CISCO *Live!*

DevNet Zone

The bridge to possible

Introducing Panoptica

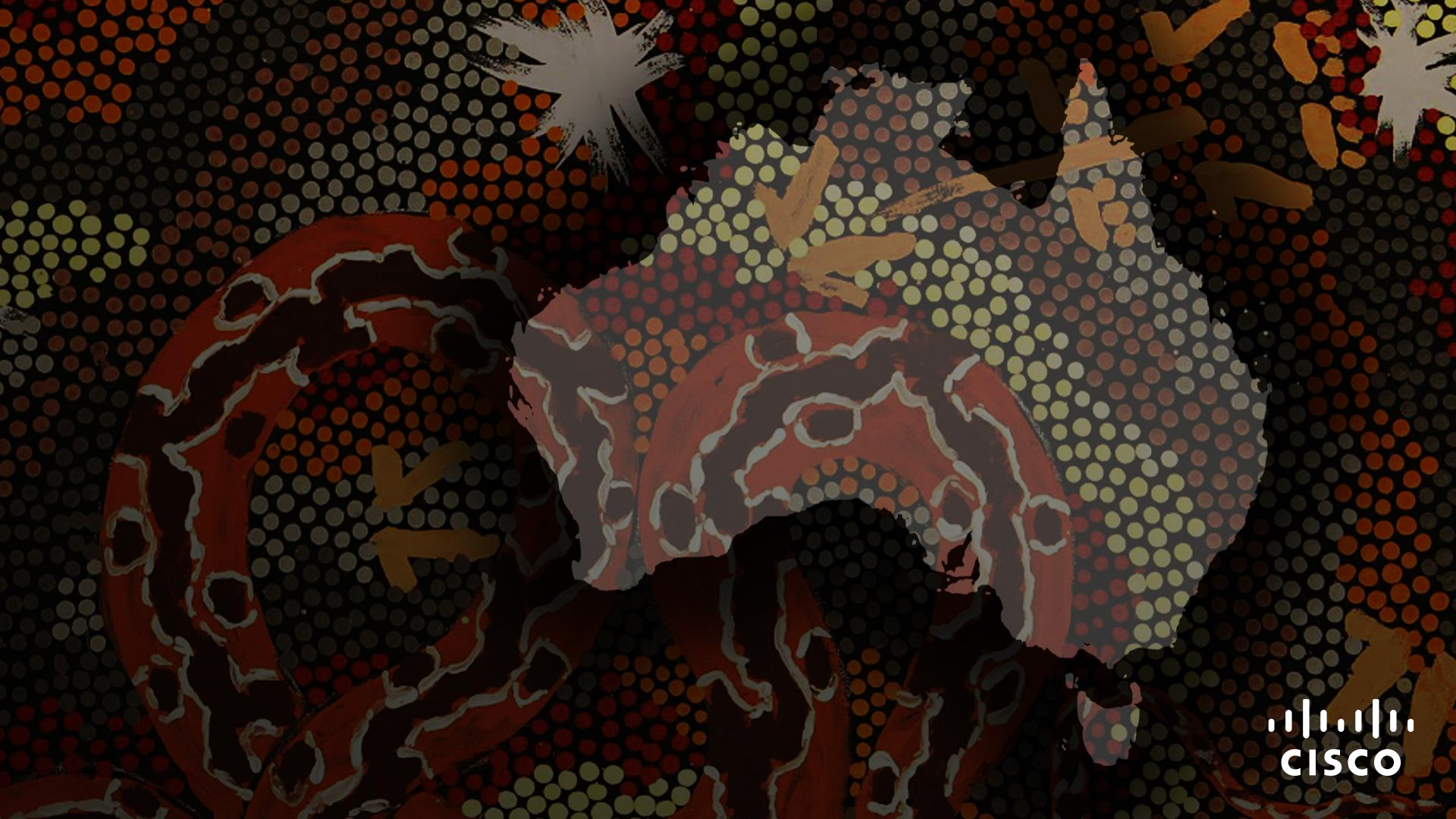
How Cisco is Bringing 30 Years of Security Leadership to Cloud Native Application Architectures

Tim Szigeti, Principal Engineer
@tim_szigeti

DEVNET-2511

Cisco Live!

DevNet Zone


CISCO

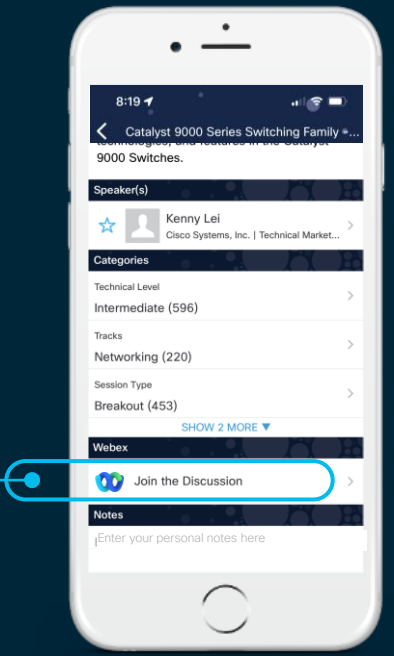
Cisco Webex App

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



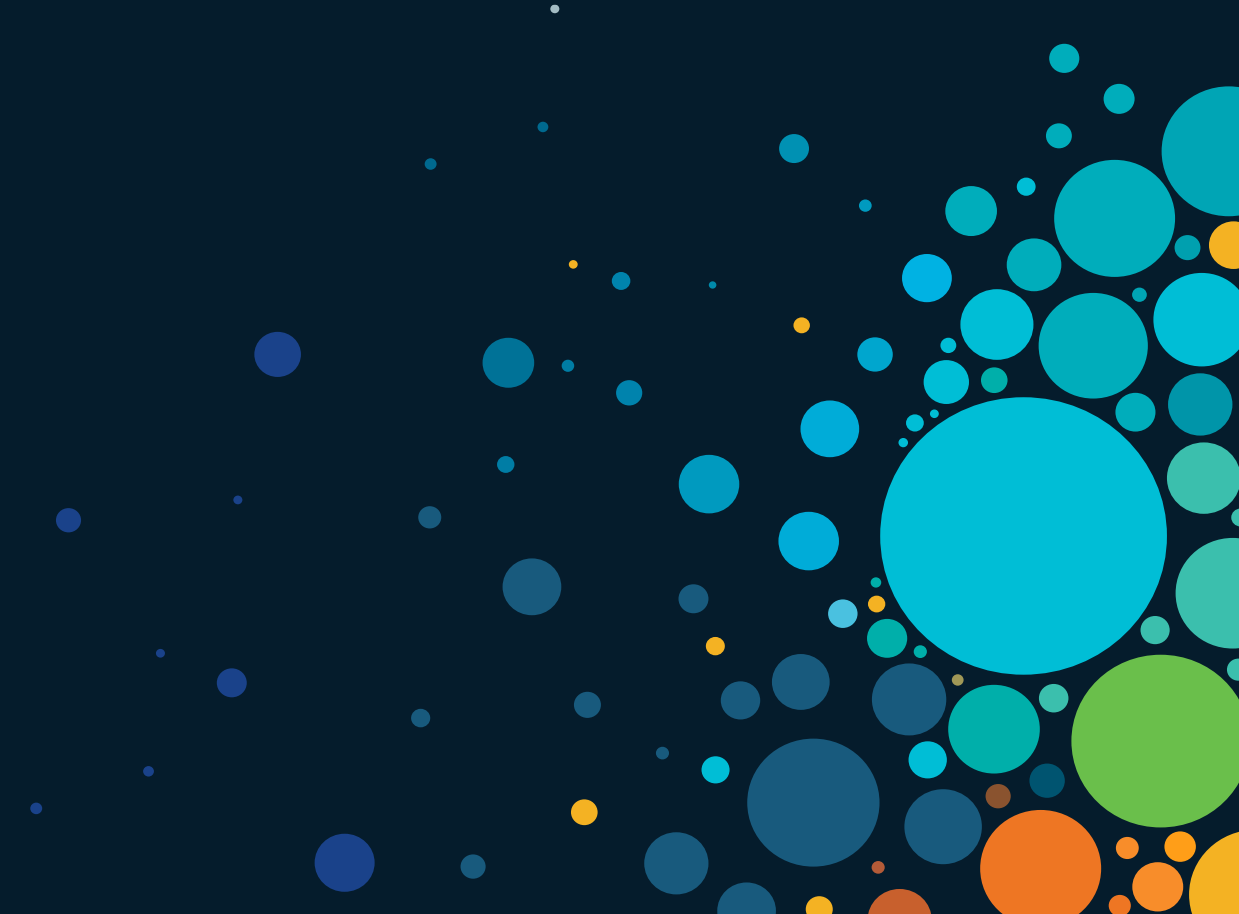
https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2511

Webex spaces will be moderated
by the speaker until Thursday 22 December, 2022.

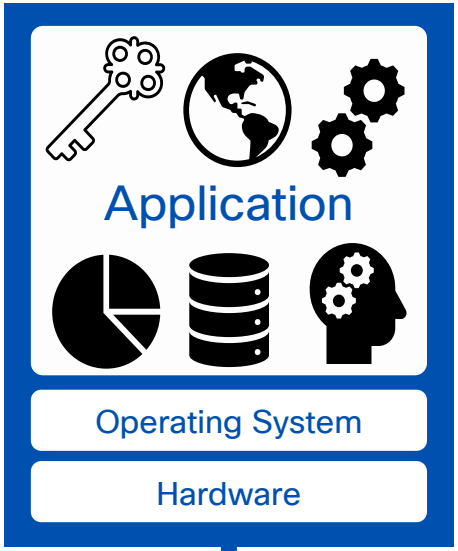
Agenda

- Introduction
- Container Security
- API Security
- Network Security
- Summary and Key Takeaways

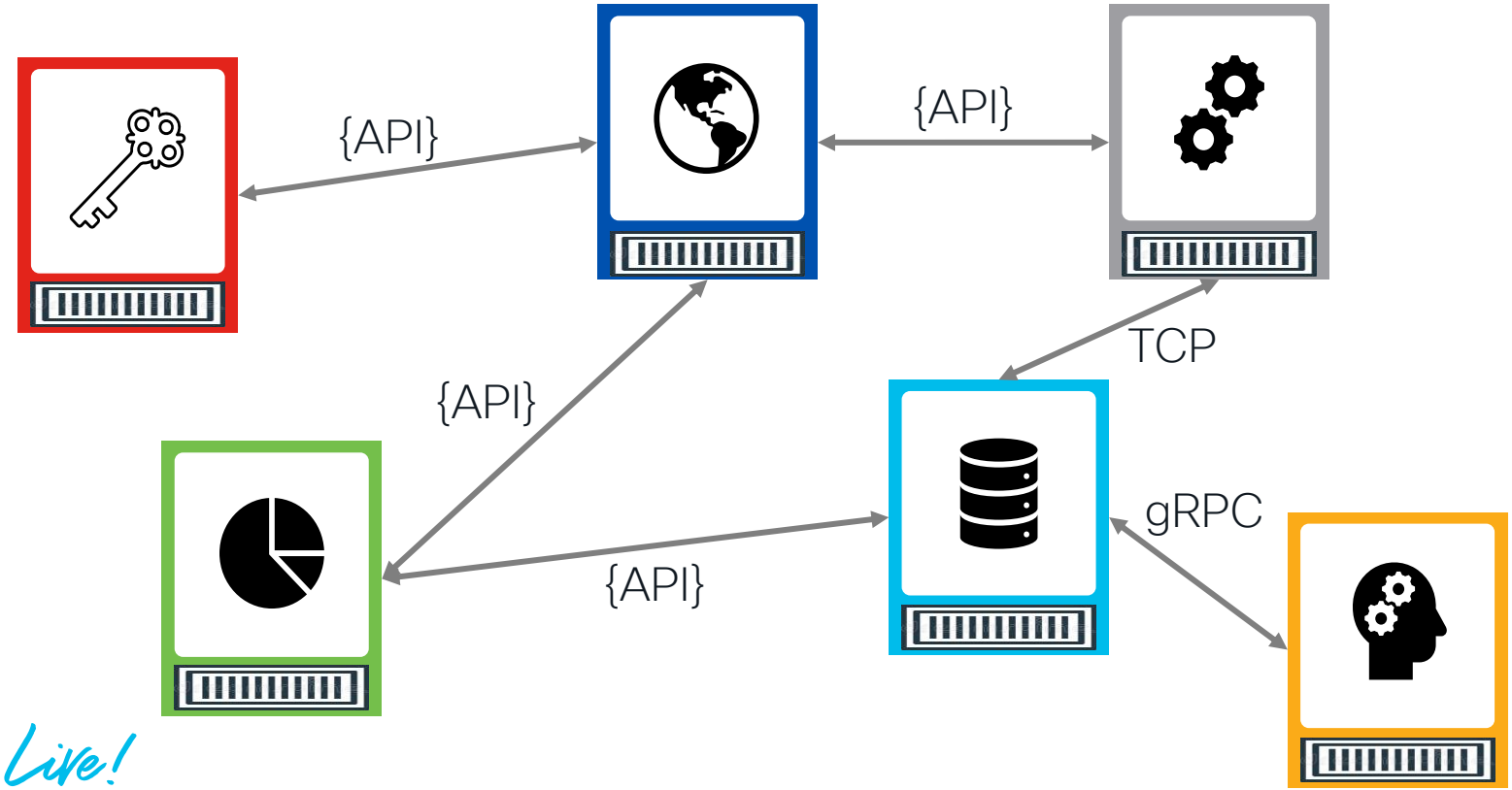
Introduction



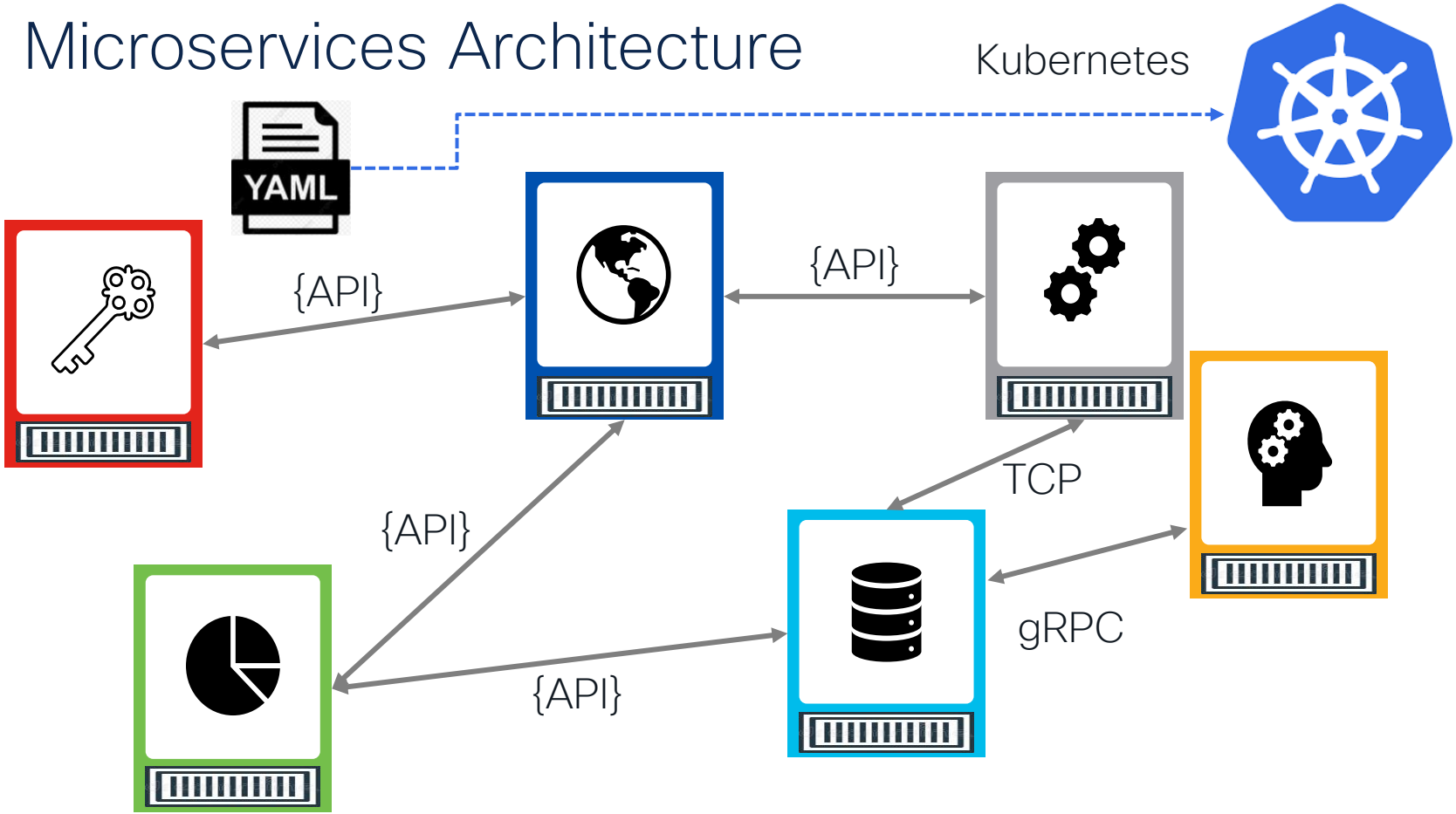
Monolithic Application Architecture



Cloud Native Microservices Architecture

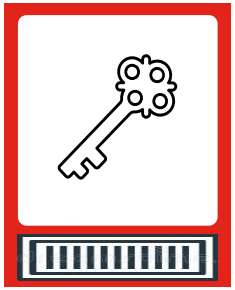


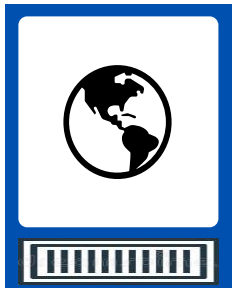
CN Microservices Architecture

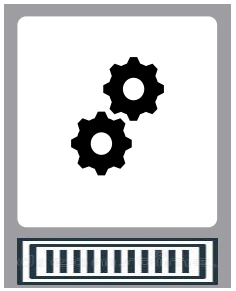


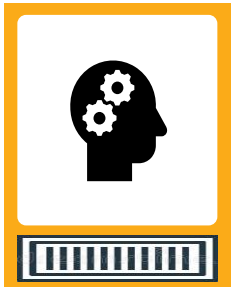
CN Microservices Architecture

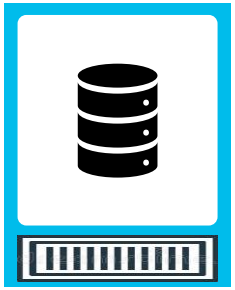
Kubernetes

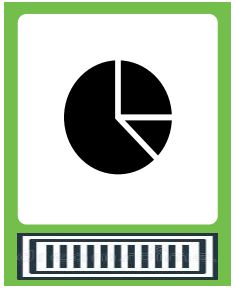






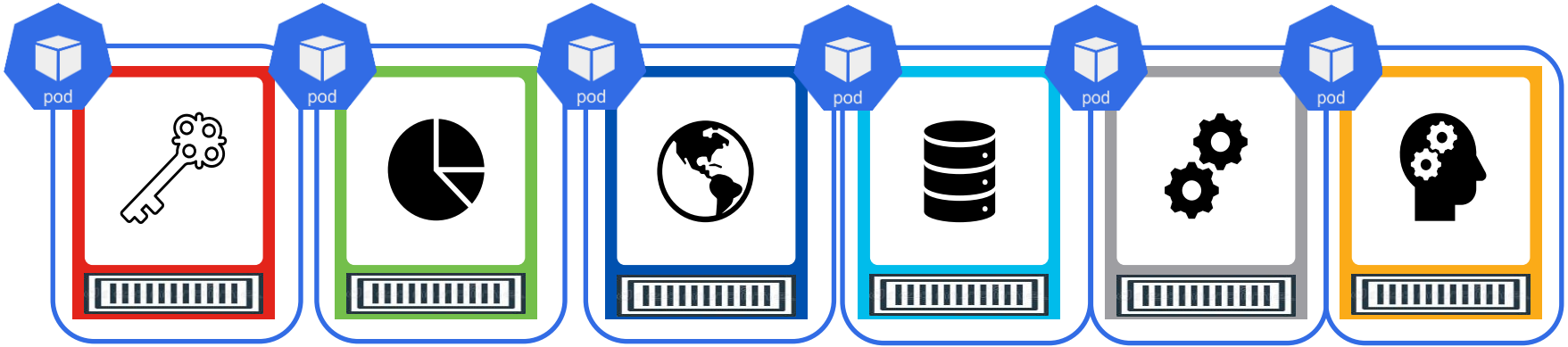




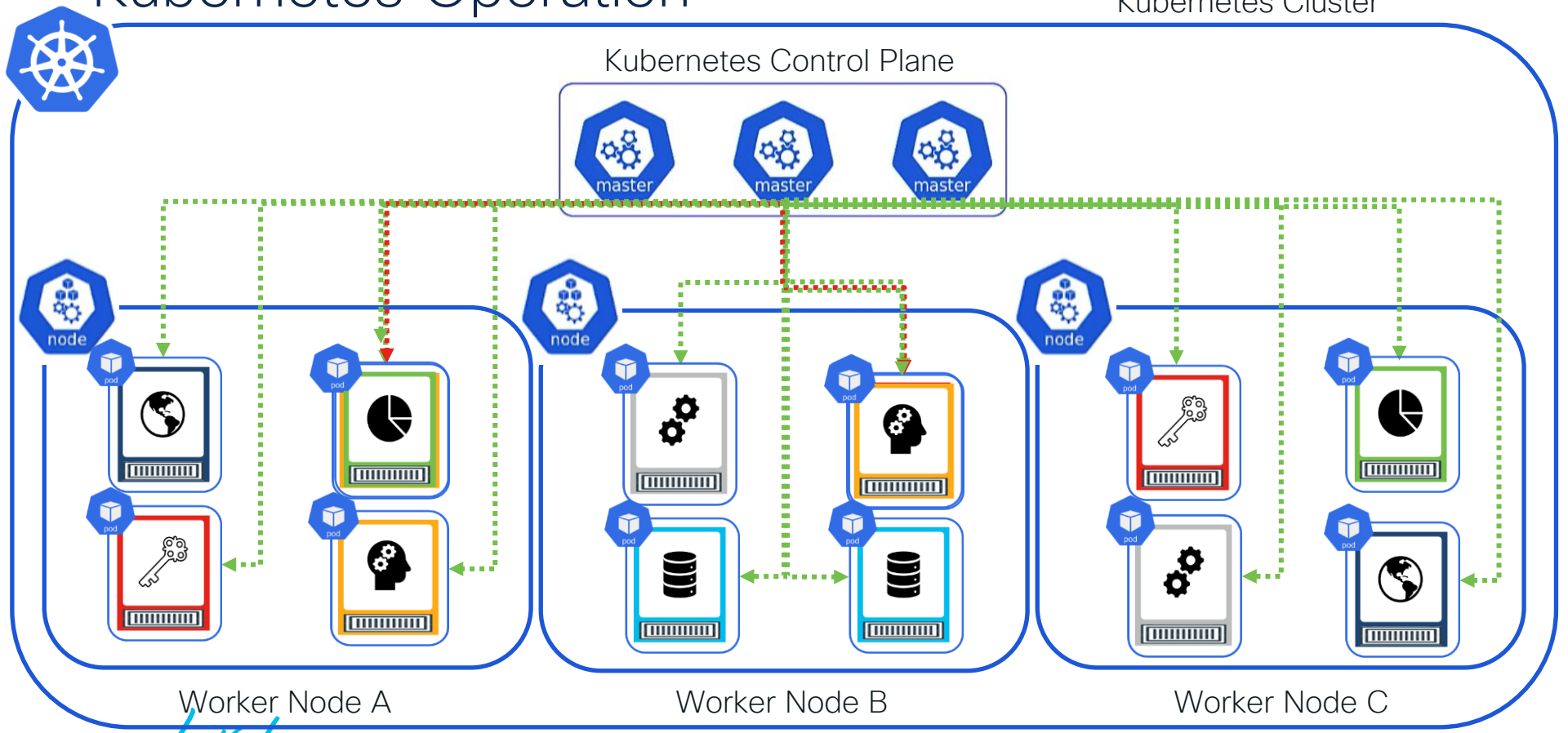


CN Microservices Architecture

Kubernetes



Kubernetes Operation



Cloud Native Security Challenges

CN Apps have unique security requirements

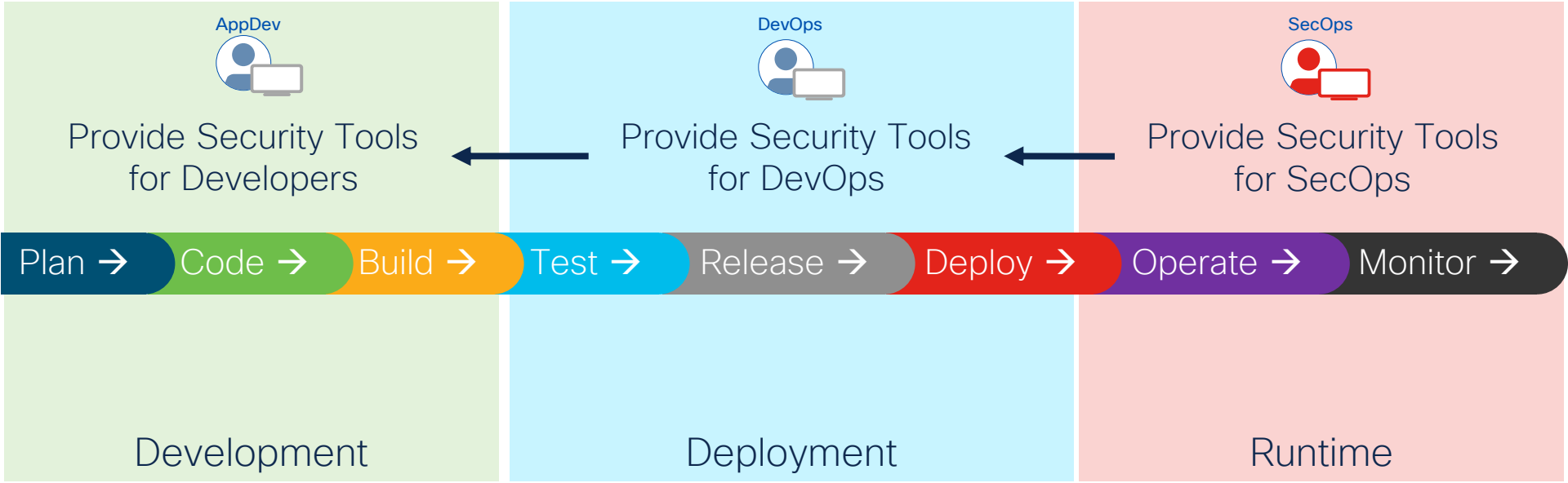
Lack of Visibility, Tools and Expertise

Multiple Layers of Security are Required

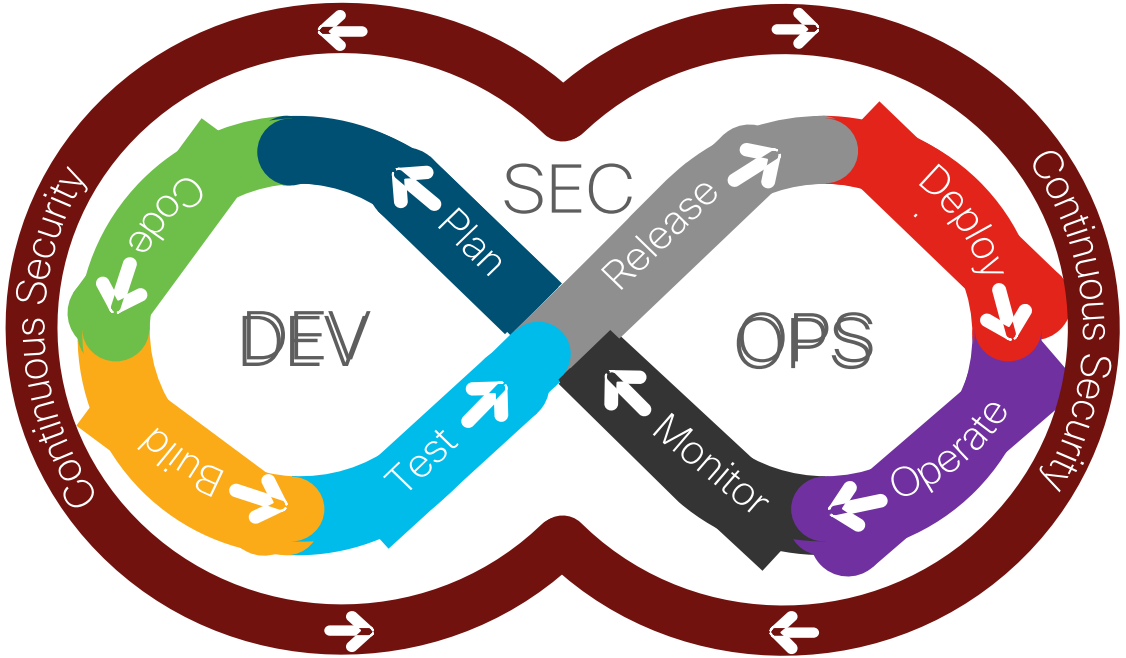
Orchestration introduces new vulnerabilities and attack vectors

Early Detection to security issues is key to saving time and money

Cisco Cloud Native Security Goal: “Shift Left”



Security Goal: “Shift Left” and Make It Continuous



Container Security

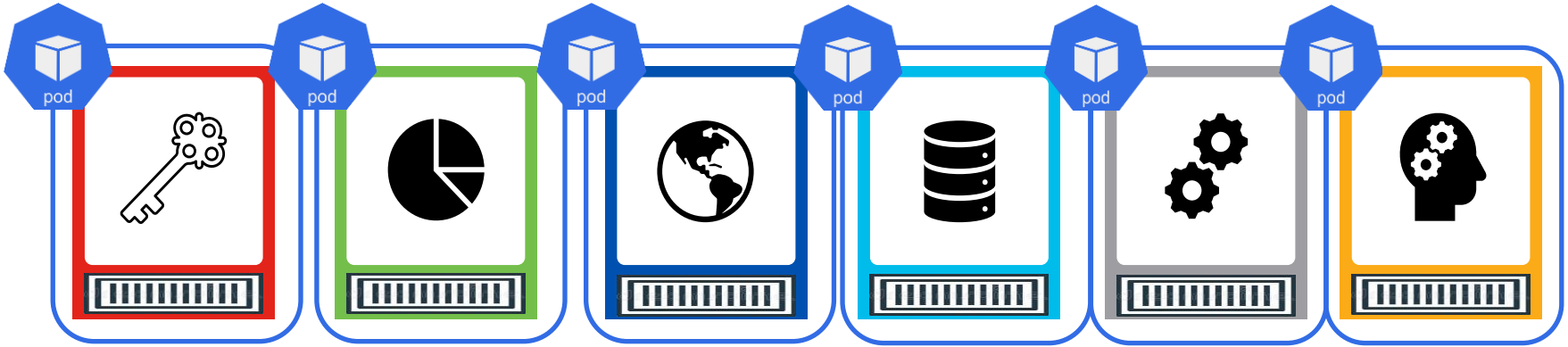
Cloud Native **Container** Security Challenges

Deployment (Application Manifest) Security Vulnerabilities:

- Security misconfigurations
- Embedded secrets and/or PII

Pod Security Challenges:

- Vulnerable configurations
- Unauthorized images



Container Security:

- Vulnerable images
- Vulnerable packages and/or dependencies

Panoptica: Open-Sourced Architectural Components

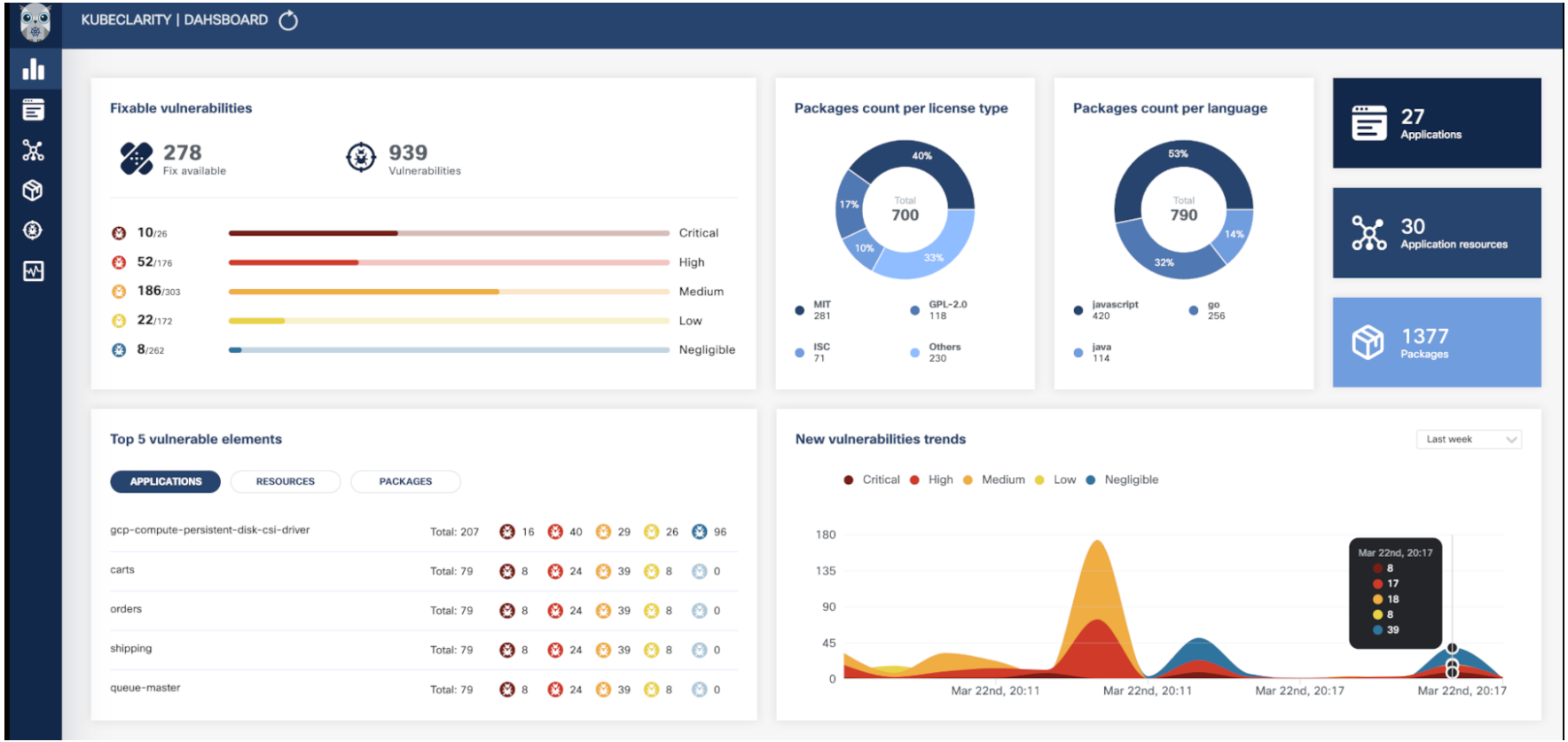
- KubeClarity is a Cisco-seeded open-source tool for detection and management of Software Bill Of Materials (SBOM) and vulnerabilities of container images and filesystems
- It scans both runtime K8s clusters and CI/CD pipelines for enhanced software supply chain security.

https://github.com/openclarity/kubeclarity/

- KubeClarity is a Cisco-seeded open-source tool for detection of API vulnerabilities and threats
- It can identify microservices that are using deprecated APIs, undocumented APIs, or APIs that exhibit behavior different from what is documented

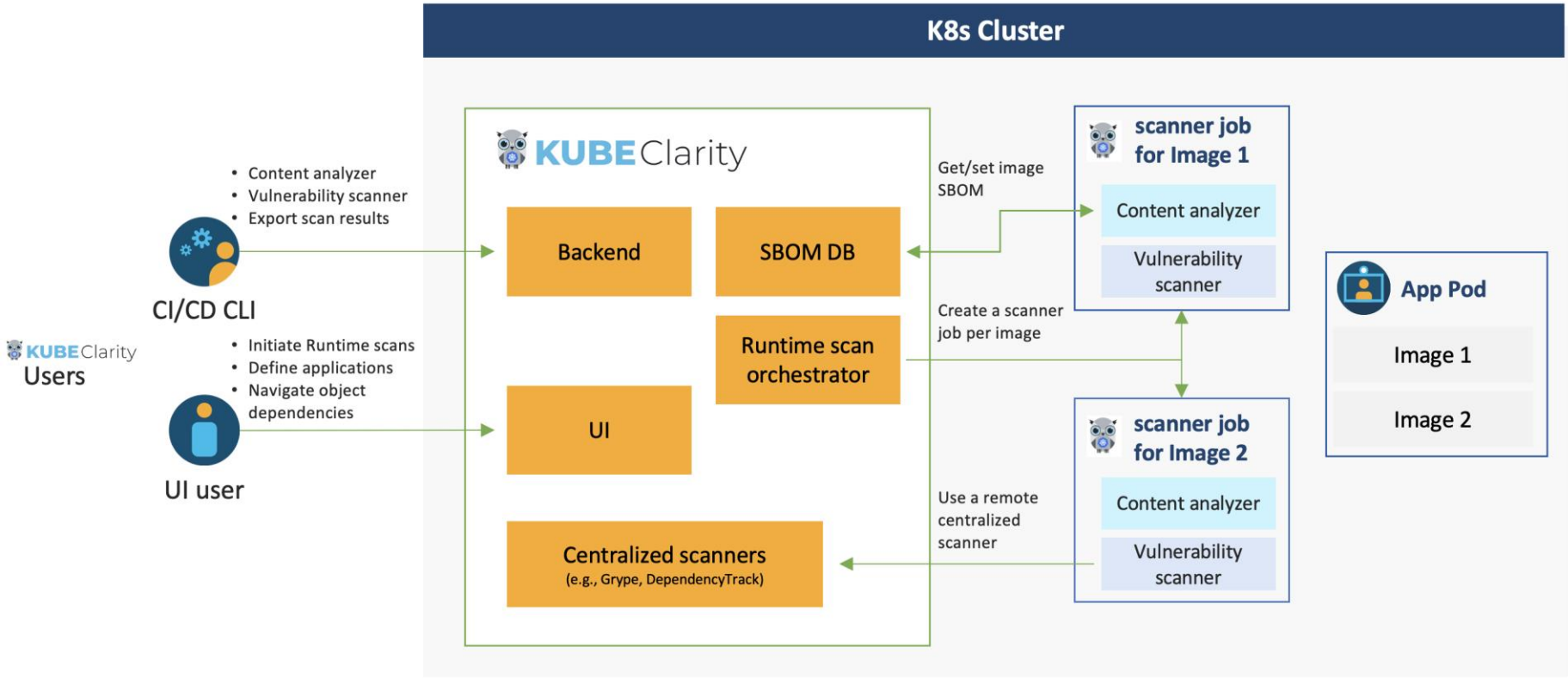
https://www.apiclarity.io/

KubeClarity



https://github.com/openclarity/kubeclarity/

KubeClarity Architecture



https://github.com/openclarity/kubeclarity/

Getting Started with KubeClarity

Reference Slide

https://github.com/openclarity/kubeclarity/

Step 1: Add Helm repo

```
helm repo add kubeclarity https://openclarity.github.io/kubeclarity
```

Step 2: Save KubeClarity default chart values

```
helm show values kubeclarity/kubeclarity > values.yaml
```

Step 3: Check the configuration in values.yaml and update (if needed)

Step 4: Deploy KubeClarity with Helm

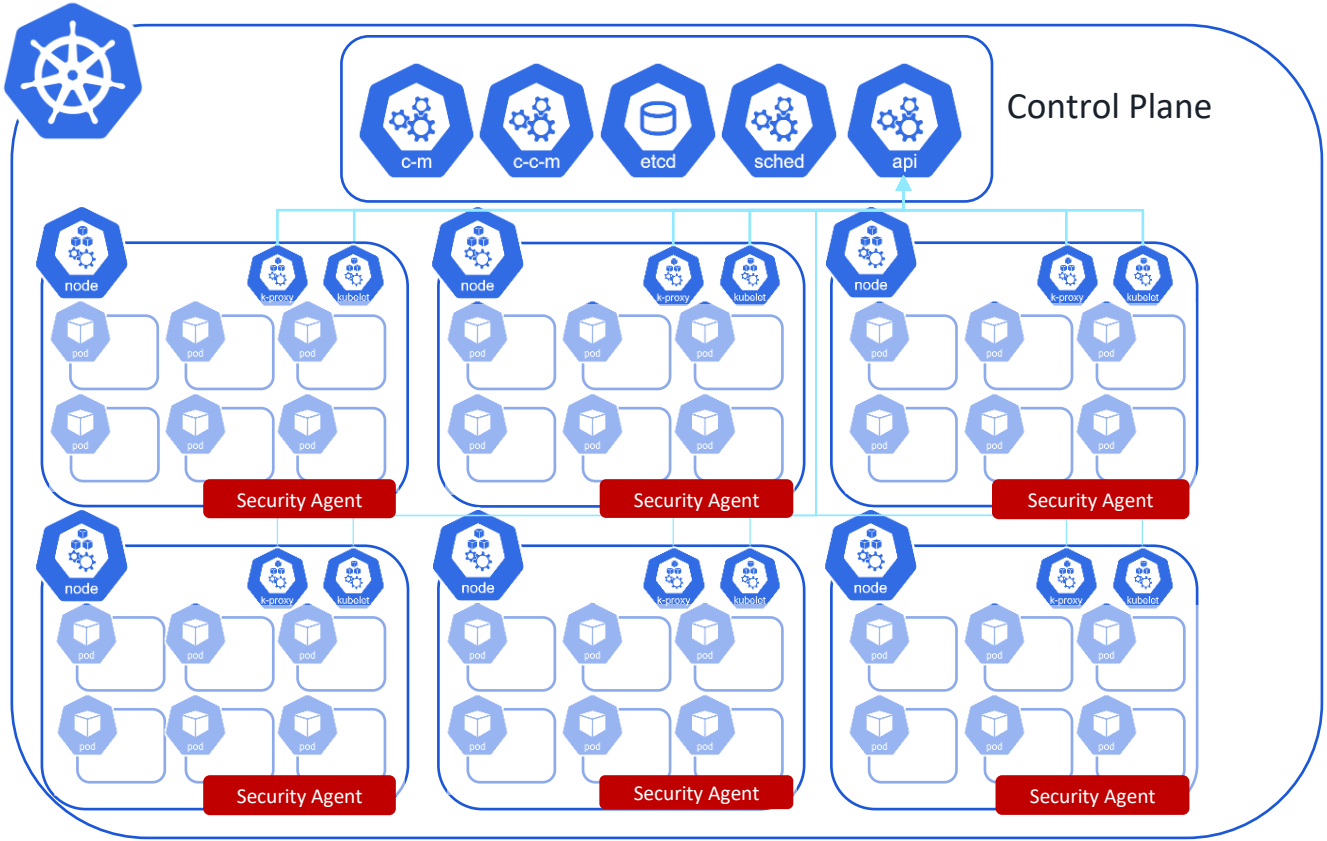
```
helm install --values values.yaml --create-namespace kubeclarity
kubeclarity/kubeclarity -n kubeclarity
```

Step 5: Port forward to KubeClarity UI

```
kubectl port-forward -n kubeclarity svc/kubeclarity-kubeclarity 9999:8080
```

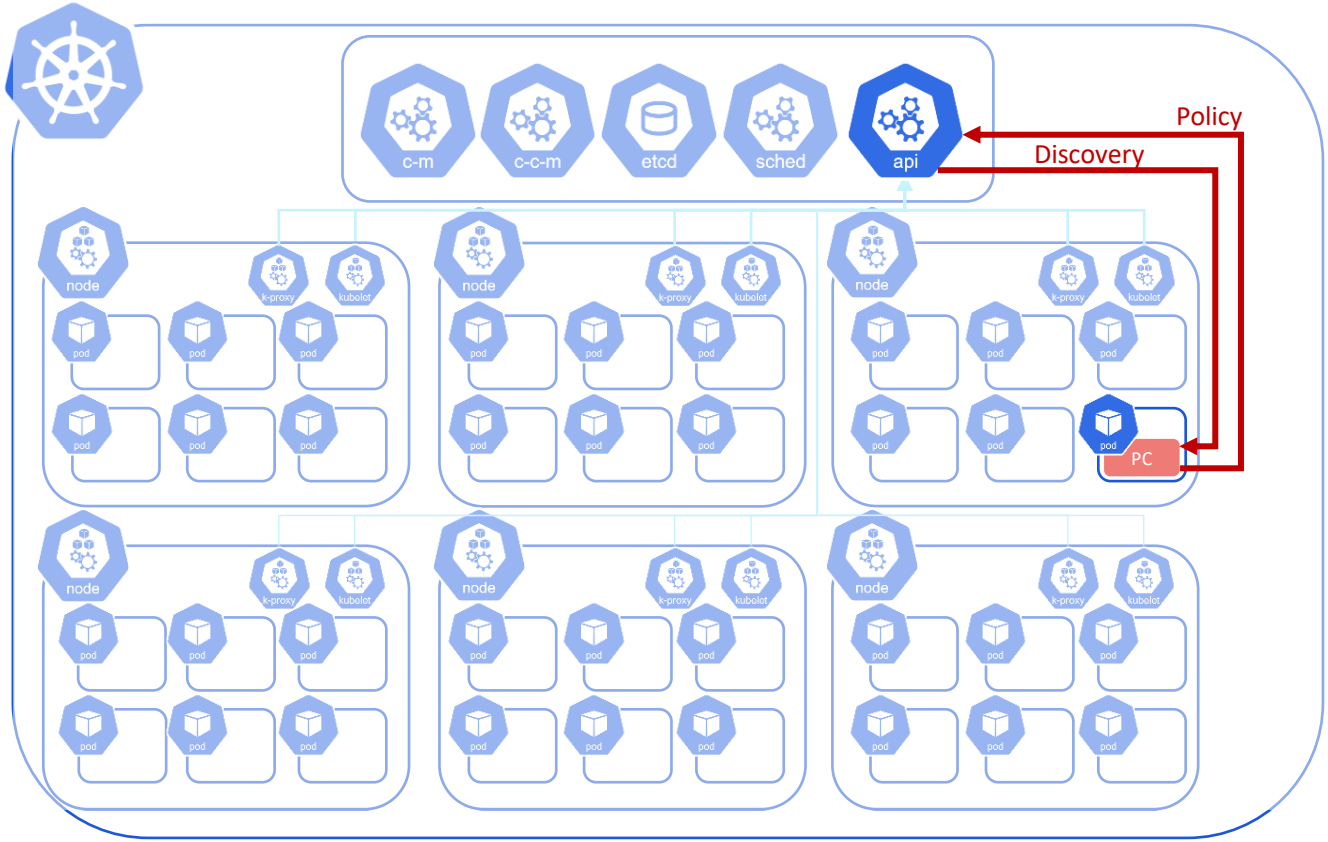
Step 6: Open KubeClarity UI in the browser: http://localhost:9999/

Agent-Based Architecture for Container Security



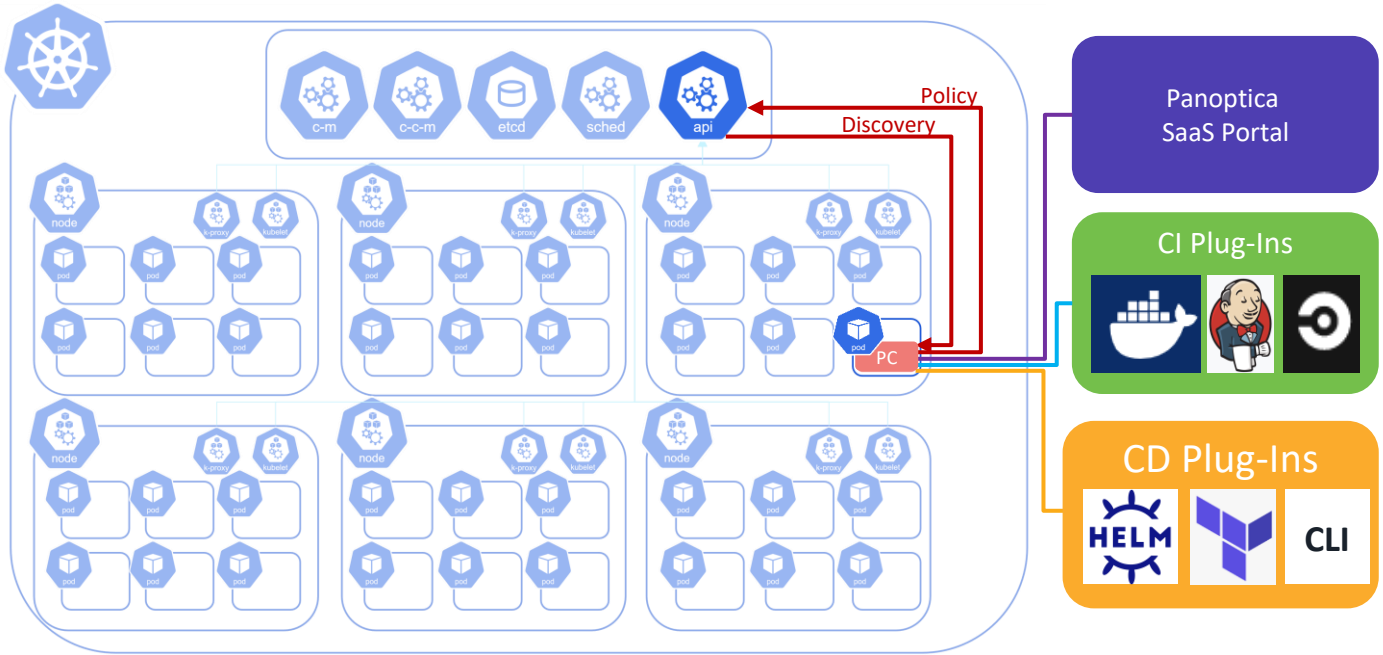
- Many competitors use an agent-based approach to container security
- This approach requires a separate agent to be installed and tailored to each worker node
- Such an approach restricts scalability and performance

Panoptica Architecture for Container Security



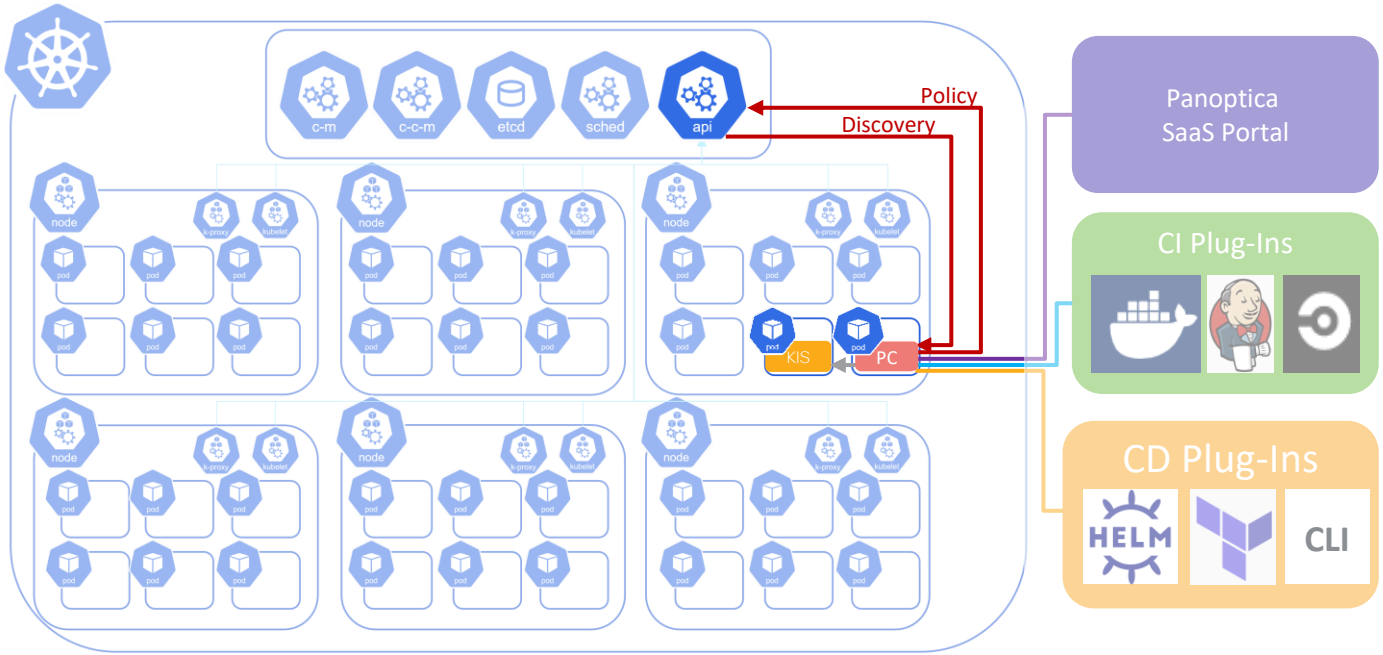
- Panoptica utilizes an agentless approach to container security
- The only dedicated resource that Panoptica requires is a single pod per cluster to serve as the Panoptica Controller (PC)
- Panoptica leverages native Kubernetes Admission Controller capabilities within the Kubernetes API Server to enforce policy

Panoptica CI/CD Integration



- The Panoptica SaaS Portal provides security visibility to operators and allows them to define security policies for their clusters
- Continuous Integration (CI) Plug-Ins ensure Docker CIS Benchmark compliance, as well as check for vulnerabilities in container images, packages and dependencies
- Continuous Delivery (CD) Plug-Ins verify image integrity at deployment, and check for misconfigurations, secrets, SSH keys, etc.

Panoptica Runtime Image Scanning



- Optionally, Panoptica can also perform on-demand image scanning of running containers
- To do so, the Panoptica Controller requests for KubeClarity Image Scanner (KIS) pod(s) to be dynamically spun up
- The KubeClarity Image Scanner scans all container images running in the cluster and reports back to the Panoptica Controller

Container Security Demo

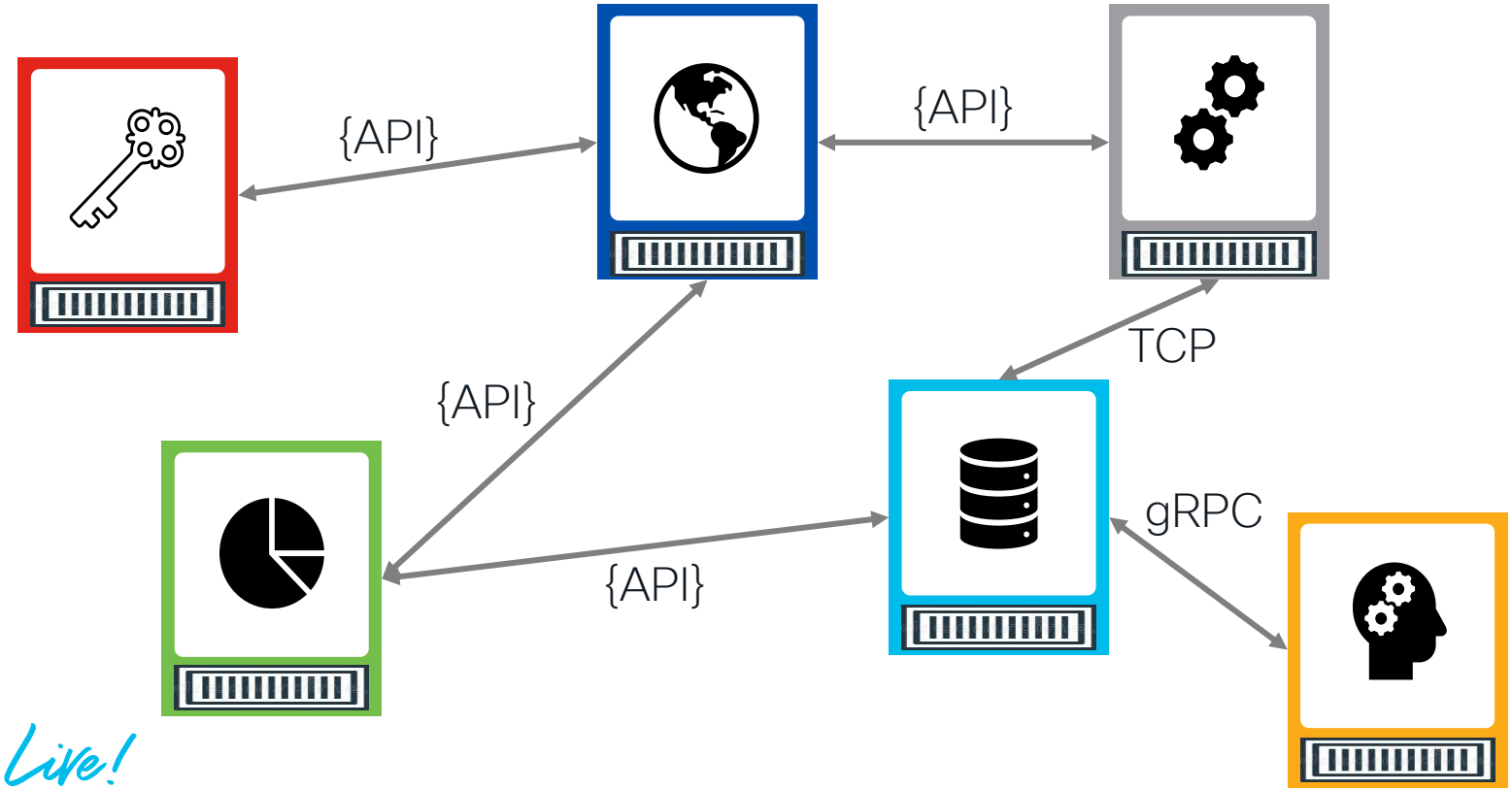
DevNet Zone

API Security

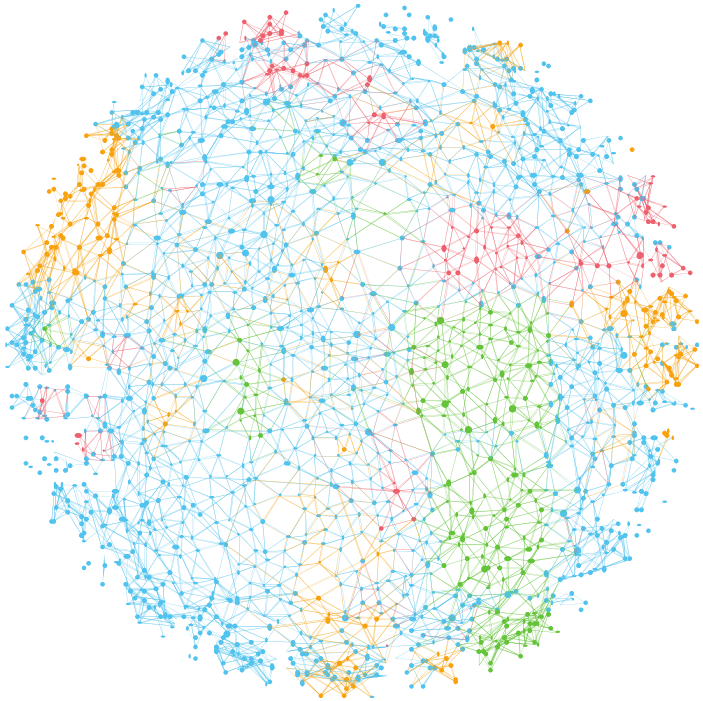
cisco Live!

DevNet Zone

Microservices Architecture



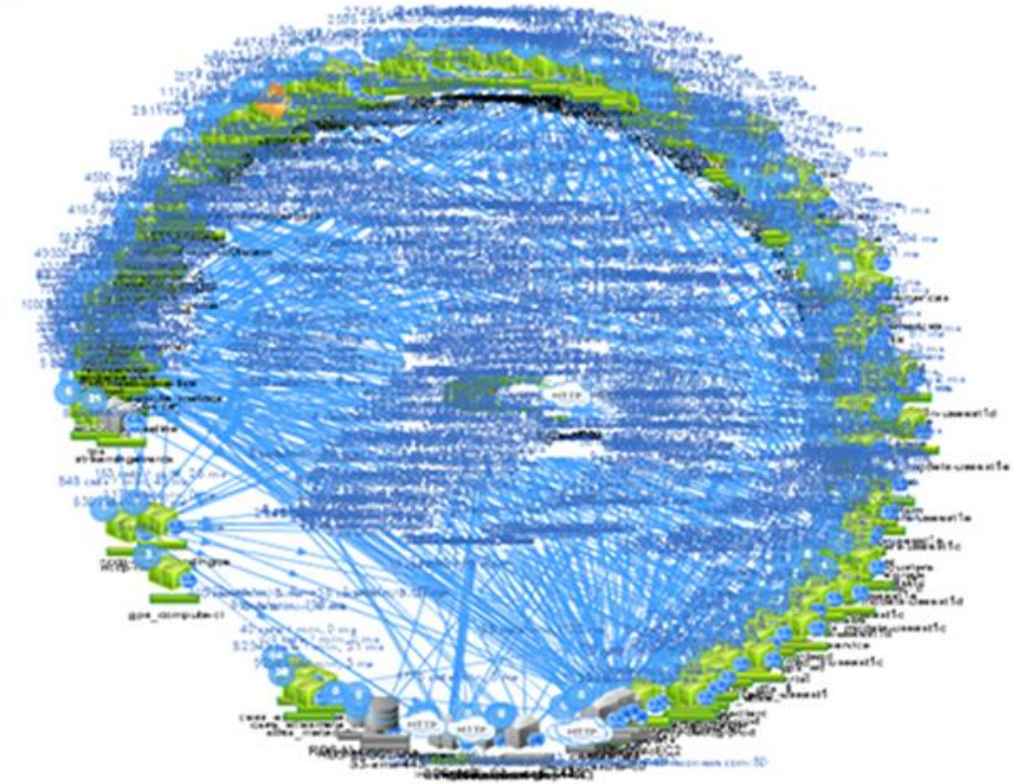
Real World Microservice Architectures



Microservice dependency graph of

monzo

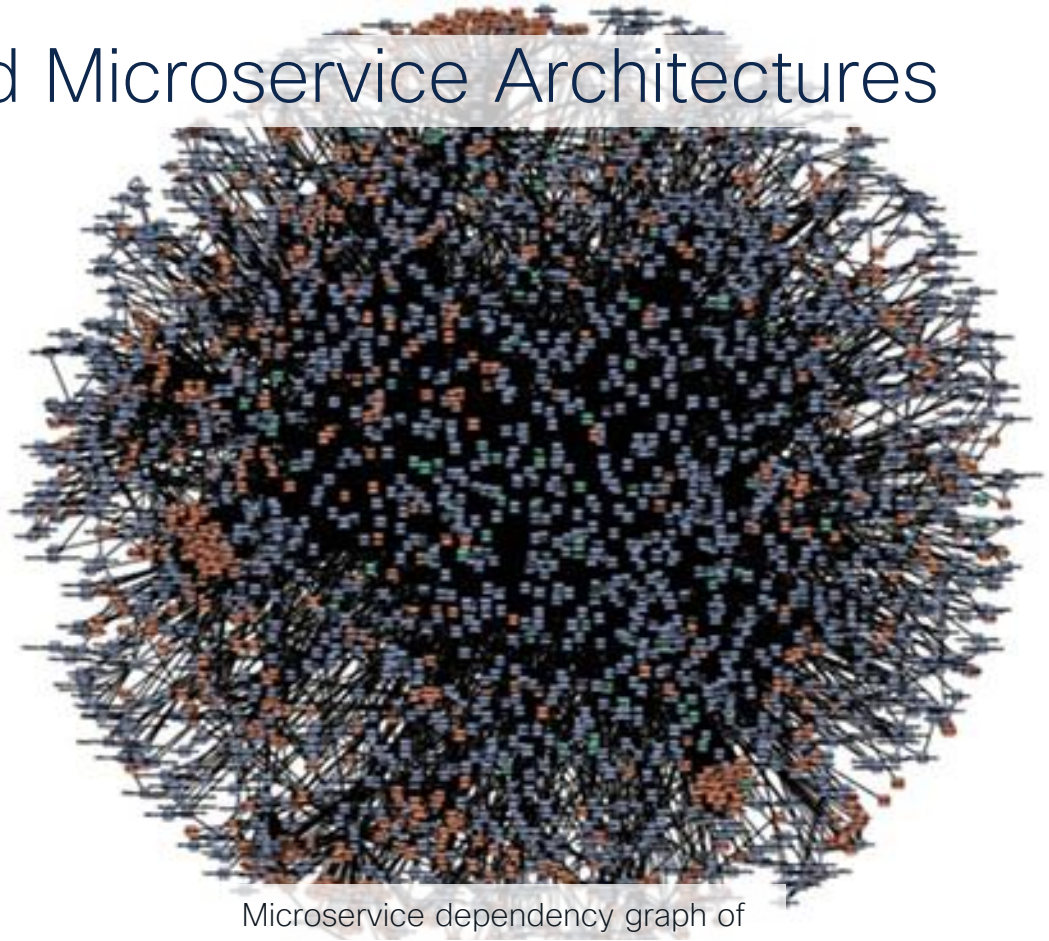
Real World Microservice Architectures



Microservice dependency graph of

NETFLIX

Real World Microservice Architectures



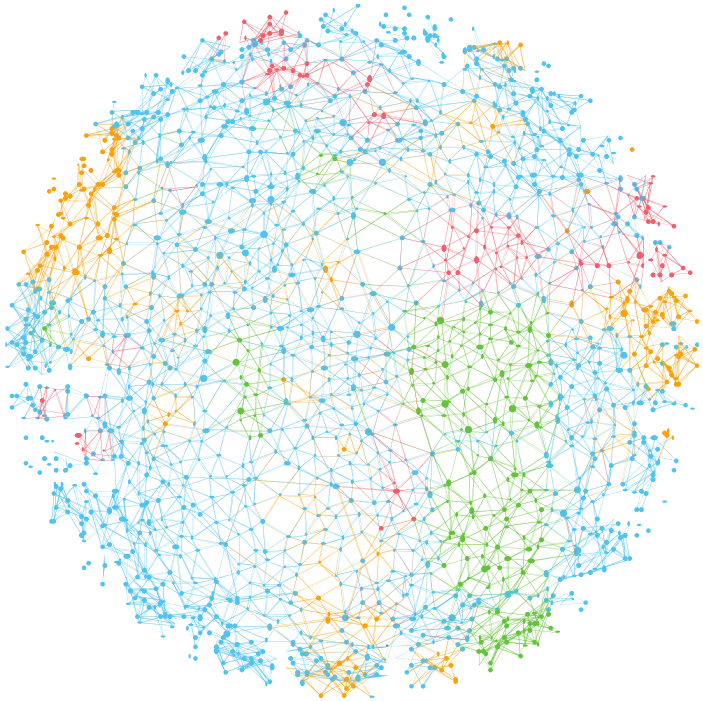
Microservice dependency graph of

amazon.com

API Security Challenges

Choosing Secure APIs

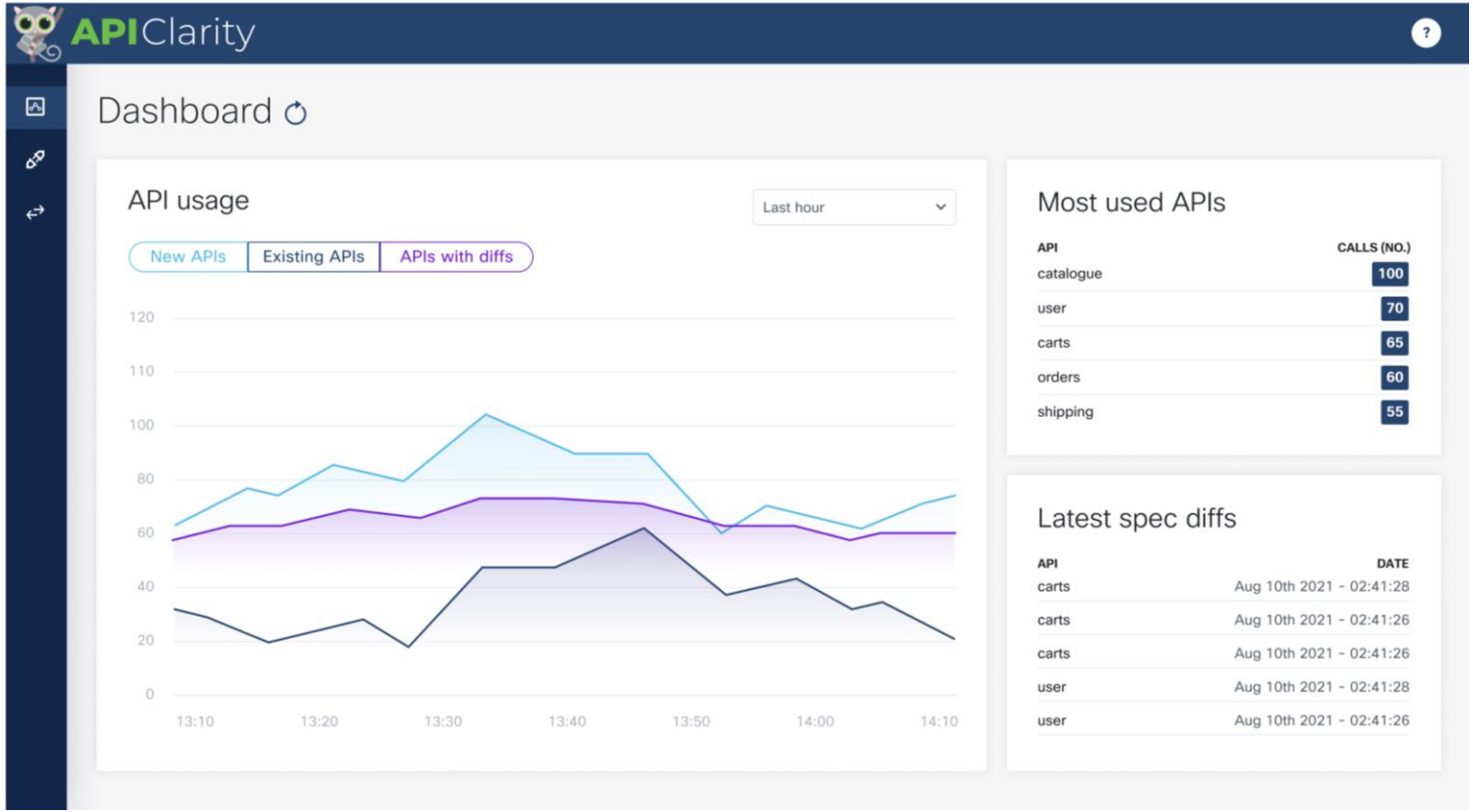
Cloud Native applications rely extensively on internal and external APIs



Key Questions:

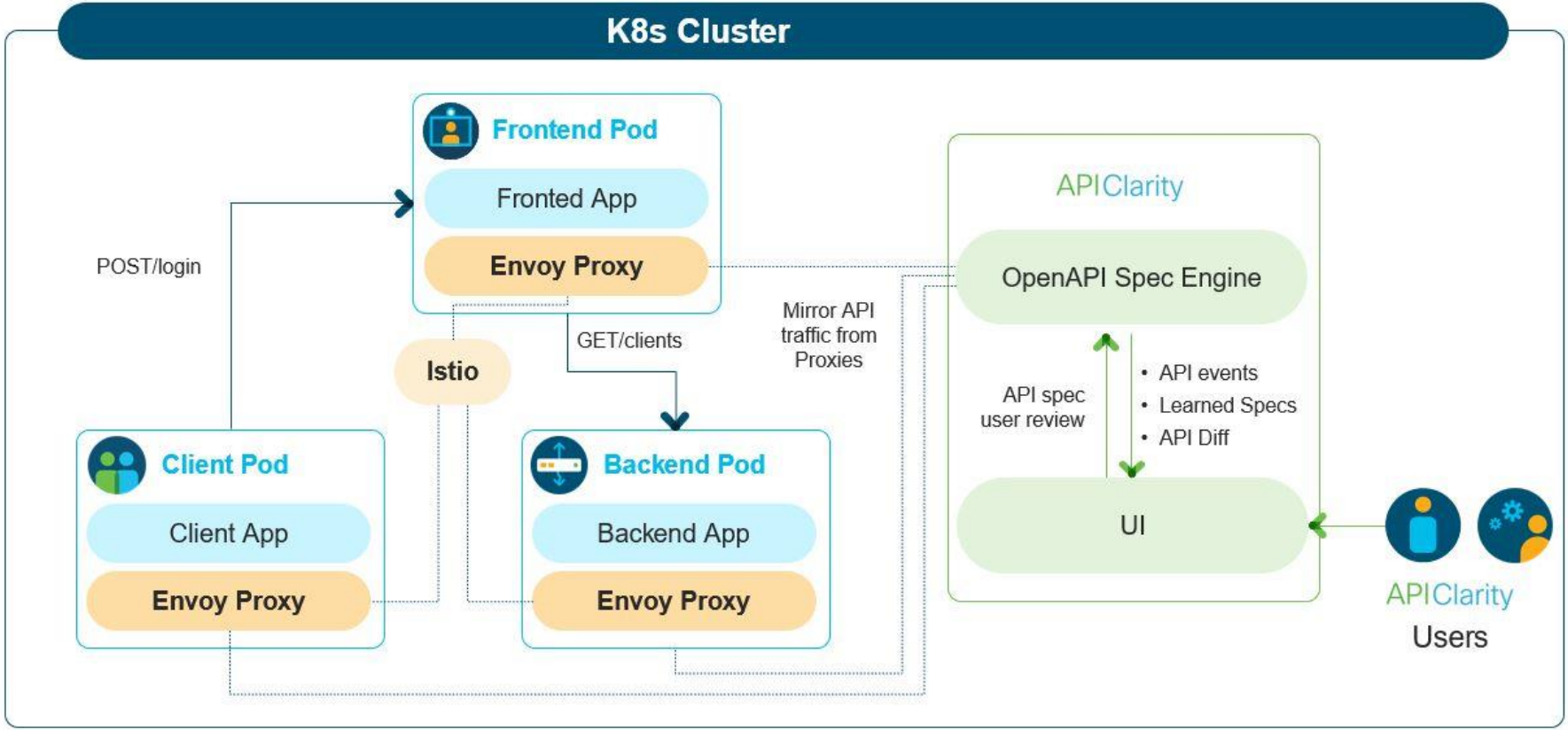
- Are ***my*** APIs vulnerable?
- Do I ***depend*** on vulnerable APIs?
- Do I have ***indirect dependencies*** on vulnerable APIs?

APIClarity Dashboard



https://www.apiclarity.io/

APIClarity Architecture



https://www.apiclarity.io/

Getting Started with APIClarity

Reference Slide

https://www.apiclarity.io/docs

Step 1: Build the APIClarity UI and backend in Docker

```
docker build -t <your repo>/api-clarity .
docker push <your repo>/apiclarity
make ui
make backend
```

Step 2: Deploy APIClarity in your Kubernetes cluster that is running Istio service mesh

```
kubectl apply -f deployment/apiclarity.yaml
```

Step 3: Deploy the Envoy WASM filter for capturing the traffic & run WASM script

```
git submodule init wasm-filters
git submodule update wasm-filters
cd wasm-filters
./deploy.sh <namespace1> <namespace2> ...
```

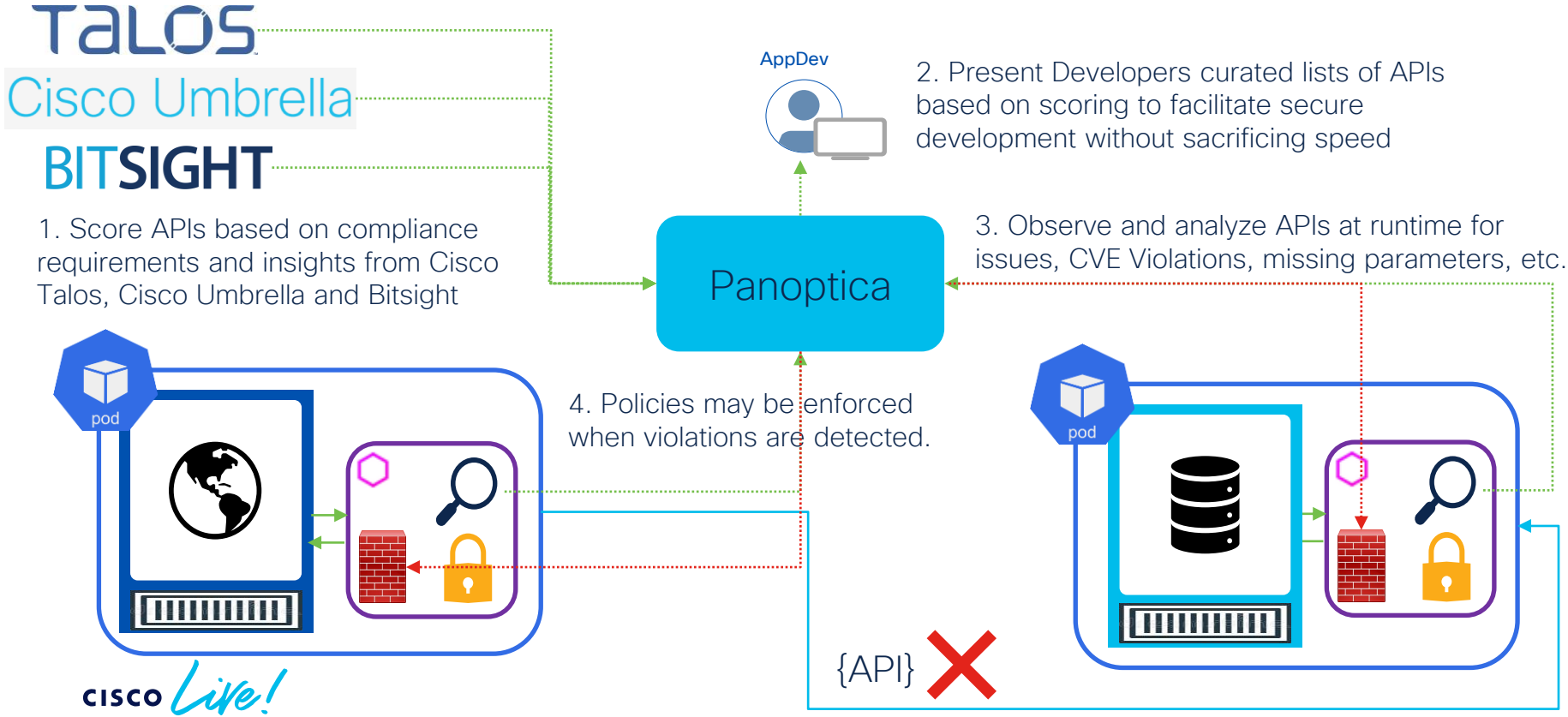
Step 4: Port forward to APIClarity UI

```
kubectl port-forward -n apiclarity svc/apiclarity 9999:8080
```

Step 5: Open APIClarity UI in the browser: http://localhost:9999

Meeting Development Security Challenges

Scoring, Curating, Observing and Enforcing Secure APIs



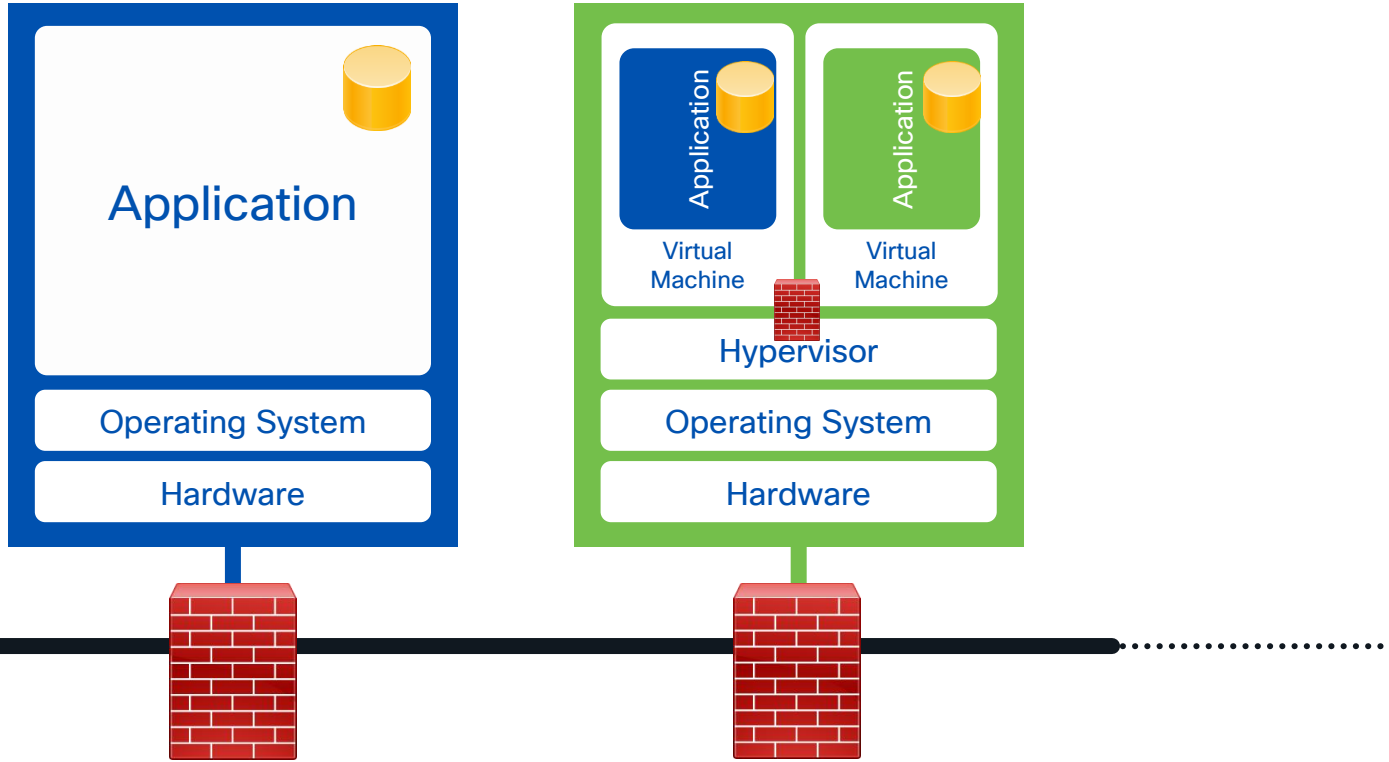
API Security Demo

Cloud Native Network Security

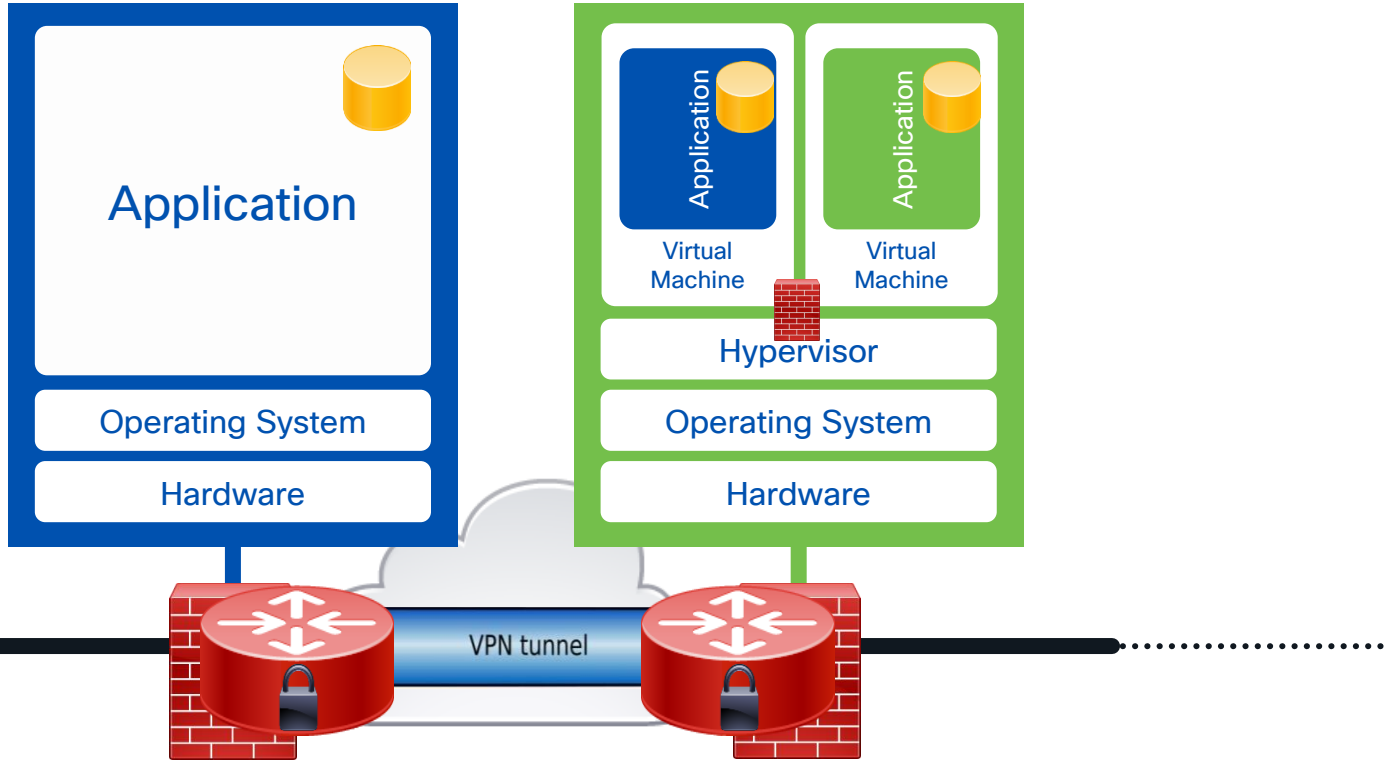
cisco Live!

DevNet Zone

Legacy Application & Network Security

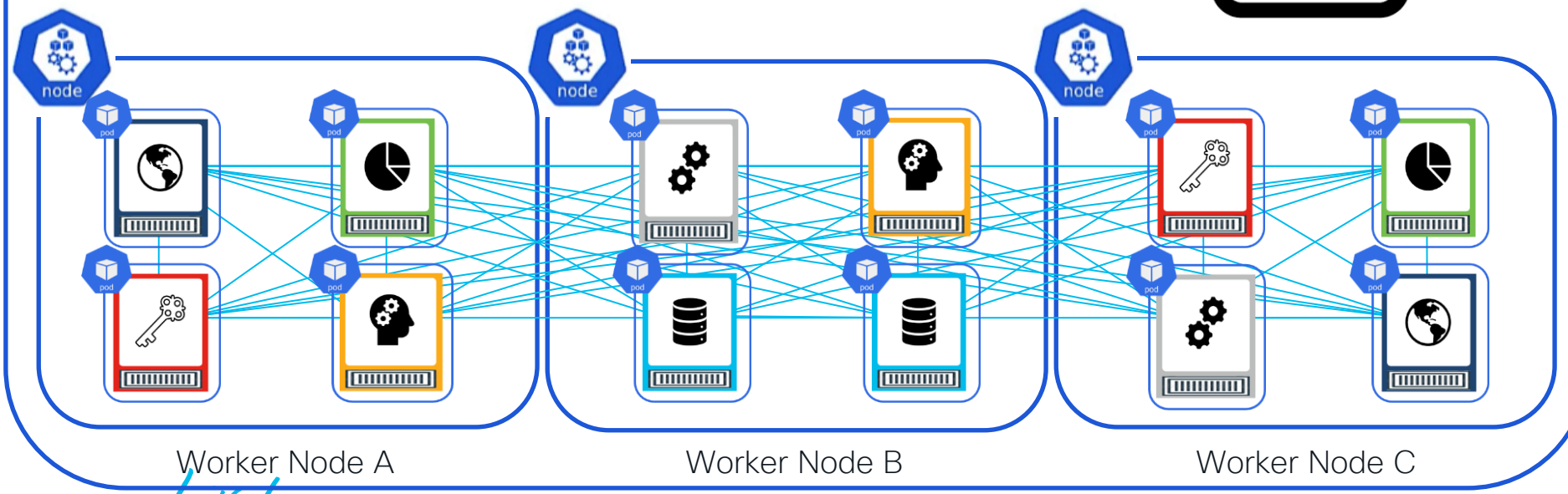


Legacy Application & Network Security

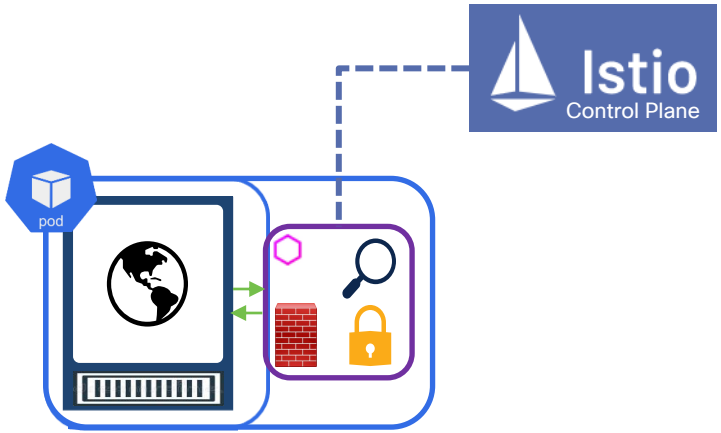


Cloud Native **Networking** Security Challenges

- Any-to-Any intra-cluster communications
- Unencrypted intra-cluster communications
- Unsecure multi-cluster communication
- Unverified service identities

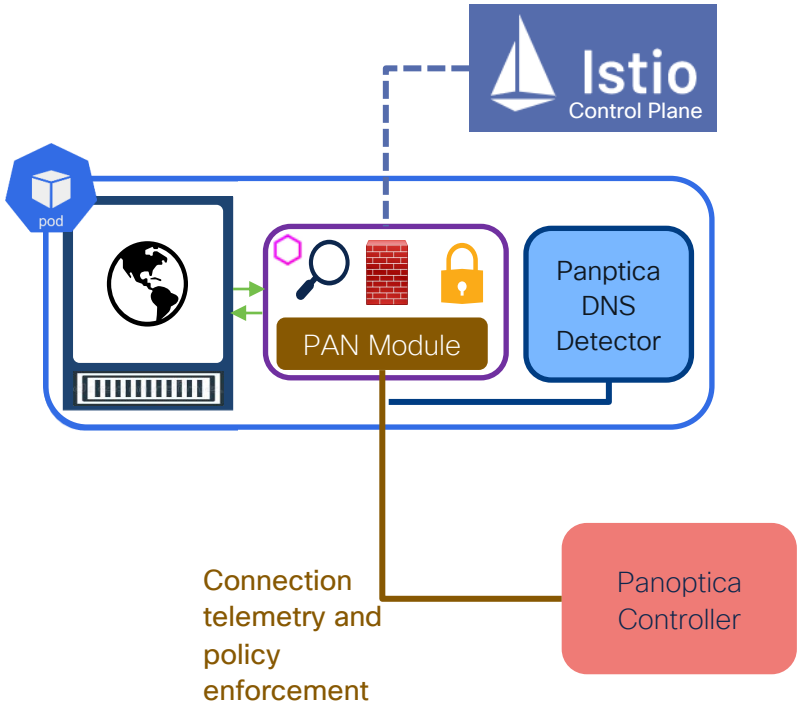


Panoptica Integration with Istio Service Mesh



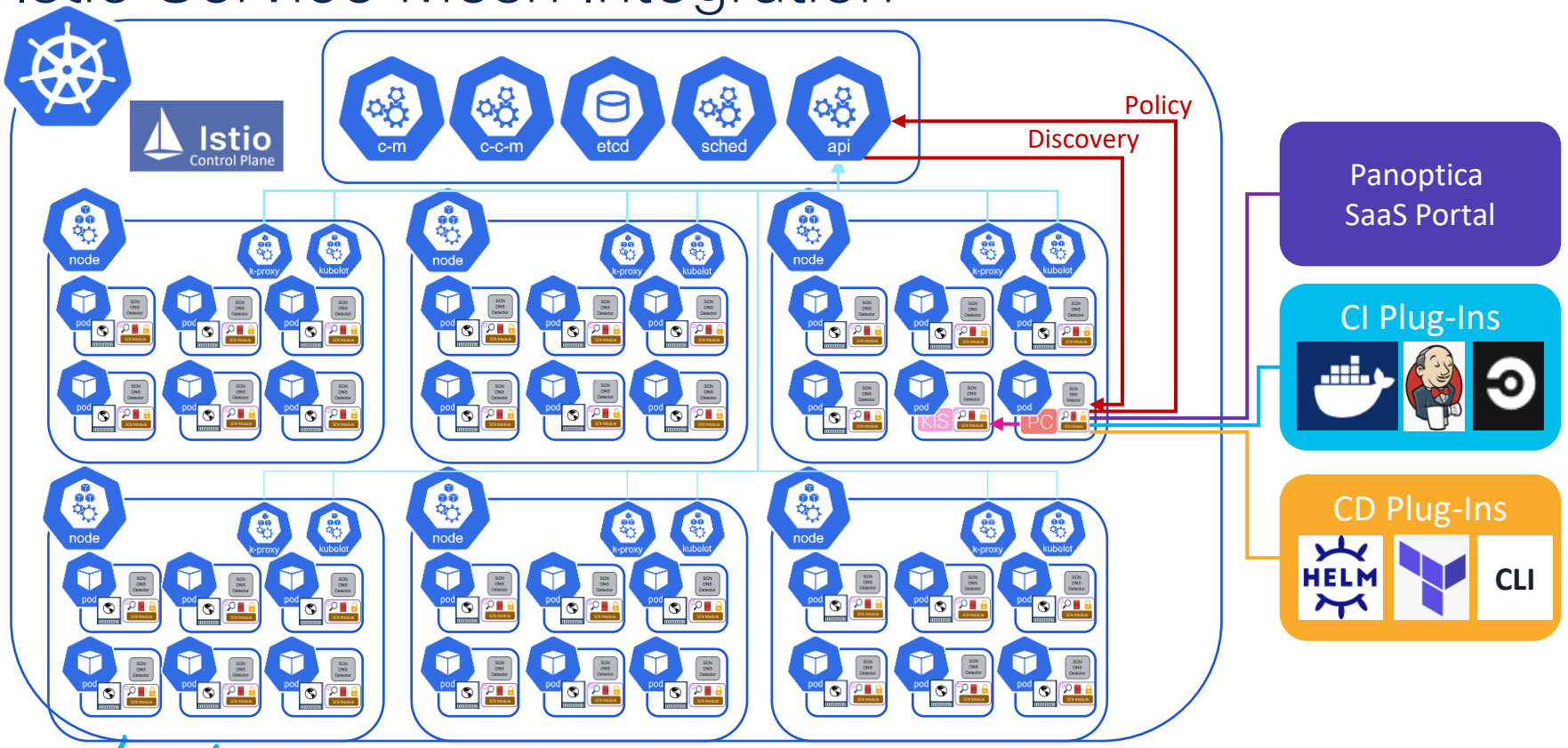
- In a generic Kubernetes environment, a containerized application microservice is usually assigned to a dedicated pod
- However, several common service functions (such as observability, access policy, encryption, load-balancing, traffic management, etc.) can be standardized and enabled by creating a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

Panoptica Integration with Istio Service Mesh (cont)



- Panoptica adds a plug-in to the sidecar proxy to gain observability and to enforce policy (PAN Module)
- Panoptical also adds DNS Detector to the pod to detect and enforce DNS-based policies
  - e.g. no connections allowed to badguys.com
- These modules allow for the Panoptica Controller to observe connections to the container and to enforce connection policies

Panoptica Architecture for Container Security with Istio Service Mesh Integration



Reference Slide

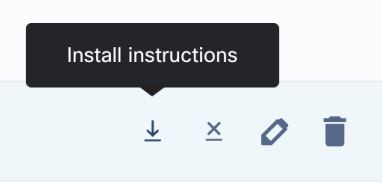
https://panoptica.app/quickstar

Getting Started with Panoptica

Step 1: Sign up at panoptica.app and log in

Step 2: Create a cluster by navigating to the **Deployments** tab and select **Clusters** and then click on **New Cluster**; enter your cluster details and click on **Finish**

Step 3: After you've created your cluster select the download icon so you can deploy it



Step 4: Once the cluster is deployed, it will appear in the K8s Controllers page as Active

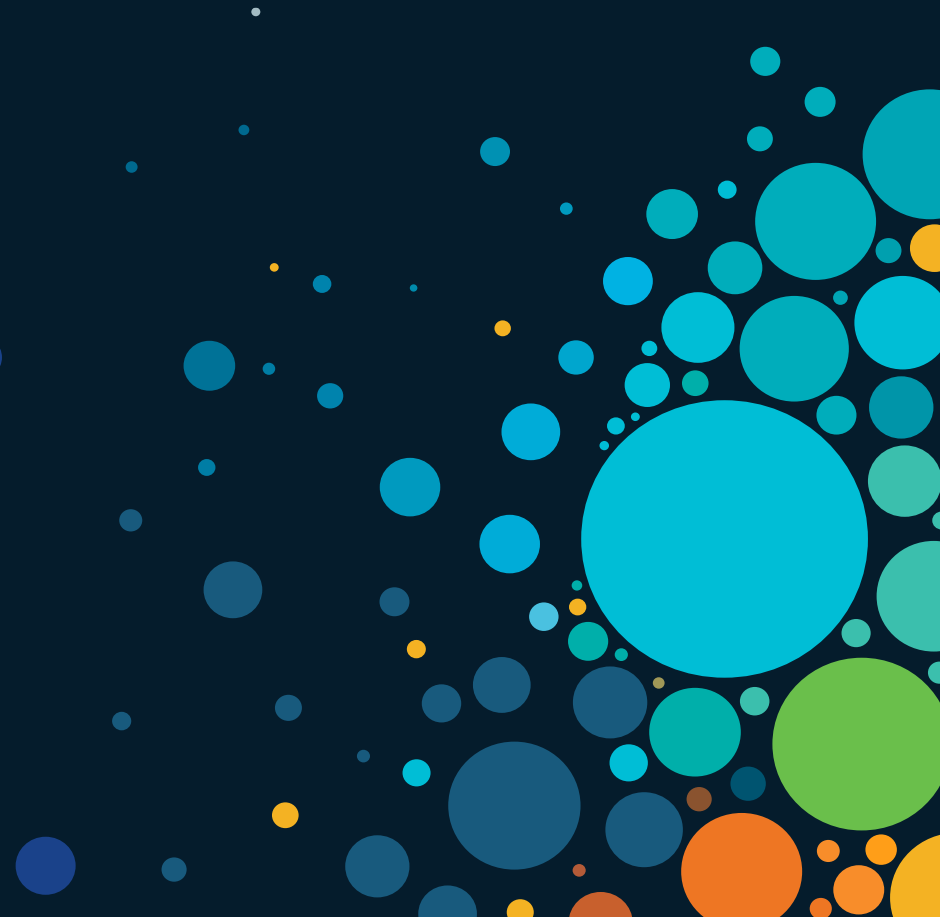
Step 5: Panoptica will begin scanning your images and provide detailed insights about potential risks

Cloud Native Networking Security Demo

cisco Live!

DevNet Zone

Summary and Key Takeaways



Summary & Key Takeaways

- Cloud Native architectures bring many business benefits, but also present new technology and security challenges to operators
- Cisco is applying its extensive expertise and experience in networking and security to the Cloud Native domains
- Cisco has seeded KubeClarity and APIClarity open-source tools to address these challenges
- Also, Cisco is offering Panoptica as an enterprise-grade Cloud Native Security tool via a Free Tier approach as part of a Product Led Growth strategy
  - Panoptica is available for Free Tier (for up to 5 nodes in a single cluster)
  - Additional nodes & clusters can be supported with a license

Next Steps

- Download and get started with KubeClarity and APIClarity
- Sign up and take Panoptica for a free test drive at: https://panoptica.app/
- Continue our discussion at the ET&I booth in the World of Solutions
- Interested in our roadmap? Visit us in the Cisco Innovation Forum
- Follow the latest Cisco Emerging Technologies & Incubation solutions at: https://eti.cisco.com/

Session Surveys

We would love to know your feedback on this session!

- Complete the session surveys in the Cisco Events mobile app. You'll earn some points in the Cisco Live Game and potentially win a prize.
- Complete a minimum of four session and the overall event surveys to claim a Cisco Live cable bag.

Continue Your Education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Expert 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

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals


The bridge to possible
Thank you
cisco Live!
DevNet Zone
#CiscoLiveAPJC

#CiscoLiveAPJC