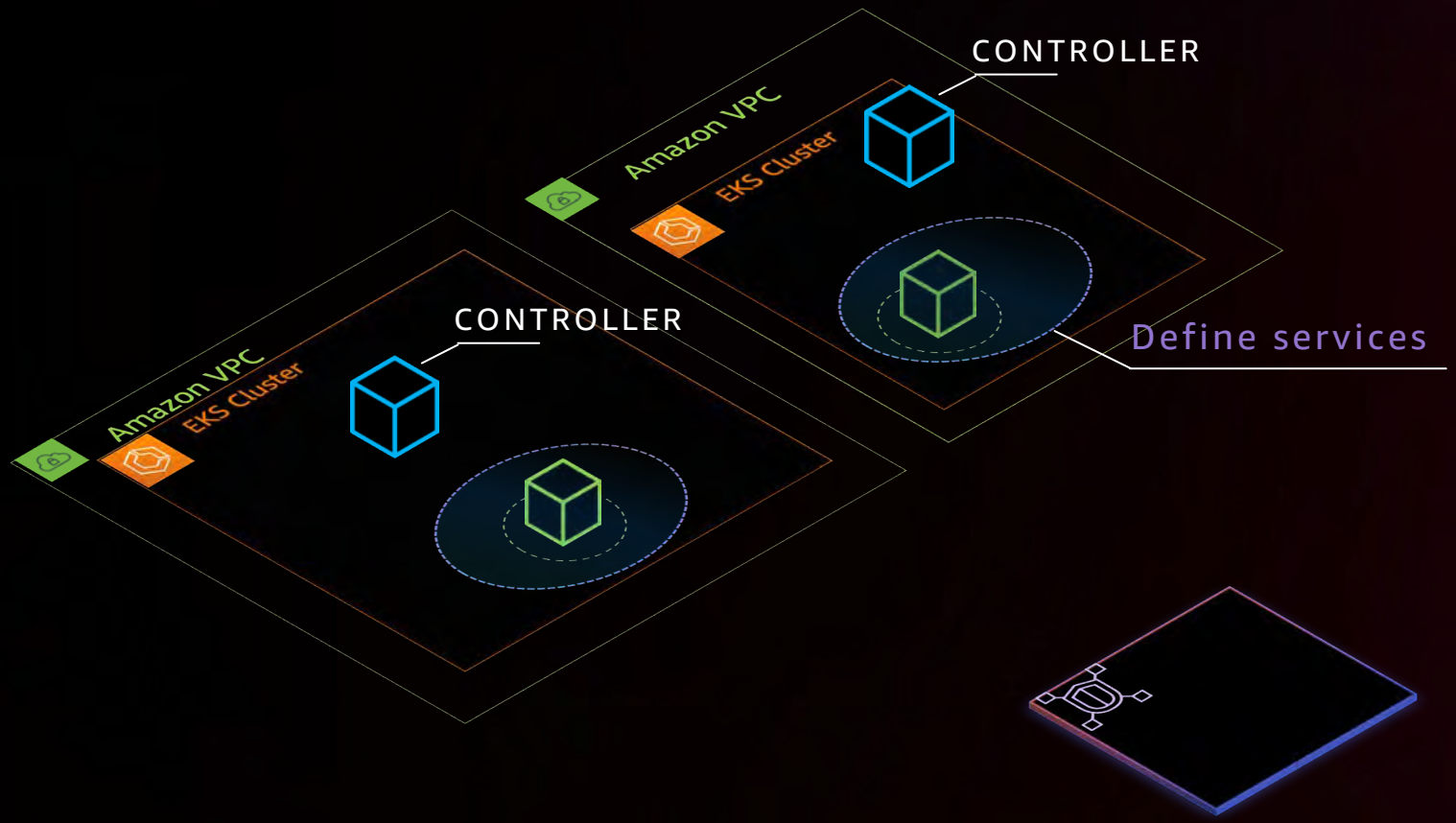
GATEWAY

```
apiVersion:
gateway.networking.k8s.io/v1alpha2
kind: Gateway
metadata:
name: my-gateway
spec:
gatewayClassName: amazon-vpc-lattice
listeners:
- name: http
protocol: HTTP
port: 80
```

Network admin

Kubernetes Lattice Controller

HOW IT WORKS



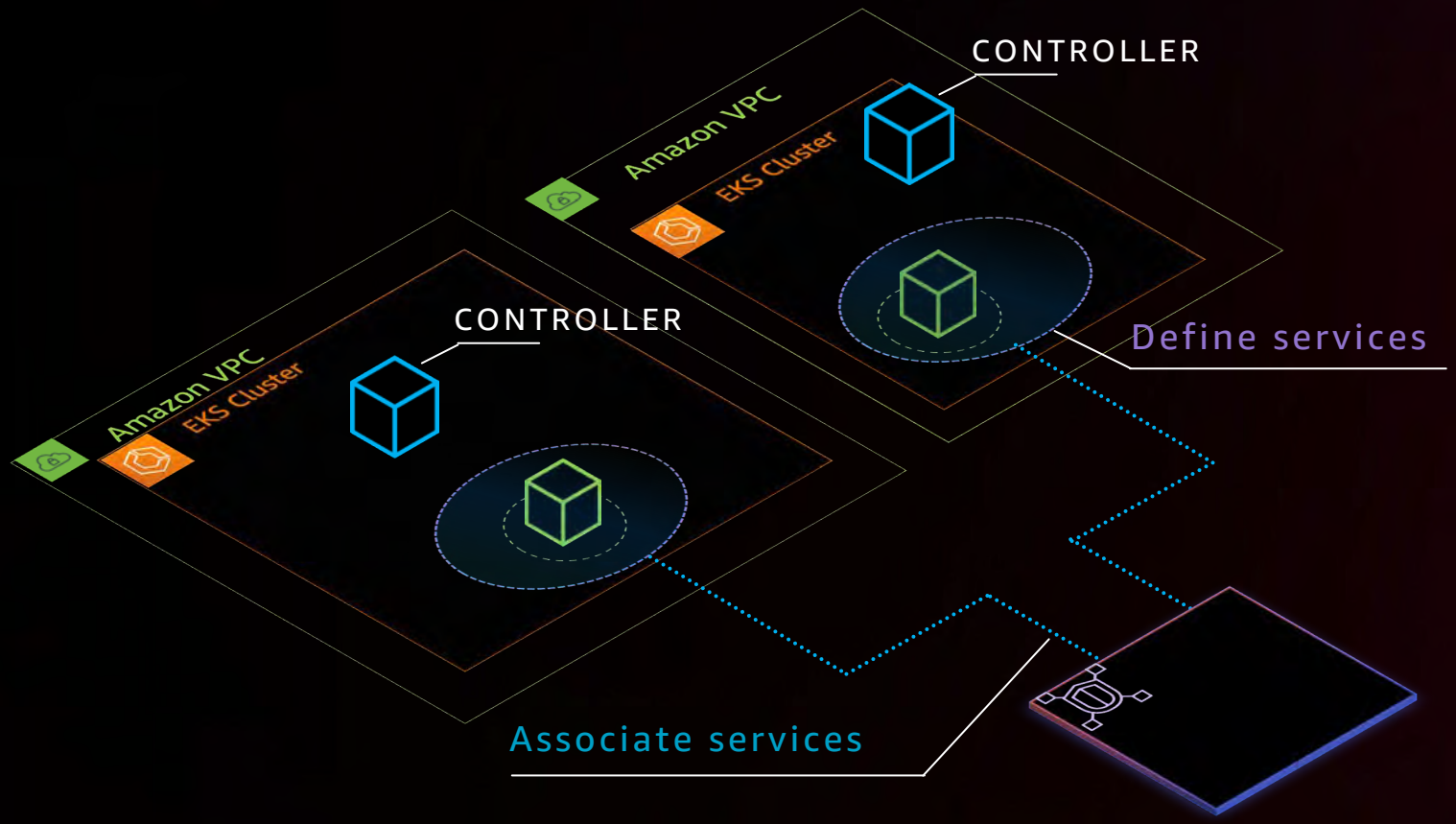
HTTPRoute

```
apiVersion:
gateway.networking.k8s…
kind: HTTPRoute
metadata:
name: inventory
spec:
parentRefs:

sectionName: http
rules:
-backendRefs:
- name: localservice
kind: Service

- name: externalservice
kind: ServiceImport
```


Developers

Kubernetes Lattice Controller

HOW IT WORKS



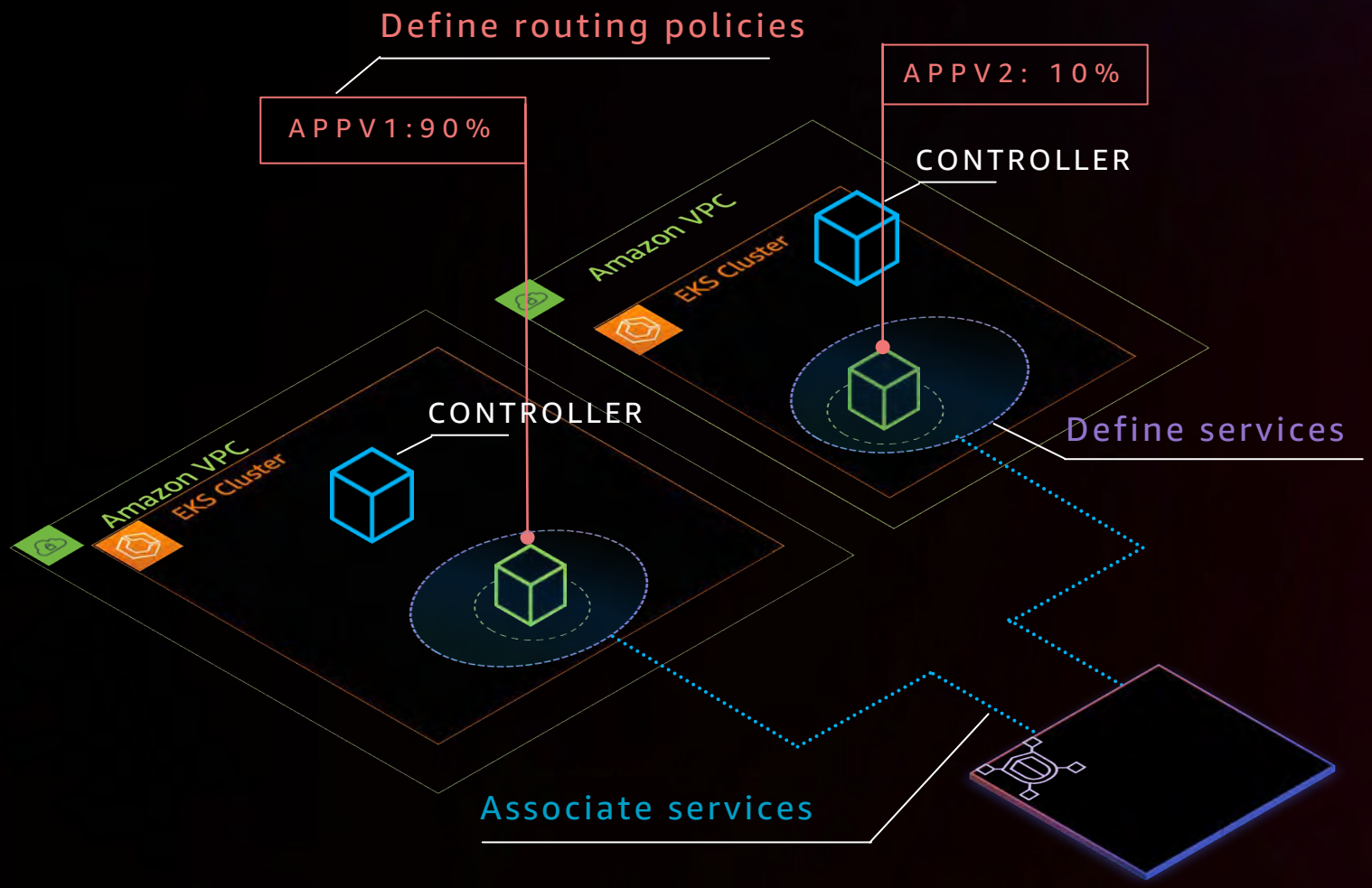
HTTPRoute

```
apiVersion:
gateway.networking.k8s…
kind: HTTPRoute
metadata:
name: inventory
spec:
parentRefs:
-name: my-gateway
sectionName: http
rules:
-backendRefs:
- name: localservice
kind: Service

- name: externalservice
kind: ServiceImport
```


Developers

Kubernetes Lattice Controller

HOW IT WORKS



HTTPRoute

```
apiVersion:
gateway.networking.k8s…
kind: HTTPRoute
metadata:
name: inventory
spec:
parentRefs:
-name: my-gateway
sectionName: http
rules:
-backendRefs:
- name: localservice
kind: Service
weight: 90
- name: externalservice
kind: ServiceImport
weight: 10
```


Developers

Thank you!

Federica Ciuffo
fciuffo@amazon.com