

# Styra DAS for Service Mesh

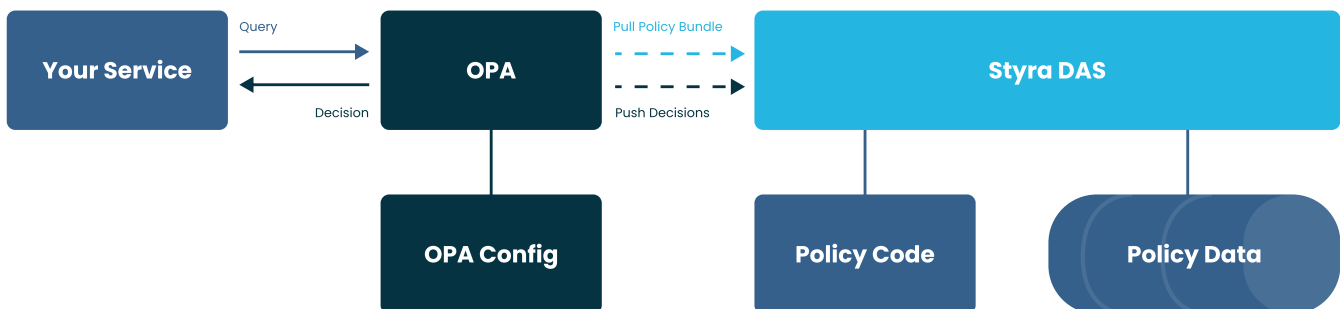
## Secure Modern Cloud-Native Applications with Dynamic, Policy-Enabled Traffic Control

Organizations today are shifting away from the monolithic application to a microservices-based approach because it makes applications more cost-effective and easier to update, scale and support. While there are significant benefits to a microservices-based approach, there are challenges to deploying and managing these services, which has led to the creation of service mesh. Developers and site reliability engineers benefit from the implementation of service mesh because it helps with observability, security, and traffic management. In the most recent CNCF Survey, 27% of respondents use service mesh in production which is a 50% increase from the previous year. Additionally, 19% of respondents are planning to implement a mesh in production within 12 months and 23% more evaluating, making service mesh a necessary element of a cloud-native approach. While we see this massive shift to implement service mesh, the issue of authorization still remains.

Introducing Open Policy Agent (OPA), an open source, general-purpose policy engine that unifies policy enforcement across the stack. OPA provides a high-level declarative language that implements policy-as-code and simple APIs to offload policy decision-making from software. The largest organizations leverage OPA to enforce policies in microservices, Kubernetes, CI/CD pipelines, API gateways, and more.

For organizations looking for a turnkey OPA control plane to manage policies across a broad spectrum of systems, like Kubernetes, microservices, public cloud, and more, Styra Declarative Authorization Service (DAS) is the solution. With Styra DAS organizations can finally decouple policy from the code base or software and unify enforcement of policy across the stack. With native support of Kong Mesh, Istio, Kuma, and Envoy, organizations have access to a single pane of glass for all microservice authorization with the ability to:

- Secure modern cloud-native applications with dynamic, policy-enabled traffic control.
- Automate policy-as-code based control for services.
- Govern, monitor, and audit traffic flow and decisions for real-time verification.
- Increase application reliability with policy-based traffic management.





Styra DAS native support of Kong Mesh, Kuma, Istio, and Envoy enables organizations manage the ingress and egress network traffic permitted within OPAs integrated service mesh. For example, permit egress traffic only to a predefined collection of endpoints, to minimize the risk of data exfiltration, and implement microservice API authorization.

### Kong Mesh

Kong Mesh is an enterprise-grade service mesh that runs on both Kubernetes and VMs on any cloud. This service mesh is built on top of CNCF's Kuma and Envoy with enterprise features and support. Additionally, Kong Mesh built 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 DAS then acts as a central management point for IT security policy distribution using these OPA or Envoy bundles for unified policy authoring. In addition to the native OPA support in Kong Mesh, there is also native support within Kong Gateway.

### Kuma

Kuma is a platform agnostic open-source control plane for service mesh and microservices management, with support for Kubernetes, VMs, or even bare metal environments. Much like most service meshes, Kuma is Envoy-based and is powered by Envoy sidecar proxies.

### Istio

Istio is an open-source service mesh that can be used to manage a distributed microservice architecture. It leverages Envoy proxies as sidecars injected into every pod to regulate the network traffic on all pod instances. Then, OPA can act as a policy enforcement engine on the traffic passing through an Envoy sidecar.

### Envoy

Envoy is a high performance distributed proxy designed for single services and applications, as well as a universal data plane for large microservice architectures, running parallel to every application. When all service traffic in an infrastructure flows through Envoy mesh, it becomes easy to visualize problem areas using consistent observability, tune overall performance, and add substrate features in a single place.

With service mesh and Styra DAS organizations can address policy lifecycle management, enterprise governance, security, and traffic control to enable IT, Security, and GRC teams.

**Give it a try today with [Styra DAS Free!](#)**

## 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](http://www.styra.com)

