



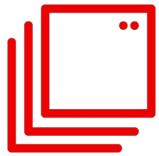
# What's Next in OpenShift

## Q3CY2021

OpenShift Product Management

# Red Hat Open Hybrid Cloud

Enabling any application, on any infrastructure, in any location



Traditional  
N-Tier Apps



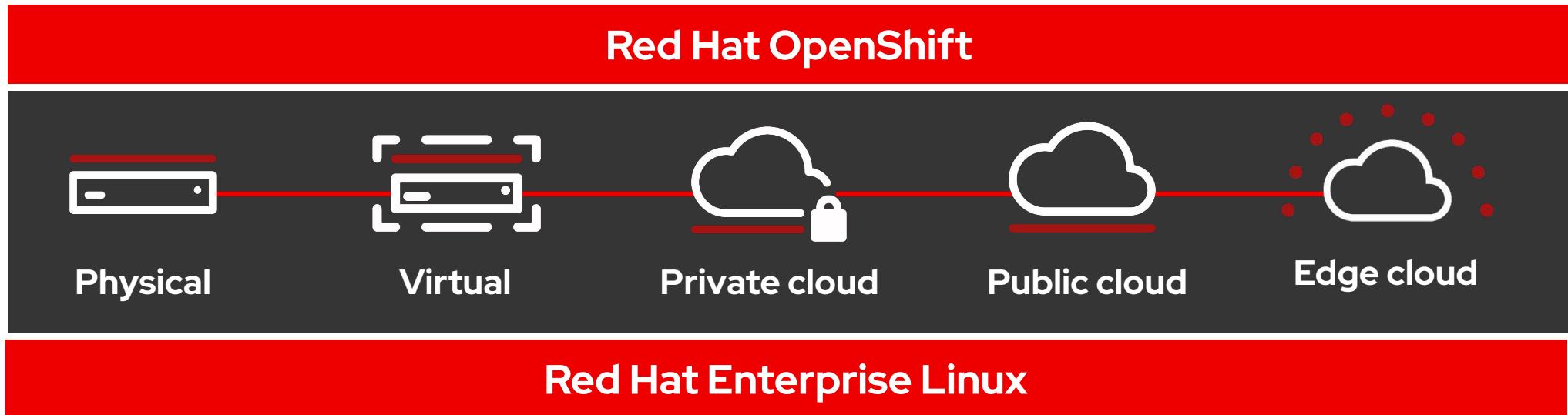
Cloud Native  
Microservices



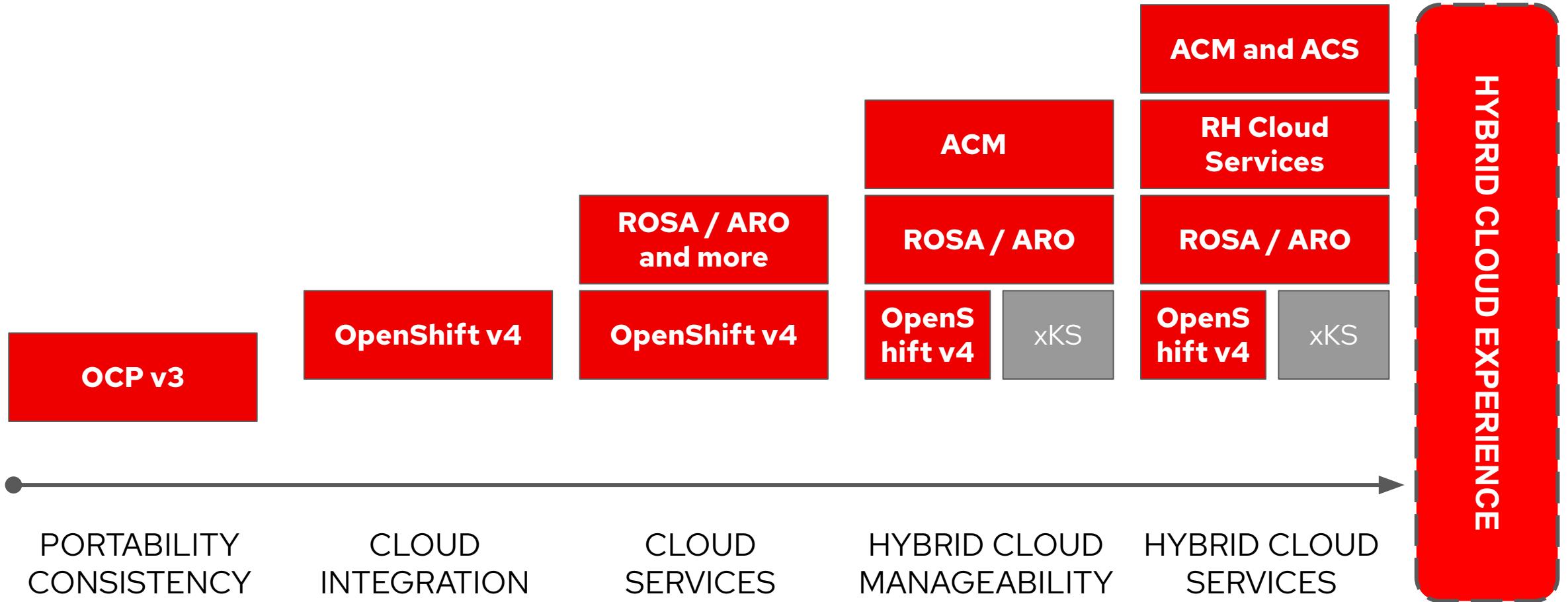
Data, Analytics  
& AI/ML



ISV Packaged  
Apps



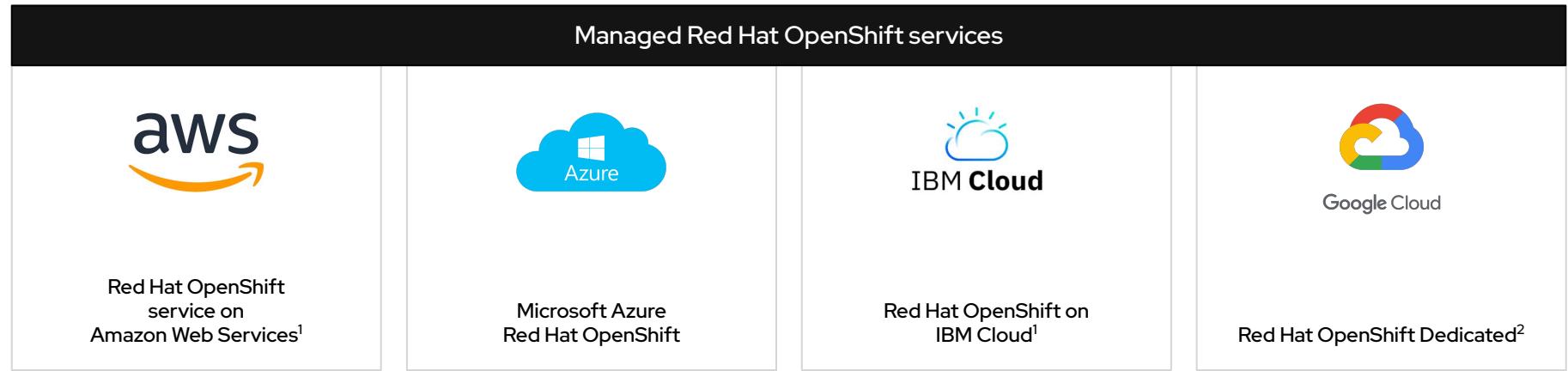
“Open Hybrid Cloud” has evolved over time...



# Available as self-managed platform or fully managed cloud service

Start quickly, we manage it for you

Cloud managed

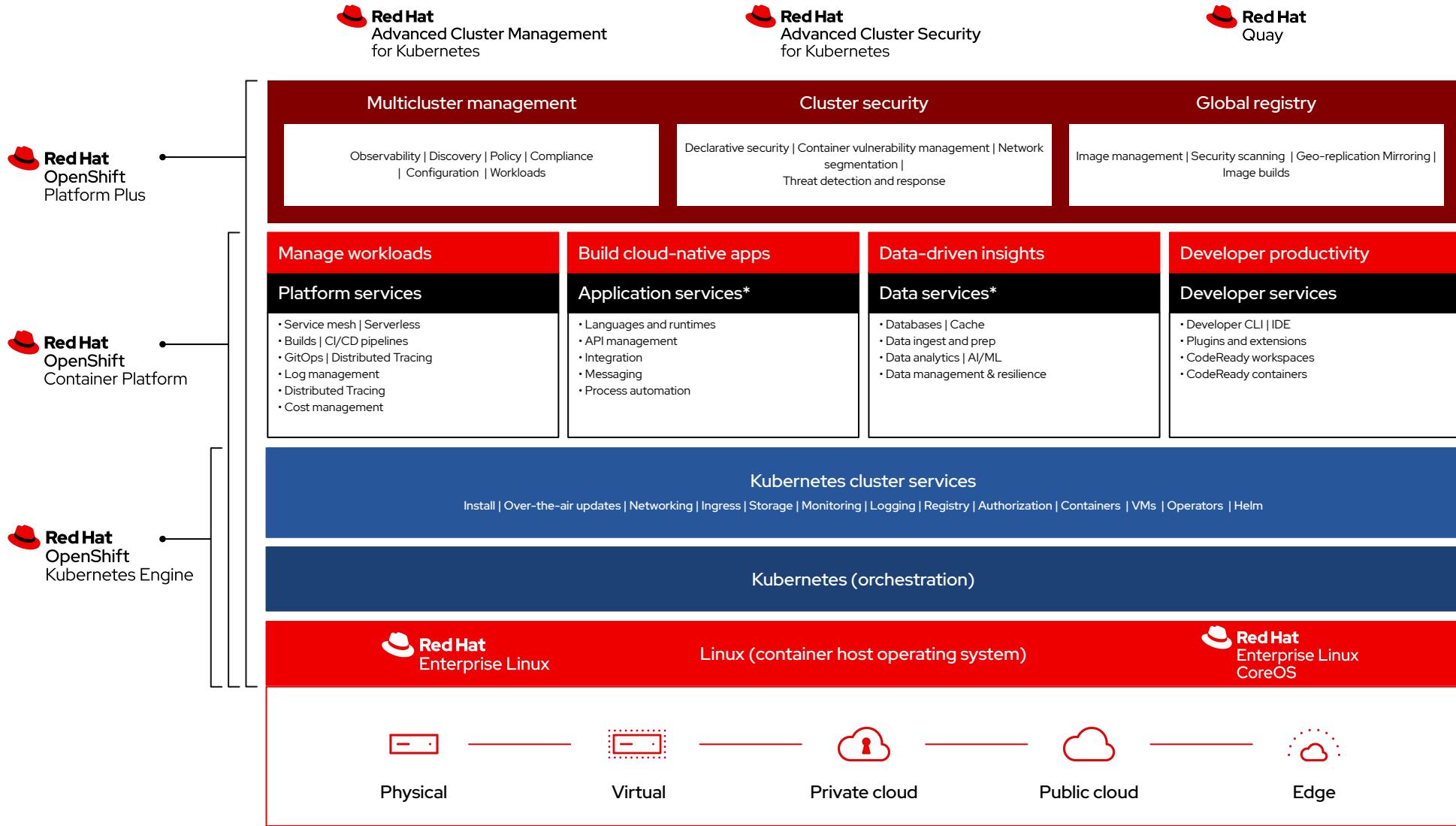


You manage it, for control and flexibility

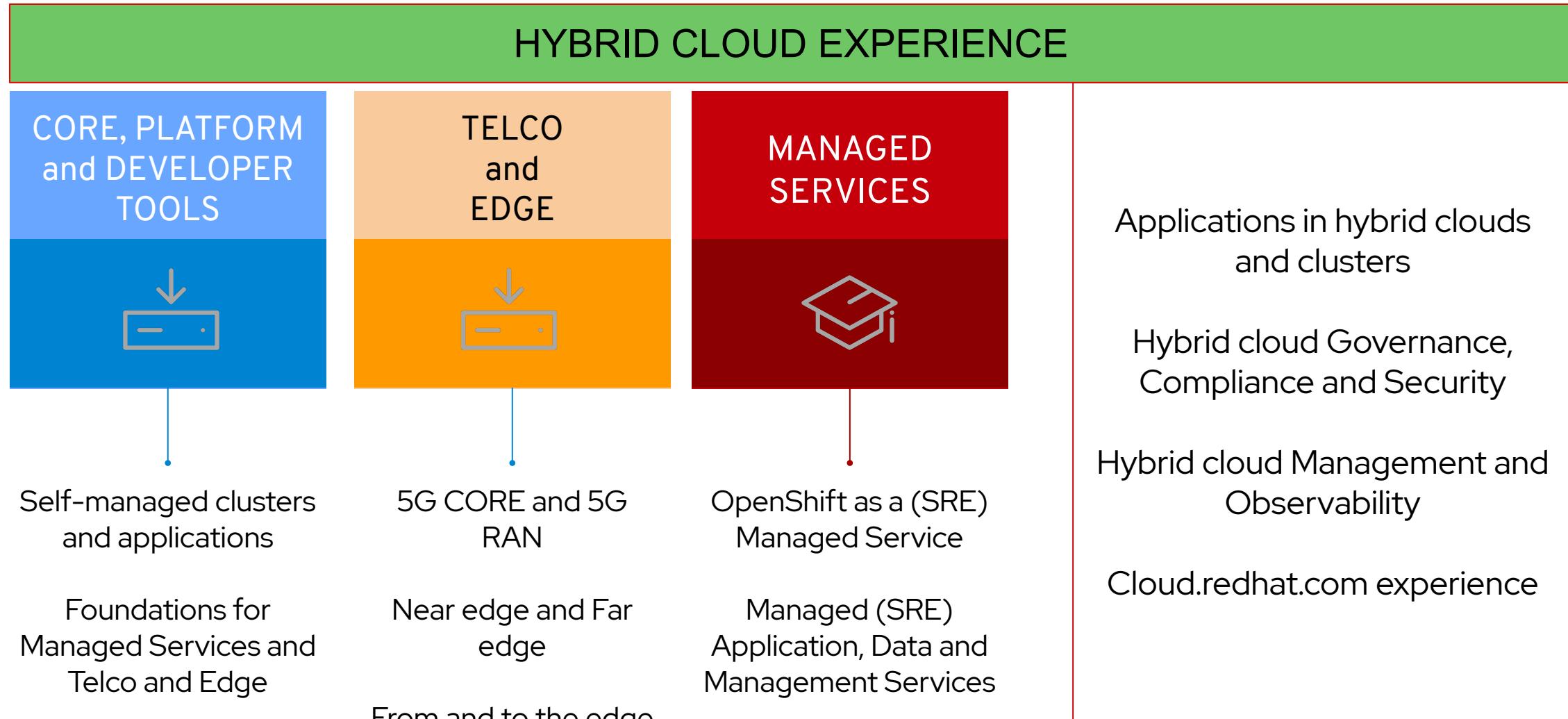
Customer managed



# Red Hat OpenShift



# OpenShift Themes



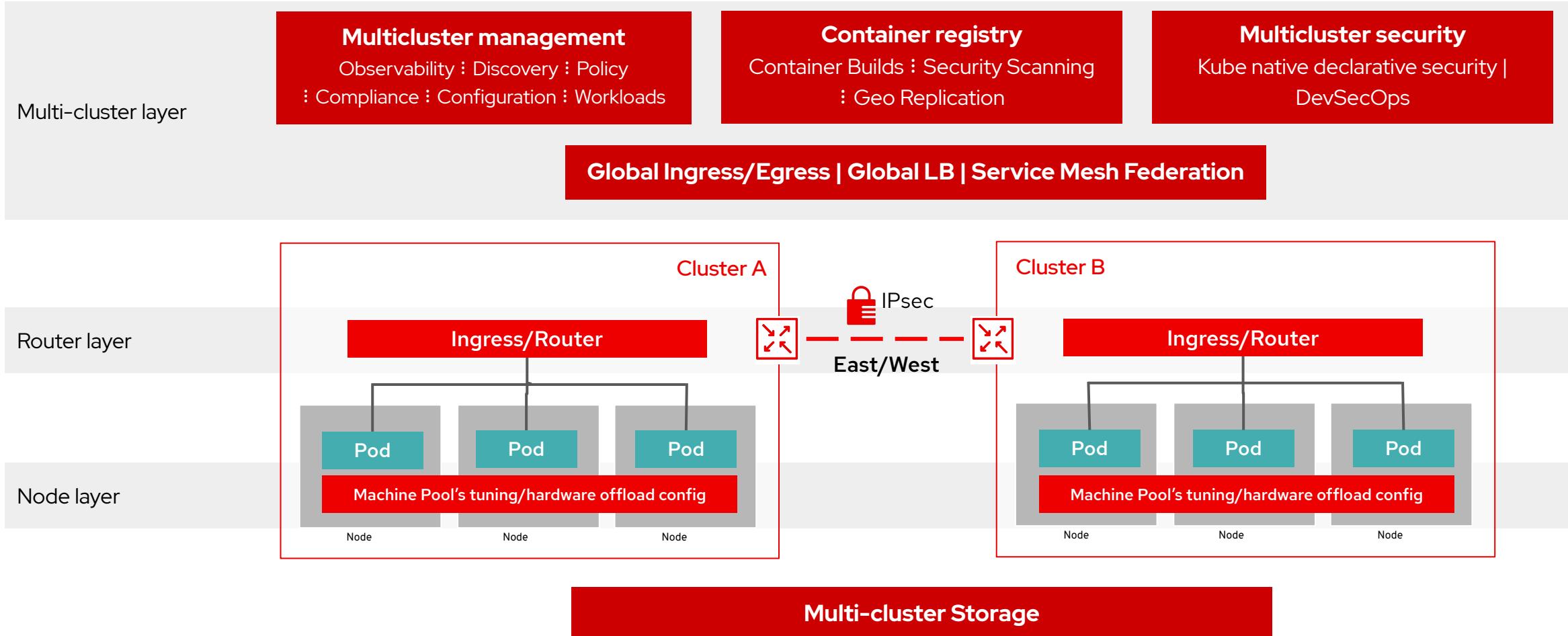
---

# HYBRID CLOUD EXPERIENCE

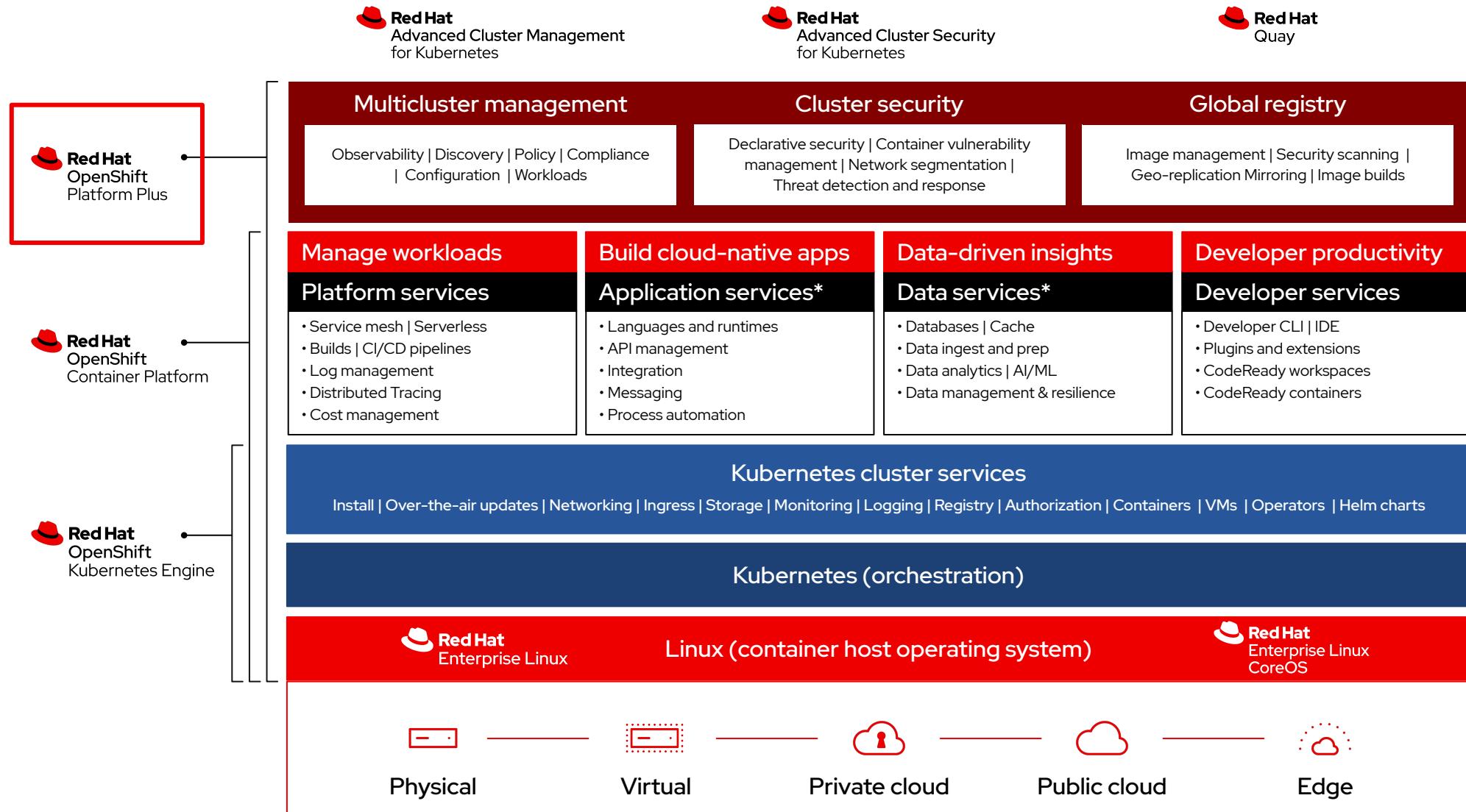
+

# OPENSHIFT PLATFORM PLUS

# Standardized tools for your 1st and 100th cluster



# Red Hat open hybrid cloud platform - OPENSHIFT PLATFORM PLUS (OCP + ACM + ACS + QUAY)



# Multi-cluster: Seamless networking mesh extends across cluster boundaries

Advanced Cluster Management (ACM) maintains East-West networking between all of your clusters using Submariner

## Overview

Multi-cluster networking makes it dead simple to span your apps across failure domains and geographies.

- ▶ Provides IPsec tunnel cluster to cluster
- ▶ IPsec = CNCF Submariner
- ▶ Service Mesh = Istio with federation

## What's Next

- ▶ Support for inter-connecting clusters with overlapping IPs (aka Globalnet), and
- ▶ Multi-cluster NetworkPolicy

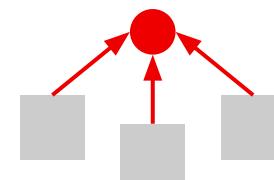
Better than stretched cluster



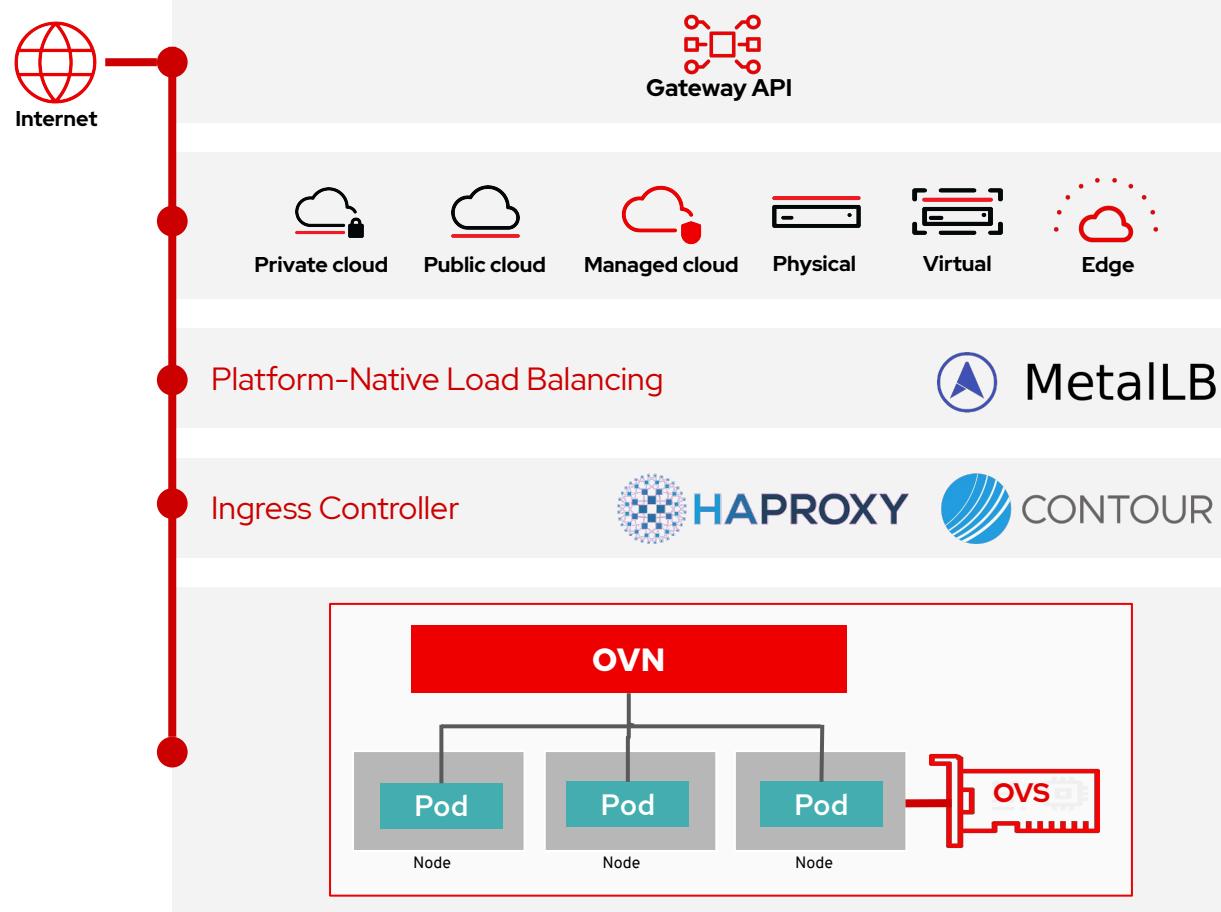
Easier HA apps across clusters



Securely access shared services



# Multi-cluster Gateway for Ingress and Egress



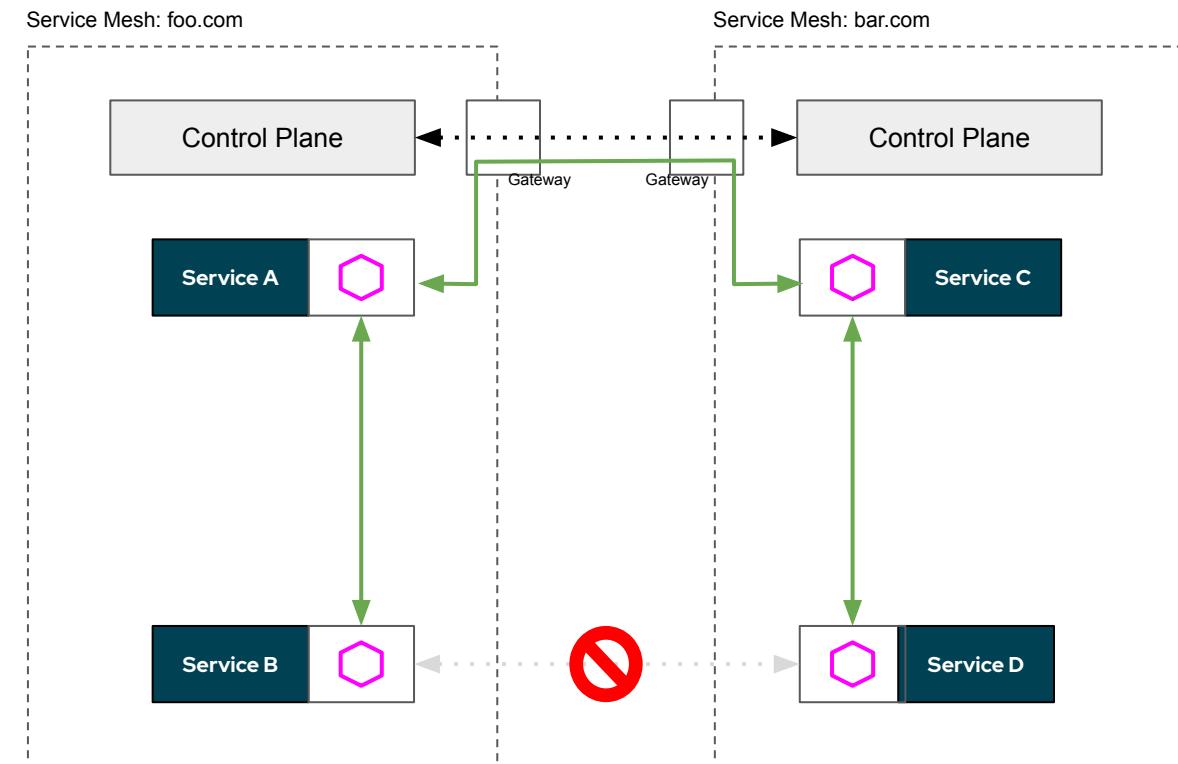
- ▶ Unified traffic handling so you configure all your traffic the same way
- ▶ Any supported platform – add or swap easily, hybrid scenarios
- ▶ Flexibility to use native traffic distribution and filtering (e.g. WAF) for optimal performance
- ▶ Your traffic, your way: L4-L7, Envoy, by-pass
- ▶ OVN for advanced traffic workloads
- ▶ IPv6 single/dual for scale
- ▶ HW Offload (OVS, IPsec, ...) for performance
- ▶ Multi-NIC support to align host networking
- ▶ BGP-advertised services (FRR)
- ▶ Observability for improved understanding
- ▶ eBPF precision traffic control
- ▶ No-overlay option
- ▶ Reduced traffic “friction” for Service Mesh, Virtualization

# Service Mesh Federation

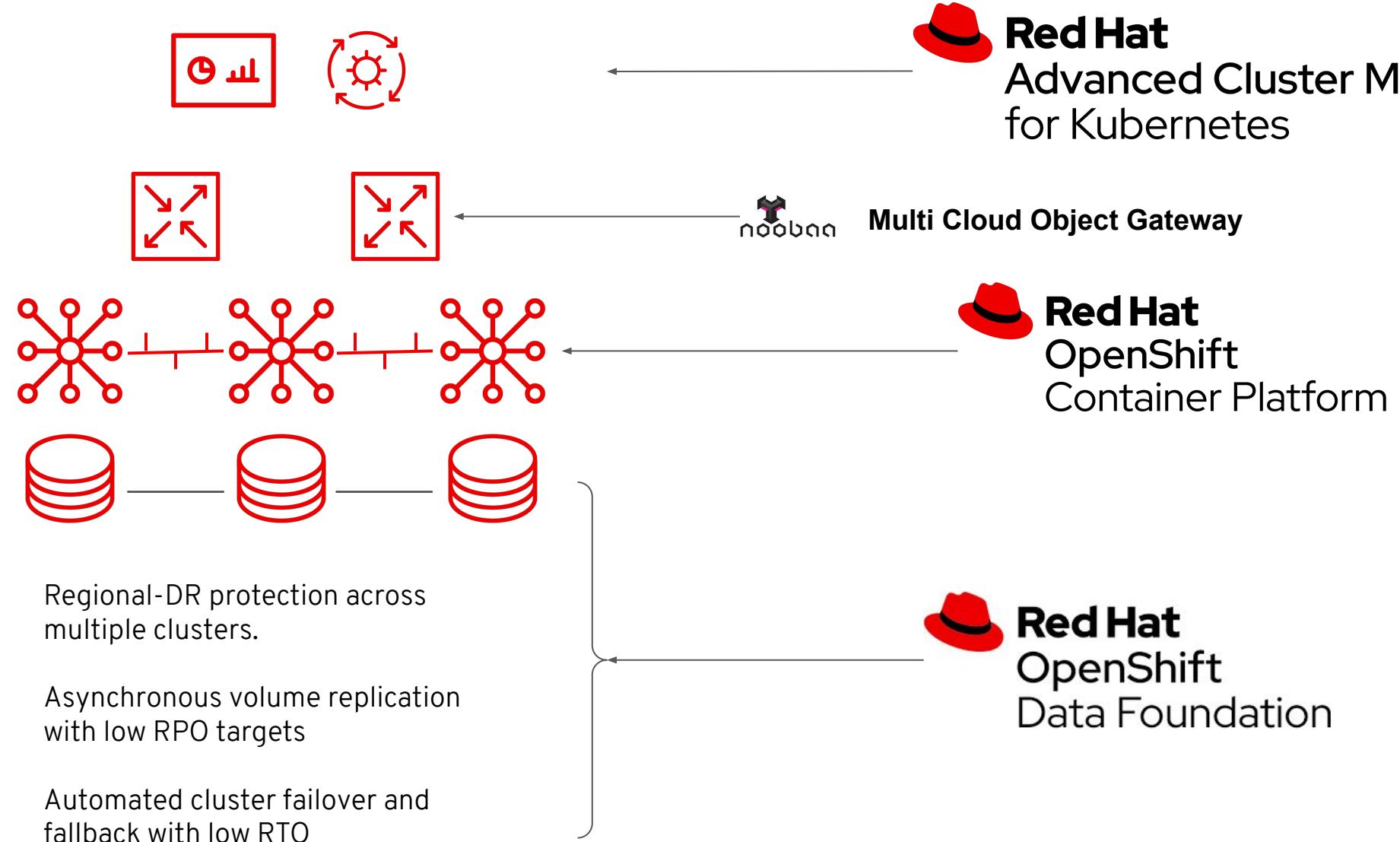
Adding scalability and high-availability to multi-tenant service mesh

Service Mesh Federation will provide guided resources for sharing services across meshes in different clusters, while maintaining the secure multi-tenant separation that customers have come to expect from OpenShift Service Mesh.

- ▶ Manage service to service connectivity between meshes in different clusters.
- ▶ Configure load balancing and “highly available” of services across meshes in different clusters.



# Multi-cluster Storage



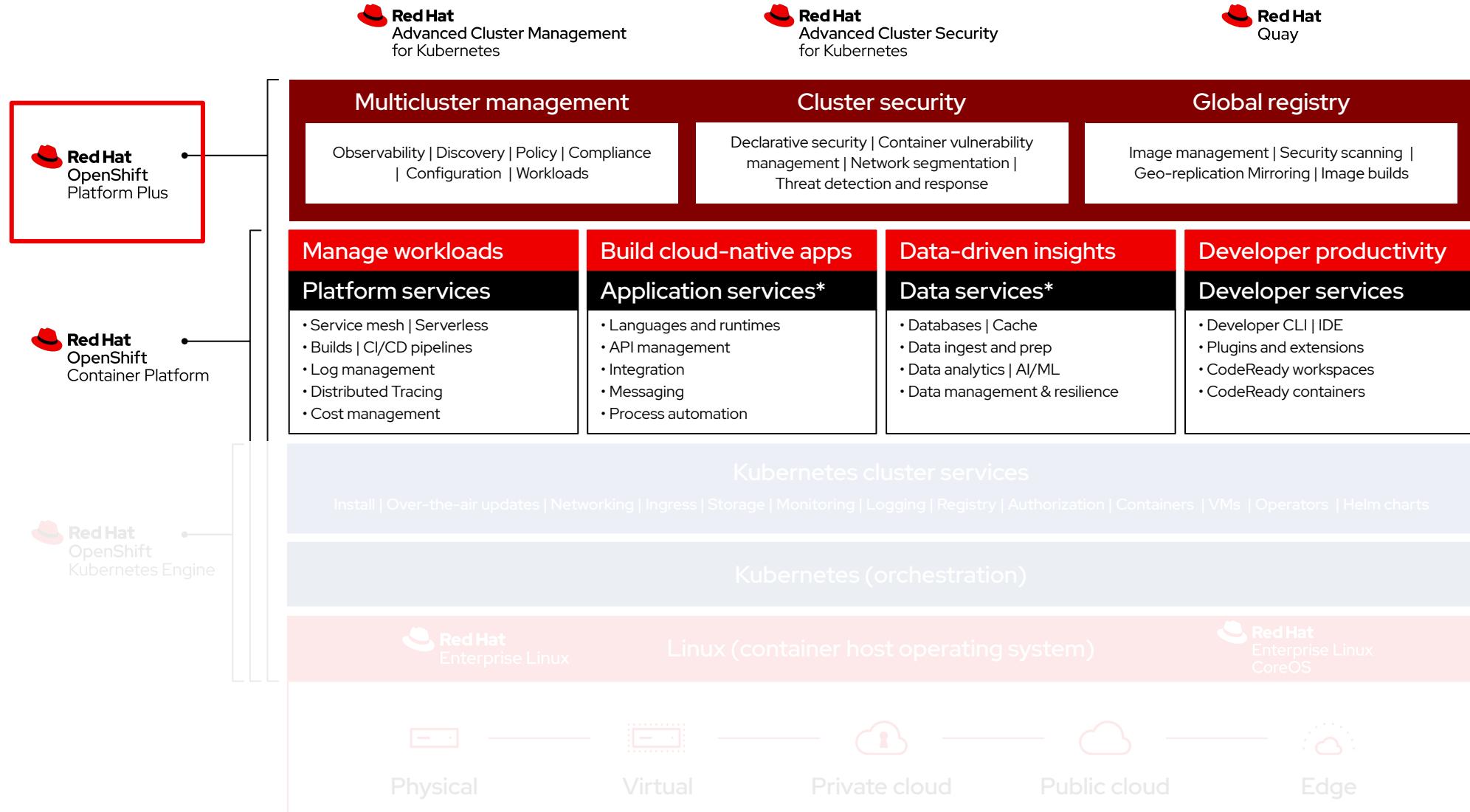
# Multi-cluster: Observe your entire fleet from one location

**Red Hat Advanced Cluster Management (RHACM) aggregates telemetry data from all your clusters**

- ▶ CCX Insights data & remediations are now visible in the ACM hub, allowing centralized issue detection and alerting based on OpenShift fleet-wide analytics
  - Avoid unplanned downtime and better manage the security risks of your entire fleet.
  - Quickly pinpoint the risks and remediate them.
  - Improved remediation status, and user experience updates for a more consistent feel across ACM/OCM
- ▶ SREs and DevOps teams
  - Improve and support SRE / DevOps practices with cluster health information and how that may impact application availability
- ▶ IT Operations / Cluster admins:
  - Centralized data and metrics from all of your ACM managed clusters into hub.
  - Alerts from the entire fleet, as well as Critical alerts from CCX Insights, all flowing into your preferred incident response tooling.
- ▶ Consumption and Usage
  - Help customers understand utilization and make adjustments via scale automatically
  - Leverage Cluster Pools (Claim and Hibernate) to mitigate cost associated to off hours and overnight spend.

Description	Category	Total risk
Code injection risk or wrong pid altering when rhnsd daemon file ...	Security	2 more
Cluster upgrade will fail when default SCC gets changed	Service Availability	1 more
Unable to set or reset the password during provisioning ...	Fault Tolerance	Moderate

# Red Hat open hybrid cloud platform - OPENSHIFT PLATFORM PLUS (OCP + ACM + ACS + QUAY)



\* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application and Data Services portfolio.

# Red Hat Advanced Cluster Management: What's Next



## Multicloud lifecycle management

- Quickly and consistently deploy clusters with desired state configuration to any cloud.
- Deploy hybrid and infrastructure agnostic clusters at scale.
- Deploy SRE-managed and self-managed clusters from a single source of truth.



## Policy driven governance and compliance

- Deploy RHACS Central and Sensors directly from RHACM hub.
- Drive alerts and notifications from policy compliance status.
- Unified governance framework provides a single entry point for all security tools.



## Advanced application lifecycle management

- Consolidated application deployment approach across various dev tools.
- Quickly observe application health and status from any deployment source.
- Include cross-cluster PV replication for business critical workloads.



## Multicloud observability for health and optimization

- Provide the complete fleet view for cluster health metrics.
- Enable operations teams to analyze metrics using preferred tooling.

# Red Hat Advanced Cluster Security Vision

## Security across the entire application lifecycle



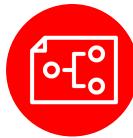
### Reduce security program costs

Enable teams to shift security left with our continued focus on improving vulnerability management and compliance workflows



### Enable effective prioritization workflows

Provide teams with the information to prioritize the issues that matter most in their environment



### Best in class OpenShift support

First class support for the OpenShift platform across clouds and managed services and security use cases



### Our commitment to open source

Creating an open source community focused on enabling Kubernetes security will enable us to tap into innovation pools not previously available



### Advanced security workflows

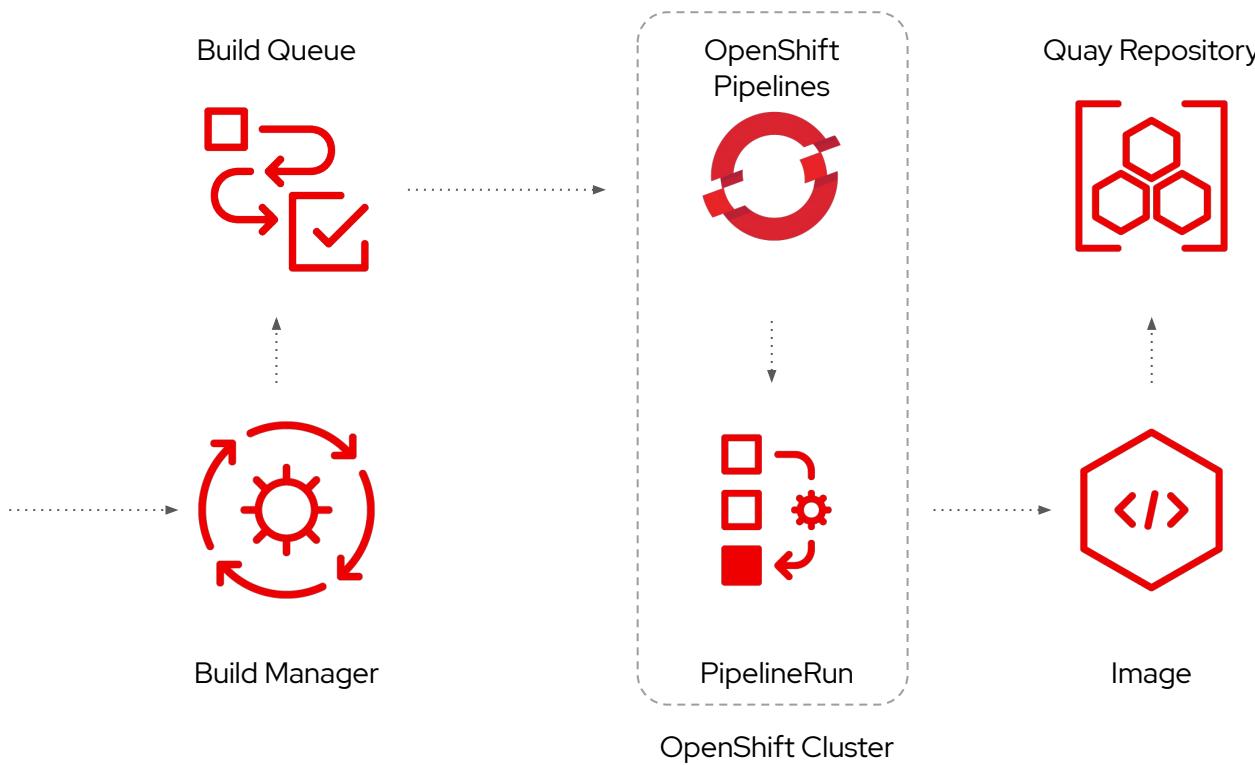
Enable advanced incident response and hardening capabilities to enable the most mature risk management programs



### Program Management

Improve cybersecurity programs by making recommendations that would have an outsized impact on an organization's security posture and exposing program metrics to showcase ROI

# Quay Container-native builds



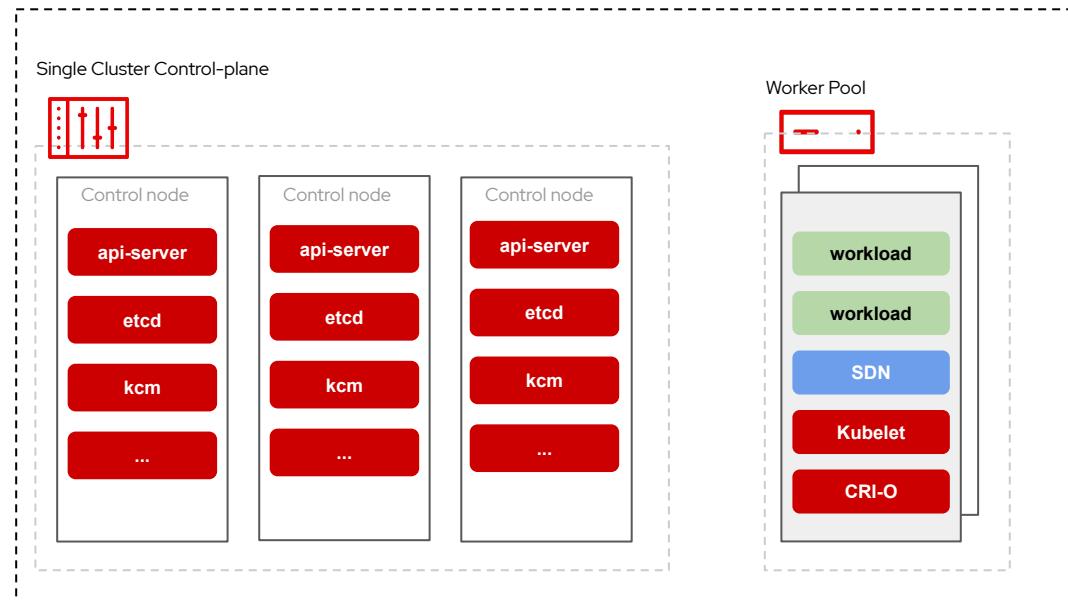
- ▶ Quay container builds trigger OpenShift Pipelines, build process containerized
- ▶ Builds execute on the same OCP cluster  
Quay is running on or a remote cluster, no VMs or bare-metal server/cluster required
- ▶ Automatically configured via the Quay Operator
- ▶ *Future:* multi-arch builds in OpenShift Pipelines

# Hypershift Brings Externally Managed Control-Planes

## Standalone OpenShift

### Control-Plane (CP) + Workers

Standalone OpenShift **Cluster** (dedicated CP nodes)



Low CAPEX and OPEX costs  
(bundling of CPs + CP as pods)



Central Management of CPs  
(easy operation & maintenance)



Multi-arch support  
(e.g. CP x86, workers ARM)



## HyperShift

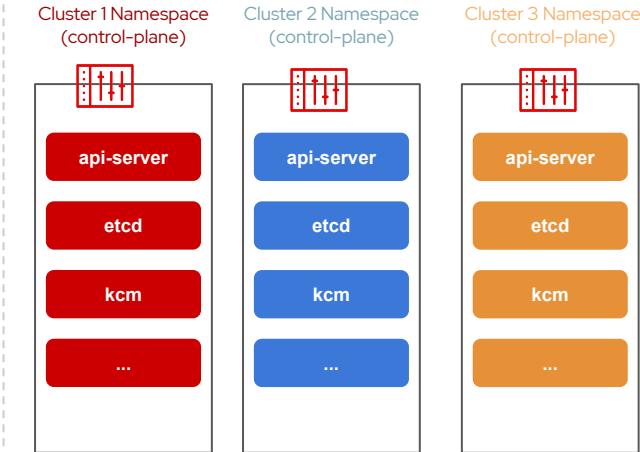
### Control-Plane (CP)



### Workers

HyperShift **Clusters** (decoupled CP and workers)

Management Cluster (Hosts Control Planes)



Network & Trust  
segmentation



Mixed IaaS For CP and  
Workers



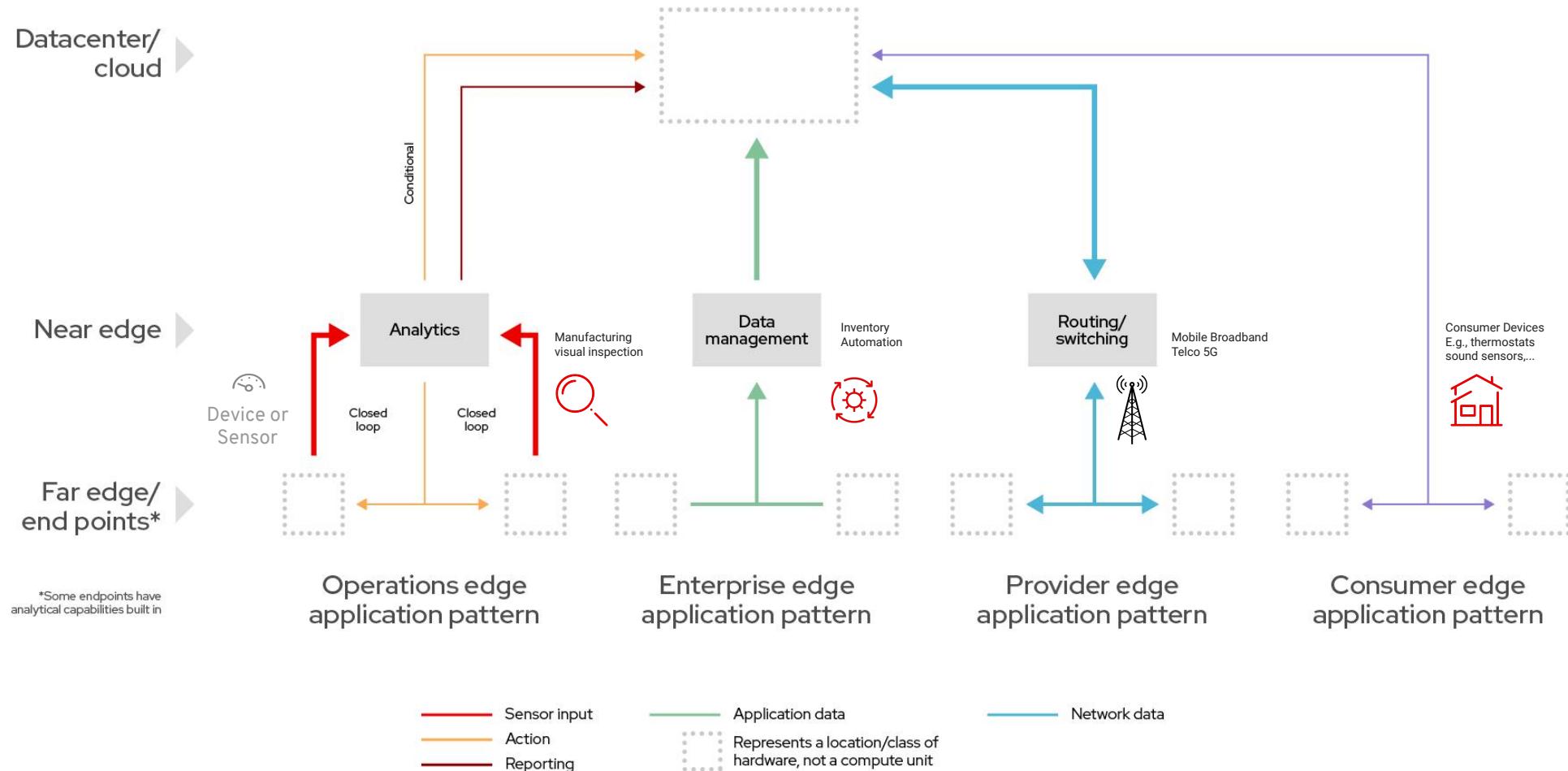
Fast cluster bootstrapping  
(CP as Pods)

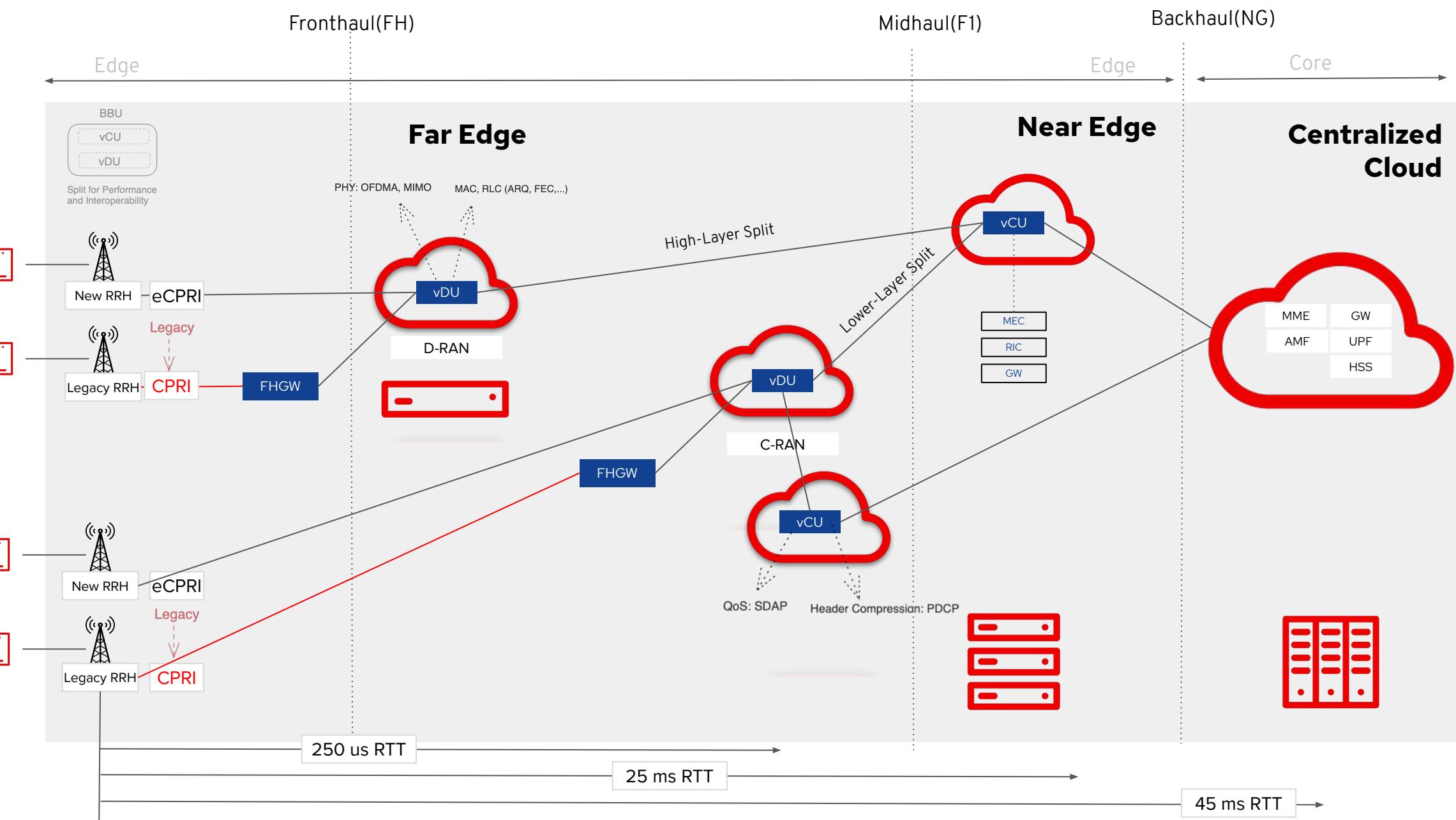


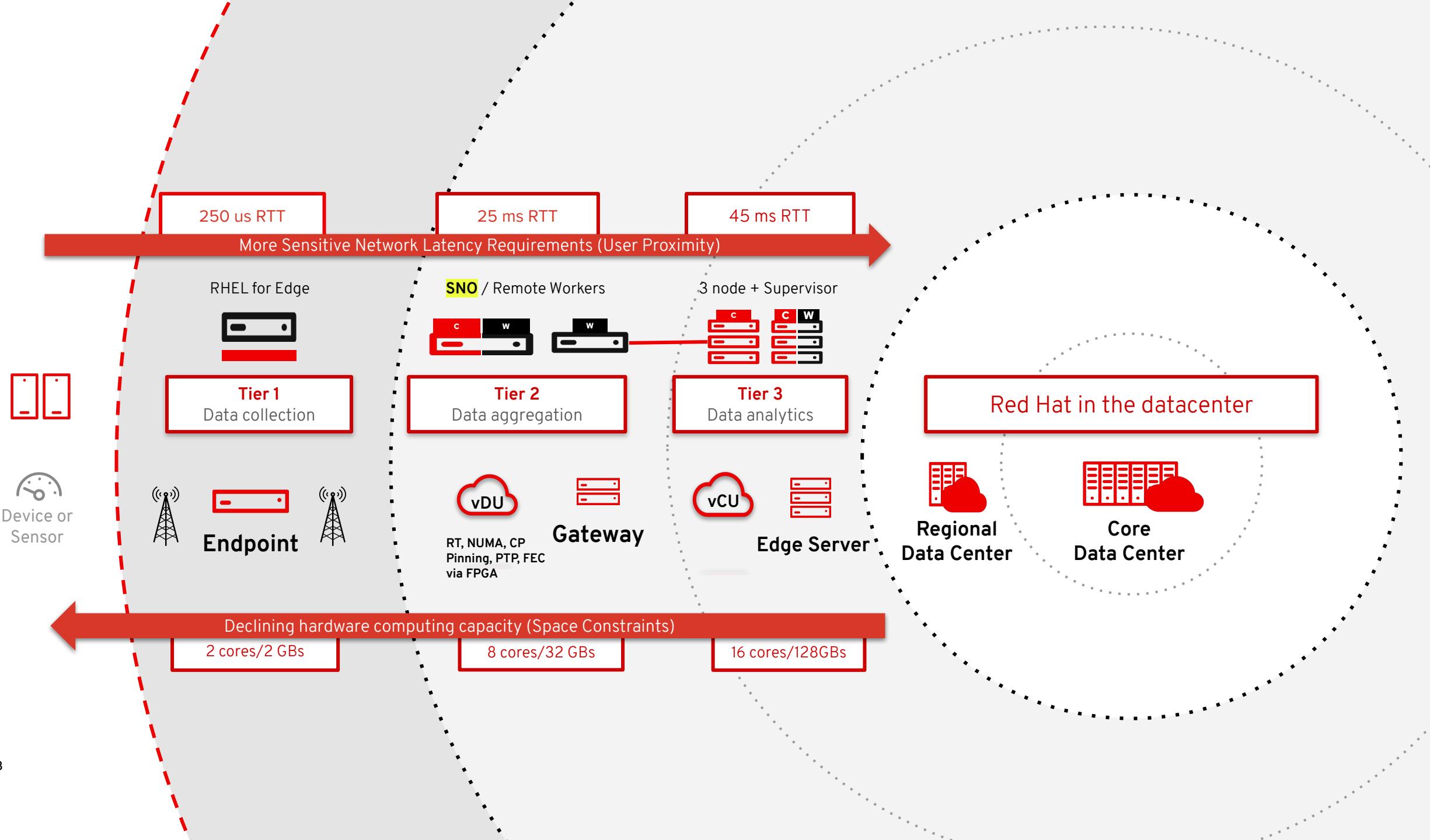
---

# TELCO AND EDGE

# From and To The Edge?







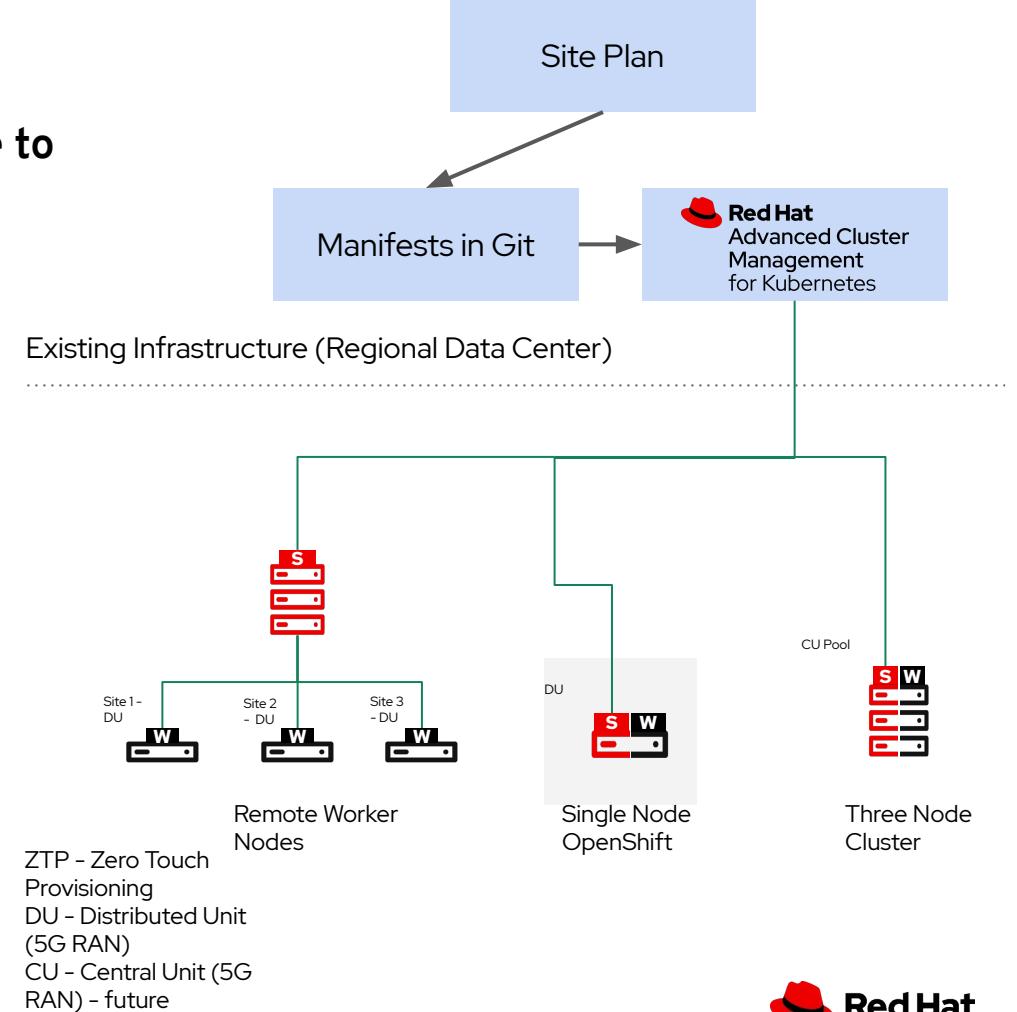
# Zero Touch Provisioning

## Technology-Preview in Advanced Cluster Management 2.4

Aimed at **regional distributed on-prem deployment**.

Enabling customer's **automated path** from **uninstalled infrastructure** to **application running on an OpenShift cluster**.

- **Integrates and leverages existing technology stack** - RHACM/Hive/Metal3/Assisted Installer
- **Minimal prerequisites** - Enables untrained technician installation flow (Barcode scan to trigger install).
- **Highly customized deployment** - Fits Connected/Disconnected, IPv4/IPv6, DHCP/Static, UPI/IPI deployment topologies
- **Edge focused** - no additional bootstrap node or external services needed for deployment.
- **GitOps enabled** - managed with kube-native declarative API
- **Late binding** - decoupling compute management and cluster provisioning. Enabling dynamic allocation of hosts to cluster deployments



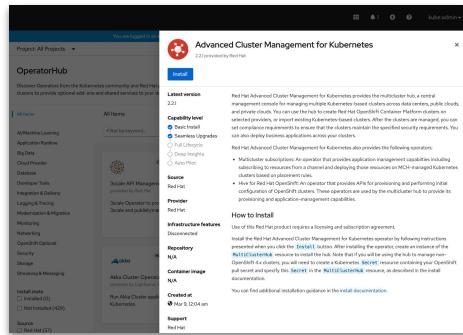
---

# CORE, PLATFORM AND DEVELOPER TOOLS

# What's next for the OpenShift Console?

## Dynamic Plugins

Enable teams to rapidly build high quality, easy to use, consistent user experiences via Operators. Operators become multi-cluster aware.



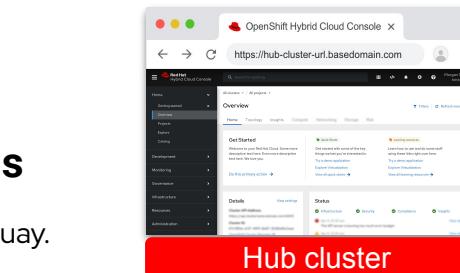
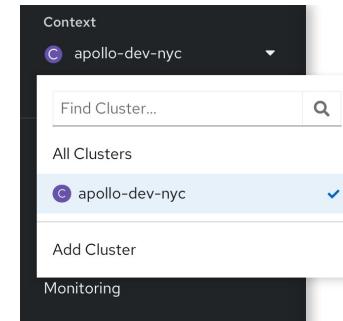
## OpenShift Platform Plus

Unification of OCP, ACM, ACS & Quay.  
Hub & spoke model, seamlessly integrated via SSO.



## OpenShift Hybrid Console

One place to see your entire fleet. Multi-cluster first. Application or administration oriented, users can customize to fit their needs.



Hub cluster

Spoke API

Spoke API

Spoke API

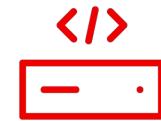


# OpenShift Serverless Future/Vision



## Serverless Ecosystem

Event sources to cover the breadth of applicability, community leadership, security by default, scaling performance



## User Serverless Experience

Intuitive hybrid developer experience with full stack integration with platform services , elevated Serverless function experience for local and remote. SandBox enablement for all Serverless functionalities



## Serverless Platform

Serverless as the **default** deployment strategy for all **workloads**.  
Serverless, **fundamental** part of the OpenShift delivered in cloud form, service form, or self-managed form, **clusters itself running in Serverless fashion**



## Centralized Hybrid Cloud

Multi-cloud developer & operator experience for creation and management of applications on a centralized hybrid cloud for a "cluster agnostic" environment

# What's next for Operators?

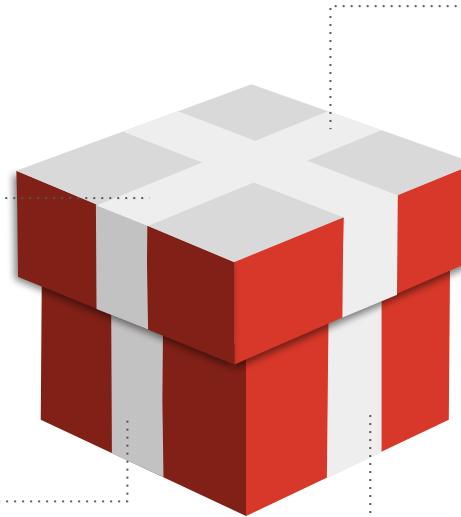
## Java-based Operators

Leverage existing developer experience and cloud-native tooling (Quarkus) to write mature Operators



## Granular Permissions

Install Operators cluster-wide and apply fine-grained rules about which tenants can see and use them.



## Cloud-native Bundles

An API to install and distribute cloud-native content on the cluster. Priming OLM to natively support other package managers, e.g. Helm.



## Catalog files

Publish and maintain Operator catalogs, update graphs and channels with a git-based and automation friendly approach using a single file.

# What's Next for Helm on OpenShift

## Simplified and integrated application development



### Enrich Helm Charts ecosystem

Developer catalog with more Helm Charts coming from trusted Partners with tested and certified Charts.



### Enable Red Hat Portfolio

Engage and enable Red Hat product teams to build and showcase Helm Charts for OpenShift developers' use.



### Best Practises for Helm Charts

Documentation and tooling to help developers creating Helm Charts following security best practises and misconfiguration issues.



### Improve Developer Experience

Improve experience in ODC and tools enabling a self-service developer experience that minimizes the need to interact with a cluster operator.

The screenshot shows the OpenShift developer console interface. At the top, it displays the project 'helm' and application 'all applications'. Below this, there is a search bar and filter options. The main area shows a list of Helm charts. One chart, 'Quarkus v0.0.1', is highlighted. A detailed view of this chart is shown on the left, including its description, version (0.0.1), app version, home page, maintainers, provider (Redhat Helm Repo), creation date (Nov 23, 9:12 am), and prerequisites. The prerequisites section contains a command-line snippet for creating a Docker pull secret:

```
oc create secret docker-registry my-pull-secret --docker-server=$SERVER_URL --dock
er-username=$USERNAME --docker-password=$PASSWORD --docker-email=$EMAIL
```

Below the command, it says you can use this secret by passing `--set build.pullSecret=my-pull-secret` to `helm install`, or you can configure this in a values file.

# What's Next for OpenShift Virtualization



## Hybrid Cloud and Edge

Optimize for smaller deployments:  
Single Node OpenShift,  
and Compact Cluster

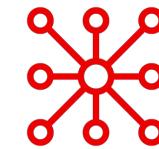
Support for Public Cloud  
Bare metal instances



## Workloads

Workload acceleration  
with virtual GPU

Interface with AI / ML  
operators



## Enterprise Scale

Enhance partner ecosystem and certifications

Validation for SAP HANA



## Migration at Scale

Modernize application workflows with warm migration from Red Hat Virtualization

# OpenShift sandboxed containers



## FIPS Compliance

Now you can run the OpenShift sandboxed containers operator on a FIPS enabled cluster without worrying about tainting its state. Our Operator, and Kata Containers are FIPS Validated.



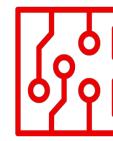
## Updates & Upgrades

You can now seamlessly upgrade a cluster, as well as the operator and it's artifacts (Kata Containers + QEMU extensions).



## Must Gather

An initial version of must-gather will be available in this release. This will help automate data-collection for you to get better support.



## Disconnected Mode

Our operator now works in disconnected mode.



## Health Metrics

Dashboard for health-metrics and insights on Kata Containers specific components.

## OpenShift on Bare Metal

# OpenShift on Bare Metal

## What's Coming Next?

### Advanced Host Network Configuration

Configure bonds, VLANs and static IPs, on your hosts at installation time and for installed hosts

### Run the Bare Metal Operator Anywhere

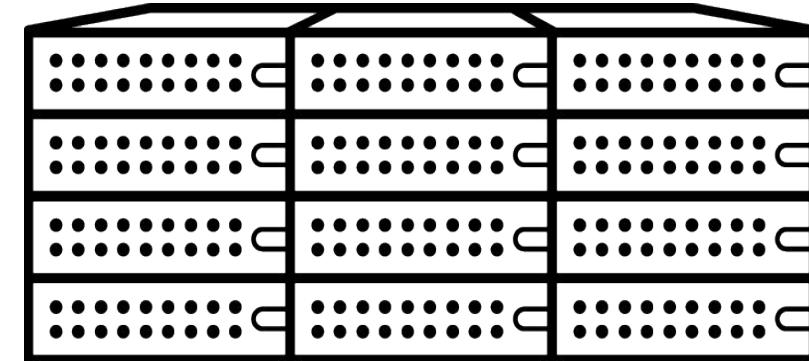
Provision and manage bare metal hosts from clusters running on VMs on non-bare metal platforms

### Node Health Checks and Remediation

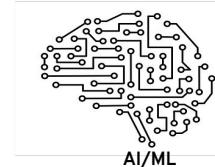
Protect your workloads on bare metal clusters from host failure, including OpenShift Virtualization clusters and Single Node OpenShift

### Hardware Management and Observability

Set BIOS attributes and place workloads in nodes with the desired attributes. See your nodes' hardware information from the console



# Specialized workload scheduling framework



## Multi-Cluster Application Dispatcher

Job Queues : Quota : Priorities

## Open Data Hub

Prometheus: Grafana: SELDON: Spark: Jupyterhub: Ceph: Kafka: Argo

Specialized workload scheduler and NUMA aware



**Red Hat Specialized workload scheduler operator for Openshift**

**Gang scheduler for specialized workload: AI/ML, HPC**

**Customer developed Specialized workload scheduler operator for Openshift**

**Customized workload with specialized scheduler requirements**

**Scheduling Profiles/Plugin/Extension points**

**Openshift**

**Red Hat Enterprise Linux & Red Hat Enterprise Linux CoreOS**



Physical



Virtual



Private cloud



Public cloud



Managed cloud  
(Azure, AWS, GCP, IBM, Red Hat)



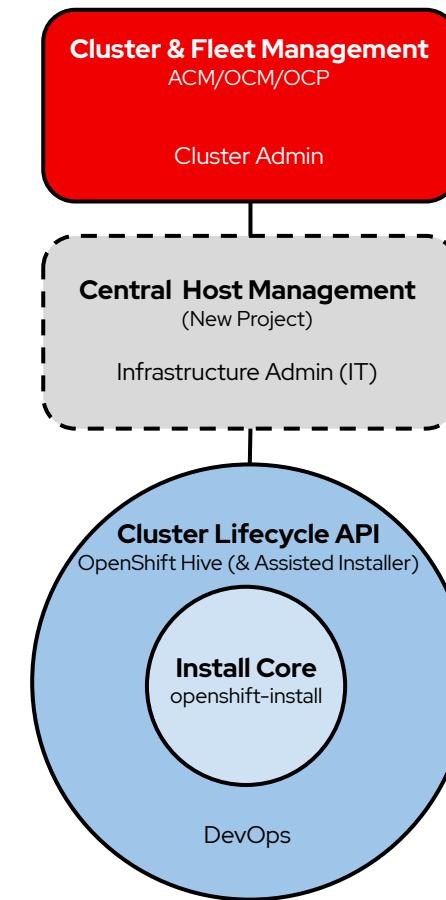
Edge cloud

# Installation & Updates

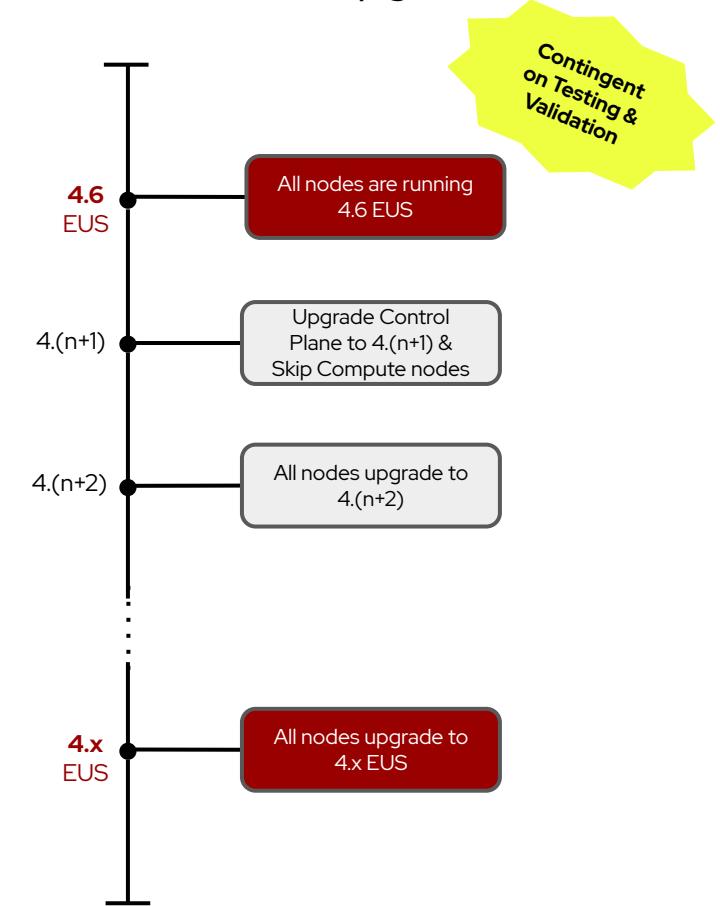
Deploy OpenShift to even more platforms & RHEL 8 compute node support



## Unified Installation Experience



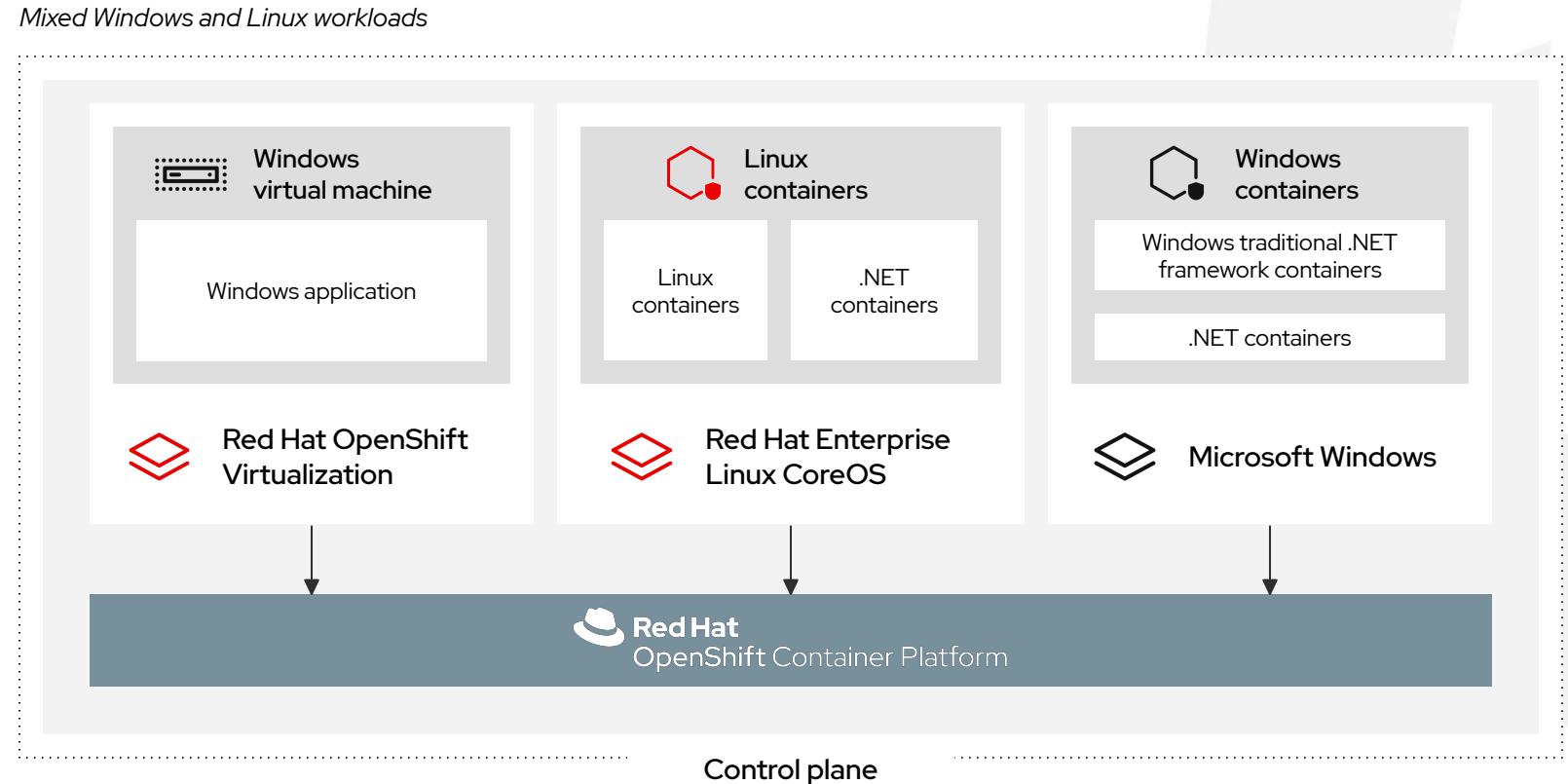
## EUS to EUS Upgrades



# Bring your own Windows Server host

## Goals

- ▶ Allow a customer to add an existing Windows instance running a variant of Windows Server 2019 (1809, 1909, 20H2 etc).
- ▶ WMCO will then perform all the required steps within the VM for it to be added to the cluster as an OpenShift worker node and removed from it.
- ▶ Handle upgrades of all components installed by WMCO.



# Preview of cert-manager in OpenShift

## Automate certificate management in cloud native environments

[cert-manager](#) builds on top of Kubernetes, introducing certificate authorities and certificates as first-class resource types in the Kubernetes API. This makes it possible to provide 'certificates as a service' to developers working within your Kubernetes cluster.

### Use Cases

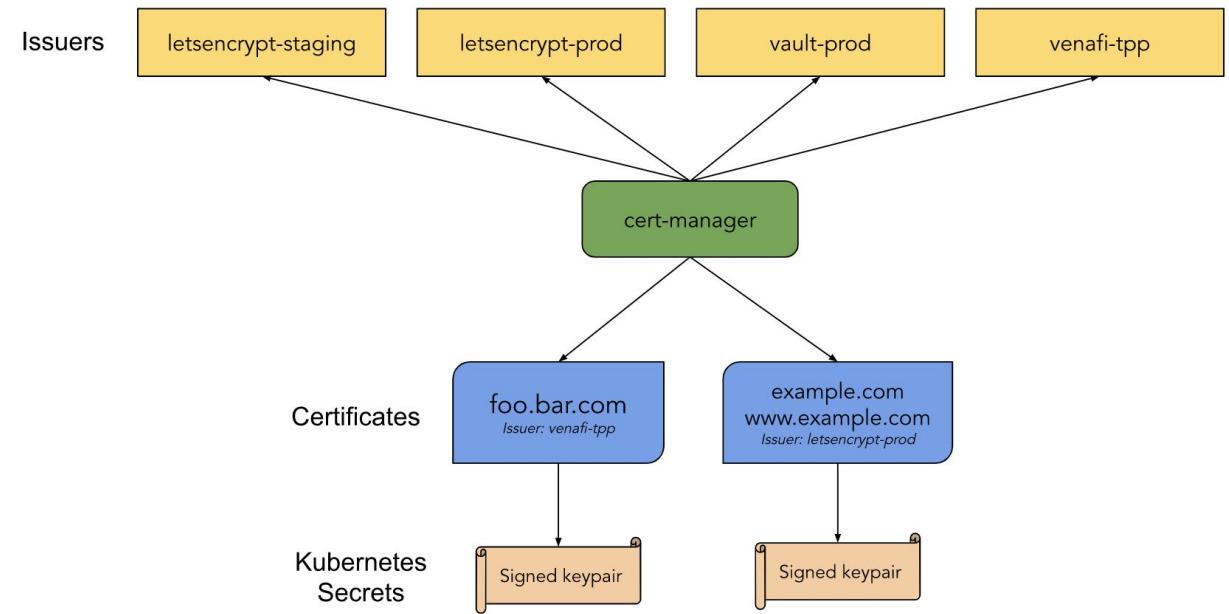
- Provide easy to use tools to manage certificates.
- A standardised API for interacting with multiple certificate authorities (CAs).
- Gives security teams the confidence to allow developers to self-serve certificates.
- Support for ACME (Let's Encrypt), HashiCorp Vault, Venafi, self signed and internal certificate authorities.
- Extensible to support custom, internal or otherwise unsupported CAs.

#### **Latest Release** (v1.3):

<https://github.com/jetstack/cert-manager/releases/tag/v1.3.0>

This service would be available to all workloads running in OpenShift (except bootstrap components that need certificates before operators exist), including:

- out-of-the box operators that are support day 2 configuration
- OLM-installed operators
- Applications managed by the above operators
- Middleware software from the Red Hat portfolio
- Applications deployed by the customer





 [linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)

 [youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)

# Thank you

## Red Hat is here to help

Responding to COVID-19 requires collaboration, transparency, and the free exchange of expertise.

[Ways to contact us](#)

