IBM WW Z Security Conference

October 6-9, 2020

Securing Workloads with OpenShift Cloud Platform on IBM Z / LinuxONE

Pradeep Parameshwaran , IBM Research and Development, Germany

Security & Compliance Lead, Linux on IBM Z & LinuxONE

PRADEEP@de.ibm.com

Contents

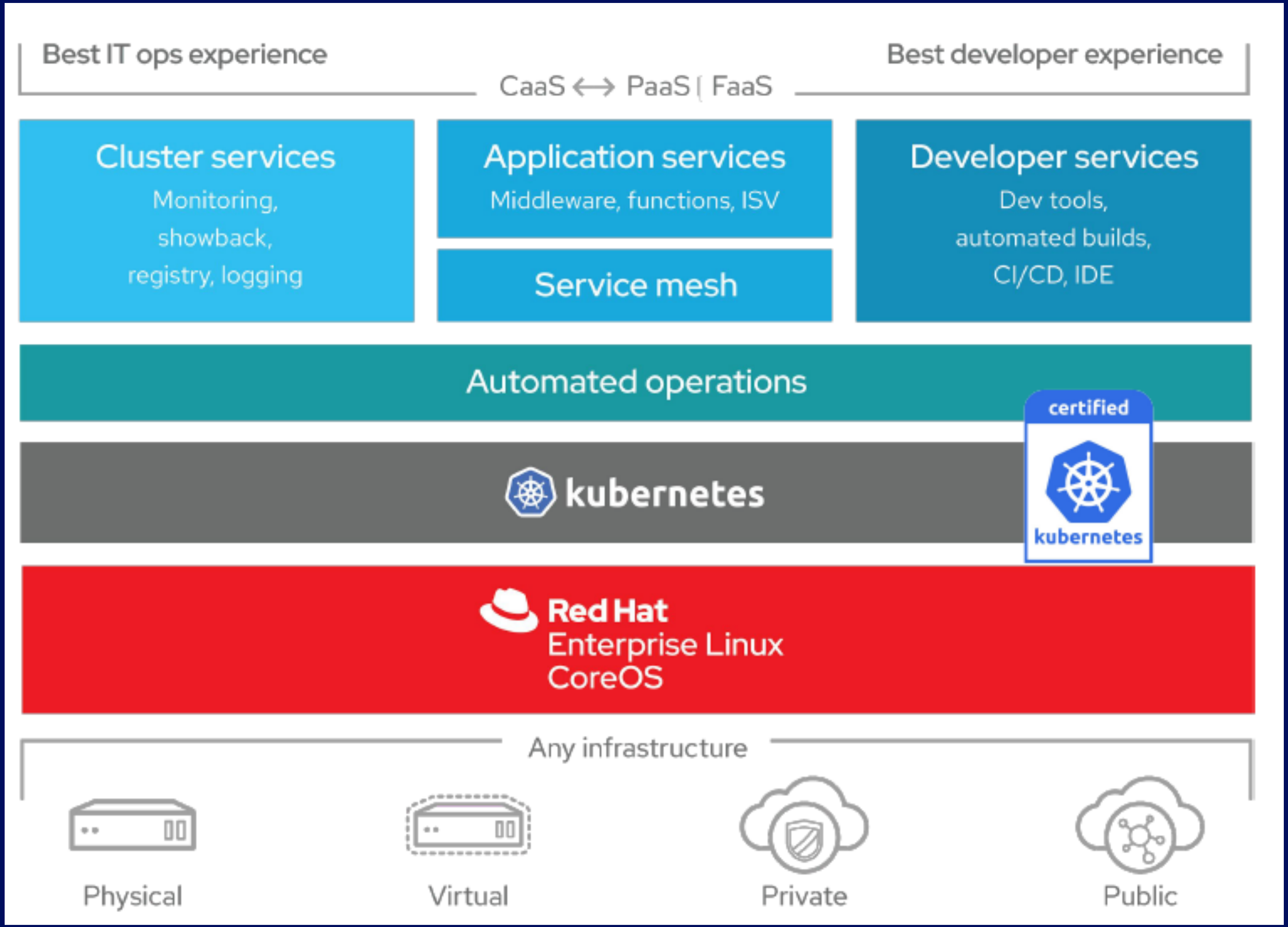
- Why OpenShift on IBM Z ?
- The cloud with the Privacy and Security
- Deployment architecture: OpenShift on IBM Z
- Security blueprint: OpenShift on IBM Z
- Summary of native and augmented security capabilities

IDC estimates that 71% of organizations are in the process of implementing containers and orchestration or are already using them regularly.

Containers are the next generation of software-defined compute that enterprises will leverage to accelerate their digital transformation initiatives," says Gary Chen, Research Director at IDC. "IDC estimates that 71% of organizations are in the process of implementing containers and orchestration or are already using them regularly, and IDC forecasts that the worldwide container infrastructure software opportunity is growing at a 63.9 % 5-year CAGR and is predicted to reach over $1.5B by 2022.

Why Red Hat OpenShift on IBM Z?

OpenShift a smart Kubernetes platform



Best IT ops experience

Best developer experience

CaaS ⟷ PaaS | FaaS

Cluster services

Monitoring,
showback,
registry, logging

Application services

Middleware, functions, ISV

Service mesh

Developer services

Dev tools,
automated builds,
CI/CD, IDE

Automated operations

certified kubernetes

kubernetes

Red Hat
Enterprise Linux
CoreOS

Any infrastructure

Physical

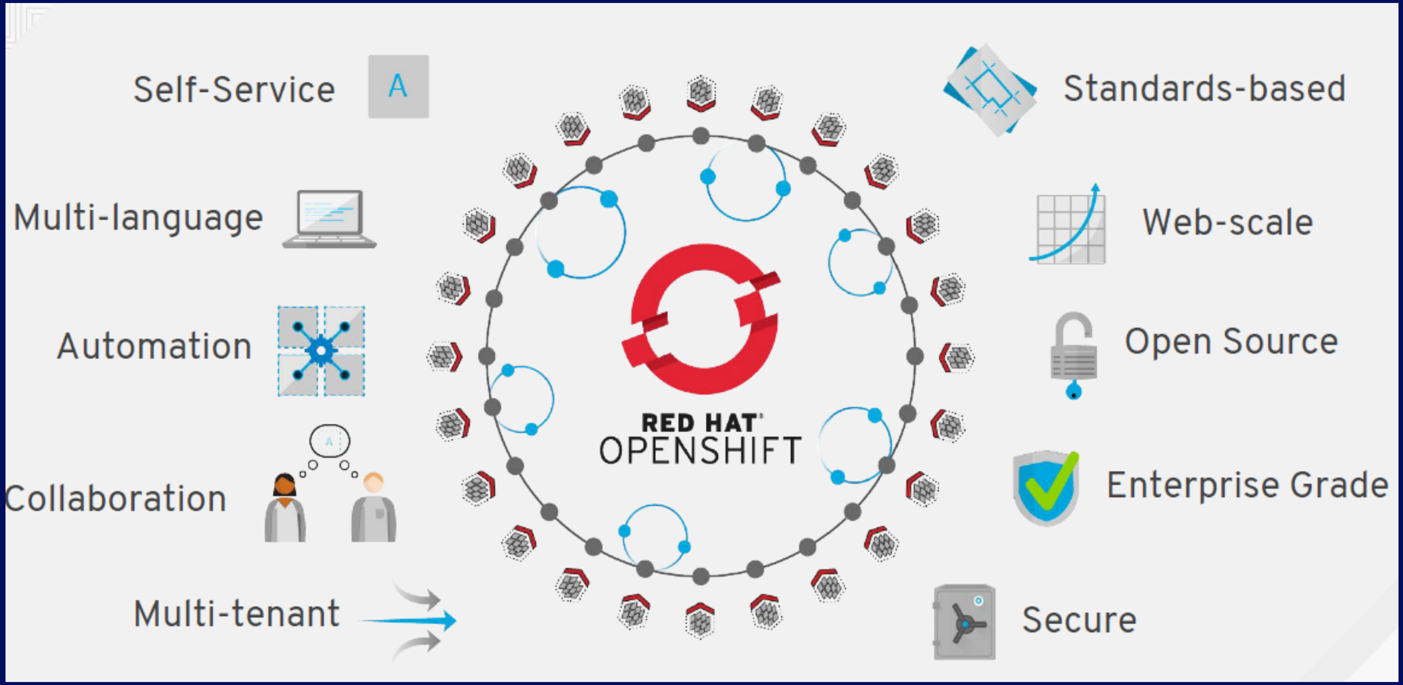
Virtual

Private

Public

Build once

- Fully integrated and automated architecture
- Seamless Kubernetes deployment on any cloud or on-premises environment
- Fully automated installation, from cloud infrastructure to OS to application services
- One click platform and application updates
- Auto-scaling of cloud resources
- Enterprise-grade security
- Ability to run enterprise workloads, “with enterprise build/manage services”, across all/multiple deployment options (private, public, hybrid/Multicloud)



Deploy anywhere

By combining the agility and portability of Red Hat OpenShift with the security features, scalability and reliability of IBM Z, businesses will have the tools to build new cloud-native applications while also modernizing current applications. Deploying Red Hat OpenShift on IBM Z reinforces key strengths and offers additional benefits →

- **Vertical scalability:**

enables existing large monolithic applications to be containerized, and horizontal scalability enables support for large numbers of containers in a single IBM Z

- **Security:**

Designed to protect data from external attacks and insider threats, with pervasive encryption

- **Reliability:**

Designed for 99.999% and more availability to meet service levels and customer expectations

- **Speed:**

Integration and co-location of cloud-native applications on the same system as the data enables faster response times than depending on network access speeds

Enterprise hybrid cloud with IBM Z

Why IBM Z

- Low latency and large-volume data serving and transaction processing
- Enterprise-class infrastructure: elastic, scalable, available and resilient
- Highest levels of security and compliance

Adoption patterns

- Enterprise-scale private cloud in a box
- Digital transformation and modernization for IBM z/OS®
- Built-in secure enclaves for zero-trust cloud native
- Extreme consolidation and scalable data serving

Scale out to 2.4 million containers on a single *system**

Reduce data center footprint by *50%#*

Process over 19 billion encrypted transactions per *day^*

* Performance result is extrapolated from IBM internal tests running in a z15 LPAR with 1 dedicated IFL and 16 GB memory 980 NGINX Docker containers. Results may vary. Operating system was SLES12 SP4 (SMT mode). Docker 18.09.6 and NGINX 1.15.9 was used.

^ This transaction rate is based on internal measurements of a z15 configuration consisting of 2 8-way LPARs and a 4-way ICF running with dataset encryption and CF encryption enabled. Using these results, full size z15 transaction rates were projected using standard LSPR MIPS. The performance that any user will experience may vary.

# On average, 70% of IBM z13 and z14 clients installing an IBM z15 can reduce raised floor space up to 50% or more depending on the configuration

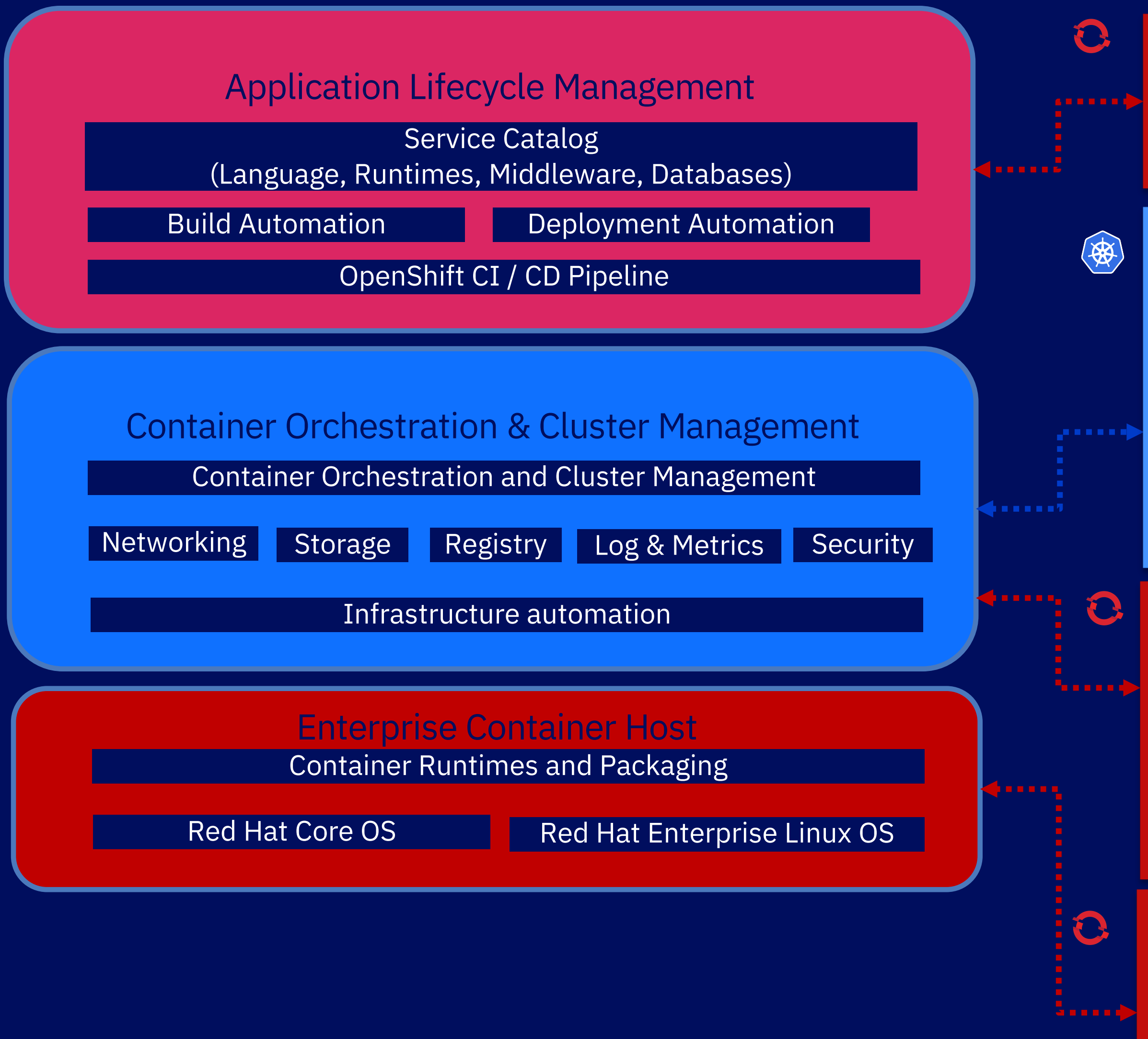
Red Hat
OpenShift

The cloud with the privacy and security

OpenShift and IBM Z with native security capabilities transforms into secure modern hybrid cloud

- OpenShift on IBM Z takes advantage of the underlying enterprise capabilities of the IBM Z server platforms, including advanced security, vertical and horizontal scalability, and 99.999% availability.
- A private cloud is a reliable and scalable cloud platform that runs on enterprise’s infrastructure. IBM Z infrastructure platform serve as the core of enterprise private cloud.
- IBM Z manage and integrate with the private cloud leveraging open standards and tech like Kubernetes, containers and microservices.
- Red Hat OpenShift and IBM Cloud Paks are designed to fully integrate IBM Z into a hybrid multicloud environment and manage everything from behind the firewall to help keep data protected from external attacks and insider threats.

Refer slides 14-18 for security capabilities overview of OpenShift and IBM Z



Application Lifecycle Management

Service Catalog
(Language, Runtimes, Middleware, Databases)

Build Automation

Deployment Automation

OpenShift CI / CD Pipeline

Container Orchestration & Cluster Management

Container Orchestration and Cluster Management

Networking

Storage

Registry

Log & Metrics

Security

Infrastructure automation

Enterprise Container Host

Container Runtimes and Packaging

Red Hat Core OS

Red Hat Enterprise Linux OS

- ✓ **Jenkins as a Service:** Supports CI/CD deployments, can utilise OCP OAuth authentication.
- ✓ **Quay - Private Registry:** Enterprise-quality container registry with image scanning (via Clair).
- ✓ **Integrated private registry:** Stores container images, retrieval permissions can be set.
- ✓ **S2I Build process:** Builds reproducible container images. Restricts the operations performed as a root user and can run the scripts as a non-root user.

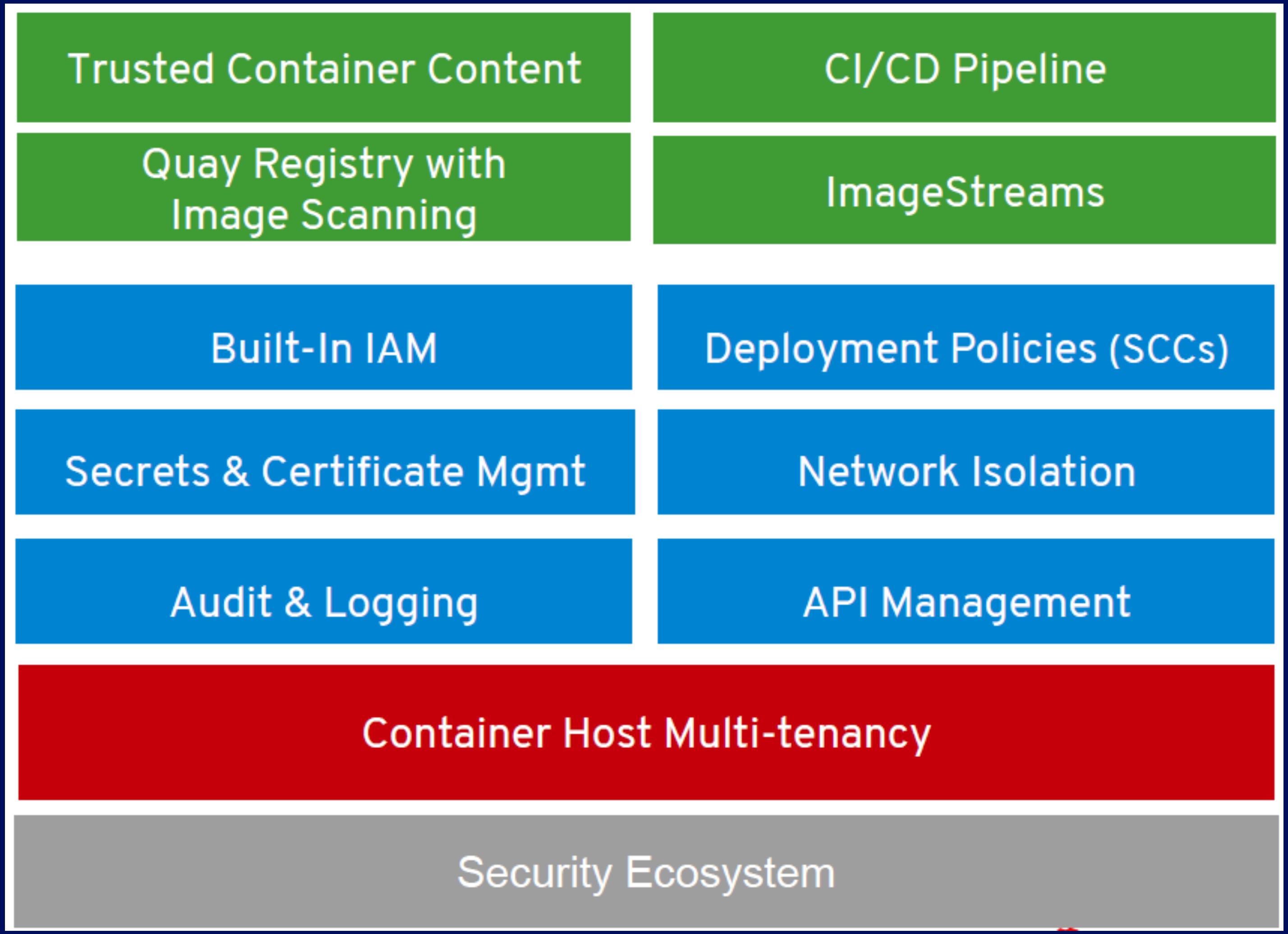
- ✓ **TLS:** Ensures secure control plane and API communication.
- ✓ **RBAC:** Authorizes user actions to occur within the cluster.
- ✓ **Admission Control:** Govern and enforce cluster resource configuration.
- ✓ **PSP & Security Contexts:** Admission control for pod security and privilege.
- ✓ **Secret Encryption:** Since 1.13, secrets in etcd can be encrypted at rest.
- ✓ **Audit:** API server auditing of each stage of every execution.
- ✓ **Resource Limitation:** Protect services from resource starvation.
- ✓ **Taints & Tolerations:** Enable service & node segregation and zoning via labels.
- ✓ **Namespace isolation:** Boundaries to segregate projects, tenants etc.
- ✓ **Network Policies:** Enable restriction of network communication within cluster and for cluster ingress/egress.

- + **CRI-O:** Container engine that interfaces with the container runtime that runs containers
- + **SCCs:** Opinionated control over security contexts permitted to pods (see K8s PSP).
- + **SDN (Project Isolation):** overlay network can isolate project pods & services.
- + **Integrated OAuth:** Provides token authentication for user interactions with API.
- + **OpenShift Service Mesh:** Provide secure comms for containers without changing application. Additional security authorization policies for extra granularity.
- + **Registry and Image Control:** Control which registries can be used and can label images to control their use.
- + **Scoped Tokens:** Cluster-admins can delegate permissions to other users.

- ✓ **SELinux:** enforces mandatory access control policies that confine user programs and system services, as well as access to files and network resources.
- ✓ **Cgroups:** enables fine grained control over allocating, managing etc. resource to containers.
- ✓ **Seccomp:** Allows a userspace program to set up syscall (user space requests into Linux kernel) filters.
- ✓ **Read-only file system:** Used by Atomic Host to prohibit unwanted file system change.
- ✓ **Kernel namespaces:** Partitioned kernel resources that provide isolated workspace (containers) .

OpenShift enables secure hybrid cloud with defense in depth

- **Linux Host Security**
  - SELinux+
  - FIPS mode
- **Authentication & Authorization**
  - Embedded OAuth Server
  - Supports 9 Identity Providers including AD/LDAP
  - Multi-Level Access Control (Users and Groups)
  - Secrets and certificate management
- **Image Security**
  - ImageStreams
  - Scanning
  - Deployment policies
- **Integrated Audit, Logging, Monitoring**
- **Security Policies**
  - SCC (Security Context Controls)
  - Non-Root Containers
  - Controlled Access to Resources
- **Networking Isolation**
  - Ingress / Egress control
  - Network microsegmentation
  - Encrypted East / West traffic



Trusted Container Content

CI/CD Pipeline

Quay Registry with Image Scanning

ImageStreams

Built-In IAM

Deployment Policies (SCCs)

Secrets & Certificate Mgmt

Network Isolation

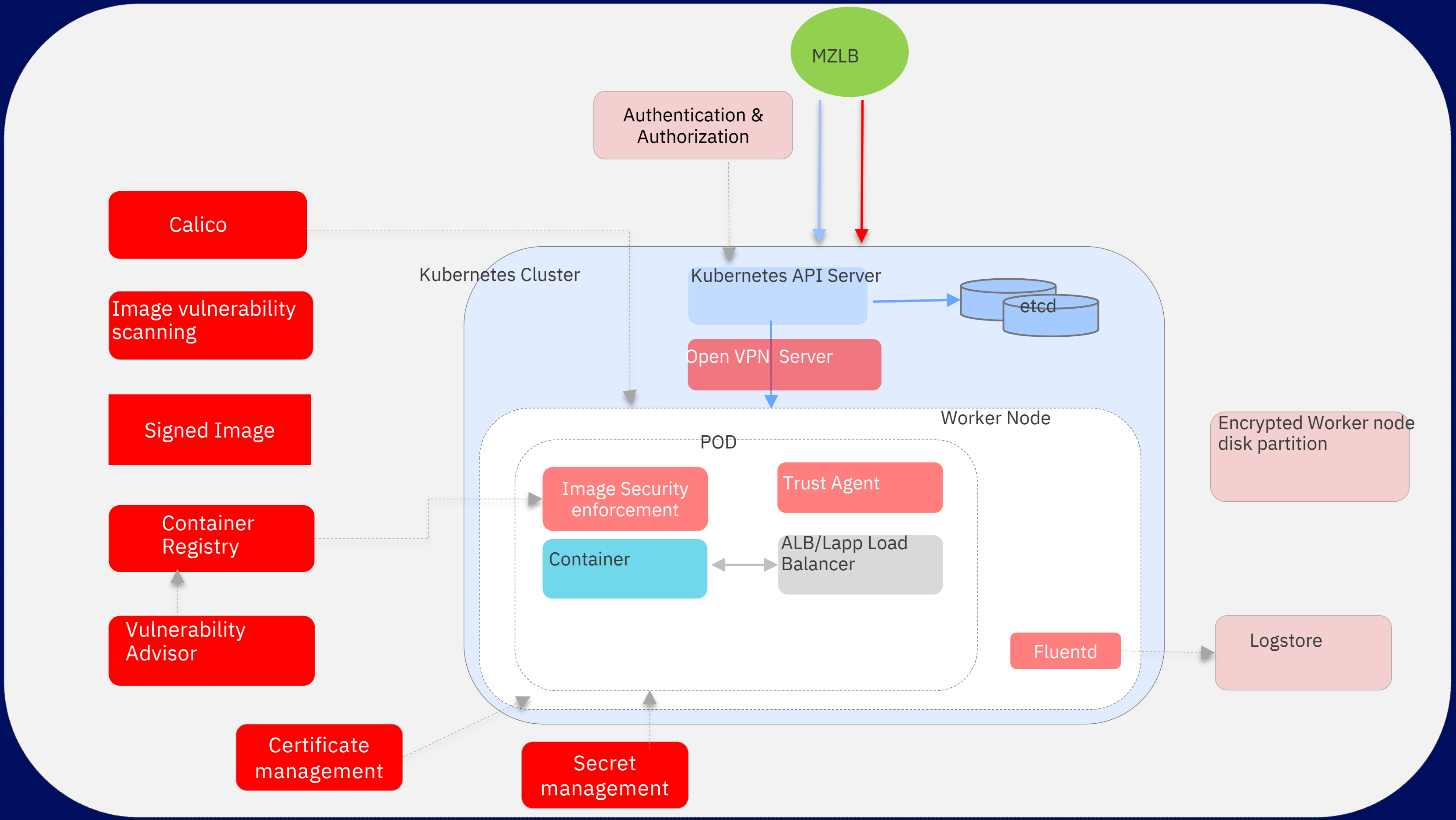
Audit & Logging

API Management

Container Host Multi-tenancy

Security Ecosystem

Overview of native security capabilities on OpenShift



PDF

Securing with OpenShift

Deployment security architecture: OpenShift on IBM Z

Red Hat OpenShift

OpenShift on IBM Z leveraging Z native security (z/VM), augmented by security services

Enterprise Key Management Foundation
Keys & Certificate Management

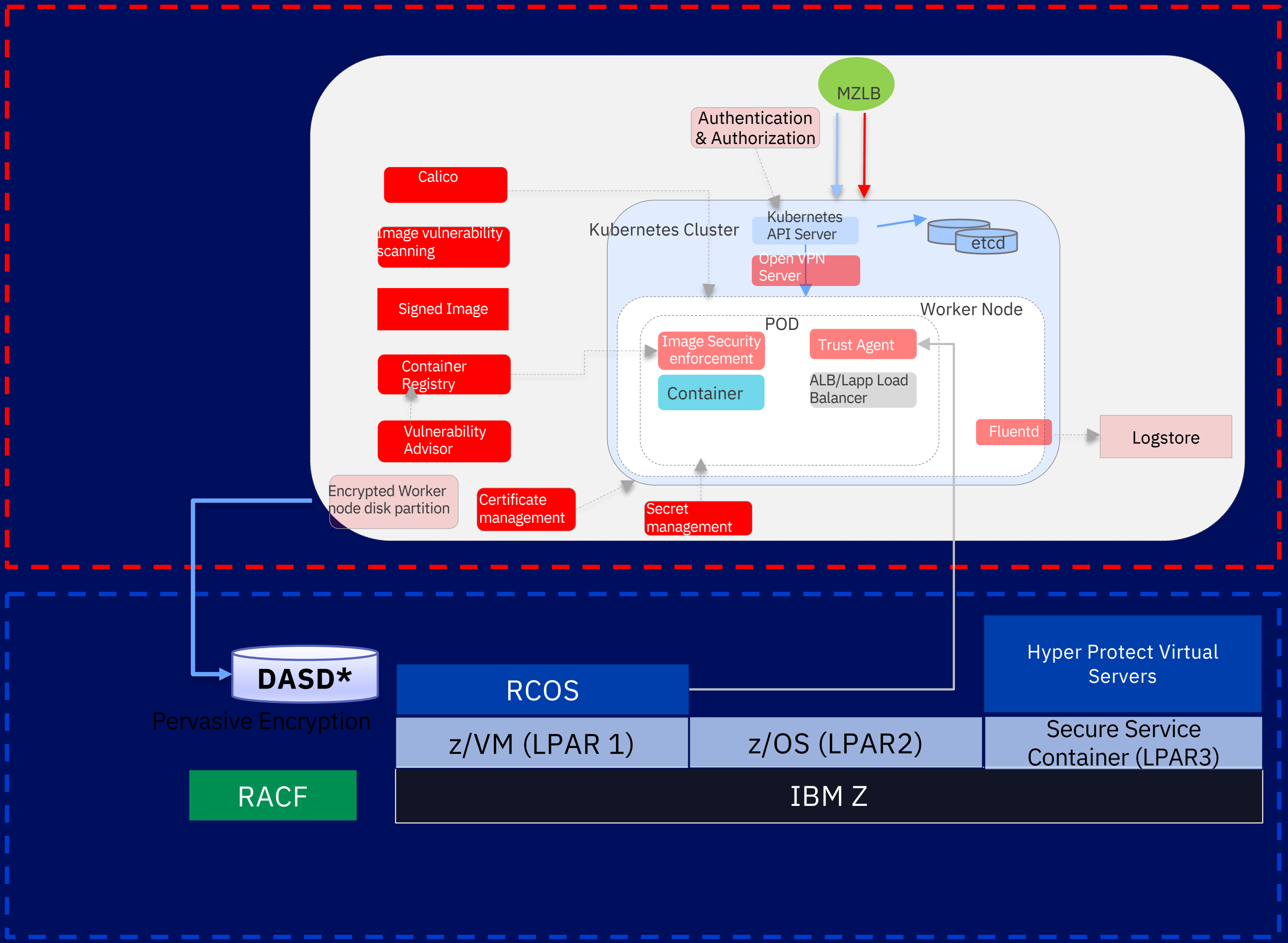
Guardium
Data Activity Monitoring

Qradar, zSecure
Security Intelligence, Audit & Reporting

IBM Identity Governance & Intelligence
Identity Governance on RACF , platform support services

DevSecOps
Secure container build, deploy and manage

Container security management



▭ Security capabilities augmented by IBM security services

▭ Security capabilities native in IBM Z

▭ Security capabilities native in OpensSift platform

* IBM DS8900F supports Red Hat OpenShift (through OpenShift flex volume driver support)

OpenShift on IBM Z leveraging Z native security (z/OS Cloud Broker), augmented by security services

Enterprise Key Management Foundation
Keys & Certificate Management

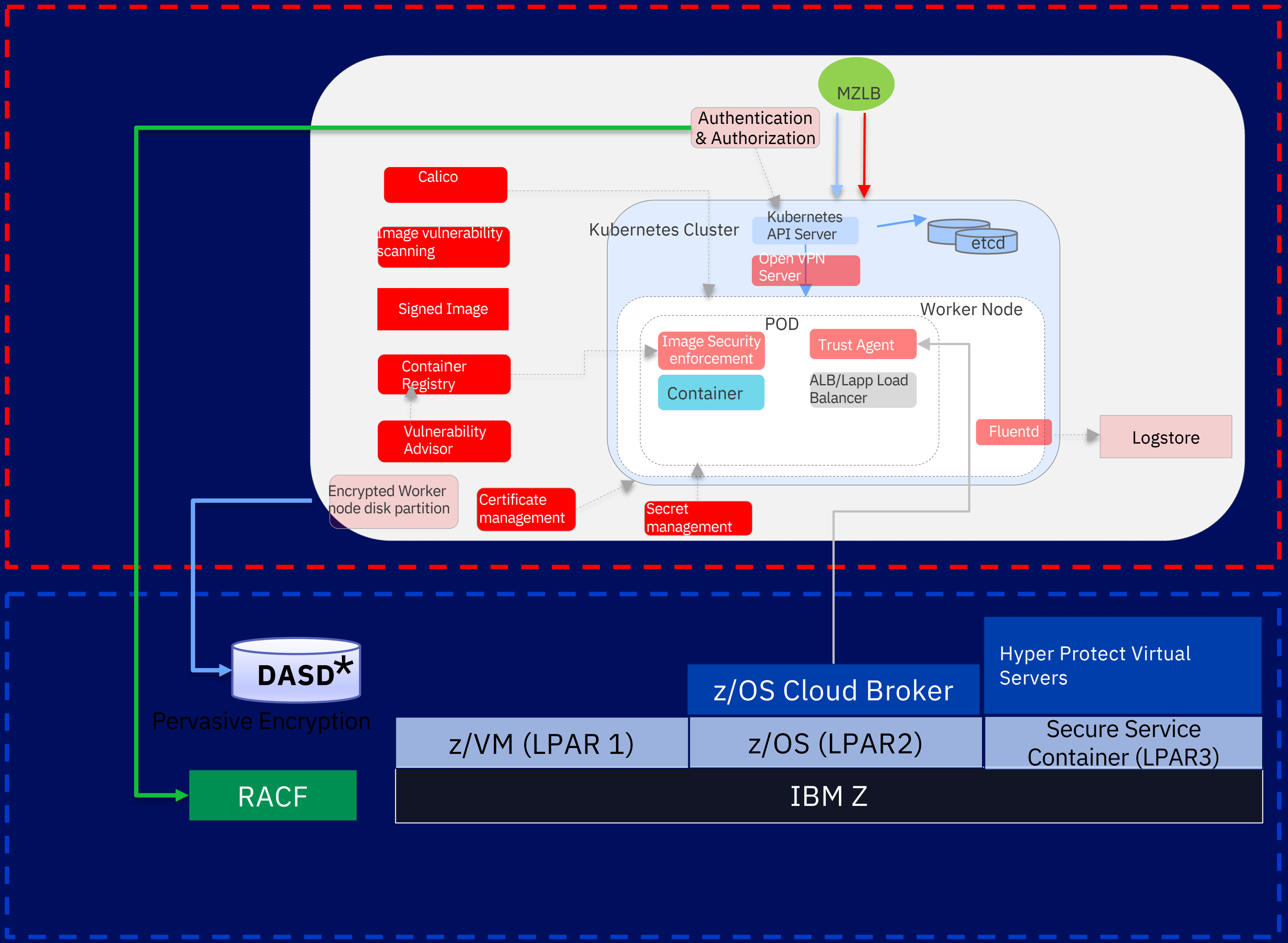
Guardium
Data Activity Monitoring

Qradar, zSecure
Security Intelligence, Audit & Reporting

IBM Identity Governance & Intelligence
Identity Governance on RACF , platform support services

DevSecOps
Secure container build, deploy and manage

Container security management



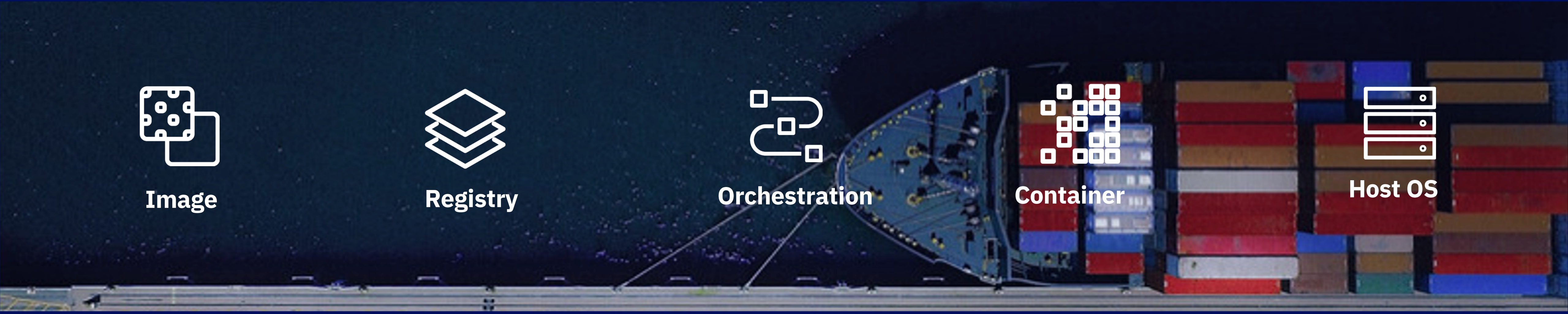
Security capabilities augmented by IBM security services

Security capabilities native in IBM Z

Security capabilities native in OpensSift platform

* IBM DS8900F supports Red Hat OpenShift (through OpenShift flex volume driver support)

Container environment introduces new threat vectors



Image

- Image vulnerabilities
- Configuration defects
- Embedded malware
- Embedded clear text secrets
- Untrusted images

Registry

- Insecure connections to registries
- Stale images in registries
- Insufficient authentication
- Insufficient authorization restrictions

Orchestration

- Unrestricted admin access
- Unauthorized orchestrator access
- Poorly isolated inter-container network traffic
- Mixing of workload sensitivity levels

Container

- Runtime software vulnerabilities
- Unbounded network access
- Insecure runtime configurations
- App vulnerabilities
- Rogue containers

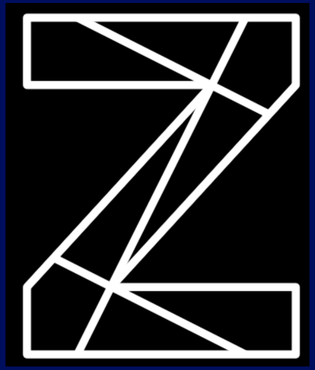
Host OS

- Large attack surface
- Host OS component vulnerabilities
- Improper user access rights
- Host OS file system tampering
- Poor host OS configuration

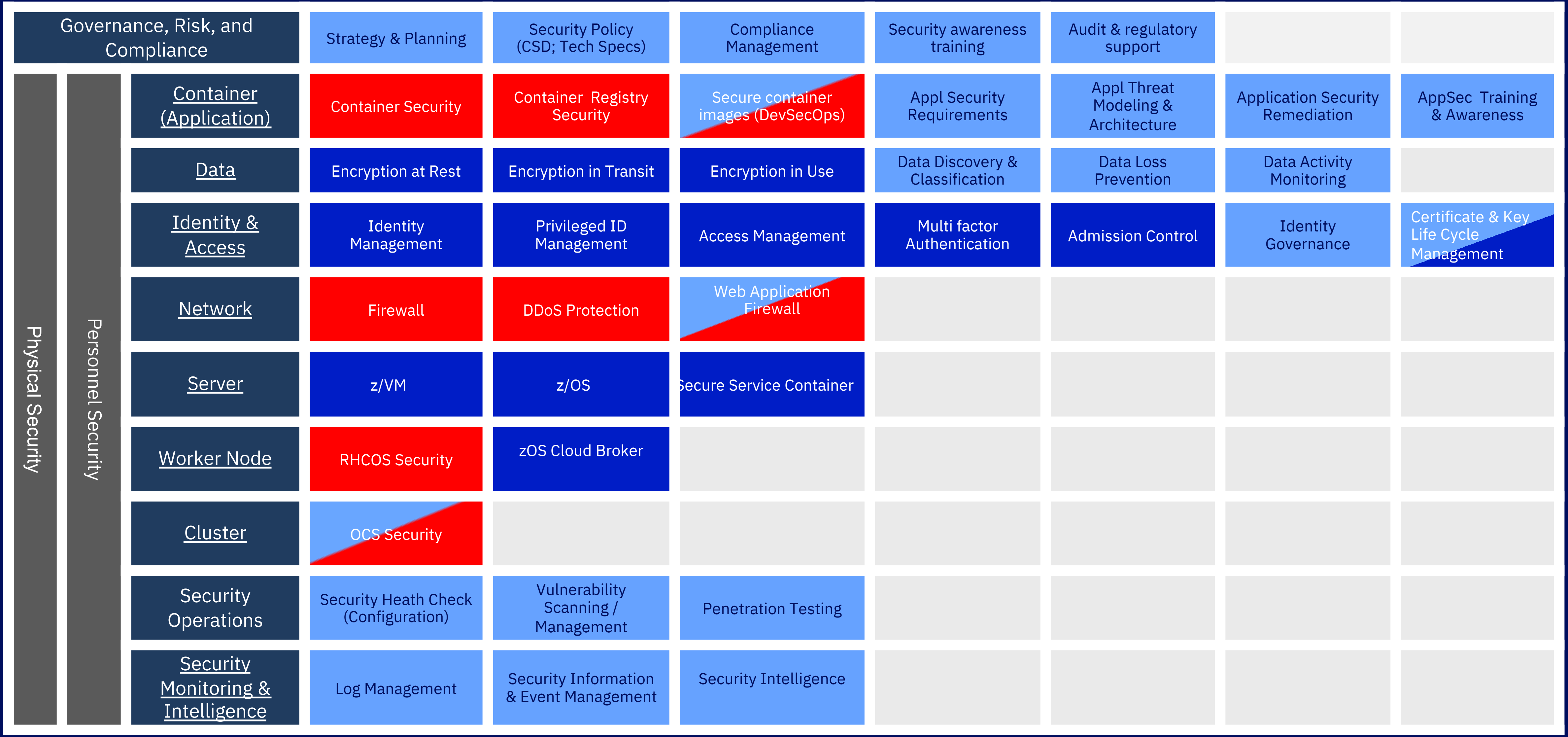
Source: NIST SP 800-190

Security architecture blueprint

Red Hat
OpenShift



Security blueprint – OpenShift on IBM Z



		Governance, Risk, and Compliance	Strategy & Planning	Security Policy (CSD; Tech Specs)	Compliance Management	Security awareness training	Audit & regulatory support		
Physical Security	Personnel Security	Container (Application)	Container Security	Container Registry Security	Secure container images (DevSecOps)	Appl Security Requirements	Appl Threat Modeling & Architecture	Application Security Remediation	AppSec Training & Awareness
		Data	Encryption at Rest	Encryption in Transit	Encryption in Use	Data Discovery & Classification	Data Loss Prevention	Data Activity Monitoring	
		Identity & Access	Identity Management	Privileged ID Management	Access Management	Multi factor Authentication	Admission Control	Identity Governance	Certificate & Key Life Cycle Management
		Network	Firewall	DDoS Protection	Web Application Firewall				
		Server	z/VM	z/OS	Secure Service Container				
		Worker Node	RHCOS Security	zOS Cloud Broker					
		Cluster	OCS Security						
		Security Operations	Security Heath Check (Configuration)	Vulnerability Scanning / Management	Penetration Testing				
		Security Monitoring & Intelligence	Log Management	Security Information & Event Management	Security Intelligence				

The Blueprint provides security capabilities required. The color of cell suggests capabilities leveraged from. Security Services can help select the right offering specific to the requirements.

OCP: OpenShift Container Platform

- OpenShift
- IBM Z
- IBM Security Service
- IBM Security service on z
- IBM Security service on OCP

Container (Application) Security Domain – Components

Security Domains	Security Controls	Security Components				
Container (Application)	Container Security	Container Security (TwistLock)	Container security (Aquasec)	Vulnerability scanning (OpenSCAP)		
	DevSecOps	Secure Image Build	SAST, DAST (AppScan)		Image Vulnerability Scanning (JfFog XRAY)	Image signing
	Container Registry Security	Container Registry (Quay, Clair)	Container Registry JFrog Artifactory			

References-

10 layers of container security

OCP DevSecOPs SANS reference

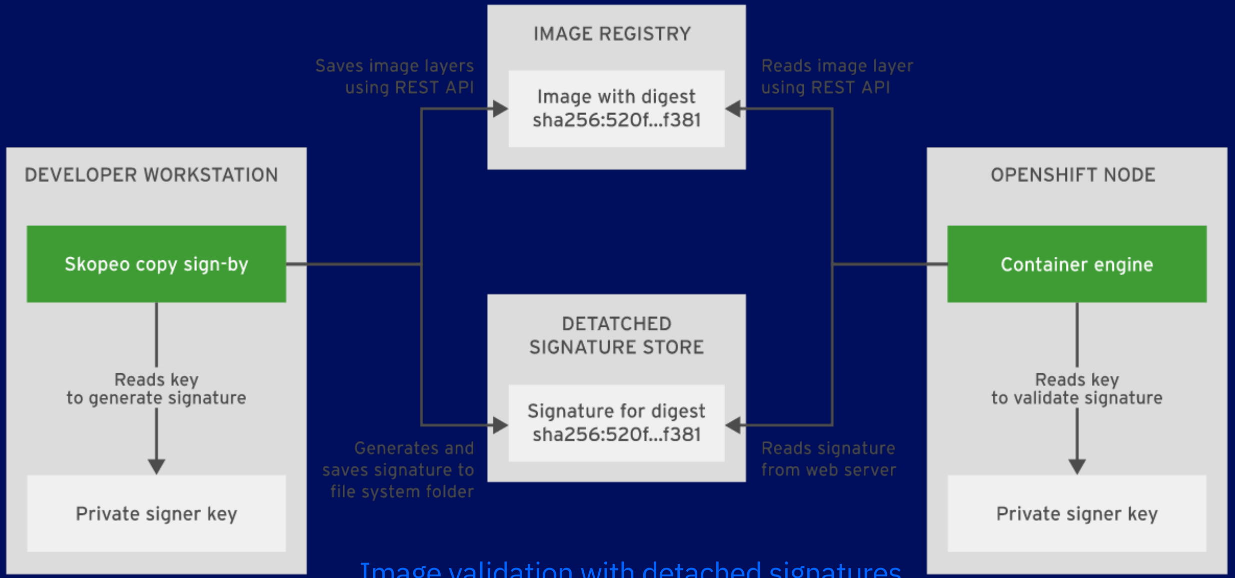


IMAGE REGISTRY
Image with digest sha256:520f...f381
Saves image layers using REST API
Reads image layer using REST API
DEVELOPER WORKSTATION
Skopeo copy sign-by
Reads key to generate signature
Private signer key
DETATCHED SIGNATURE STORE
Signature for digest sha256:520f...f381
Generates and saves signature to file system folder
Reads signature from web server
OPENSHIFT NODE
Container engine
Reads key to validate signature
Private signer key

Image validation with detached signatures

Legend:

Security Components

IBM Z native	IBM Security Services
OCP native	

Data Security Domain - Components

Security Domain	Security Controls	Security Components	
Data Security	Data discovery & classification	Guardium	
	Data encryption at rest	Dm-crypt	Data Privacy Passport
	Data encryption in transit	Data Privacy Passport	zERT
	Encryption in use	Data Privacy Passport	Libssl, libcrypto, ibmca, libica
	DLP	Guardium	
	Data activity monitoring	Guardium	
	Key management	ICSF	EKMF

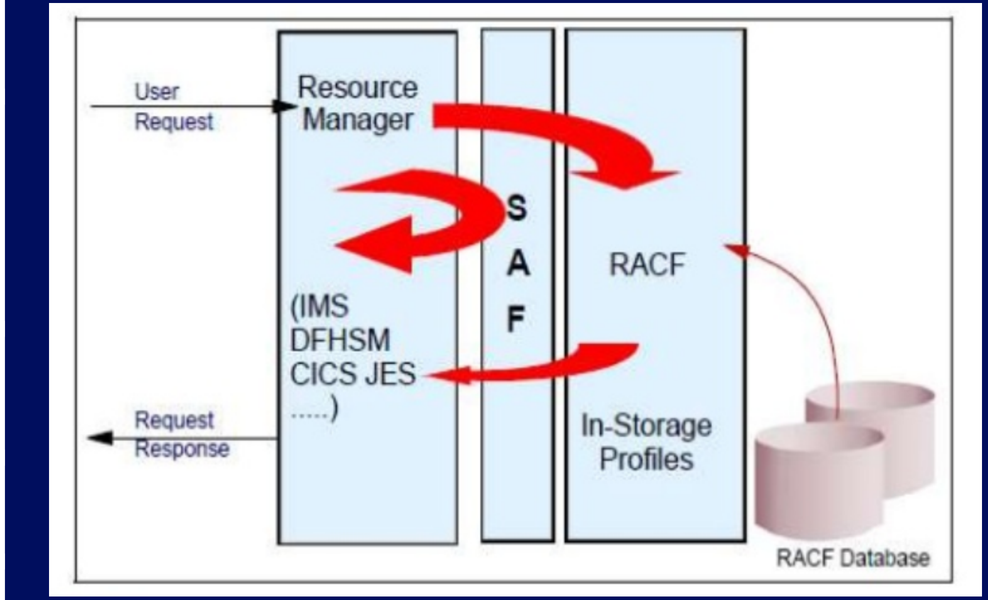
Legend:
Security Components

- IBM Z native
- OCP native
- IBM Security Services

ICSF: Integrated cryptographic service facility
EKMF: Enterprise key management foundation
DLP: Data leak prevention

Identity & Access (IAM) Security Domain - Components

Security Domain	Security Controls	Security Components		
Identity & Access	Identity Governance	Identity Governance & Administration	zSecure Admin	
	Identity Management	RACF	LDAP	IBM IAM
	Access Management			
	Privileged ID Management/Access Control	RACF	LDAP	PAM
	Multi factor authentication	IBM Z MFA		
	Admission control	Admission control plugin		



System authorization facility

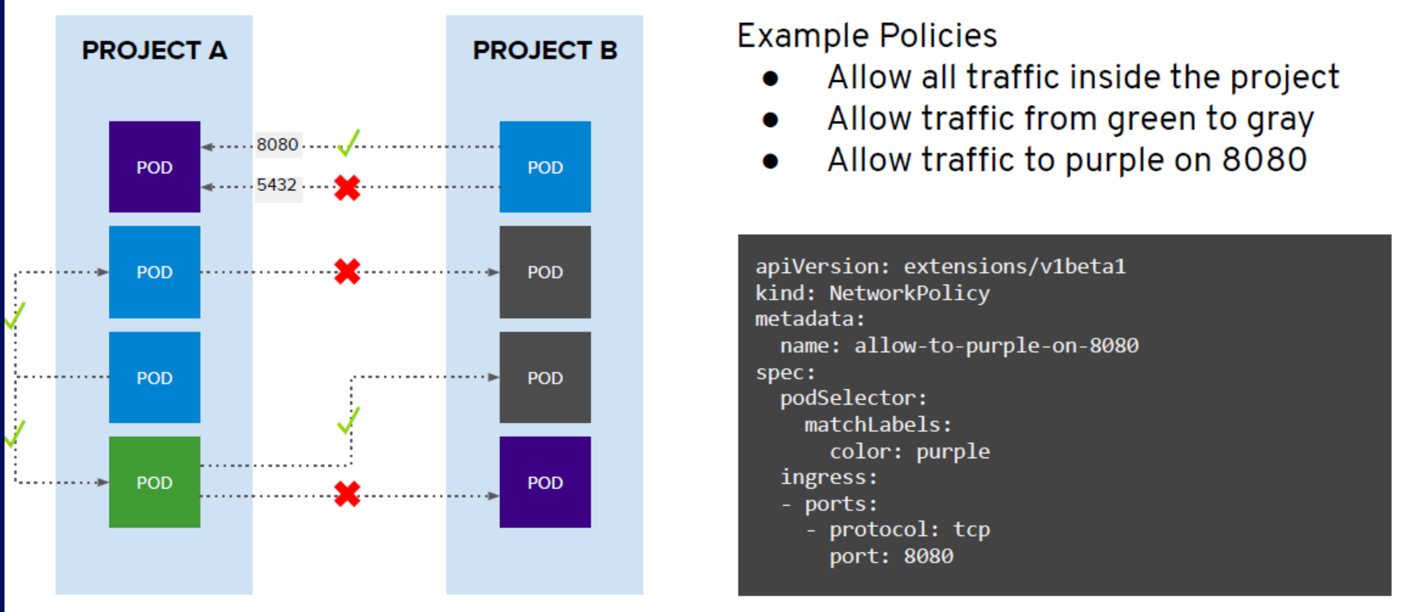
Legend:
Security Components

- IBM Z native
- OCP native
- IBM Security Services

PAM: Privileged Access Management
LDAP: Lightweight Directory Access Protocol
RACF: Resource Access Control Facility

Network Security Domain - Components

Security Domain	Security Controls	Security Components		
Network Security	Container Firewall	NeuVector	Ingress Cluster Traffic controller	Calico
	Web Application Firewall	NGINX		
	DDoS Protection	NGINX		



Example Policies

- Allow all traffic inside the project
- Allow traffic from green to gray
- Allow traffic to purple on 8080

```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
  - ports:
    - protocol: tcp
      port: 8080
```

OpenShift multitenancy- fine grained control with network policy

Legend:

Security Components

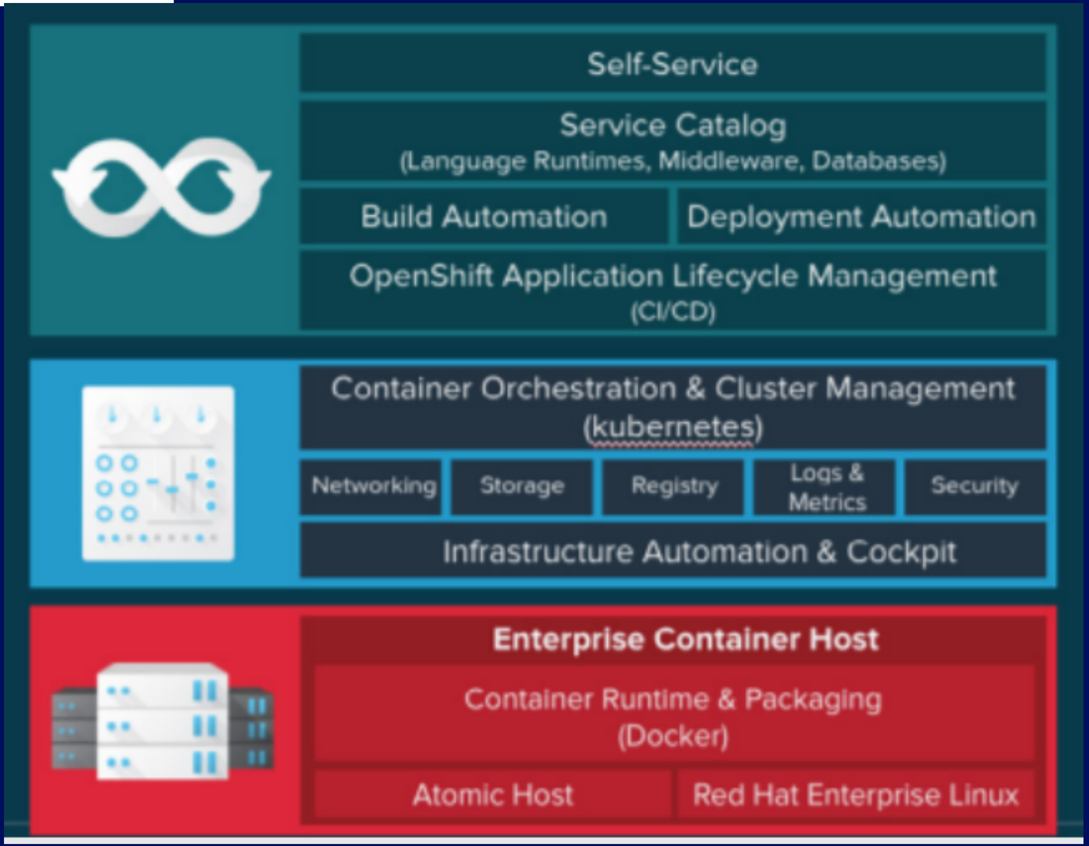
🟥 OCP native

🟦 IBM Security Services

Cluster Security Domain - Components

Security Domain	Security Controls	Security Components			
Cluster	Cluster Security	Security context constraints (SCCs)	Security with Sysdig	Twistlock	Hashicorp vault

Overview of OpenShift cluster. Each layer shall be secured to secure the cluster i.e from RHCOS till application lifecycle management and orchestration.


Self-Service
Service Catalog
(Language Runtimes, Middleware, Databases)
Build Automation
Deployment Automation
OpenShift Application Lifecycle Management
(CI/CD)
Container Orchestration & Cluster Management
(kubernetes)
Networking
Storage
Registry
Logs & Metrics
Security
Infrastructure Automation & Cockpit
Enterprise Container Host
Container Runtime & Packaging
(Docker)
Atomic Host
Red Hat Enterprise Linux

Legend:
Security Components

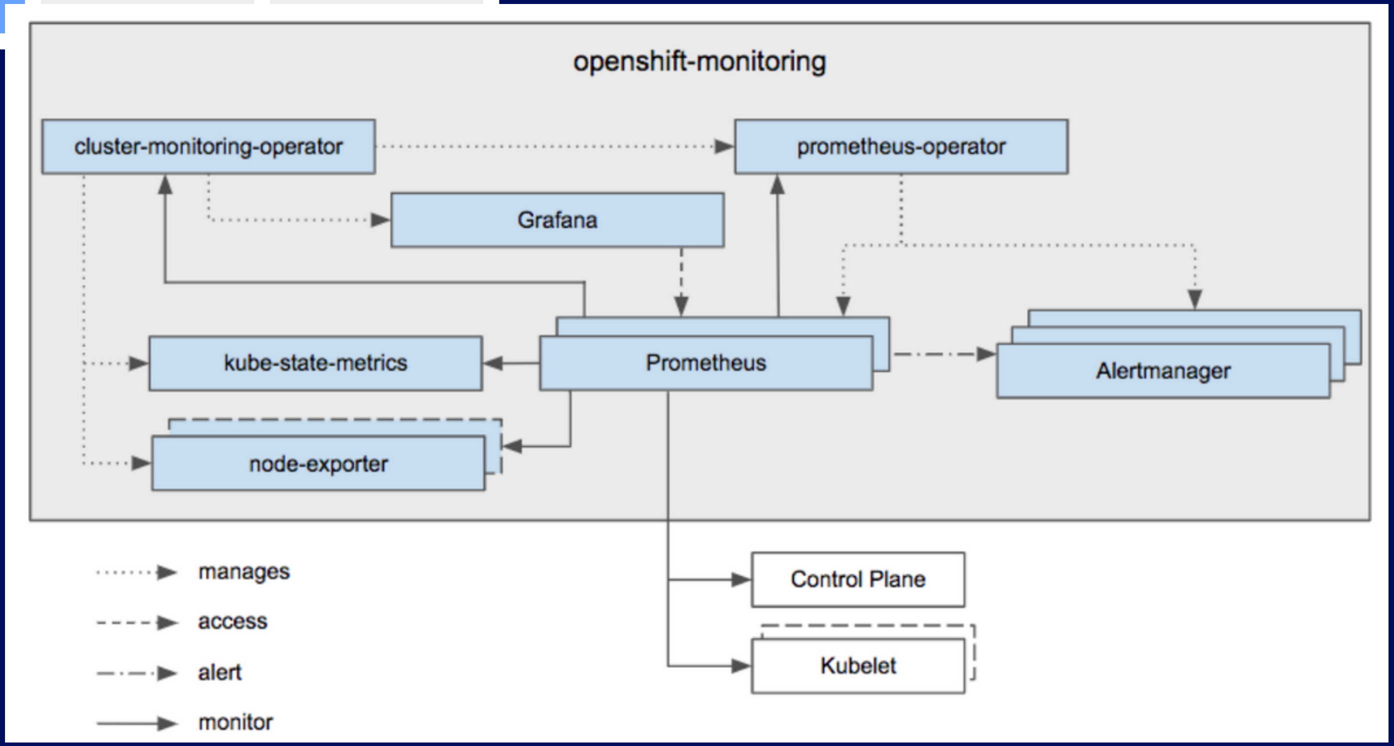
🟥 OCP native

🟦 IBM Security Services

Security Monitoring & Intelligence - Components

Security Domain	Security Controls	Security Components		
Security Monitoring & Intelligence	Logging & Log Management	EFK	Prometheus	zSecure adapter for SIEM
	Security Information & Event Management	QRadar		
	Security Intelligence	XFTM		

OpenShift Container Platform ships with a pre-configured and self-updating monitoring stack that is based on the Prometheus open source project



Legend:

Security Components

OCP native

IBM Security Services

Summary

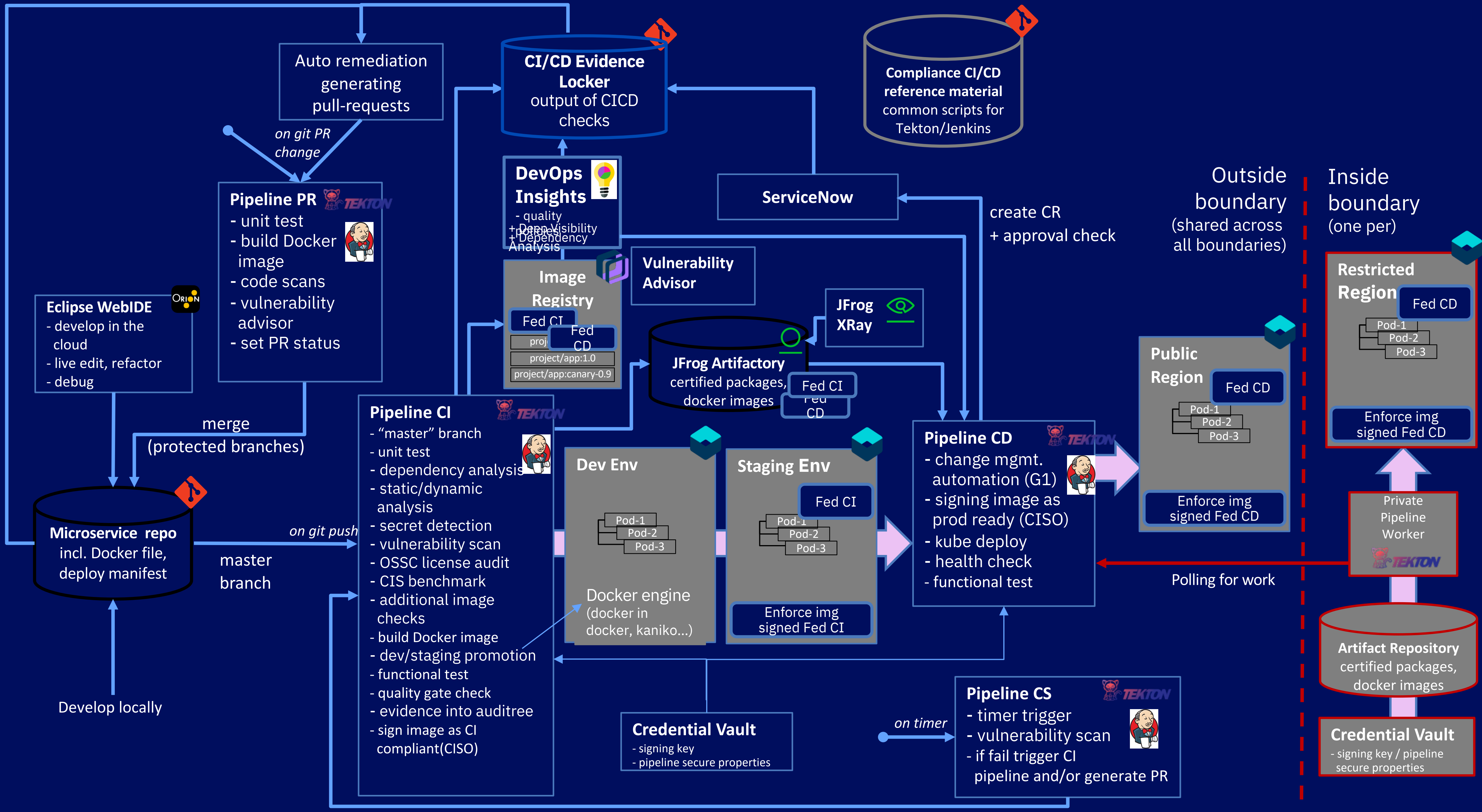
This session focused on,

- Secure Hybrid cloud deployment on IBM Z with OpenShift Cloud Platform
- Security Blueprint for OpenShift on IBM Z

Backup

DevSecOps with OpenShift Cloud Platform on IBM Z – Reference Architecture

Red Hat
OpenShift



Auto remediation generating pull-requests

CI/CD Evidence Locker
output of CICD checks

Compliance CI/CD reference material
common scripts for Tekton/Jenkins

on git PR change

DevOps Insights
- quality
- policies
+ Deep Visibility
+ Dependency Analysis

ServiceNow

create CR
+ approval check

Outside boundary
(shared across all boundaries)

Inside boundary
(one per)

Pipeline PR
- unit test
- build Docker image
- code scans
- vulnerability advisor
- set PR status

Image Registry
Fed CI
proj
Fed CD
project/app:1.0
project/app:canary-0.9

Vulnerability Advisor

JFrog XRay

JFrog Artifactory
certified packages, docker images
Fed CI
Fed CD

Restricted Region
Fed CD
Pod-1
Pod-2
Pod-3
Enforce img signed Fed CD

Public Region
Fed CD
Pod-1
Pod-2
Pod-3
Enforce img signed Fed CD

Eclipse WebIDE
- develop in the cloud
- live edit, refactor
- debug

merge
(protected branches)

Pipeline CI
- “master” branch
- unit test
- dependency analysis
- static/dynamic analysis
- secret detection
- vulnerability scan
- OSSC license audit
- CIS benchmark
- additional image checks
- build Docker image
- dev/staging promotion
- functional test
- quality gate check
- evidence into auditree
- sign image as CI compliant(CISO)

Dev Env
Pod-1
Pod-2
Pod-3
Docker engine
(docker in docker, kaniko...)

Staging Env
Fed CI
Pod-1
Pod-2
Pod-3
Enforce img signed Fed CI

Pipeline CD
- change mgmt. automation (G1)
- signing image as prod ready (CISO)
- kube deploy
- health check
- functional test

Private Pipeline Worker

Polling for work

Microservice repo
incl. Docker file, deploy manifest

on git push

master branch

Develop locally

Credential Vault
- signing key
- pipeline secure properties

on timer

Pipeline CS
- timer trigger
- vulnerability scan
- if fail trigger CI pipeline and/or generate PR

Artifact Repository
certified packages, docker images

Credential Vault
- signing key / pipeline secure properties