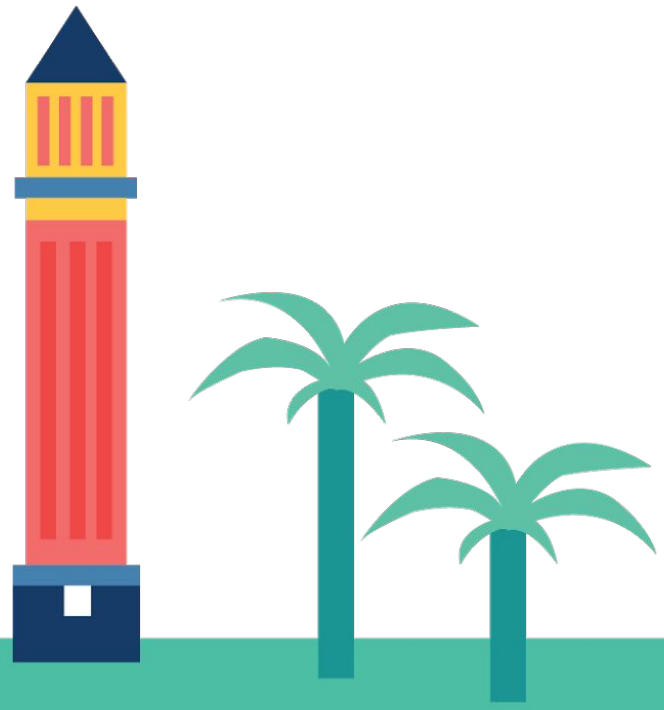
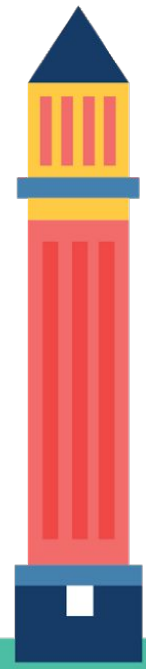
Docker Container Security



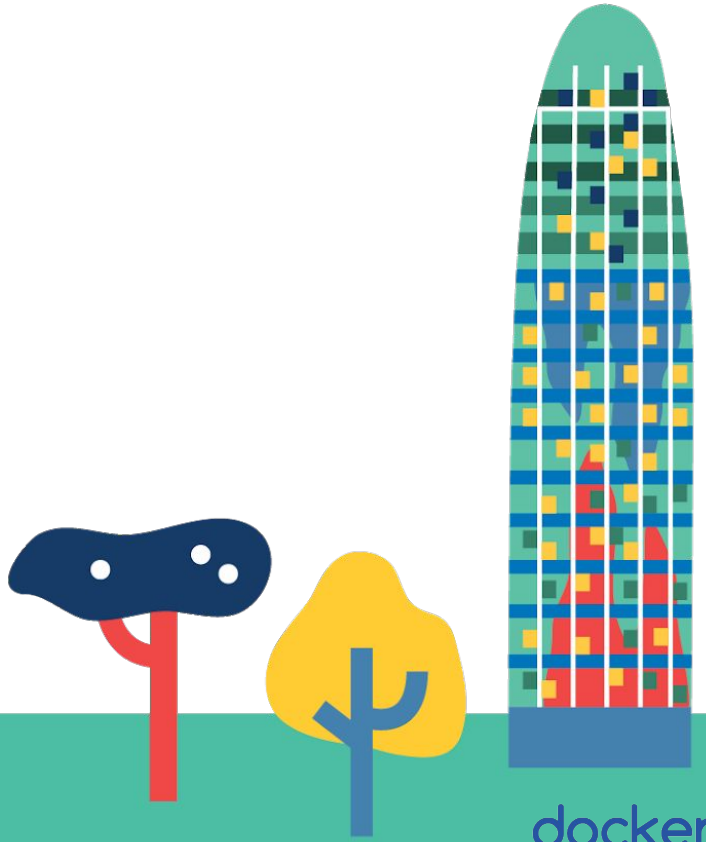


Yuvraj Mehta

Group Product Manager, Docker

Steve Richards

Solutions Architect, Docker



Agenda

- Container Security Verticals
- Secure Software Supply Chain
- Runtime Security
- Infrastructure Security
- Compliance
- DEMO TIME!!

Docker Enterprise Security Verticals

Secure Supply Chain

Securing the Software Pipeline

Runtime Security

Securing the Application in Production

Infrastructure Security

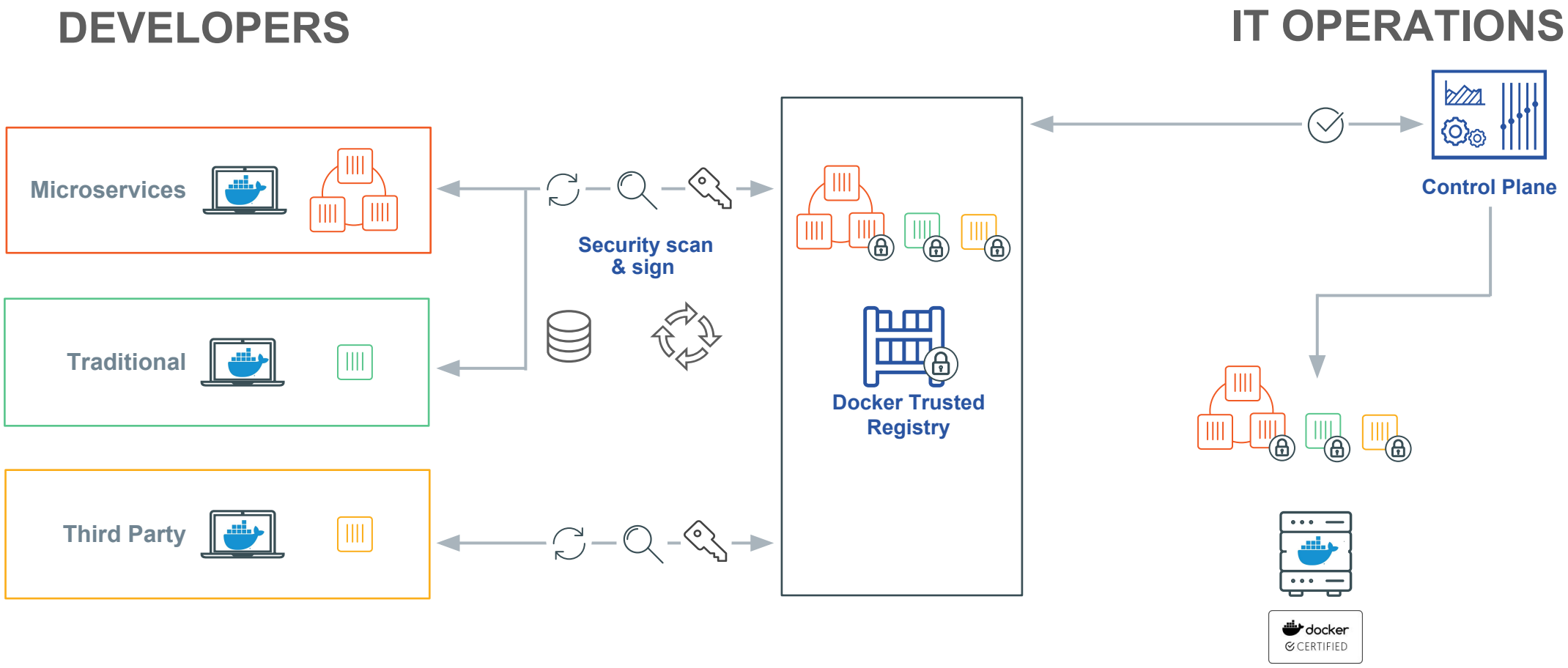
Securing Infrastructure from the Application

Compliance

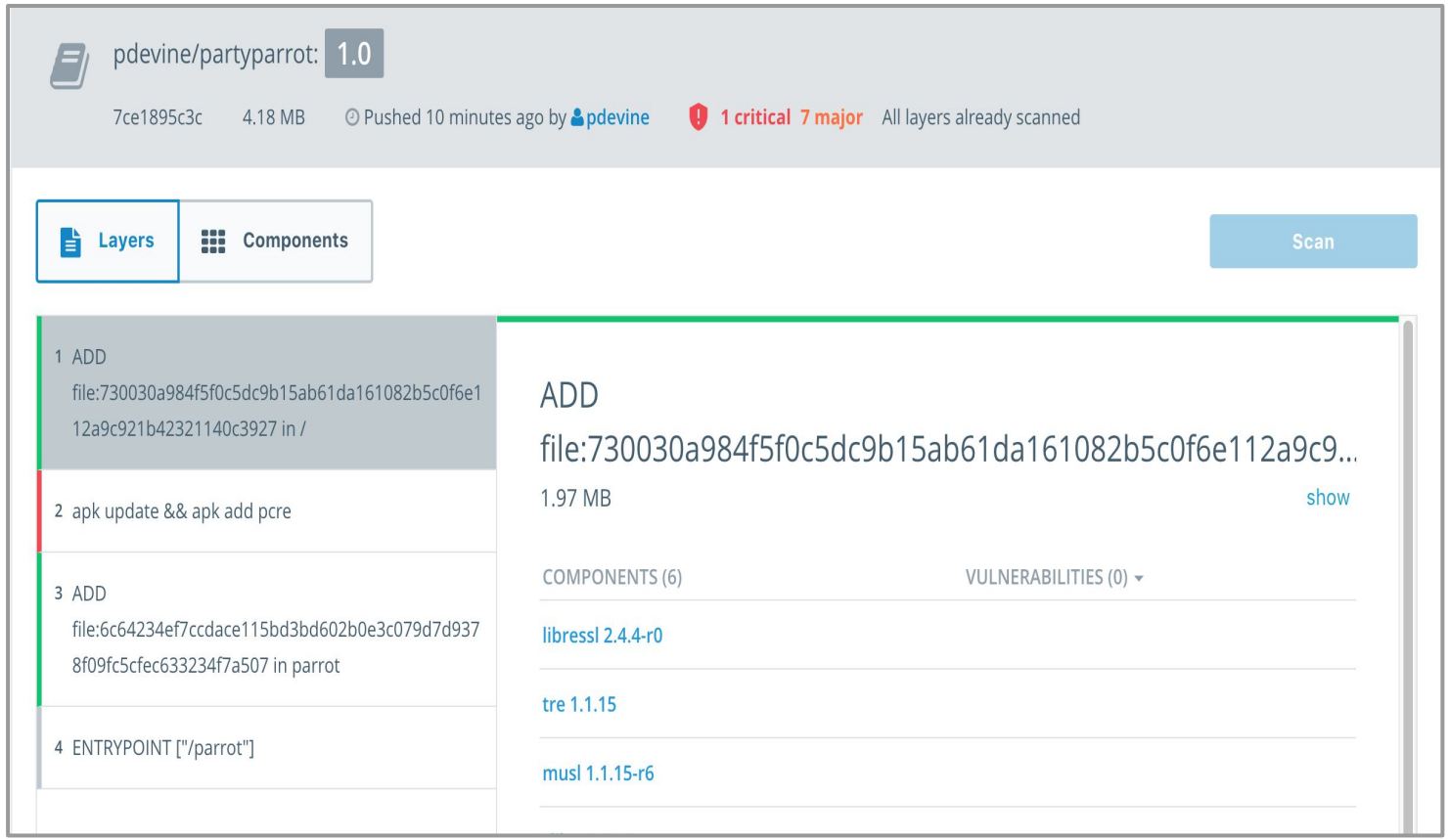
Meet Regulatory Standards

Secure Software Supply Chain

Secure Software Supply Chain



Trusted Images: Scanning



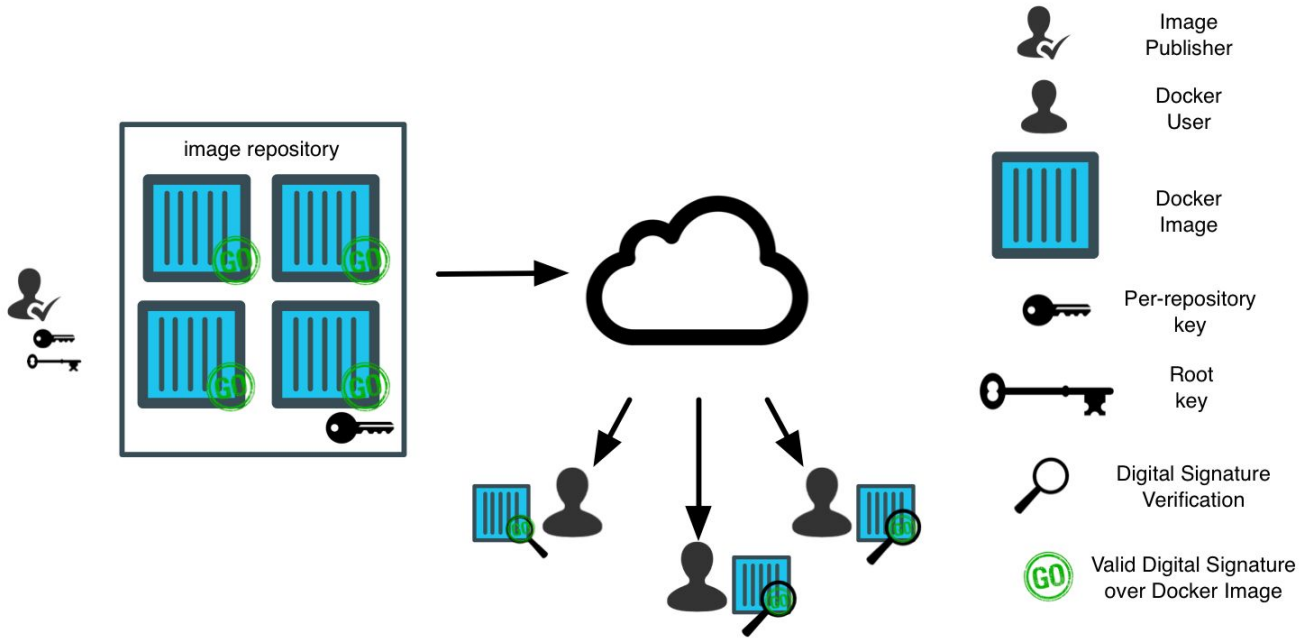
FEATURE

- Detailed BOM of included components and vulnerability profile
- Covers wide array of languages & OS including Windows

BENEFITS

- Deep visibility with binary level scanning
- Integrated workflow for a secure supply chain
- Enable proactive risk management

Trusted Images: Signing



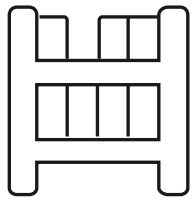
FEATURE

- Sign Docker images from developer to operations
- Verifies the publisher of Docker images
- Integrated with Docker CLI

BENEFITS

- Run only trusted images in production
- Establish a chain of custody for Docker images

WebHooks



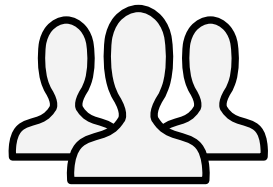
Security scan completed

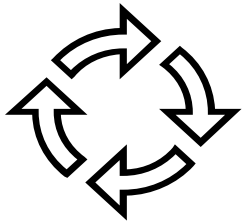
Security scan failed

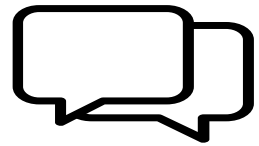
Image promoted from repository

Image mirrored from repository

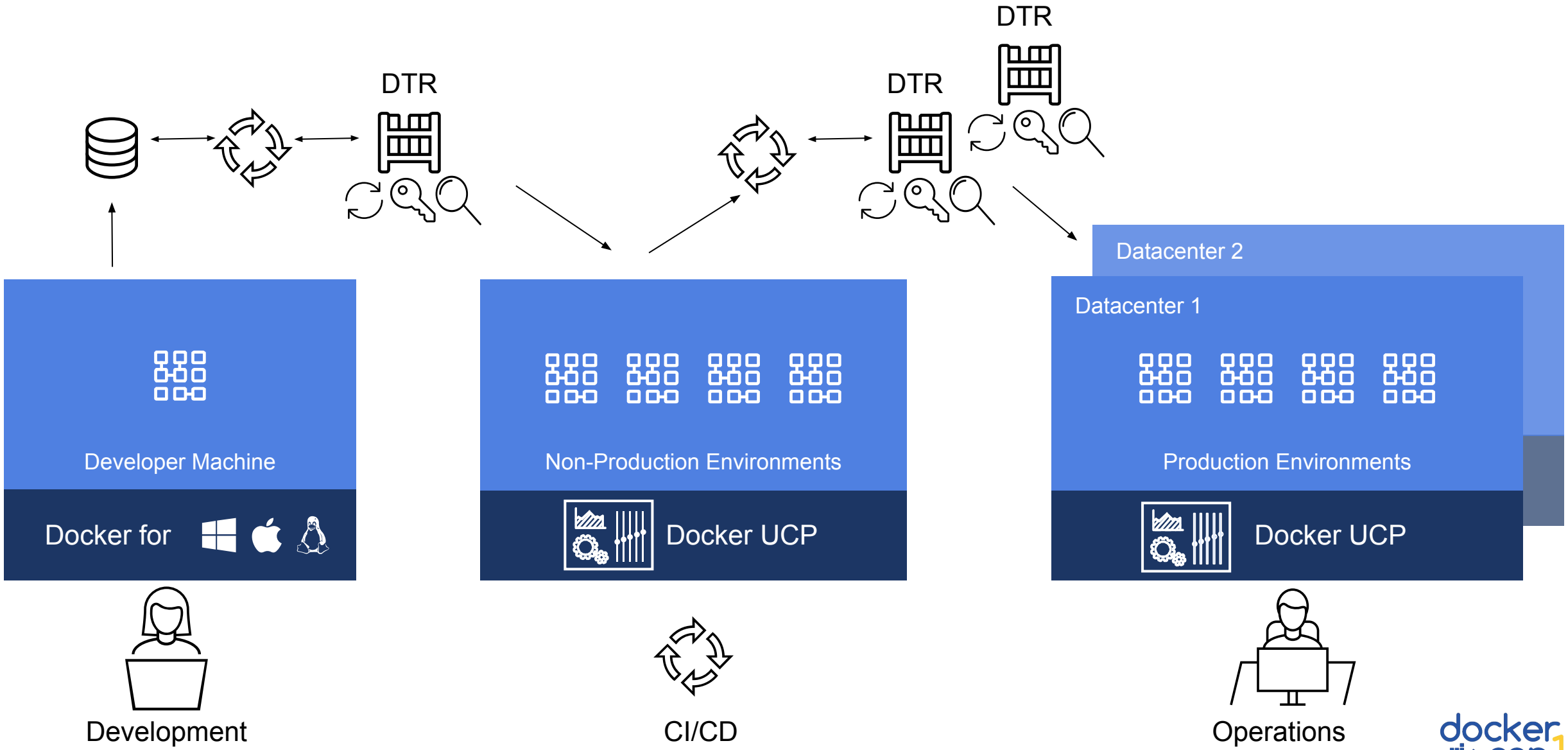
Image mirrored from remote repository





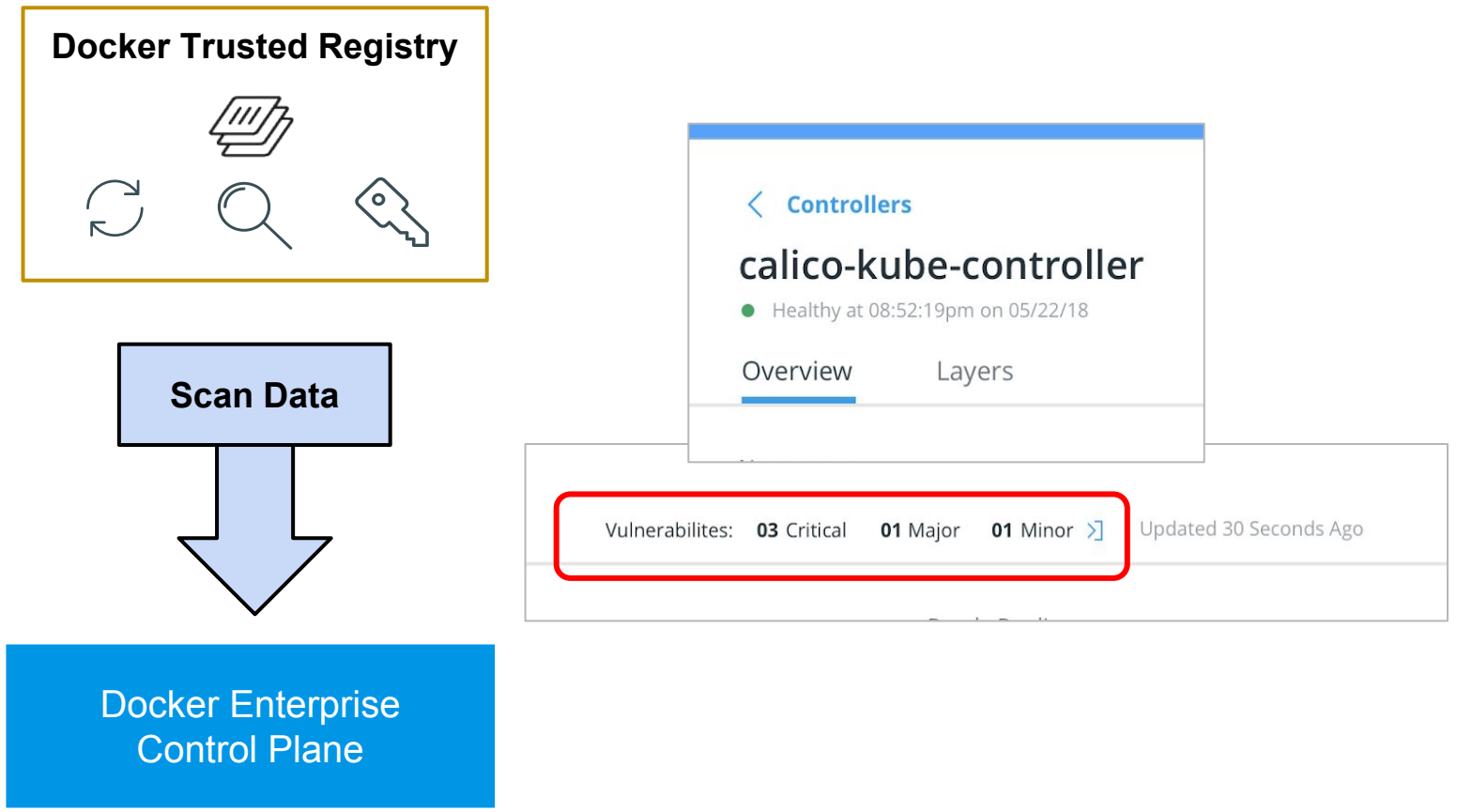


Automated Promotions



Runtime Security

Identify Vulnerabilities in Production



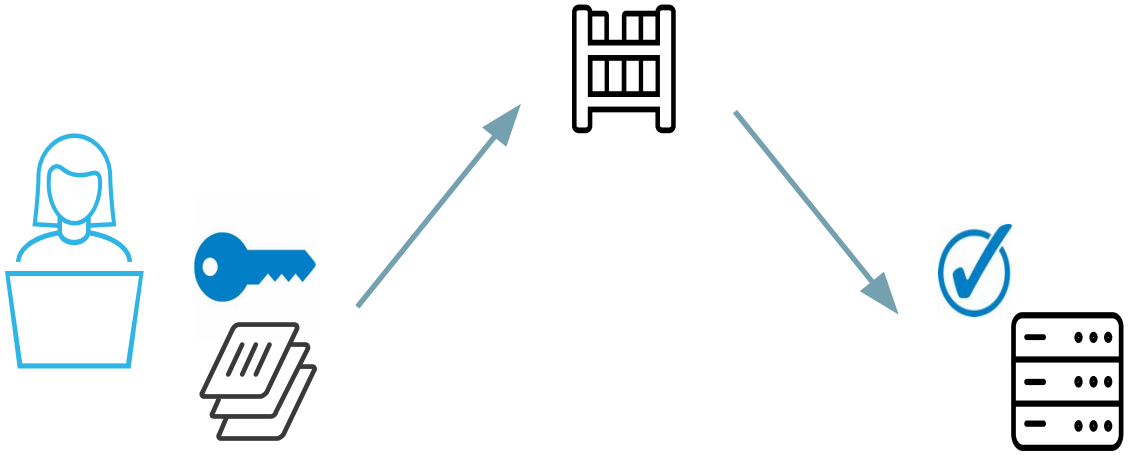
FEATURE

- View vulnerability data of images deployed through the control plane
- Roll up views for services & pods

BENEFITS

- Create policies to manage service deployments using image vulnerability data
- Maintain compliant deployment of production services

Run Trusted Images



Developer signs an image and checks it into a registry

Engine verifies that image is signed before pulling to local environment

FEATURE

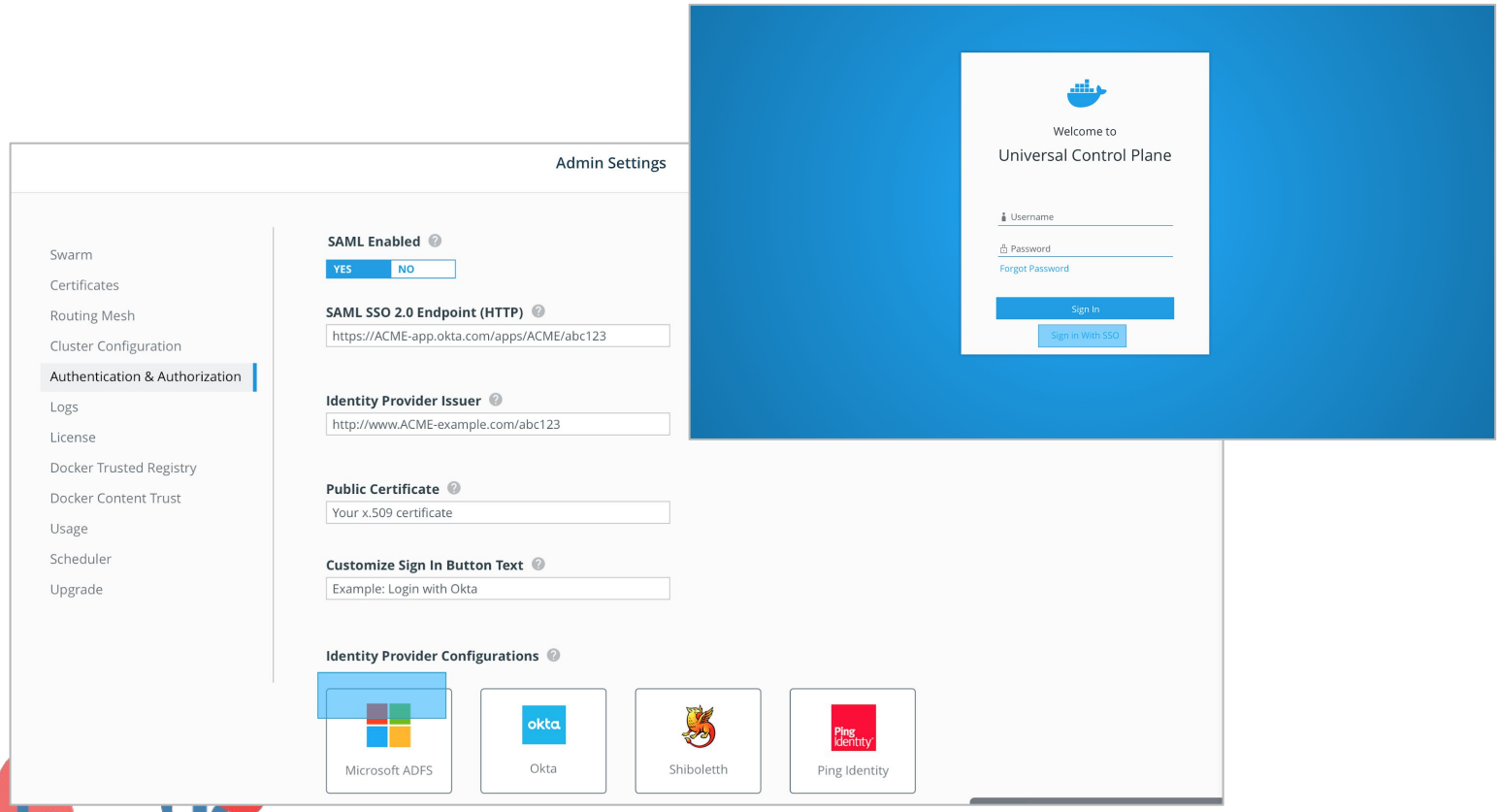
- Verify that images are signed before pulling from registry
- Enable or disable on a per-shell or per-invocation basis

BENEFITS

- Prevent the deployment of containers that use unsigned images
- Enforce policies around image signing

Infrastructure Security

Secure Access: Single Sign-On with SAML v2.0



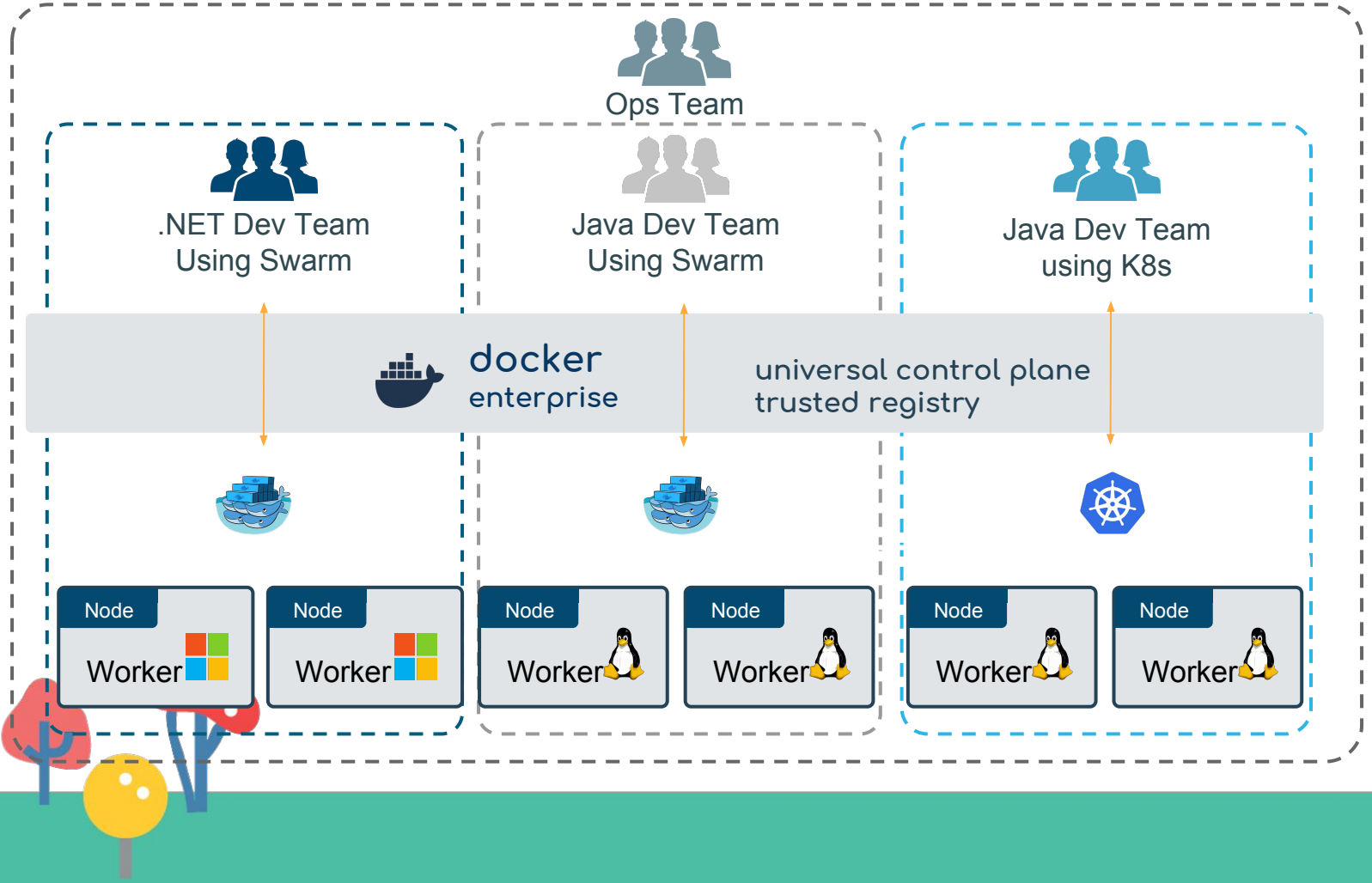
FEATURE

- Allow for SSO to Docker Enterprise through existing identity provider (IdP)
  - Support for Okta and ADFS, with more IdPs added in the future
- Continue to use LDAP synch for client bundle access

BENEFITS

- Achieve 2FA through identity provider
- Credentials stored in IdP only; no local hosting of passwords

Secure Access: Native Kubernetes RBAC



FEATURE

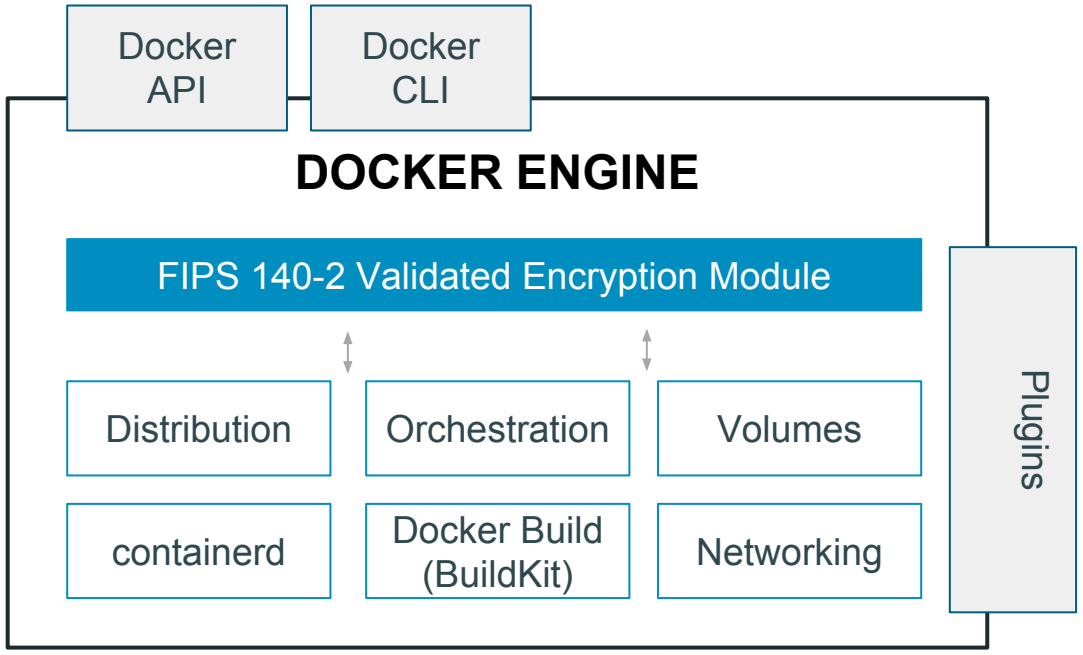
- Add native Kubernetes roles defined in YAML file
- Distinct view of Kubernetes roles from Swarm roles
- Define grants similar to Swarm

BENEFITS

- Deploy Helm charts
- Use native Kubernetes RBAC primitives

Compliance

FIPS 140-2 Validated Docker Enterprise-Engine



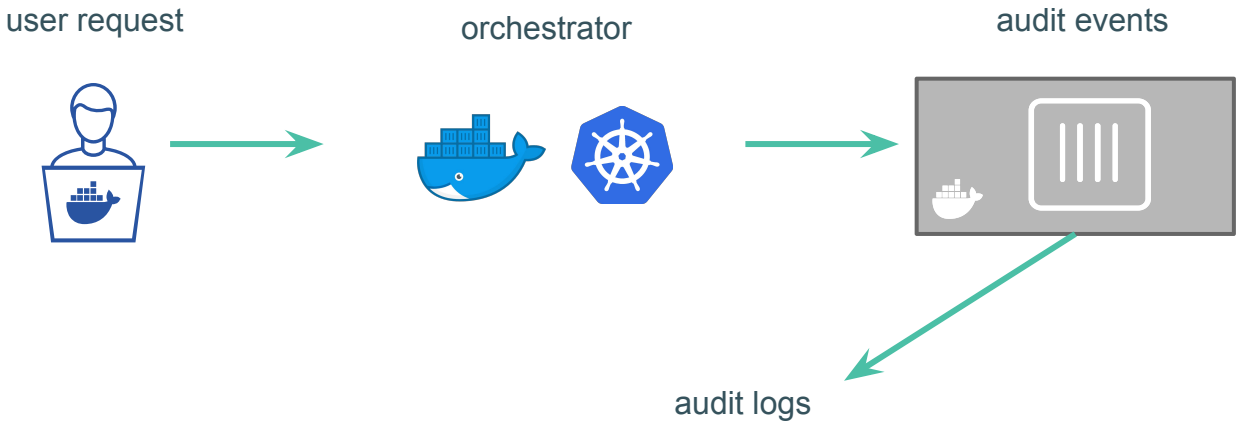
FEATURE

- Linux support included in 18.03 Engine, 18.09 now adds FIPS compliance for Windows
- Automatically enable FIPS mode for Docker engine based upon host OS FIPS status
- Use env variable to override O/S FIPS state

BENEFITS

- Meet regulatory requirements by deploying Docker Engines in a FIPS compliant mode
- Prevent non-FIPS nodes from joining a FIPS compliant cluster

Detailed Audit Logs




```
{"audit": {
      "metadata": {...},
      "level": "Metadata",
      "timestamp": "2018-08-07T22:10:35Z",
      "auditID":
"7559d301-fa6b-4ad6-901c-b587fab75277",
      "stage": "RequestReceived",
      "requestURI":
"/api/v1/namespaces/default/pods",
      "verb": "list",
      "user": {"username": "alice",...},
      "sourceIPs": ["127.0.0.1"],
      ...,
      "requestReceivedTimestamp":
"2018-08-07T22:10:35.428850Z"}}
```

kubernetes pod listing

```
{"audit": {
      "metadata": {...},
      "level": "Metadata",
      "timestamp": "2018-08-07T22:10:35Z",
      "auditID":
"7559d301-94e7-4ad6-901c-b587fab31512",
      "stage": "RequestReceived",
      "requestURI": "/v1.30/configs/create",
      "verb": "post",
      "user": {"username": "alice",...},
      "sourceIPs": ["127.0.0.1"],
      ...,
      "requestReceivedTimestamp":
"2018-08-07T22:10:35.428850Z"}}
```

swarm config create

FEATURE

- Configurable audit logs for both Swarm and Kubernetes
- Logs API calls tracking request, time, user, and response
- Persistent storage of audit log

BENEFITS

- Track and investigate all security-relevant user activity in the cluster

Demo Time

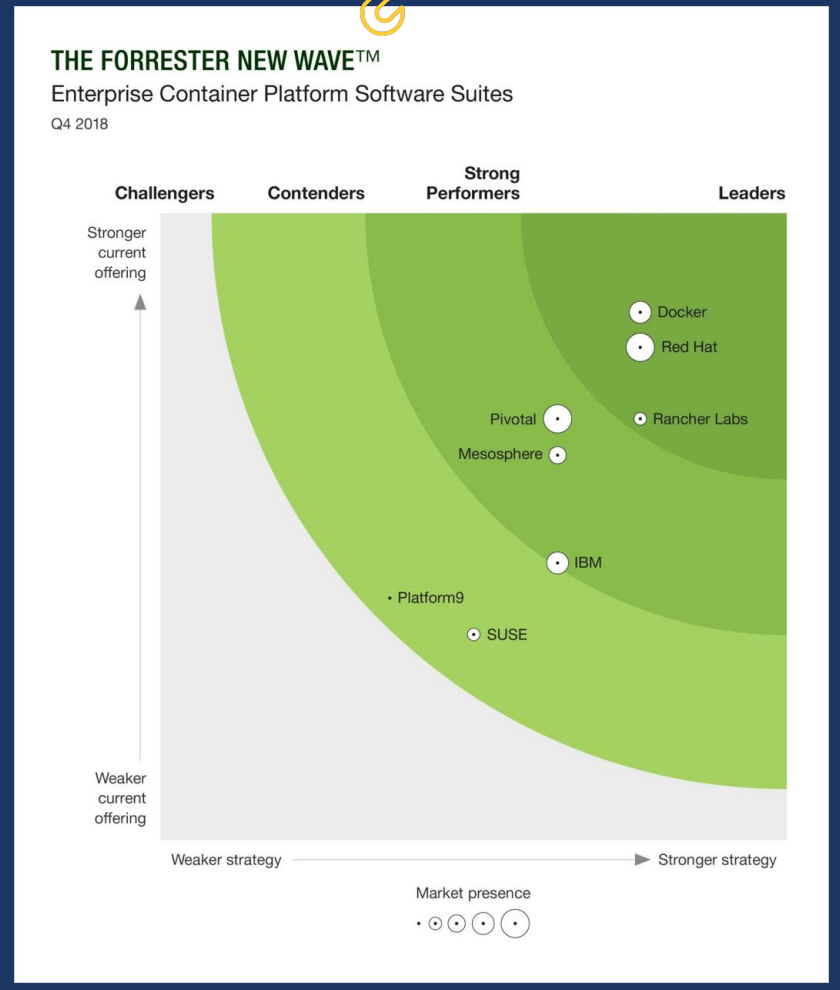
Next Steps

Get the Forrester Report

on Container Platforms

For more information visit:

https://dockr.ly/Forrester



Migrate Legacy Windows Before End of Support

For more information visit:

https://dockr.ly/WindowsServerUpgrade

trial.docker.com

Give Docker Enterprise a spin!

Thank you!