KubeCon CloudNativeCon

THE LINUX FOUNDATION

OPEN SOURCE SUMMIT

AI_dev

Open Source GenAI & ML Summit

China 2024

Enforceable Supply Chain Security Policy with OPA Gatekeeper and Ratify

Faynman Zhou, Microsoft & Dahu Kuang, Alibaba Cloud

Who we are

- Feynman Zhou
- Product Manager for Microsoft Azure
- Ratify Maintainer, CNCF Ambassador

@FeynmanZhou

- Kuang Dahu
- Alibaba Cloud
- ACK Team, Senior Engineer
- github.com/DahuK

@DahuK

Agenda

- Why Software Supply Chain Security matters?
- Popular Open-Source Projects & Framework in the industry and CNCF
- How Ratify and OPA Gatekeeper help secure your supply chain
- End-to-end demo: Signing and verify images on Kubernetes

KubeCon

CloudNativeCon

THE LINUX FOUNDATION

China 2024

Concepts and Challenges of Software Supply Chain Security

Traditional supply chain v.s. Software supply chain

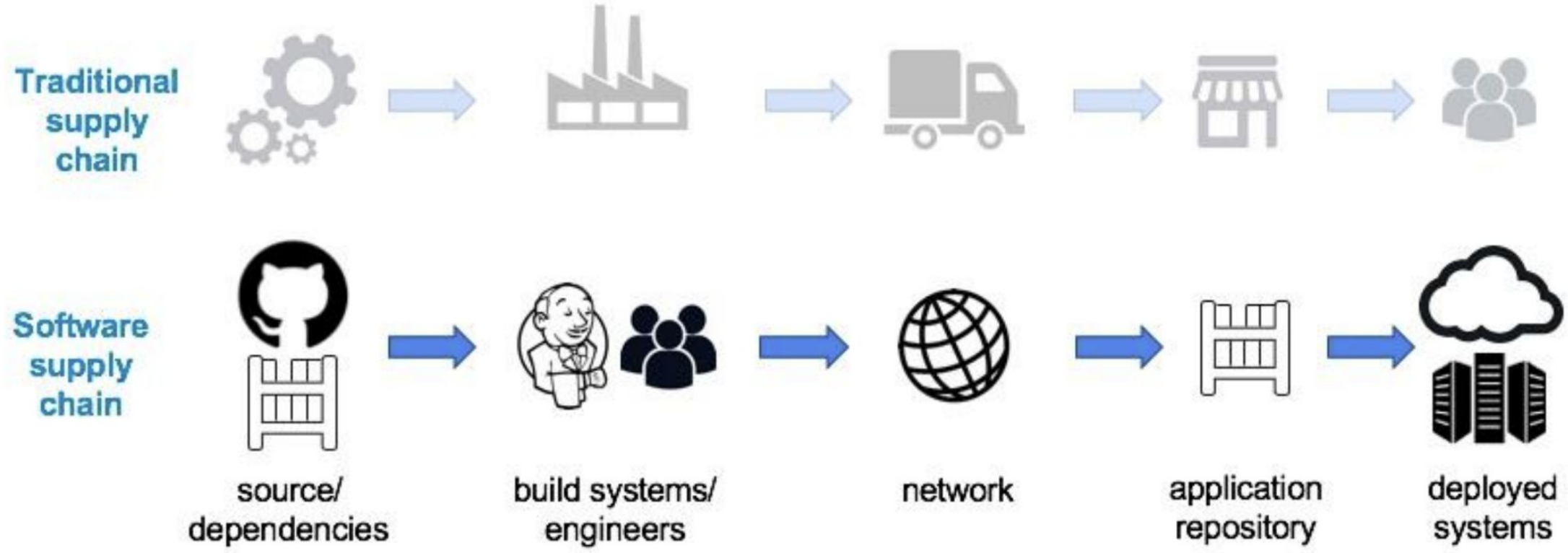


Image source: CNCF Software Supply Chain Security Paper

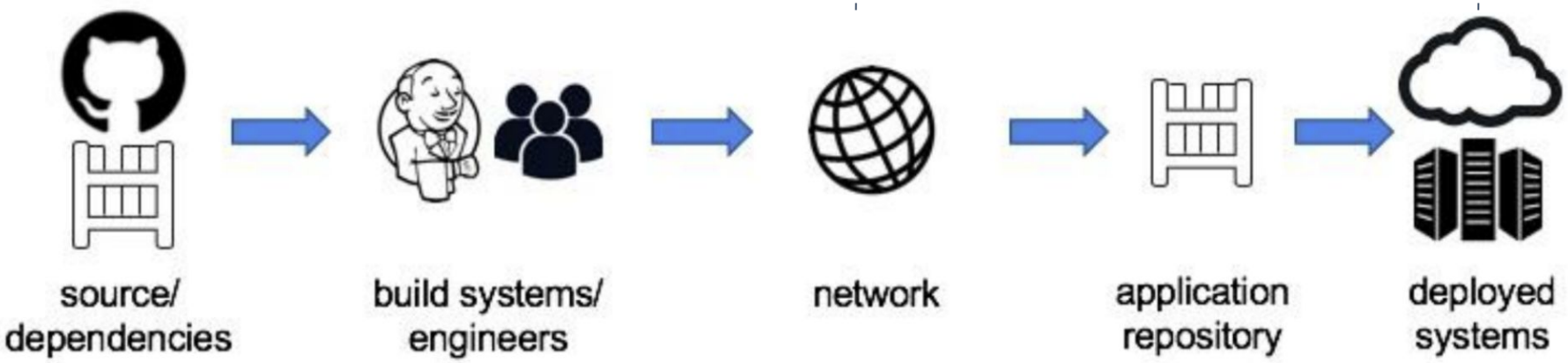
Potential security attacks and incidents

Code compromised
Non-compliant license

2021 hypocrite commits
2024 HashiCorp changed its OSS license

Network transformation attack

Deploy non-compliant code
System credential leak



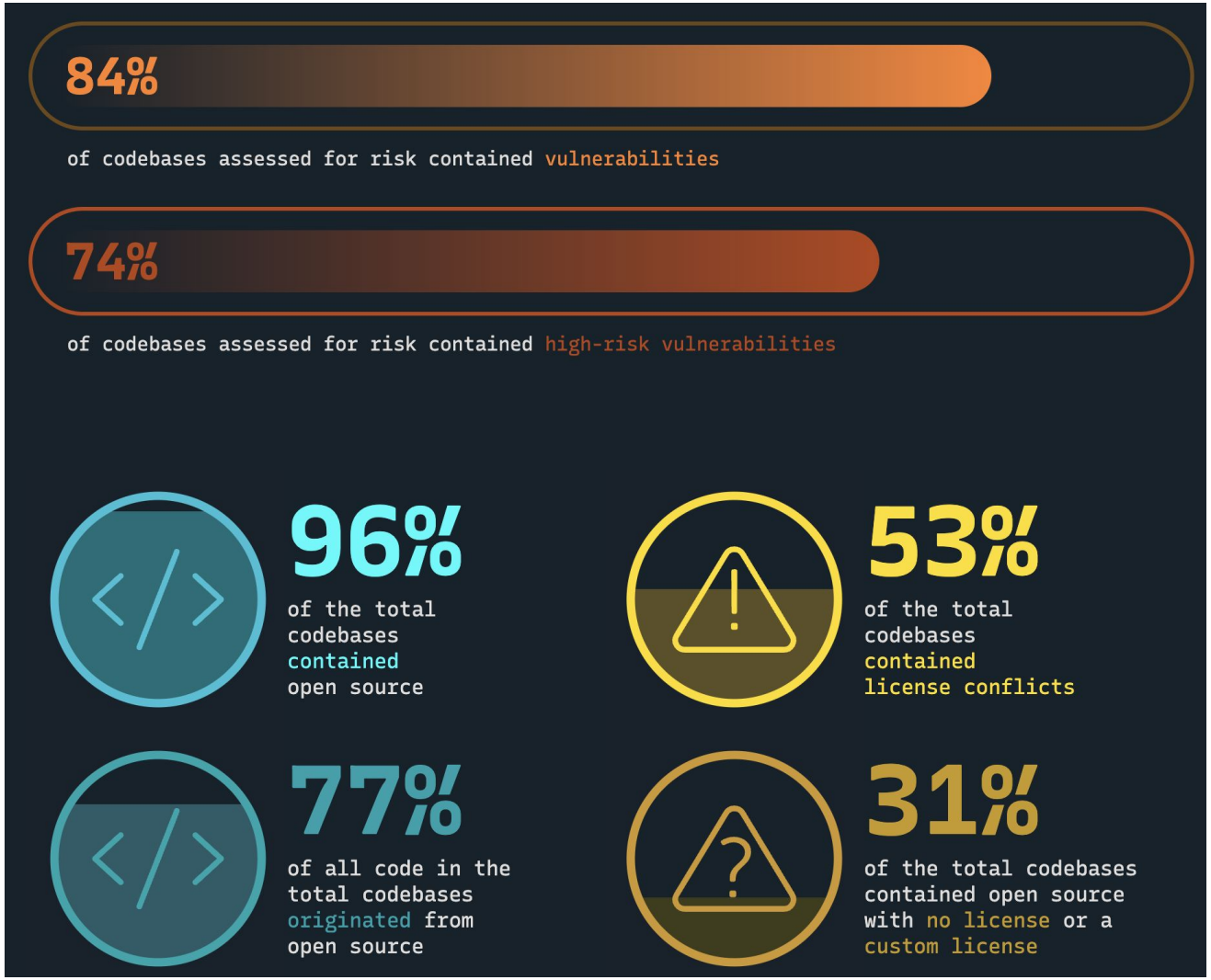
2024 XZ Utils (CVE-2024-3094)
2023 OpenAI
2021 CodeCov
2021 Log4j
2020 SolarWinds

Vulnerabilities in components or dependencies

Repository comprised

Security attack and risk assessments

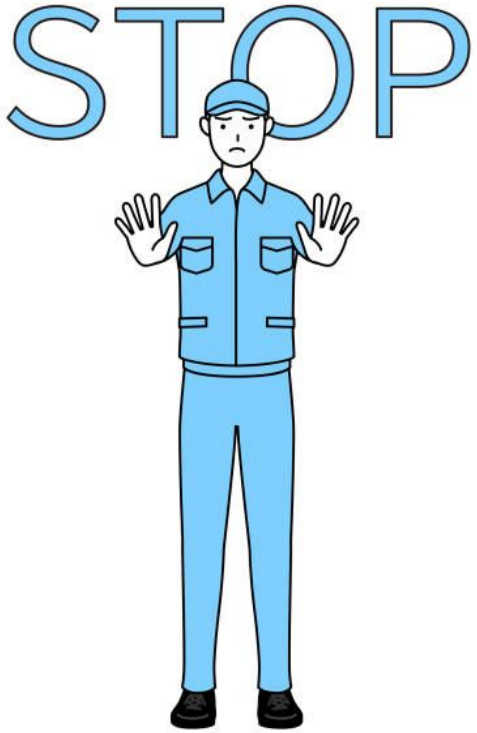
From《Synosys Open Source Security and Risk Analysis report - 2024》:



Security attack and risk assessments

Do not use any vulnerable dependencies!

Policy team



Do not use any outdated images from external registry!

Security manager

Do not use non-compliant open-source project

Compliance team

KubeCon

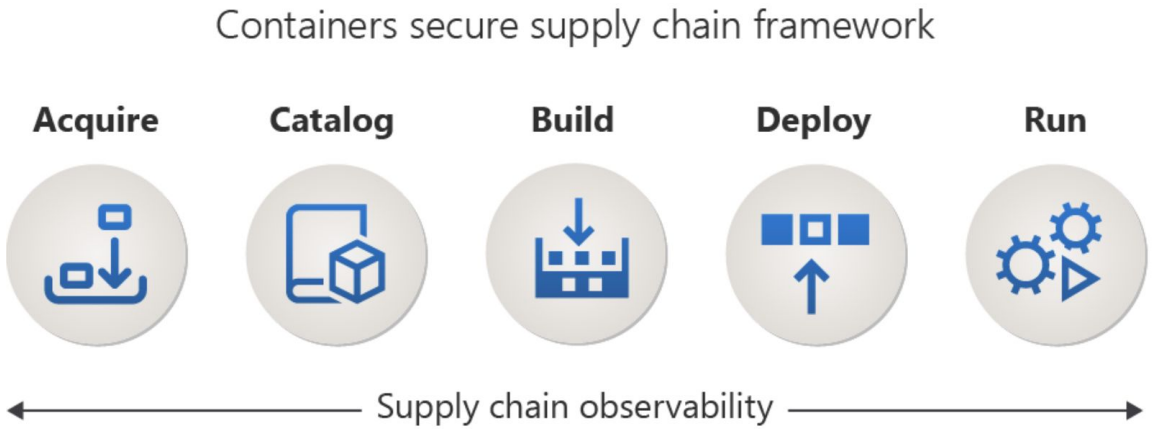
CloudNativeCon

China 2024

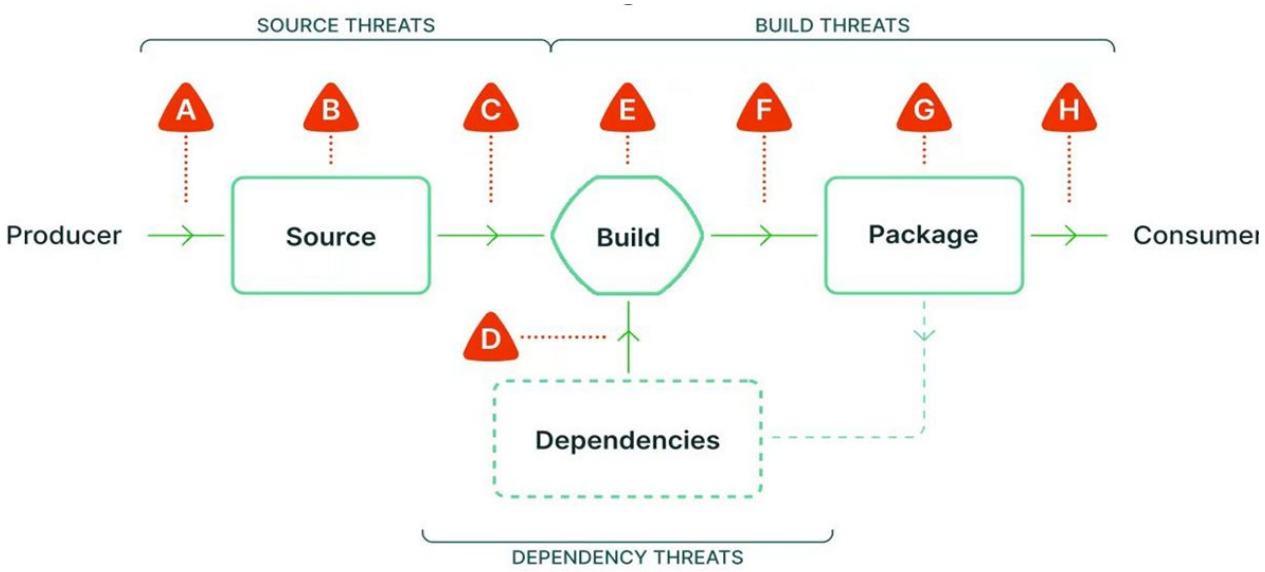
Popular OSS solutions and framework in the industry and CNCF

Popular Supply Chain Security frameworks

Containers Secure Supply Chain (CSSC) Framework



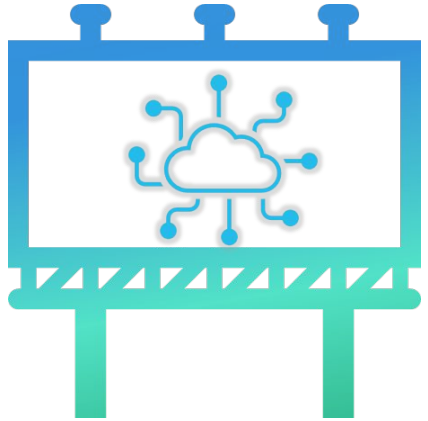
SLSA Framework



Popular OSS projects for securing supply chain

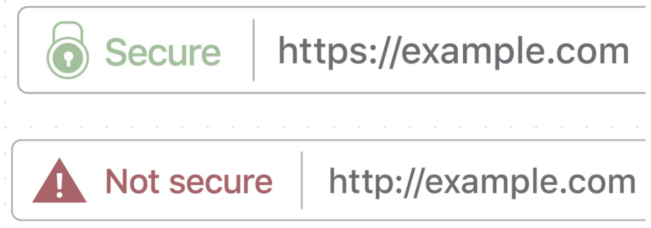
- **Sign and verify OCI Image**
  - Notation (Notary Project)
  - Cosign
- **OCI Artifact distribution**
  - ORAS
  - Regctl
  - Skopeo
  - Crane
- **Generate SBOM**
  - Microsoft sbom-tool
  - Syft / Docker SBOM
  - Xeol
- **Provenance attestation**
  - in-toto attestation

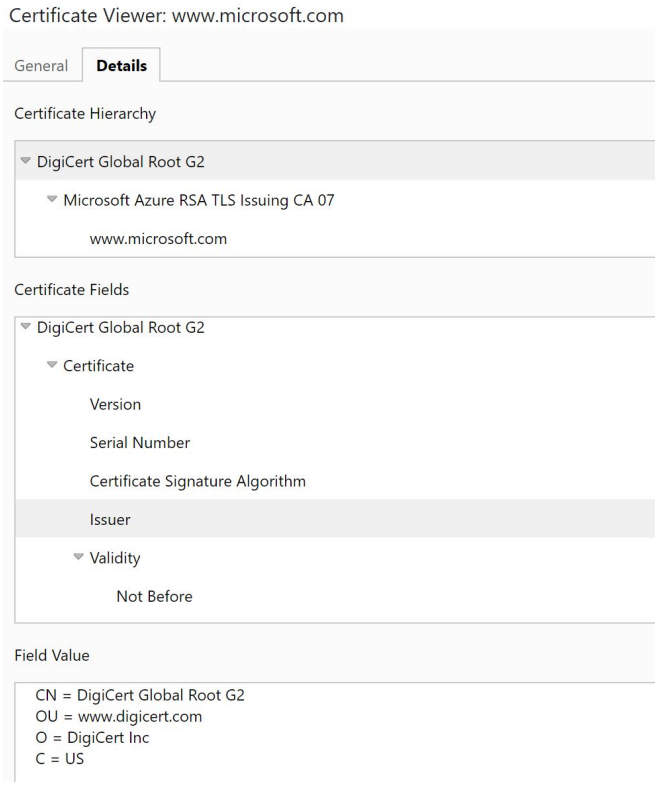
- **Policy Management**
  - Kyverno
  - Open Policy Agent (OPA) gatekeeper
- **Admission controller**
  - Ratify, Connaisseur
- **Runtime security**
  - Falco
- **Vulnerability scanning**
  - Trivy
  - Synk
  - Clair



Improve security posture in the digital world

How SSL Certificate secures the website?





Compare it with today's cloud-native application

- ✅ ghcr.io/kubecon/sample-image:signed
  - ✅ Signature
  - ✅ SBOM
  - ✅ Vulnerability scanning report
  - ✅ Provenance attestation
  - ✅ Image lifecycle metadata

KubeCon

CloudNativeCon

THE LINUX FOUNDATION

OPEN SOURCE SUMMIT

AI_dev

Open Source GenAI & ML Summit

China 2024

How Ratify and Gatekeeper help secure software supply chain

What is Notary Project

Ensure software authenticity and integrity

- Sign software artifacts, verify artifact with fine-grained policy
- Provide CLI, library, standard-based spec
- Built on standard PKI, support two signature envelope formats (JWS and COSE)
- Plugin extensibility for multi-cloud and on-prem: Alibaba Cloud, AWS, Microsoft Azure, Venafi, HashiCorp Vault

Adopters and Contributors

aws Microsoft Alibaba Cloud

VMware Tanzu containerd HARBOR

Venafi Kyverno

Notation CLI Command Sets

```
notation certificate: Manage certificates in trust store
notation key:         Manage keys used for signing
notation list:        List signatures of the signed artifact
notation login:       Log in to the registry
notation logout:      Log out from the registry
notation plugin:      Manage plugins
notation sign:        Sign artifacts
notation verify:      Verify OCI artifacts
notation version:     Show the notation version information
```

What is Ratify

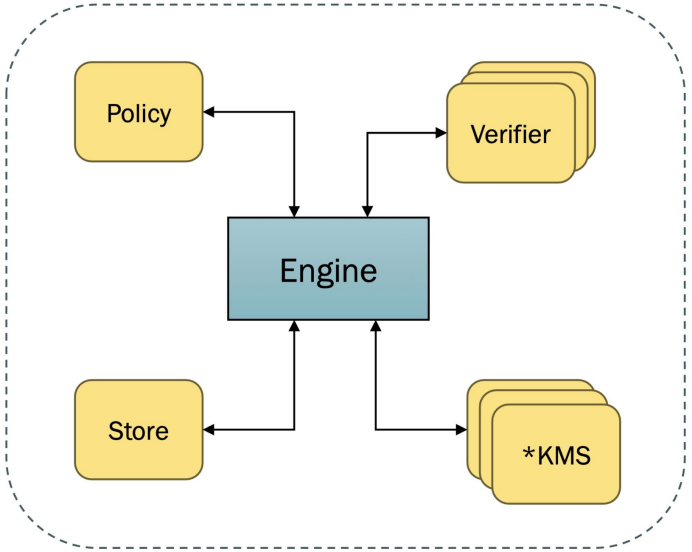
Verification framework for supply chain artifacts

Ratify

- Verify supply chain metadata including signatures (Notary Project, Cosign), vulnerability reports, and SBOMs
- Provide admission control on Kubernetes and a CLI tool for non-K8s scenarios
- Multiple artifact verifiers. Support Bring your own!
- Integration with AWS, Azure, Alibaba Cloud. Support any OCI compliant registries
- Multi-tenancy support

Community ecosystem and support

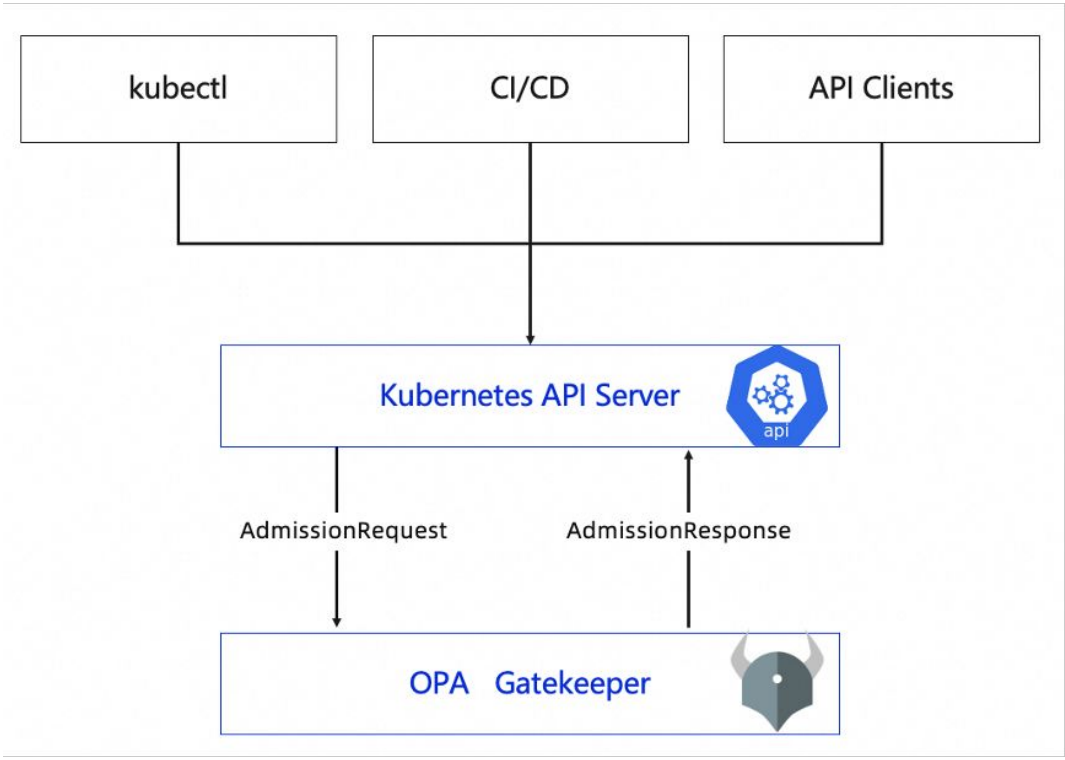
ORAS · Open Policy Agent · aqua trivy · notary project · sigstore cosign · Venafi · aws · Microsoft Azure · Alibaba Cloud



*KMS = Key Management System

What is OPA Gatekeeper

- Policy Enforcement & Real-time control
- CRD: first-class integration between OPA and Kubernetes
- ConstraintTemplate: Add a new policy via a new CR
- Constraints: Instantiations of policy template
- Multiple policy driver: Rego/CEL
- Stand library of policies
- External data and customized providers
- Enforcement and violations audits



From PSP to OPA Gatekeeper

2020

2021

Open Policy Agent

Pro:

- Secure by default

Con:

- too complex and inflexibility
- bug-prone
- hard to extend and maintain
- long-term beta or pending deprecation status

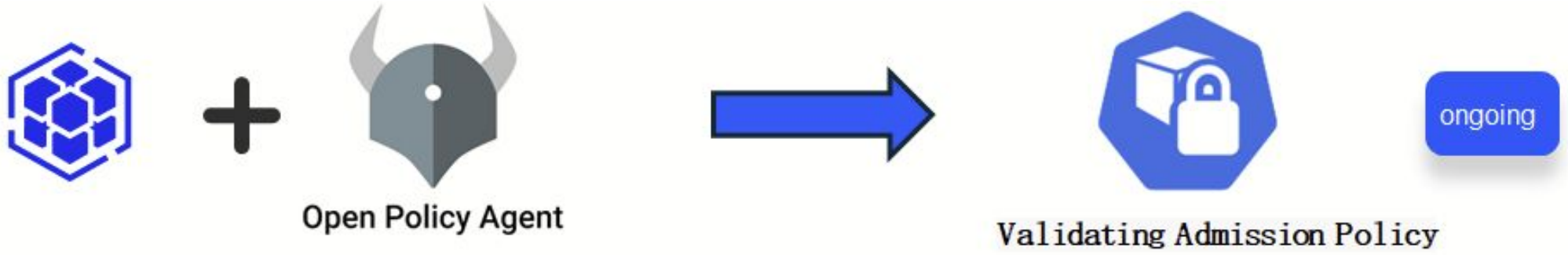
Pro:

- portability and extensibility
- active community and maintainability
- CRD based & mutating support

Con:

- learning cost on Rego
- hard integrate

Deep Integration with OPA Gatekeeper



- Pre-set policies
- Visualized policy governance
- Real-time viewing the enforcement and violation
- Integration with external cloud service

- Flexible
- Native support
- The best performance
- No additional webhook and controller

Performance Comparison

OPA & Gatekeeper

VS

Validating Admission Policy

- 3 master (4u8G) & 3 worker & 3 gatekeeper pods (1u512M limit)
- Max QPS of **880** and policy escape happen

- 3 master (4u8G)) & 3 worker
- Reach the maximum supported **1800**+ QPS of Apiserver without policy escape

Whitelist + static scan, is it enough?

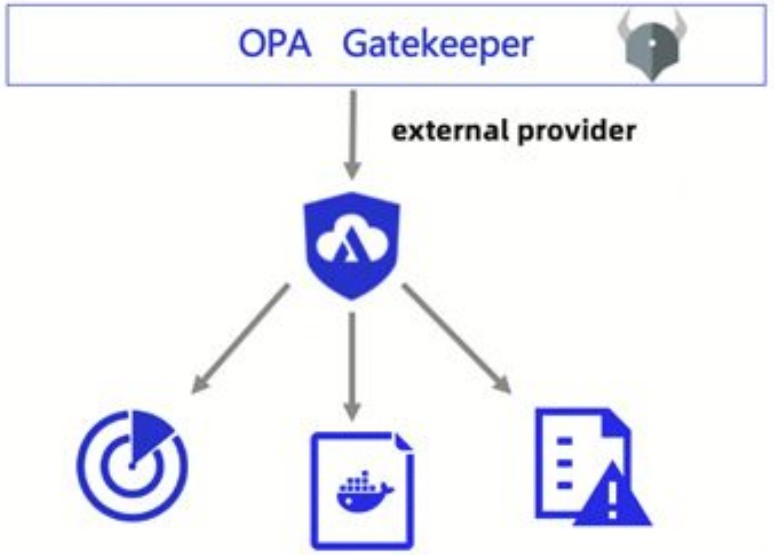
Whitelisted repos

```yaml
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: ACKAllowedRepos
metadata:
  name: allowed-repos
spec:
  match:
    kinds:
      - apiGroups: [""]
        kinds: ["Pod"]
    namespaces:
      - "test-gatekeeper"
  parameters:
    repos:
      - "registry-vpc.cn-hangzhou.aliyuncs.com/acs/"
      - "registry.cn-hangzhou.aliyuncs.com/acs/"
```

Only allow images from whitelisted repositories

+

Detect malicious image + misconfiguration



[redacted] 100K+ violations per day in all ACK clusters

Proactive defense based on security scan results from external service

KubeCon

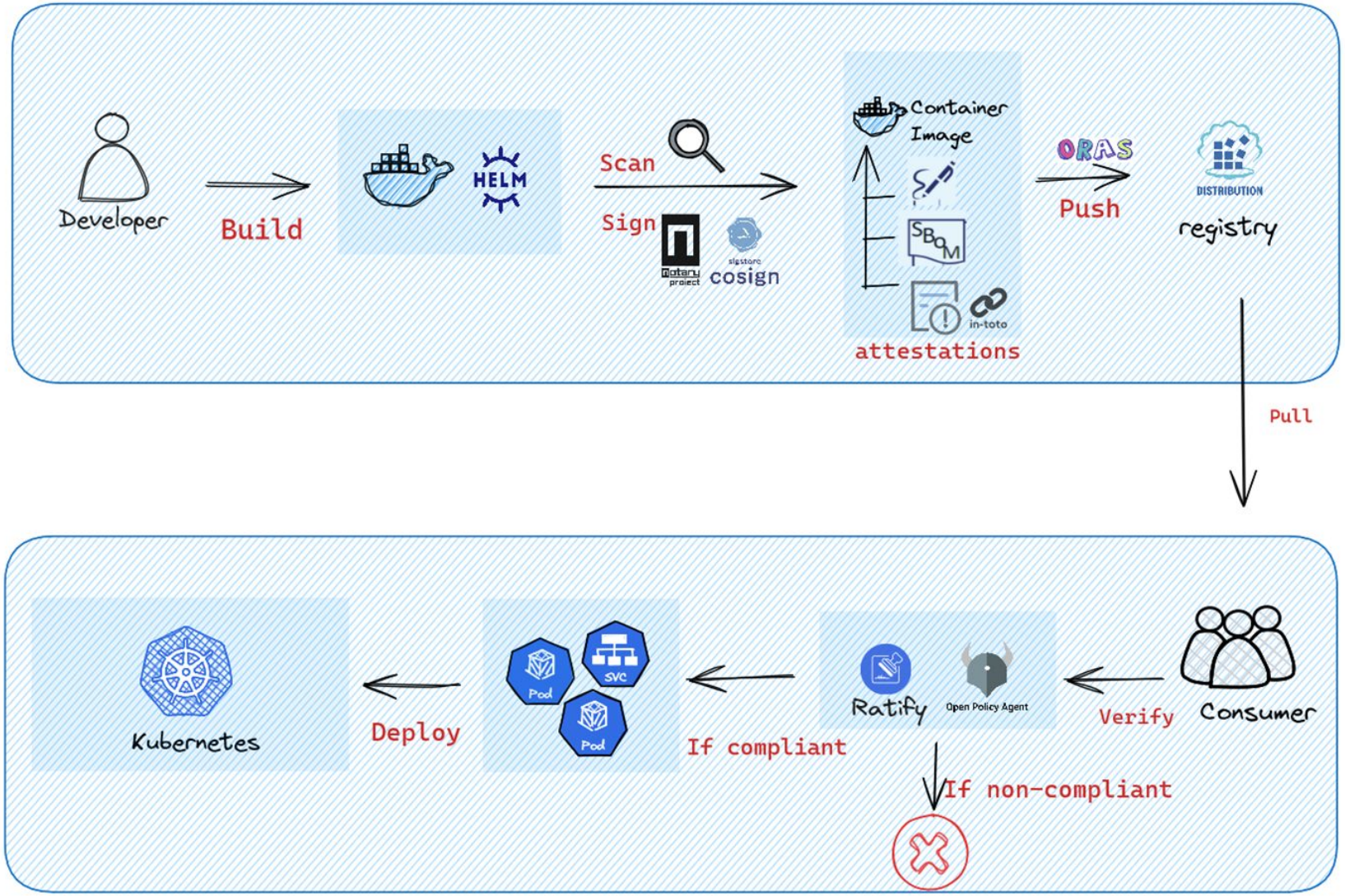
CloudNativeCon

THE LINUX FOUNDATION

China 2024

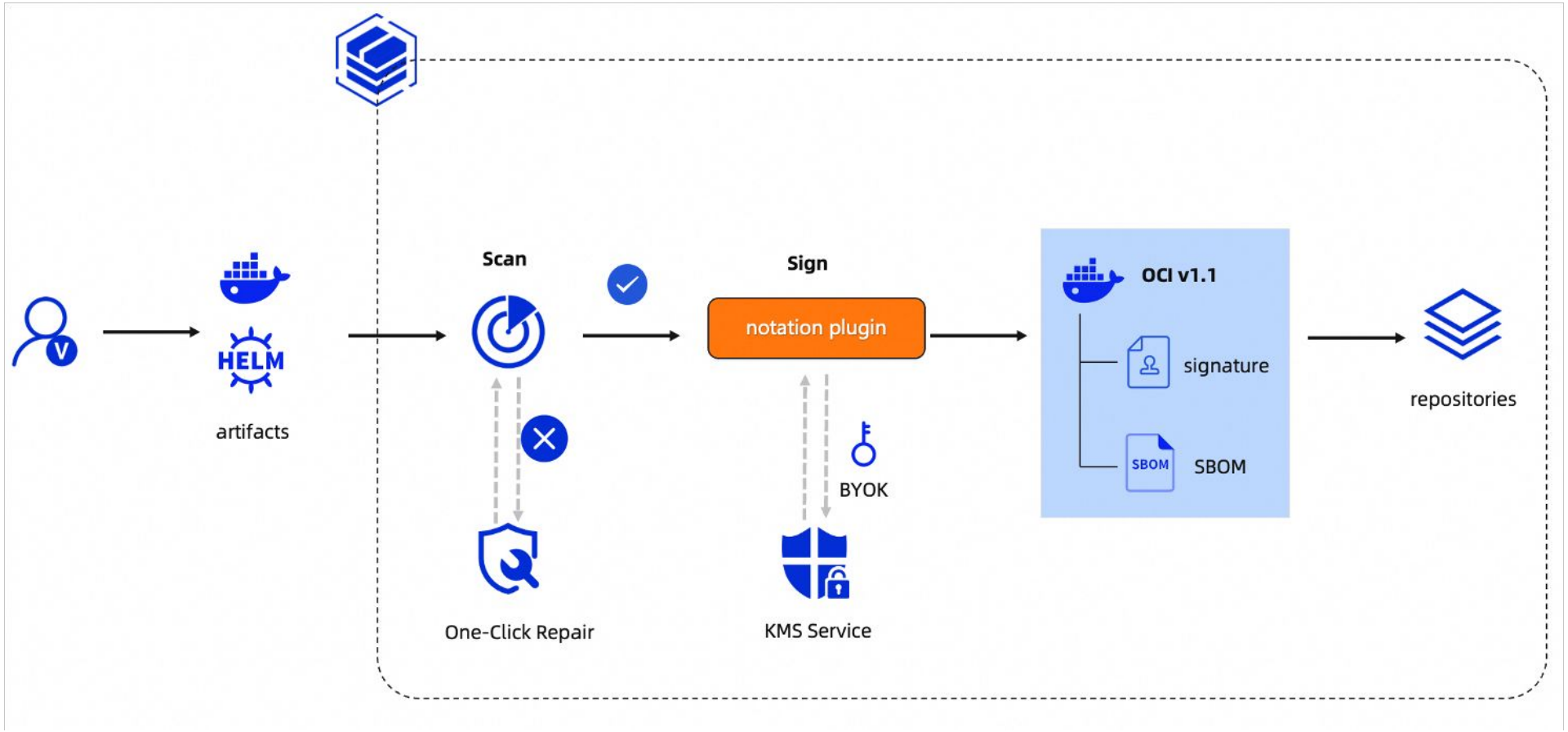
End-to-end demo: Signing and verify images on Kubernetes

Secure Supply Chain with Ratify and OPA Gatekeeper

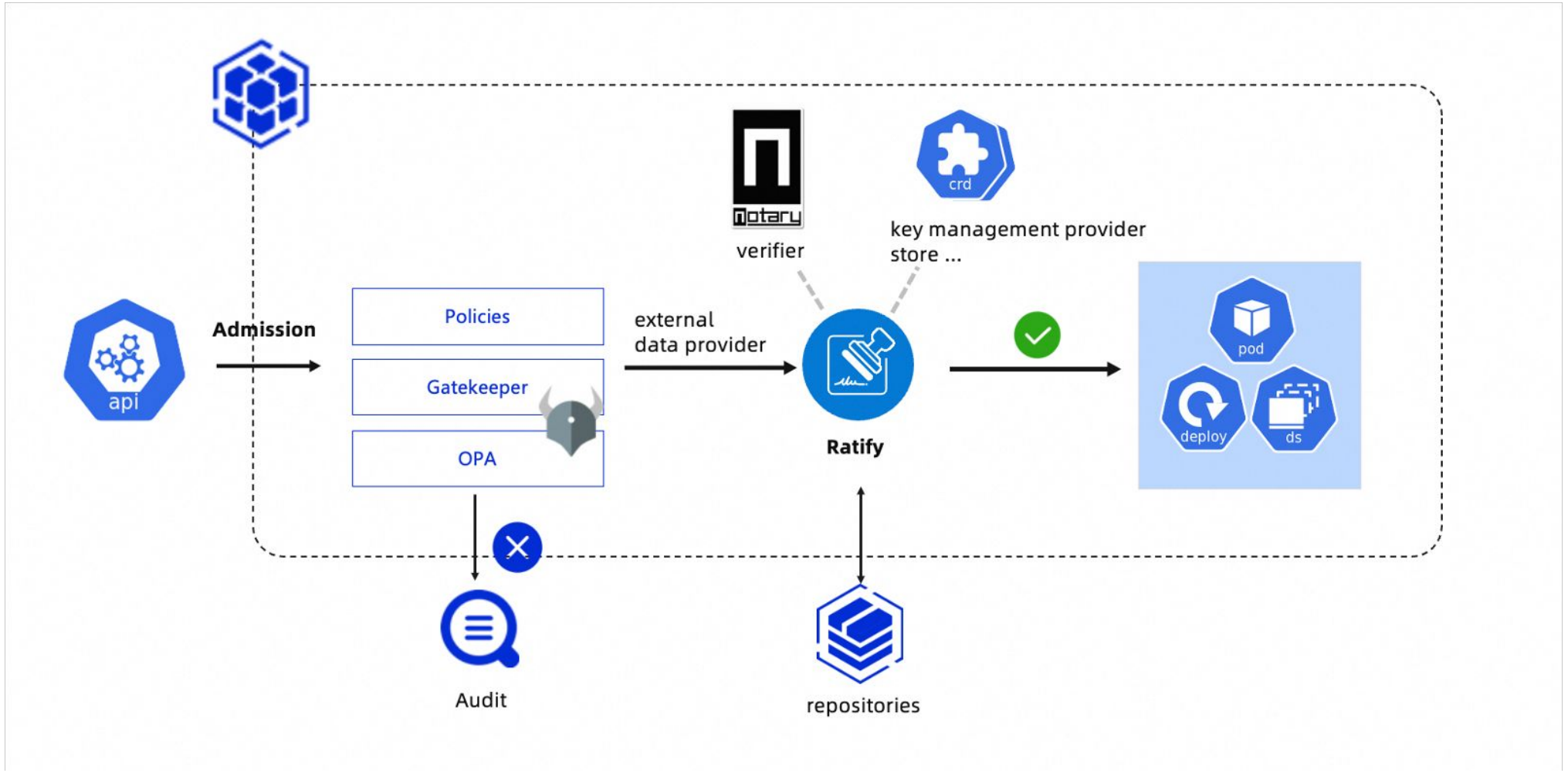


Secure Supply Chain with signing

Sign OCI image/artifact with Notation plugin



Verify signature in Kubernetes using Ratify



Verify signature in Kubernetes using Ratify

Demo

Verify SBOM and vulnerability report in Kubernetes using Ratify

Demo and doc:

- Vulnerability Report | Ratify
- SBOM Validation | Ratify

Check out: https://ratify.dev/

Wrap up & Questions

- Concepts and Challenges of Software Supply Chain Security
- Popular OSS solutions and framework in the industry and CNCF
- How Ratify and Gatekeeper help secure software supply chain
- End-to-end demo: Signing and verify images on Kubernetes

Useful links:

- Notary Project: https://notaryproject.dev
- Ratify: https://ratify.dev
- OPA Gatekeeper: https://open-policy-agent.github.io/gatekeeper/