Declarative Authorization
For Kubernetes Guardrails

Kubernetes is Now Business Critical Infrastructure

Kubernetes has evolved from experimentation to production. Now, enterprises must secure these new environments just as they've done for traditional infrastructure. However, the dynamism and scale of the new cloud-native stack adds an exponential level of security complexity.

Dynamic Environments Require Dynamic Security

In a containerized environment, changes are constant, and runtime is too dynamic for traditional security measures. Kubernetes provides the orchestration to ensure that runtime is always being brought back to desired-state—but that desired state must be well defined, with clear security guardrails to prevent drift, risk, and accidental missteps.

Security Must Move to A Declarative Model

Styra's Declarative Authorization Service works with Kubernetes APIs to provide desired-state security. Styra lets you implement policy before runtime, allowing teams to define, enforce, and validate security with no black-boxes, additional servers, or complex configuration.

Styra lets you easily create policies such as:

- *Prevent one network ingress from stealing traffic from another*
- *Only allow images from trusted repositories*
- *Business critical storage volumes must use the 'retain' storage policy*

Styra's simple graphical library of customizable policies—all based on business context—allows Security and DevOps teams to mitigate risks, reduce human error, and accelerate development across their clusters.

Built on the open-source Open Policy Agent, and declarative by design, Styra is the fastest and easiest way to put guardrails around Kubernetes—whether you're a developer, an admin, or a bit of both.

styra

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.

styra

The Benefits of Declarative Authorization for Kubernetes Security

Simple
Built-in libraries and simple GUI let teams build policy-as-code—without the code

Safe
Validate policy before enforcement to eliminate unintended consequences

Proactive
Declarative model defines desired state to prevent drift before it can occur

Flexible
Incorporates dynamic business context, not just simple scans or static policy

Trusted
Built by the originators of the Open Policy Agent project, hosted by the CNCF

Built-in security best practices
The future of security is policy-as-code. But not every security team is made up of coders. That's why Styra provides a rich policy editor, with the choice of a simple graphical interface, or a command line interface. **Eliminate Day 1 hassle as well as ongoing maintenance overhead.**

Verify before enforcement
Styra allows you to pre-run policies to see their impact before deployment. Compare changes against historical data, to see what would have been different if the updates had been made. Put rules into monitor-only mode to see where violations occur. **Gain insight and deploy more confidently, with less risk.**

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. **Shift left to stop errors, and eliminate rogue deployments.**

Customizable, context-aware policies
Hard-coded rules can't handle context changes as requirements evolve, and lead to constant rework. Styra lets you customize existing policies, or create your own. Incorporate context like dynamic roles, user load, payload safety, and more to meet business requirements, and end brittleness. **Future-proof your policy.**

Trusted in the largest Kubernetes deployments
Styra is built on the Open Policy Agent—a popular and widely deployed open source project founded by the same team that built Styra. With primary credibility for for the underlying technology, the Styra team and technology are both proven in production across verticals. **Get best of breed technology, proven at scale.**

Styra enables enterprises to define, enforce and monitor policy across their cloud-native environments. With a combination of open source (Open Policy Agent) and commercial solutions (Declarative Authorization Service), Styra provides security, operations and compliance guardrails to protect applications, as well as the infrastructure they run on.

Styra policy-as-code solutions lets developers, DevOps and security teams mitigate risks, reduce human error and accelerate application development.

For more information visit styra.com, or follow @StyraInc on Twitter

styra

1800 Broadway, Suite 1
Redwood City, CA 94063

www.styra.com