Discover Kyverno !

The Kubernetes Native Policy Engine

Christian Dussol

Introduction

Looking to secure and standardize your **Kubernetes** deployments without complexity?

Discover **Kyverno**, the **Kubernetes-native policy** engine that transforms your **governance**.

The Problem

The Kubernetes Governance Challenge

- Misconfigurations → leading cause of K8s security incidents
- Documentation and manual checks difficult to maintain
- Complex compliance controls to implement
- Inconsistent adoption of best practices across teams

What is Kyverno?

Kyverno in a Nutshell

- ✅ **Kubernetes-native policy engine** (no proprietary language)
- ✅ No agent to install (works with the **admission controller**)
- ✅ Defines policies in **YAML** (like your other K8s resources) with **Policy-as-Code**
- ✅ Seamlessly integrates with your **GitOps** pipelines

The 3 powers of Kyverno

3 ways to apply your policies

- **Validation**: Block non-compliant resources
- **Mutation**: Automatically modify to ensure compliance
- **Generation**: Create necessary complementary resources

Use case : DevOps

Automate your best practices

🚀 Require standardized labels and annotations

🚀 Enforce naming conventions

🚀 Ensure readiness/liveness probes are present

🚀 Apply default security configurations

🚀 Validate multi-tenant configurations

Use case : security

Strengthen your Security

- 🛡️ Block privileged containers
- 🛡️ Enforce resource limits on all workloads
- 🛡️ Verify image provenance and compliance
- 🛡️ Automatically generate NetworkPolicies
- 🛡️ Apply CIS Benchmarks

USE CASE : FINANCIAL SERVICES

Kyverno for Financial Services

Kyverno addresses critical regulatory and security needs in financial institutions:

🏛️ **Regulatory Compliance**:

- Enforce PCI-DSS requirements for data segregation
- Validate GDPR-compliant configurations
- Implement controls for SOX and Basel requirements

🔐 **Risk Management**:

- Prevent deployment of vulnerable components
- Ensure proper data encryption in transit and at rest
- Validate geographic boundaries for data sovereignty

USE CASE : FINANCIAL SERVICES

Kyverno for Financial Services

📊 Audit & Governance:

- Automatically generate compliance reports
- Provide evidence for regulatory examinations
- Create audit trails of configuration changes

💼 Multi-tenant Isolation:

- Critical for financial platforms serving multiple clients
- Enforce strict namespace boundaries
- Prevent cross-contamination of customer data

Behind the Scenes: Admission Controller & CRDs

🔄 **Admission Controller**: Intercepts all API requests to the K8s cluster before they are executed

🧩 **Custom Resource Definitions (CRDs)**:

- **Policy**: Namespace-scoped rules
- **ClusterPolicy**: Cluster-wide rules
- **PolicyReport**: Compliance status tracking

Protection at every level

Kyverno and the 4C Cloud Native Security

Kyverno acts at multiple levels of the **4C security model**:

- **Cluster**: Primary operational level (admission controller)
- **Container**: Strong influence on security parameters
- Indirect influence on **Cloud** and **Code** layers

Getting Started

How to start with Kyverno

1. Try the **Kyverno Playground** first: playground.kyverno.io

- Interactive web UI to test policies without installation
- Pre-built examples for common use cases
- Visualize exactly how policies work

2. **Simple installation:**

```
helm repo add kyverno https://kyverno.github.io/kyverno/
helm repo update
helm install kyverno kyverno/kyverno
```

3. Start in “**audit mode**” (monitor without blocking)

4. **Gradually** implement security policies and **integrate into CI/CD**

MONITORING & REPORTING

Observability into Policy Compliance

Kyverno offers comprehensive monitoring capabilities for **governance observability** :

📊 **Native PolicyReports**:

- Built-in Custom Resources track policy results
- Detailed history of compliance evaluations
- Namespace and cluster-level reporting

🔍 **Kyverno Monitor**:

- Official web UI for visualizing policy results
- Filter violations by namespace, resource or policy
- Export compliance reports for audits

📈 **Observability Integrations**:

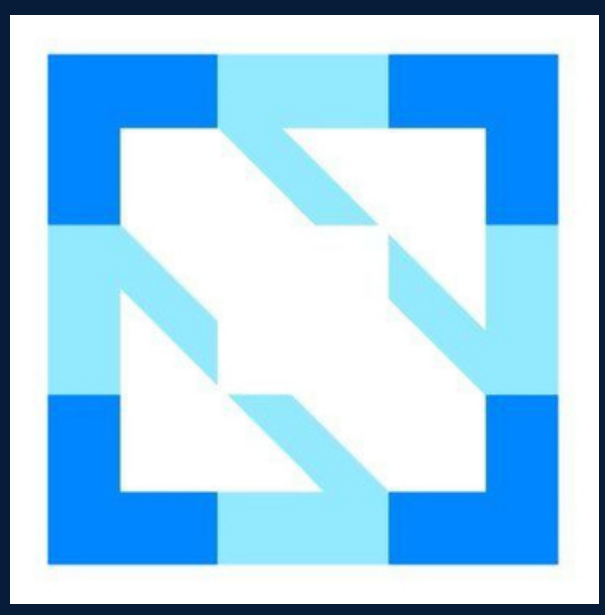
- Prometheus metrics for real-time monitoring
- Grafana dashboards for compliance trends
- Alerting for policy violations
- Works with OpenTelemetry for unified observability

Perfect for **demonstrating** regulatory compliance in **financial environments**.

CNCF

CNCF Support and Governance

- **CNCF Project**: Kyverno reached **incubating** status in the **Cloud Native Computing Foundation**
- **Industry Trust**: supported by the same foundation behind Kubernetes and Prometheus
- **Security Focus**: Regular security audits and community-driven improvements
- **Vibrant Ecosystem**: Active community with contributions from major enterprises
- **Long-term Sustainability**: Vendor-neutral governance ensures focus on solving real problems



Conclusion

Why Adopt Kyverno ?

- Rapidly growing adoption in the cloud-native ecosystem
- Project supported by the CNCF
- Facilitates regulatory compliance critical for financial institutions
- Reduces risks without slowing innovation
- Transforms governance from a constraint into an advantage