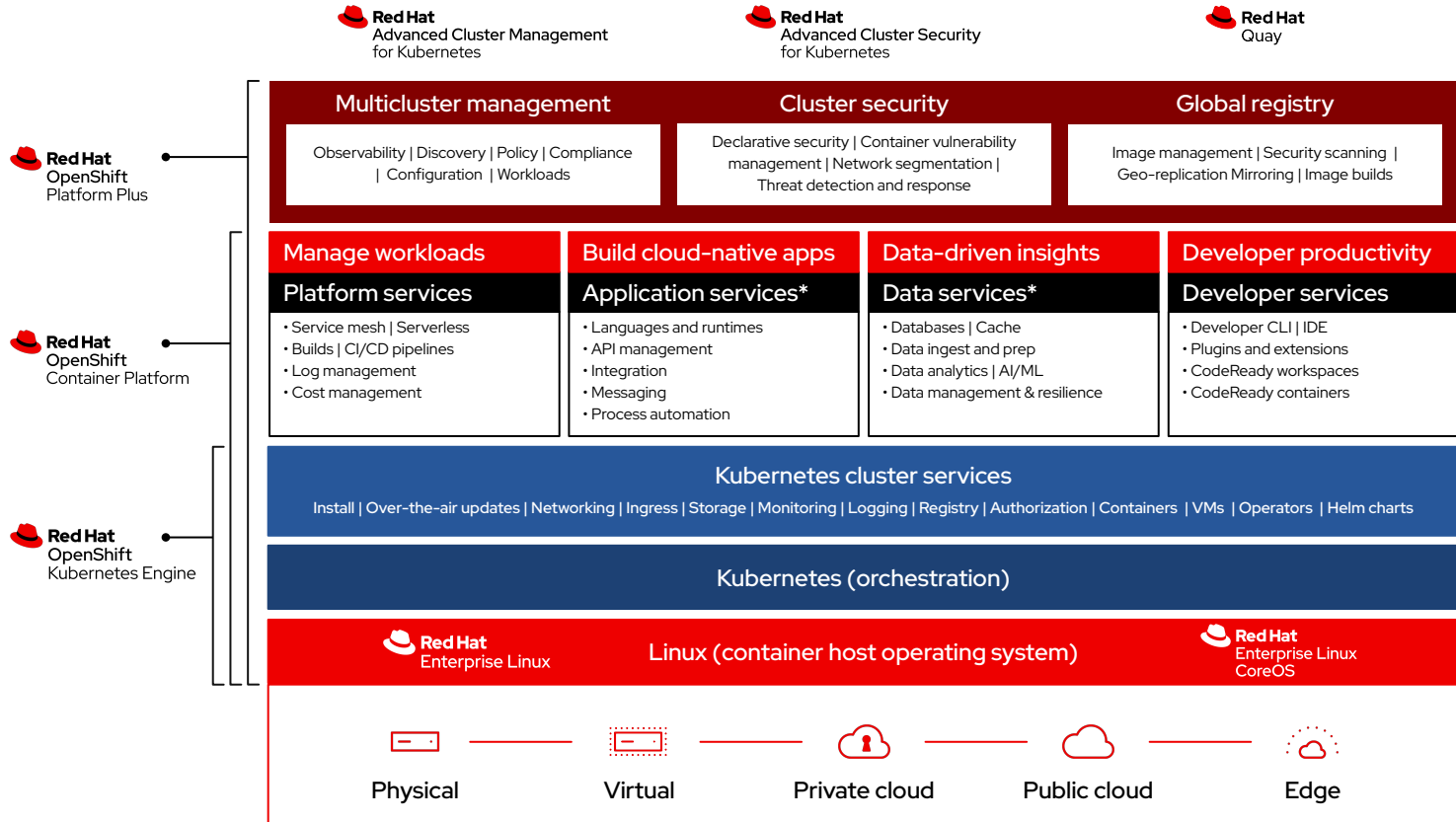




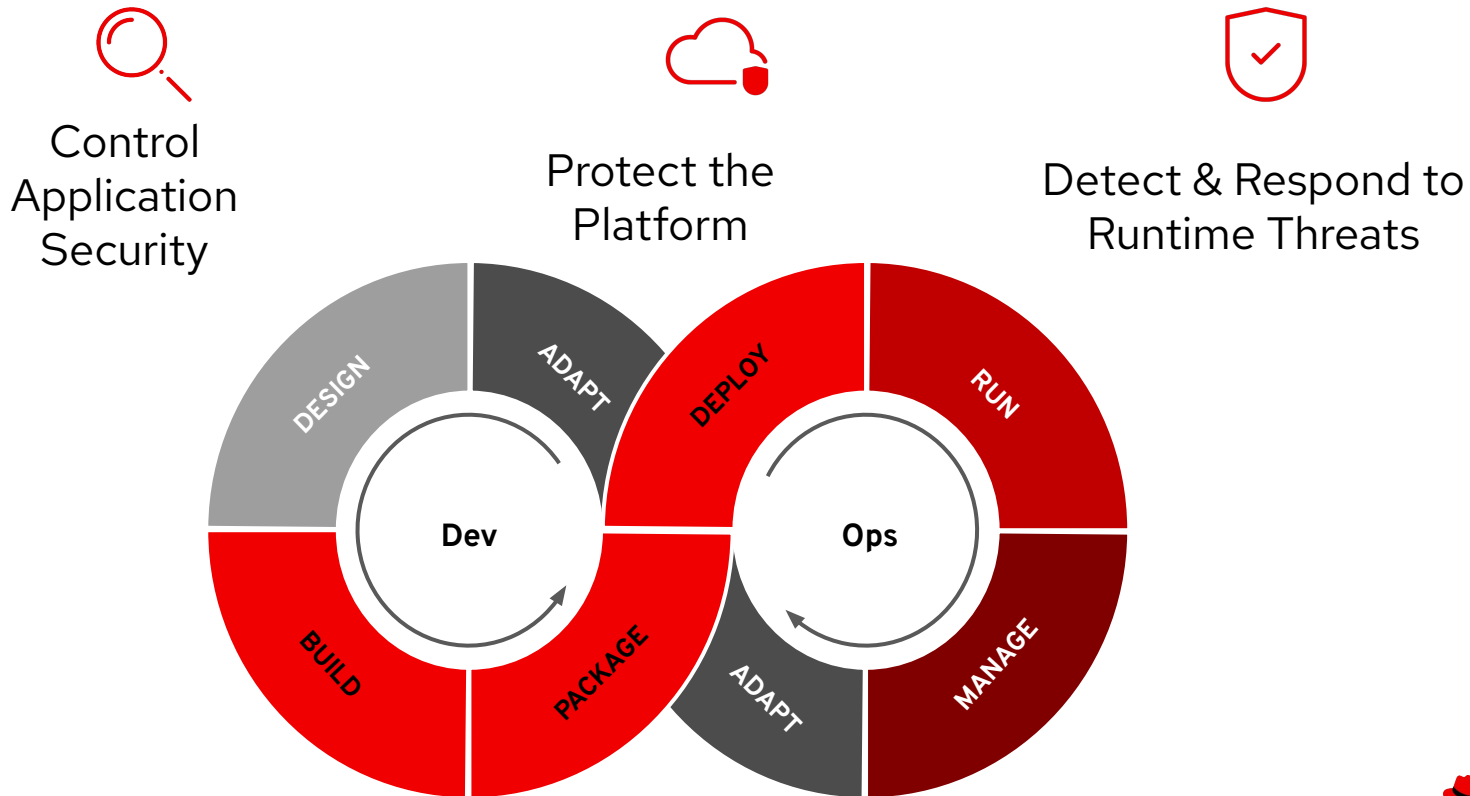
Continuous security for cloud-native applications

Red Hat® Advanced Cluster Security
for Kubernetes, powered by StackRox

OpenShift Platform Plus



Security must be continuous and holistic



OpenShift delivers continuous security



Control



Protect



Detect & Respond

ACM

Application Lifecycle and Locality

Fleet Management

Fleet Observability & Alerts

Vulnerability analysis

Policy admission controller

Runtime behavioral analysis

App config analysis

Compliance assessments

Auto-suggest network policies

APIs for CI/CD integrations

Risk profiling

Threat detection / incident response

Trusted content

Kubernetes platform lifecycle

Container isolation

Container registry

Identity and access management

Network isolation

Build management

Platform data

Application access and data

CI/CD pipeline

Deployment policies

Observability

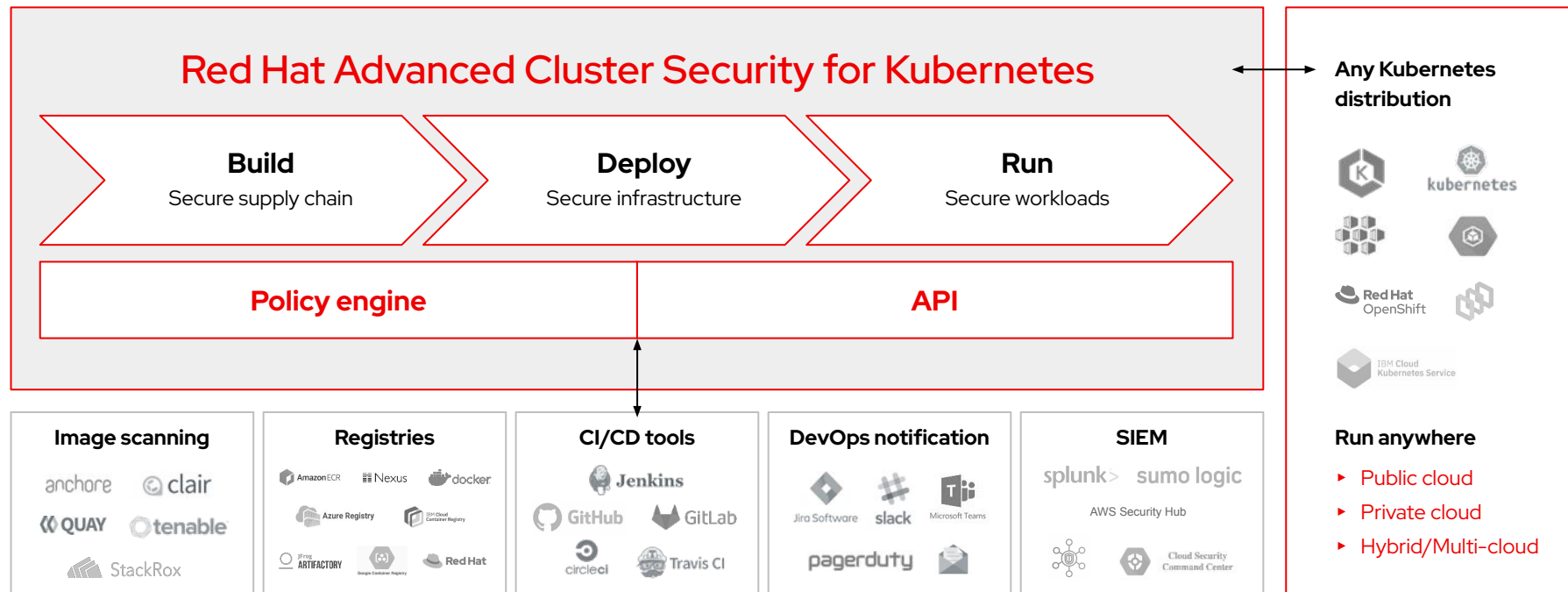
BUILD

DEPLOY

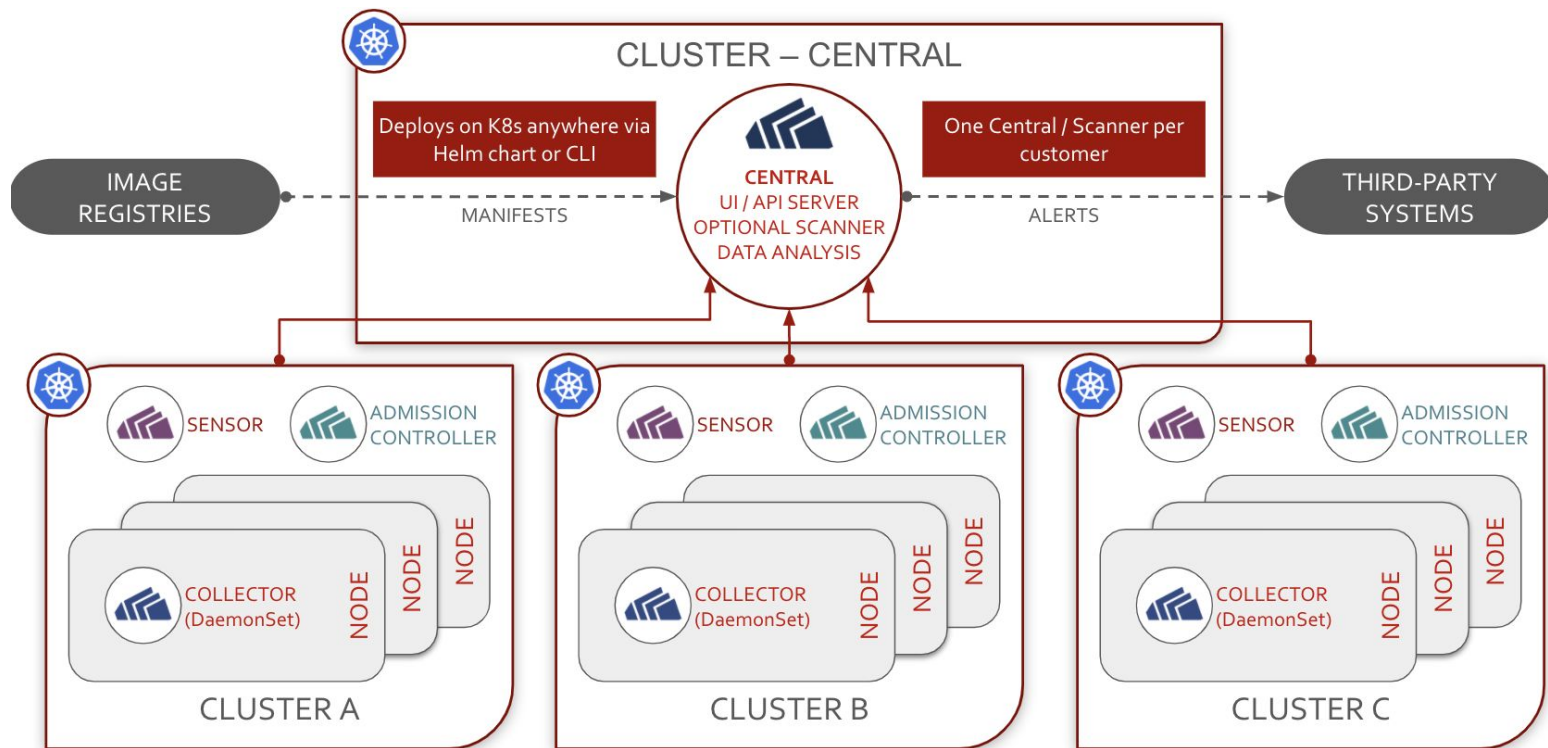
RUN

DevSecOps

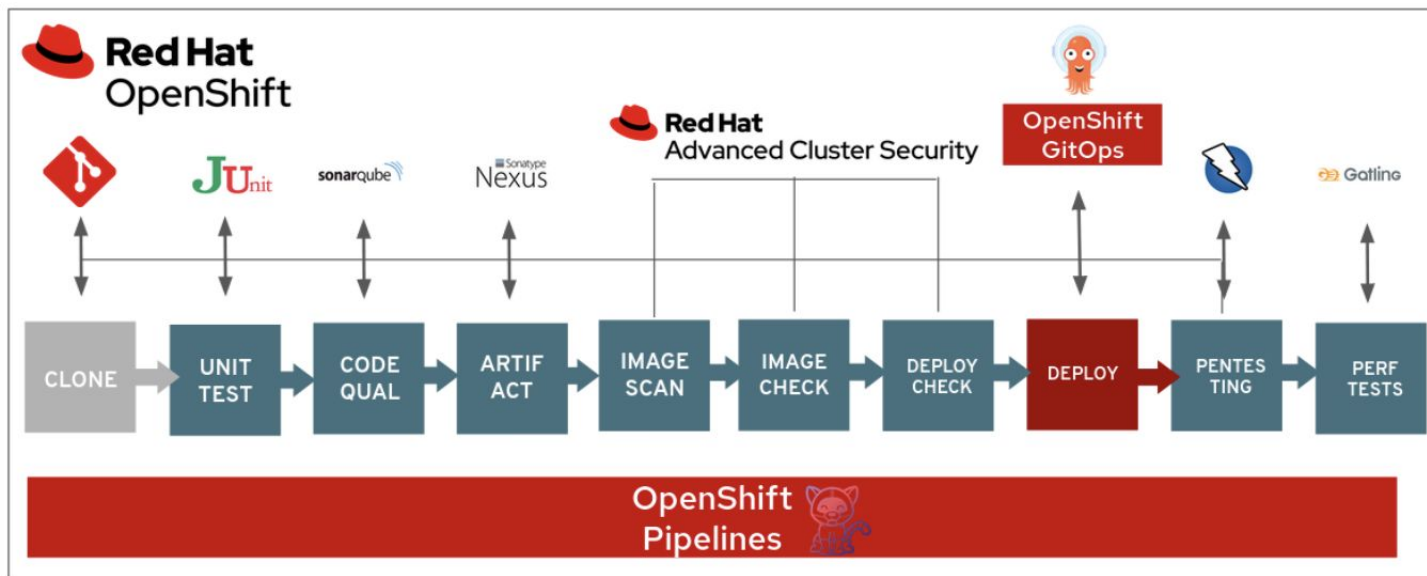
The first Kubernetes-native security platform



Architecture



DevSecOps Demo

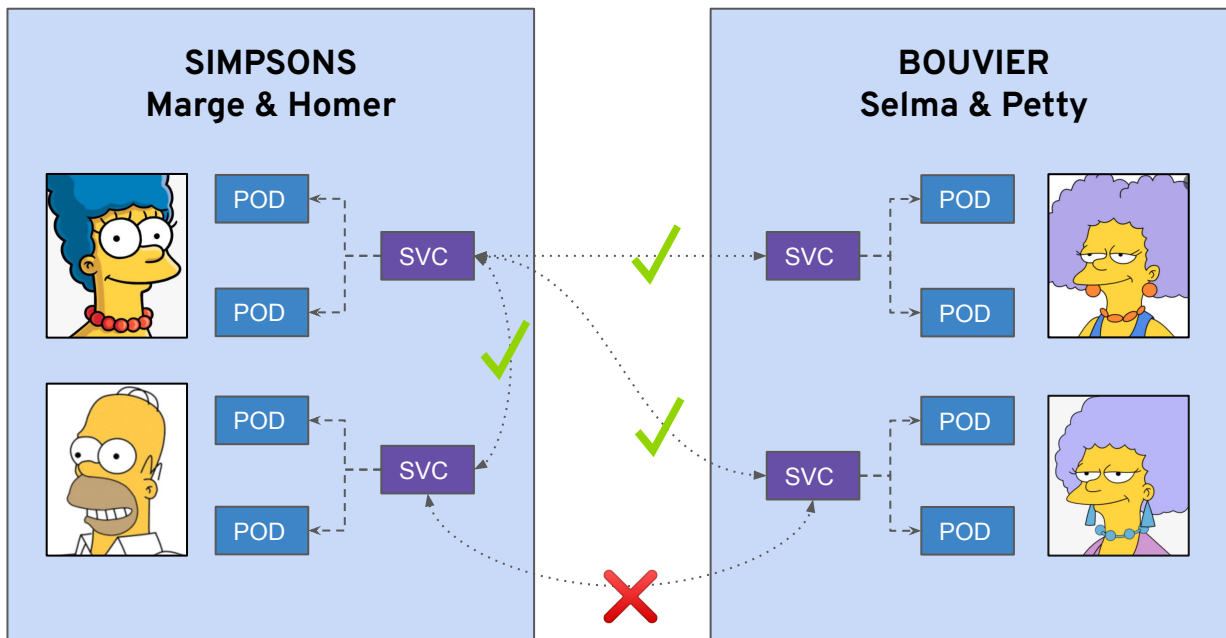


Vulnerability and configuration management methods included in this demo are the following:

- **Static application security testing (SAST)**
- **Software composition analysis (SCA)**
- **Interactive application security testing (IAST) and dynamic application security testing (DAST)**
- **Configuration management**
- **Image risk** is any risk associated with a container image. This includes vulnerable dependencies, embedded secrets, bad configurations, malware, or images that are not trusted.

DEMO

NetworkPolicy



Deny ALL!!!