

Red Hat Partner Bootcamp

OpenShift Topics

Alfred Bach

Principal Solution Architect

Red Hat EMEA

Agenda

- ▶ Innovation without limitation
- ▶ OpenShift Architecture
- ▶ OpenShift Container Platform (OCP) Install
- ▶ OpenShift Plus

Agenda

- ▶ Innovation without limitation
- ▶ OpenShift Architecture
- ▶ OpenShift Container Platform (OCP) Install
- ▶ **OpenShift Plus**



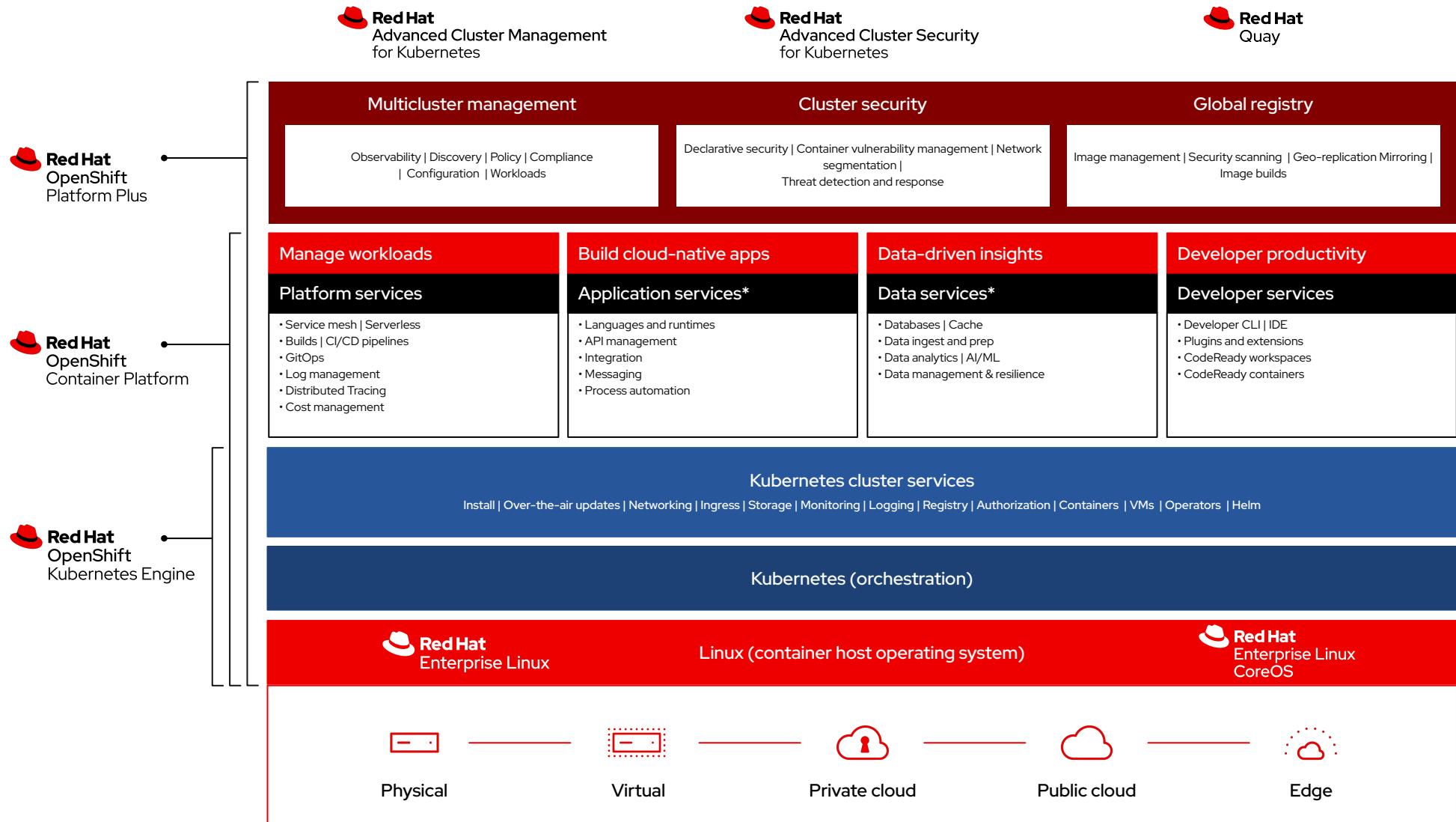
OpenShift Plus

As part of Partner Boot Camp

Alfred Bach

Principal Solution Architect

Red Hat OpenShift



HYBRID CLOUD EXPERIENCE

Applications in hybrid clouds and clusters

CORE, PLATFORM
& DEVELOPER
TOOLS

TELCO & EDGE

MANAGED CLOUD
SERVICES



Self-managed clusters
and applications

Foundations for
Managed Services and
Telco and Edge



5G CORE and 5G
RAN

Near edge and Far
edge

From and to the edge



OpenShift as a (SRE)
Managed Service

Managed (SRE)
Application, Data and
Management Services

Unified Experience

Security Everywhere

Platform Consistency

Red Hat Advanced Cluster Management for Kubernetes

Why Red Hat Advanced Cluster Management is important

Why you should care

- ▶ App modernization is a top industry priority.
- ▶ Kubernetes is platform modernization.
- ▶ Enterprises are rapidly adopting Kubernetes.
- ▶ There is intense competition for Kubernetes.
- ▶ Not all Kubernetes solutions are equal.
- ▶ Kubernetes management is complicated.

Key solutions



Move quickly and win the platform



Use the best, most complete solution - OpenShift



Differentiate and win Red Hat OpenShift Container Platform



Recognize VMware as the biggest threat

But Hybrid Multi-Cloud management is really hard

As organizations deploy more across multiple clouds, new challenges arise.

- ▶ **Difficult and error prone** to manage at scale
- ▶ **Inconsistent security controls** across environments
- ▶ **Overwhelming to verify** components, configurations, policies, and compliance

IDC Survey of 200 US-based \$1B companies actively using two or more “infrastructure clouds” for production applications

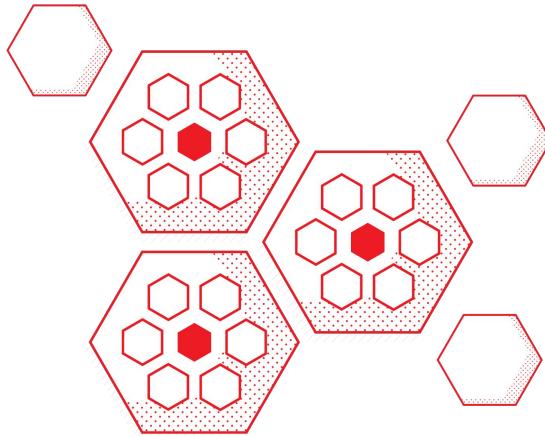


—
Using multiple infrastructure clouds*



—
Using multiple public clouds and one or more private/dedicated clouds*

Kubernetes adoption leads to multicloud



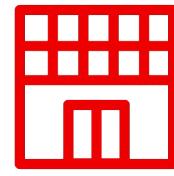
“As Kubernetes gains adoption across the industry, scenarios are arising in which I&O teams are finding **they must deploy and manage multiple clusters**, either in a single region on-premises or in the cloud, or across multiple regions....for a number of reasons, including multi-tenancy, disaster recovery, and with hybrid, multicloud, or edge deployments.”

Where is the growth in cluster deployments?



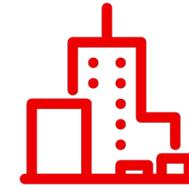
Small Scale Dev teams

- Managing and syncing across Dev/QE/Pre-Prod/Prod clusters can be difficult



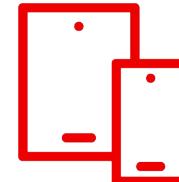
Medium Scale Organizations

- Retail with small clusters across 100s of locations
- Organizations with plan for growth 10-15 clusters moving to 100s



Large Scale

- Global organizations with 100s of clusters, hosting thousand of applications
- Large Retail with 1000s of stores



Edge Scale Telco

- 100s of zones, 1000s of clusters and nodes across complex topologies

Reasons for deploying clusters



Application availability



Reduced latency



Address industry standards



Geopolitical data residency guidelines



Disaster recovery



Edge deployments



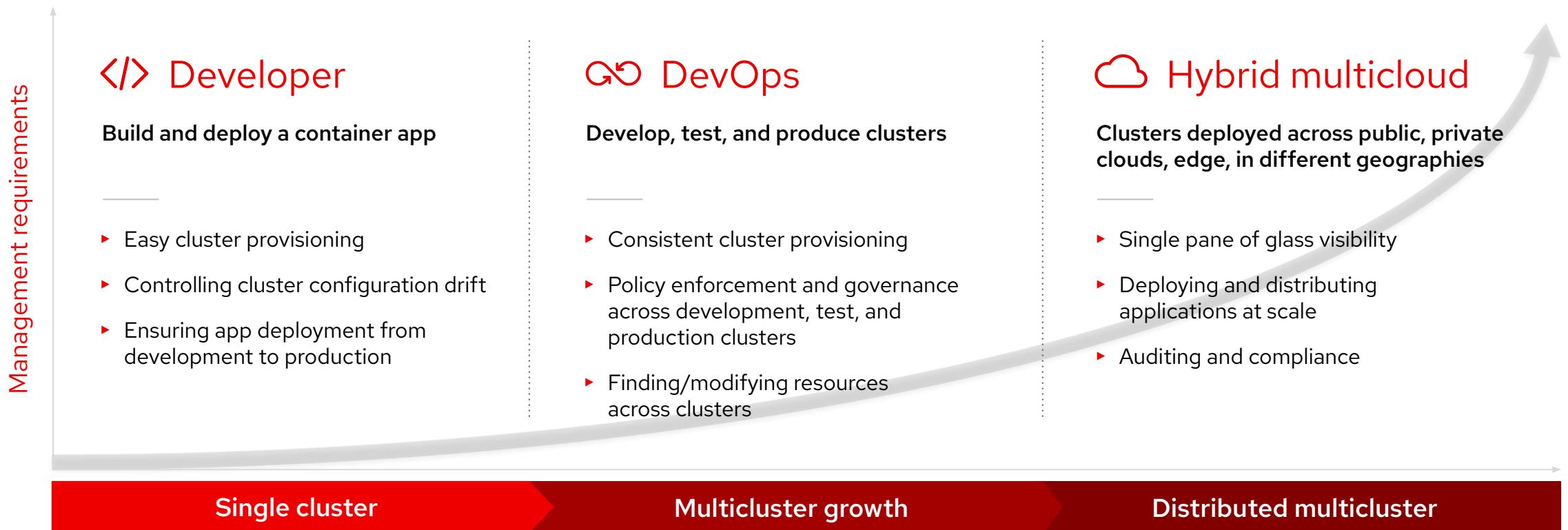
CapEx cost reduction



Avoid vendor lock-in

Multicloud management challenges

How do I normalize and centralize key functions across environments?



Robust. Proven. Award winning.



Multicloud lifecycle management



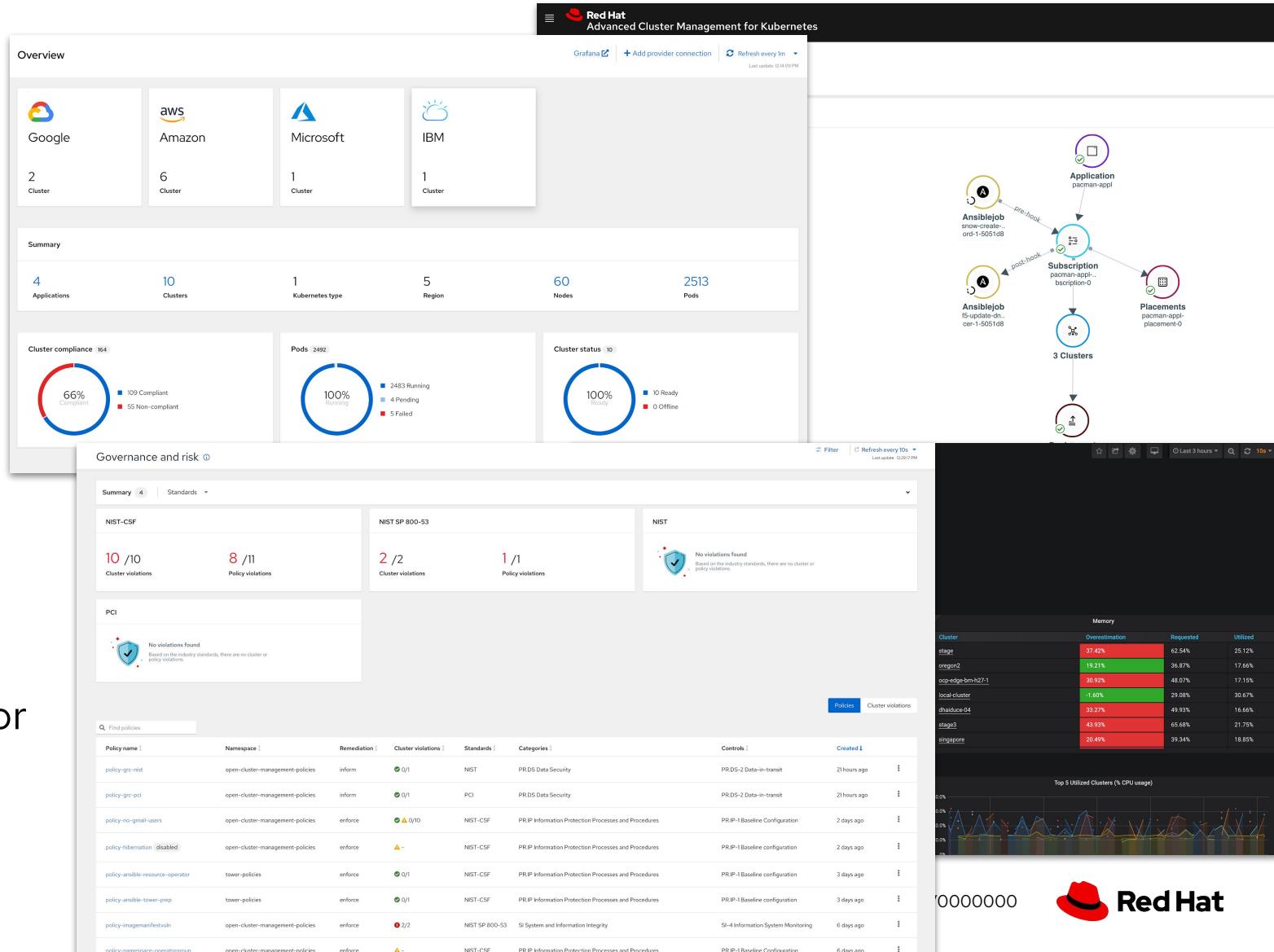
Policy driven governance, risk, and compliance



Advanced application lifecycle management



Multicloud observability for health and optimization



Unified Multi-Cluster Management

CONFIDENTIAL designator

Single Pane for all your Kubernetes Clusters

The screenshot displays two views of the Red Hat Advanced Cluster Management for Kubernetes platform. The top view is the 'Overview' page, which shows a summary of clusters across four cloud providers: Google (3 clusters), Amazon (5 clusters), Microsoft (1 cluster), and IBM (1 cluster). Below this is a 'Summary' section with metrics: 4 Applications, 10 Clusters, 3 Kubernetes type, 5 Region, 59 Nodes, and 2346 Pods. The bottom view is the 'Cluster management' page, featuring a 'Cluster compliance' donut chart (63% Compliant) and a detailed list of 10 clusters. The clusters are categorized by provider: Google Cloud Platform (foxtrot-gcp-europe, foxtrot-whiskey), Amazon Web Services (foxtrot-us-west-1, sberens-eks-west, sberens-roks-south, sberens-rosa-west), Microsoft Azure (sberens-aro-central), and IBM Cloud (local-cluster, sberens-gke-central, sberens-osd-gcp-central). Each cluster entry includes its name, status (Ready), provider, distribution version, labels, and node count.

Name	Status	Provider	Distribution	Labels	Nodes
foxtrot-gcp-europe	Ready	Google Cloud Platform	OpenShift 4.6.16 Upgrade available	apps.pacman=deployed, apps.ship-tracker=deployed, region=europe-west3	6
foxtrot-us-west-1	Ready	Amazon Web Services	OpenShift 4.6.16 Upgrade available	apps.pacman=deployed, apps.ship-tracker=deployed, enforceSecureImages=true, region=us-west-1	6
foxtrot-whiskey	Ready	Amazon Web Services	OpenShift 4.6.16 Upgrade available	apps.ship-tracker=deployed, enforceSecureImages=true, purpose=production, region=us-east-1, shipcommander=deployed	6
local-cluster	Ready	Amazon Web Services	OpenShift 4.6.9 Upgrade available	local-cluster=true	13
sberens-aro-central	Ready	Microsoft Azure	OpenShift 4.5.30		6
sberens-eks-west	Ready	Amazon Web Services	v1.18.9-eks-dldb3c		2
sberens-gke-central	Ready	Google Cloud Platform	v1.18.12-gke.1206		3
sberens-osd-gcp-central	Ready	Google Cloud Platform	OpenShift 4.6.17		7
sberens-roks-south	Ready	IBM Cloud	OpenShift 4.5.24	region=us-south-1	3
sberens-rosa-west	Ready	Amazon Web Services	OpenShift 4.6.16 Upgrade available	region=us-west-1	7

- **Centrally** create, update and delete Kubernetes clusters **across multiple** private and public clouds
- Search, find and modify **any** kubernetes resource across the **entire** domain.
- **Quickly** troubleshoot and resolve issues across your **federated** domain

Policy based Governance, Risk and Compliance

CONFIDENTIAL designator

Don't wait for your security team to tap you on the shoulder

Governance and risk ⓘ

Last update: 2:09 PM

Filter Refresh every 10s Create policy

NIST-CSF

10 /10 Cluster violations

4 /11 Policy violations

NIST SP 800-53

2 /2 Cluster violations

1 /1 Policy violations

Policies Cluster violations

Find policies

Policy name ⓘ	Namespace ⓘ	Remediation ⓘ	Cluster violations ⓘ	Standards ⓘ	Categories ⓘ	Controls ⓘ	Created ⓘ
policy-imagemanifestvuln	open-cluster-management-policies	enforce	1 /2/2	NIST SP 800-53	SI System and Information Integrity	SI-4 Information System Monitoring	12 days ago

Governance and risk / Policies / Create policy ⓘ YAML: On

All fields marked with an asterisk (*) are mandatory.

Name *

policy-pod

Namespace *

default

Specifications *

Pod

Cluster binding ⓘ

Begin typing to search for cluster label to select. If not selected, all clusters will be applied.

Standards ⓘ

FISMA, NIST-CSF

Categories ⓘ

PR.DS Data Security, PR.IIP Information Protection Processes and Procedures, PR. PT-3 Least Functional

Controls ⓘ

PR.DS-2 Data-in-transit, PR.IIP-1 Baseline Configuration, PR.PT-3 Least Functional

Enforce if supported ⓘ

Disable policy ⓘ

Policy YAML

```
apiVersion: policy.open-cluster-management.io/v1
kind: Policy
metadata:
  name: policy-pod
  namespace: default
  annotations:
    policy.open-cluster-management.io/standards: FISMA, NIST-CSF
    policy.open-cluster-management.io/categories: PR.DS Data Security, PR.IIP Information Protection Processes and Procedures, PR.PT-3 Least Functional
spec:
  remediationAction: inform
  disabled: false
  policyType: pod
  - objectDefinition:
    apiVersion: policy.open-cluster-management.io/v1
    kind: ConfigurationPolicy
    metadata:
      name: policy-pod-nginx-pod
    spec:
      remediationAction: inform # will be overridden by remediationAction in parent policy
      severity: low
      namespaceSelector:
        exclude: ["kube-*"]
        include: ["default"]
      objectDefinition:
        - containerImage: musthave
          objectDefinition:
            apiVersion: v1
            kind: Pod # nginx pod must exist
            metadata:
              name: nginx-pod
            spec:
              containers:
                - image: nginx:1.7.9
                  name: nginx
                  ports:
                    - containerPort: 80
    ...
  apiVersion: policy.open-cluster-management.io/v1
  kind: PlacementBinding
  metadata:
    name: binding-policy-pod
    namespace: default
    owner: placement-policy-pod
    kind: PlacementRule
```

- **Centrally** set & enforce policies for security, applications, & infrastructure
 - Quickly **visualize** detailed **auditing** on configuration of apps and clusters
 - Built-in compliance policies and audit checks
 - **Immediate** visibility into your compliance posture based on **your** defined standards

Advanced Application Lifecycle Management

CONFIDENTIAL designator

Simplify your Application Lifecycle

Applications /

Create an application

YAML: On

All fields marked with an asterisk (*) are mandatory. Fill out the form or edit the YAML directly.

Name* ⓘ newapp

Namespace* ⓘ default

Repository location for resources

Repository types

Select the type of repository where resources that you want to deploy are located

Git

URL* ⓘ https://github.com/mdekel/pac... Branch ⓘ master Path ⓘ s2i Reconcile option ⓘ merge Set pre and post c...

Application YAML

```
apiVersion: app.k8s.io/v1beta1
kind: Application
metadata:
  name: newapp
  namespace: default
spec:
  componentKinds:
    - group: apps.open-cluster-management.io
      kind: Subscription
      description: {}
      selector:
        matchExpressions:
          - key: app
            operator: In
            values:
              - newapp
  apiVersion: apps.open-cluster-management.io/v1
  kind: Subscription
  metadata:
    annotations:
      apps.open-cluster-management.io/git-branch: master
      apps.open-cluster-management.io/git-path: .git
      apps.open-cluster-management.io/reconcile-option: merge
  labels:
    app: newapp
    name: newapp-subscription-1
  namespace: default
```

Resource topology

How to read topology

Cluster

Launch resource in Search →

Select a cluster to view details

Clusters (2)

Find cluster

foxtrot-gcp-europe

Namespace: foxtrot-gcp-europe

Details

Name: foxtrot-gcp-europe
Namespace: foxtrot-gcp-europe
Open cluster console
Status: ok
CPU: 12%
Memory: 7%
Created: 9 days ago

foxtrot-us-west-1

Namespace: foxtrot-us-west-1

Details

Name: foxtrot-us-west-1
Namespace: foxtrot-us-west-1
Open cluster console
Status: ok
CPU: 12%
Memory: 7%
Created: 9 days ago

17

- **Easily** deploy an Application using the **Application Builder**
 - Deploy Applications from **Multiple** Sources (GIT / HELM / Object Storage)
 - Quickly **visualize** application relationships **across** clusters and those that **span** clusters

Benefits

Red Hat OpenShift and Red Hat Advanced Cluster Management for Kubernetes



Accelerate development to production

Self-service provisioning allows app dev teams to request clusters directly from a catalog removing central IT as a bottleneck.



Increase application availability

Placement rules can allow quick deployment of clusters across distributed locations for availability, capacity, and security reasons.



Reduce costs

Centralized management of clusters reduces operational cost, makes the environment consistent, and removes the need to manually manage individual clusters.

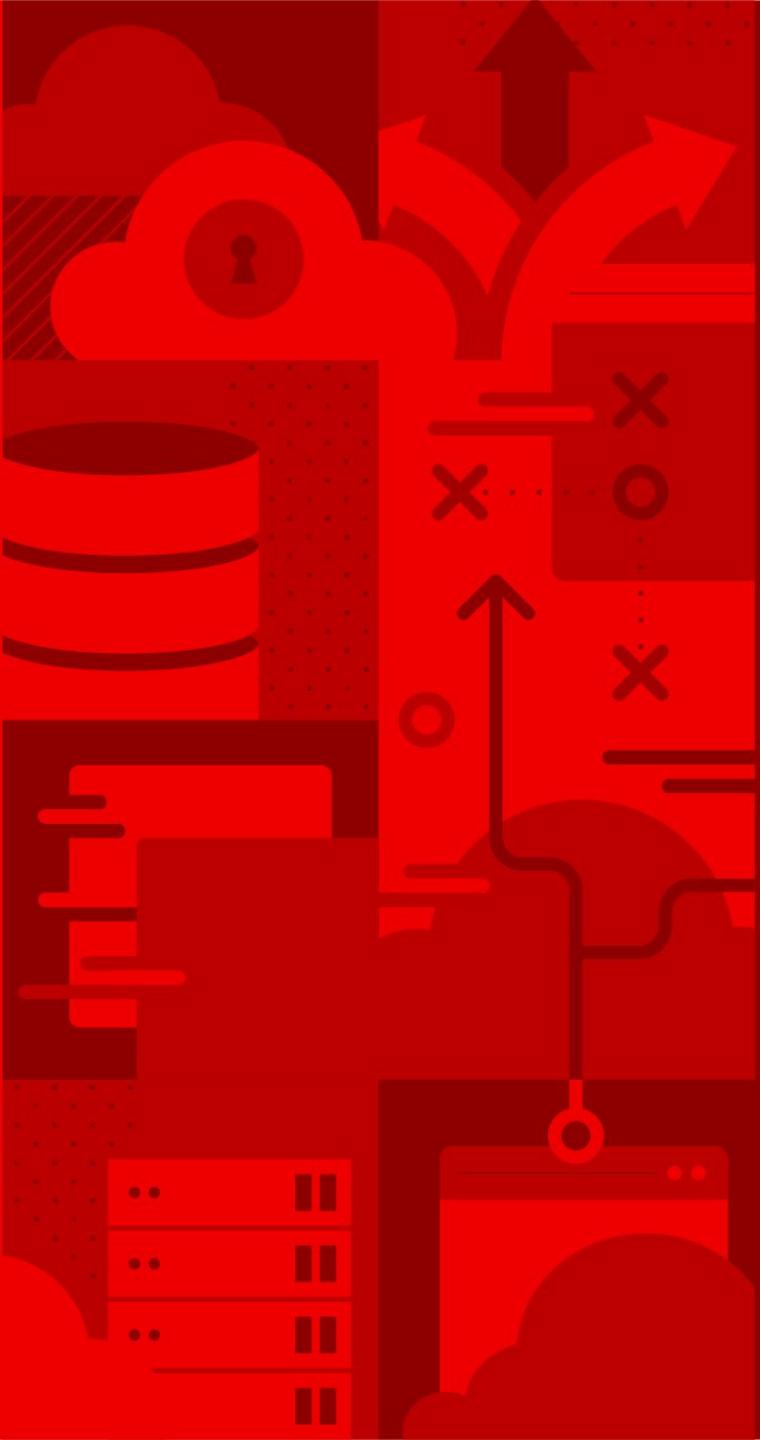


Ease compliance

Policies can be written by the security team and enforced at each cluster, allowing environments to conform to your policy.

Architecture

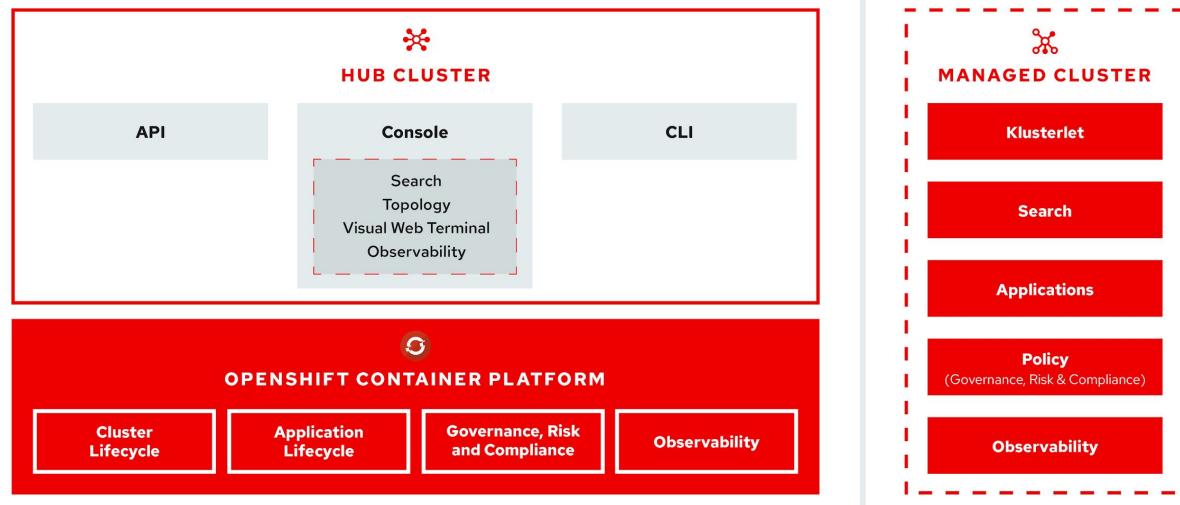
Red Hat Advanced Cluster Management For
Kubernetes



Architecture overview



IT Operations



Hub architecture and components

Red Hat Advanced Cluster Management uses the **multicloud-hub** operator and runs in the **open-cluster-management** namespace

Managed cluster architecture and components

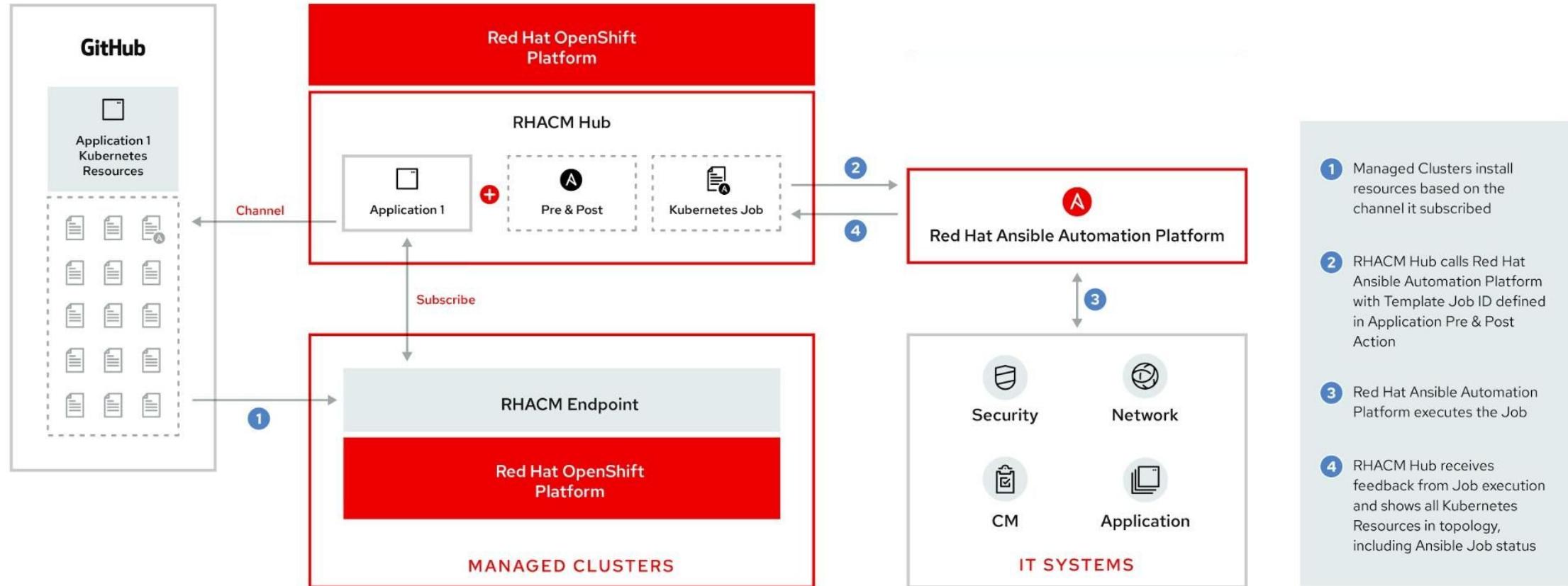
Red Hat Advanced Cluster Management managed clusters use the **multicloud-endpoint** operator which runs in the **open-cluster-management** namespace

Tech preview

Architecture Overview for Application Lifecycle



Red Hat
Advanced Cluster
Management
for Kubernetes





StackRox | Red Hat ACS

Alfred Bach

Principal Solution Architect - Cloud, Security & DC- Infrastructure

Partner Enablement Team EMEA

abach@redhat.com

Kubernetes is the standard
for application innovation...



- ▶ Microservices architecture
- ▶ Declarative definition
- ▶ Immutable infrastructure

...and Kubernetes-native
security is increasingly critical



- ▶ Secure supply chain
- ▶ Secure infrastructure
- ▶ Secure workloads

DevOps

DevSecOps

Security

Benefits of a Kubernetes-native approach to security



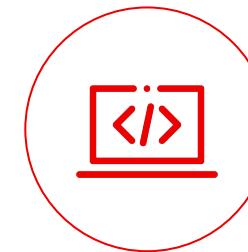
Lower operational cost

DevOps and Security teams can use a common language and source of truth



Reduce operational risk

Ensure alignment between security and infrastructure to reduce application downtime



Increase developer productivity

Leverage Kubernetes to seamlessly provide guardrails supporting developer velocity

Red Hat Advanced Cluster Security for Kubernetes

A cloud workload protection platform and cloud security posture management to enable you to “shift left”

Shift left

Secure supply chain

Extend scanning and compliance into development (DevSecOps)

Cloud security posture management (CSPM)

Secure infrastructure

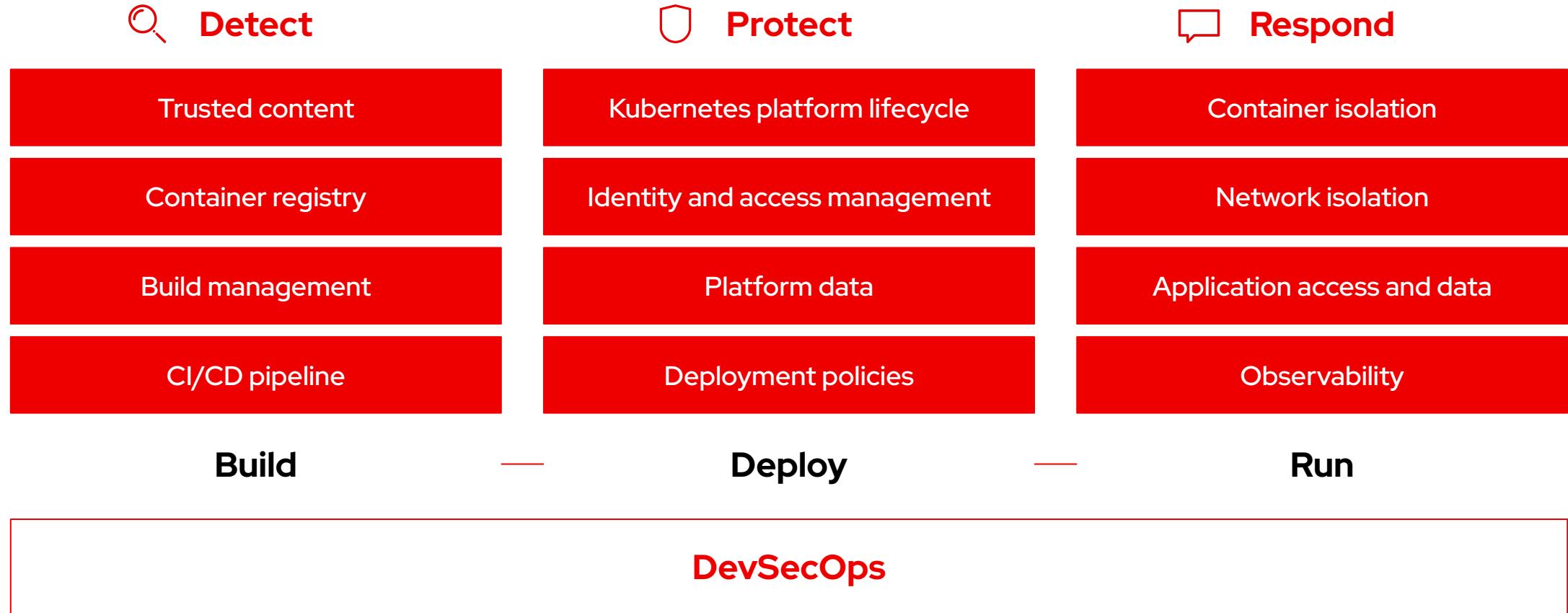
Leverage built-in Kubernetes CSPM to identify and remediate risky configurations

Cloud workload protection (CWPP)

Secure workloads

Maintain and enforce a “zero-trust execution” approach to workload protection

Red Hat OpenShift provides a secure foundation



RHACS delivers security depth to entire application lifecycle

Detect

Trusted content
Container registry
Build management
CI/CD pipeline

Protect

Kubernetes platform lifecycle
Identity and access management
Platform data
Deployment policies

Respond

Container isolation
Network isolation
Application access and data
Observability



Vulnerability analysis
App config analysis
APIs for CI/CD integrations

Image assurance and policy admission controller
Compliance assessments
Risk profiling

Runtime behavioral analysis
Auto-suggest network policies
Threat detection / incident response

Build

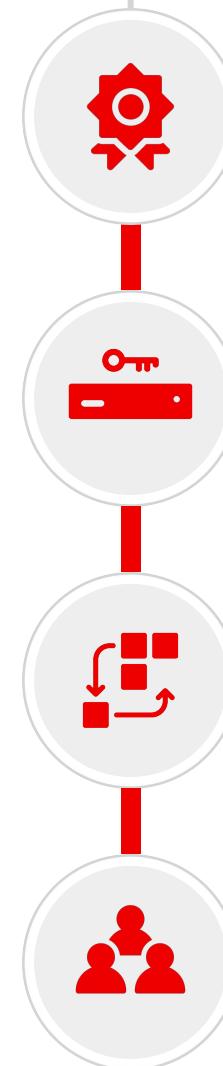
Deploy

Run

DevSecOps



RED HAT QUAY



Industry-leading, **trusted**, and **open source** registry platform operating at scale since 2014

Built to **efficiently manage content** under governance and security **controls** globally

Runs **everywhere**, easy to **integrate** and **automate** but works best with **OpenShift**

Developed in **collaboration** with a broad open source, customer, and ecosystem **community**

Red Hat Quay Key Features

Massive Scale Testing Quay.io
Real Time Garbage Collection
Automated Squashing

SCALABILITY

Seamless Git Integration
Build Workers
Webhooks

BUILD AUTOMATION

Extensible API
Webhooks, OAuth
Robot Accounts

INTEGRATION

Vulnerability Scanning
Logging & Auditing
Notifications & Alerting

SECURITY

REGISTRY

High Availability
Full Standards / Spec Support
Long-Term Protocol Support
Application Registry
Enterprise Grade Support
Regular Updates

CONTENT DISTRIBUTION

Geo-Replication
Repository Mirroring
Air-Gapped Environments

ACCESS CONTROL

Authentication Providers
Fine-Grained RBAC
Organizations & Teams

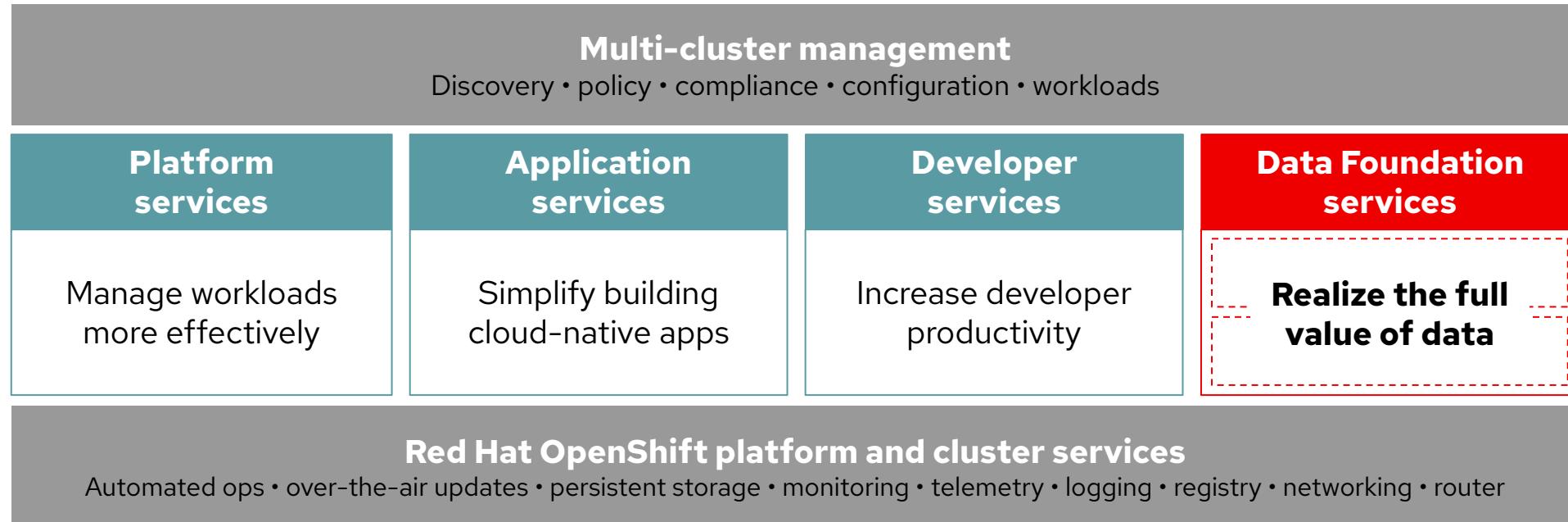


Red Hat
Data Services

Red Hat OpenShift Data Foundation 4.x

How Red Hat Data Foundation services fit

CONFIDENTIAL designator



Physical



Virtual machines



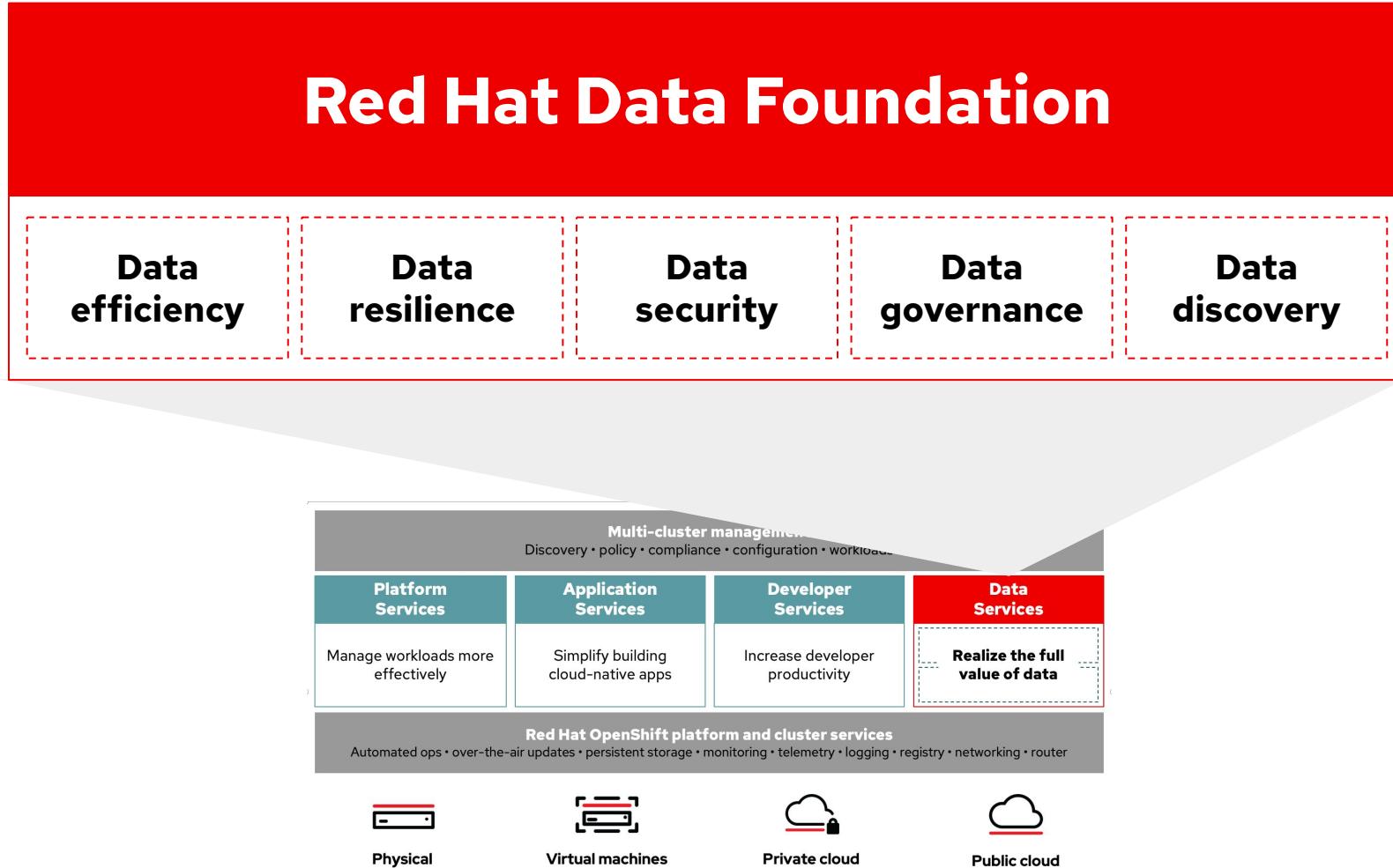
Private cloud



Public cloud

The Red Hat Data Foundation opportunity

CONFIDENTIAL designator

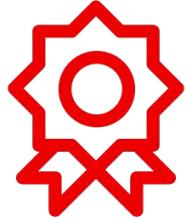


Red Hat Data Foundation in a nutshell

CONFIDENTIAL designator



Data efficiency



Data resilience



Data security



Data governance



Data discovery

- Erasure coding
- Compression
- Performance

- Snapshots
- Clones
- Backup
- Recovery
- Business continuity
- Disaster recovery

- At rest encryption
- In flight encryption
- Key management

- WORM
- Auditing
- Compliance
- SEC & FINRA
- GDPR

- Cataloging
- Tagging
- Search

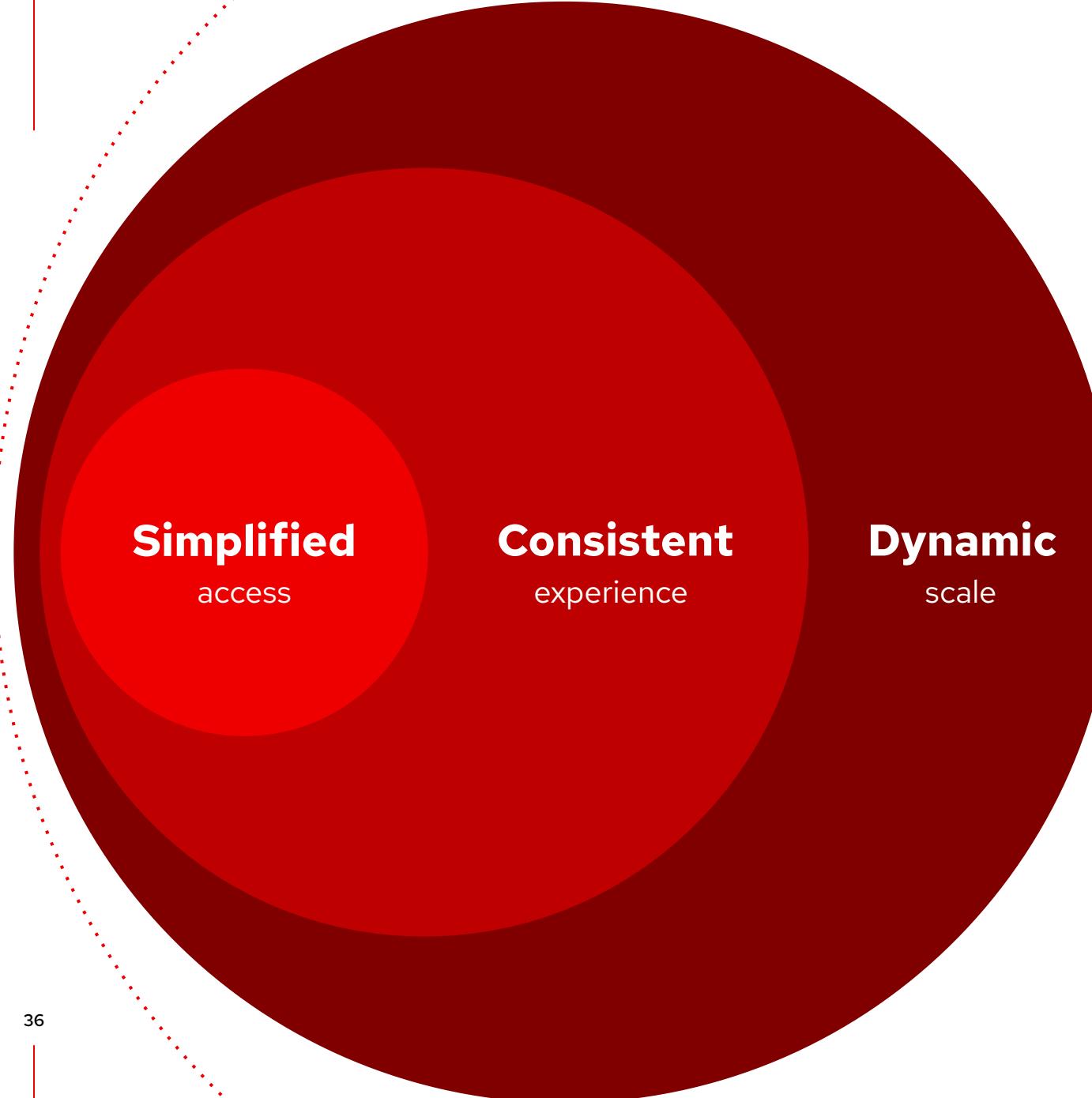


Traditional, static approach

- Focus on improving efficiency
- Infrastructure-up view
- Poor performance at scale
- Disconnected
- Manual, monolithic and rigid

Dynamic, data foundation approach

- Focus on innovation
- Application-oriented view
- Highly scalable
- Always-on
- Automated, on-demand, and flexible



Red Hat Data Services
mission:

To make data
accessible to
applications across
the hybrid cloud,
unlocking its power
in new and
impactful ways

Delivering on the Red Hat OpenShift
promise:

Innovation without
limitation

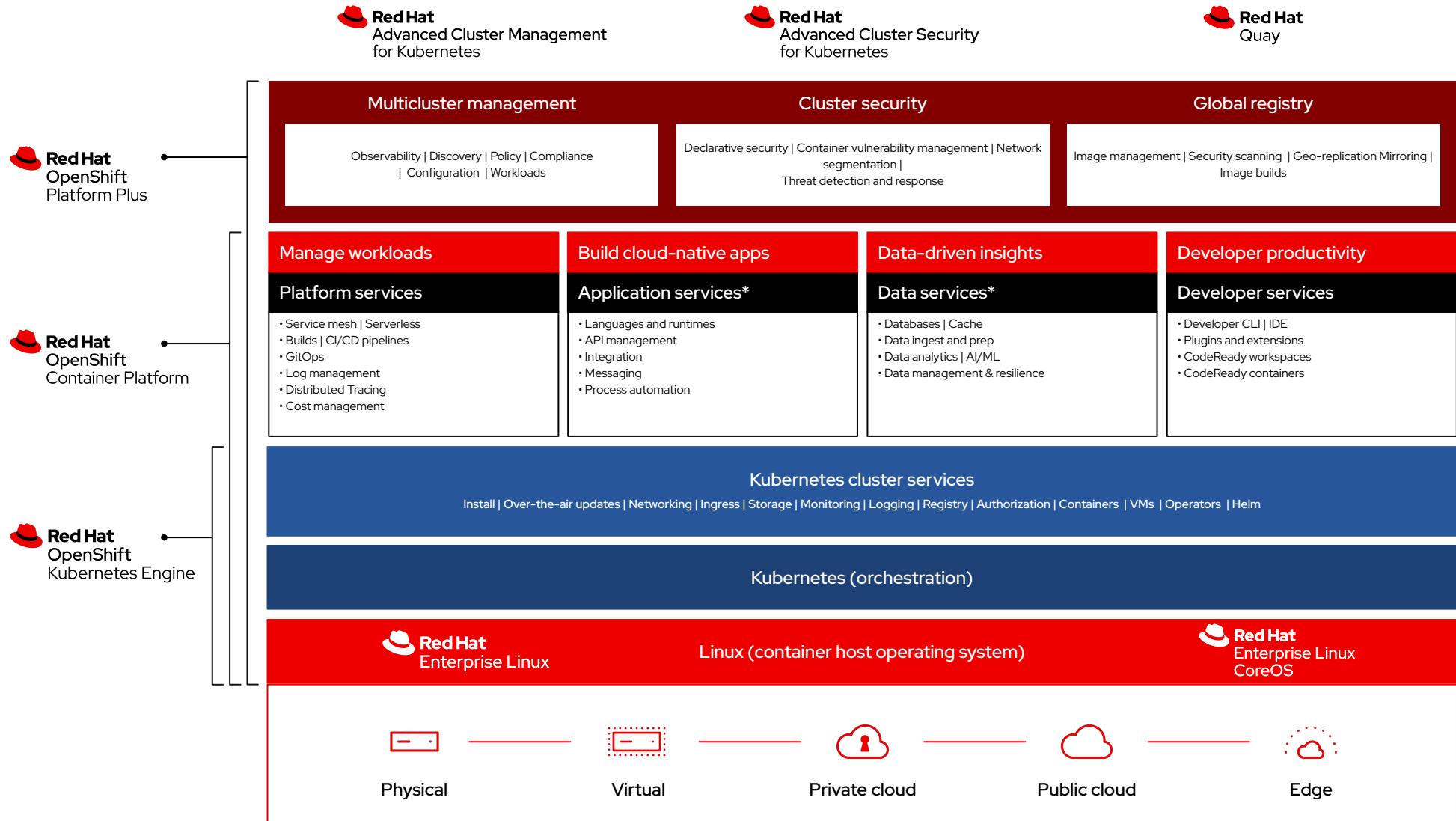
Data is the most significant asset in today's businesses—give it data foundation

CONFIDENTIAL designator



- Data foundation focuses on infrastructure and application needs so they can run and interact with ease and efficiency
- Provides a foundational data layer for applications to function and interact with data in a simplified, consistent and scalable manner
- Red Hat Ceph Storage is a foundational component to drive data services

Red Hat OpenShift



Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



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



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



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



twitter.com/RedHat