



DevOPs Journey

Technical Solution Architect

KwaiSeng

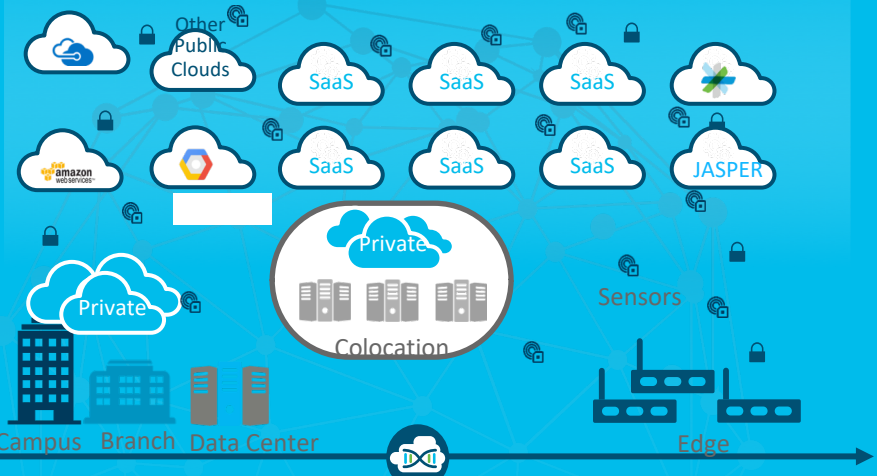


Oct 2018



Hello  World

MULTICLOUD



Some expectations..

Customers want...



Business Agility

24 / 7 / 365



DevOps want...



Freedom to Innovate

Build/ Add new versions easily



ITOps want...



Simplicity & Speed

Multicloud deployment and
management

Specific to Microservices



DEVELOPERS

Consistent K8 experience on Public
Cloud



IT OPS

Support Developers Current and
Future Needs



SECURITY

Visibility, Threat Detection and
Control

- Kubernetes As A Service

Cisco Container Platform



Turnkey Solution
For Production-Grade Container
Environments

Native Kubernetes (100% Upstream)

Direct updates and best practices from open source community

Hybrid Cloud Optimized

Integrated

Networking | Management | Security | Analytics

Flexible Deployment Model

VM | Bare metal \leftrightarrow HX, ACI | Public cloud

Easy to acquire, deploy & manage | Open & consistent | Extensible platform | World-class advisory & support

Cisco Container Platform Feature Set

Kubernetes-as-a-Service



Setup

- Deploy Kubernetes clusters on HyperFlex IaaS (VMware)
- Container Networking (Contiv / ACI)
- **Persistent storage (Flex Driver)**
- Layer-4 and Layer-7 load balancing
- **High availability**



Consume

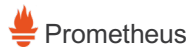
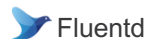
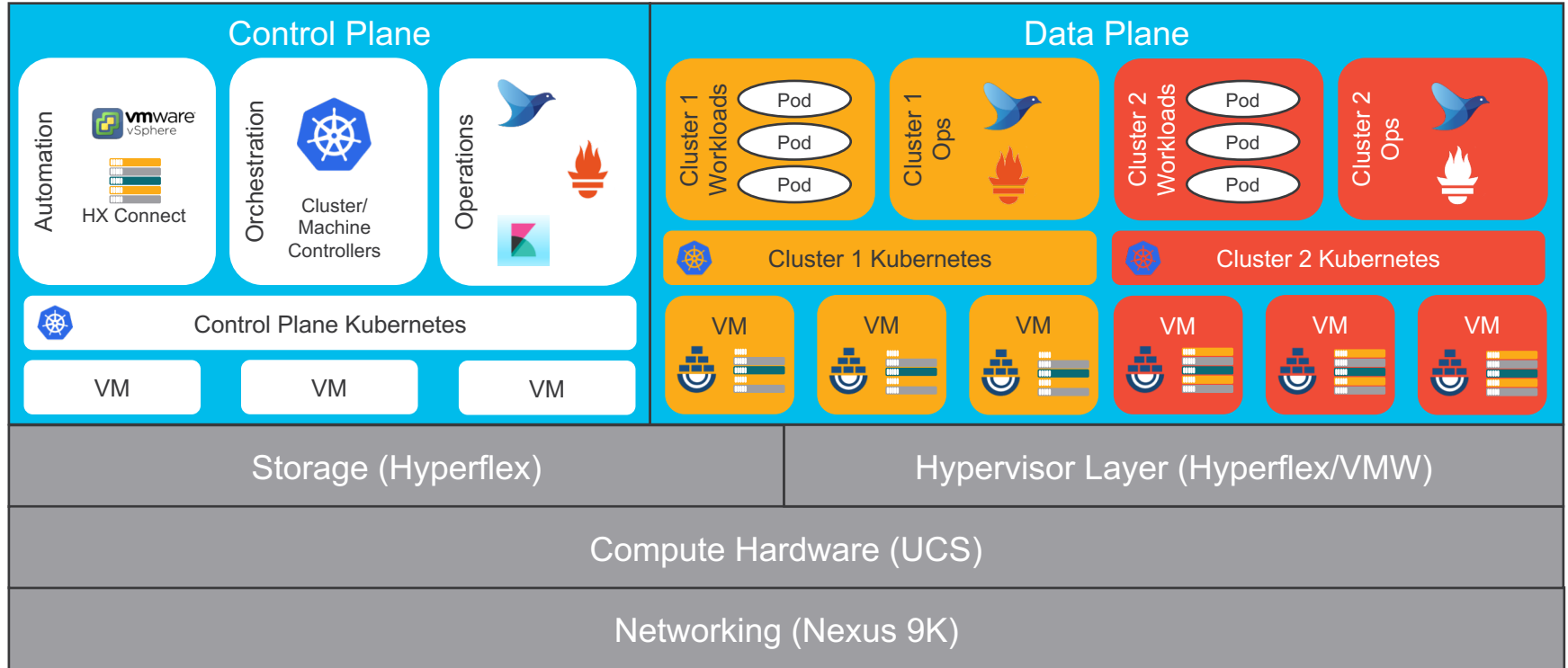
- Authentication with Active Directory
- **Role based access control**
- Communication between containers and external VMs / BMs
- UI – Kubernetes, API
- Security (policies, encryption)



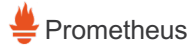
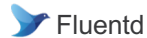
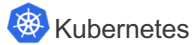
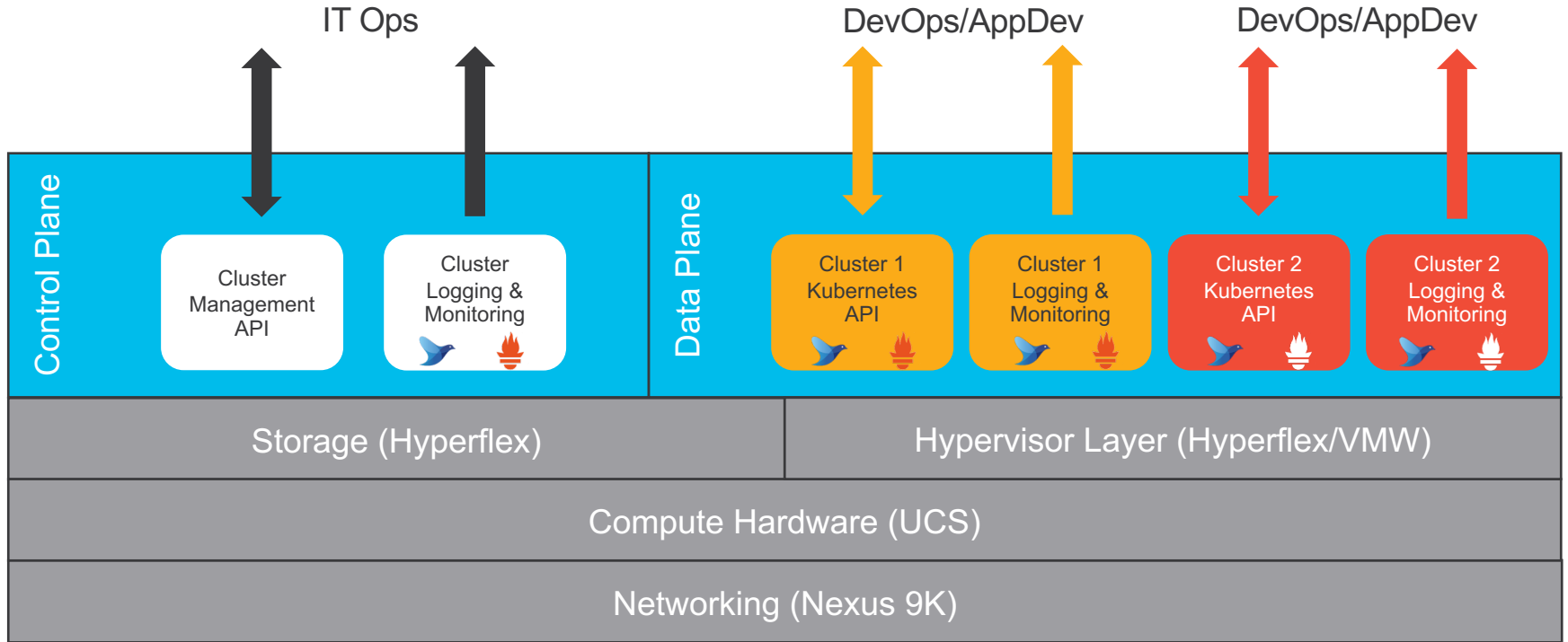
Manage

- **Add / remove Kubernetes nodes**
- Lifecycle management (OS updates, Kubernetes upgrades)
- Monitoring (Prometheus)
- Logging (EFK)




Cisco Container Platform Stack



Interacting with Cisco Container Platform

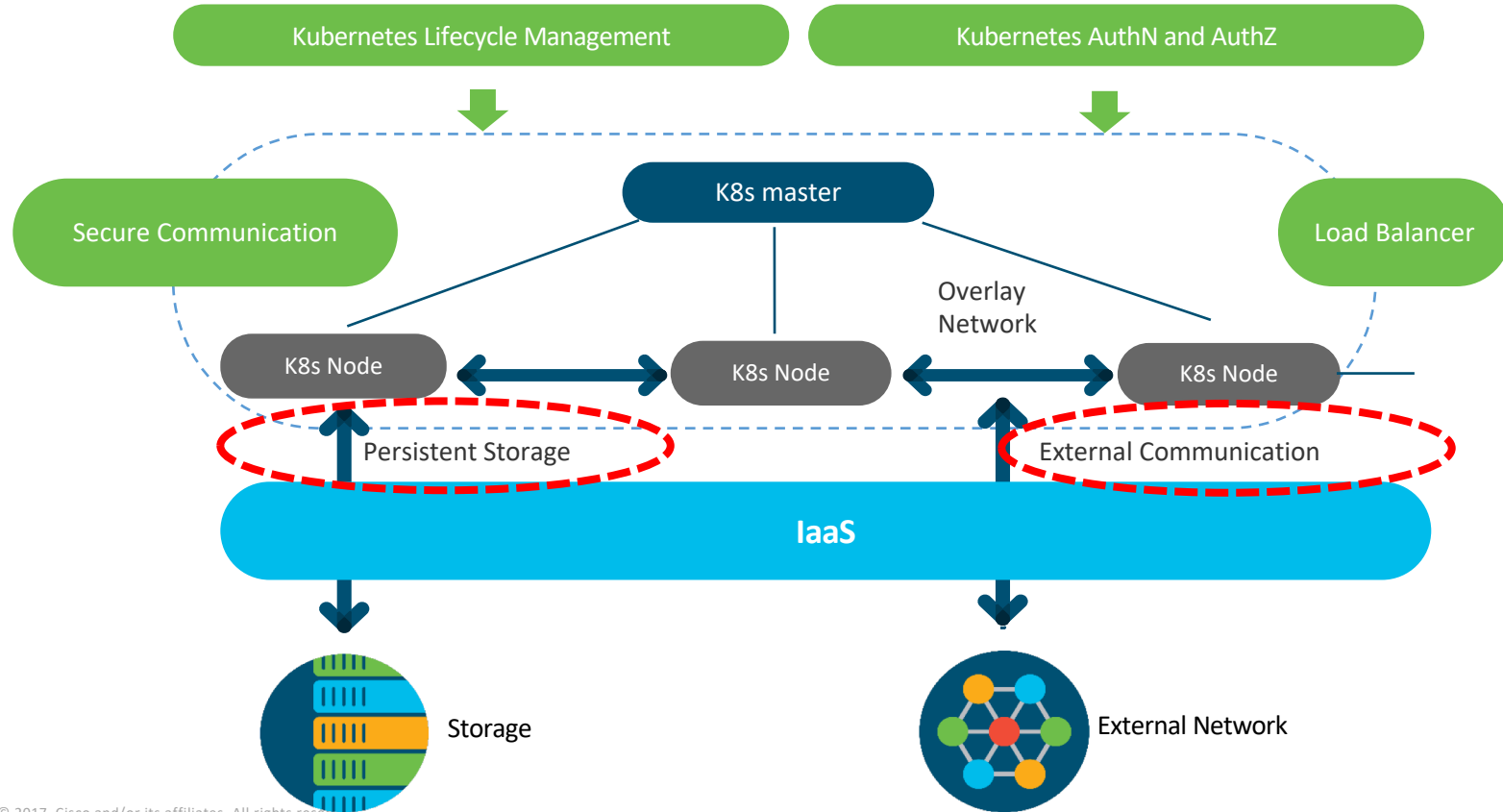


The Problems CCP is Solving

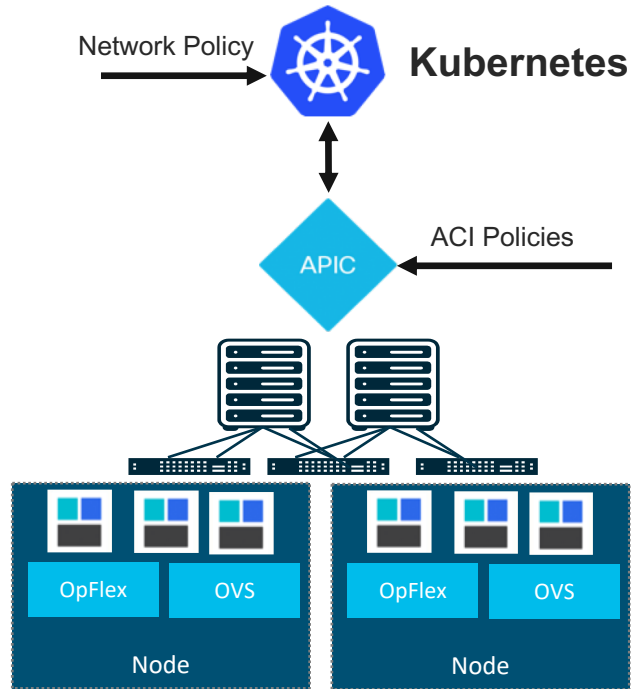
 OPERATIONS	Automated repetitive tasks & simplified complex ones	Open architecture delivering high performance and security for containers at scale	Fully integrated CaaS with lifecycle management for all software and hardware stack elements
 DEVELOPMENT	Cloud Native on premise built on the best Opensource and best OTS	Build Your Own Pipeline on K8S with the tools and methodologies you love	Leverage both on premise services for application development
 BUSINESS	Accelerate Cloud Native transformation and application delivery	Single Support Contract for Whole Stack	24/7/365 Business Agility

- Kubernetes Ready Infrastructure

Kubernetes Ready Infrastructure



Kubernetes Contiv-ACI Solution Overview



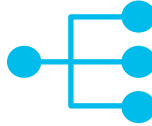
Technical Description

- Network policies of Kubernetes supported **using standard upstream format but enforced through OpFlex / OVS using APIC Host Protection Profiles**
- Kubernetes **app configurations can be moved without modification** to/from ACI and non-ACI environments
- **Embedded fabric and virtual switch load balancing**
 - PBR in fabric for external service load balancing
 - OVS used for internal service load balancing
- **VMM Domain for Kubernetes**
 - Stats per namespace, deployment, service, pod
 - Physical to container correlation

Why deploy K8 on ACI?



Unified networking:
Containers, VMs, and
bare-metal



Micro-services
load balancing integrated in
fabric for HA / performance



Seamless integration of
Kubernetes network
policies and ACI policies



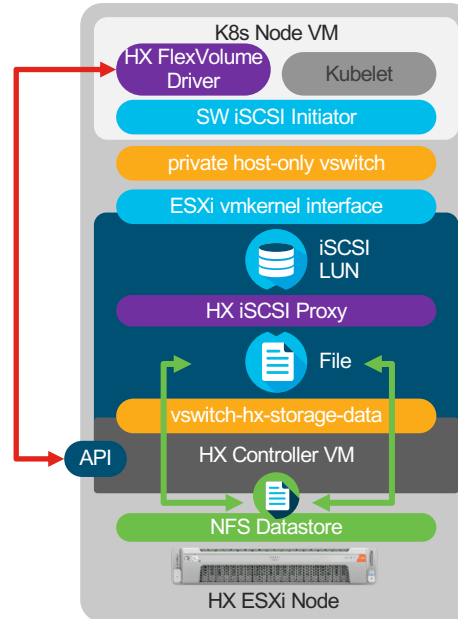
Visibility: Live
statistics in APIC per
container and health
metrics



Secure multi tenancy
and separation of
concerns

HyperFlex 3.0 FlexVolume Driver

- Integration with Kubernetes FlexVolume Driver framework
- Engineered based on close consultation with GCP & Kubernetes teams
- Enables developers to leverage HyperFlex storage for stateful container storage
- Purpose built for Container scale, Performance, Data Svc & Resiliency requirements



Why Deploy HX with K8



Visibility

Single Dashboard



Integrated Workflow

IT, Developer



Data Protection

Build In Data Persistency across
Physical Nodes



Build In Replication

Active Active Replication
Across DC's



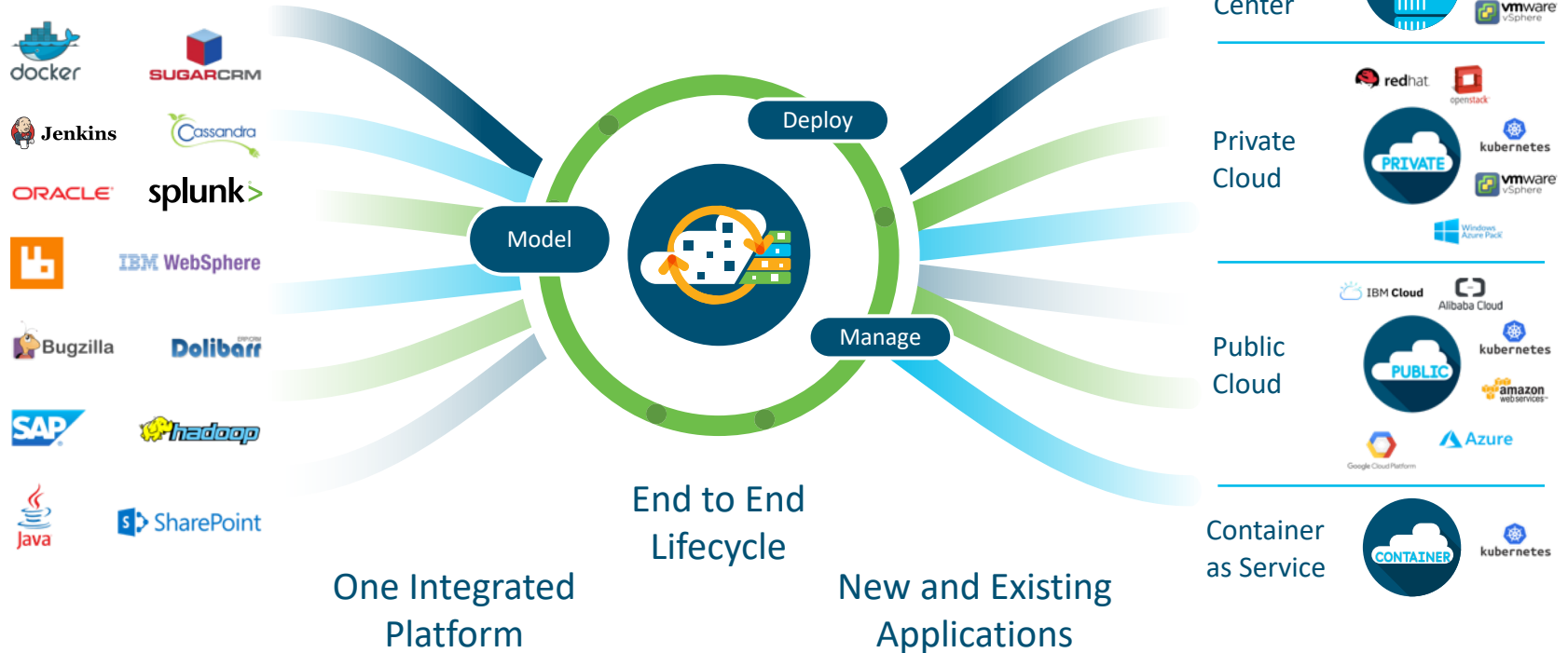
Horizontal Scalability

Easy Add/Remove Nodes

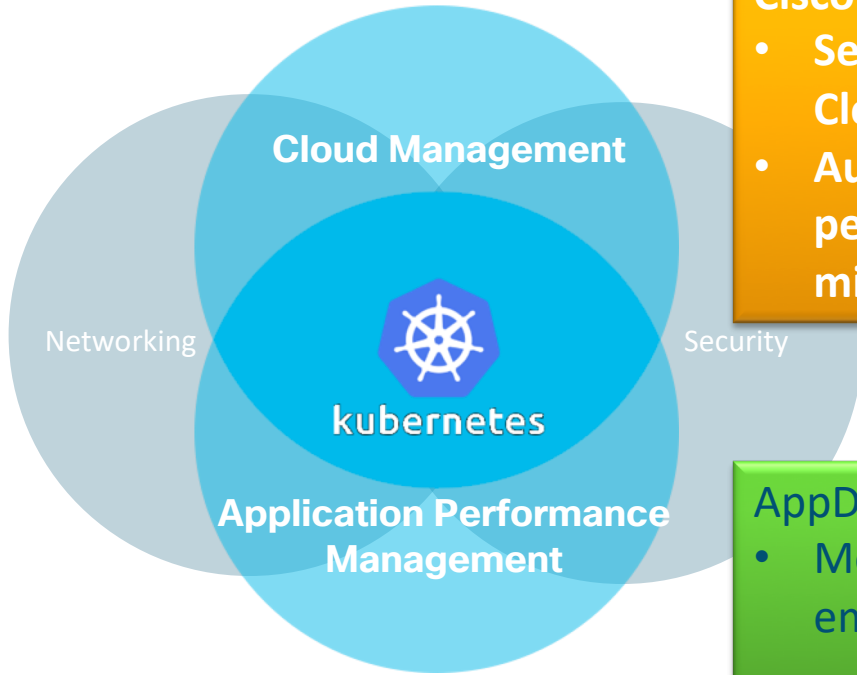
- Modelling Application

CloudCenter – Multicloud Management Platform

Securely Model, Deploy, and Manage Anywhere.



Intelligent Application Orchestration



Cisco CloudCenter

- Seamlessly Application Deployment Across Clouds
- Automate scale out to preserve performance and minimize cost

AppDynamics

- Monitor Application ecosystem and identify emerging issues

CloudCenter & Kubernetes



Enables portability
across Kubernetes
clusters with automated
visibility



Unified governance and
security for VMs and
containers



Accelerate adoption of
containers and
Kubernetes

DEMO

Add Cloud

DESCRIPTION

* Select Cloud Provider

PUBLIC CLOUDS

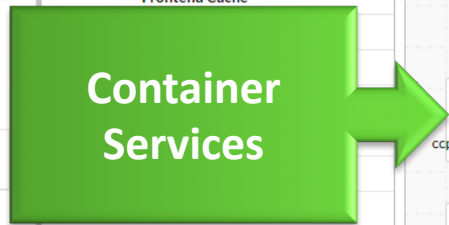
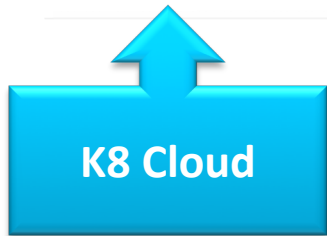
- Alibaba Cloud
- amazon web services
- Azure AzureRM
- dimension data Cloud
- Google cloud platform
- IBM Bluemix

PRIVATE CLOUDS

- Microsoft Azure Stack
- CISCO Cisco UCS
- openstack
- VMware Private Cloud
- vmware vCloud Director
- Windows Azure Pack

CONTAINER CLOUDS

- kubernetes



Edit "Cisco-Shop" Application Profile

Version: 0.1 (Revision: 2)

Basic Information Global Parameters Topology Modeler

Services

- Orchestration
- OS Service
- Custom Service
- File System
- Workflow
- Frontend Cache

Topology Modeler

Diagram showing application components: ccp_fro..., ccp_cat..., ccp_ord..., ccp_use..., ccp_car..., ccp_que..., ccp_pay..., ccp_ship..., and their dependencies on services like Apache2, Geronimo3, IIS, Jetty, and Ruby On Rails.



Hybrid Cloud Solution Use Cases

1

Cloud application consumes data from a legacy application running on-premises



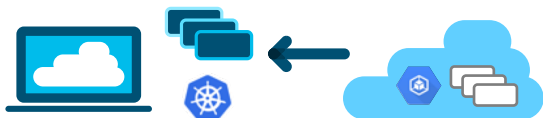
Developers: Legacy applications can participate in a cloud native architecture

IT Admin: Support developer's current and future container needs

Security Team: Maintain and enhance control in containers, across multiple environments

2

An application running on-premises consumes leading edge cloud services



Developers: Use the latest cloud services to differentiate their application

IT Admin: Production-ready Kubernetes solution installed and maintained

Security Team: Extend visibility, threat detection and control

3

Seamless CI/CD workflow for containerized apps across both cloud and on-premises



Developers: Optimize my development lifecycle wherever it makes sense, not location dependent

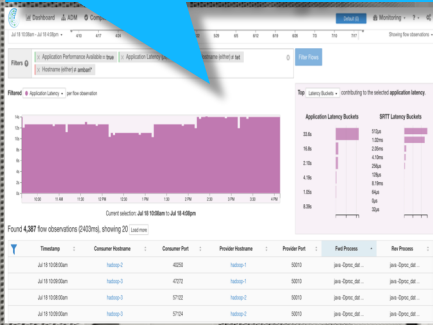
IT Admin: Ensure services can reach other services between on-premises and cloud

Security Team: Insights into network traffic between on-premises and cloud

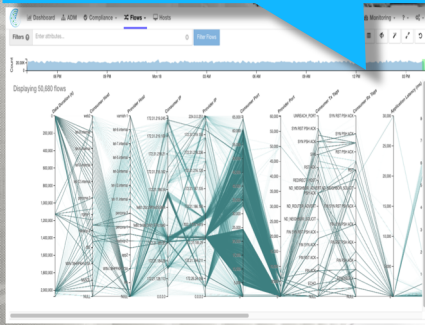
- Visibility

Visibility to Optimize Security Policy

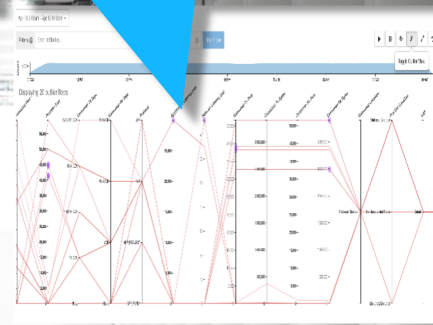
What's going on now and 6 months ago?



What's normal /Baseline?



What's outlier?



How to reduce MTTI?

Jun 7 02:16:00 pm (+08)

Provider 0

Flags PSH ACK

Byte Count 31,200 (so far) 6,010 (6,084 so far)

Packet Count 64 (64 so far) 63 (64 so far)

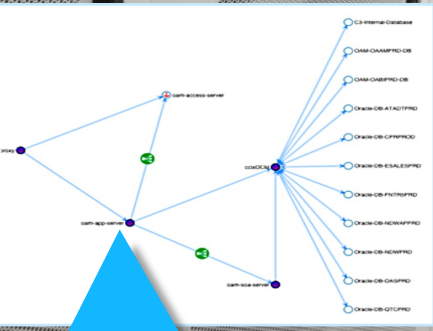
SRTT 53.6ms

Est. Network latency 26.9ms

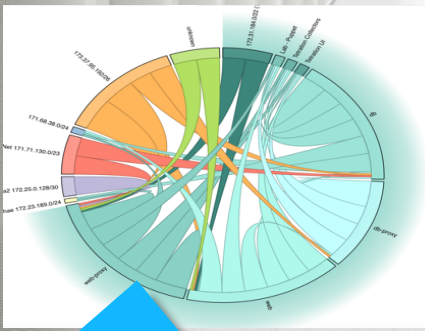
Application latency 1.35ms

Process tet-sensor-f-sensor.conf

```
log/latency/collector/tet_collector--config_file
log/latency/collector/collector.config--
timestamp_flow_info--logtsid--
max_num_ssl_sw_sensors 63000--
enable_client_certificate true--write_empty_files
true
```



Who is talking to who?



Real time Whitelist Policy?

Quick Analysis

Absolute Policies

Default Policies

Priority	Action	Consumer	Provider	Services
100	ALLOW	pod02-haproxy01	Default	UDP: 53 ...
100	ALLOW	pod02-epg0	Default: Testation-#s	TCP: 443 ...
100	ALLOW	pod02-epg0	Default: Shared	UDP: 111 ...
100	ALLOW	Default	pod02-redist01	TCP: 22 ...
100	ALLOW	pod02-ocp0	pod02-redist01	TCP: 6379 ...
100	ALLOW	pod02-ocp0	Default: Testation-#s	TCP: 443 ...
100	ALLOW	pod02-redist01	Default	ICMP ...
100	ALLOW	Default	pod02-haproxy01	ICMP ...
100	ALLOW	Dchub	pod02-ocp0	TCP: 80 ...

Catch All Policy DENY

How to enforce policy to heterogenesis env.?

Endpoint: 172.31.185.156

Hostname memcached-1

Cluster caching

Route Tags

Distinctive Processes (1)

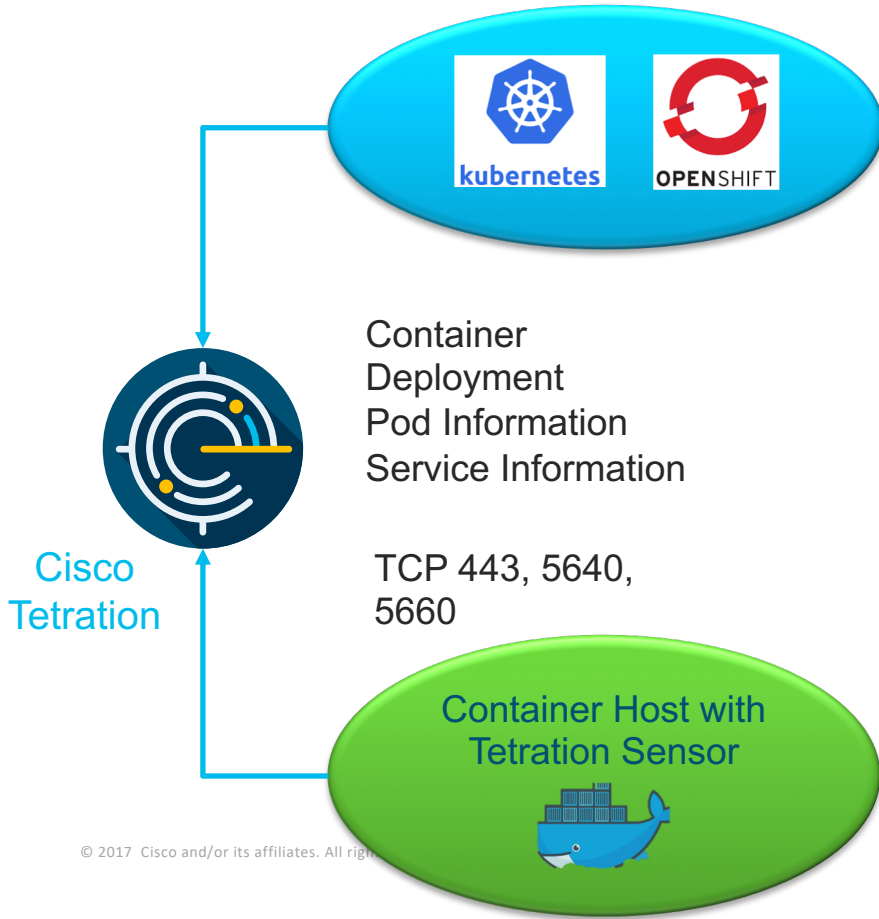
Provides (4)

TCP : 22 /usr/sbin/sshd
 UDP : 123 /usr/sbin/ntpd
 TCP : 11211 /usr/bin/memcached
 UDP : 11211 /usr/bin/memcached

Consumes (6)

How to hardenize servers/VMs?

Knowing what happen with the containers..



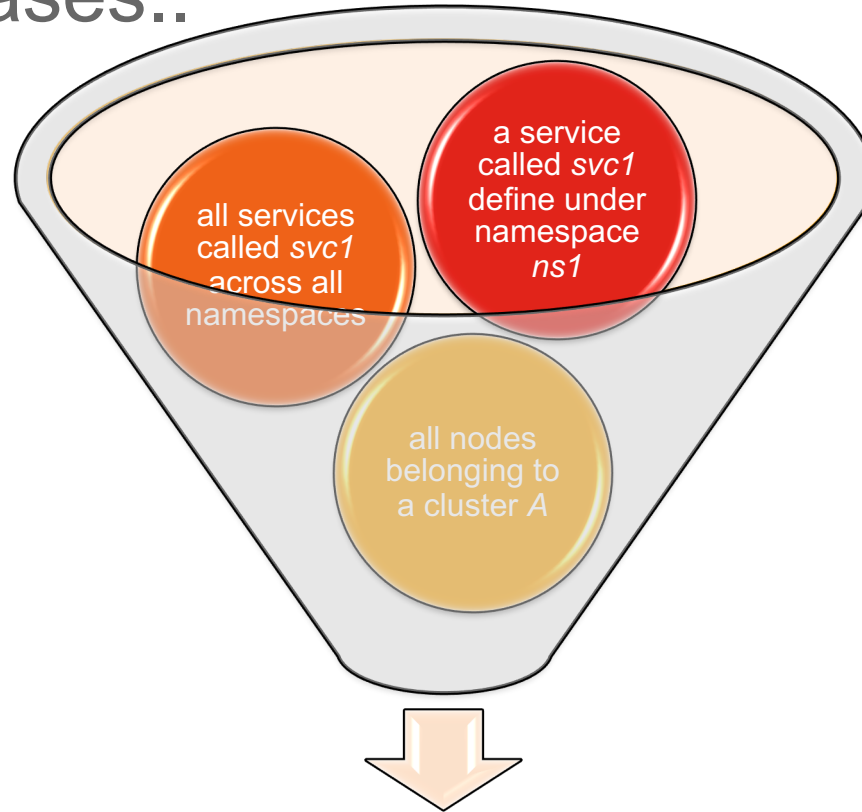
Container
Deployment
Pod Information
Service Information

TCP 443, 5640,
5660

- Container deployment
- Container Pods (IP, Meta data)
- Tags

- Flow information
- Process inventory
- Software inventory in the container host

Some Sample Cases..

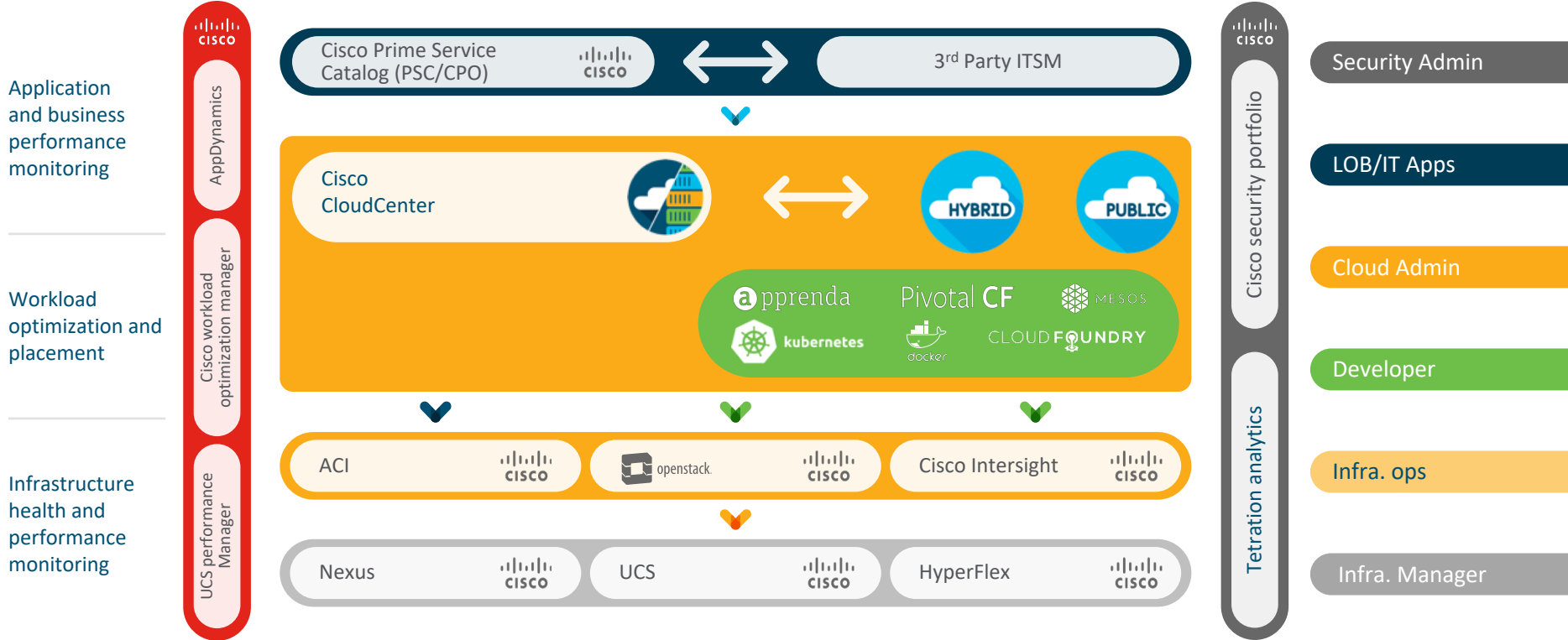


What about Containers that
run in my DC?



- Kubernetes as a Service
- Consistent Interaction
- Performance
- Security Policies
- Visibility

Cisco Data Center Reference Architecture



Look at the bigger picture

- Step 0 : Embarking on Kubernetes
- Beyond :
 - How to Speed Up
 - How to Protect
 - How to Self Service
 - How to Consume MultiCloud Service
 - How to Manage cost



