redhat.

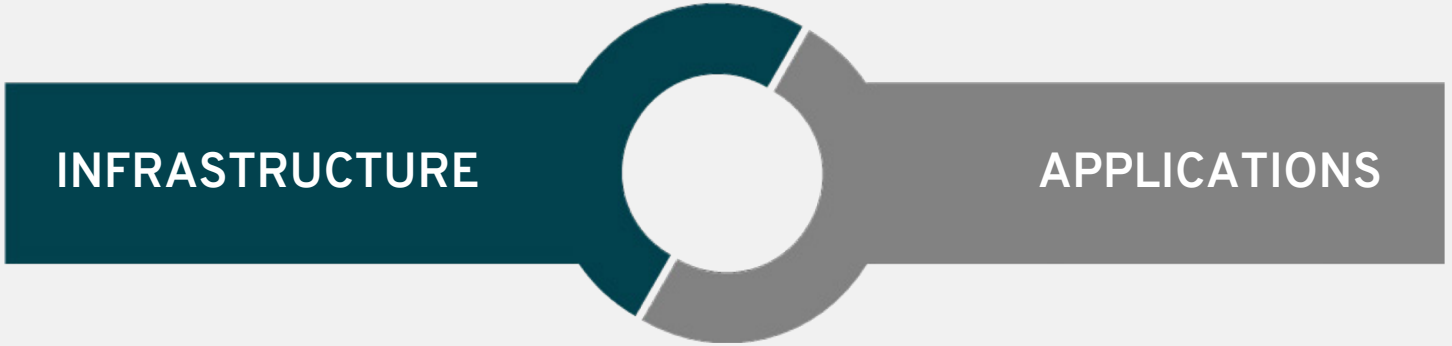
CONTAINERS AND SECURITY: A MATCH MADE IN CYBERSPACE

Ted Brunell
Chief Architect, DoD Programs
Principal Solutions Architect
tbrunell@redhat.com
@DoDCloudGuy

"The views expressed in this presentation are those of the author(s) and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government."

redhat.

CONTAINERS CHANGE HOW WE DEVELOP, DEPLOY AND MANAGE APPLICATIONS



- Application processes on a shared kernel
- Simpler, lighter, and denser than VMs
- Portable across different environments

- Package apps with all dependencies
- Deploy to any environment in seconds
- Easily accessed and shared

redhat.

THEY ALSO CHANGE HOW WE SECURE OUR WORKLOADS

redhat.

AUTOMATED & INTEGRATED SECURITY

CONTROL
Application Security

Container Content | CI/CD Pipeline
Container Registry | Deployment Policies

DEFEND
Infrastructure

Container Platform | Container Host Multi-tenancy
Network Isolation | Storage
Audit & Logging | API Management

EXTEND

Security Ecosystem

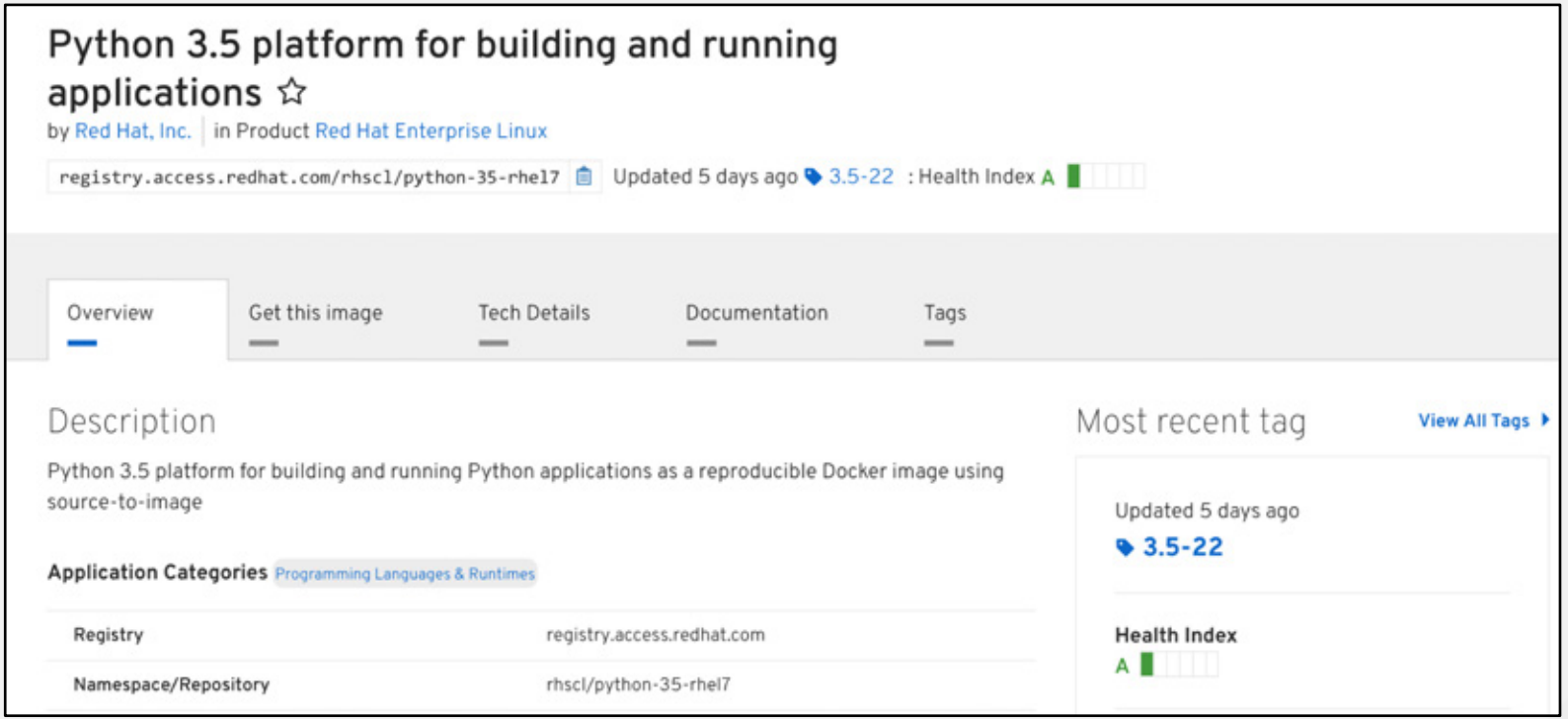
redhat.

CONTROL

Secure the Pipeline & the Applications

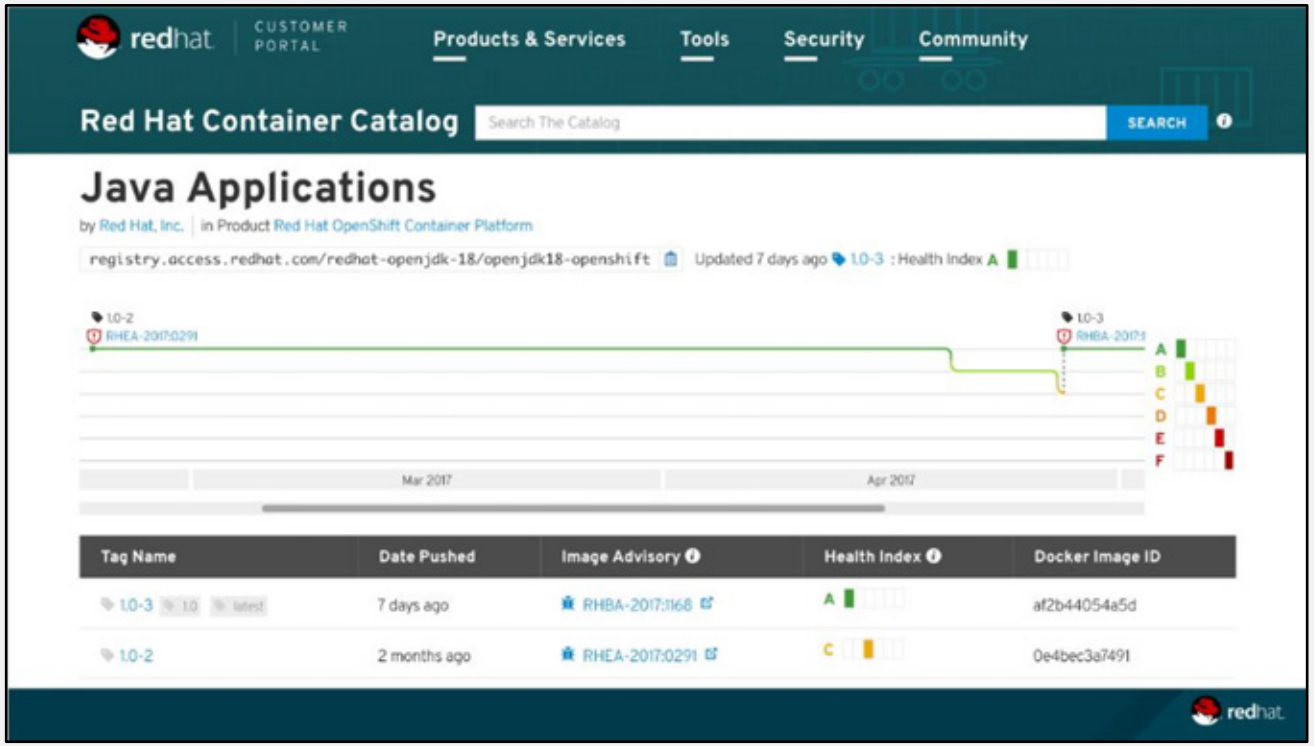
Container Content	CI/CD Pipeline
Container Registry	Deployment Policies

IT STARTS WITH TRUSTED SOURCES



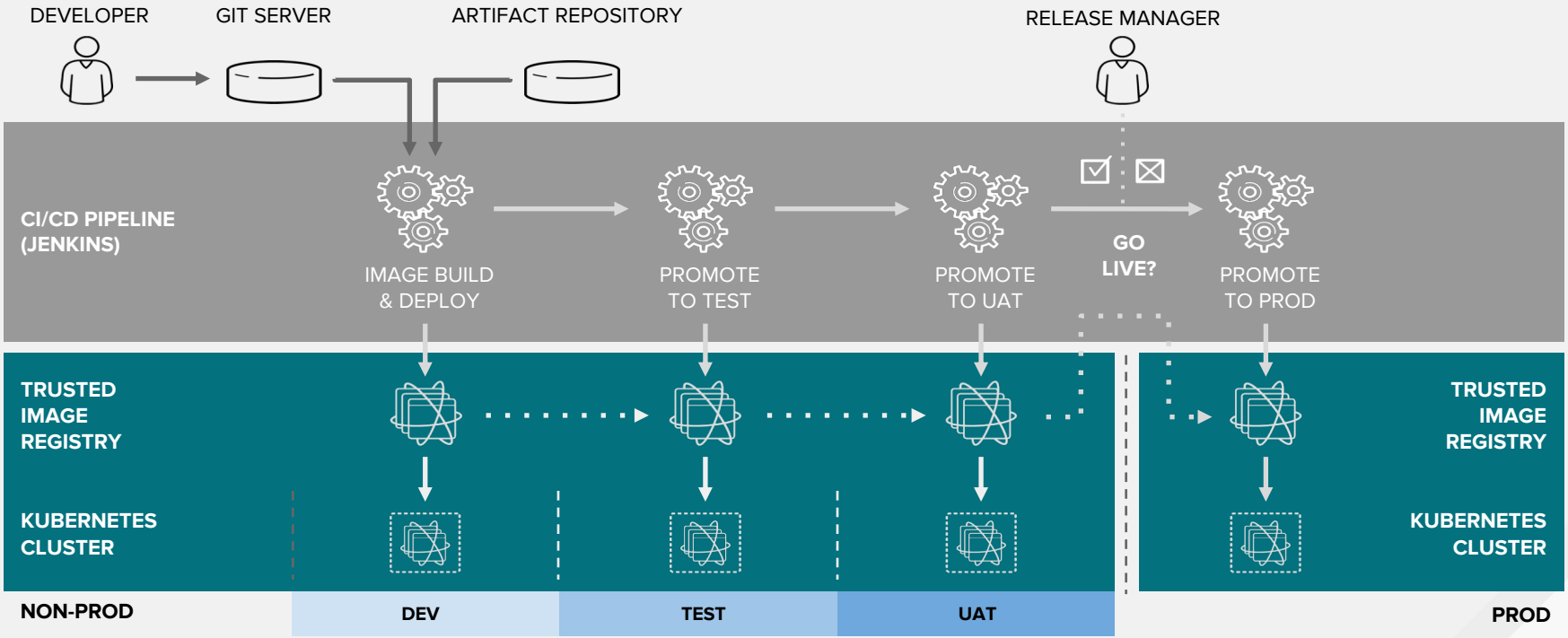
redhat.

CONTAINER HEALTH CHECKS



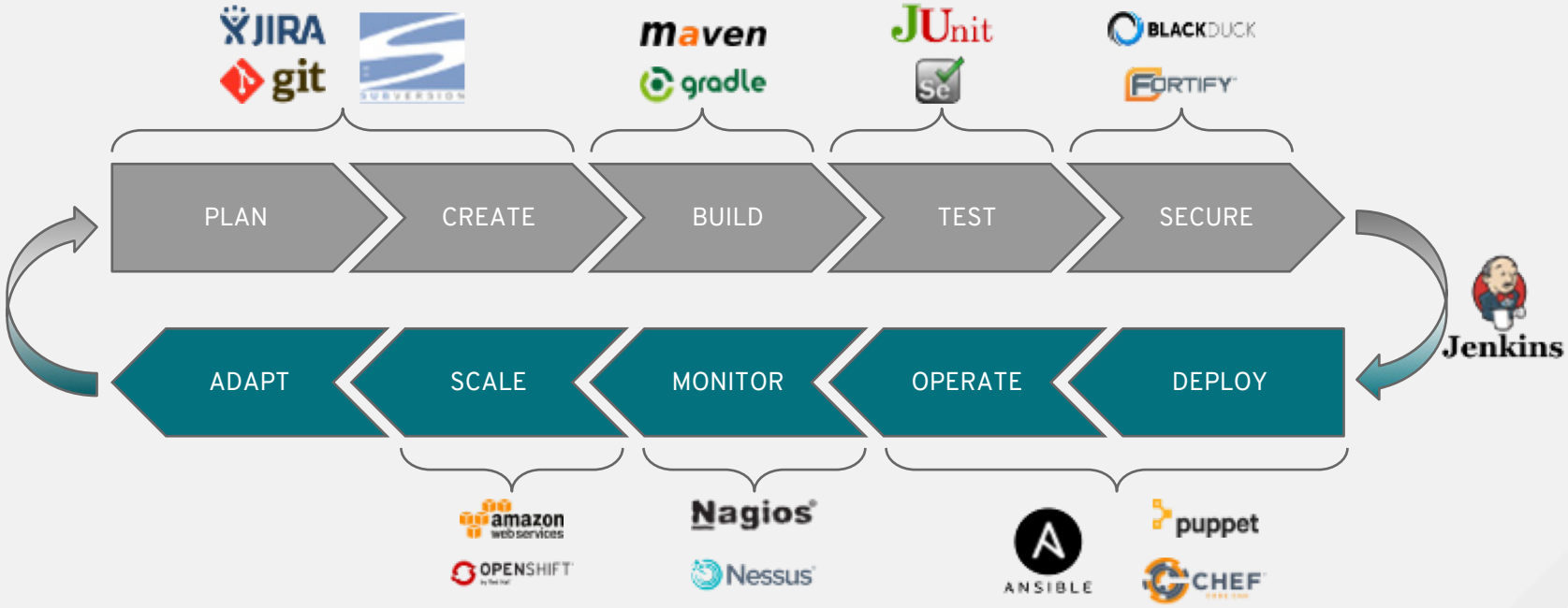
https://access.redhat.com/containers/

SECURE CONTAINER LIFECYCLE



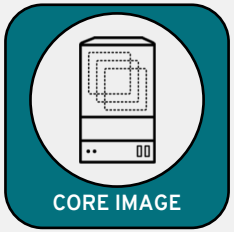
redhat.

AUTOMATING DEVOPS AND DEPLOYMENT POLICIES

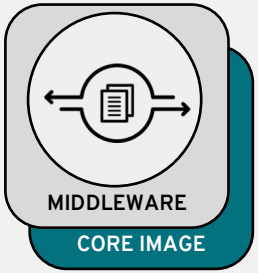


redhat. | intel

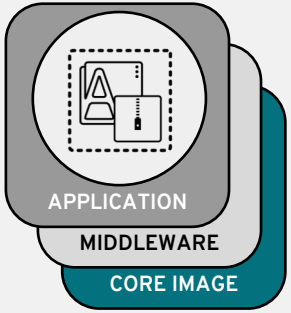
DESIGN FOR SEPARATION OF CONCERNS



IT Operations



Architects



Application Developers

redhat.

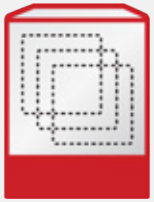
DEFEND

Secure the Infrastructure

Container Platform	Container Host Multi-tenancy
Network Isolation	Storage
Audit & Logging	API Management

THE OS MATTERS: CONTAINER HOST & MULTI-TENANCY

RED HAT ENTERPRISE LINUX



RED HAT ENTERPRISE LINUX ATOMIC HOST

THE FOUNDATION FOR SECURE, SCALABLE CONTAINERS

A stable, reliable host environment with built-in security features that allow you to isolate containers from other containers and from the kernel.

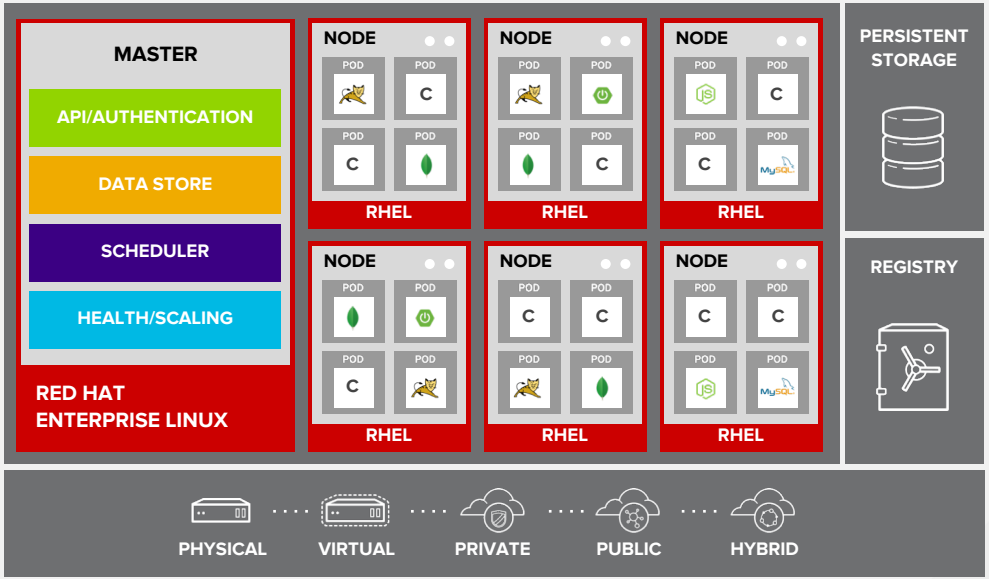
Minimized host environment tuned for running Linux containers while maintaining the built-in security features of Red Hat Enterprise Linux.

SELinux | kernel namespaces | capabilities | cgroups | seccomp

redhat.

SECURING THE CONTAINER PLATFORM

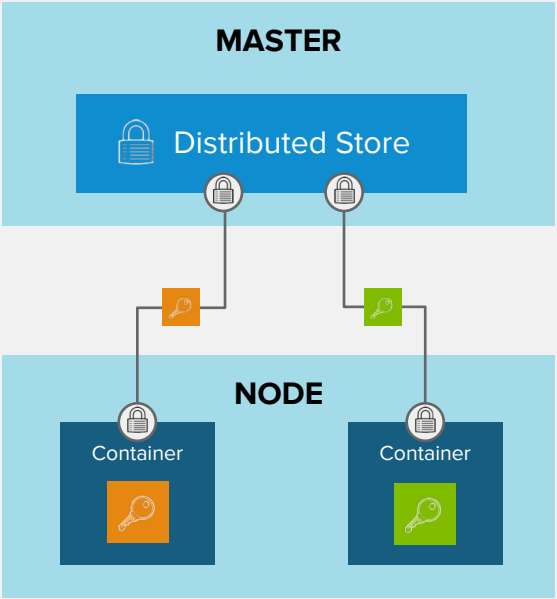
- Role-based Access Controls with LDAP and OAuth integration
- Secure communication
- Platform multi-tenant security
- Integrated & extensible secrets management
- Logging, Monitoring, Metrics
- Consistency across multiple infrastructures



redhat.

SECRETS MANAGEMENT

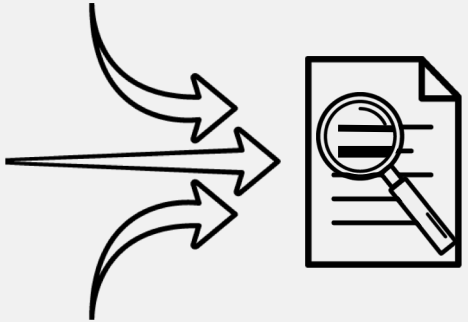
- Secure mechanism for holding sensitive data e.g.
  - Passwords and credentials
  - SSH Keys
  - Certificates
- Secrets are made available as
  - Environment variables
  - Volume mounts
  - Interaction with external systems
- Encrypted in transit and at rest
- Never rest on the nodes



redhat.

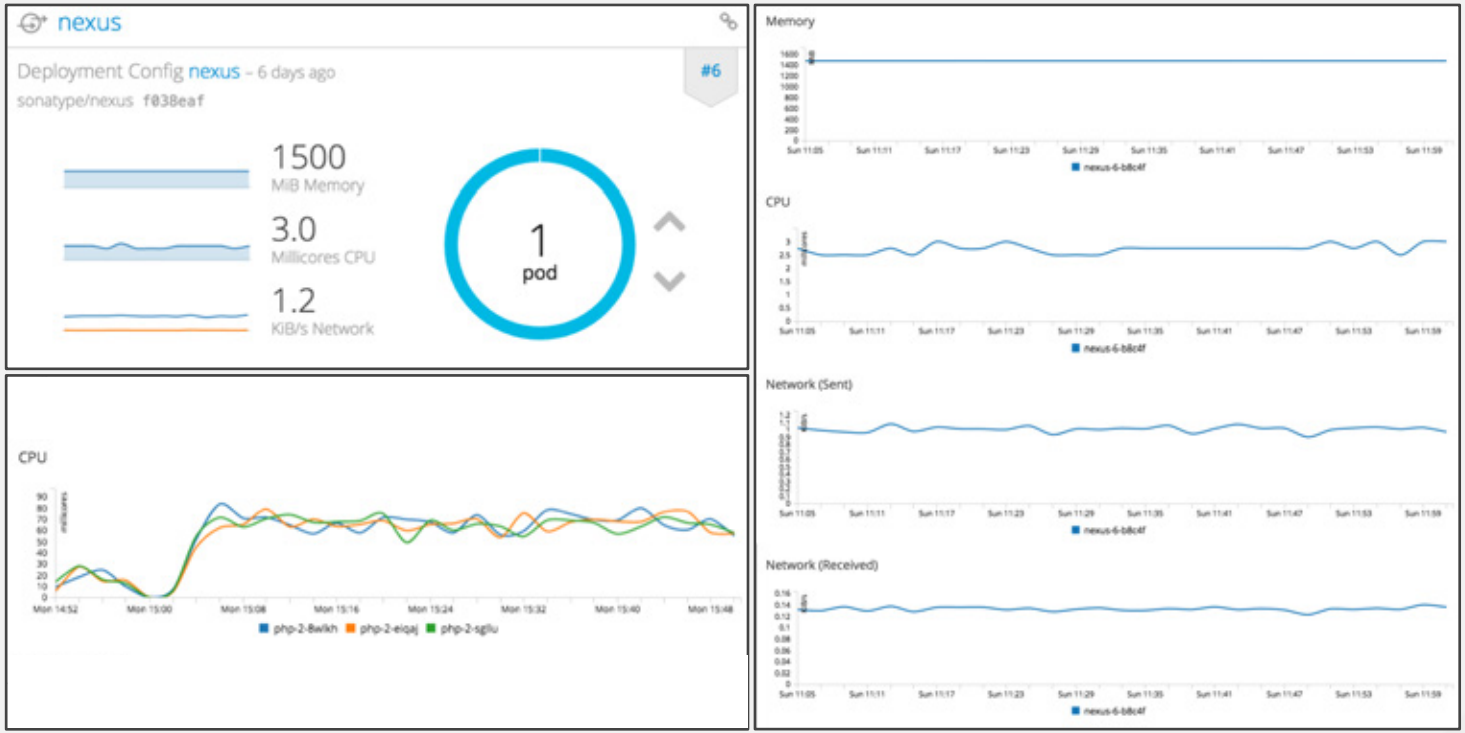
LOGGING and AUDITING

- Aggregate logs for hosts and applications
- Access control
  - Cluster administrators can view all logs
  - Users can view logs for their projects
- Ability to send logs elsewhere
  - External elasticsearch, Splunk, etc



redhat.

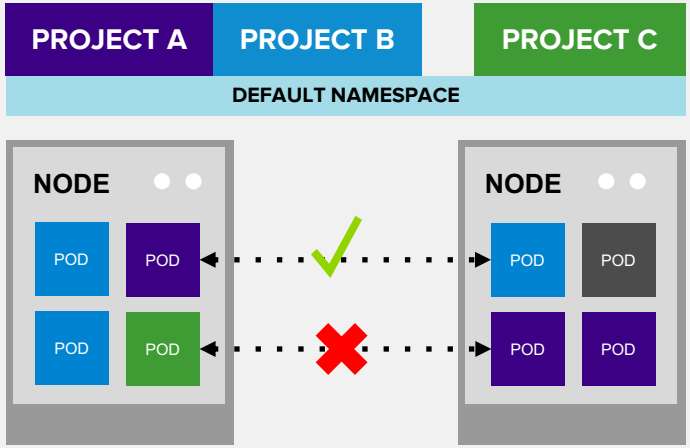
CONTAINER METRICS



redhat.

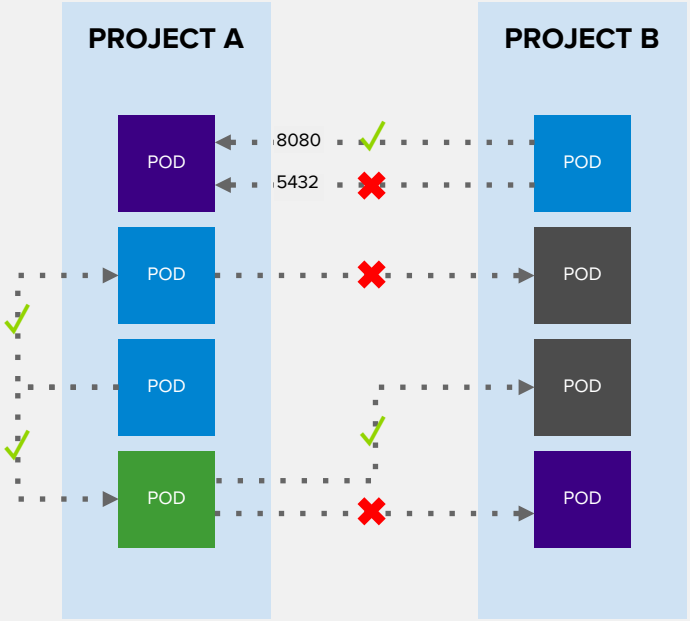
NETWORK DEFENSE

- Multi-tenant Network Support
  - Project-level network isolation
  - Multicast support
  - Egress network policies
- Network Policy
  - Granular policy-based isolation



redhat.

NETWORK POLICY: FINE GRAINED ISOLATION



Example Policies

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

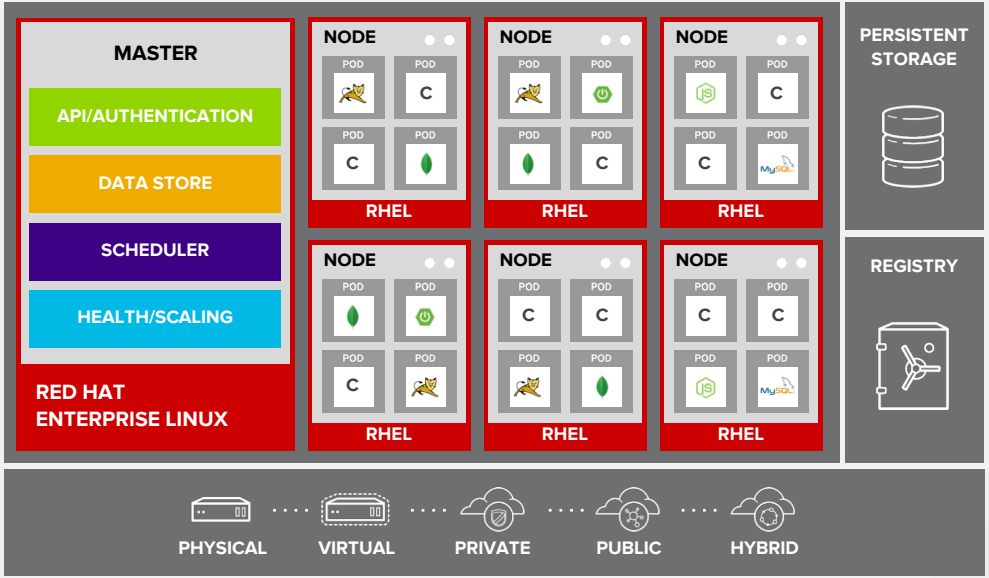
```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
  - ports:
    - protocol: tcp
      port: 8080
```


redhat.

ATTACHED STORAGE

Secure storage by using

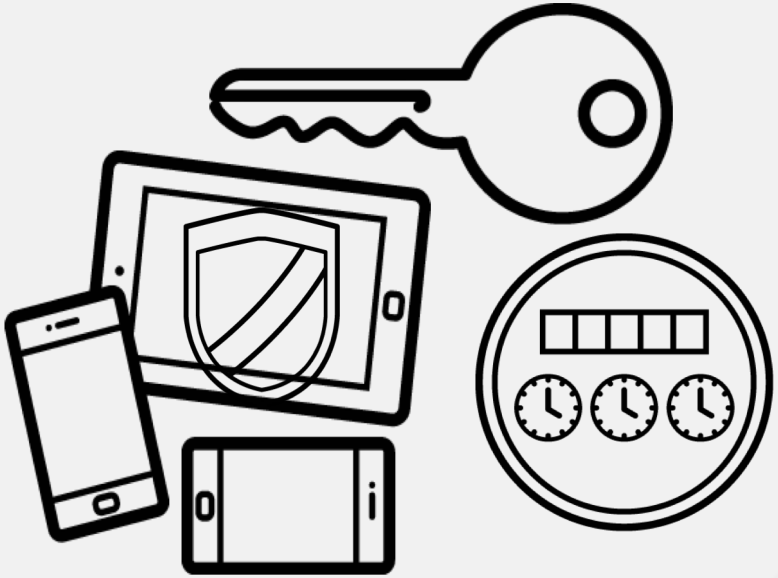
- SELinux Mandatory Access Controls
- Secure mounts
- Supplemental group IDs for shared storage



redhat.

API MANAGEMENT

- Authentication and authorization
- LDAP integration
- End-point access controls
- Rate limiting



redhat.

EXTEND

Leverage the Ecosystem

THE SECURITY ECOSYSTEM

For enhanced security, or to meet existing policies, integrate with enterprise security tools, such as

- Identity and Access Management / Privileged Access Management
- External Certificate Authorities
- External Vaults / Key Management solutions
- External Hardware Security Modules (HSM)
- Filesystem encryption tools
- Container content scanners & vulnerability management tools
- Container runtime analysis tools
- Security Information and Event Monitoring (SIEM)

redhat.

Aporeto

Black Duck

Cisco Contiv

NGINX

Sonatype

Sysdig

Tigera

Tremolo

Twistlock

redhat.

LOOKING INTO THE NOT SO DISTANT FUTURE

CONTAINER CHALLENGES

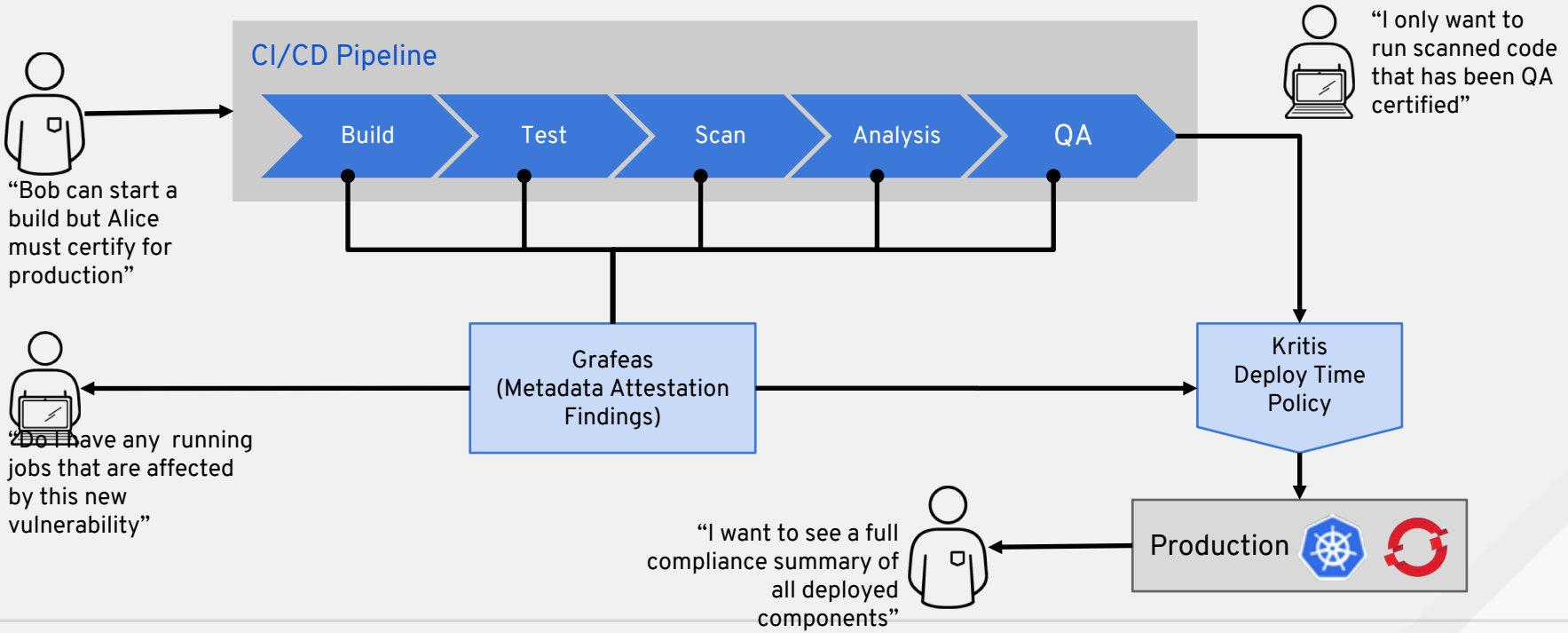
Enterprise Build, Pipeline and Runtime concerns

- Supply chain needs further security policy services
- Microservices have special networking and governance needs
- Build and runtime tools and services need decoupling

redhat.

ATTESTATION OF SECURITY POLICY

Grafeas (Scribe) and Kritis (Judge)



redhat.

ISTIO AND MICROSERVICES

Connect, manage, and secure microservices.

- Collaborative offert between Red Hat, Google Cloud and IBM
  - Sidecar container with the features and functions for creating and managing microservices
    - Monitoring
    - Tracing
    - circuit breakers
    - Routing
    - load balancing
    - fault injection
    - Retries
    - Timeouts
    - Mirroring
    - Access control
    - Rate limiting
    - ...And more

v1.0 ANNOUNCED 07/31/2018!

redhat.

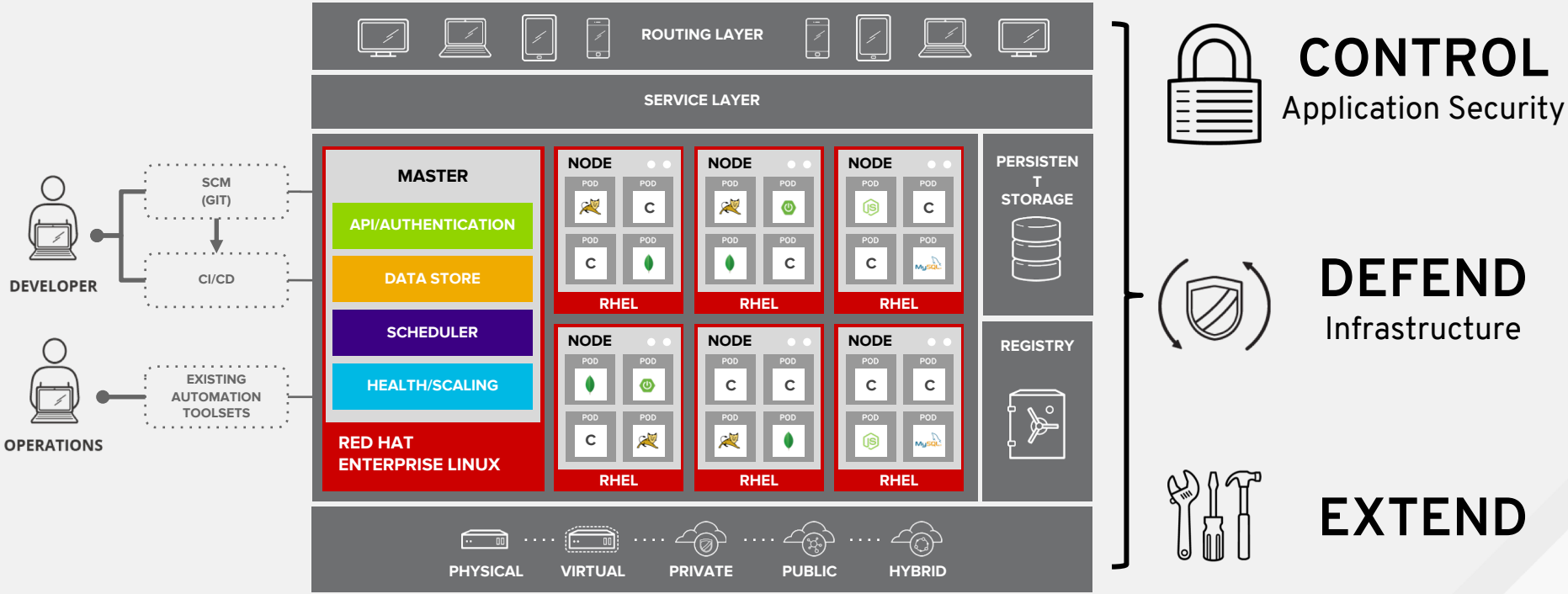
OCI BASED INNOVATION

- A lightweight, OCI-compliant container runtime designed for Kubernetes
- Runs any OCI / Docker container from any OCI / Docker registry
- Focus on stability and life cycle *with* the platform
- Improve container security & performance at scale

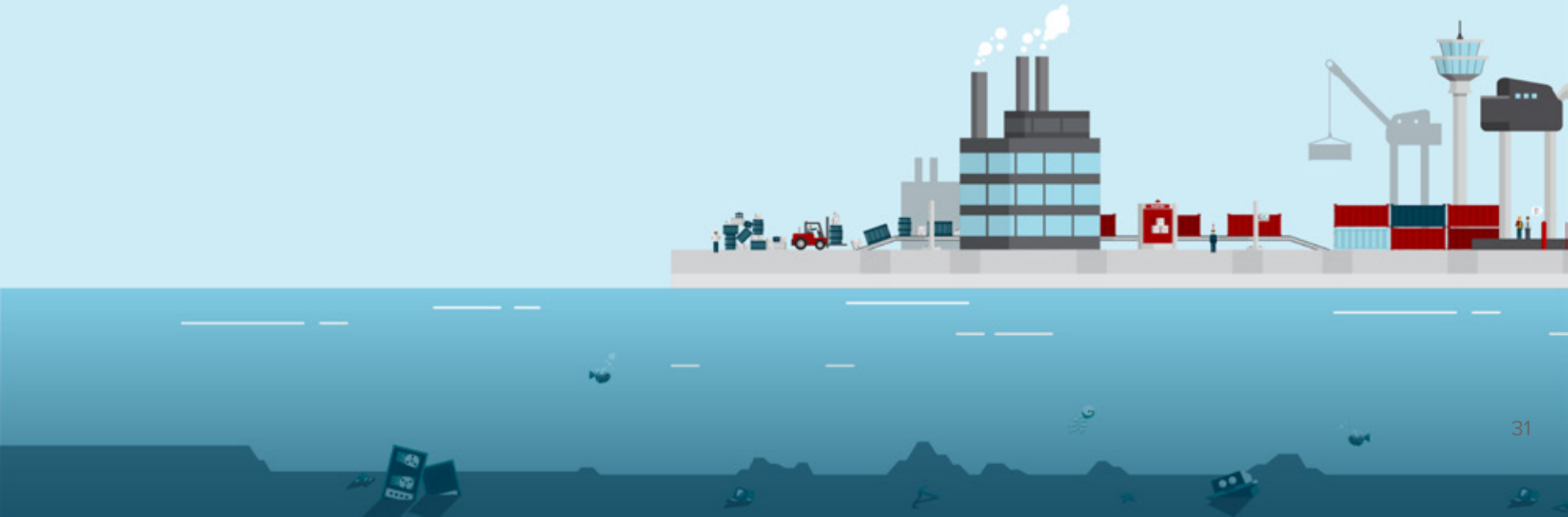
- OCI-compliant, daemon-less tool for building/modifying OCI/Docker images.
- Enables fine-grain control over the commands and content of each image layer
- Container host utils. can optionally be leveraged as part of the build
- Can use a Dockerfile
- Shares the underlying image and storage components with CRI-O

redhat.

BRINGING IT ALL TOGETHER



redhat.

redhat.

THANK YOU