Styra DAS: Enterprise-Grade Kubernetes Admission Control

Kubernetes is Now Business Critical Infrastructure

Kubernetes has evolved from experimentation to production. Now, platform teams are responsible for deploying and securing Kubernetes across AWS, Azure, GCP and self-hosted environments — supporting hundreds to thousands of developers. With Kubernetes being mission-critical for enterprise applications, cloud infrastructure teams need a way to secure these complex deployments using policy-as-code guardrails at scale.

Kubernetes Requires Security Automation

As platform teams configure infrastructure for hundreds or thousands of developers, they must ensure security and compliance through automation at scale. Kubernetes admission control provides the means to enforce policy guardrails on clusters before runtime — ensuring that security and compliance best practices are applied by default, and that accidental missteps and misconfigurations are avoided.

Policy as Code Provides Security by Default

Using Open Policy Agent (OPA), created and maintained by Styra, platform teams can provide desired-state security using policy as code at admission control, via the Kubernetes API server. Styra Declarative Authorization Service (DAS) delivers the mature enterprise functionality that teams need to manage policy as code in large, complex Kubernetes deployments while avoiding the significant DIY engineering investments of open source.

Styra empowers cloud infrastructure teams to:

- Automatically enforce security, compliance and operational best practices.
- Systematically reduce Kubernetes production risk.
- Deliver efficiency gains by eliminating manual efforts and deploying infrastructure faster.

With the broadest policy library and authorization toolset on Kubernetes, Styra DAS allows cloud infrastructure teams to eliminate manual policy creation, validate policy changes before impact, monitor all non-compliant resources, easily audit decisions and instantly enforce best practices with pre-built Compliance Packs for NIST SP 800-190 Application Container Security, Pod Security and more.

OPA has become the de facto standard for Kubernetes admission control, while Styra DAS is the leading way implement OPA and policy as code at scale.

Mitigate risk. Minimize human error. Accelerate delivery.

Styra's Declarative Authorization Service was purpose-built for the challenges of Kubernetes and the cloud-native stack. Built on Open Policy Agent, Styra DAS provides compliance guardrails delivered as policy-as-code, and implemented directly via Kubernetes APIs.

The Benefits of Benefits: Styra DAS for Kubernetes Deployments

Systematically reduce production risk across complex Kubernetes deployments.	**Built-in Security Best Practices** With a validated policy library and pre-built Compliance Packs for NIST SP 800-190 Application Container Security, PCI DSS, MITRE ATT&CK, CIS Benchmarks, and Pod Security Compliance, platform teams can instantly enforce security, compliance, and operational best practices on production clusters.
Establish a mature policy-as-code strategy with a single OPA control plane.	**Enterprise-Grade Deployment** Easily manage policy as code across tens, hundreds or thousands of clusters. A fully mature enterprise feature set — including multi-cloud support, impact analysis, auditing, compliance view for all K8s resources, shift-left for CI/CD and much more — allows you to instantly deploy on Day 0, while avoiding the extensive DIY engineering investments required for pure open source.
Shift left to stop errors, and eliminate rogue deployments.	**Shift Security Left** Security policy works best when it eliminates risk early. Unlike runtime security solutions, Styra works with the declarative nature of Kubernetes to define and enforce desired state. Prevent issues before they begin, with declarative authorization.
Support fine-grained access control (FGAC) with external data.	**Customizable, Context-aware Policies** Support data-driven policy decisions with OPA. Teams can leverage lists of approved users or groups who can deploy applications to namespaces to limit access, or limit production changes to on-call administrators in PagerDuty.
Deploy trusted technology, proven at scale.	**Trusted in the Largest Kubernetes Deployments** Styra is built on OPA — the de facto general-purpose policy engine for cloud-native authorization, created and maintained by Styra. Moreover, Styra DAS is trusted to manage OPA in some of the largest Kubernetes production deployments on the planet, by Fortune 500 enterprises in highly regulated environments, across industry verticals.

About Styra

We are reinventing policy and authorization for cloud-native. Today's cloud app infrastructure has evolved. Access, security, and compliance must also evolve. It's time for a new paradigm. It's time for authorization-as-code.

Learn more at www.styra.com

styra

 styra_ds_styra-das-enterprise-grade-kubernetes-admission-control_011723