Styra Declarative Authorization Service & Kong Mesh

Governance, Authorization, and Traffic Control for Cloud Security and Platform Teams

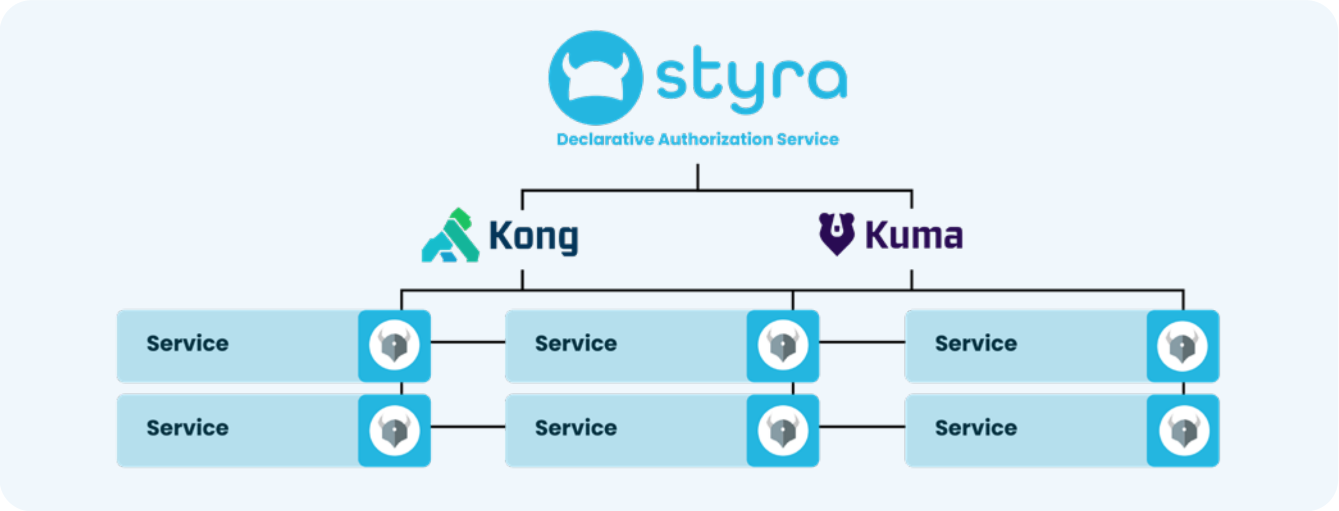
Organizations today are faced with monumental battles when it comes to their digital transformation journey. One of those battles is the transition to distributed software architectures in support of accelerated innovation and a hopeful reduction in costs. A successful transition to microservices requires many pieces to fall into place: that services are connected reliably with minimal latency, that they are discoverable and fully observable, and that policy-as-code is properly implemented to ensure that they are properly secured. However, most organizations face deadlines that make a successful transition darn near impossible to have standardized and consistent policies across applications, implement consistent rules at appropriate enforcement points, and migrate applications seamlessly.

Joint Solution Benefits

Together, Styra Declarative Authorization Service (DAS) and Kong Mesh address policy lifecycle management, enterprise governance, security, and traffic control to enable IT, Security, and GRC teams. With these solutions, organizations can:

- Reduce operational overhead with automated policy-as-code based control of multiple service meshes with enterprise-grade management planes
- Govern, monitor and audit traffic flow and decisions for real-time verification of performance and risk
- Increase application reliability with policy-based traffic management
- Collaborate across organizational siloed and disparate platforms and clouds to accelerate deployments
- Rapidly implement leading open-source solutions at global scale

Kong Mesh builds Open Policy Agent (OPA) into its version of the Envoy proxy, so users don't have to deploy multiple agents within the IT infrastructure to use OPA Styra's Declarative Authorization Service (DAS) acts as a central management point for IT security policy distribution using these OPA/Envoy bundles for unified policy authoring.



Kong Mesh:

Global observability across all traffic, including cross-cluster deployments.

Start, secure, and scale with ease:

- Deploy a turnkey service mesh with a single command.
- Group services by attributes to efficiently apply policies.
- Manage multiple service meshes as tenants of a single control plane to provide scale and reduce operational costs.

Run anywhere:

- Deploy the service mesh across any environment, including multi-cluster, multi-cloud, and multi-platform.
- Manage service meshes natively in Kubernetes using CRDs, or start with a service mesh in a VM environment and migrate to Kubernetes at your own pace.

Connect services end-to-end:

- Deploy the • Integrate into the Kong Gateway (Enterprise) platform for full stack connectivity, including Ingress and Egress traffic for your service mesh.
- Expose mesh services for internal or external consumption and manage the full lifecycle of APIs.

Styra DAS:

Global observability across all traffic, including cross-cluster deployments.

Enterprise grade policy development lifecycle, including policy:

- Authoring
- Impact Analysis
- Distribution
- Monitoring
- Audit

Use a single language (Rego) for expressing policy and a single software system for:

- Managing policies across a broad spectrum of software systems, like Kubernetes, microservices, public cloud, Linux, and databases.

Evaluate real-time context against custom authorization policy to:

- Tightly control microservice interaction, minimizing risk and maximizing performance.
- Eliminate the need to build logic into services directly, or maintain multiple policy silos.
- Protect against lateral movement attacks and hot patch policies to isolate unusual activity.

Built by the founders of Open Policy Agent to provide a unified policy-development lifecycle for any OPA use case, while also providing an elegant experience for the most popular use cases.

Joint Solution Benefits

Styra DAS for OPA Application Authorization with Kong Gateway and Kong Mesh

A large national telecommunications company with more than 65,000 employees, $15B in revenue, six divisions, and three subsidiaries needed to enforce authorization policy throughout their application stack to meet both internal goals and external regulations. They needed to tightly control north-south traffic to prevent unauthorized access and limit the risk of data exfiltration, in addition they needed to control east-west traffic between app services to achieve two goals:

- Limit the risk of lateral movement as per data security best practices.
- Ensure that application components worked together appropriately, with access only granted based on business context to ensure end users had the correct experience based on their level of privilege (access/role/etc.).

Using Styra DAS, they were able to externalize authorization with automated policy-as-code based control that enables them to separate their application access logic from the app code itself, so as secure and access needs change, app teams don't have to get involved. In addition, they have been able to govern, monitor and audit traffic flow and decisions across all their traffic control points — including NS and EW — all from a single management plane empowering disparate development and ensuring that all policy instances are working as intended, and can be updated from a central control point.

With Styra DAS and Kong Mesh, security and operations teams get granular control over traffic flow, as well as global, real-time monitoring and historical audit records of both the traffic flow and policy decisions that were made to protect data and meet internal and external regulations.

Solutions Used:

- Kong Gateway
- Kong Mesh/Kuma
- Styra DAS
- OPA

Environment Details:

- NodeJS Apps
- AWS and GCP
- Kubernetes on GKE and EKS

Kong provides a next-generation service connectivity platform to intelligently broker information across modern architectures. The world's largest companies, financial institutions, and government agencies use Kong to orchestrate, secure, manage, and monitor their services infrastructure.

For more information visit konghq.com, or follow @thekonginc on Twitter

Styra, the founders of Open Policy Agent (OPA), provides open source and commercial solutions that enable enterprises to define, enforce and monitor authorization policy across their cloud-native applications, as well as the infrastructure they run on. Styra policy-as-code solutions let 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

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