
AWS
re:Invent
DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

KUB406

Networking strategies for Kubernetes

Federica Ciuffo

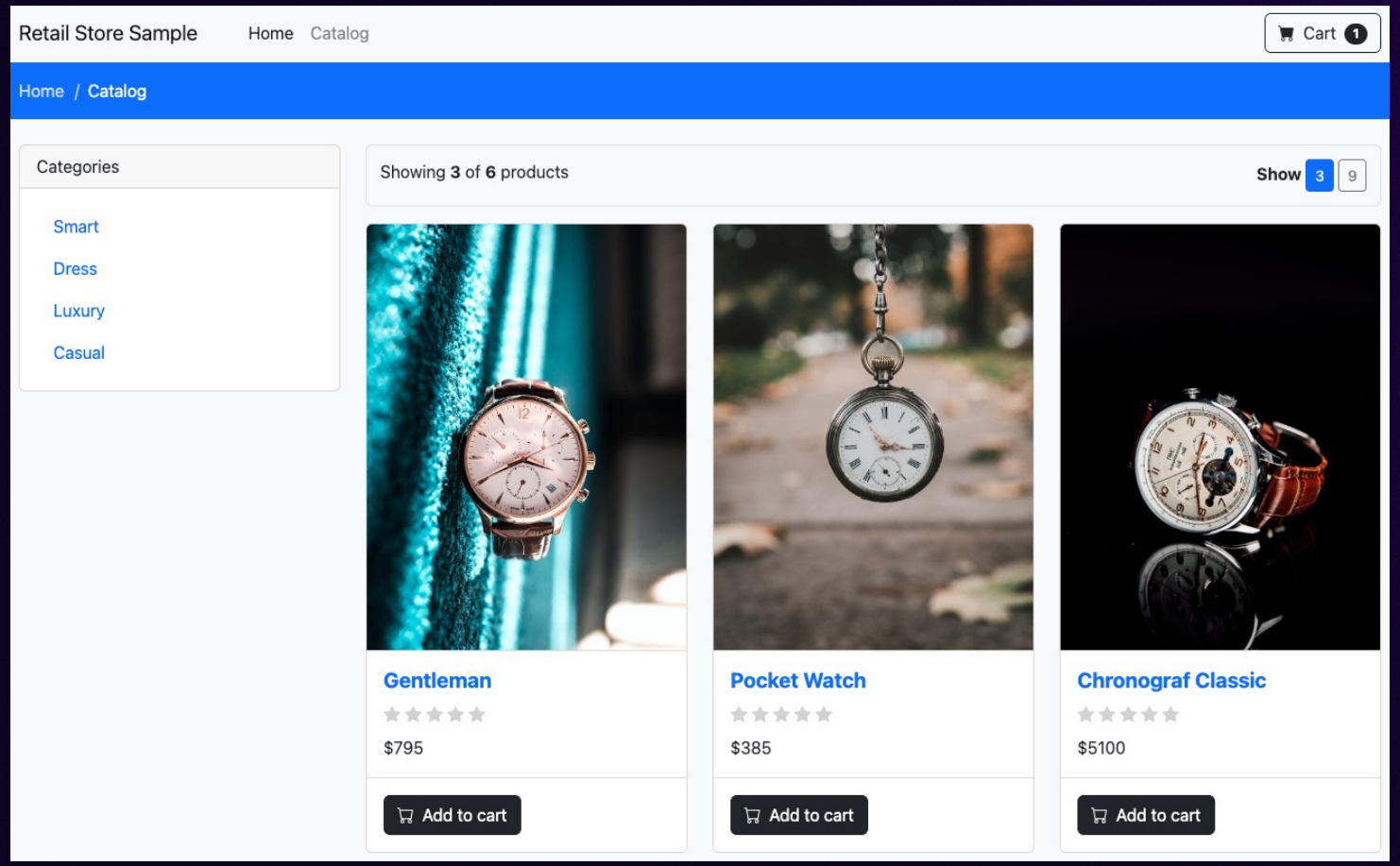
Sr Containers Specialist SA
AWS

Sai Vennam

Principal WW Containers Specialist
AWS

Rental Store

THE APPLICATION



Cloud Architect
FEDE

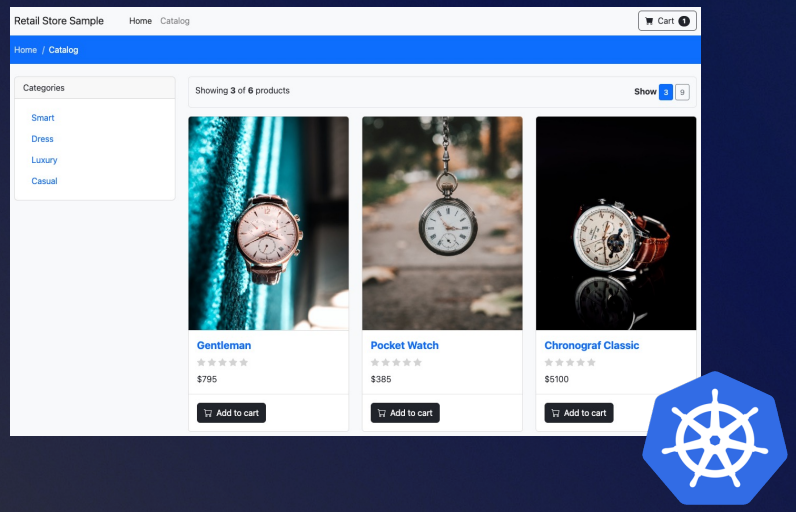
Cluster Operator
SAI

Cloud Architect

FEDE

Cluster Operator

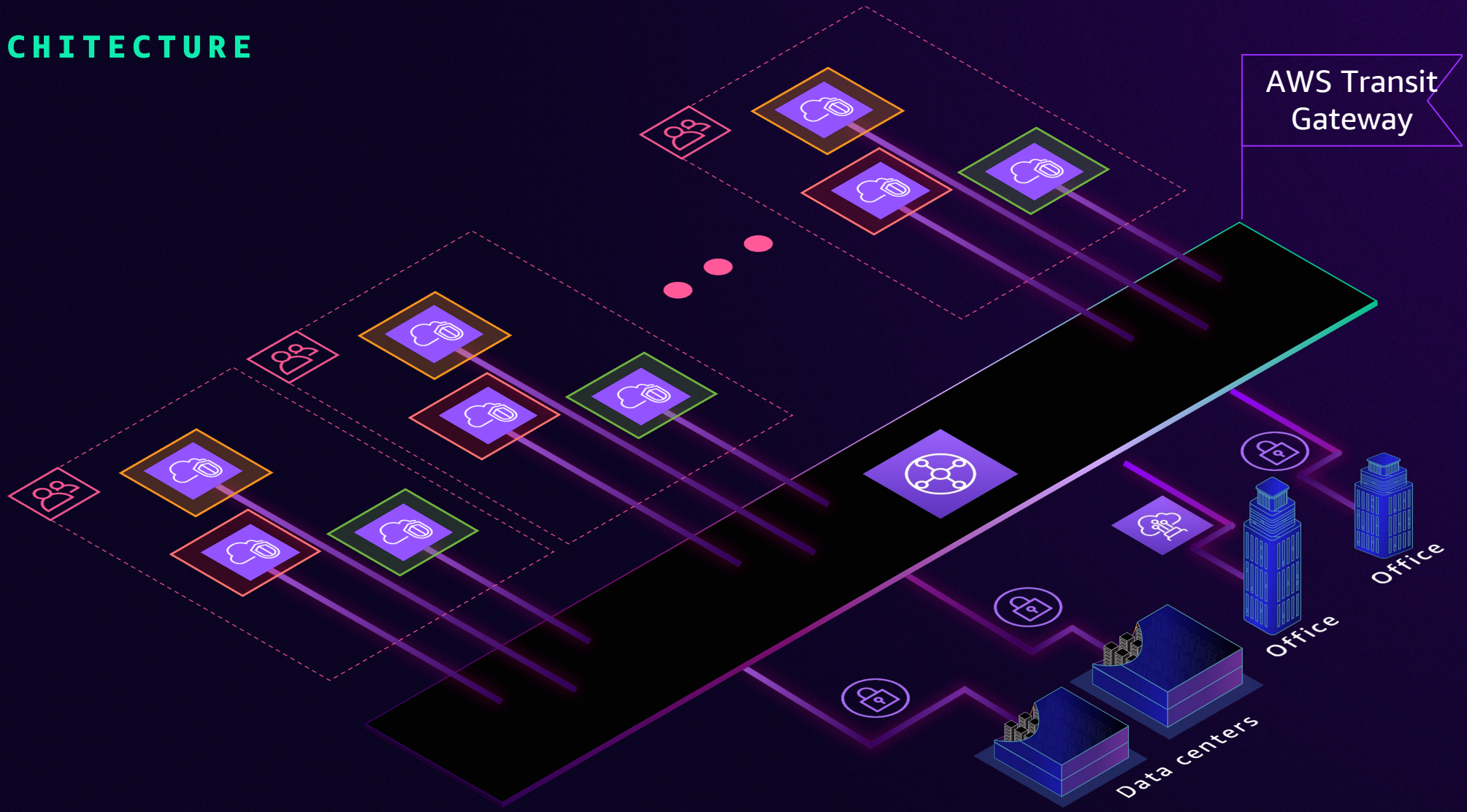
SAI



- Simplify cluster operations
- Enable external access to application
- Improve network resiliency
- Monitor performance and secure communication
- Mitigate deployment risk with blue-green strategies

The environment

ARCHITECTURE

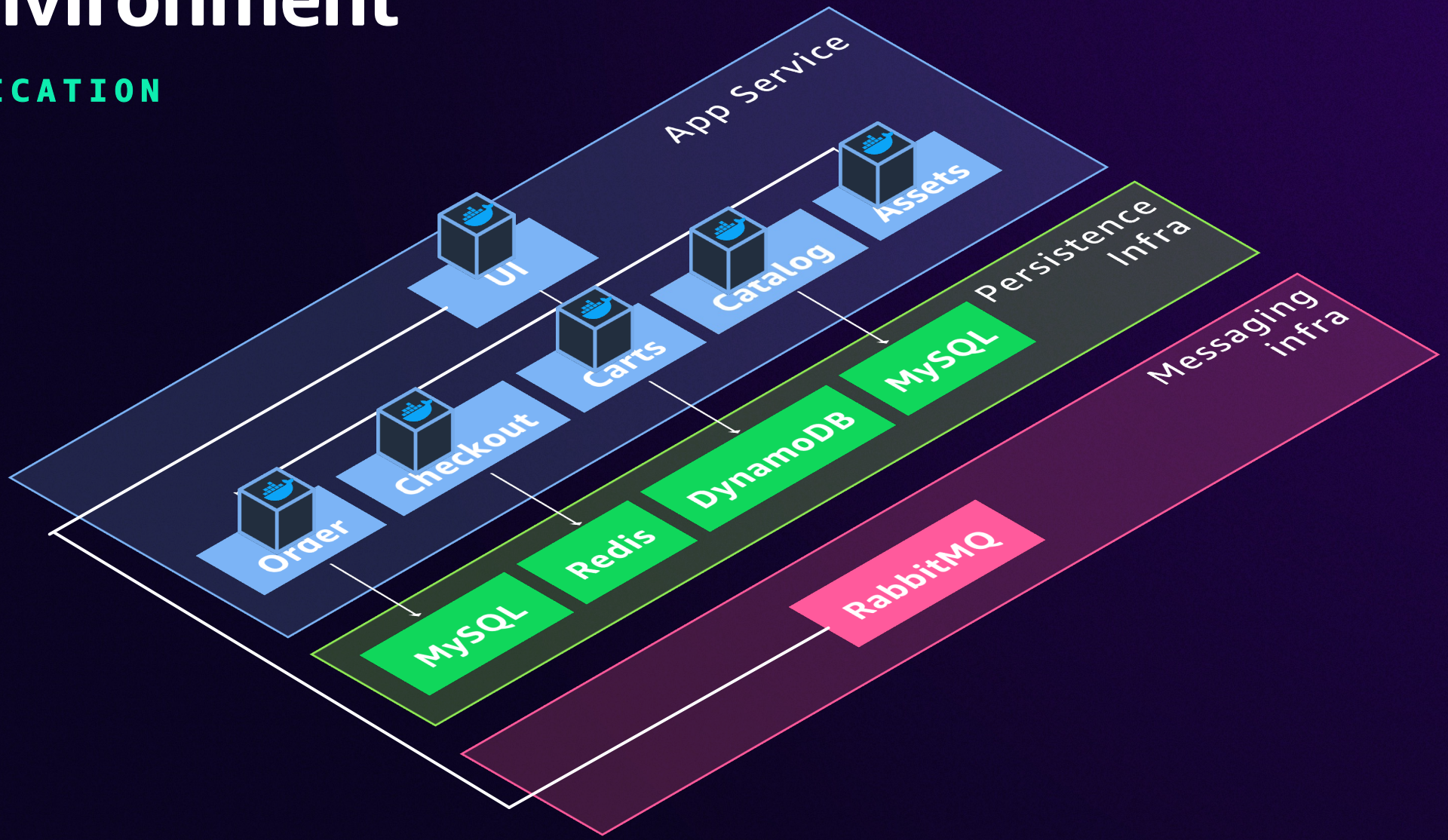


The environment

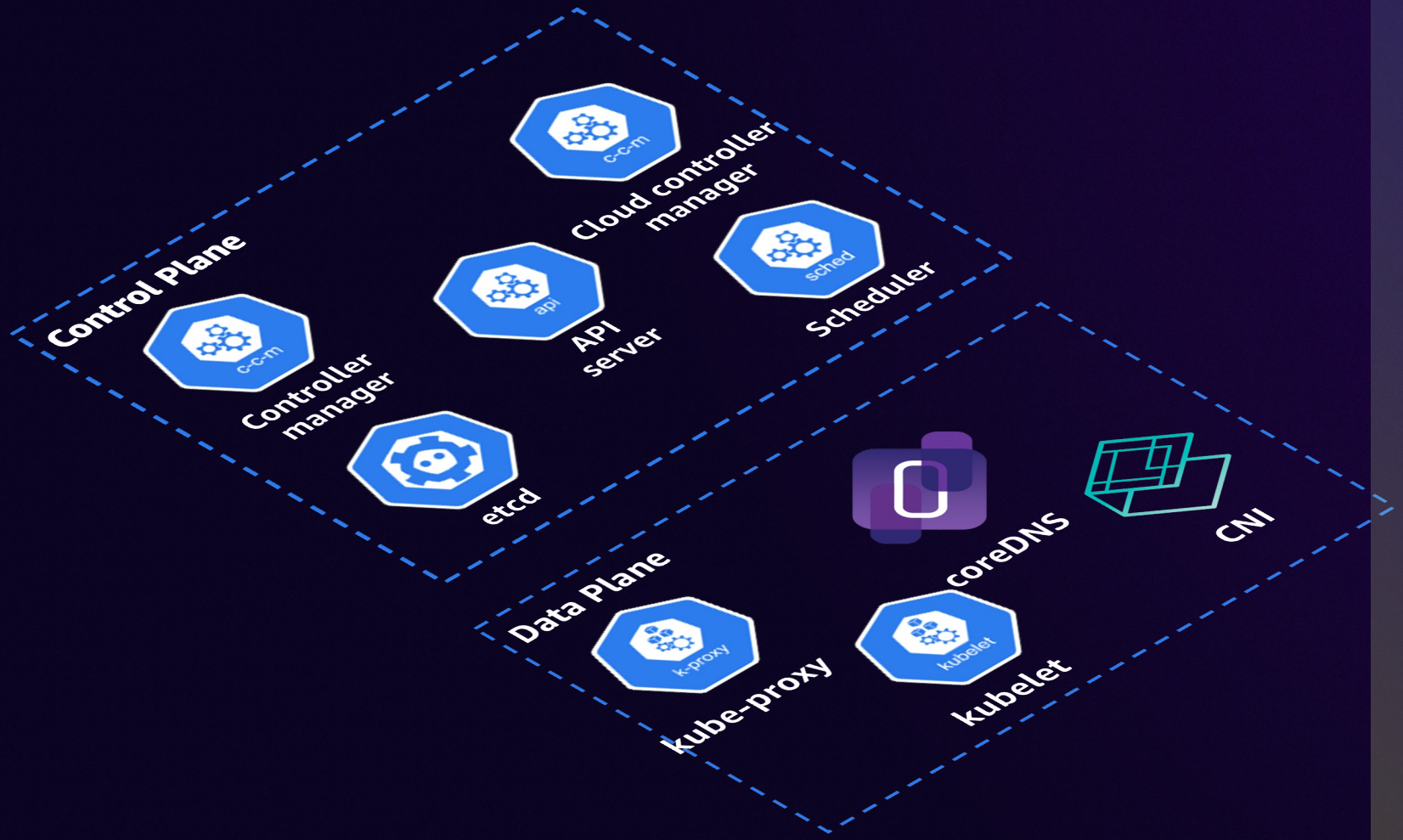
RETAIL ACCOUNT

The environment

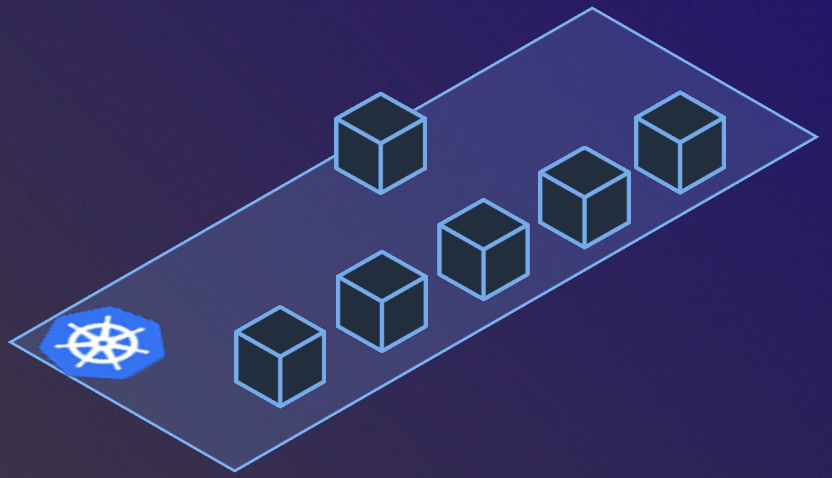
THE APPLICATION



Kubernetes architecture



Simplify cluster operations



Amazon EKS

MANAGED KUBERNETES EXPERIENCE

- ✓ Upstream and certified conformant version of Kubernetes (with backported security fixes)
- ✓ Provides a managed Kubernetes experience for performant, reliable, and secure Kubernetes
- ✓ Simplifies Kubernetes operations, administration, and management

Includes core capabilities for production-ready clusters

Automatically provisions cluster infrastructure

Create cluster 1

Core Network Components

WITH AMAZON EKS

Auto Mode

Automatically updates nodes and core capabilities

Dynamically scales resources

Continuously optimizes for cost

Managed capabilities for networking

Out-of-the box managed CoreDNS on every node

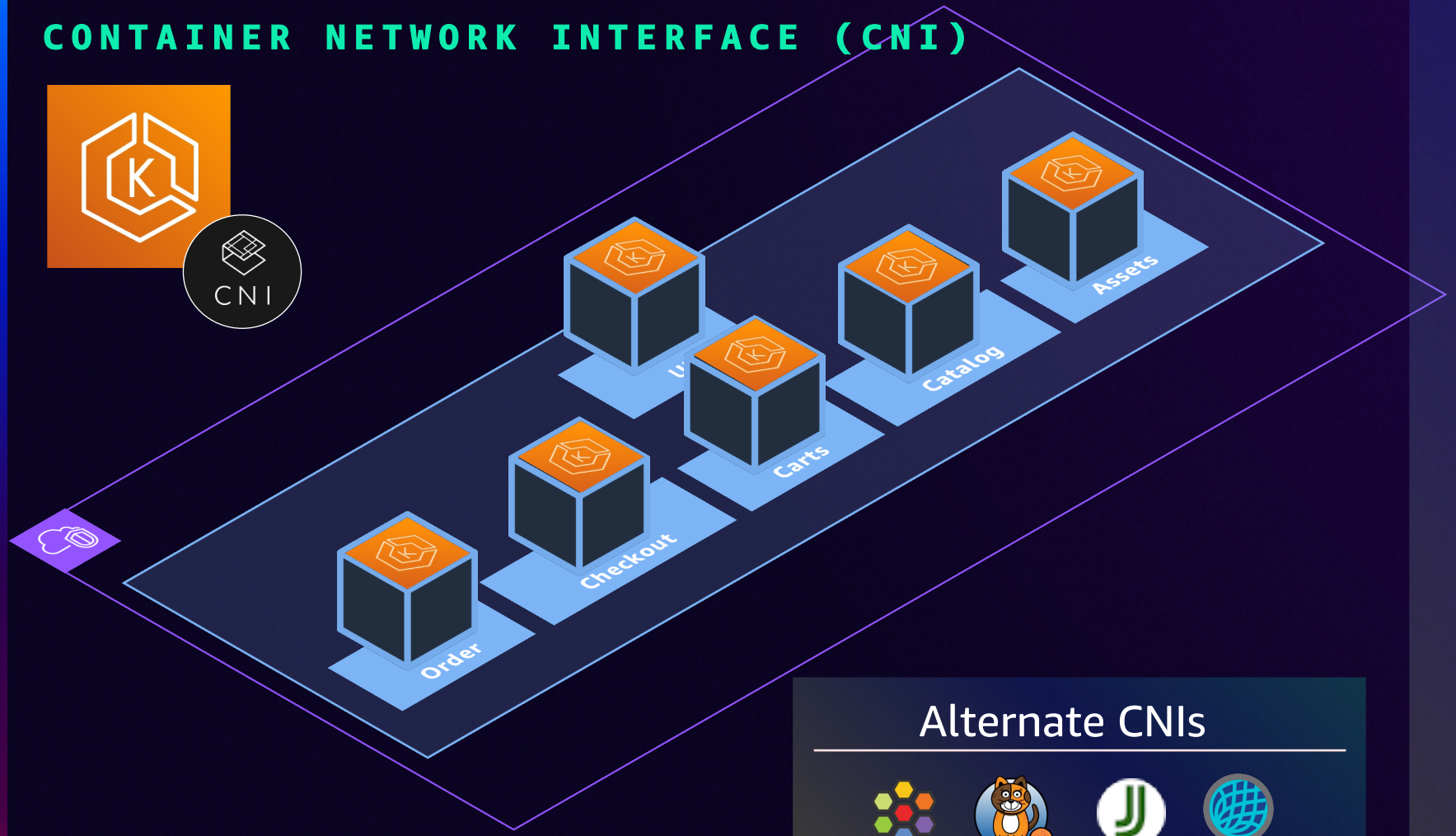
Fully managed and simplified Amazon VPC CNI for pod networking and default security enforcement through network policy

Fully managed kube-proxy in iptables mode

Now run as systemd services on the node

Amazon EKS

CONTAINER NETWORK INTERFACE (CNI)

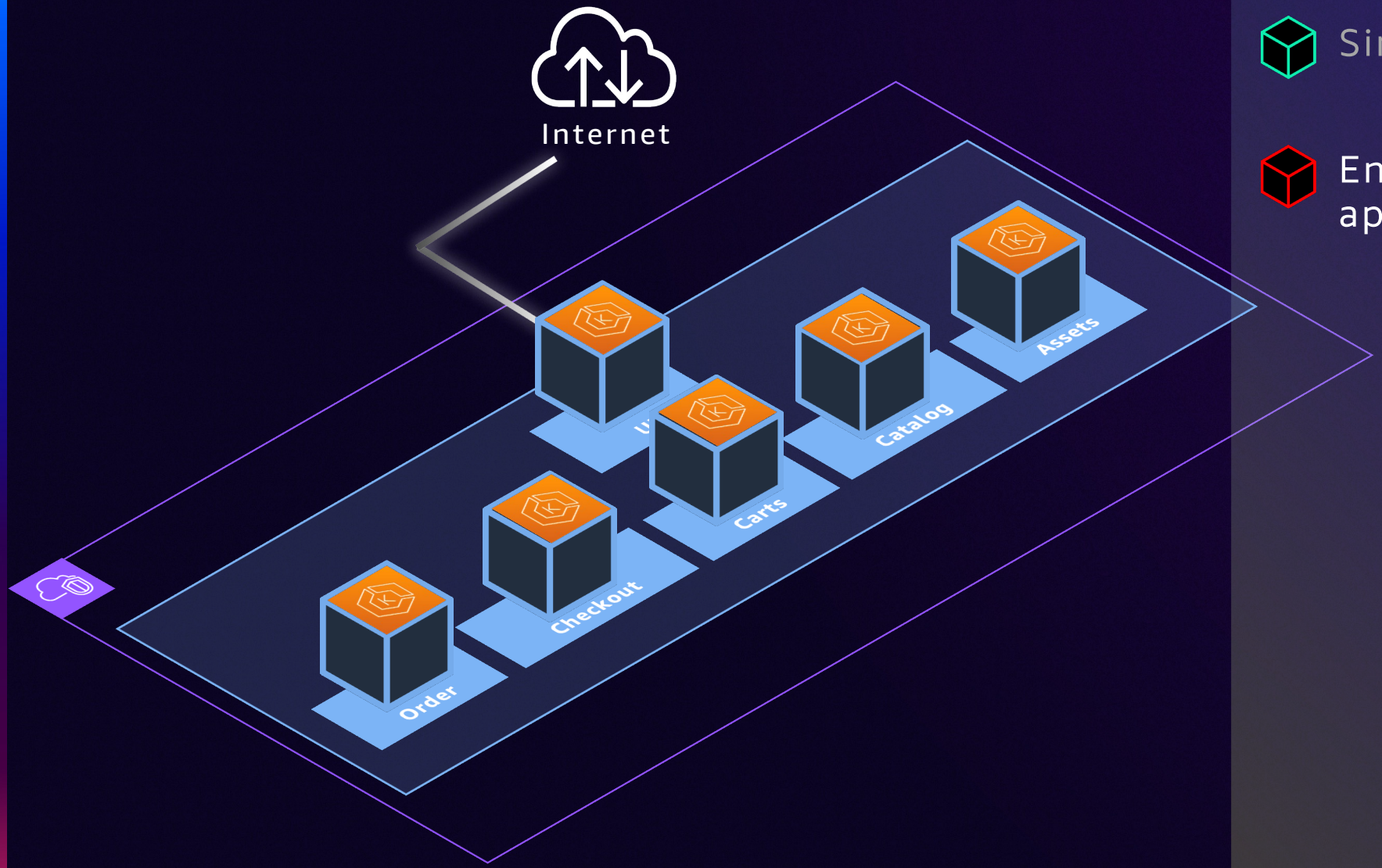


Alternate CNIs

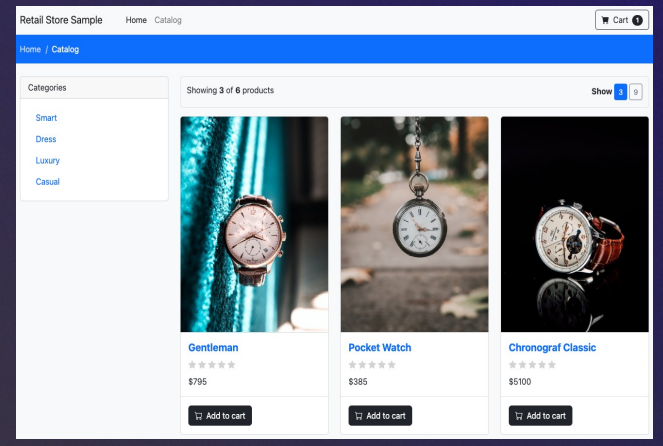
! Commercial support from vendor is recommended

Amazon VPC CNI

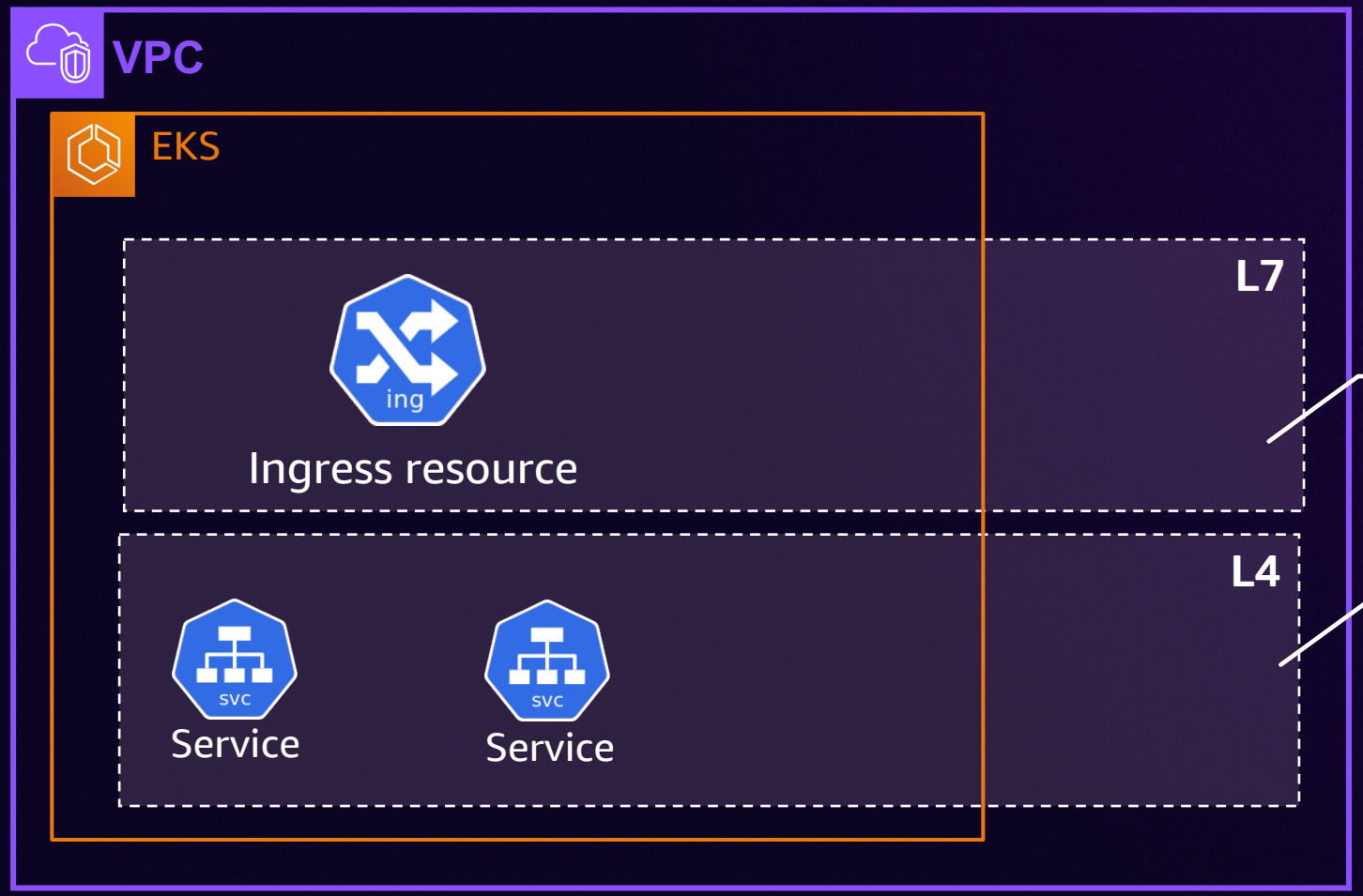
- ✓ **Reduced complexity**
  Integrates with Amazon VPC networking
- ✓ **Improved performance**
  No network translation required
- ✓ **Security**
  Integrates with AWS security features
- ✓ **Enables diverse workloads**
  Highly customizable CNI



- Simplify cluster operations
- Enable external access to application



Inbound traffic

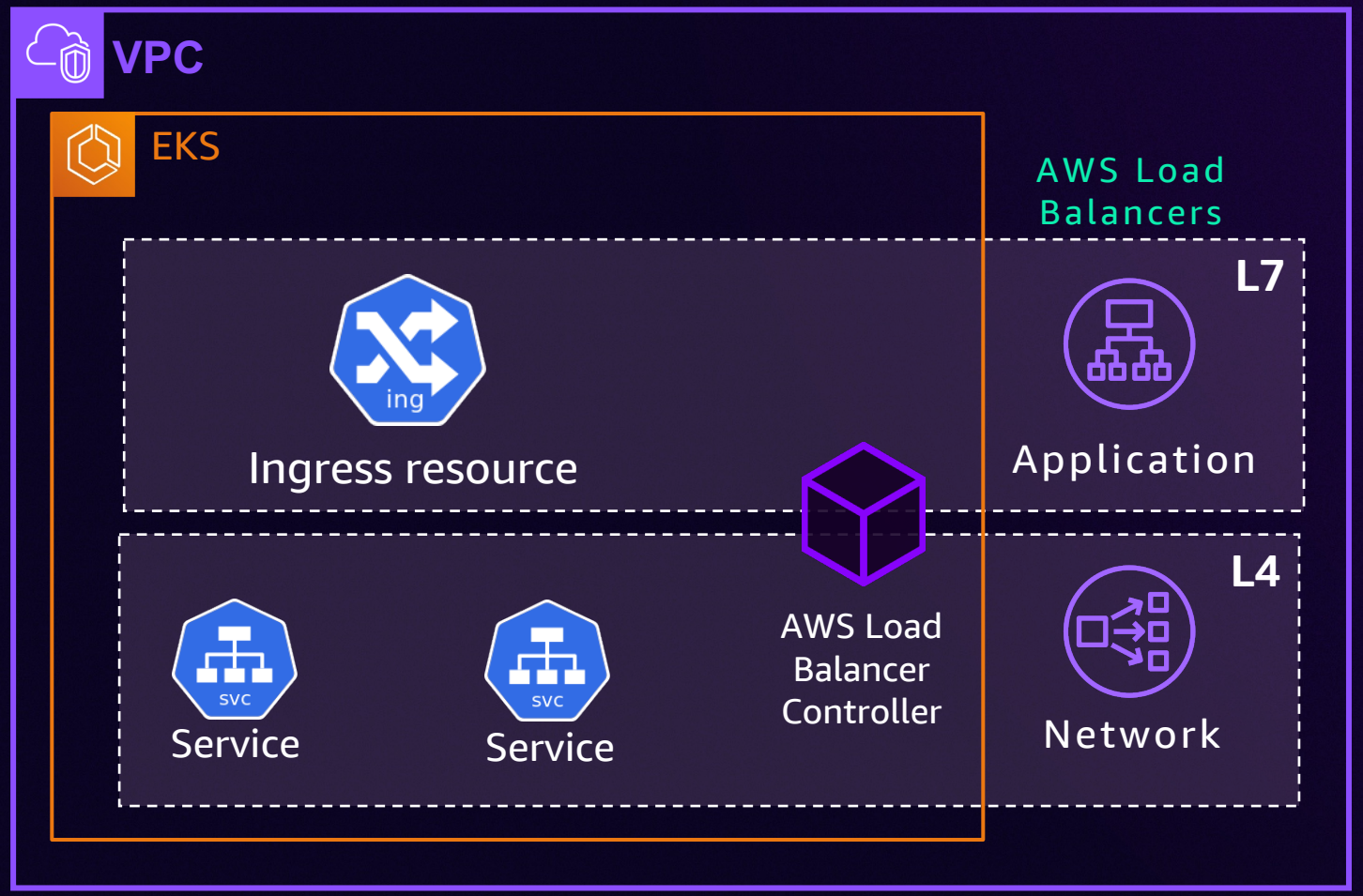


Application Layer

Transport/Network Layer

Inbound traffic

AWS LOAD BALANCER CONTROLLER

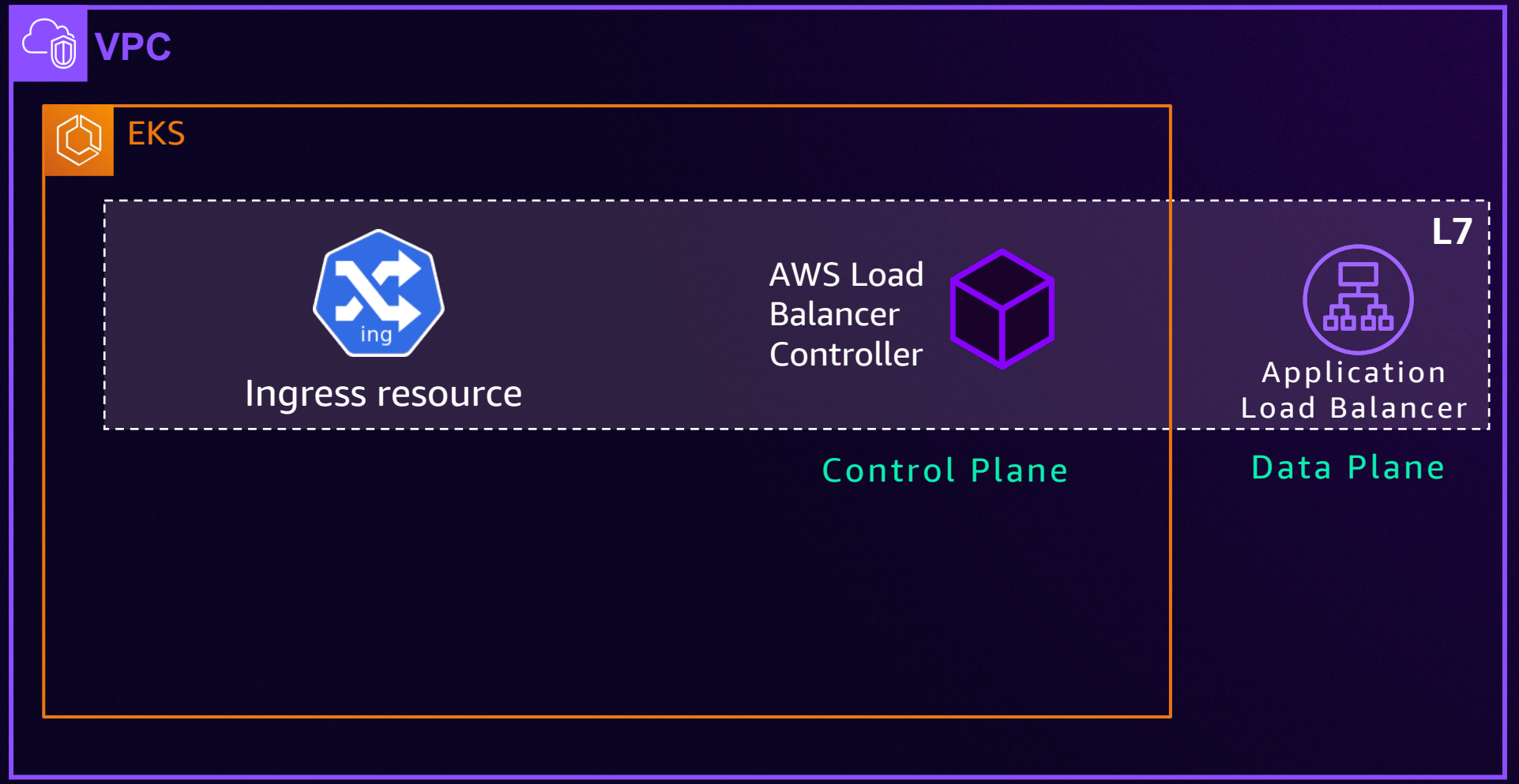


HOW IT WORKS

- ✓ It satisfies ingress resources by provisioning Application Load Balancers (ALB)
- ✓ It satisfies service resources by provisioning Network Load Balancers (NLB)
- ✓ Supported in Automode!

Inbound traffic

AWS LOAD BALANCER CONTROLLER

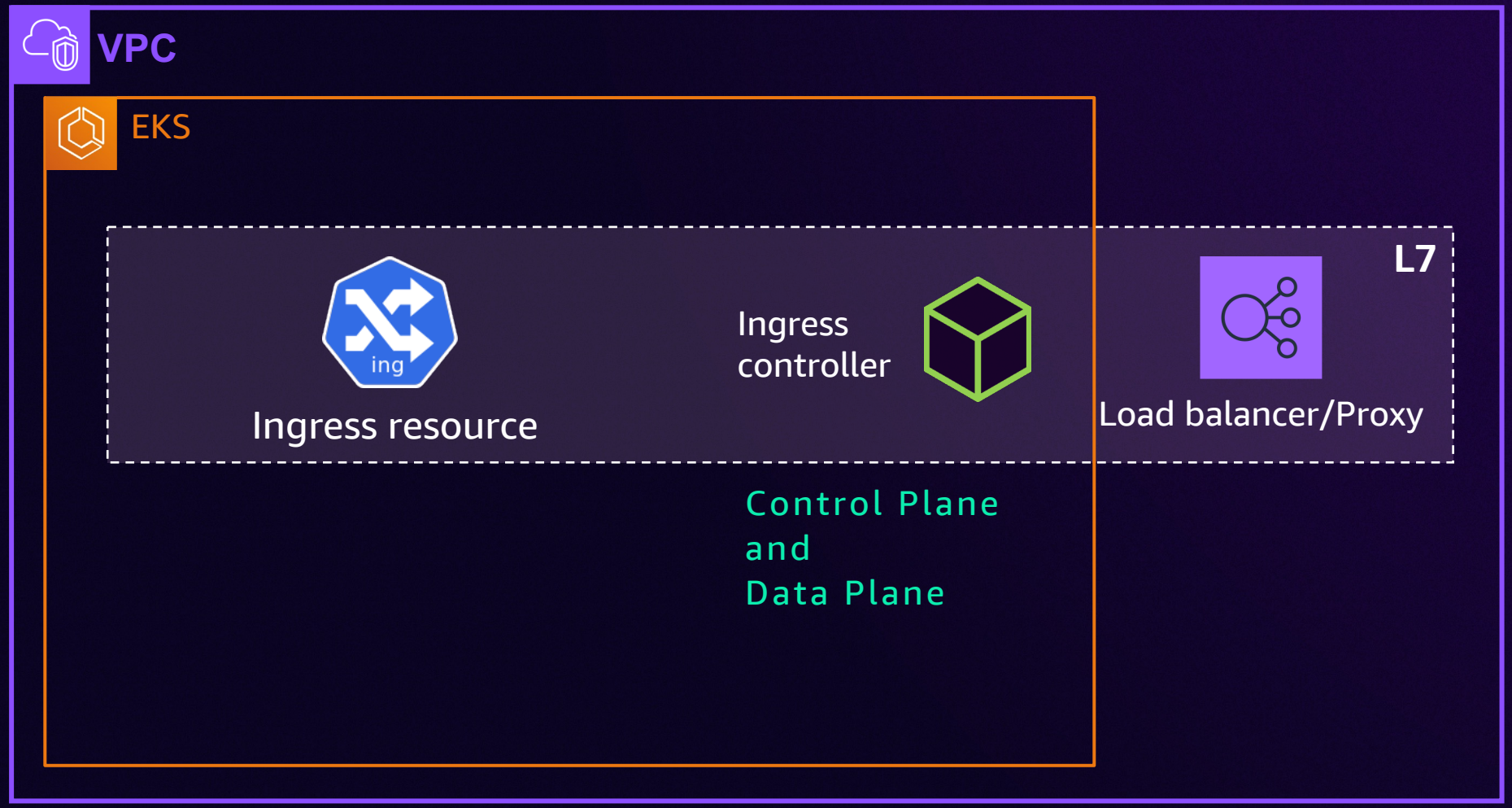


APPLICATION LOAD BALANCER INTEGRATIONS

- AWS Certificate Manager (ACM)
- AWS WAF
- Amazon CloudFront
- Amazon Route 53 Application Recovery Controller (ARC)
- AWS Global Accelerator

Inbound traffic

THIRD-PARTY INGRESS CONTROLLERS



IMPLEMENTATIONS

Nginx

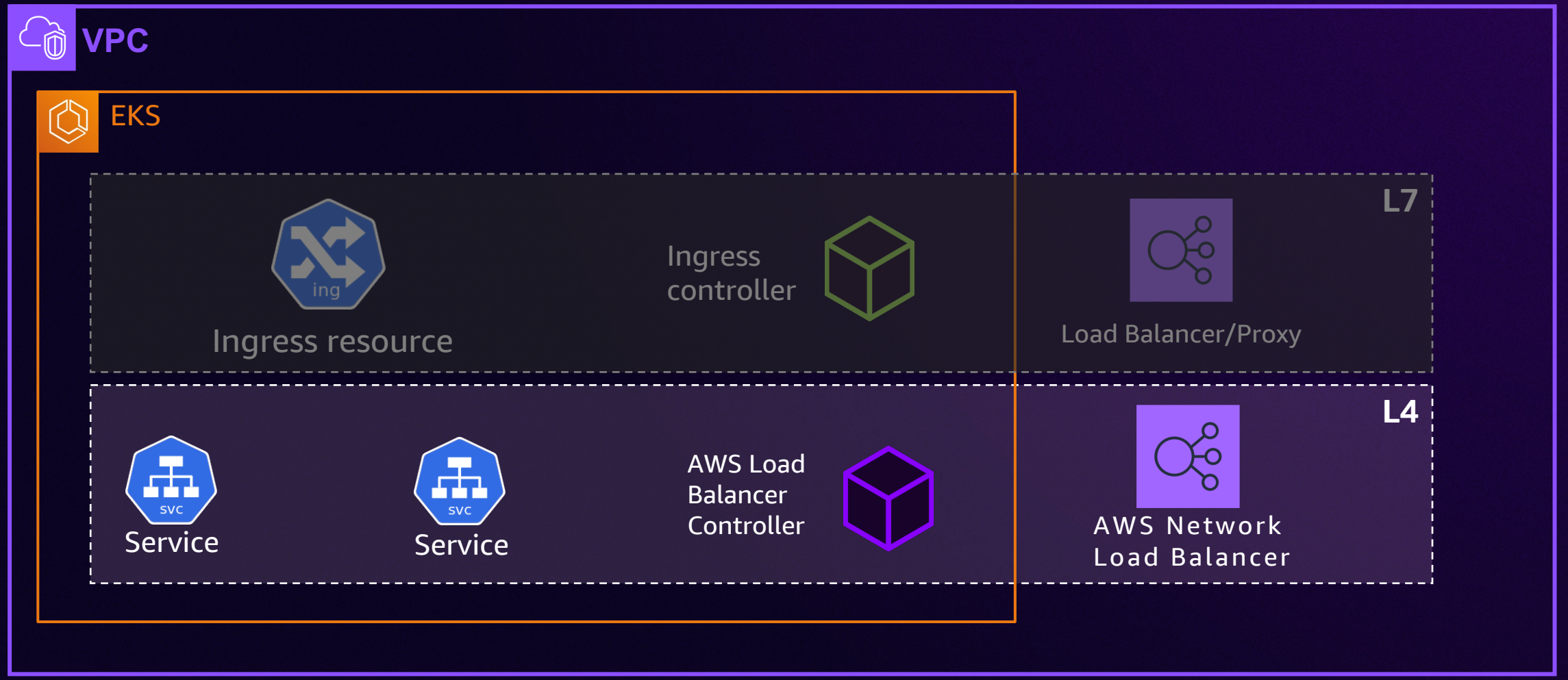
HAProxy

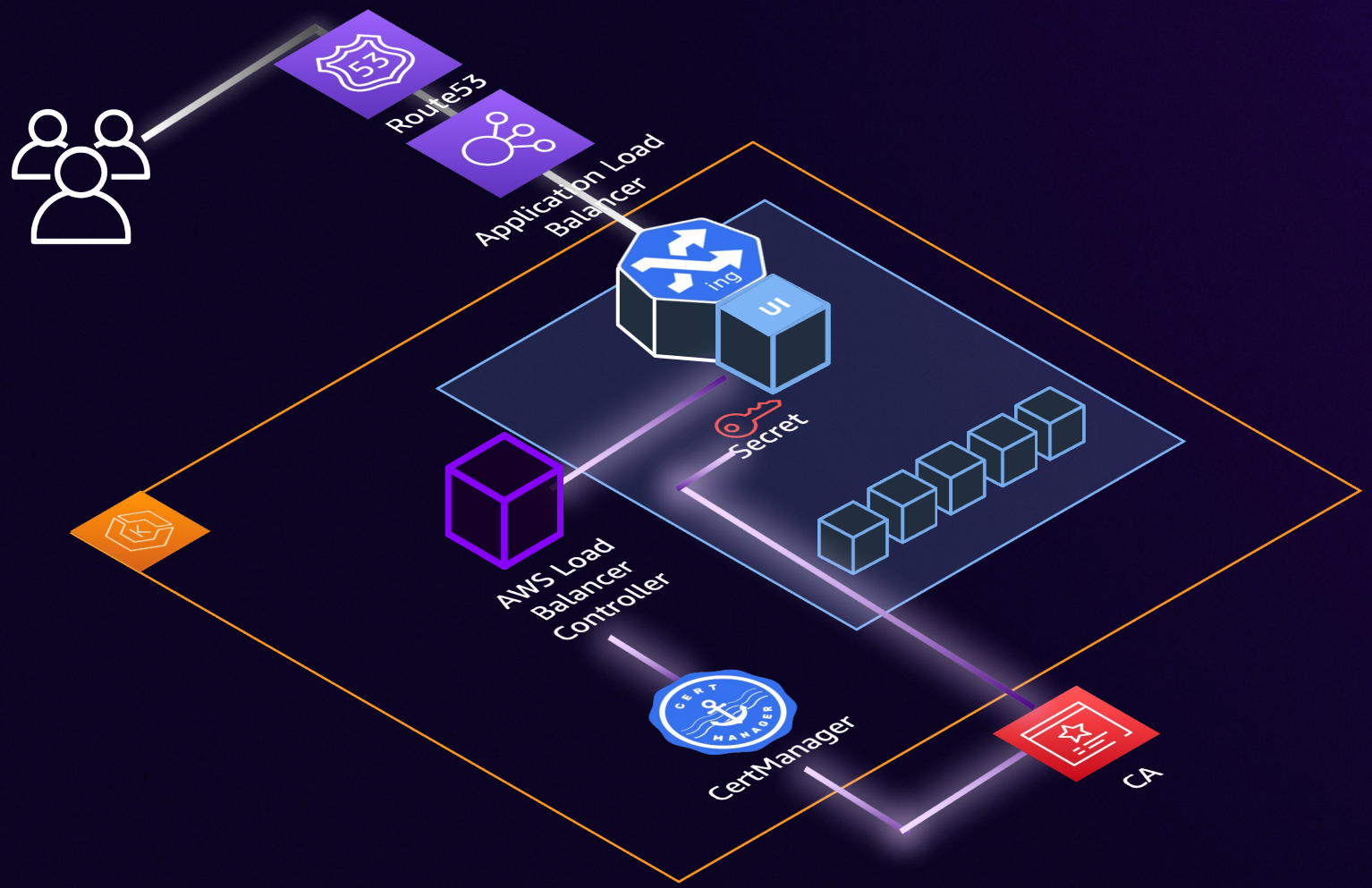
Istio

...and many more!

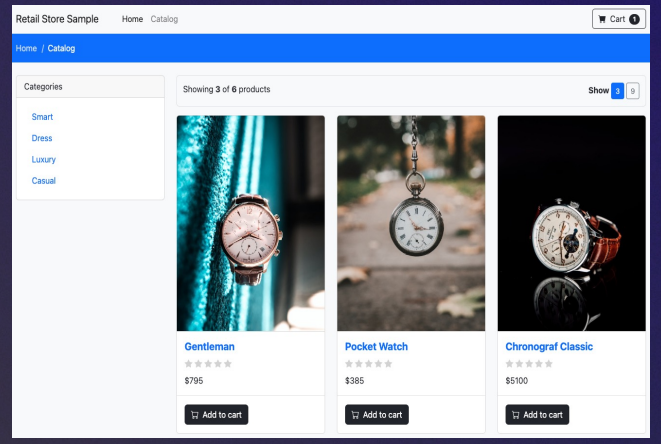
Inbound traffic

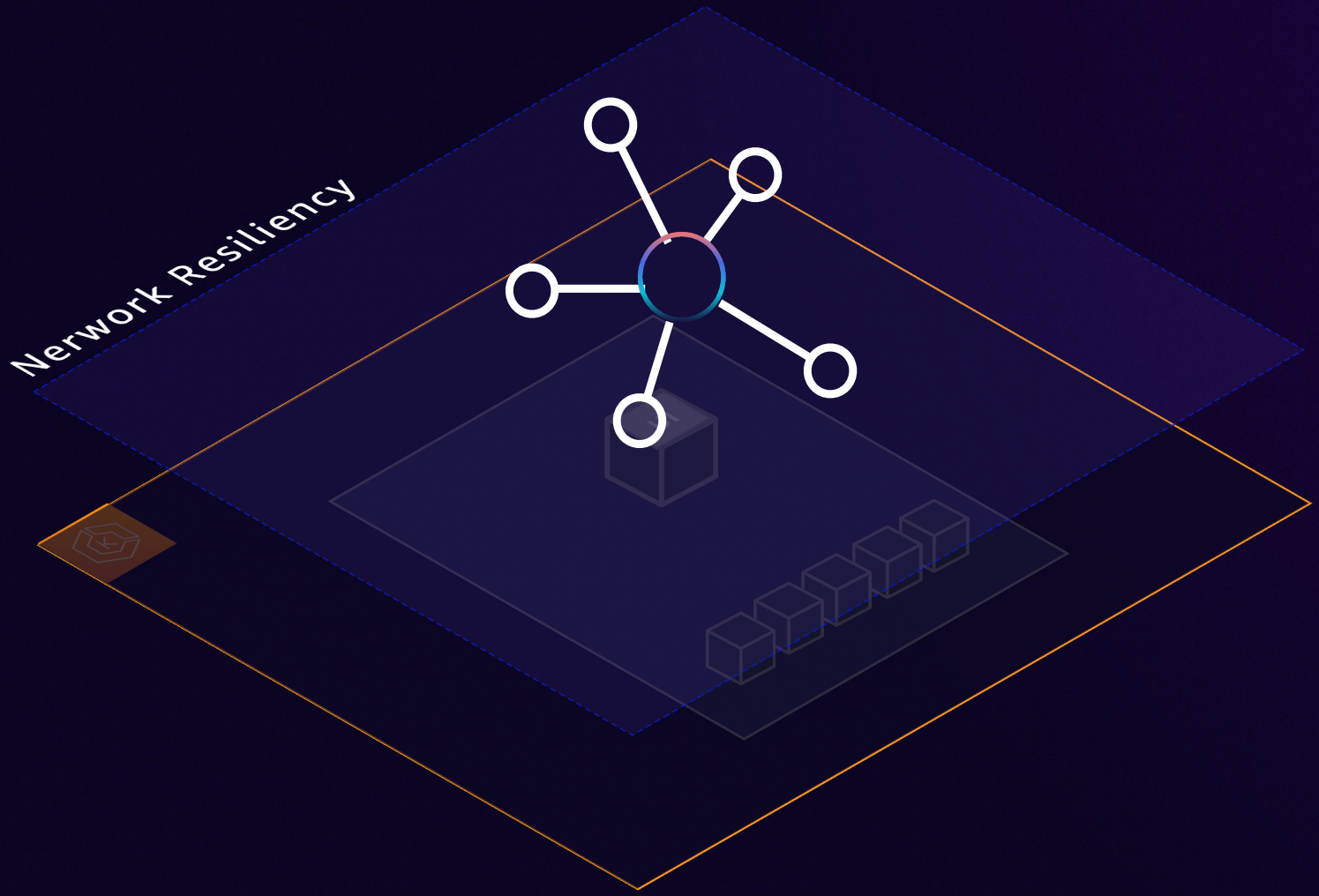
SERVICE CONTROLLERS WITH THIRD-PARTY INGRESS CONTROLLERS





- Simplify cluster operations
- Enable external access to application

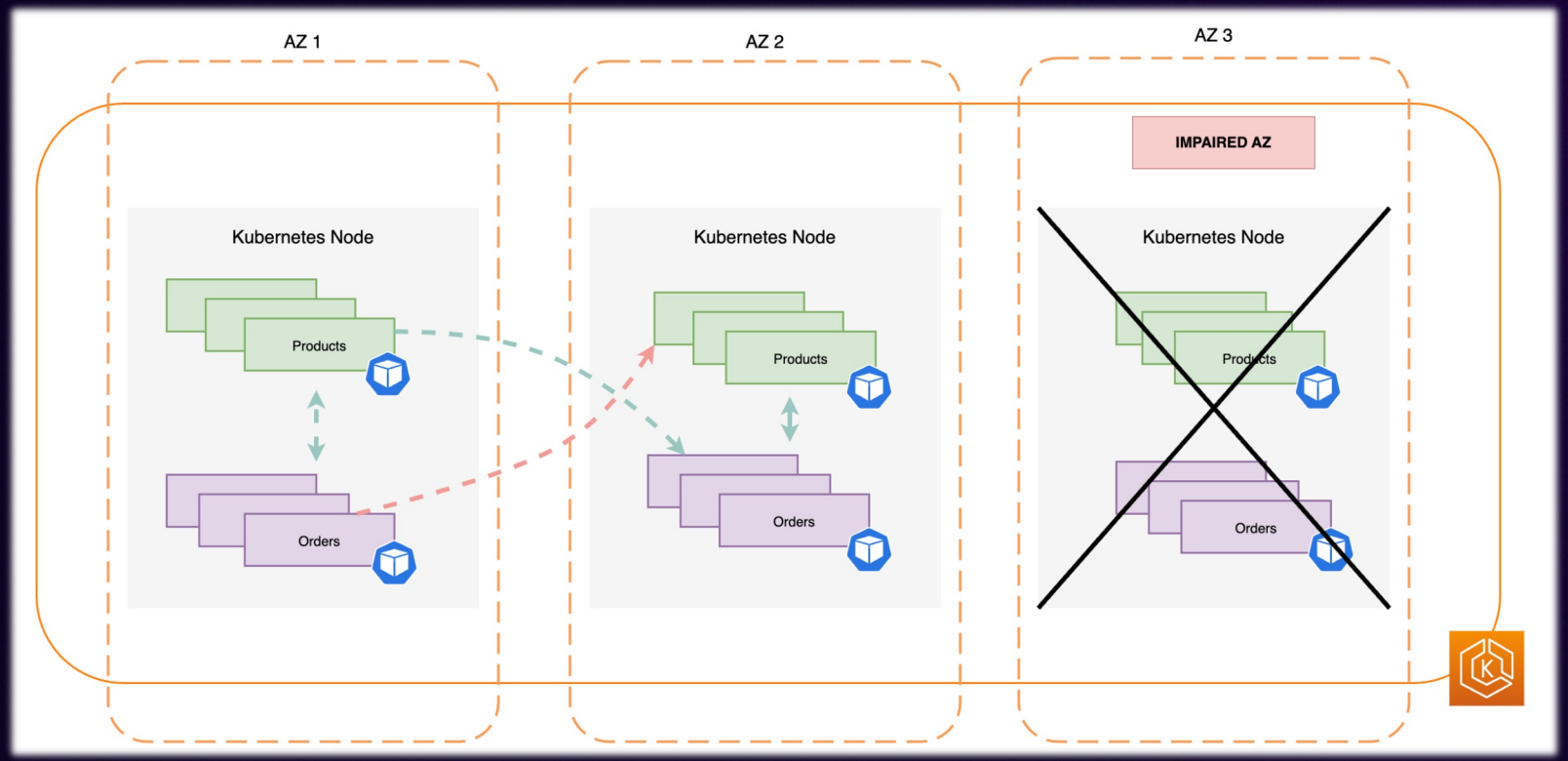




- Simplify cluster operations
- Enable external access to application
- Improve network resiliency

Enhanced High Availability

AMAZON RECOVERY CONTROLLER (ARC) INTEGRATION



BENEFITS

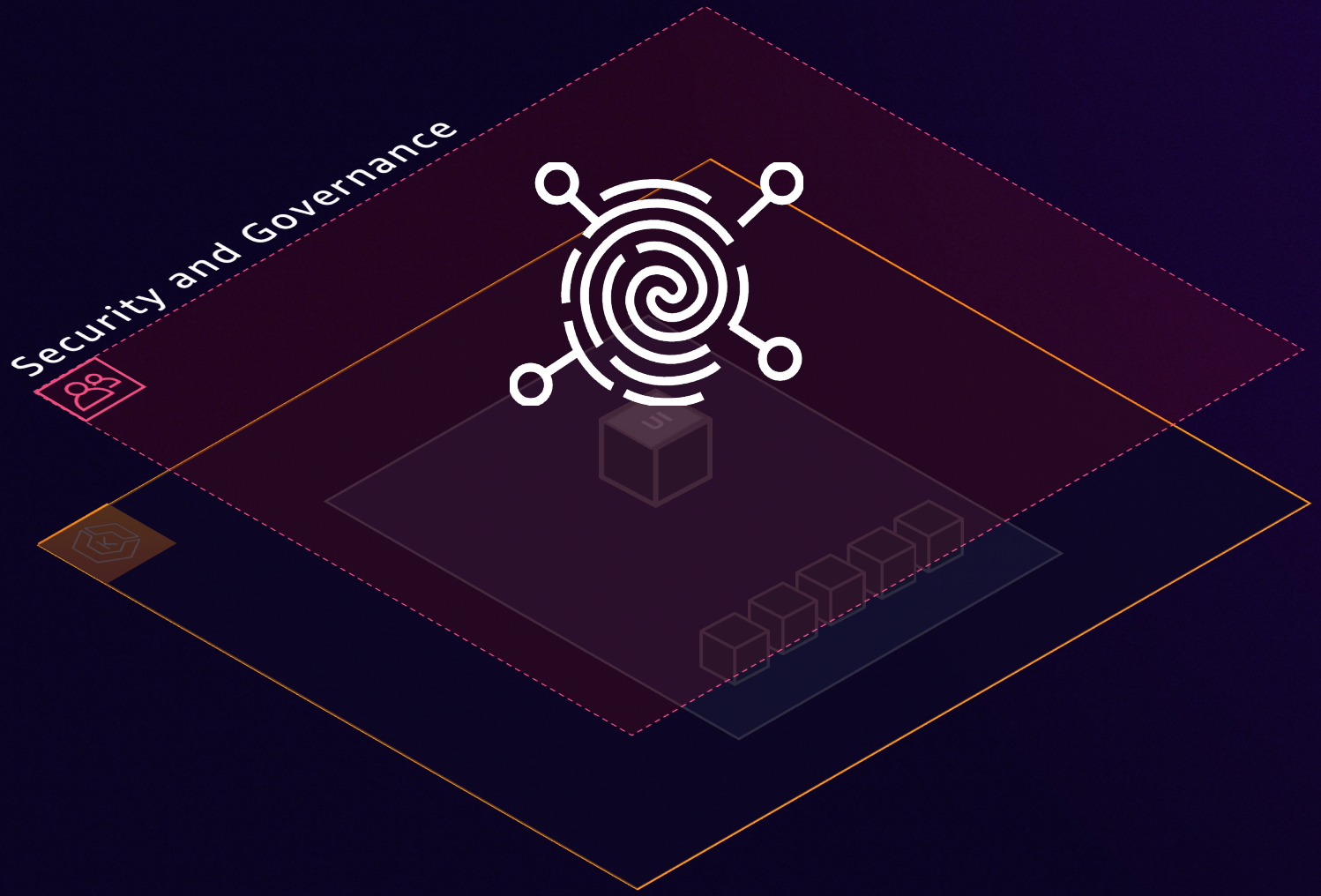
- ✓ Improved Resiliency
  Enables fast fail away from impaired AZs
- ✓ Simplifies Operations
  with Zonal Auto Shift

HOW IT WORKS

- ✓ Traffic will not be sent to affected pods
- ✓ Manual and Automatic options

LIMITATIONS

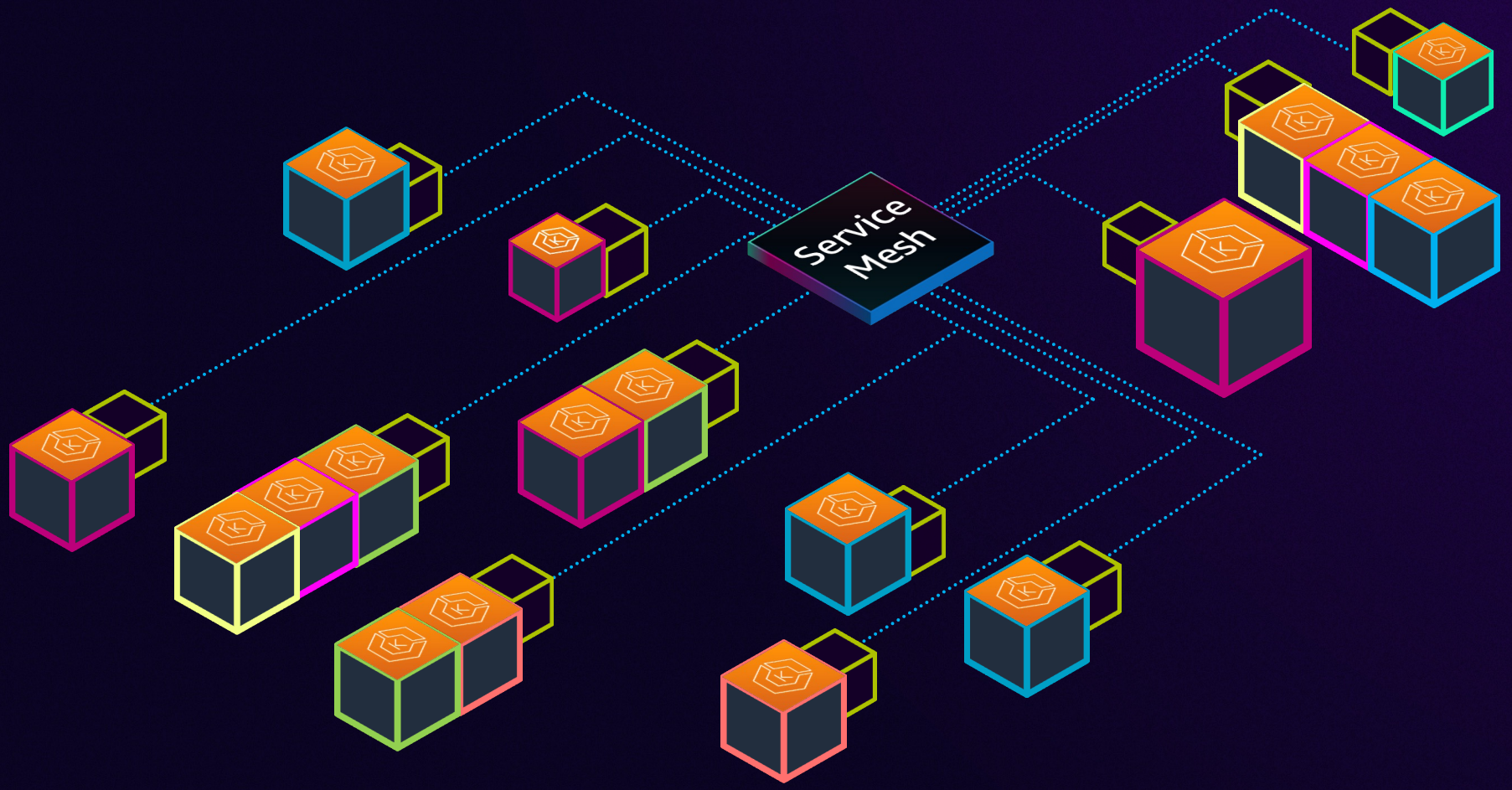
- ✓ Workload Architecture specific



- Simplify cluster operations
- Enable external access to application
- Improve network resiliency
- Monitor performance and secure communication

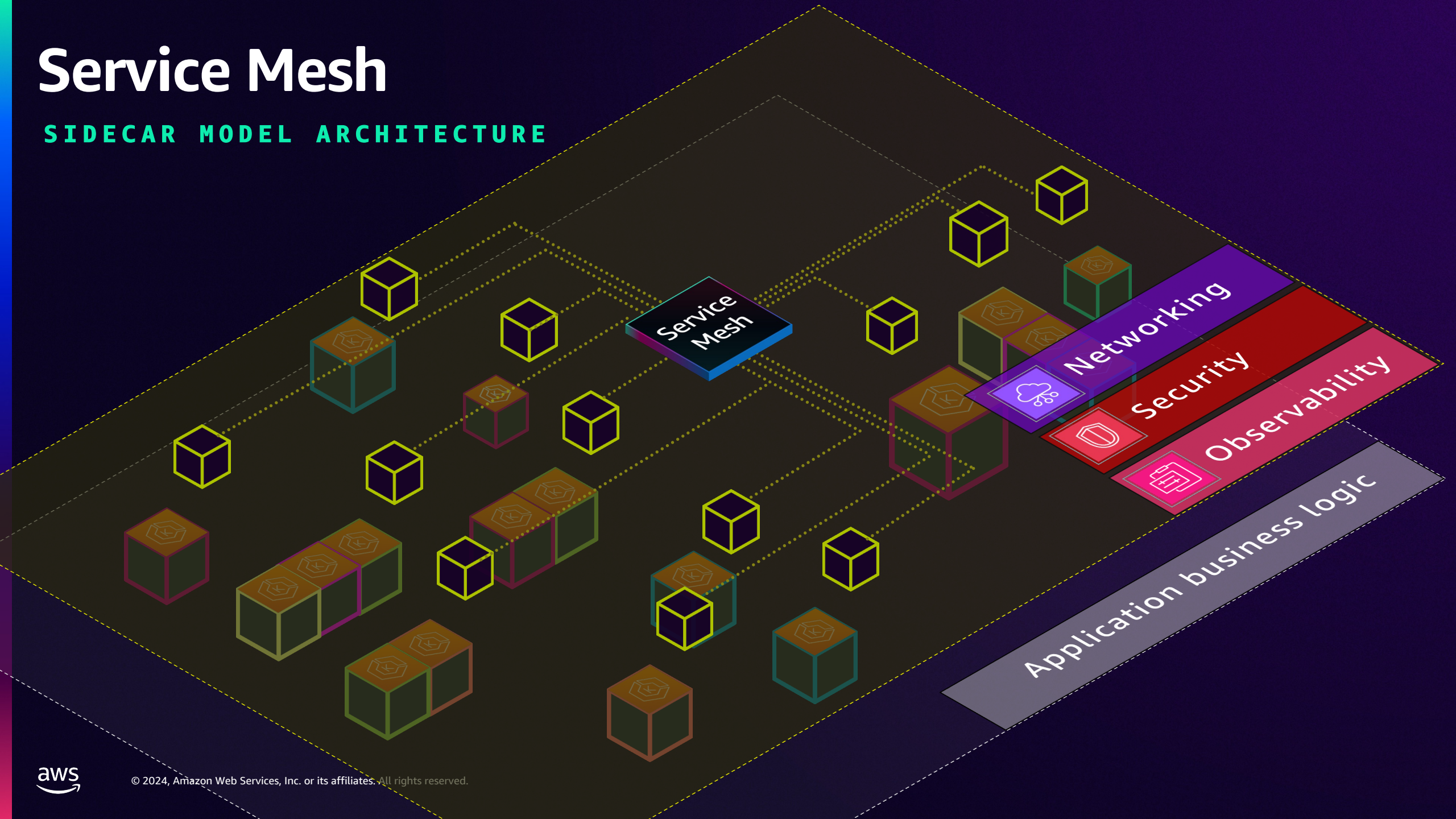
Service Mesh

SIDECAR MODEL ARCHITECTURE



Service Mesh

SIDECAR MODEL ARCHITECTURE



Service Mesh

USE CASES

Networking

✓ **Advanced traffic routing**

Granular traffic routing and weighting for Blue/Green or Canary releases.

✓ **Increased Network Reliability**

Protect applications from traffic spikes to maintain service levels.

✓ **Cluster Federation**

Connect and federate services across clusters.

Security

✓ **Allow and deny communications**

Create an allow list for internal and external services.

✓ **Encrypt communications**

Encrypt all communication without burdening application teams.

✓ **Authentication and Authorization**

Ensure all services have identities for secure access.

Observability

✓ **Uniform network logging**

The proxy provides a uniform way to observe service-to-service communications.

✓ **Tracing**

Understand end-to-end traffic flows without modifying application code.

Service Mesh

USE CASES AND CHALLENGES

Networking

- ✓ Advanced traffic routing
- ✓ Increased Network Reliability
- ✓ Cluster Federation

Security

- ✓ Allow and deny communications
- ✓ Encrypt communications
- ✓ Authentication and Authorization

Observability

- ✓ Uniform network logging
- ✓ Tracing

Challenges

Engineering effort

Sidecars add complexity to pod specs and require proxy management (patch, upgrade)

Resource inefficiency

Sidecars can waste resources when underutilized

Security Boundaries

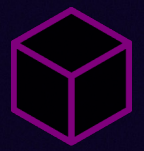
Complexity of multi-tenant management

Traffic Disruptions

Sidecar-based traffic capture can be challenging for legacy apps

Istio Ambient Mesh

A LAYERED APPROACH



ZTUNNEL PROXY (L4)

SECURE OVERLAY

Takes care of routing and ensuring zero-trust security for traffic.

- Per node Proxy: runs as Daemonset
- Manages identity, mTLS and L4 authorizations
- Written in Rust

WAYPOINT PROXY (L7)

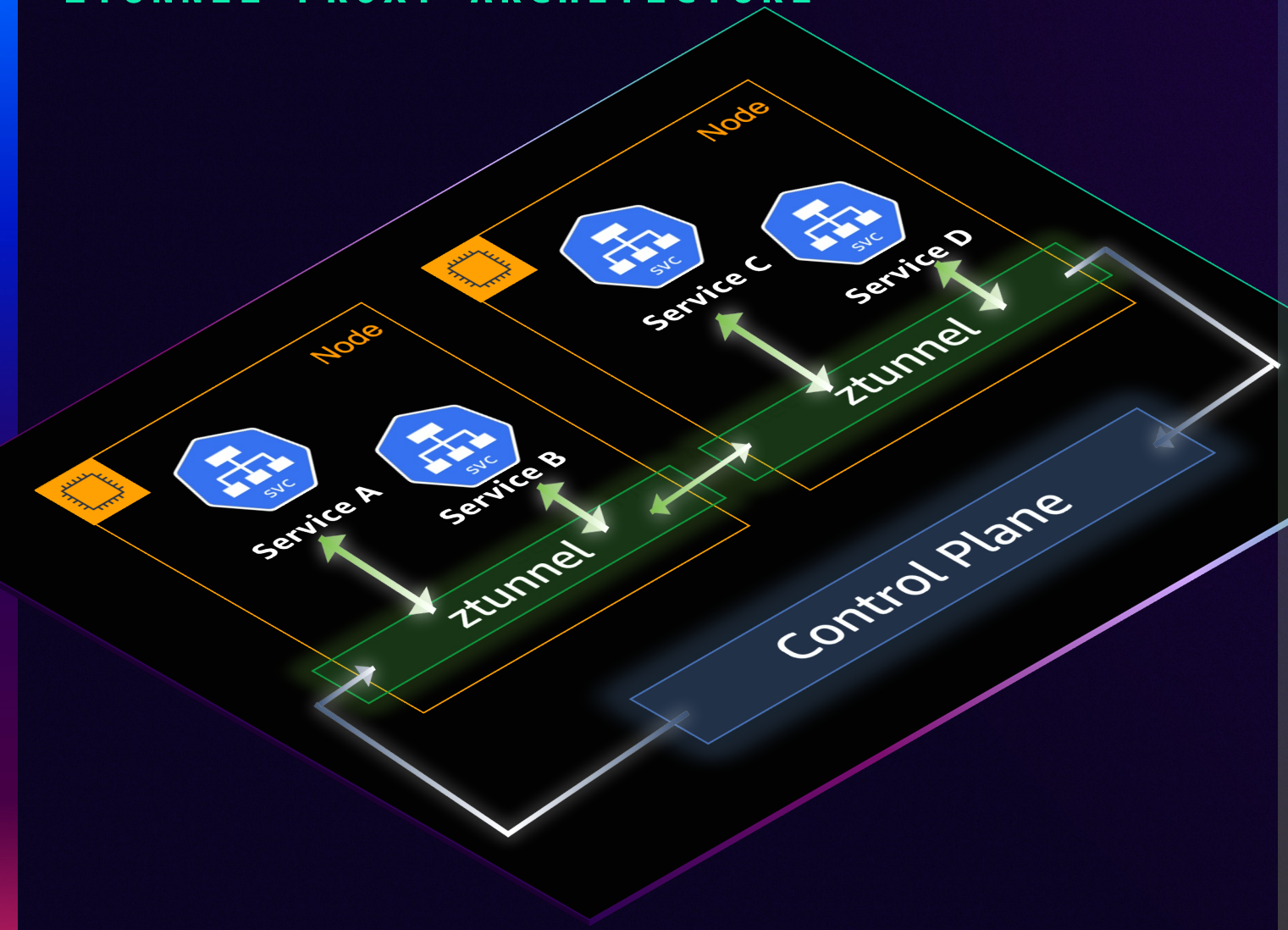
L7 CAPABILITIES

Users can enable L7 processing when they need access to Istio's extensive features, without altering the application pods.

- Per identity Proxy: runs on a per-namespace or per-service account basis and handles all traffic entering that namespace.
- Manages L7 operations (path based routing, retries, timeouts, …)
- Envoy

Istio Ambient Mesh

ZTUNNEL PROXY ARCHITECTURE



HOW IT WORKS

Only L4 traffic

Ztunnel processes only L4 traffic, separating Istio's data plane from the application logic.

Shared Agent

A shared agent (ztunnel) is present on each node in the Kubernetes cluster, responsible for secure connections within the mesh.

Zero-trust

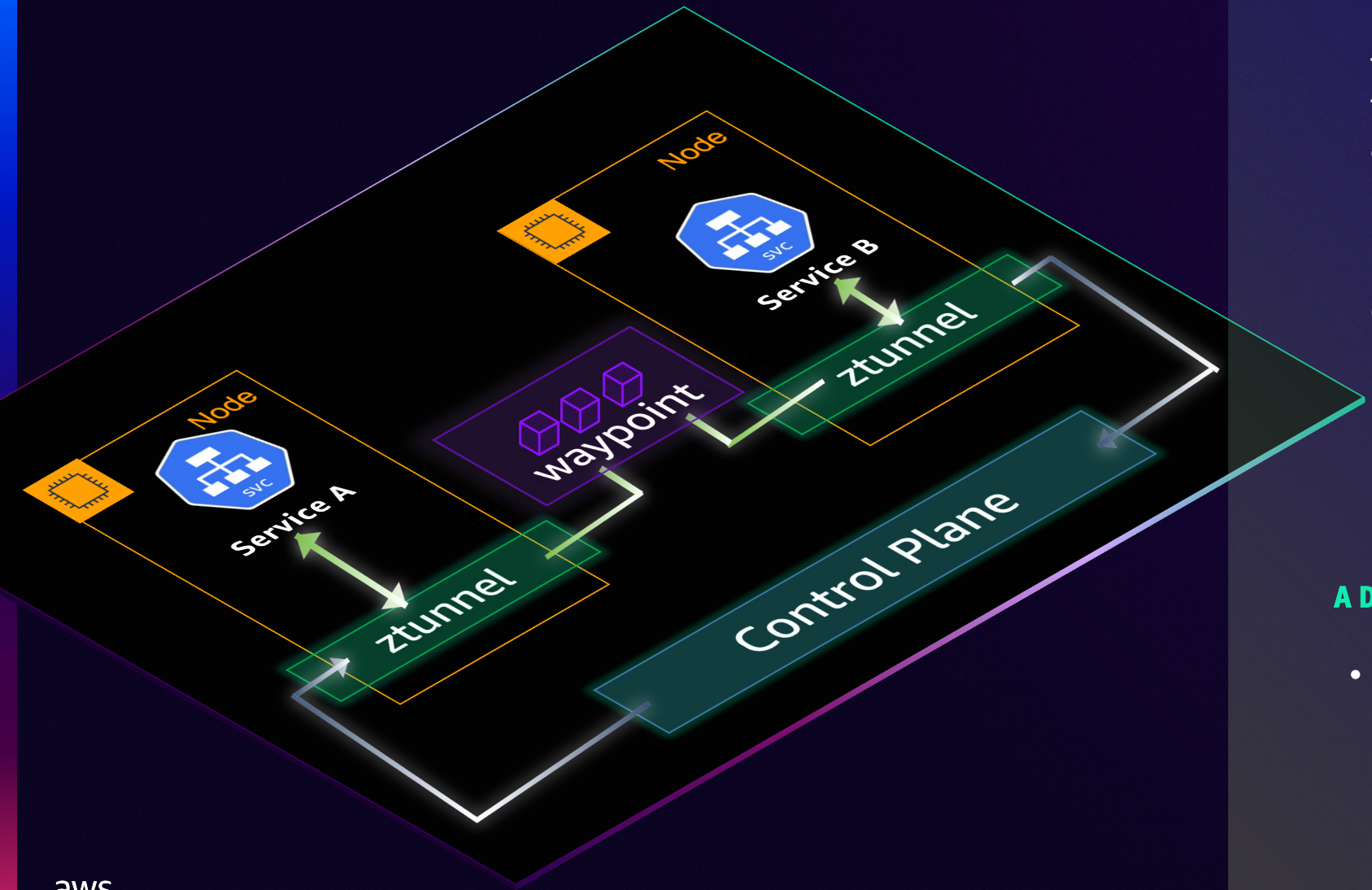
A zero-trust overlay (with mTLS, telemetry, authentication, and L4 authorization) is established when the ambient mode is activated for a namespace.

ADVANTAGES

- Lower resource utilization
- Lower operational complexity
- mTLS between nodes out of the box

Istio Ambient Mesh

WAYPOINT PROXY ARCHITECTURE



HOW IT WORKS

Only L7 traffic

Users can enable L7 processing when they need access to Istio's extensive features, all while not altering the application pods.

Identity based

For L7 features, a namespace can deploy one or more Envoy-based waypoint proxies.

Autoscaling

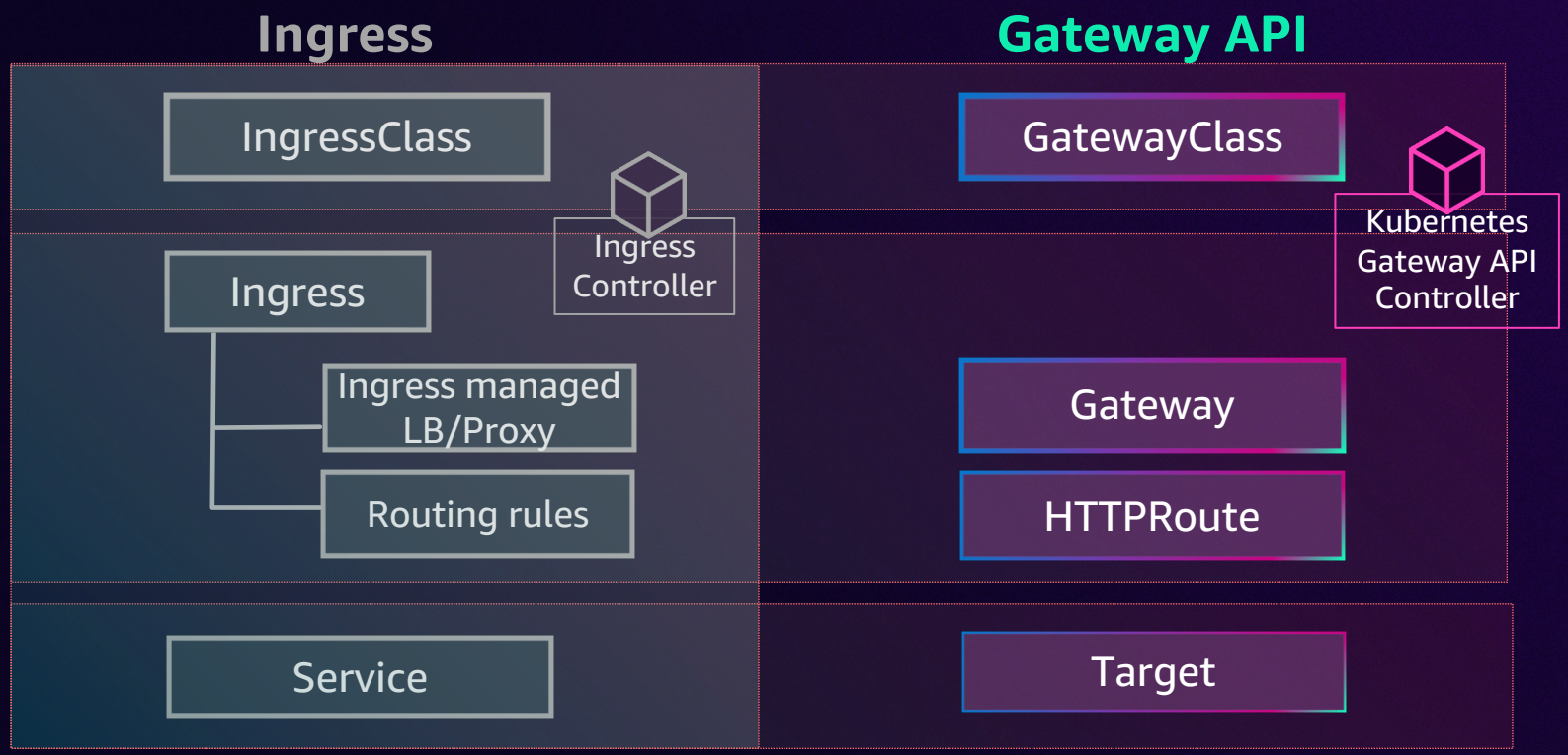
Proxies can be auto-scaled according to real-time traffic demand.

ADVANTAGES

- L7 traffic management complexity confined to workloads that require it.

Kubernetes Gateway API

API OVERVIEW



Limited API

Lack of advanced networking features

Proprietary annotations and CRDs

Lessons learned from Ingress API and service meshes

Expressive API

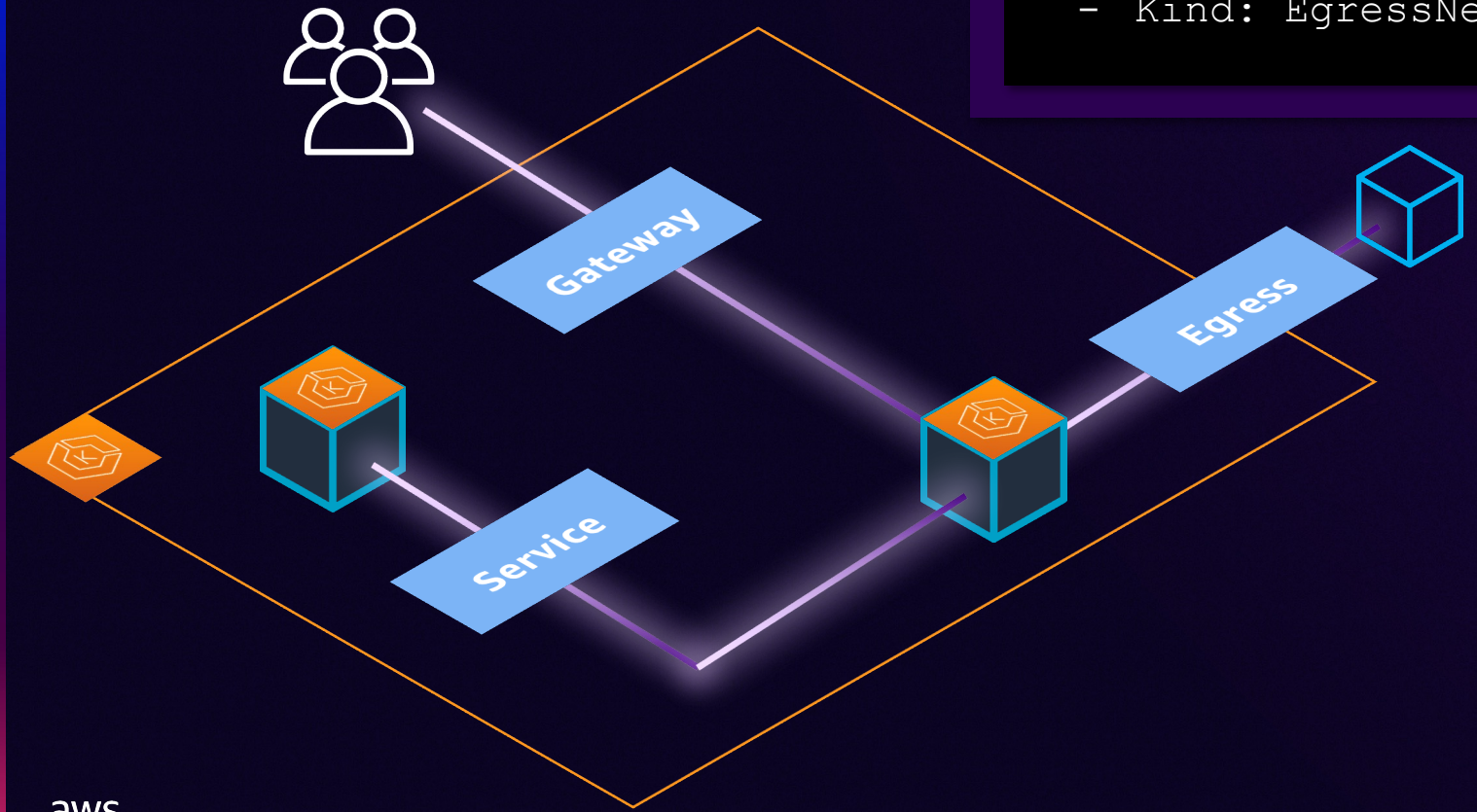
Advanced networking features are built in the k8s API

Kubernetes Gateway API

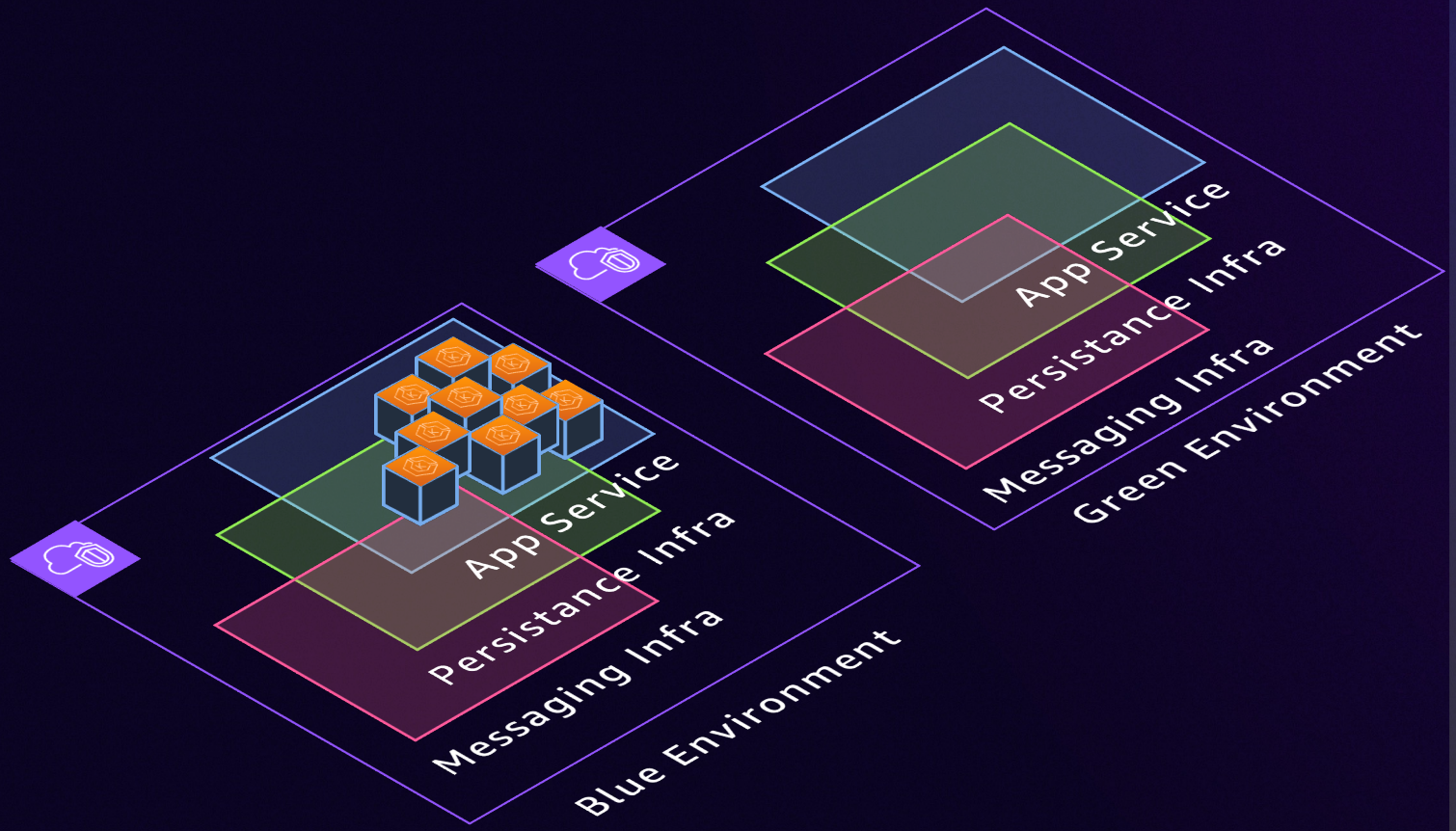
API FLEXIBILITY

Httproute.yaml

```
parentRefs:
  - Kind: Gateway
  - Kind: Service
  - Kind: EgressNetwork
```



- ✓ Ingress Traffic
- ✓ Service to service (Gamma Initiative)
- ✓ Egress Traffic

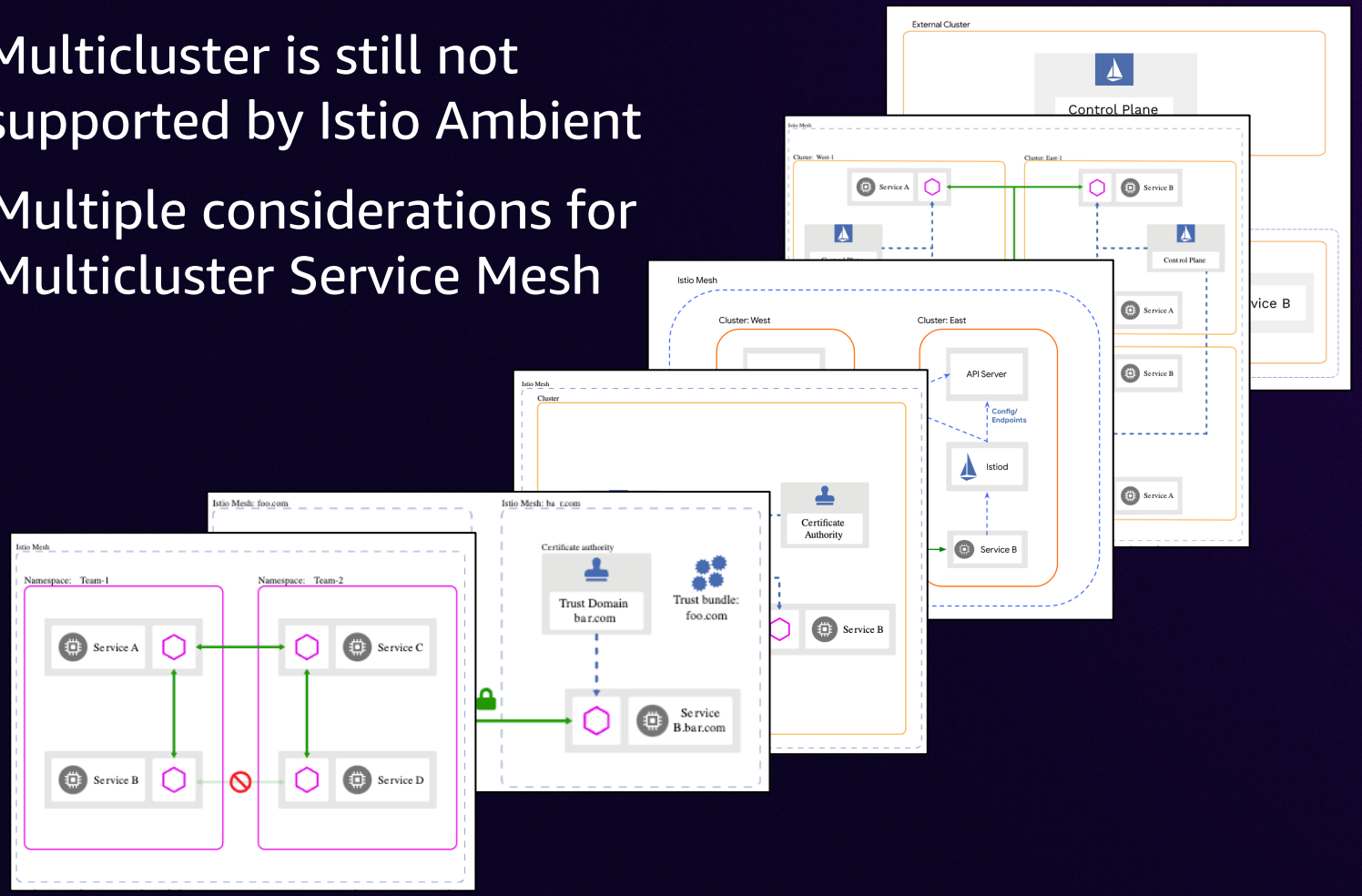


- Simplify cluster operations
- Enable external access to application
- Improve network resiliency
- Monitor performance and secure communication
- Mitigate deployment risk with Blue-Green strategies

Network connectivity and federation

CHALLENGES WITH THE CURRENT IMPLEMENTATION

- Multicluster is still not supported by Istio Ambient
- Multiple considerations for Multicluster Service Mesh



Source: https://istio.io/latest/docs/ops/deployment/deployment-models/

External Control Plane control plane and HA

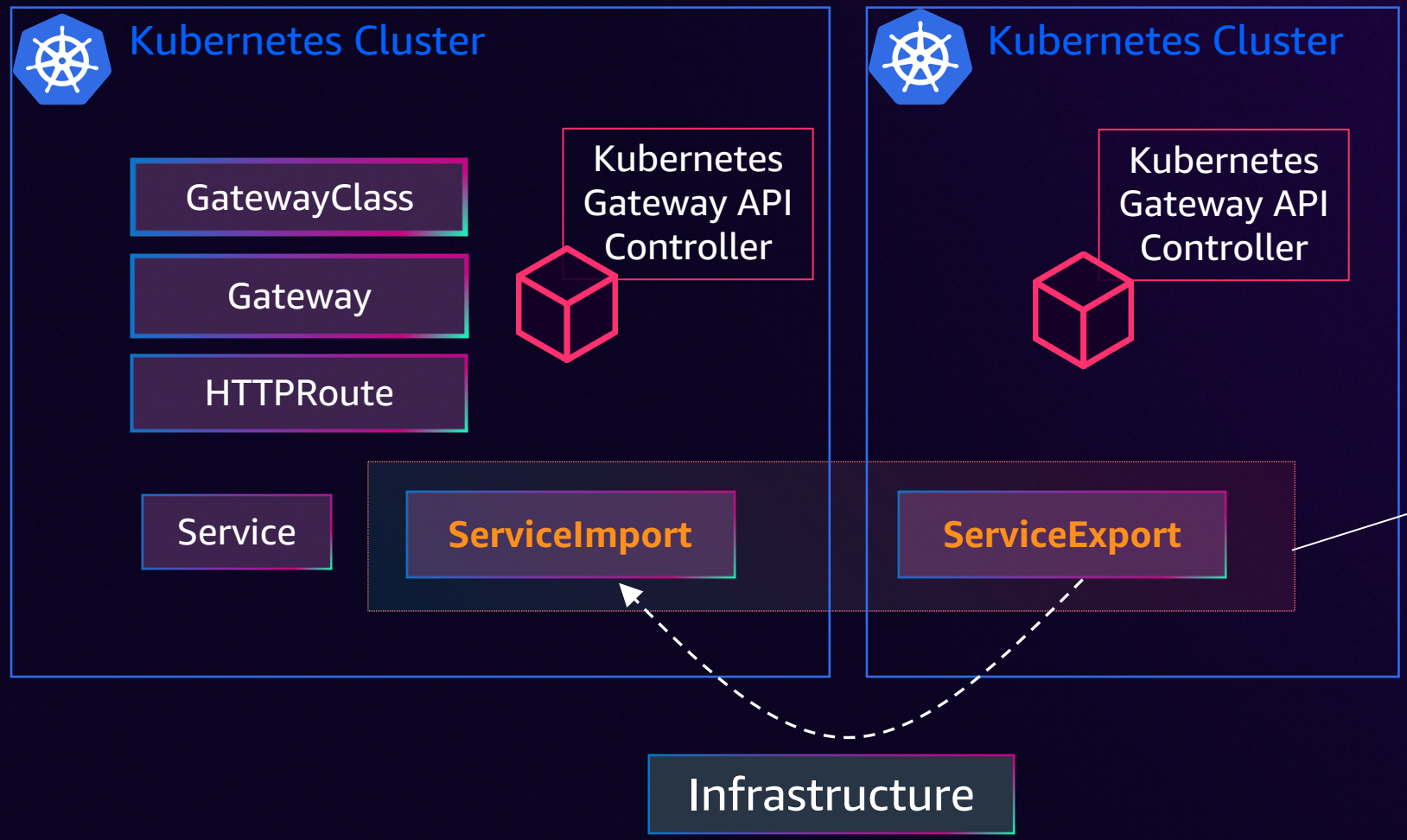
API Permissions

Encryption and tenancy Boundaries

Trust between meshes

Kubernetes Gateway API

AND MULTICLUSTER SERVICES

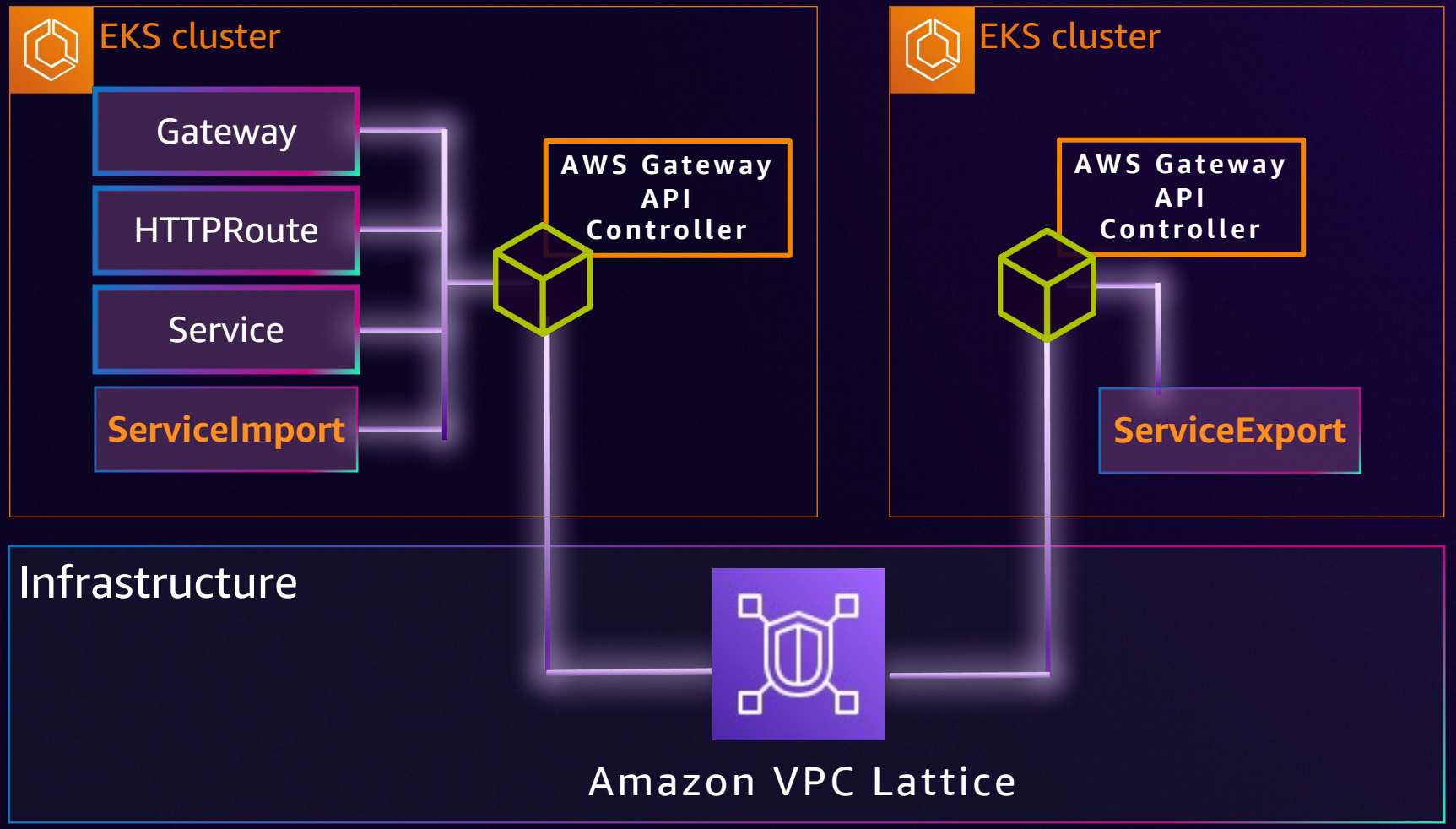


Multicluster services API

Traffic can be routed to Targets outside the cluster!

Kubernetes Gateway API

AWS INTEGRATION

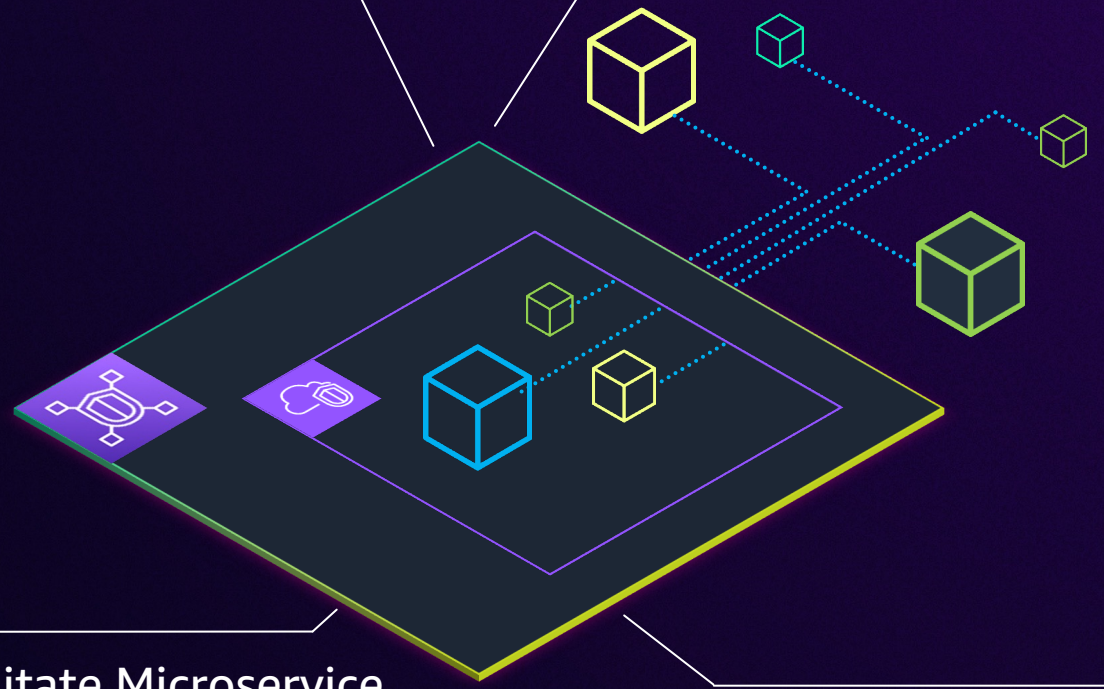


AWS Gateway API Controller for Amazon VPC Lattice

Amazon VPC Lattice

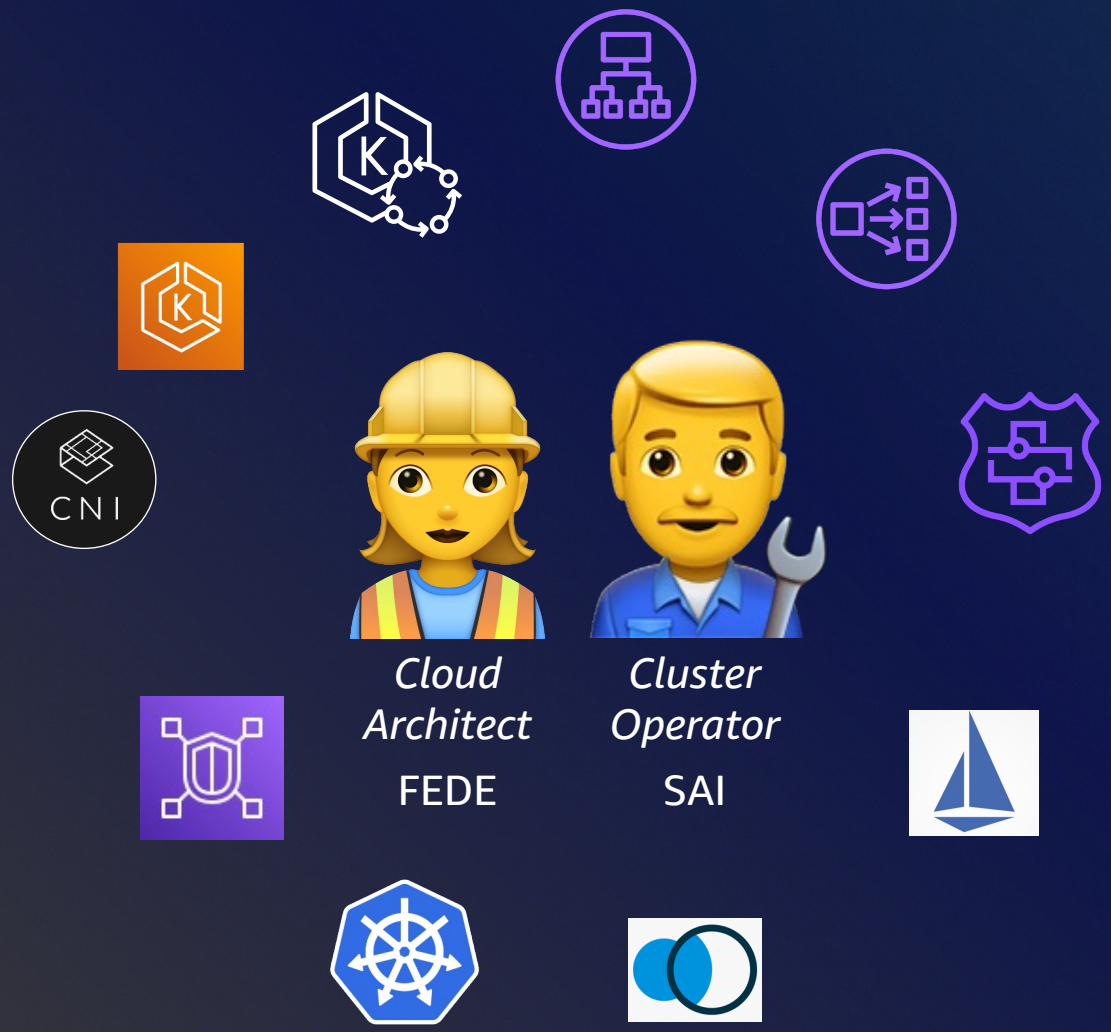
Network Service that adds L7 features to Amazon VPC

AWS Identity and Access Management (IAM) identity and access policies for Zero Trust architectures



Facilitate Microservice Communication across compute options

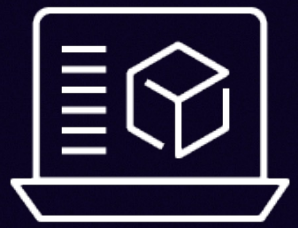
Connects applications across VPCs and Accounts without the need to set up Transit Gateway, Peering (etc.)



- Simplify cluster operations
- Enable external access to application
- Improve network resiliency
- Monitor performance and secure communication
- Mitigate deployment risk with Blue-Green strategies

Continue your Amazon EKS learning

Learn at your own pace



Take the **Amazon EKS Workshop** to expand your EKS skills

Increase your knowledge

Use our **Best Practices Guide** to build your Kubernetes knowledge

Earn Amazon EKS badge

Demonstrate your knowledge by achieving **digital badges**

https://github.com/aws-samples/reinvent24

Thank you!

Please complete the session survey in the mobile app

Federica Ciuffo

Scan this QR for my socials!

Sai Vennam

linkedin.com/in/saivennam/

x.com/birdsaiview