Gain Confidence in Compliance

Advanced Image Scanning with Harbor

Michael Michael @michmike77
Core Maintainer, Harbor
Director of Product Management, VMware

Liz Rice @lizrice
Technical Oversight Committee Chair, CNCF
VP of Open Source Engineering, Aqua Security

CLOUD NATIVE
COMPUTING FOUNDATION

Top ten most popular docker images each contain at least 30 vulnerabilities

Source: Snyk State of Open Source Security report 2019
https://snyk.io/blog/top-ten-most-popular-docker-images-each-contain-at-least-30-vulnerabilities

Why run your own registry?

Security & Compliance

- Comprehensive
- Registry and
- Identity Fed
  Multitenan

Infrastructure

- infrastructure
- sted, edge)
- ker compliant

Scale & Control

- Control access to artifacts
- Replicate resources based on business needs

- ry
- ng investments
- services

- Syslog integration
- Webhooks
- REST API
- Robot Accounts

- Replicate Harbor artifacts to Harbor, Docker Registry, Docker Hub, Huawei Cloud, AWS, Azure, GCP, Alibaba

- Vulnerability Scanning
- CVE Exceptions
- Image Signing
- Quotas
- Retention
- OIDC/LDAP Integration w/ RBAC & CLI secrets
- Project Isolation

A Cloud Native Computing Foundation Incubating project

goharbor.io

9400+
Stars

CLOUD NATIVE
COMPUTING FOUNDATION

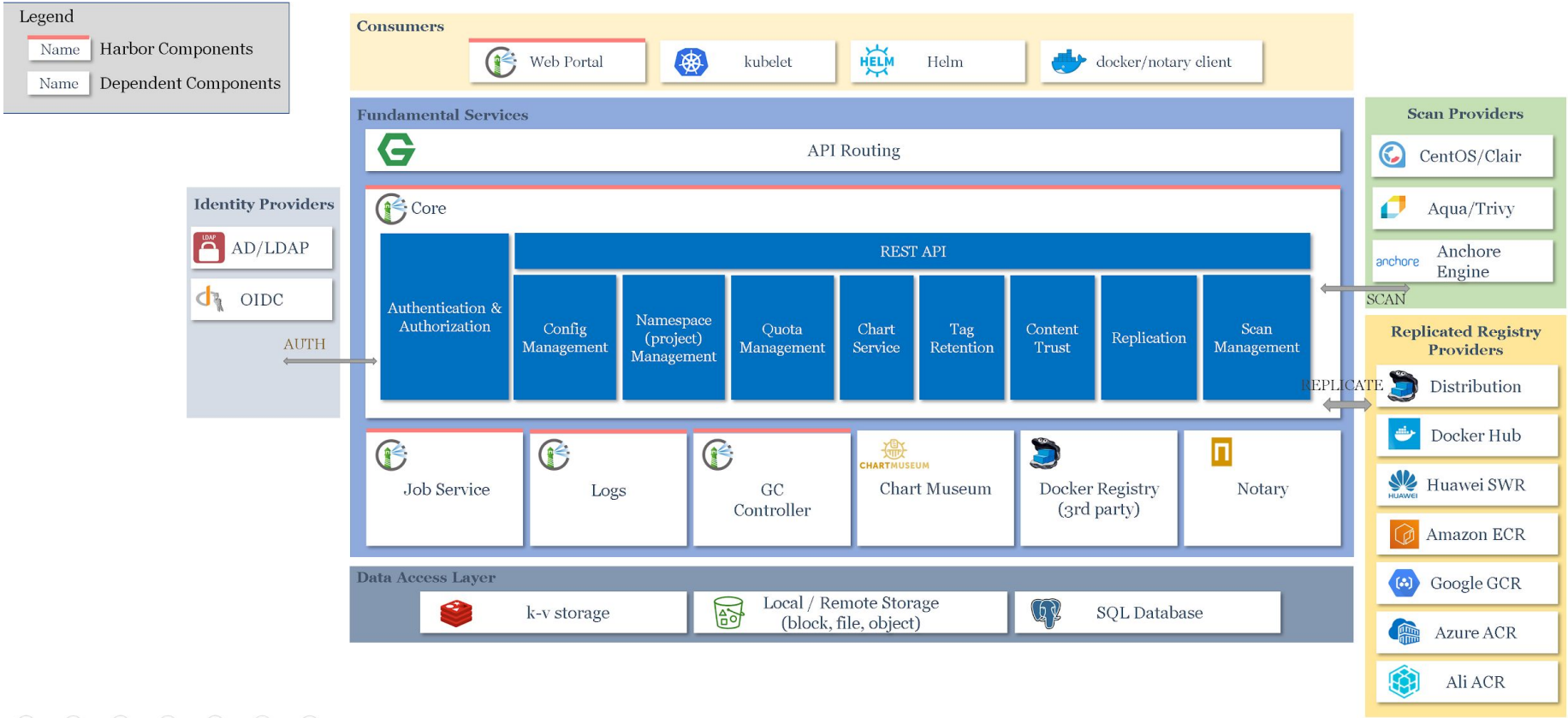
Harbor in a nutshell

Open source container image registry that secures images with role-based access control, scans images for vulnerabilities, and signs images as trusted

- Security & Compliance
- Performance
- Interoperability
- Consistent image management for Kubernetes

 |

Architecture



Harbor 1.9

Advancing multitenancy with key enterprise features

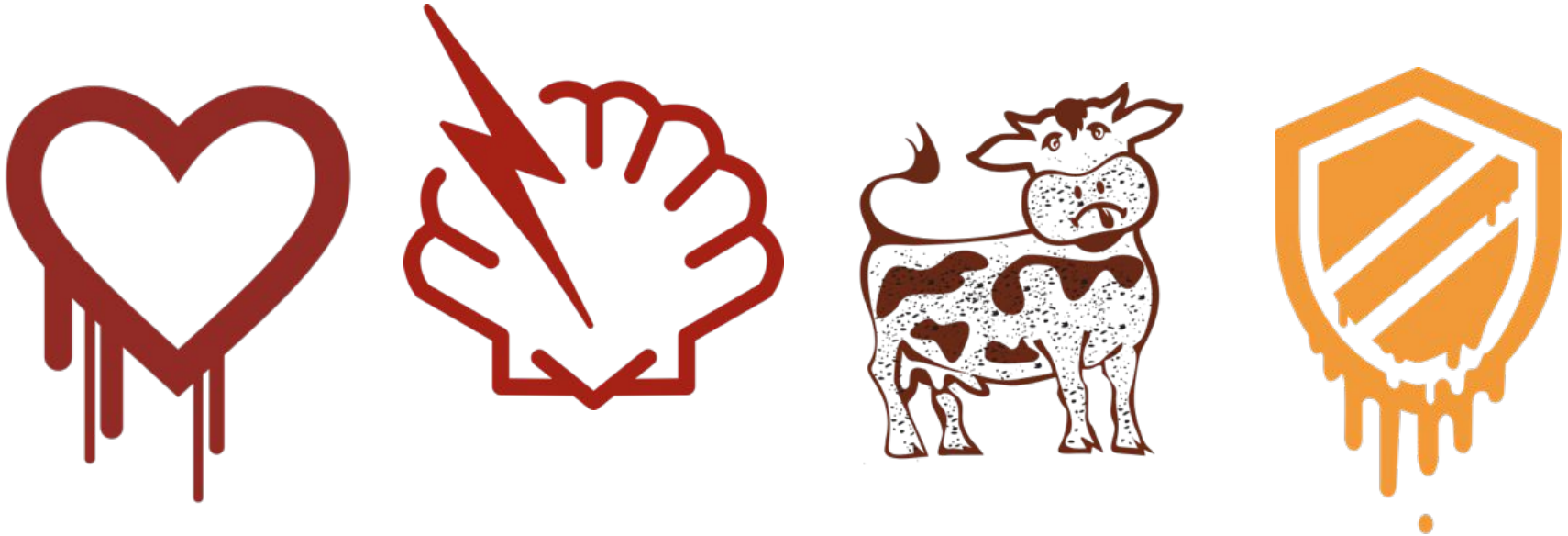
1. Image Retention Policies
2. Project Quotas
3. Webhook Events for CI/CD Integration
4. Replication Integration with AWS, Azure, GCP, Alibaba Cloud
5. CVE Exception Policies

Harbor 1.10 (In Progress)

Security & Compliance Theme

1. Immutable Images and Repositories
2. OIDC Group Support
3. Limited Guest Role
4. CLI Secret and Robot account enhancements
5. Interrogation Service
    a. Pluggable out-of-tree scanners by Anchore and Aqua

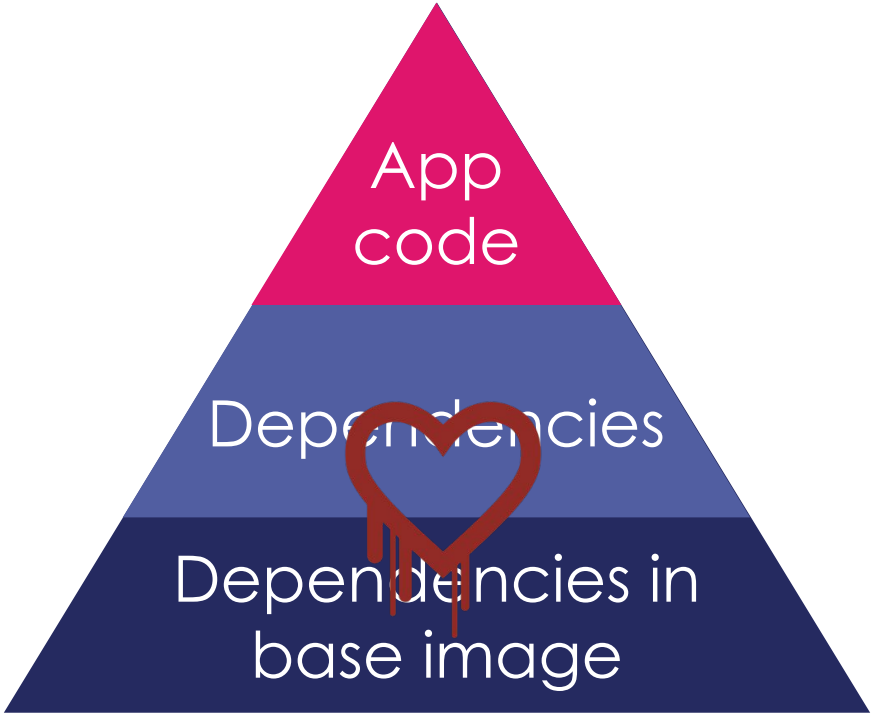
Package vulnerabilities



Container image vulnerability scanning

`yum / apt / apk`

`FROM <base image>`



Not all scanners are created equal

Which package versions have vulns?

Is package patched for this vuln in this distro?

Additional info from vendor

Additional info from security researchers

Relevant, up-to-date information sources

Accuracy & rate of false positives

Not all scanners are created equal

Which package versions have vulns?

Is package patched for this vuln in this distro?

Additional info from vendor

Additional info from security researchers

Support for language packages

Sensitive data checks

Malware scanning

Windows containers

Relevant, up-to-date information sources

Accuracy & rate of false positives

Options:

- **Open Source**
- **Free**
- **Commercial**

Functionality

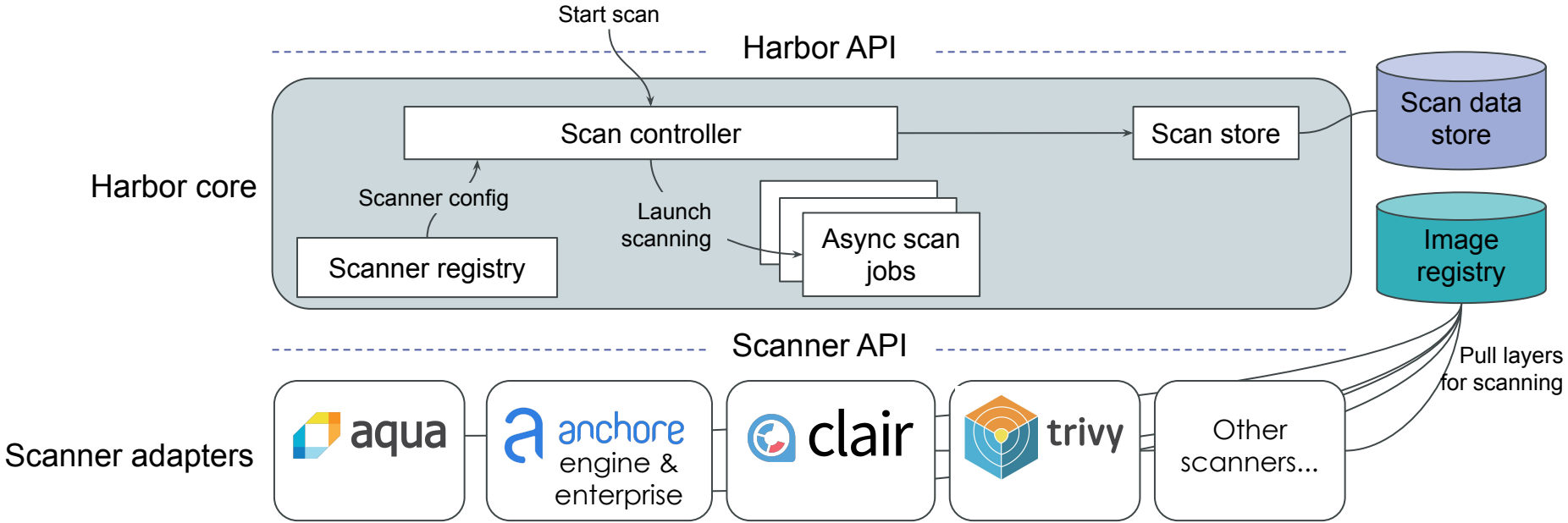
Commercial information sources

Support

Pluggable scanners in Harbor

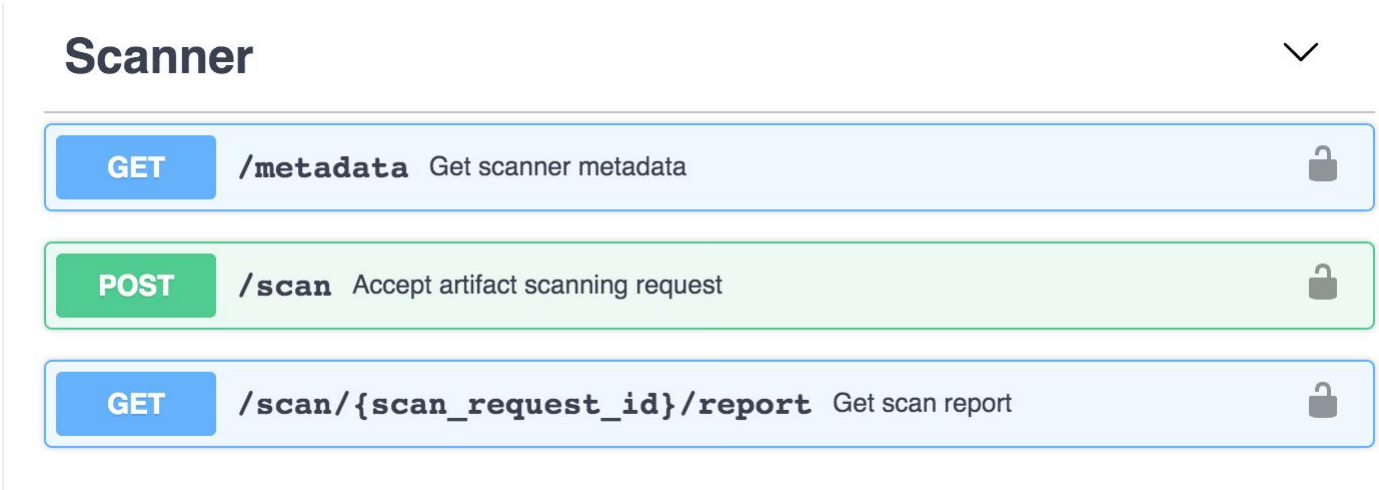
Use your preferred scanner

Per-project configuration



 |

Generic Scanner API



Demo!

CLOUD NATIVE
COMPUTING FOUNDATION

Roadmap

Management

Kubernetes Operator

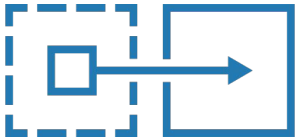
Signing Policy Replication

Metadata Management

Perf & Scale

Observability

Image Distribution



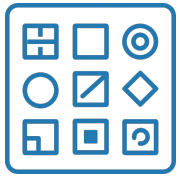
Proxy Cache

P2P Distribution

Extensibility

Webhooks++

Interrogation Service



Cloud Native Artifact Management

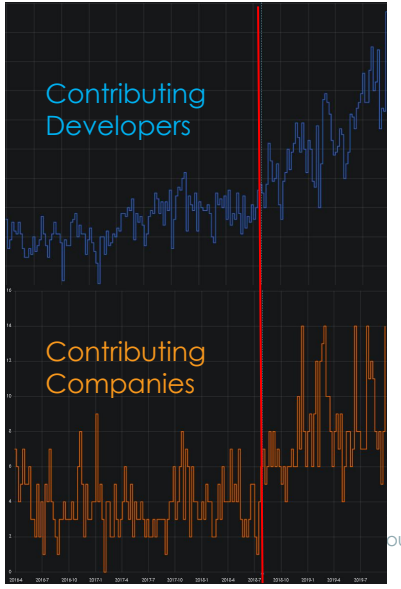
OCI conformance

The Community is Thriving

GitHub Stars	Contributors
9400+	200+

Data as of 10/10/2019

Downloads	Forks
30K+	2700+



Donated to CNCF in August 2018

oundation

HARBOR

20+ Product Implementations

vmware · caicloud 才云 · 时速云 · RANCHER · BingoCloud 品高云 · CloudChef · ise2c · Pivotal

115+ Contributing Organizations

Hyland creator of OnBase · DigitalOcean · anchore · aqua · sina 新浪 · adorsys · GM · TVM 天脉

300+ Community Members

National Commercial Bank Jamaica Limited · SLAMTEC · TREND MICRO · 360 www.360.cn · OnStar · 中国移动 China Mobile · 腾讯云 · 京东

Collaborate with the Harbor team

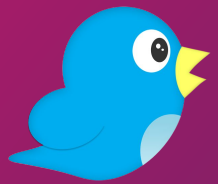
GoHarbor.io

lists.cncf.io/g/harbor-users
lists.cncf.io/g/harbor-dev

#harbor
#harbor-dev

demo.goharbor.io

- *Username: admin*
- *Password: Ask in Slack*



@project_harbor

github.com/goharbor/community/blob/master/MEETING_SCHEDULE.md

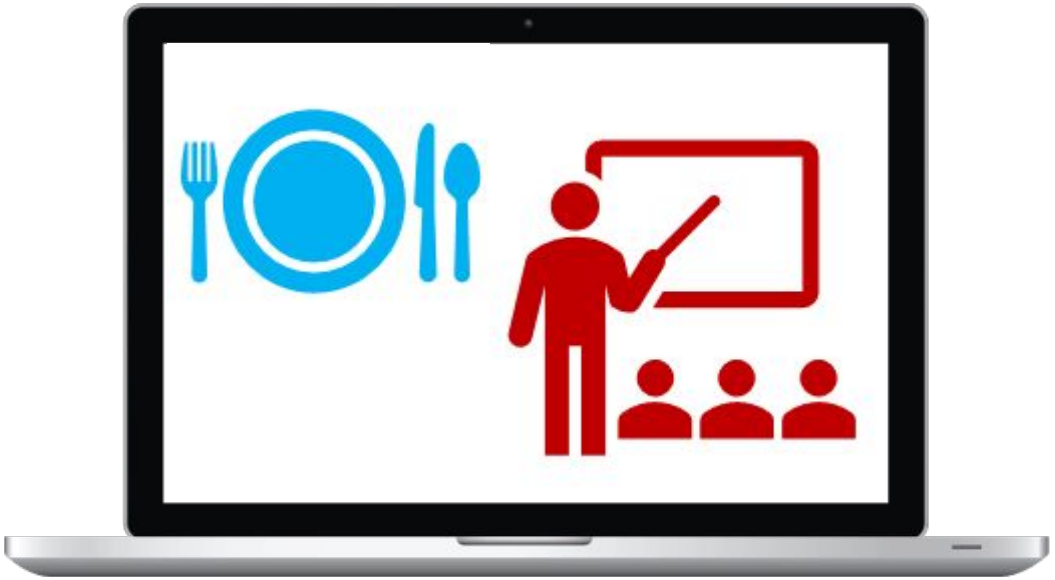
- APAC+EU zone: 9pm UTC+8 time zone
- *Americas+EU zone: 1pm Pacific time zone*

CLOUD NATIVE
COMPUTING FOUNDATION

Join us for a working lunch at KubeCon

Monday, November 18th
12:30pm-4:00pm

Join us for lunch with Joe Beda, co-founder of Kubernetes, at 12:30, and then get real hands-on experience with installing, configuring, and using Harbor at the Harbor Lunch and Learn workshop



 |