cisco Live!

Let's go

The bridge to possible

Explore complexities and best practices for deploying applications in multi cluster service mesh

Sundar Srinivasaraghavan – Principal Architect
Ravi Jandyala – Product Management Architect

BRKCLD-2019

Cisco Webex App

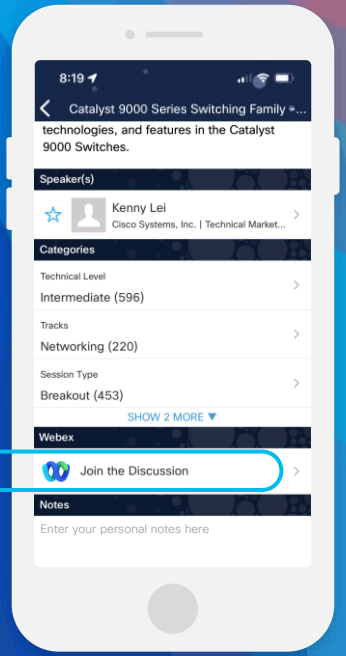
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



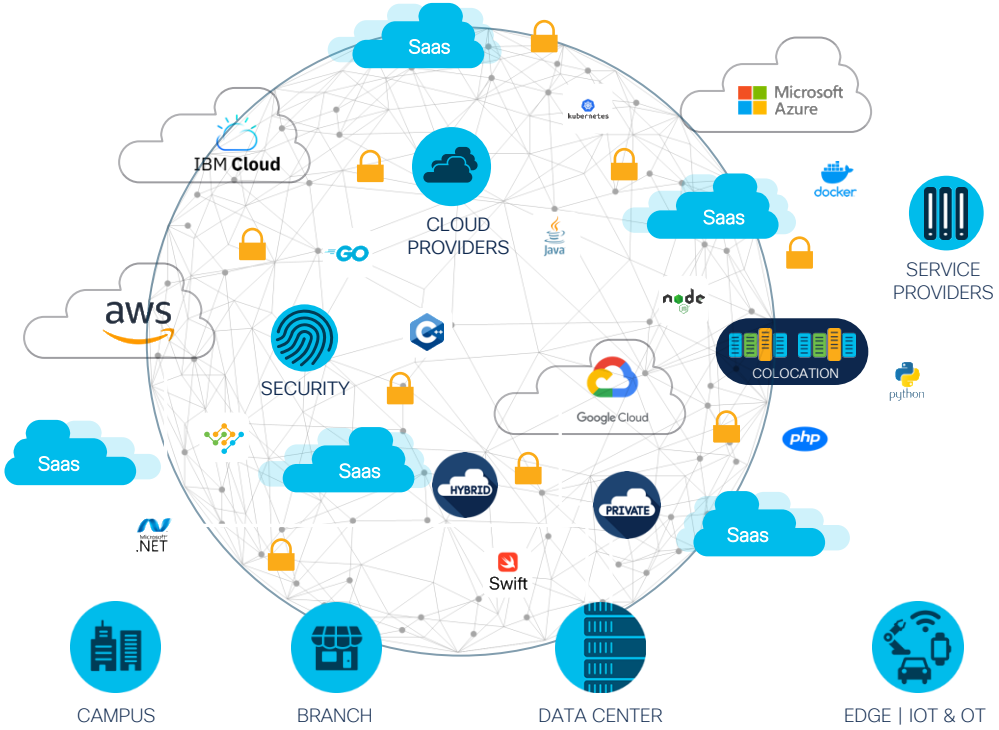
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCLD-2019

Agenda

- Introduction
- Service Mesh Deployment Models
- Service Mesh Deployment Challenges
- Introducing Cisco Calisti
- Demo
- Conclusion

Introduction

The new normal is a hyper-distributed, extremely diverse IT landscape…



...with hybrid cloud complexity beyond human scale.

Visibility across clouds, users, apps and data

Deploy and manage service mesh

Deploy and configure infrastructure on public clouds and DC

Monitor app performance

Right-size and optimize for performance and cost

Manage apps across bare metal, VMs and containers

Replicate operating model for individual clouds

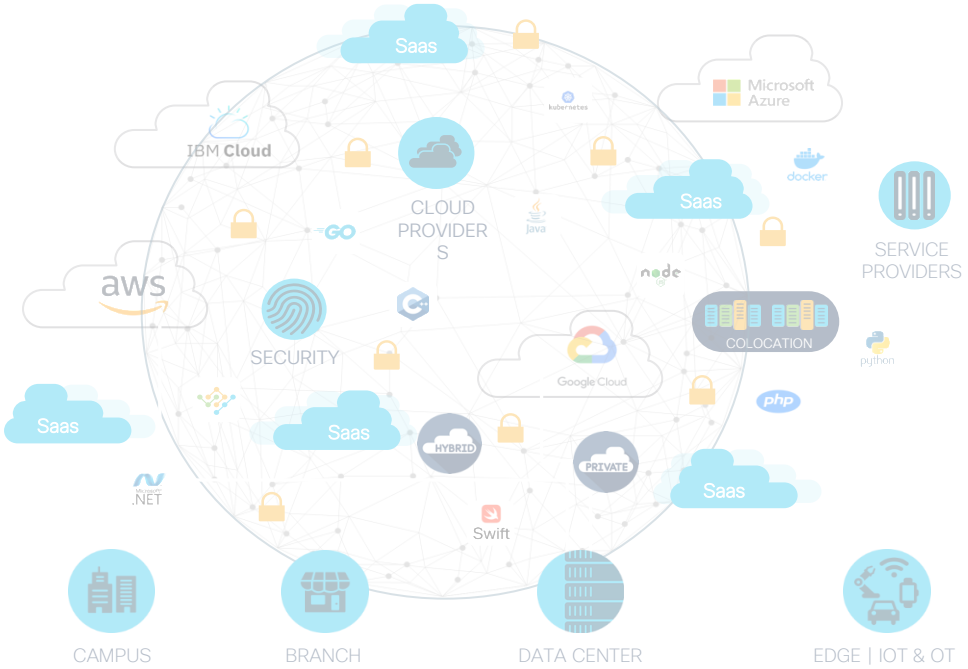
Configure and segment networks and devices

Enforce policies for governance

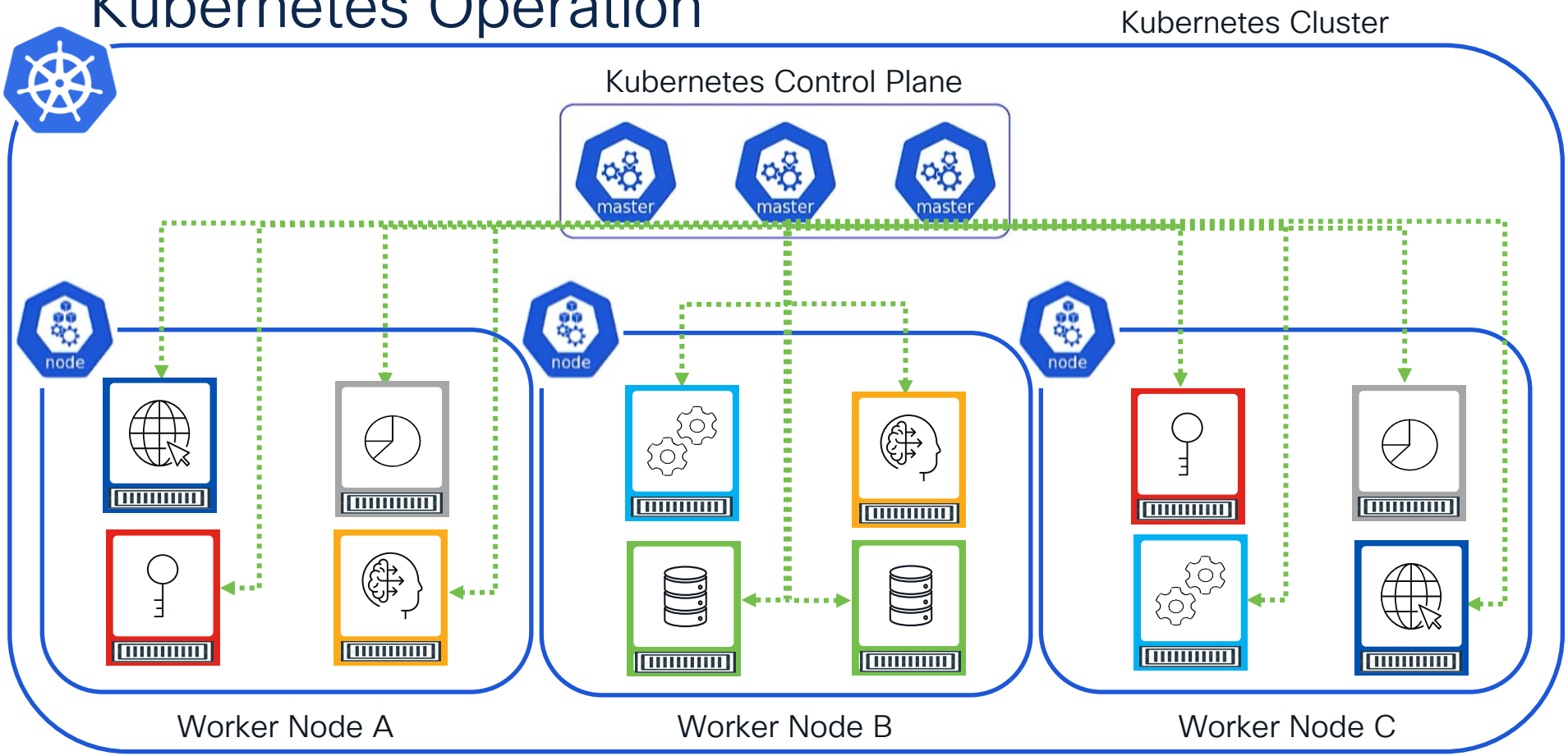
Integrate and automate infra with CI/CD tools

Map app dependencies

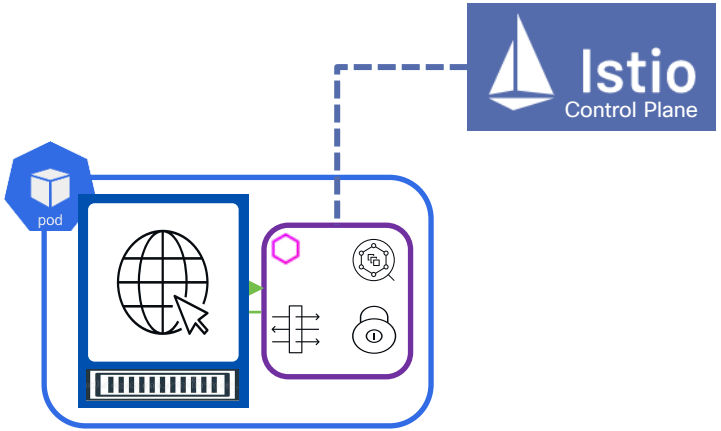
Connect to legacy systems



Kubernetes Operation

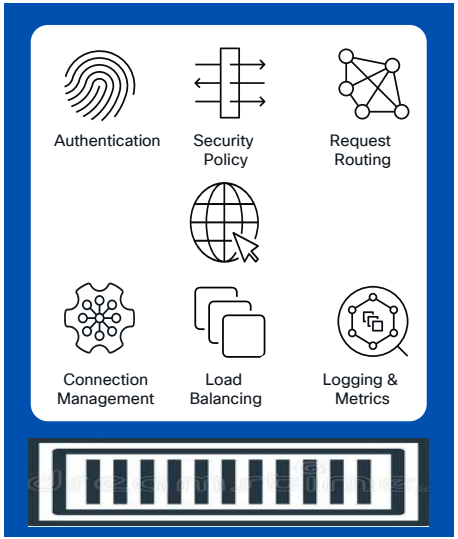


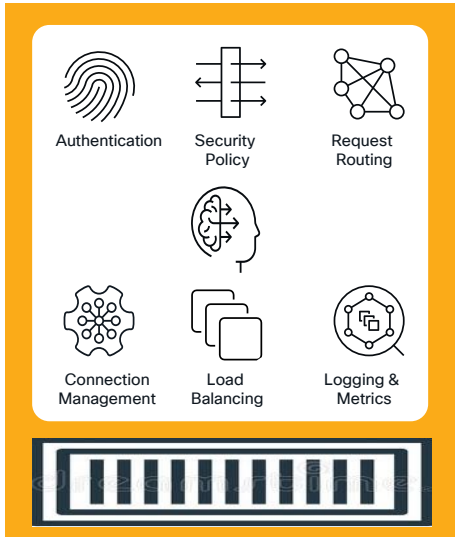
Sidecar Proxies and Service Mesh

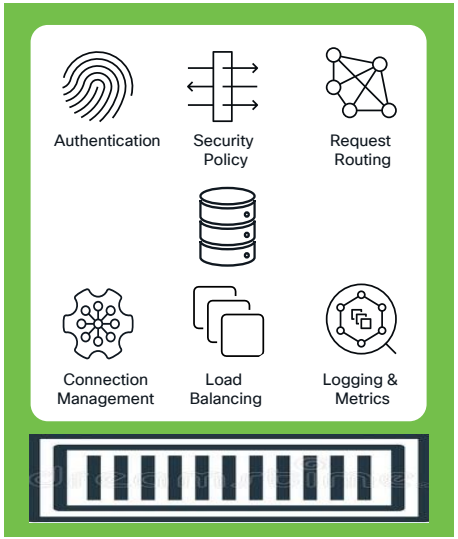


- In a generic Kubernetes environment, a containerized application microservice is usually assigned to a dedicated pod
- However, several common service functions (such as observability, access policy, encryption, load-balancing, traffic management, etc.) can be standardized and enabled by creating a sidecar within the pod
- These common services are in turn centrally controlled by the service mesh control plane

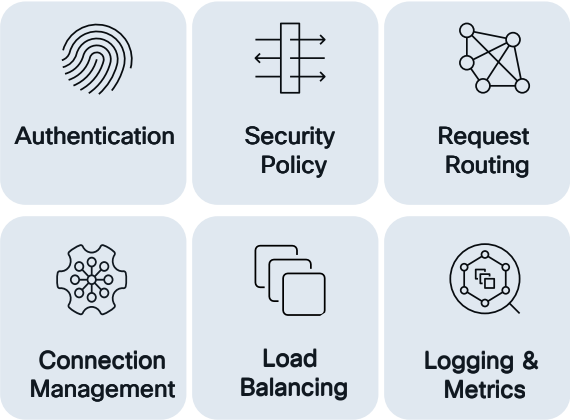
Microservice Common Functions

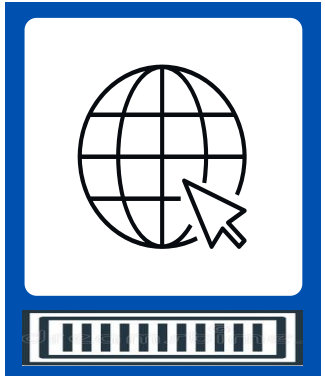


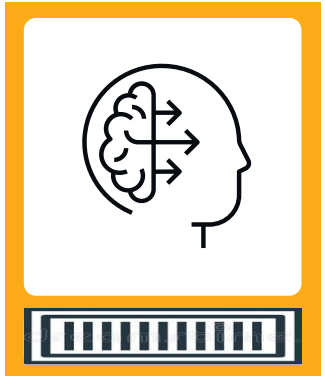




Microservice Common Functions

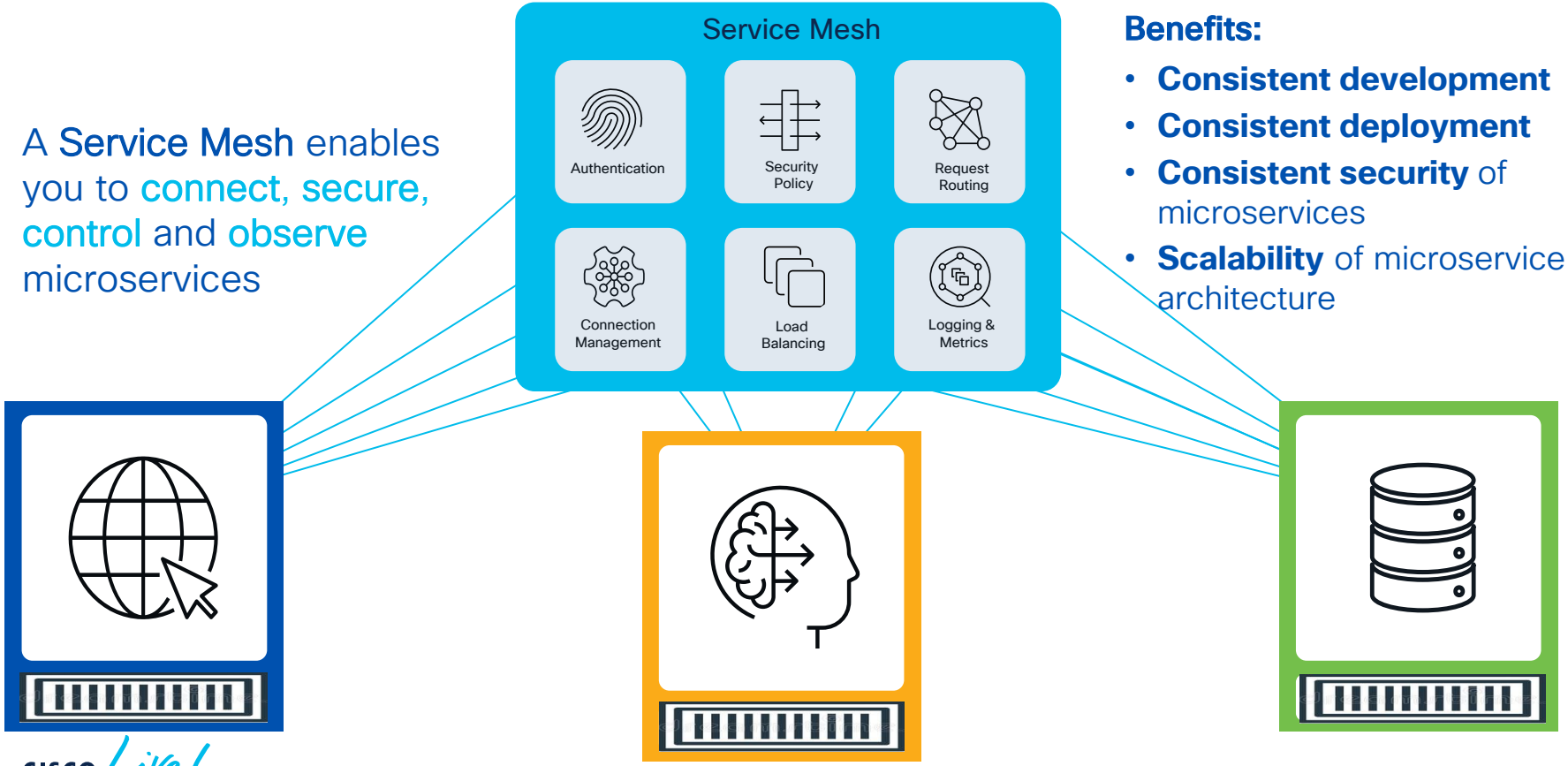






Service Mesh

A **Service Mesh** enables you to **connect**, **secure**, **control** and **observe** microservices



Benefits:

- **Consistent development**
- **Consistent deployment**
- **Consistent security** of microservices
- **Scalability** of microservice architecture

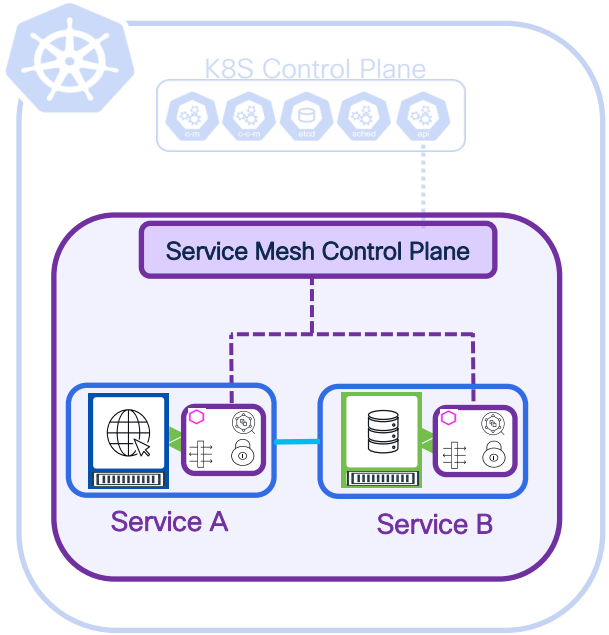
Istio Service Mesh Benefits

- Automatic load balancing for HTTP, gRPC, WebSocket, and TCP traffic
- Robust multicluster connectivity
- Fine-grained control of traffic behavior with rich routing rules, retries, failovers, and fault injection
- A pluggable policy layer and configuration API supporting access controls, rate limits and quotas
- Automatic metrics, logs, and traces for all traffic within a cluster, including cluster ingress and egress
- Secure service-to-service authentication with strong identity assertions between services in a cluster

gRPC - Cross-platform Remote, Open Source, High Performace Remote Procedure Calls

Service Mesh Deployment Models

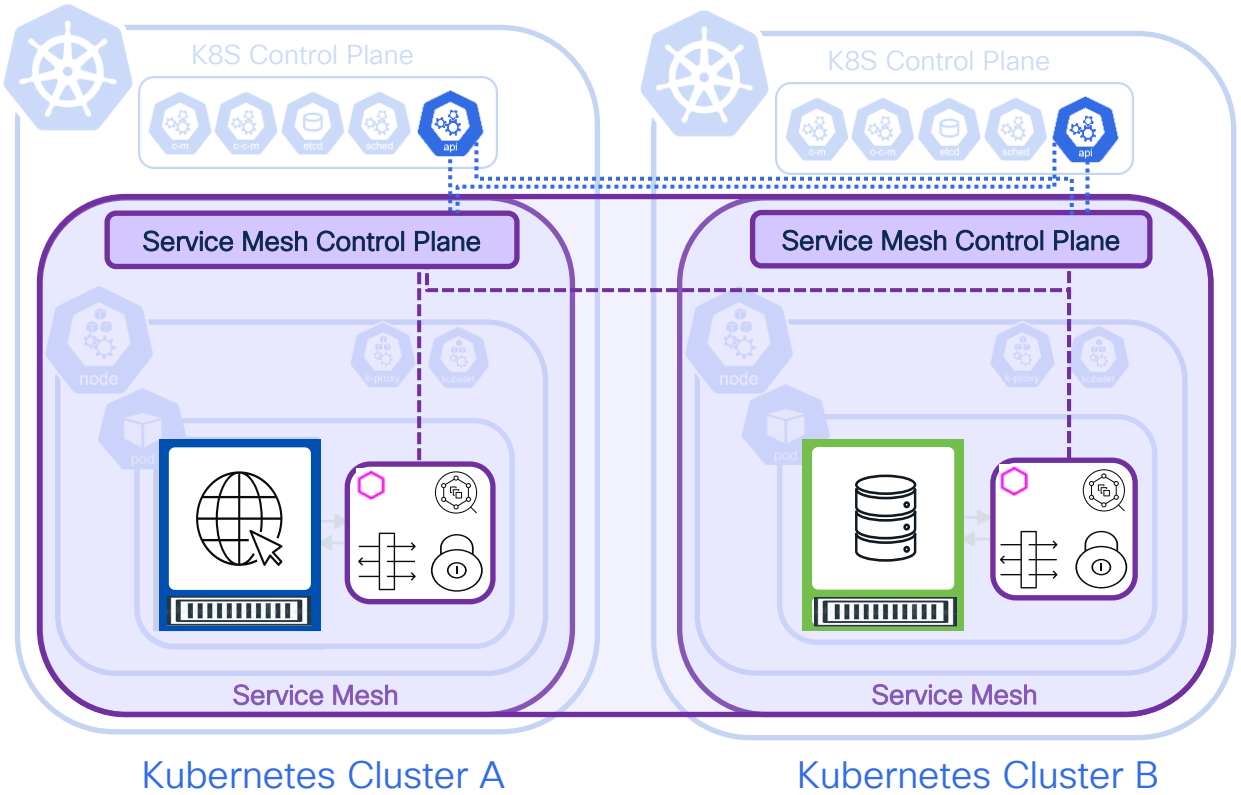
Single Cluster Deployment



Single Cluster

- Simplest Deployment
- Single Mesh/Control Plane
- Typically over same subnet
- End to end service visibility

Multi Cluster Deployment



- Multiple options
  - Single or Multiple Networks
  - Single or Multiple control planes
  - Zones or Regions
  - Distributed Applications
  - Loadbalancing and Istio Gateways

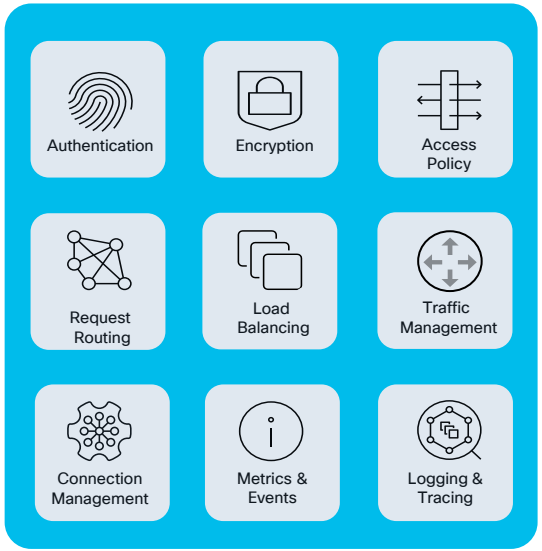
Multiple Networks

- Overlapping IP or VIP ranges for **service endpoints**
- Crossing of administrative boundaries
- Fault tolerance
- Scaling of network addresses
- Compliance with standards that require network segmentation

Service Mesh Deployment Challenges

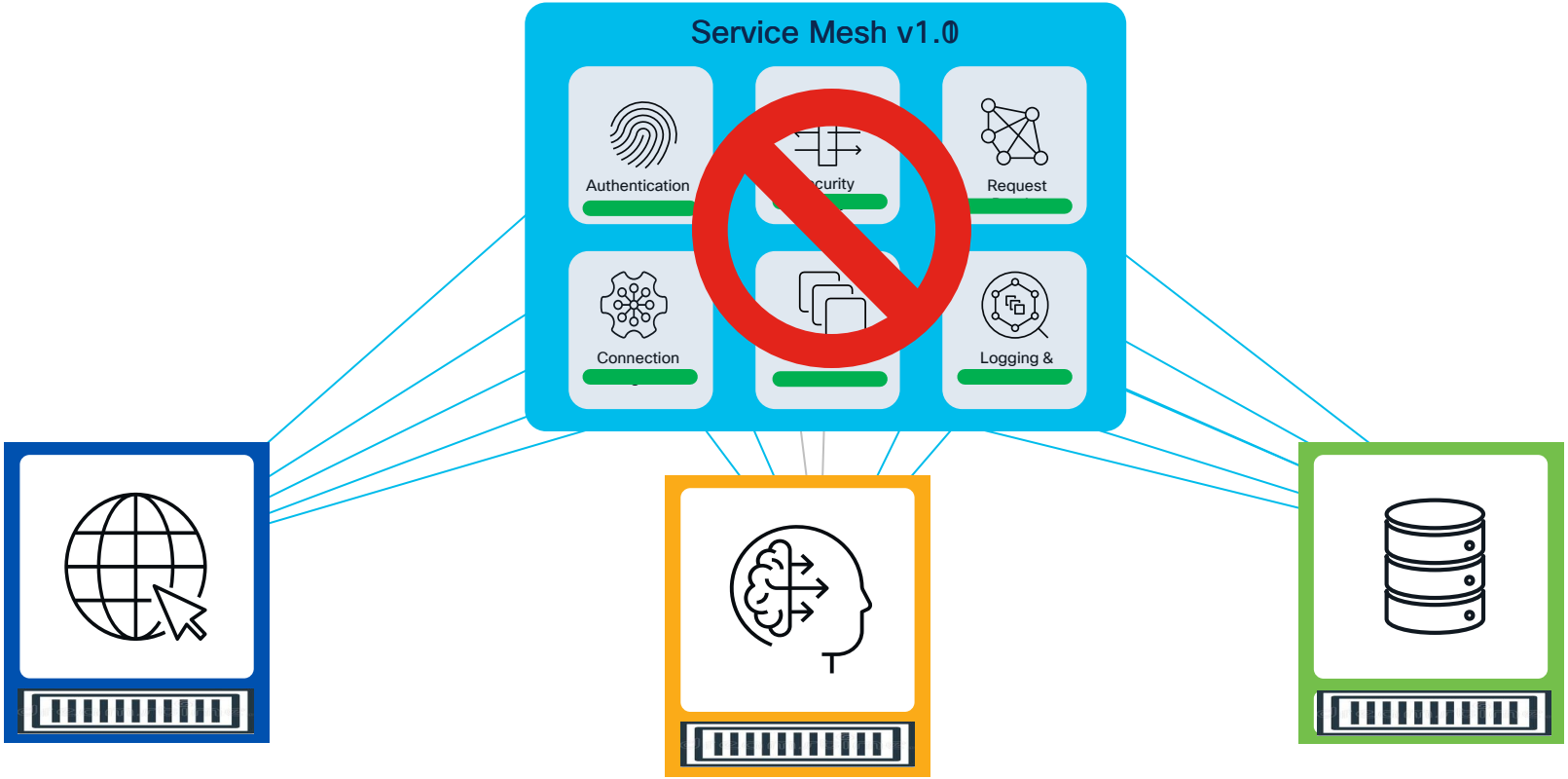
Service Mesh Deployment Challenges

- Lifecycle management
- Disparate/fragmented observability
- Multi-cluster challenges:
  - Availability
  - Cross-cluster service discovery
  - Inter-cluster traffic management policy
  - Multi-Tenancy



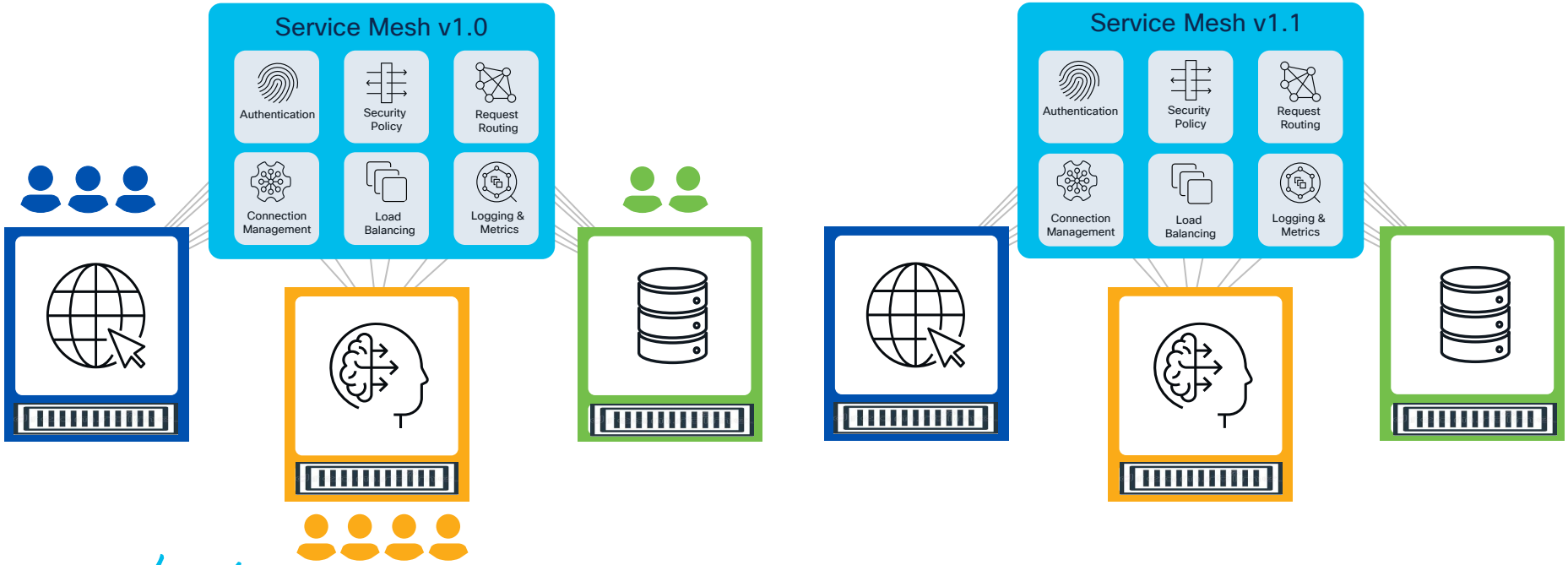
Service Mesh

Service Mesh Lifecycle Management

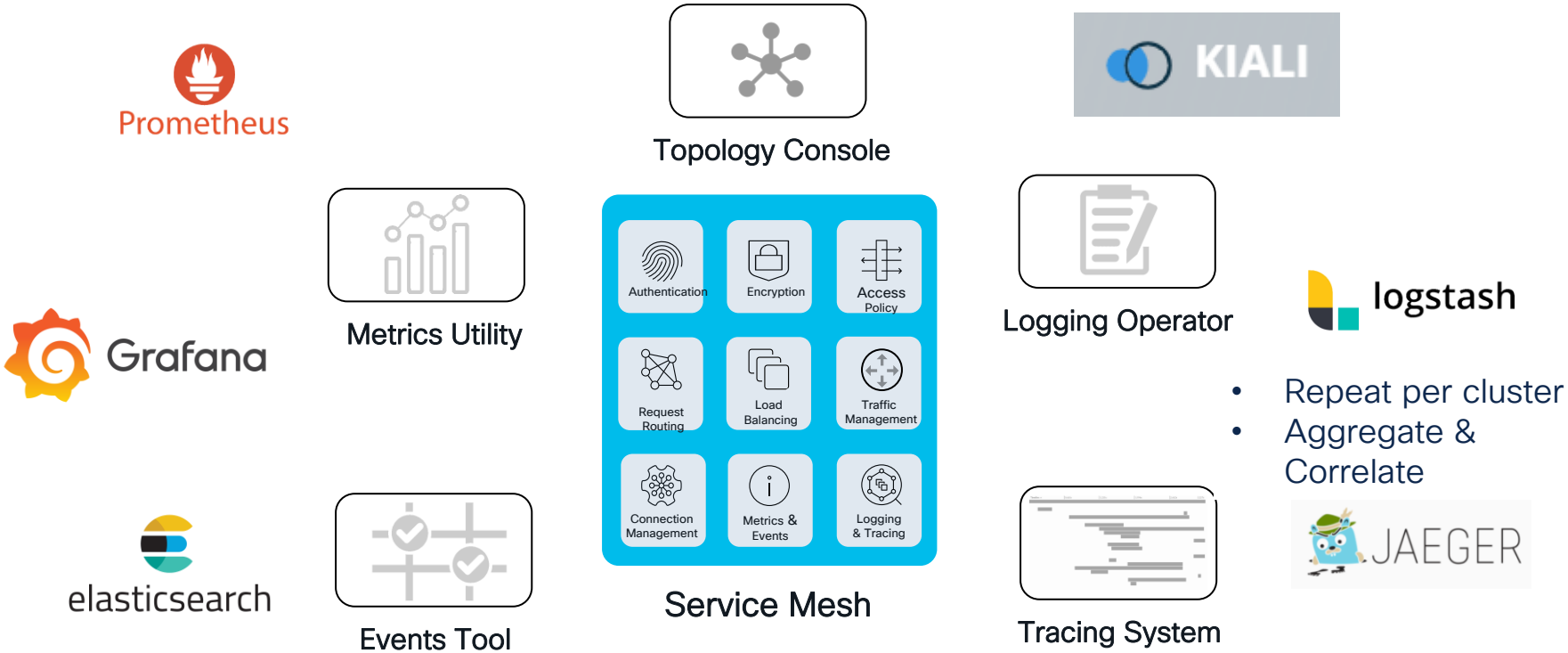


Service Mesh Lifecycle Management

- Most service meshes require upgrades every 3 months
- Service Meshes are upgraded on a cluster-by-cluster basis

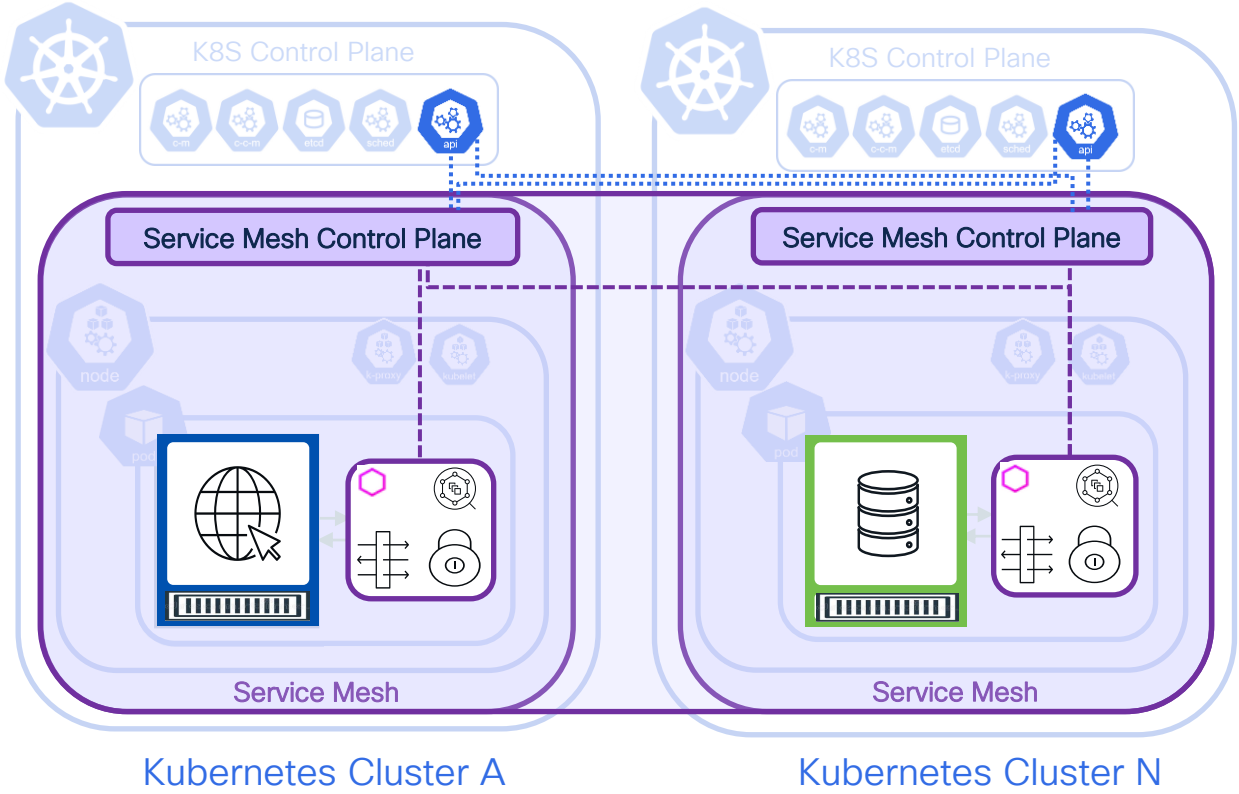


Service Mesh Observability Challenges



- Repeat per cluster
- Aggregate & Correlate

Enabling a Multi-Primary Control Plane



- Service meshes can be extended across clusters, such as by extending the control plane from a **primary** cluster to a **remote** cluster
  - Stable IP
  - Expose Control Plane via Istio GW
- Deploying multiple control planes across clusters, which is called a **multi-primary control plane**

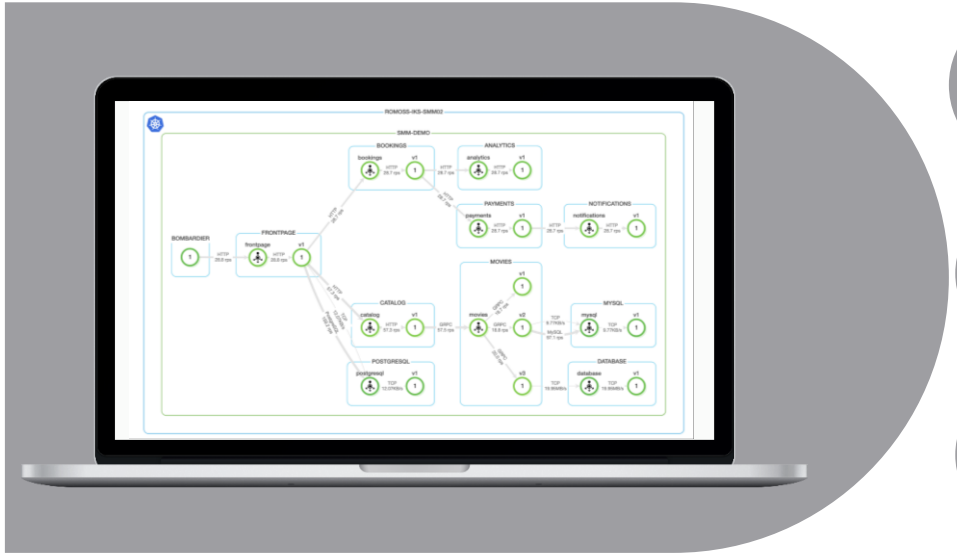
Pre-planning

- Network CIDR
- Service Naming
- Enable DNS Proxy
- Istio Gateway
- External Load balancer
- Expose services via multiple steps

Introducing Cisco Calisti

Cisco Calisti (Cisco Service Mesh Manager)

Operationalize the service mesh



Multi-cloud, multi-cluster observability
Connect any on-prem and public cloud together

Simplifies service mesh management
Single pane of glass, in depth metrics

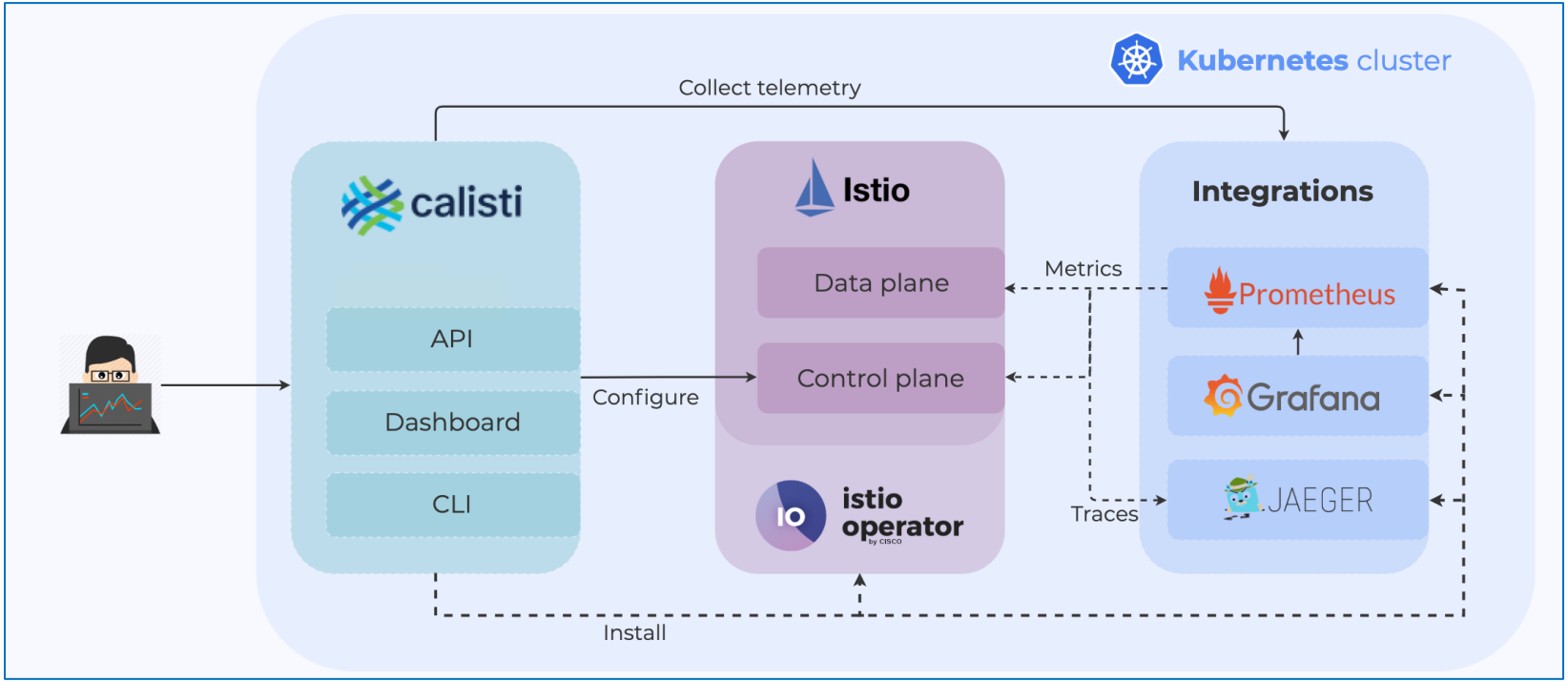
Policy-based app networking & security
Policy management for DevOps practices

Traffic management ensures smooth app updates

Complete application and health **observability**

Security at all layers between clusters and clouds

High Level Architecture



Key Capabilities

- Istio Distribution
- Mesh Lifecycle Management
- Observability Toolbox
- Multi-Cluster Topologies
- Multi-Gateway
- Security & Compliance

Cisco Calisti Setup

- Install Cisco Calisti with full Istio control plane and identify Primary K8s cluster
  - ./smm install -a -cluster-name kubernetes
- Extend Istio control plane to attach a Remote K8s Cluster
  - ./smm istio cluster attach -c ~/.kube/kubeconfig-calisti.yaml ~/.kube/backup-cluster-kubeconfig.yaml
- Enable sidecar injection on a namespace
  - ./smm sidecar-proxy auto-inject on default

Mesh Status

Calisti | MESH

control planes	clusters	istio proxies memory usage	istio proxies CPU usage	istio proxies not running
1	2	3.12GB	0.43vCPU	0

Clusters

NAME	TYPE	PROVIDER	VERSION	STATUS
backup-cluster	Peer	()	v1.23.6 ()	Ready
kubernetes	Local	()	v1.23.6 ()	Ready

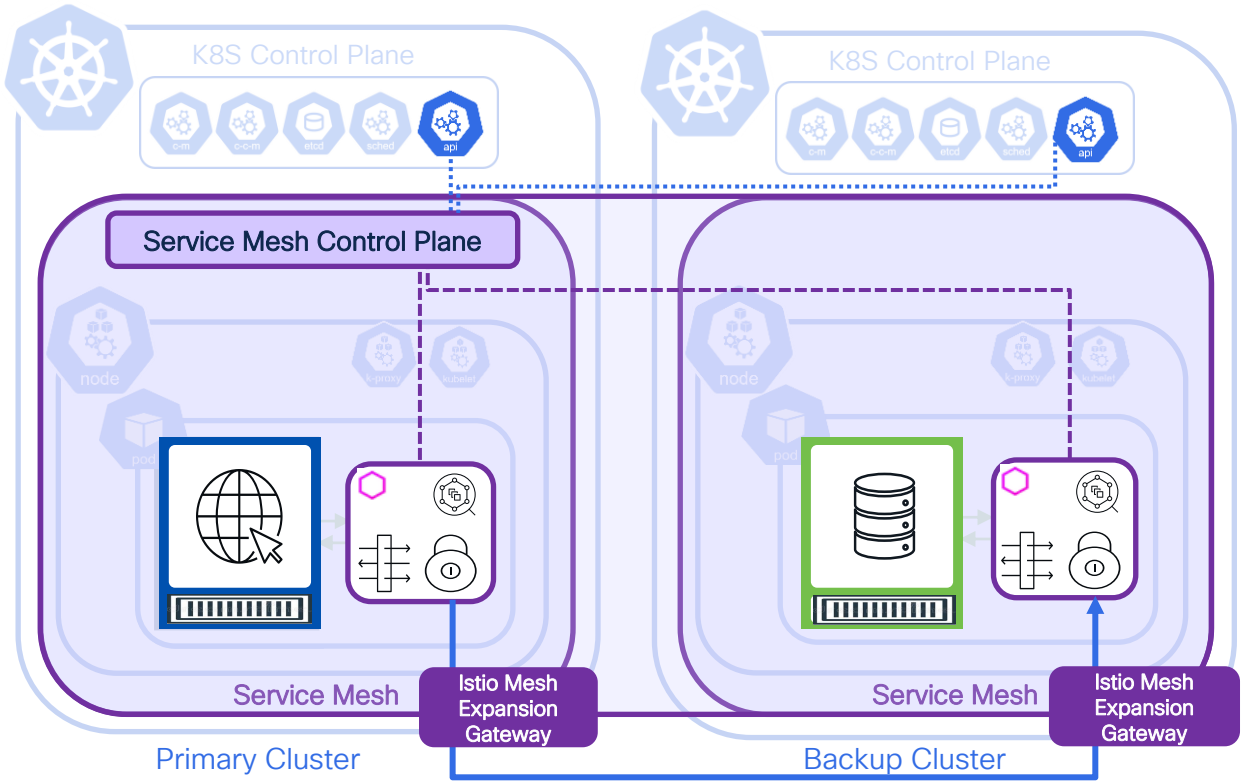
Control planes

NAME	CLUSTER	VERSION	TRUST DOMAIN	PODS	PROXIES	CONFIG
cp-v115x.istio-system	kubernetes	1.15.3	cluster.local	istiod-cp-v115x-584d5bb95d-cbbt4.istio-system	46 / 46	

```
administrator@sundar-k8s-master:~$ ./smm istio cluster status
✓ validate-kubeconfig ❯ checking cluster reachability...
logged in as kubernetes-admin
Clusters
---
Name            Type    Provider  Regions  Version  Distribution  Status  Message
backup-cluster  Peer              []       v1.23.6                Ready
kubernetes      Local             []       v1.23.6                Ready


ControlPlanes
---
Cluster     Name                   Version  Trust Domain     Pods                                          Proxies
kubernetes  cp-v115x.istio-system  1.15.3   [cluster.local]  [istiod-cp-v115x-584d5bb95d-cbbt4.istio-system]  46/46
```

Extend Control Plane across Multi Cluster



- Mesh Expansion Gateways Deployed in Backup Cluster (Remote)
- Gateway reachable IPs
- Cross-cluster endpoint/service discovery
- Service isolation/limited visibility

Mesh Expansion Gateways

```
administrator@sundar-k8s-master:~$ kubectl get istiocontrolplane -n istio-system
NAME        MODE      NETWORK    STATUS      MESH EXPANSION   EXPANSION GW IPS      ERROR   AGE
cp-v115x    ACTIVE    network1   Available   true             ["172.40.143.194"]            153d
administrator@sundar-k8s-master:~$
administrator@sundar-k8s-master:~$ kubectl get istiocontrolplane -n istio-system --kubeconfig ~/.kube/backup-cluster-kubeconfig.yaml
NAME        MODE      NETWORK          STATUS      MESH EXPANSION   EXPANSION GW IPS      ERROR   AGE
cp-v115x    PASSIVE   backup-cluster   Available   true             ["172.40.143.181"]            11d
```

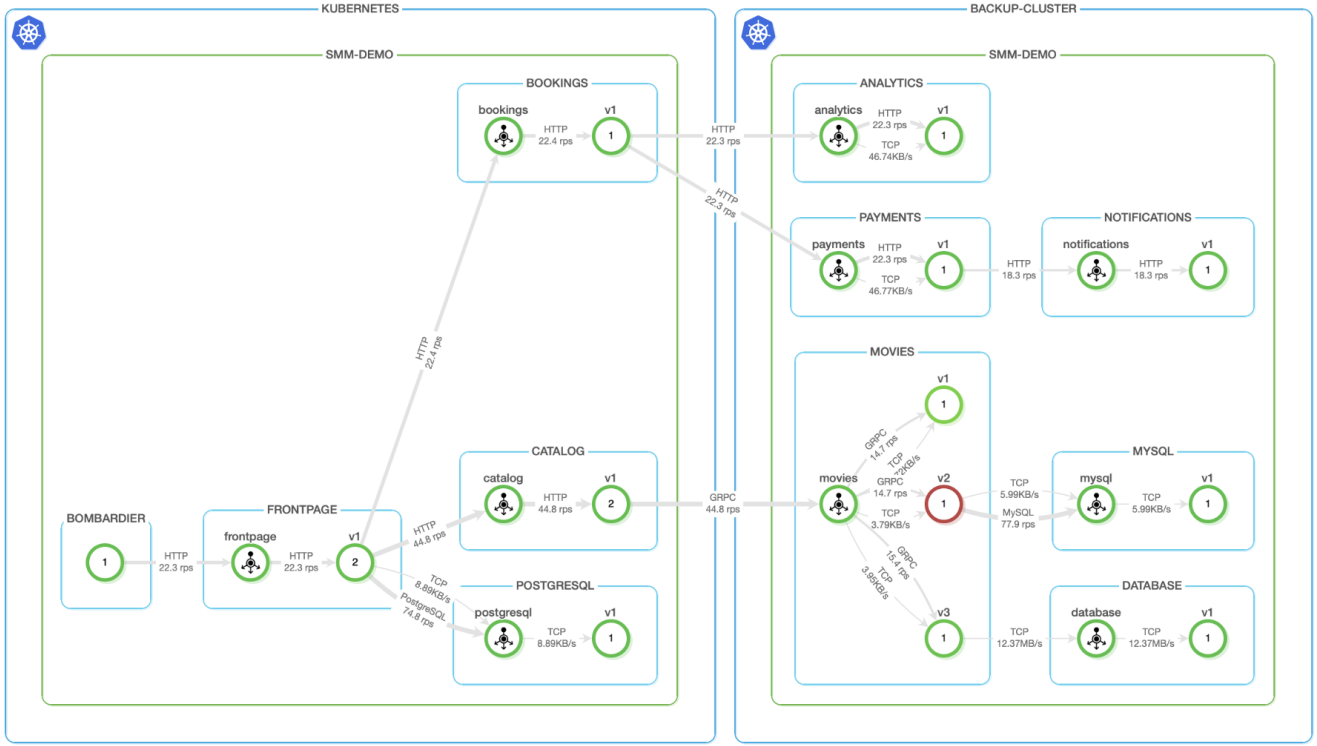
```
administrator@sundar-k8s-master:~$ kubectl get svc -n istio-system
NAME                                    TYPE           CLUSTER-IP      EXTERNAL-IP      PORT(S)
                AGE
istio-meshexpansion-cp-v115x            LoadBalancer   10.102.76.217   172.40.143.194   15021:31694/TCP,15012:30554/TCP,15017:30071/TCP,15443:30560/TCP,50600:32129/TCP,594
11:32686/TCP   153d
istio-meshexpansion-cp-v115x-external   ClusterIP      None            <none>           15021/TCP,15012/TCP,15017/TCP,15443/TCP,50600/TCP,59411/TCP
                153d
istiod-cp-v115x                         ClusterIP      10.99.218.143   <none>           15010/TCP,15012/TCP,443/TCP,15014/TCP
                153d
administrator@sundar-k8s-master:~$ kubectl get svc -n istio-system --kubeconfig ~/.kube/backup-cluster-kubeconfig.yaml
NAME                                    TYPE           CLUSTER-IP       EXTERNAL-IP      PORT(S)
                            AGE
istio-meshexpansion-cp-v115x            LoadBalancer   10.106.234.123   172.40.143.181   15021:32226/TCP,15012:30463/TCP,15017:30410/TCP,15443:30147/TCP,50600:3
2139/TCP,59411:31243/TCP   11d
istio-meshexpansion-cp-v115x-external   ClusterIP      None             <none>           15021/TCP,15012/TCP,15017/TCP,15443/TCP,50600/TCP,59411/TCP
                            11d
istio-meshexpansion-cp-v115x-external-kubernetes   ClusterIP      None             <none>           15021/TCP,15012/TCP,15017/TCP,15443/TCP,50600/TCP,59411/TCP
                            11d
istio-sidecar-injector-cp-v115x         ClusterIP      10.102.246.162   <none>           443/TCP,15014/TCP
                            11d
istiod-cp-v115x                         ClusterIP      None             <none>           15010/TCP,15012/TCP,443/TCP,15014/TCP
                            11d
```

Deploy Application in Multi cluster

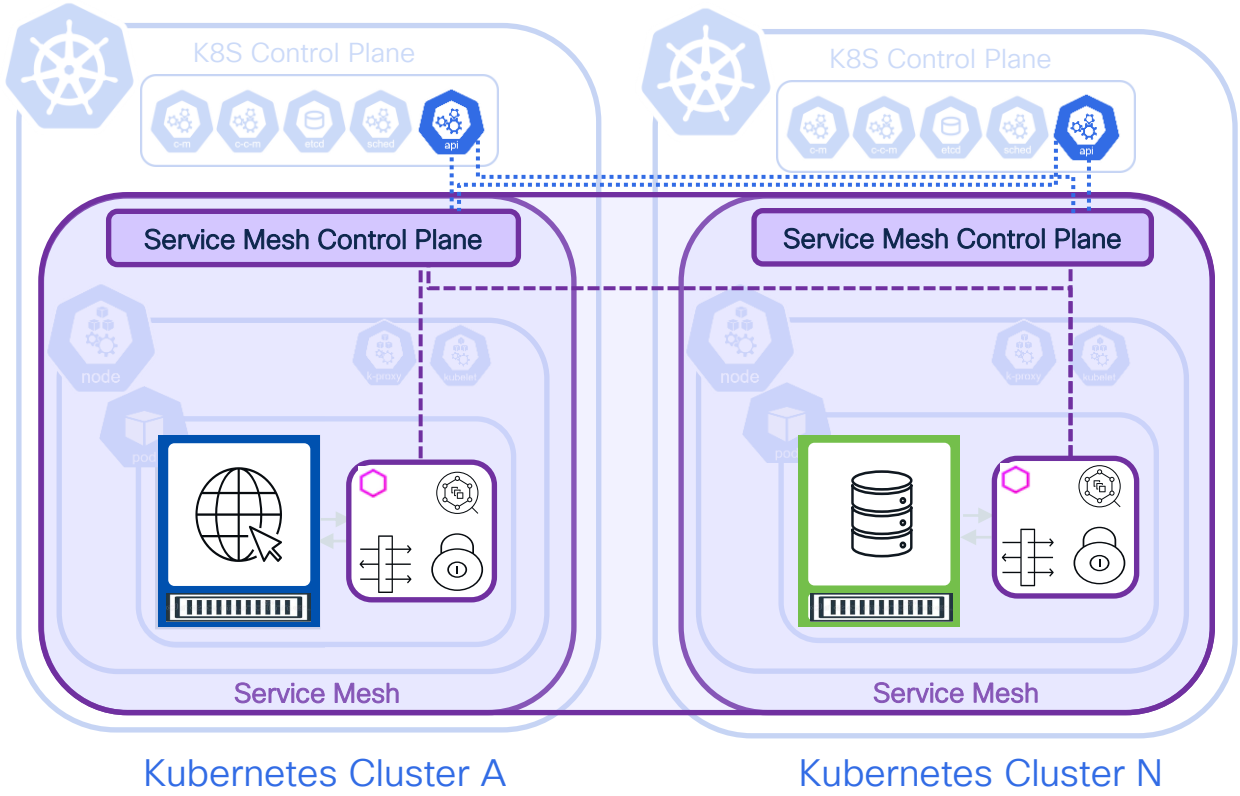
- Deploy few microservices in Primary Cluster
  - ./smm demoapp install -s frontpage,catalog,bookings,postgresql --kubeconfig ~/.kube/kubeconfig-calisti.yaml

- Deploy remaining microservices in Backup Cluster (Remote)
  - ./smm -c ~/.kube/backup-cluster-kubeconfig.yaml demoapp install -s movies,payments,notifications,analytics,database,mysql --peer

Multi Cluster Application Deployment



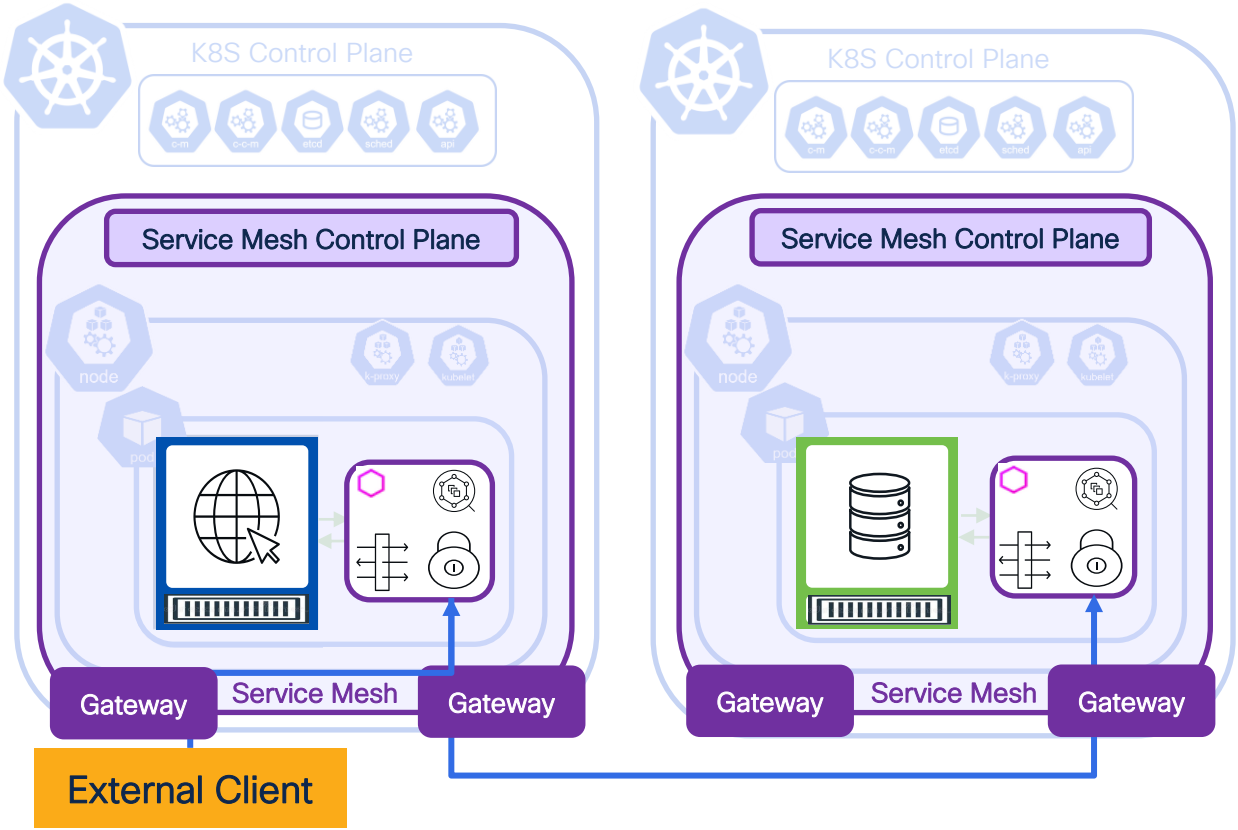
Enabling a Multi-Primary Control Plane



Benefits :

- Limited Scope
  - Cluster specific Configuration changes
  - Cluster specific impact if control plane is unavailable
  - Controlled Configuration rollout
- Service isolation/limited visibility
- High availability
- Cross-cluster endpoint/service discovery

Enabling Multi-Tenancy and Direct-Connect



- Typically, service meshes support only a single gateway per mesh
- Cisco's Istio distribution includes a custom resource definition that enables **multi-gateway support**, providing ingress/egress flexibility and extended policy options, such as multi-tenancy support for MSPs
- Additionally, Cisco supports **direct connect**, which enables mTLS communication to a workload from an external client

Demo

Key Takeaways from Demo

- Calisti Dashboard
- Microservices Topology
- Integrated Observability Tools
  - Metrics
  - Traces
  - Traffic Tap
- Custom Application deployment across multi-cluster
- Traffic management

Conclusion

- Targeted Use Cases for Multi cluster Service Mesh
- Multi Network Deployment
- Cross-cluster Service Discovery
- Cisco Calisti for
  - Istio Operations
  - Observability Toolbox
  - Multi Cluster Topologies
  - Multi Gateway support

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

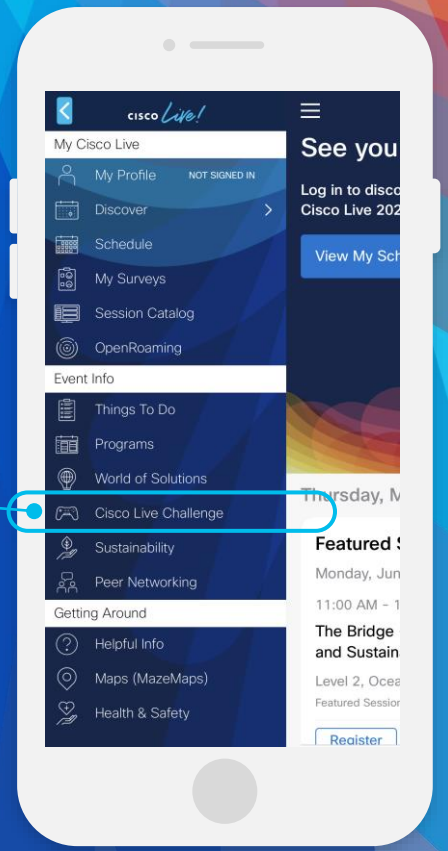
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

cisco Live!

Let's go