OPENSHIFT INTEGRATION
April, 2018

CYBERARK ROADMAP

This presentation is for information only and represents CyberArk's current view of its product direction. It is not a commitment or an obligation to deliver any feature or functionality. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion

WHO IS CYBERARK?

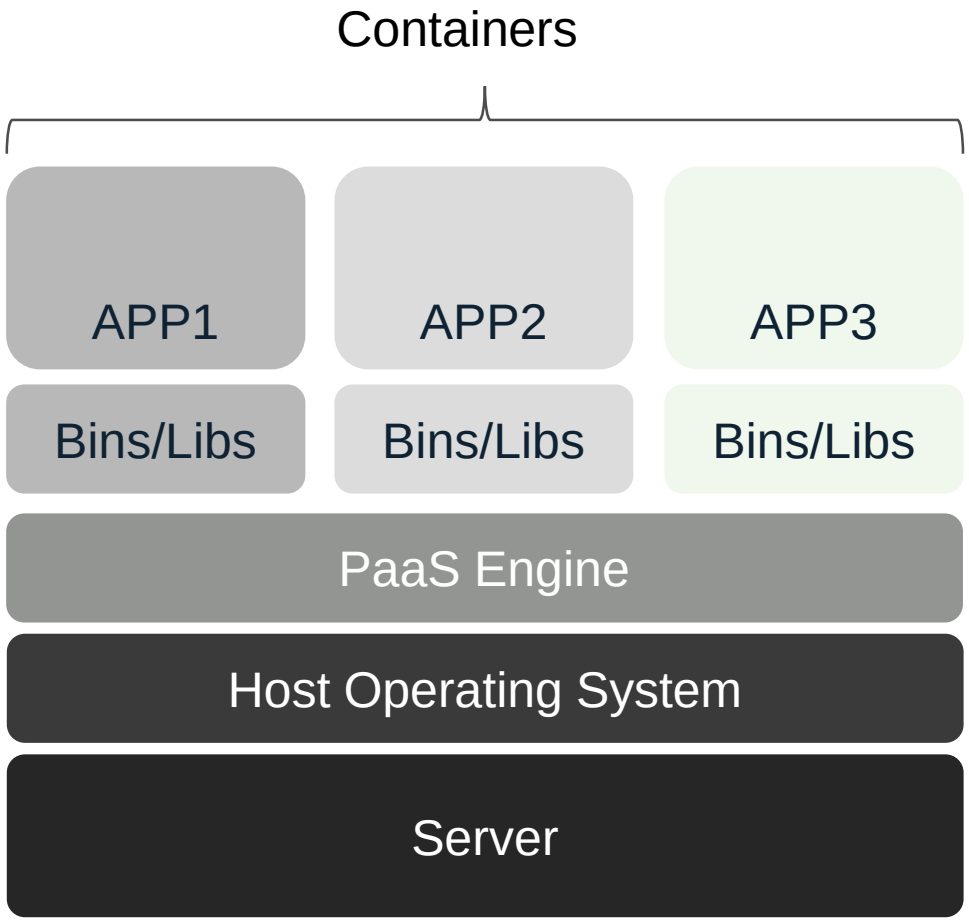
- Market Leader in **Privileged Account Security**
- **Protecting the heart of the enterprise against advanced cyber attacks**
- **2nd largest Israeli Cyber Security Company in the World**
- Proven successful **continuous innovation**
- Award Winning Enterprise Class Solutions

CYBERARK CONJUR

CyberArk Conjur is a DevOps and cloud security solution

- Addresses the unique secrets management and privileged access security challenges of the DevOps pipeline
- Native integration with cloud management and DevOps orchestration solutions
- Focused on security – supports Separation of Duties
- Designed for developers – Open Source accessible, well documented, fully supported

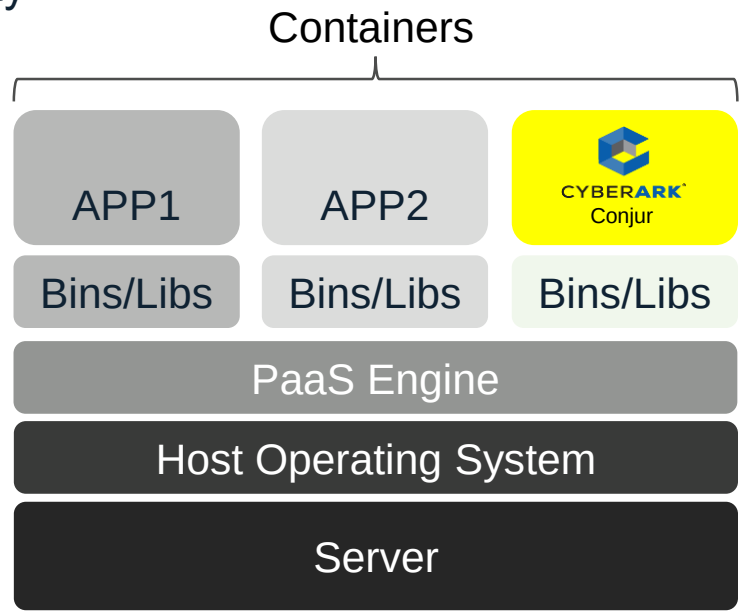
SECURING APPLICATIONS WITHIN CONTAINERIZED PLATFORMS



- **Popular methods for providing secrets to containers**
  - Via environment variables
  - Via volume mount
  - Secret encryption
- **Main challenges**
  - Secrets can be easily exposed
  - No runtime authentication process of the calling container
  - Lack of segregation of duties
  - No audit trail

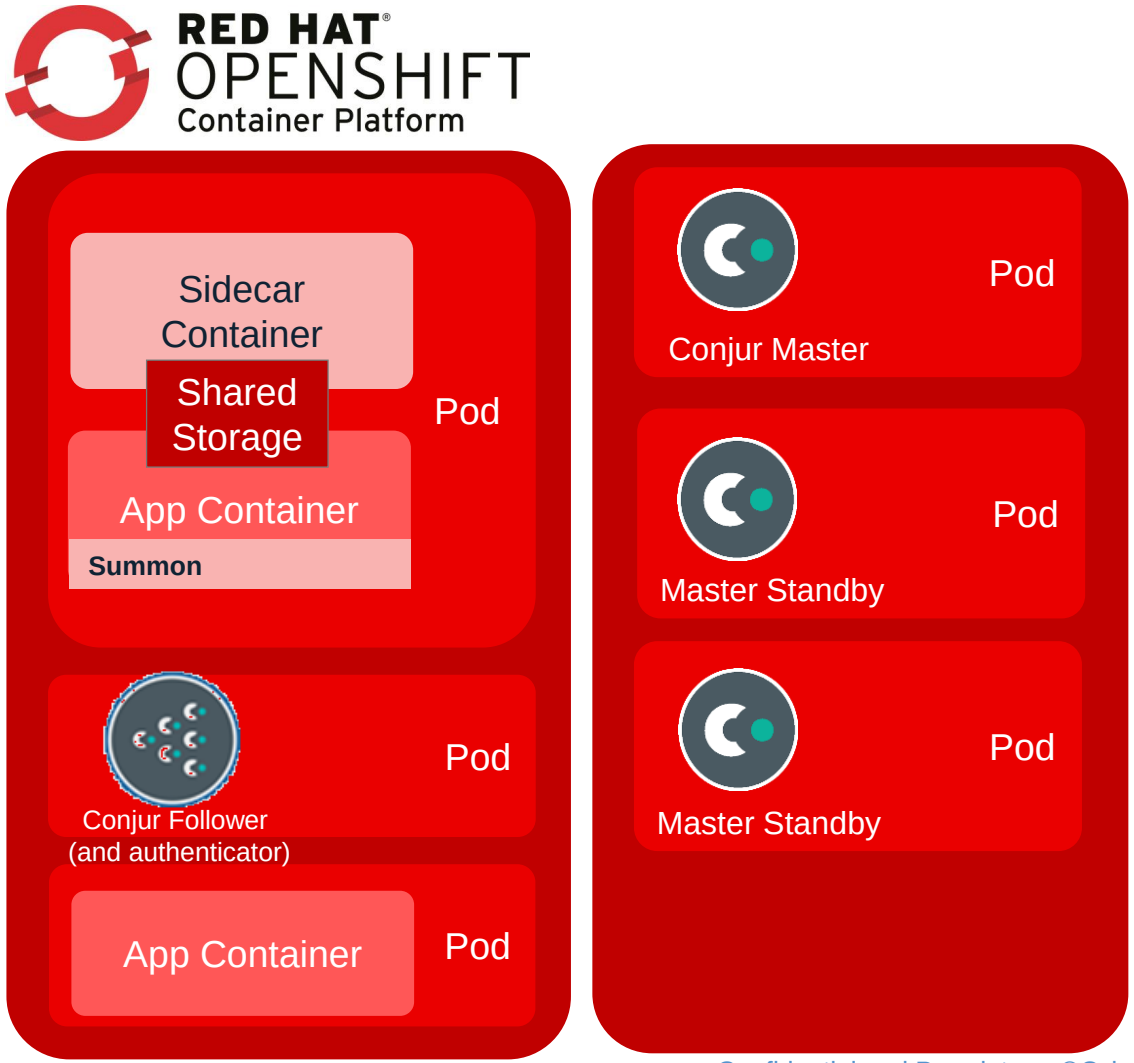
INTEGRATION GOALS AND BENEFITS

- Securely provide secrets to application running in PaaS
- Ease of use - Seamlessly integrate into the PaaS environment
- Strong Authentication of the calling container/ pod based on its properties
  - Leverage the OpenShift API's to verify the application container identity
- Conjur running inside OpenShift
  - Elastic, can scale out
  - Can run on the same physical host (performance)
- Central audit
- Secret rotation



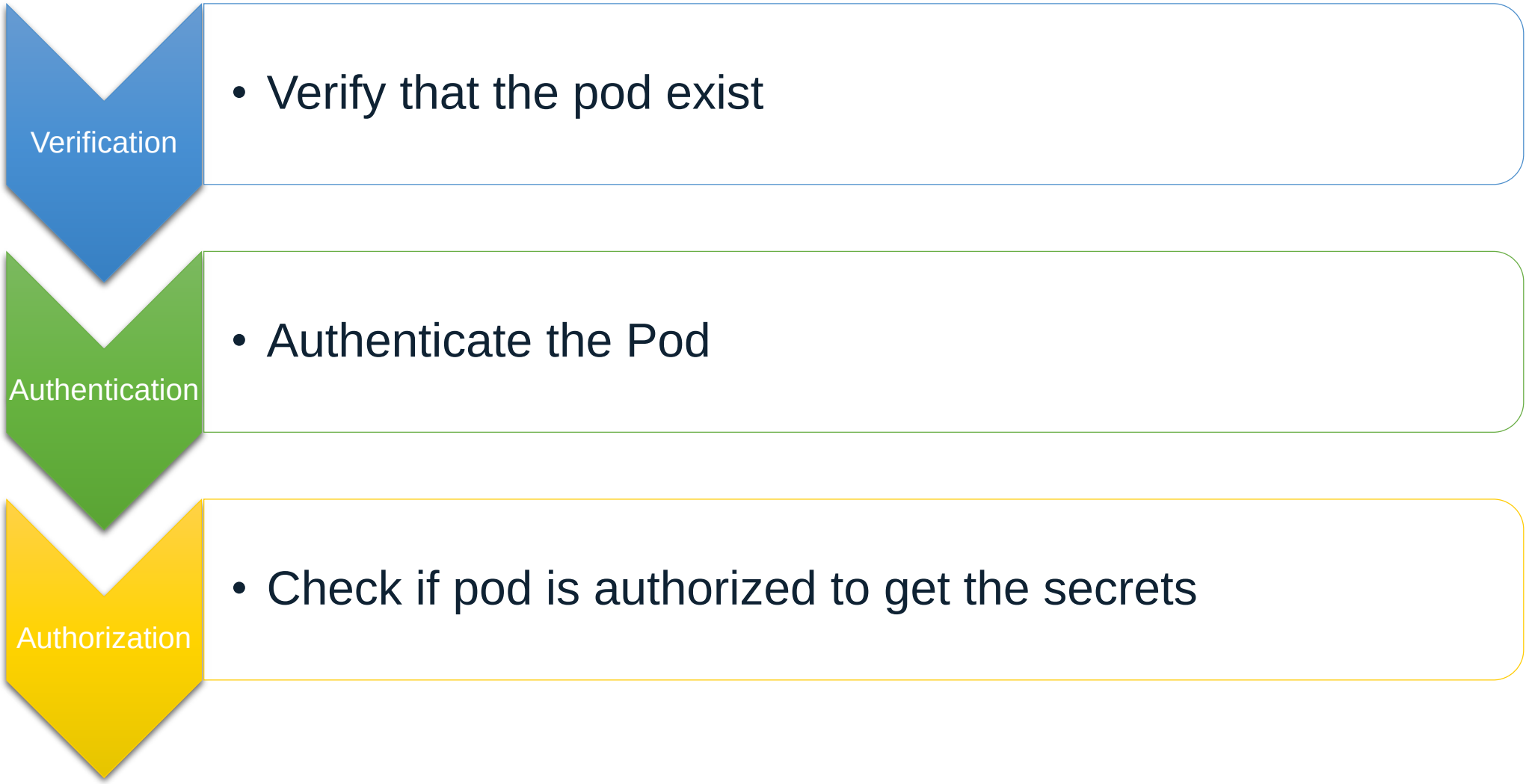
RED HAT® OPENSHIFT Container Platform

INTEGRATION COMPONENTS

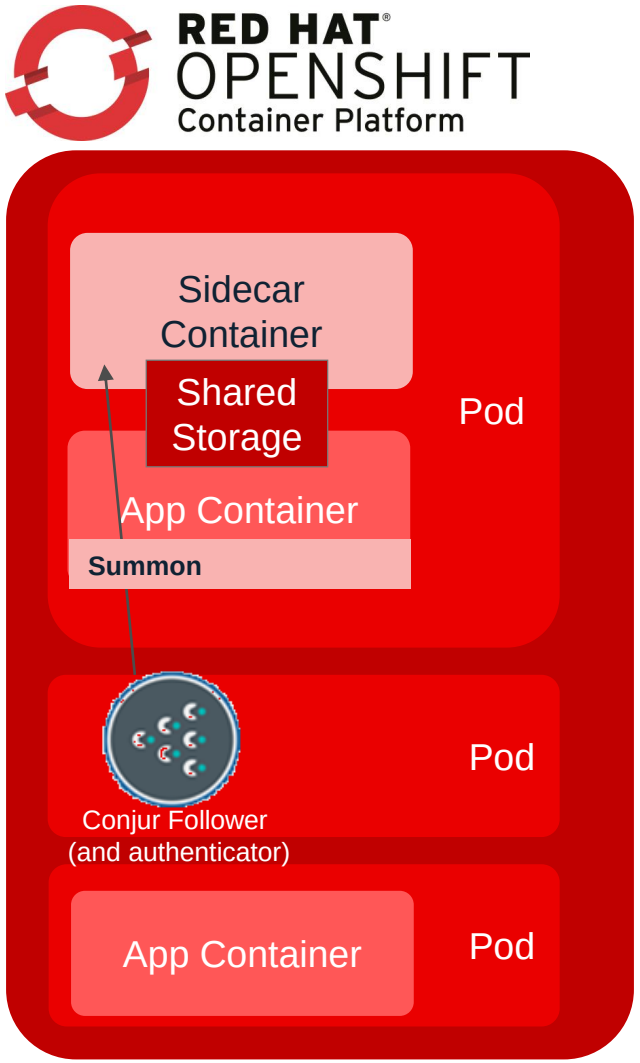


- **Conjur Master** – Secret managed repository. Supports full read/write operations such as permission checks, as well as management of policies, secrets and all Conjur services.
- **Conjur Follower** – Read only replica of the Master. Distributed across data centers and geographies to locally support application read requests and to distribute load from the Master. Can scale horizontally, and each additional follower adds read capacity.
- **Authenticator** – Kubernetes authentication component, part of the Follower.
- **Summon** – Open Source component, used for control the process order as well as push the secrets into the environment variables.
- **Sidecar container** – CyberArk container, responsible for the login process of the pod against the authenticator.

HIGH LEVEL STEPS



OPENSHIFT – CONJUR FLOW



1. When the Pod starts, a Sidecar container goes up, and creates a CSR (Certificate Signing Request)

2. Login to Conjur authenticator with the CSR and pod details. Conjur verifies the pod exists, using the pod details against Kubernetes API, and generates a signed certificate and writes it to the sidecar container (out of band)

3. Sidecar container calls Conjur authenticate using the signed certificate and verifies that the pod identity against Conjur policies using the pod details and gets an encrypted token back.

4. Sidecar container uses the pod certificate private key to decrypt the access token. Sidecar Container writes the decrypted token to the pod shared memory.

5. Summon uses the token to fetch the secrets from Conjur and writes the retrieved secrets to the environment variables.

6. Application starts and uses the secrets.

CYBERARK

DEMO TIME…

BENEFITS

- ✓ Simple, context free, secure method for retrieving credentials in containers
- ✓ End to End encryption
- ✓ Only authenticated & authorized apps can get credentials
  - ✓ Leveraging Kubernetes API's for the authentication
- ✓ Conjur running inside OpenShift
  - ✓ Elastic, can scale out
  - ✓ Can run on the same physical host (performance)
- ✓ SoD between applications
  - ✓ SoD also between the OpenShift security operator and the development teams using Conjur policy
- ✓ Credentials are not exposed to any 3rd party, reside only in memory
- ✓ Full audit trail

KEY TAKEAWAYS & WHERE TO LEARN MORE

Key Takeaways

- Use Conjur-OpenShift integration to authenticate your application pods, and retrieve the secrets needed only to the authorized applications
- Easy deployment, no code change to your application containers

Where to Start

- Documentation on the Conjur-OpenShift Integration is available here
- For more information on the integration please contact CyberArk
- CyberArk Conjur - Free and Open Source version of Conjur is available at conjur.org.
  - This integration is available only in Conjur Enterprise version
- Visit us at www.cyberark.com/conjur

CYBERARK

THANK YOU