KubeCon

CloudNativeCon

THE LINUX FOUNDATION

OPEN SOURCE SUMMIT

AI_dev

Open Source GenAI & ML Summit

China 2024

KubeCon | CloudNativeCon

THE LINUX FOUNDATION OPEN SOURCE SUMMIT

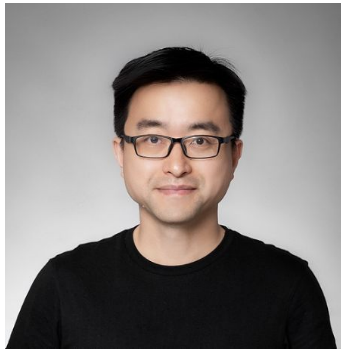
AI_dev Open Source GenAI & ML Summit

China 2024

Strengthening Container Security: A Collaborative Journey

Beltran Rueda, Sr Eng Manager, VMWare Tanzu / Broadcom
Yi Zha, Senior Product Manager, Microsoft

About us



Yi Zha

Sr Product Manager at Microsoft
Maintainer at CNCF project Notary Project
Cloud Native Supply Chain Security and Ecosystem

Beltran Rueda

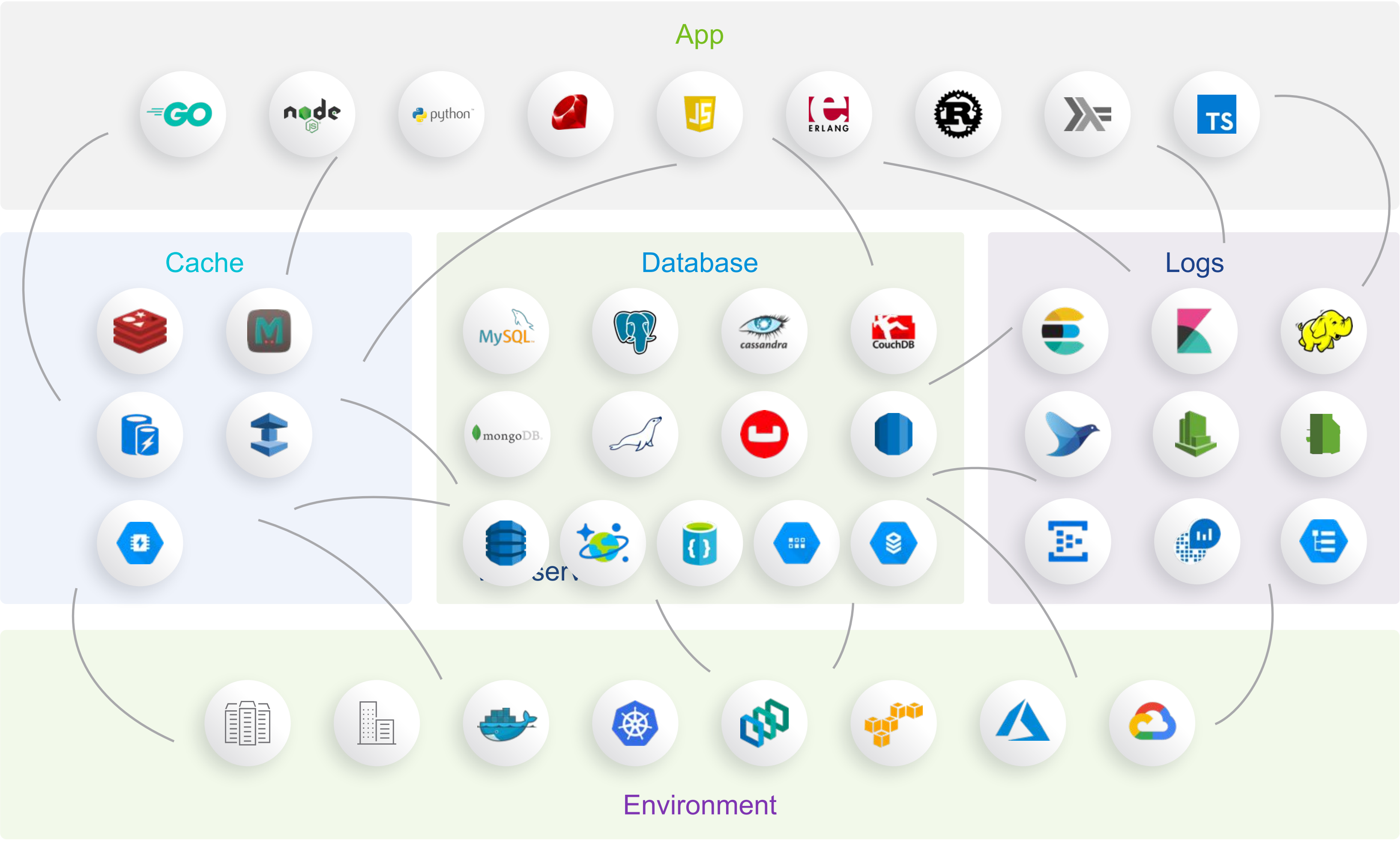
Sr Engineering Manager at VMware Tanzu (Broadcom)
+16 years as part of the Bitnami project
Secure Software Supply Chain, Continuous Delivery,
Kubernetes native solutions

Agenda

- Background
- How Bitnami solves the problems?
- Notary Project - Authenticity and Integrity
- OCI specification - Storage and Distribution
- Demo
- Takeaways
- Q&A

Background

Your modern application architecture



Questions

1. How can I ensure images are from trusted identities?

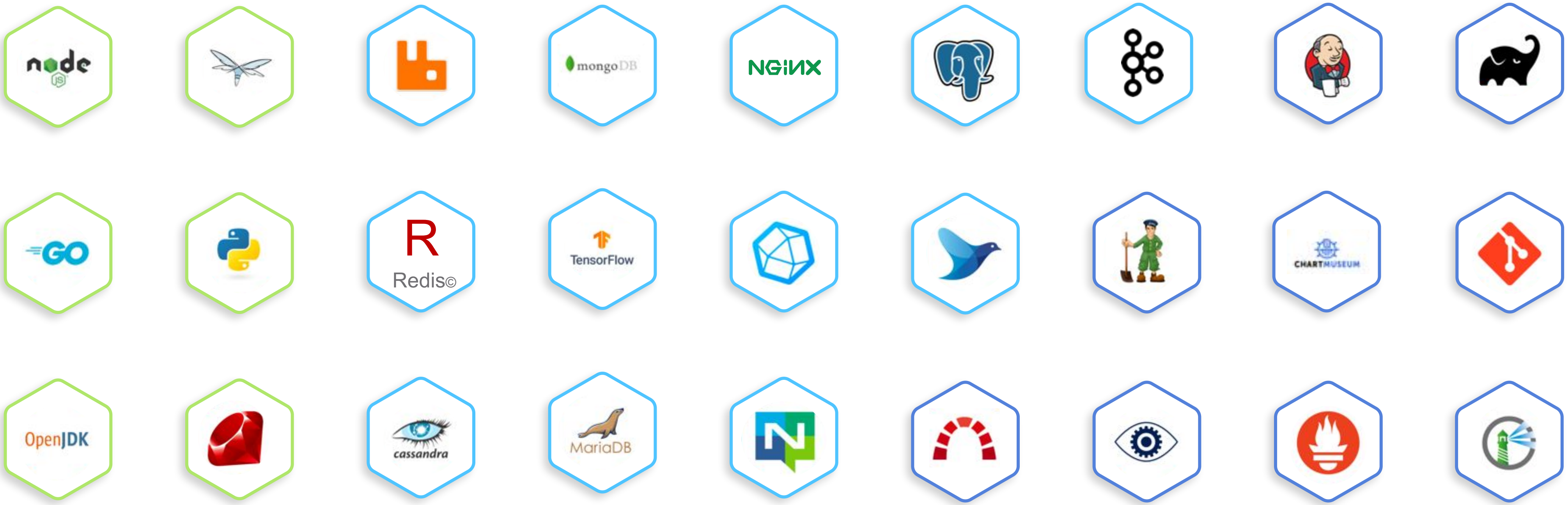
2. How can I ensure images are not modified since built?

3. How can I ensure images are distributed securely across registries, even in multi-clouds environment?

How Bitnami solves the problems?

<u>Trusted catalog</u> of +240 OS applications in multiple formats all of them built, tested & up-to-date

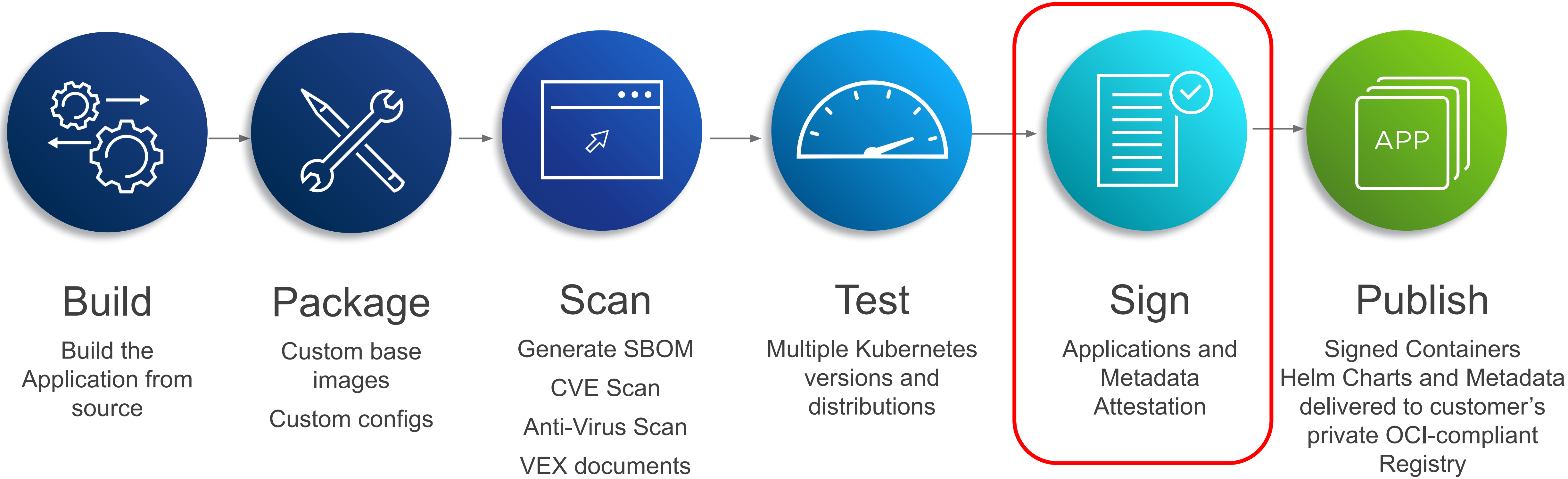
Language Runtimes | App Components | Supporting Apps



Containers, Helm Charts, Virtual Machines

How Bitnami solves the problems?

You choose the applications needed for your private catalog.
We build, test and deliver them, and we keep them up to date



Build

Build the Application from source

Package

Custom base images

Custom configs

Scan

Generate SBOM

CVE Scan

Anti-Virus Scan

VEX documents

Test

Multiple Kubernetes versions and distributions

Sign

Applications and Metadata Attestation

Publish

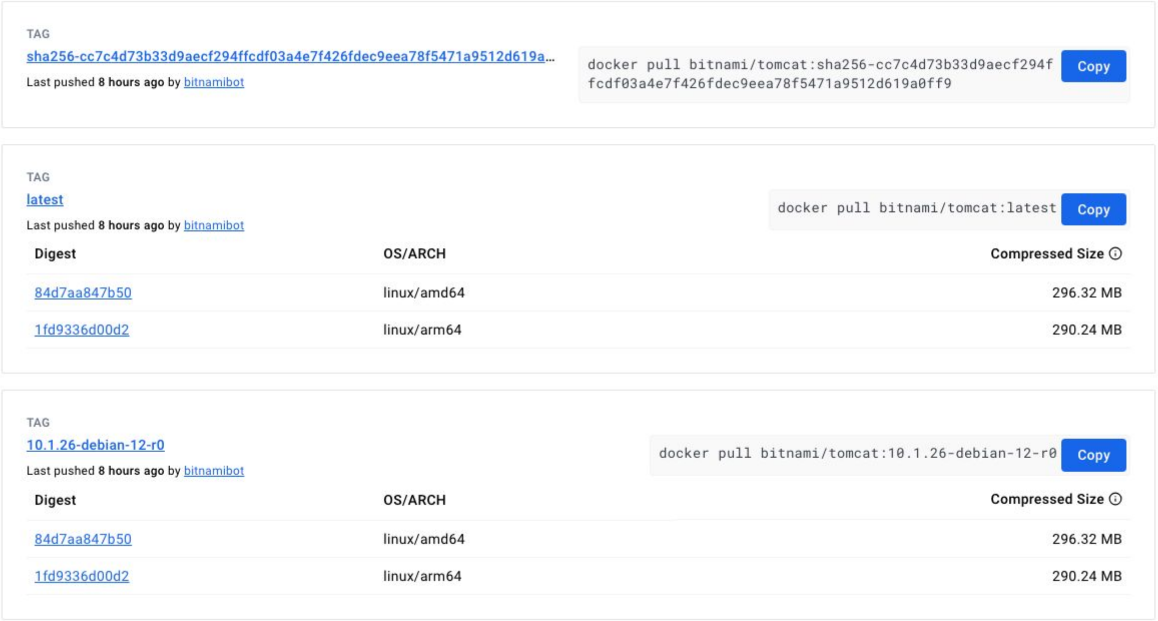
Signed Containers Helm Charts and Metadata delivered to customer's private OCI-compliant Registry

Signed artifacts at Bitnami and Tanzu Application Catalog

Bitnami

Container images signed with Notation

Up-to-date and available in DockerHub



TAG

sha256-cc7c4d73b33d9aecf294ffcdf03a4e7f426fdec9eea78f5471a9512d619a...

Last pushed **8 hours ago** by bitnamibot

```
docker pull bitnami/tomcat:sha256-cc7c4d73b33d9aecf294f
fcdf03a4e7f426fdec9eea78f5471a9512d619a0ff9
```

TAG

latest

Last pushed **8 hours ago** by bitnamibot

```
docker pull bitnami/tomcat:latest
```

Digest	OS/ARCH	Compressed Size ⓘ
84d7aa847b50	linux/amd64	296.32 MB
1fd9336d00d2	linux/arm64	290.24 MB

TAG

10.1.26-debian-12-r0

Last pushed **8 hours ago** by bitnamibot

```
docker pull bitnami/tomcat:10.1.26-debian-12-r0
```

Digest	OS/ARCH	Compressed Size ⓘ
84d7aa847b50	linux/amd64	296.32 MB
1fd9336d00d2	linux/arm64	290.24 MB

Tanzu Application Catalog (TAC)

Signed images signed with Notation

OCI Metadata signed with Notation

- SBOM “Software Bill of Materials”
- VEX “Vulnerability Exploitability eXchange”
- In-toto attestation document
- CVE, Antivirus scans
- Verification test results

Custom delivery in private registries and support for air-gapped environments

Notary project
- Safeguard cloud native supply chains

Notary project

CNCF Incubating project

https://notaryproject.dev

1. How can I ensure images are from trusted identities?

2. How can I ensure images are not modified since built?

aws

Microsoft

bitnami by vmware

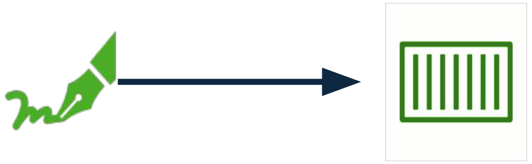
Alibaba Cloud

Venafi

HARBOR

OCI specifications
Store and distribute any content using OCI registries

Open Container Initiative (OCI)
Linux Foundation project
https://github.com/opencontainers



3. How can I ensure images are distributed securely across registries, even in multi-clouds environment?

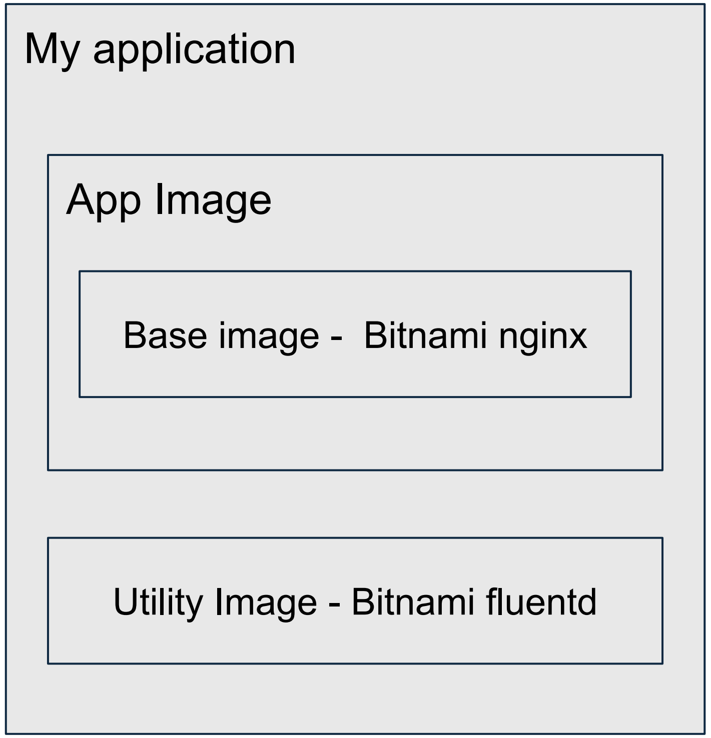
OCI v1.1 is stable now! The release blog

OCI Registries:

Clients:

CNCF sandbox project
https://oras.land

Demo



My application

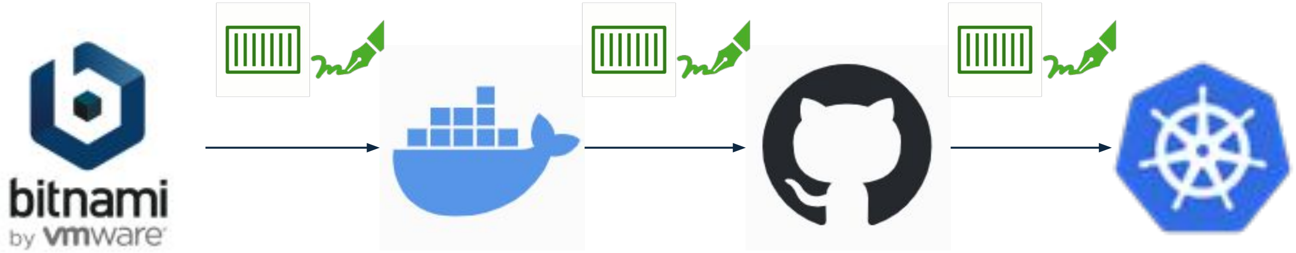
App Image

Base image - Bitnami nginx

Utility Image - Bitnami fluentd

Workflows:

1. Acquire the base image published by Bitnami
2. Acquire the utility image published by Bitnami
3. Build my application
4. Promote images to production
5. Deploy my application to K8s



Takeaways

- Authenticity and Integrity are essential for strengthening container security.
- Always validate images before using them.

How can I ensure images do not contain vulnerabilities or non-compliant software?

Q&A

Thank you!

Welcome to visit and contribute to the Notary Project community!

- Slack: https://app.slack.com/client/T08PSQ7BQ/CQUH8U287/
- Website: https://notaryproject.dev/

Deploy hundreds of apps easily in Kubernetes with the Bitnami Helm charts

- Slack: @Beltran
- E-mail: beltran.rueda-borrego@broadcom.com