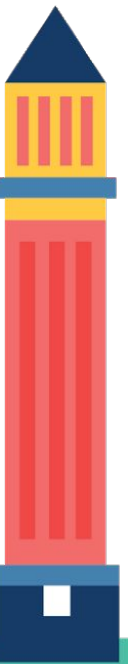
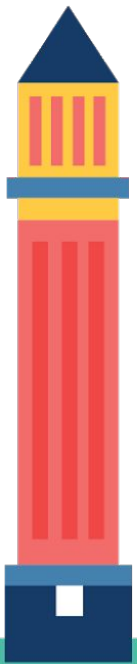


# Docker Container Security





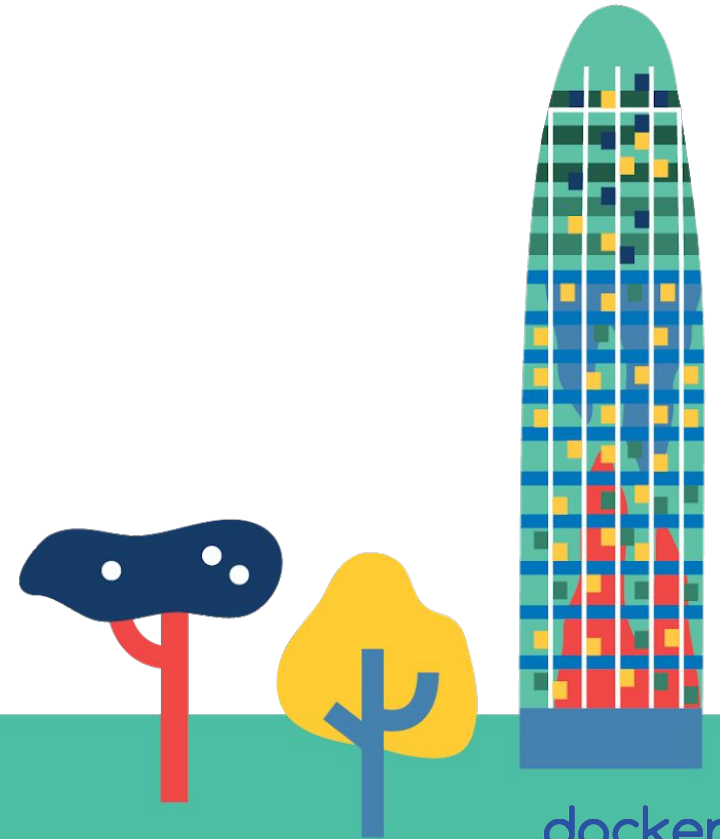
## Yuvraj Mehta

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

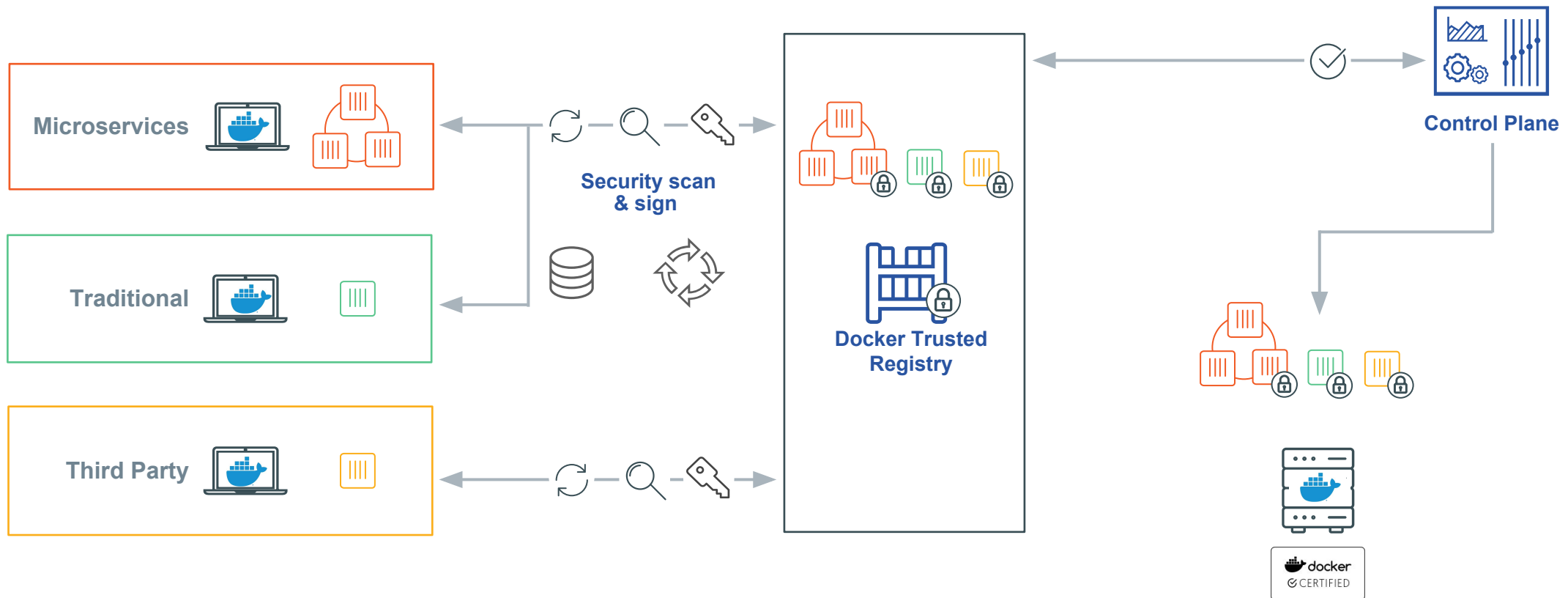
Meet Regulatory Standards



# Secure Software Supply Chain

## DEVELOPERS

## IT OPERATIONS



# Trusted Images: Scanning

The screenshot shows the Docker Trusted Images scanning interface for the image `pdevine/partyparrot: 1.0`. The image ID is `7ce1895c3c`, size is `4.18 MB`, and it was pushed 10 minutes ago by `pdevine`. It shows `1 critical` and `7 major` vulnerabilities. The interface has tabs for `Layers` and `Components`, and a `Scan` button.

**Layers:**

- 1 ADD  
file:730030a984f5f0c5dc9b15ab61da161082b5c0f6e112a9c921b42321140c3927 in /
- 2 apk update && apk add pcre
- 3 ADD  
file:6c64234ef7ccdace115bd3bd602b0e3c079d7d9378f09fc5cfec633234f7a507 in parrot
- 4 ENTRYPOINT ["/parrot"]

**Components (6):**

- libressl 2.4.4-r0
- tre 1.1.15
- musl 1.1.15-r6

**Vulnerabilities (0):**



## FEATURE

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

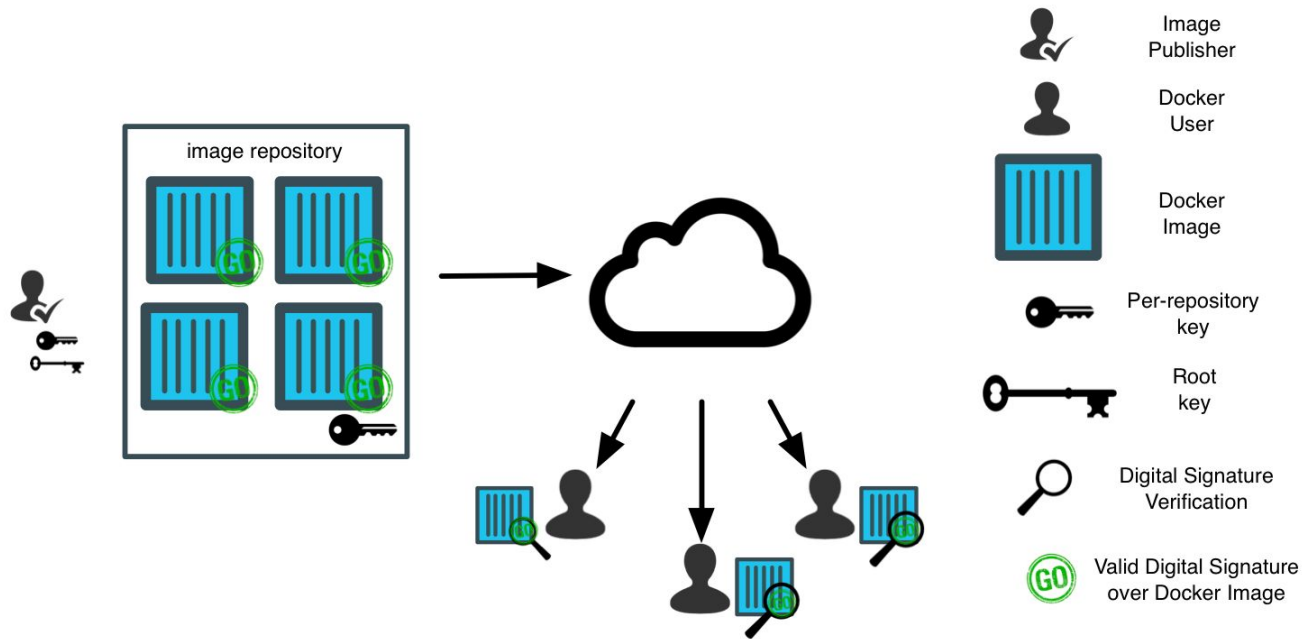


## BENEFITS

- 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



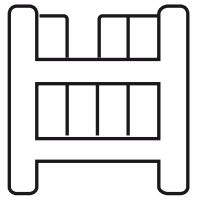
## BENEFITS

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





# WebHooks



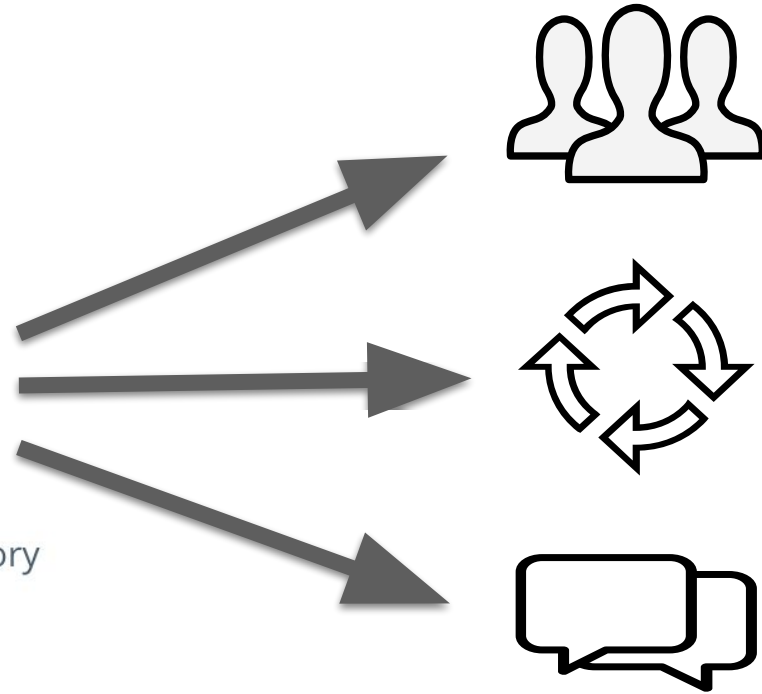
Security scan completed

Security scan failed

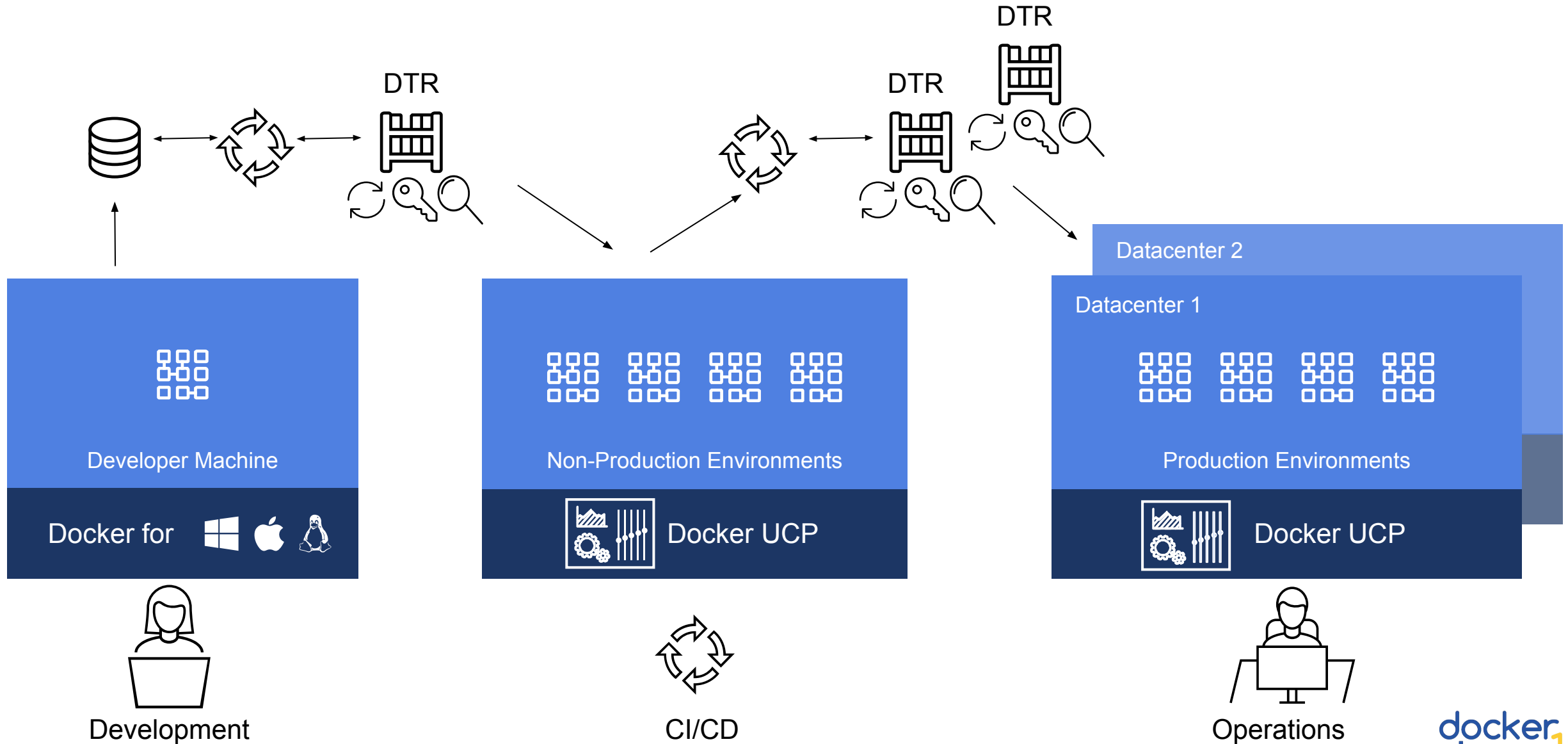
Image promoted from repository

Image mirrored from repository

Image mirrored from remote repository

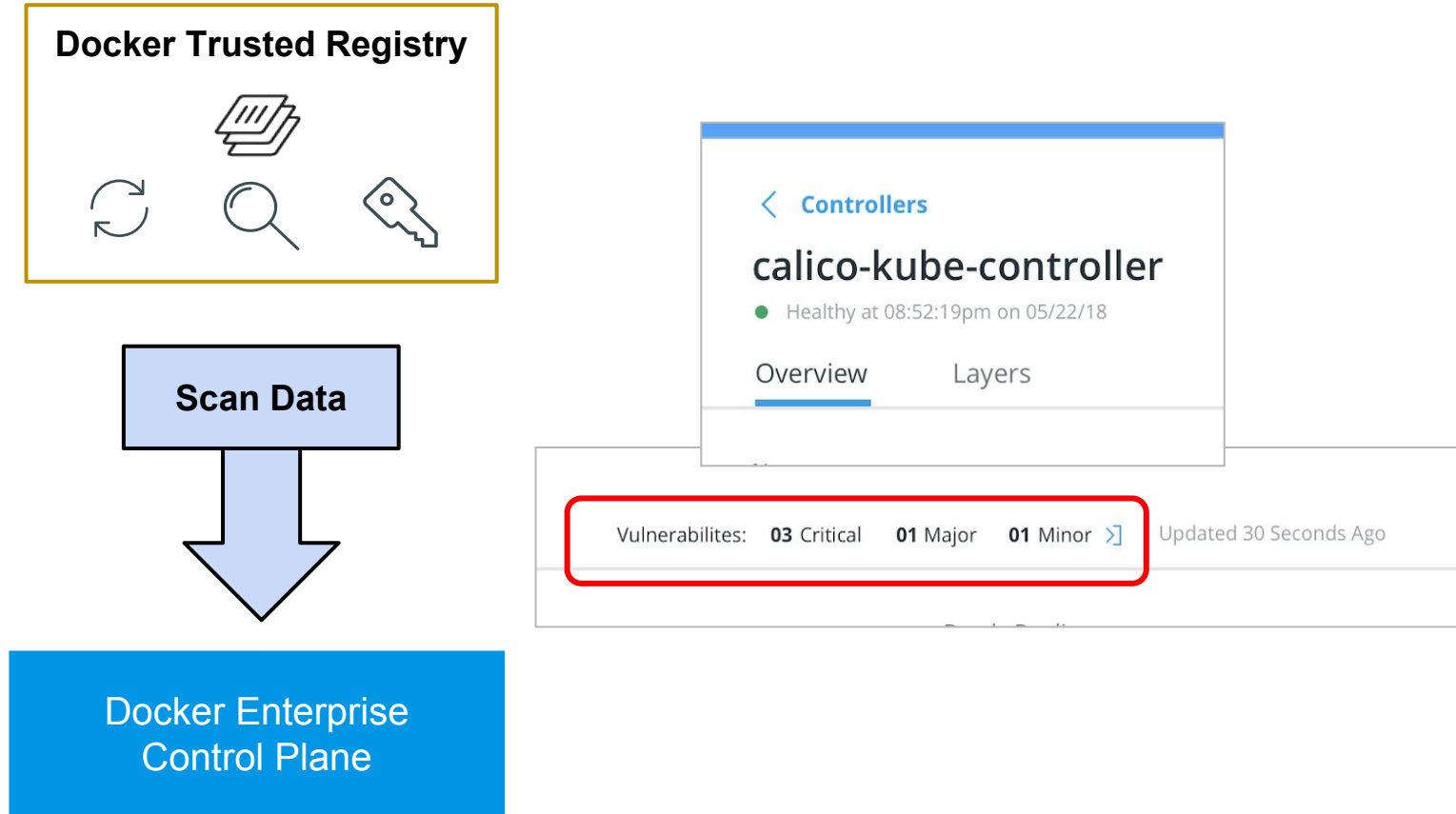


# Automated Promotions



## A vibrant, stylized illustration of a city map. The map is composed of a grid of white lines on a light orange background. Various colorful buildings, trees, and people are scattered across the grid, representing different urban features. In the top left, there's a red church with a white steeple. Next to it is a green tree. In the top center, a person is riding a bicycle. To the right, there's a blue and white building with a ship on top. In the middle left, there's a large red and white building with multiple spires. Below it, a person is walking. In the middle right, there's a tall blue and white building. In the bottom left, there's a red and white building with a tower. In the bottom center, there's a red and white building with a tower. In the bottom right, there's a red and white building with a tower. The overall style is flat and colorful, with a focus on geometric shapes and primary colors.

# Identify Vulnerabilities in Production



## FEATURE

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

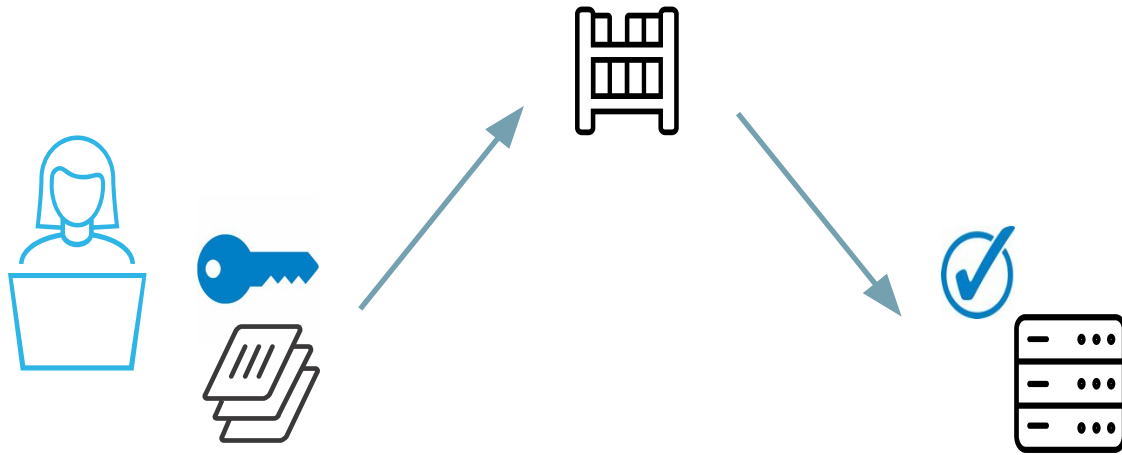


## BENEFITS

- 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



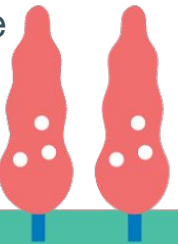
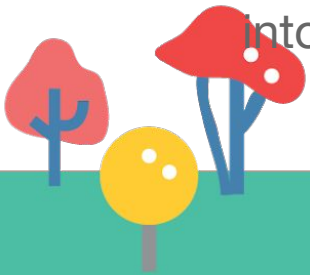
## FEATURE

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



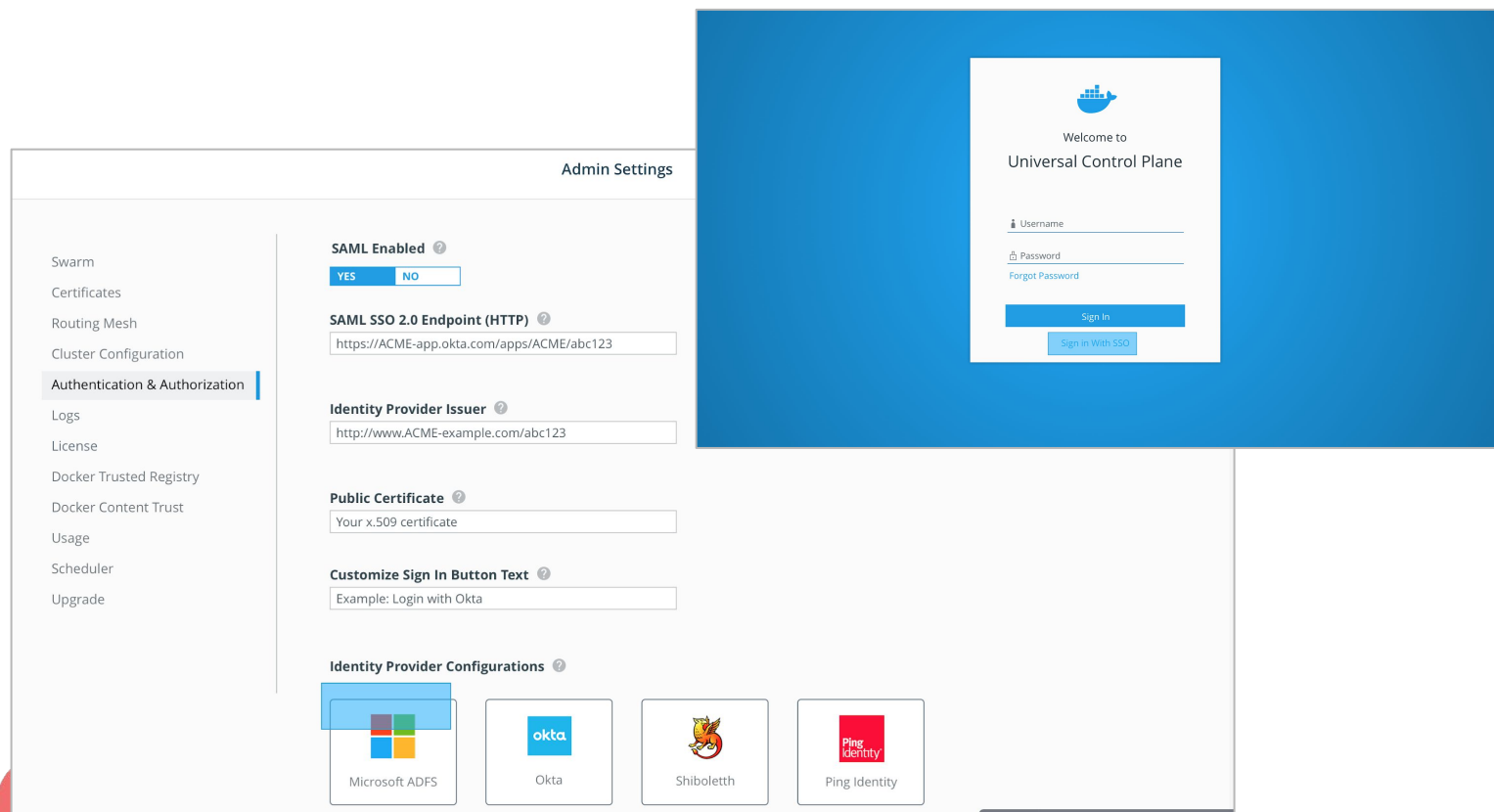
## BENEFITS

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



## A vibrant, stylized illustration of a city map, likely Barcelona, Spain. The map is rendered in a flat, graphic style with a warm orange-yellow background. White lines delineate the street grid. Various colorful icons represent different parts of the city: a large red and white church (Sagrada Família), a modern glass skyscraper (Guggenheim Museum), a colorful building (Picasso Museum), a tall tower (Torre de Colònia), a bridge (Pont de la Barceloneta), and a beach area with palm trees and people. Numerous small figures of people are scattered throughout, engaged in various activities like walking, cycling, and playing sports, adding a sense of life and movement to the map. The overall aesthetic is modern and artistic, capturing the essence of the city's diverse architecture and urban environment.

# 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

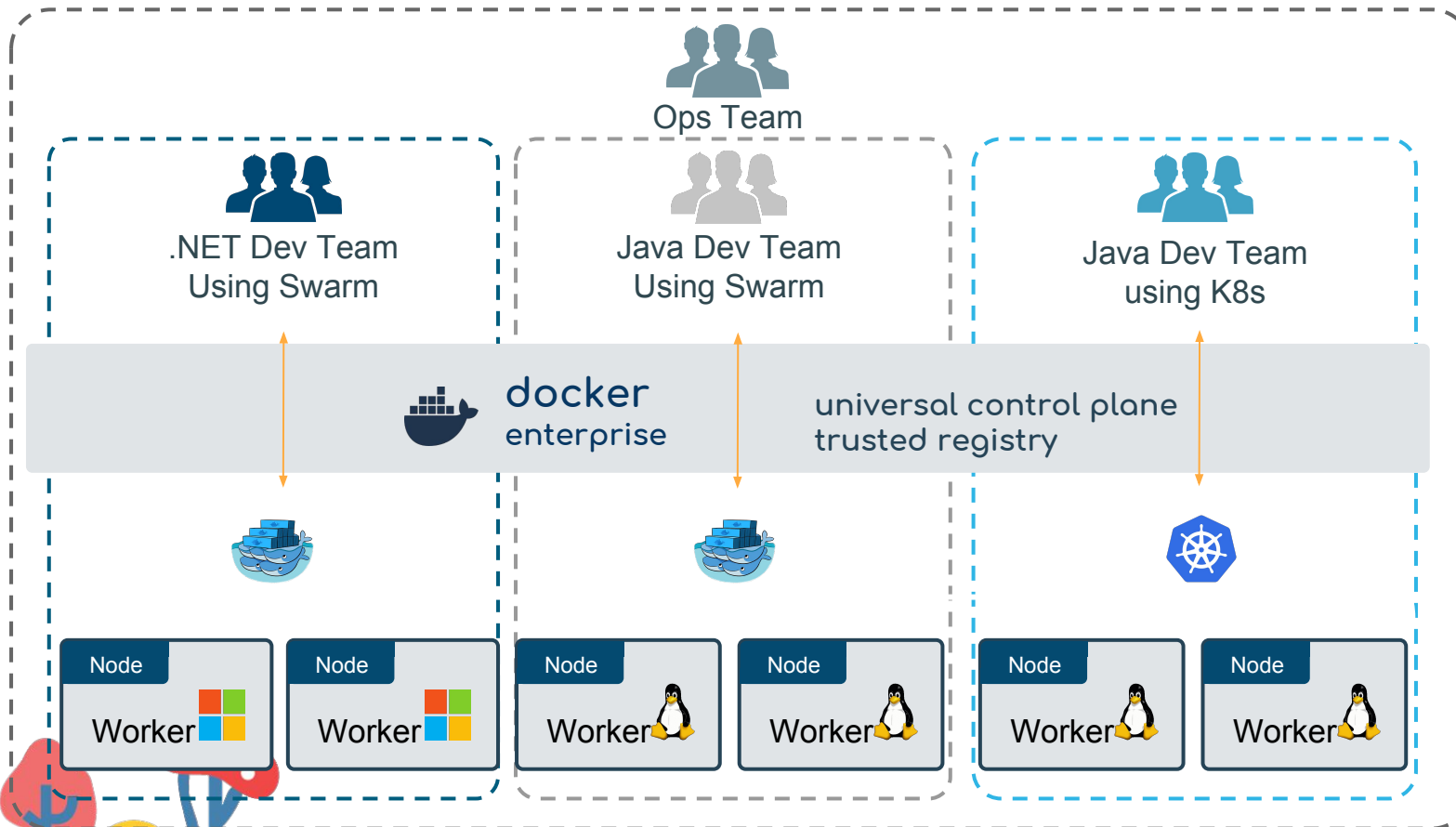


## BENEFITS

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



# Secure Access: Native Kubernetes RBAC



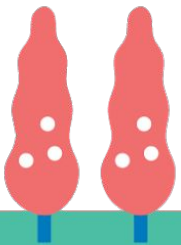
## FEATURE

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



## BENEFITS

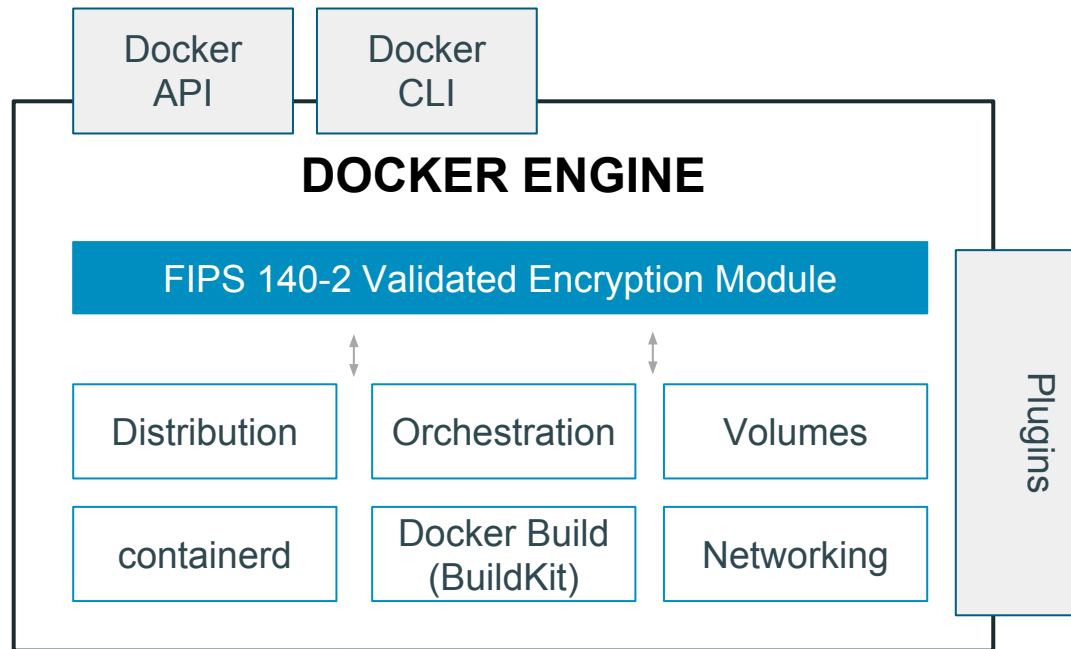
- Deploy Helm charts
- Use native Kubernetes RBAC primitives







# FIPS 140-2 Validated Docker Enterprise-Engine



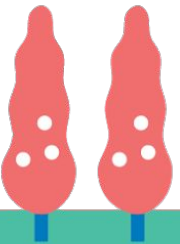
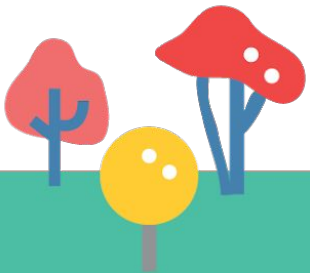
## FEATURE

- 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

user request

orchestrator

audit events



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





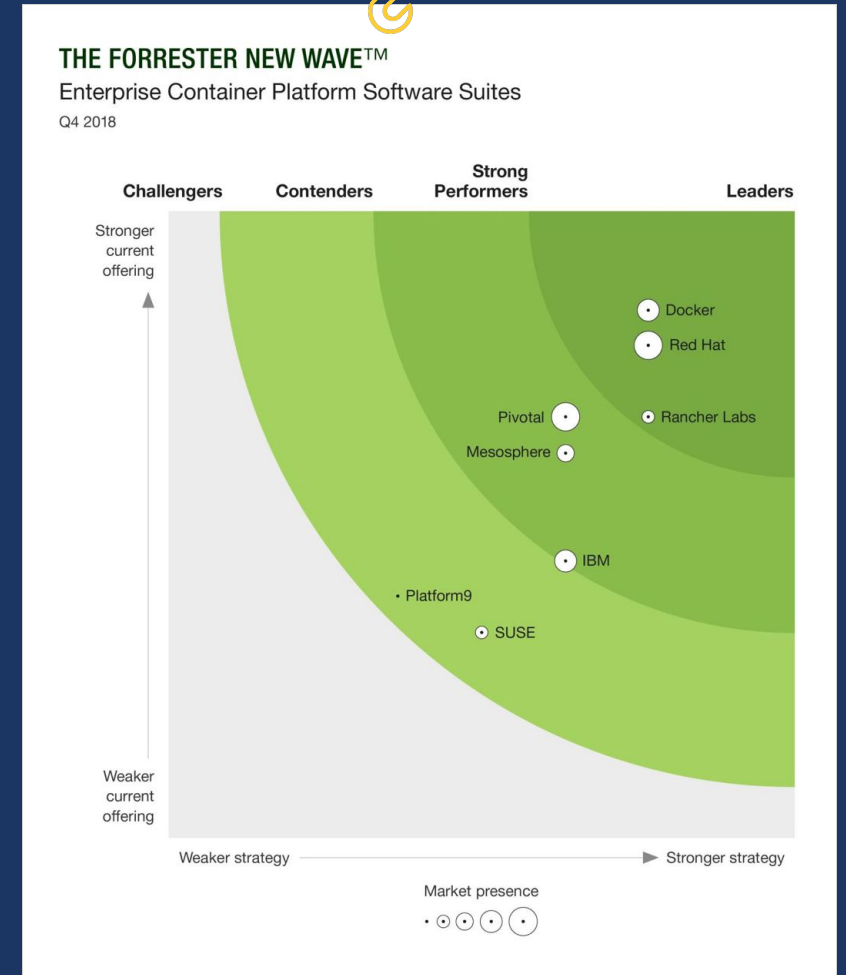




# Get the Forrester Report on Container Platforms

For more information visit:

<https://dockr.ly/Forrester>



# Migrate Legacy Windows Before End of Support

For more information visit:

<https://dockr.ly/WindowsServerUpgrade>







