

Sidecar-less Service mesh, Is it a dream or a reality?



Rohit Ghumare

Independent Developer Advocate

\$ whoami

Cloud native
TALKS



devopsguys.in

Rohit Ghumare

I am Developer Advocate, GDE for
Google Cloud

Founder of communities:

- Keep Up  **KEEP UP**
- DevOps Community  **DevOps Community**
- Developer Relations Community



Connect with me:

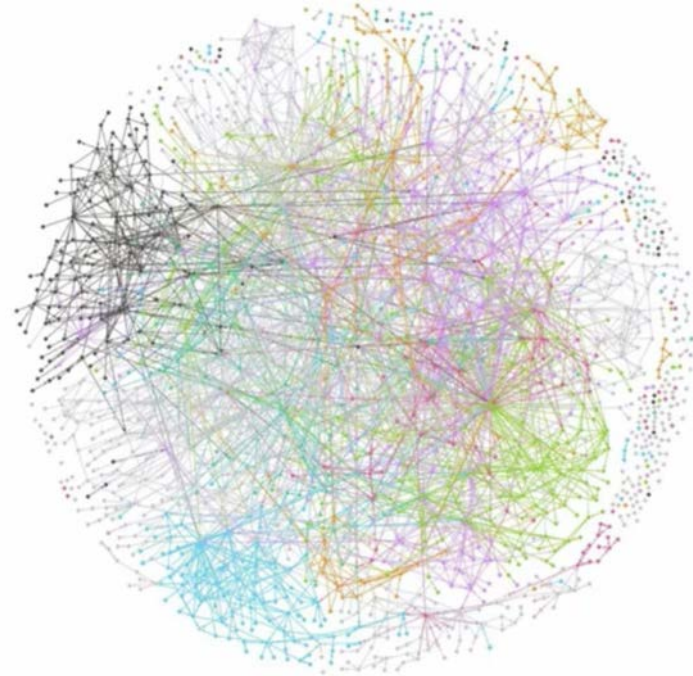
Twitter/YouTube: [@ghumare64](#)

LinkedIn: [/in/rohit-ghumare](#)

Portfolio: [devopsguys.in](#)

Challenges with Microservices

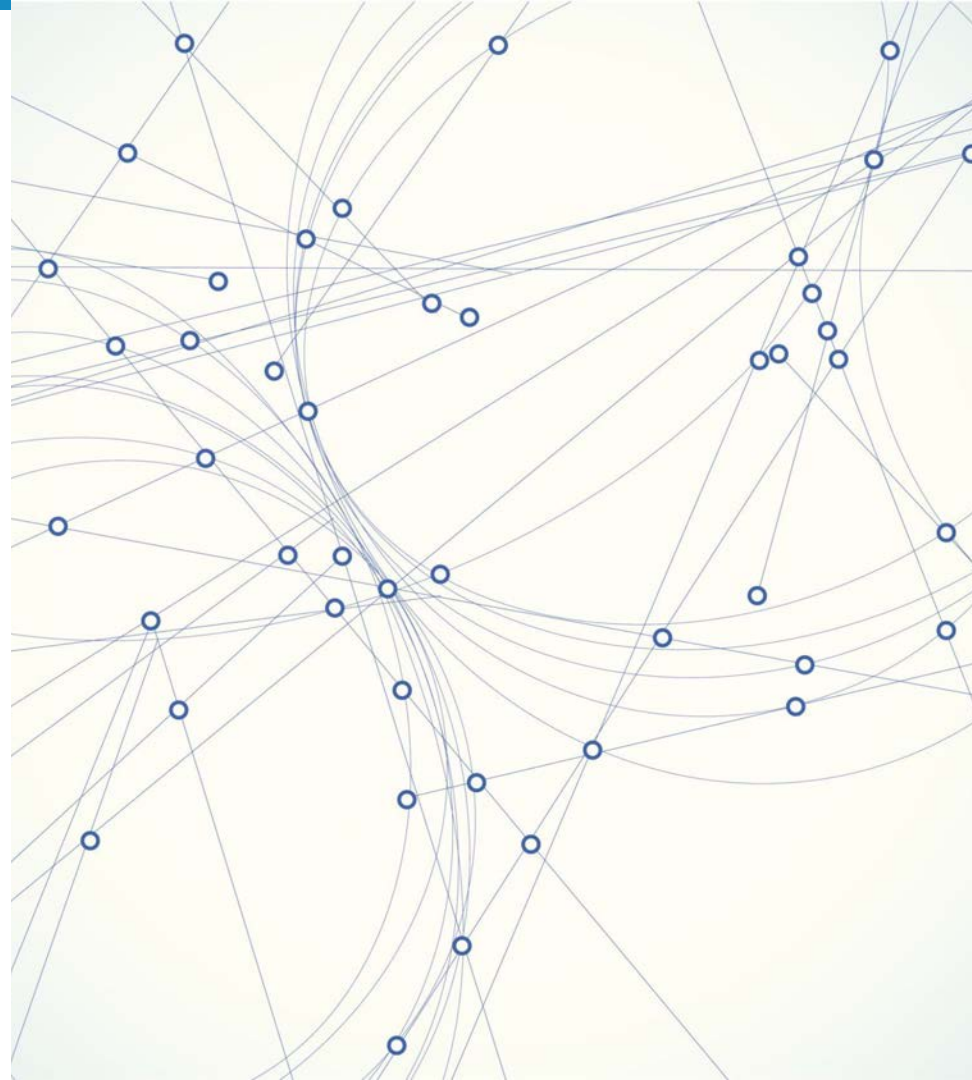
- How to observe interactions among services?
- How to secure service communication?
- How to manage timeouts and communication failures?
- How to control traffic?



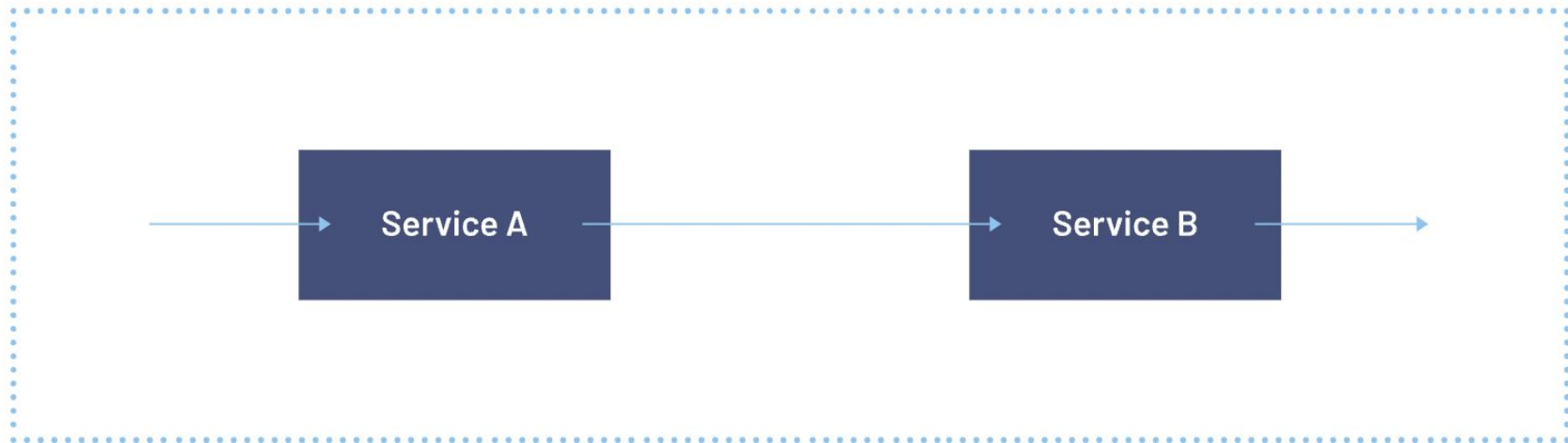
Miles Bryant (@milesbxf) and Suhail Patel (@suhailpatel)

What is a service mesh?

A service mesh is a **programmable** framework that allows you to **observe**, **secure**, and **connect** microservices.



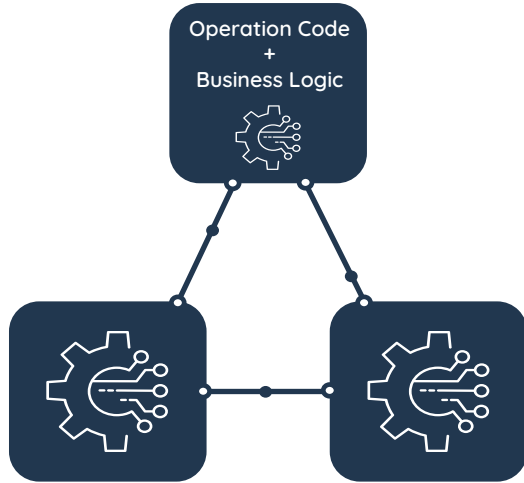
Before Service Mesh



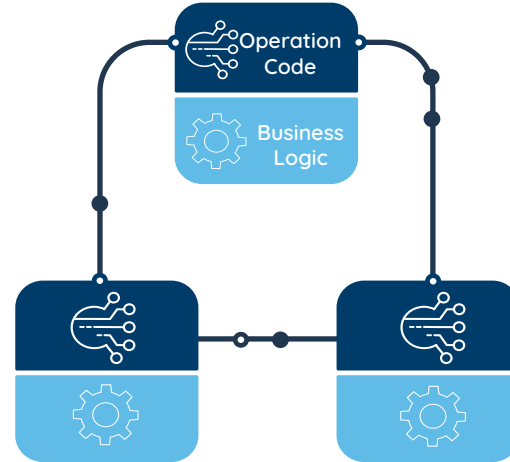
Before utilizing Istio

Service Mesh

Before Service Mesh



After Service Mesh



Service Mesh Functions



Service discovery / Load balancing



Secure service-to-service communication



Traffic control / shaping / shifting



Policy / Intention based access control



Traffic metric collection



Service resilience



API / programmable interface

Platform Goals with Service Mesh (Istio)



Application-Level Routing

- Offload application-level traffic routing
- Offload application-level filtering | transformations

Observability

- Anchor point for traffic capture
- Anchor point for logging
- Anchor point for observability integration

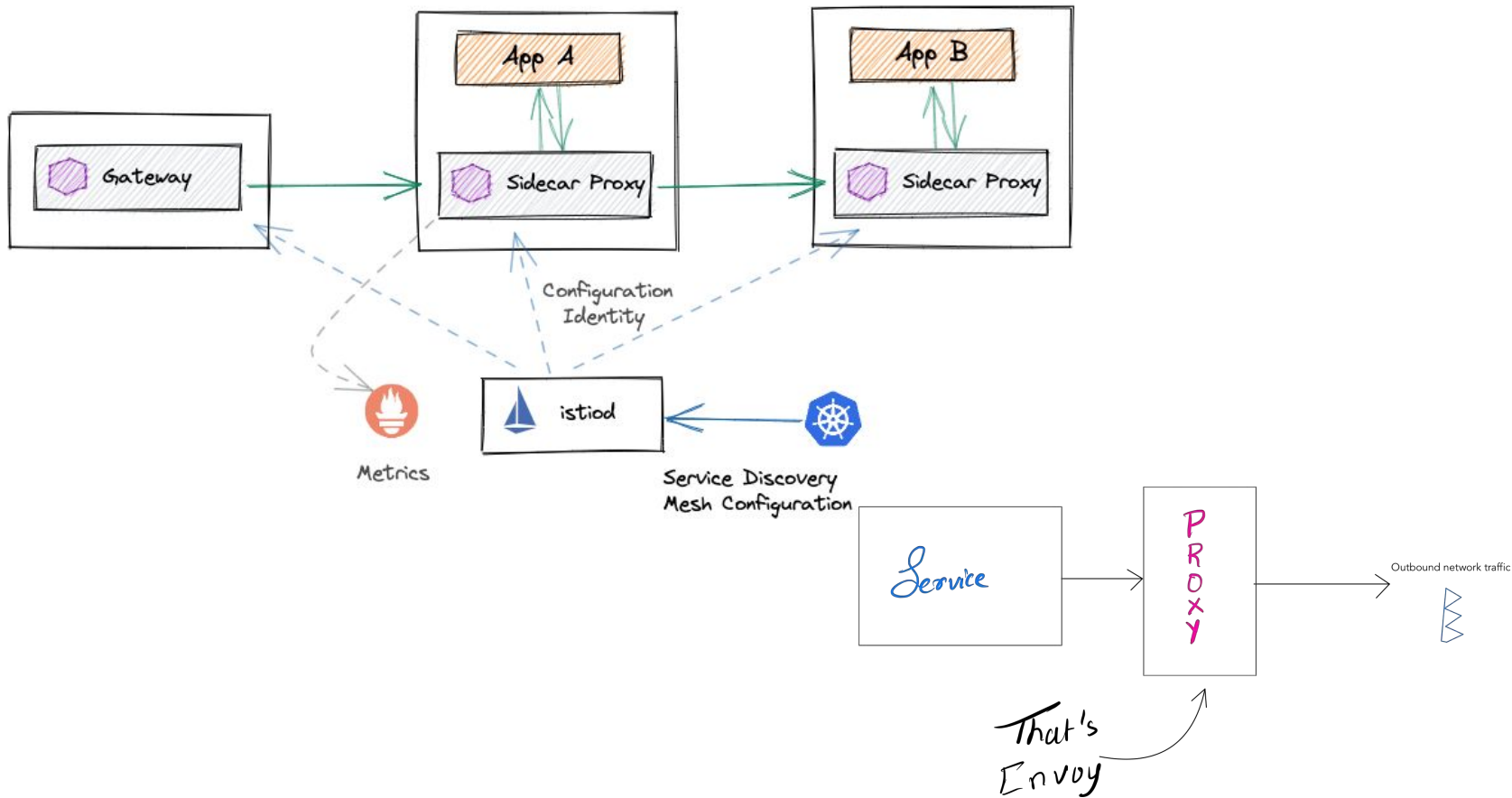
Resiliency

- Enable traffic resiliency
- Enable failover routing
- Enable high-availability

Zero Trust Security

- Secure communication between microservices
- Manage mTLS | Certs | Cert-Rotation
- Enforce security filters | policies

Istio

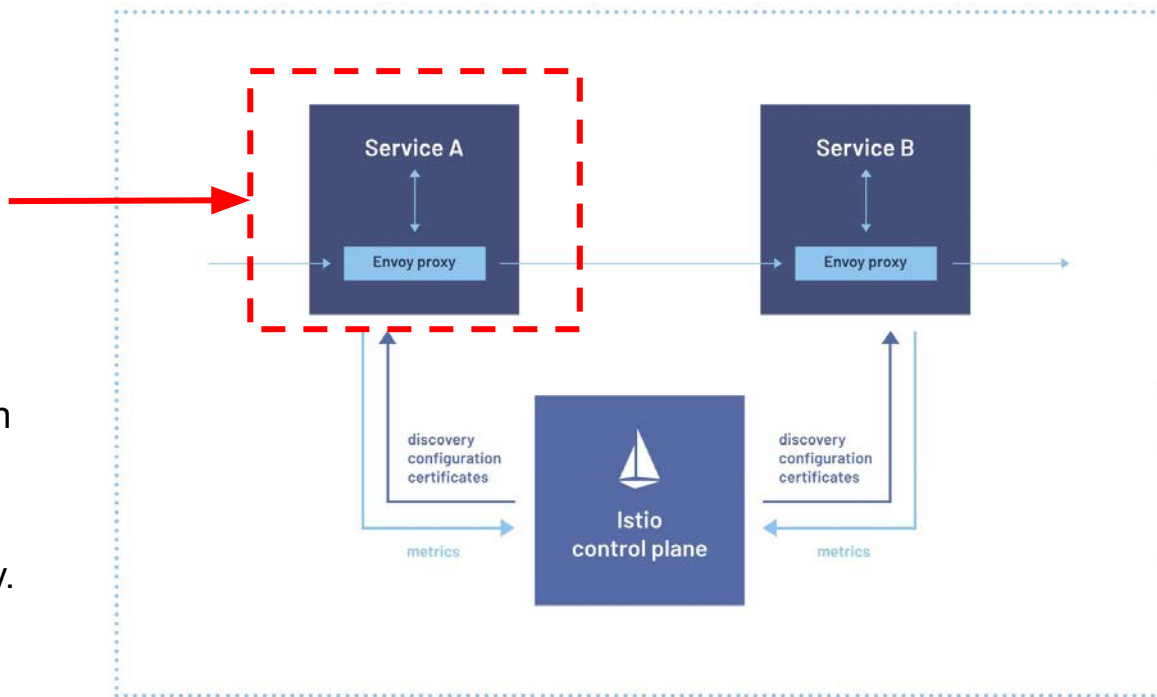


How Istio works today - Data Plane - Sidecar Proxies

Data plane. Every application pod is deployed with a proxy

The proxy (Envoy) is a **sidecar** of the Application

All L4 or L7 traffic goes through the sidecar proxy.



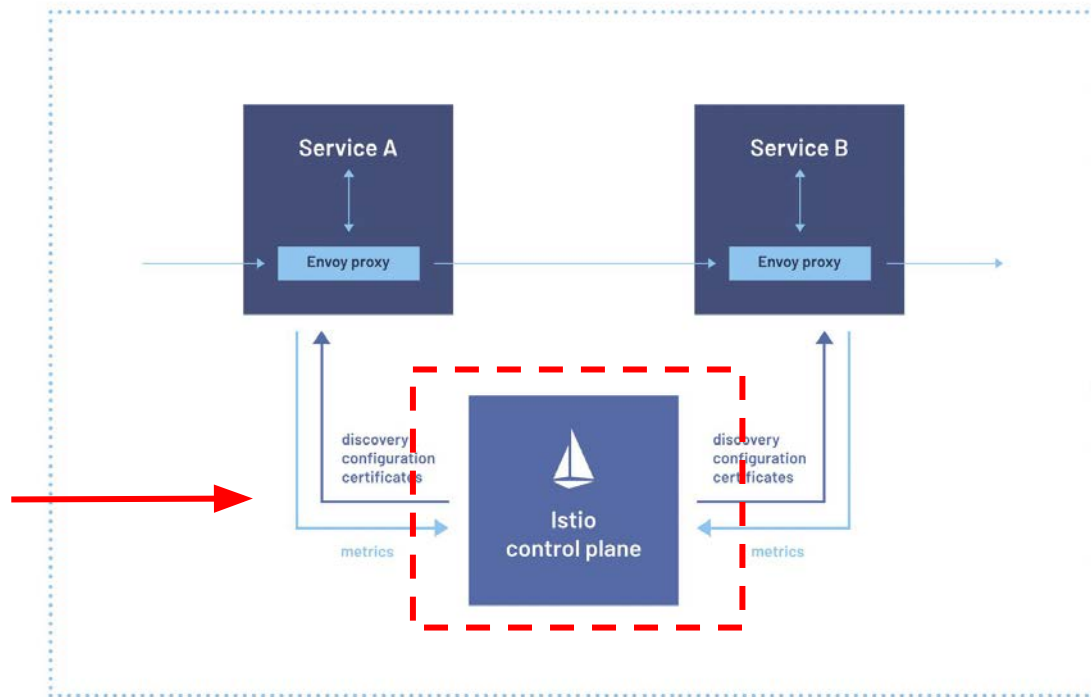
By adding a proxy "sidecar" along with every application deployed, Istio lets you program application-aware traffic management, incredible observability, and robust security capabilities into your network.

How Istio works today - Control Plane

Control Plane keeps track of service mesh.

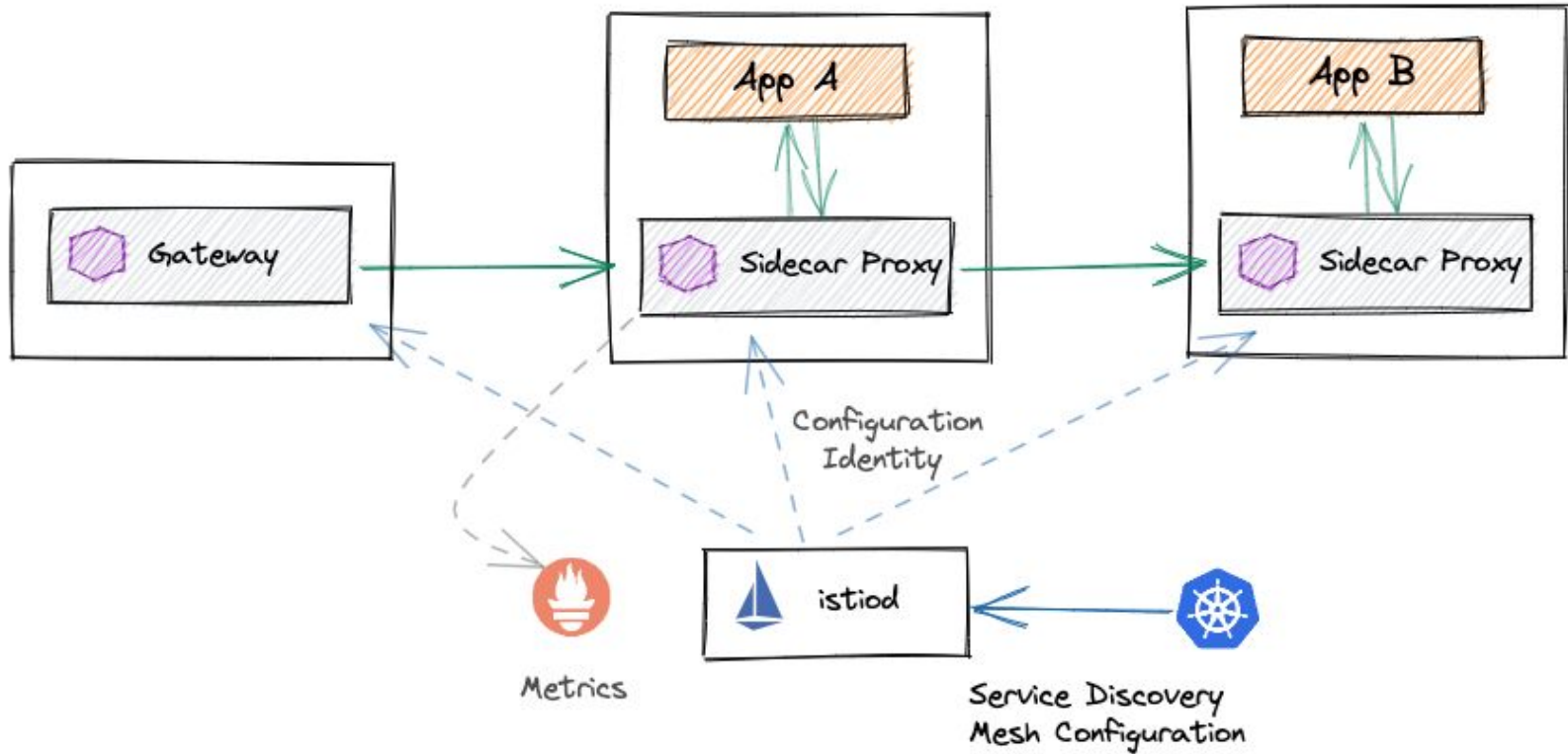
Control plane deploys proxies, filters, policies

Control plane is separate from proxy **data plane**.

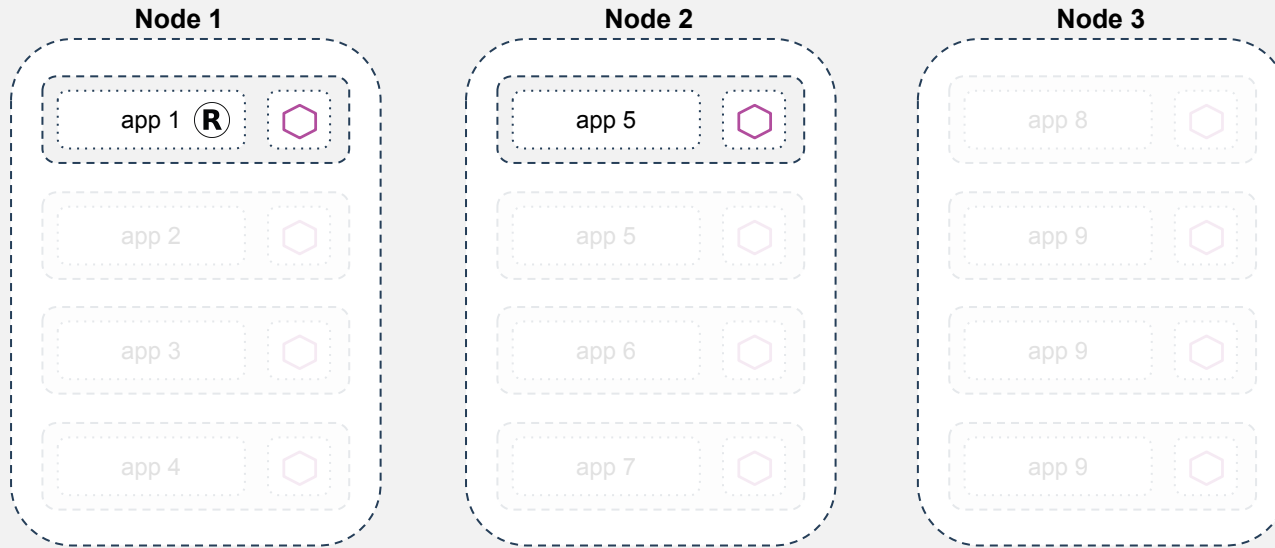


By adding a proxy "sidecar" along with every application deployed, Istio lets you program application-aware traffic management, incredible observability, and robust security capabilities into your network.

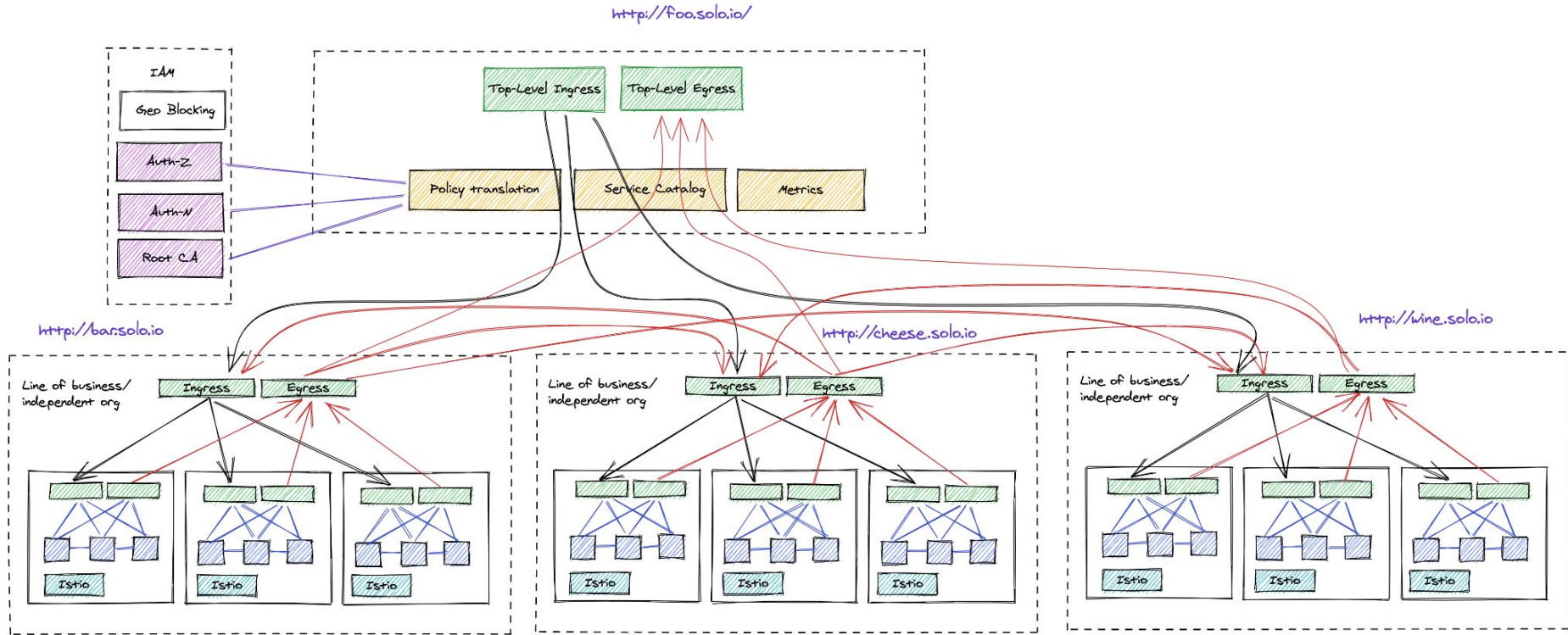
Istio



Istio sidecar model



Large deployments of enterprise service mesh

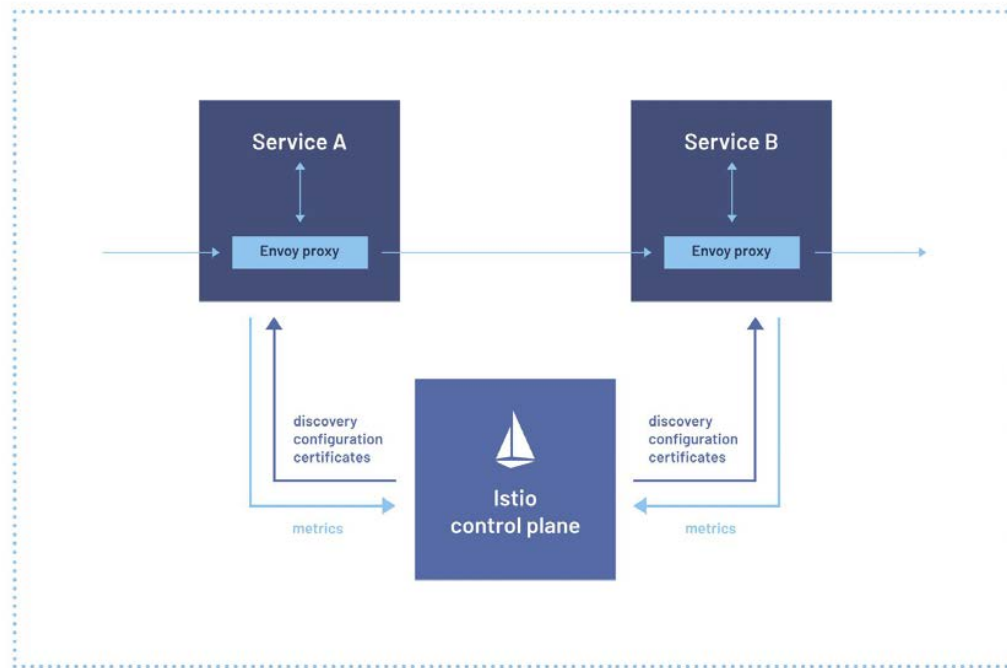


Potential Challenges with Sidecar Proxies

OVERHEAD
COST

OPERATIONAL
COMPLEXITY

PERFORMANCE

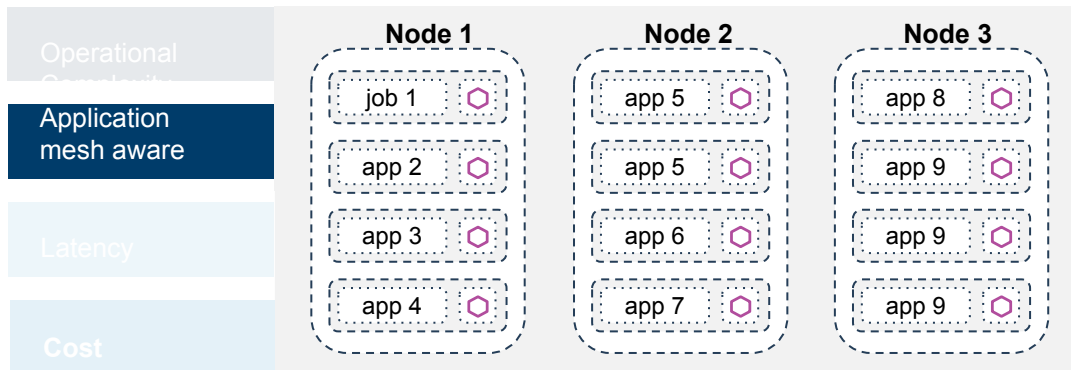
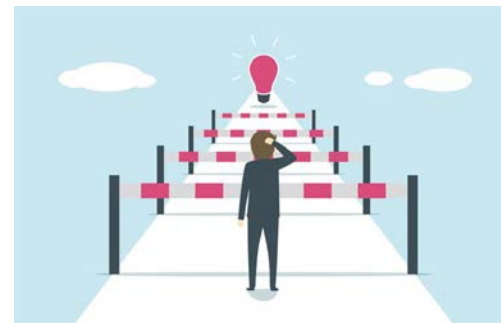
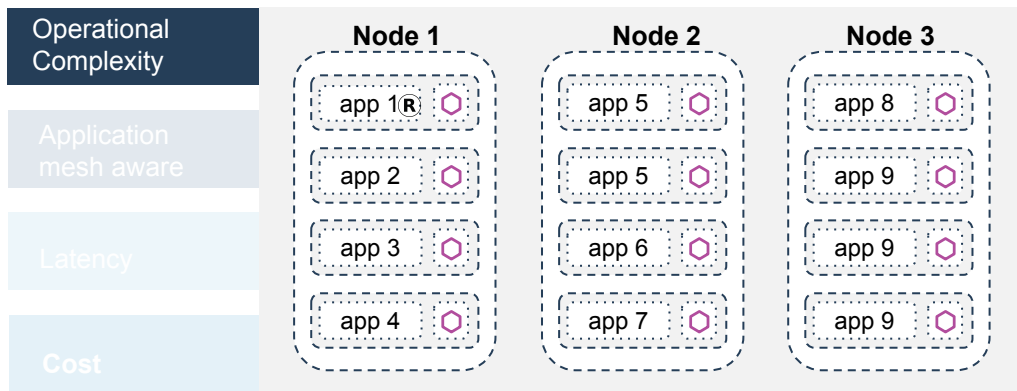


By adding a proxy "sidecar" along with every application deployed, Istio lets you program application-aware traffic management, incredible observability, and robust security capabilities into your network.

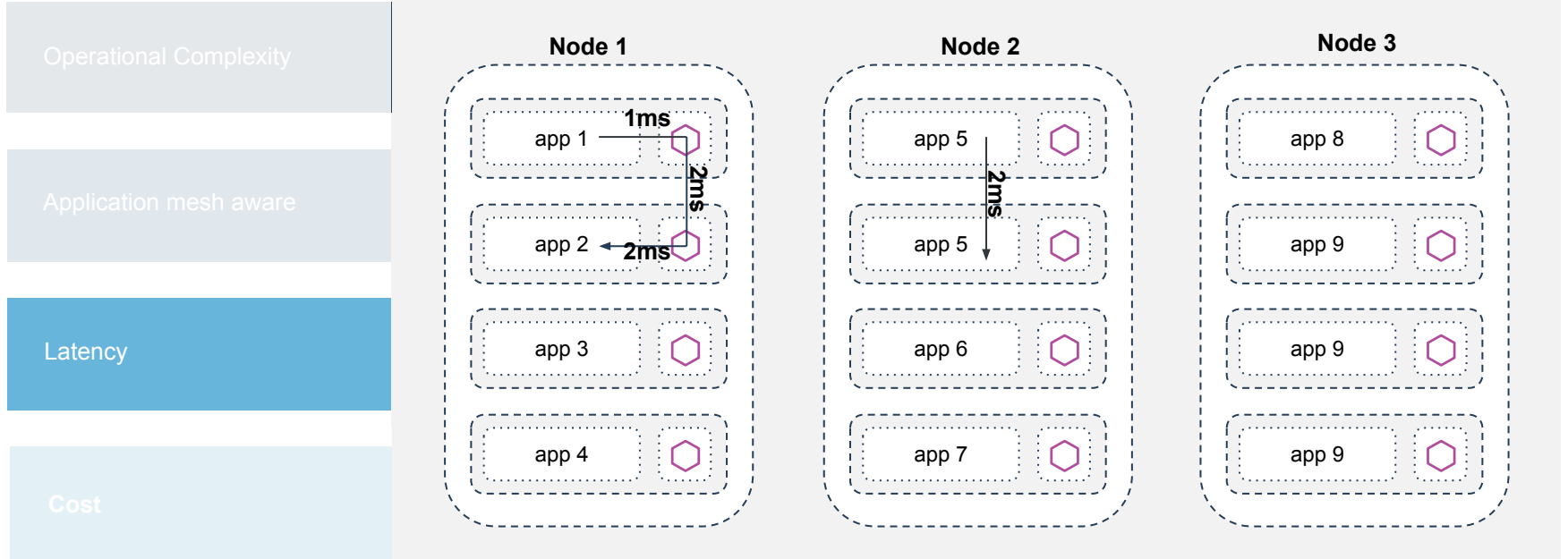
Sample Istio - Bookinfo page deployment

```
rohit-mac@Rohits-MacBook-Pro istio-1.13.7 % kubectl get pods
NAME                                READY    STATUS    RESTARTS    AGE
productpage-v1-7795568889-56qb4    2/2     Running  0           13d
details-v1-7d88846999-rkr58        2/2     Running  0           13d
ratings-v1-754f9c4975-qktzv        2/2     Running  0           13d
reviews-v3-7886dd86b9-9s7ff        2/2     Running  0           13d
reviews-v2-858f99c99-12mdg         2/2     Running  0           13d
reviews-v1-55b668fc65-mpqrv        2/2     Running  0           13d
```

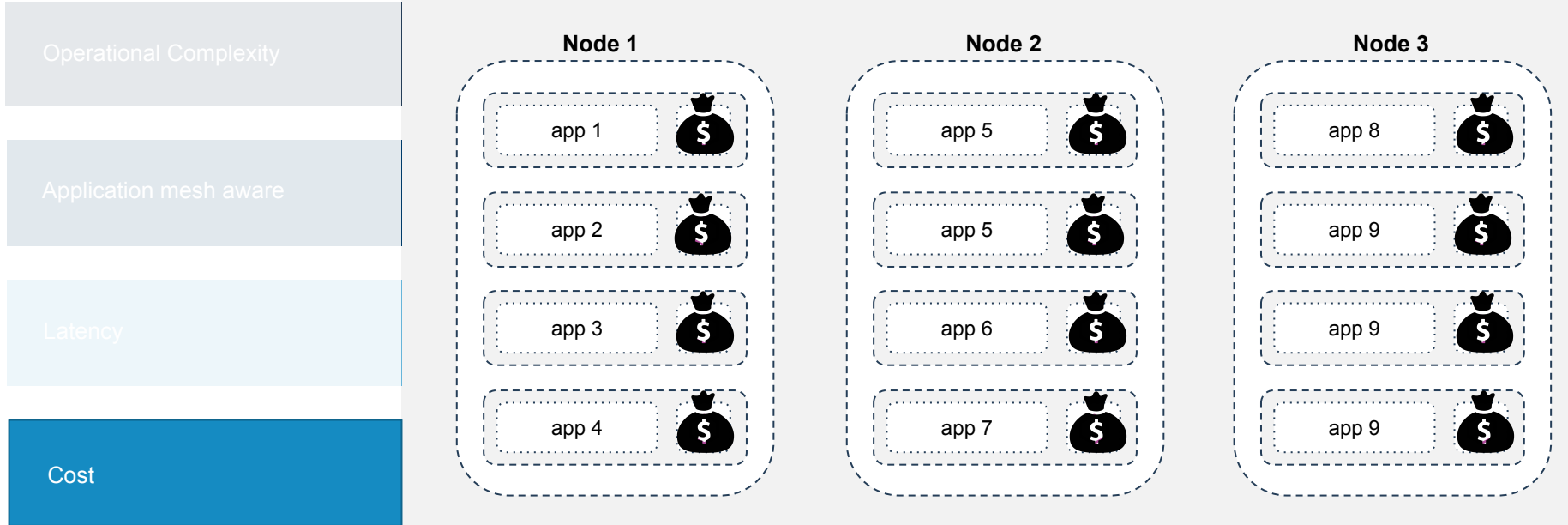

Istio sidecar model challenges



Istio sidecar model challenges



Istio sidecar model challenges

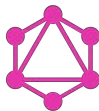




The Future of Service Mesh...

...happens in and around the data plane

Data plane is where the innovation continues to happen



Extending the data plane



- Web Assembly
- HTTP/3
- Universal Data Plane API



Optimizing the data plane

Introducing Istio Ambient Mesh



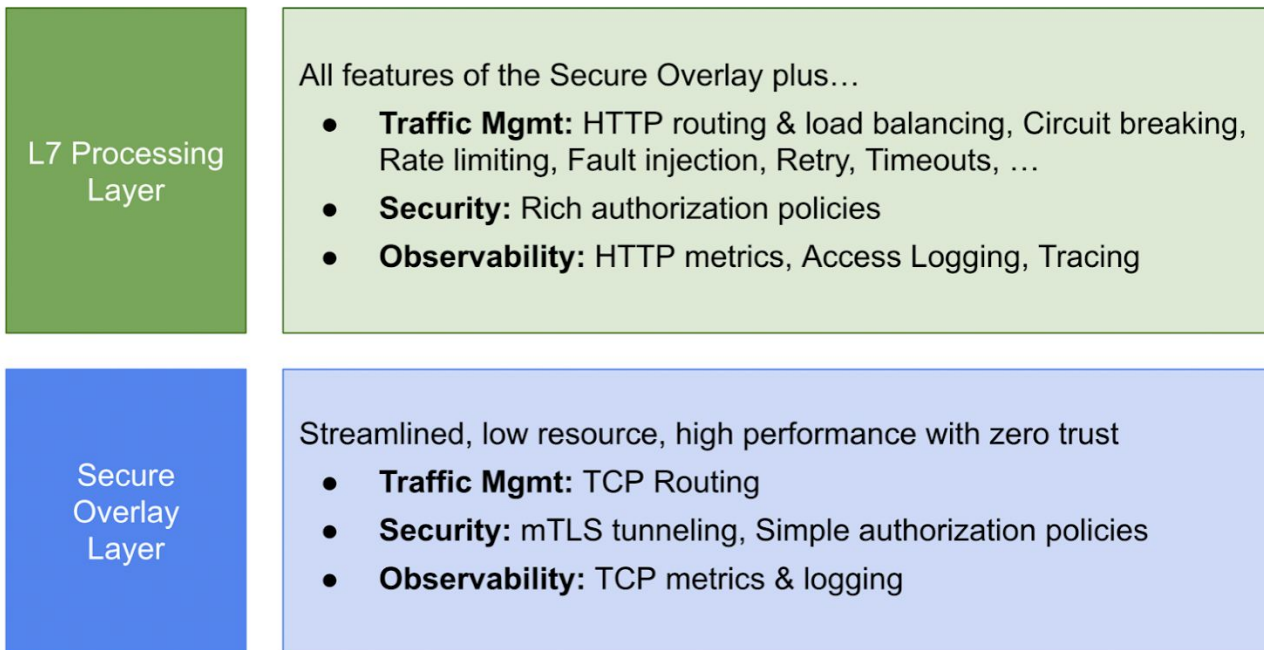
A new, open source contribution to the Istio project, that defines a new sidecar-less data plane.



Solo.io and Google are the lead contributors to Istio Ambient Mesh.

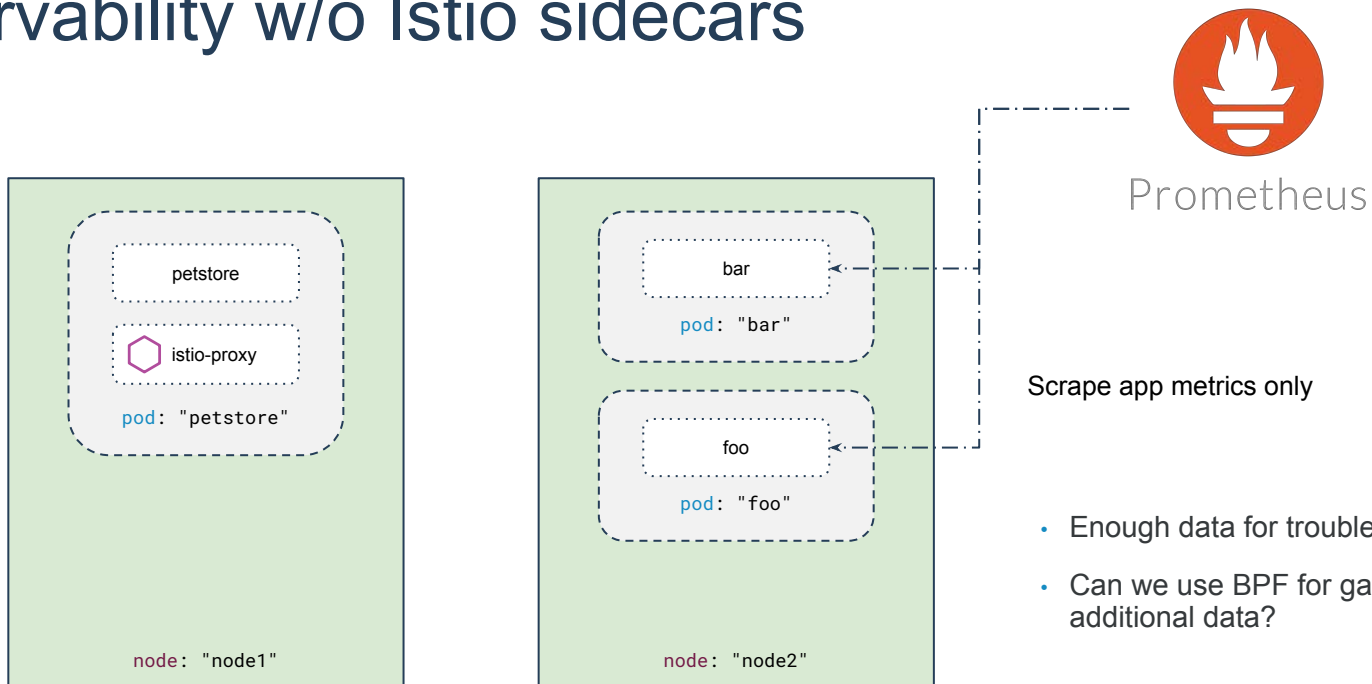


Slicing the layers



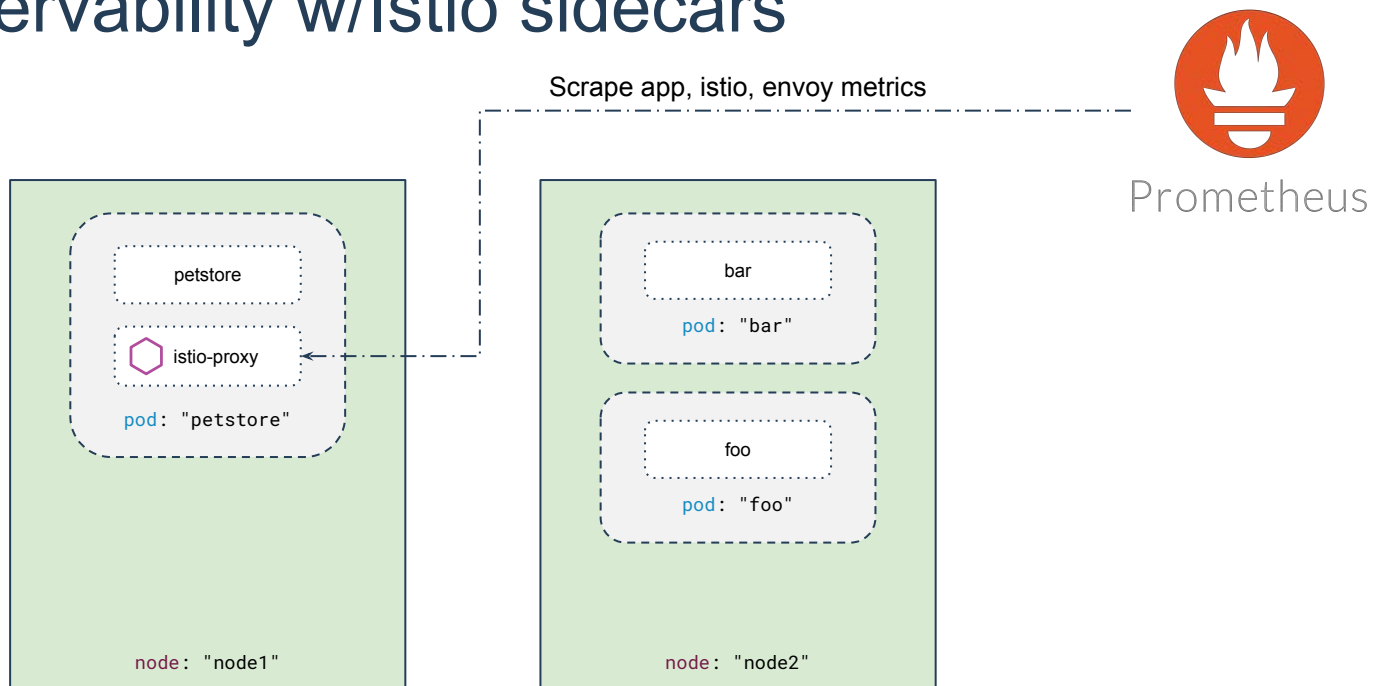
Layers of the ambient mesh

Observability w/o Istio sidecars

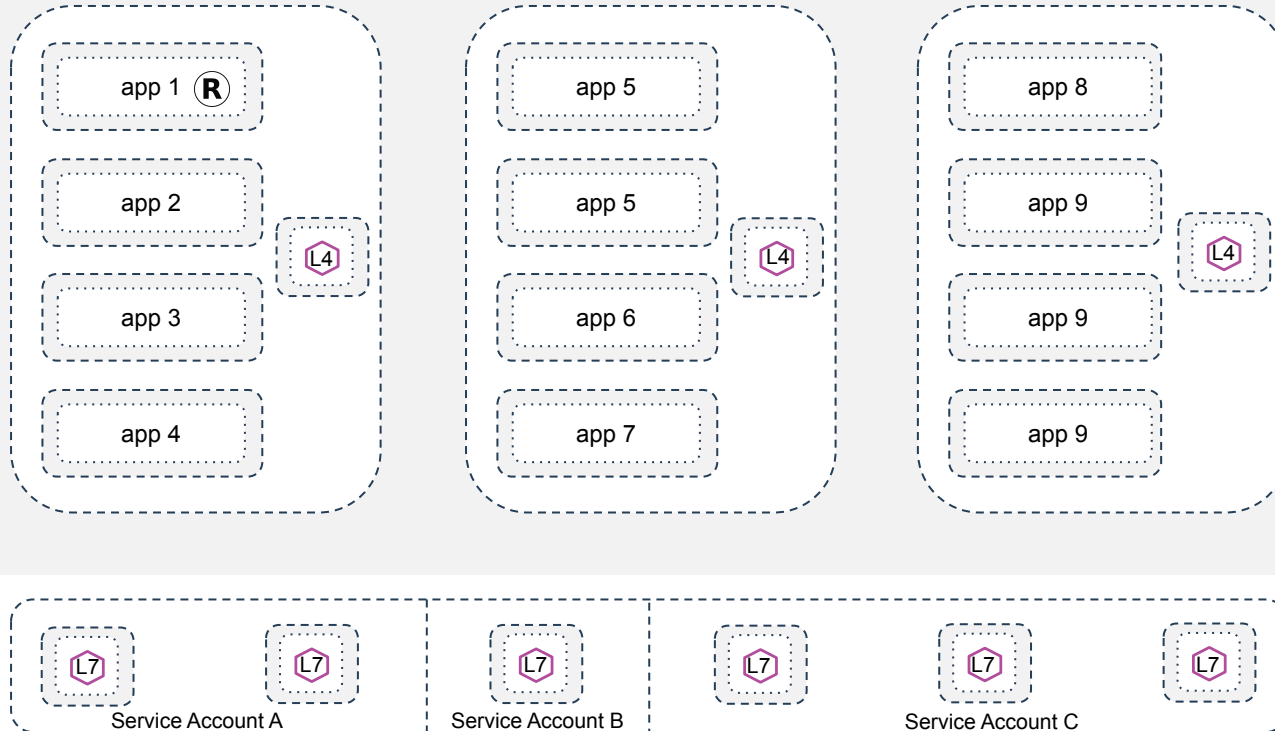


- Enough data for troubleshooting?
- Can we use BPF for gathering additional data?

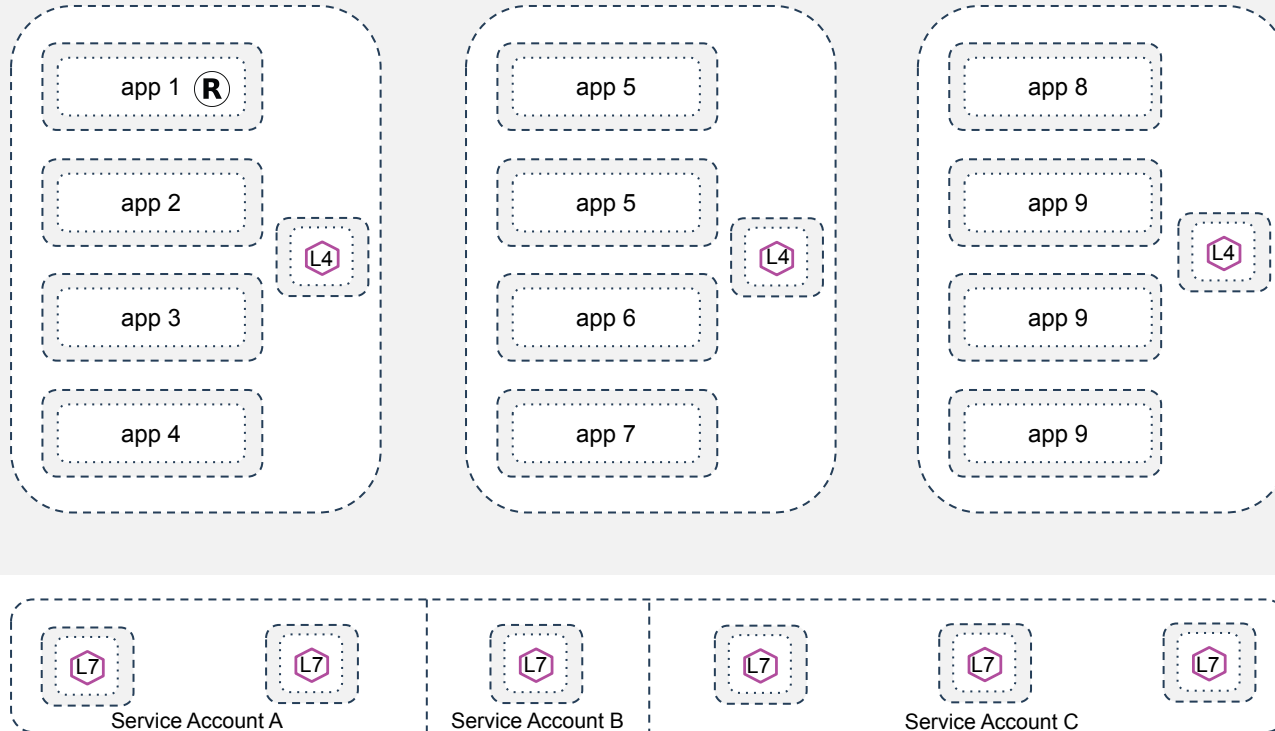
Observability w/Istio sidecars



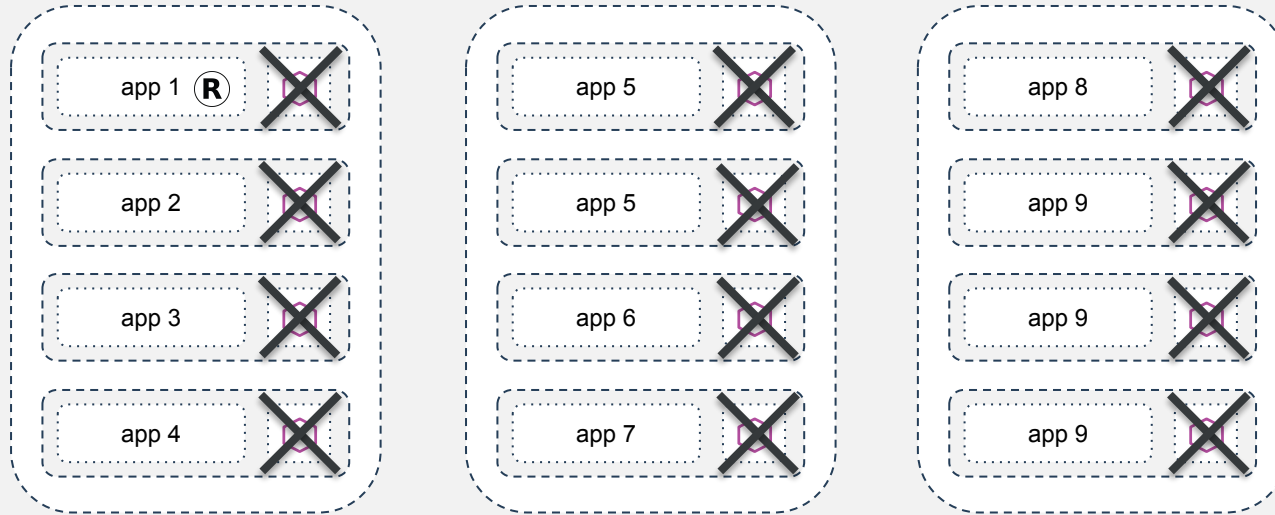
Istio ambient model L4



Istio ambient model L7

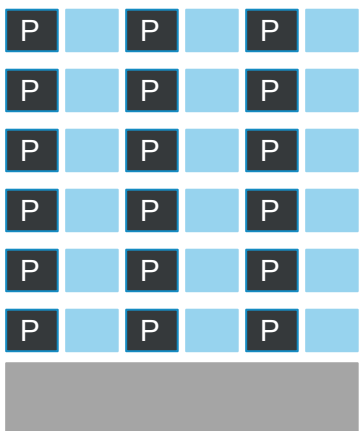


Istio ambient advantage: Reduced cost

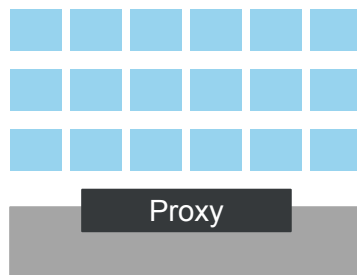


What is Istio Ambient Mesh? Reduce Costs

Move from Sidecar Proxy per-pod architecture to a Proxy per-node architecture.



Istio Sidecar Data Plane
1 Pod/Container = 1
Proxy



Ambient Mesh Data Plane
1 Node = 1 Proxy

What Istio Ambient Mesh Means for Your Wallet?

	Sidecar	Ambient (L4 only)	Ambient (L4 + L7)
# Istio Proxy Containers Required	31	3	6
Total CPU	3.1 vCPU	0.3 vCPU	0.6 vCPU
Total Memory	3968 Mi	384 Mi	768 Mi

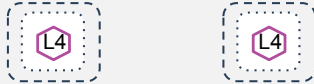
Blog: <https://www.solo.io/blog/what-istio-ambient-mesh-means-for-your-wallet/>

Istio ambient advantage: Performances

No Mesh

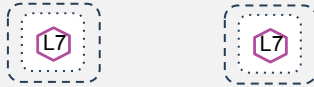
0ms

Mesh Sidecar L4



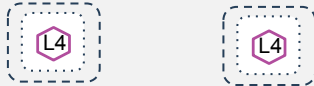
1ms

Mesh Sidecar L7



4ms

Ambient Mesh L4



1ms

Ambient Mesh L7



3ms



0.5ms



2ms

Introducing Istio Ambient Mesh



Reduce Costs

- Proxy per Node
- Multi-Tenant Proxy
- Lightweight (L4) Proxy implementation (uProxy)

Simplify Operations

- Mesh is Transparent to Applications
- Decouple Proxy from Applications
- Simplify Adding new Apps
- Simplify App Updates

Improve Performance

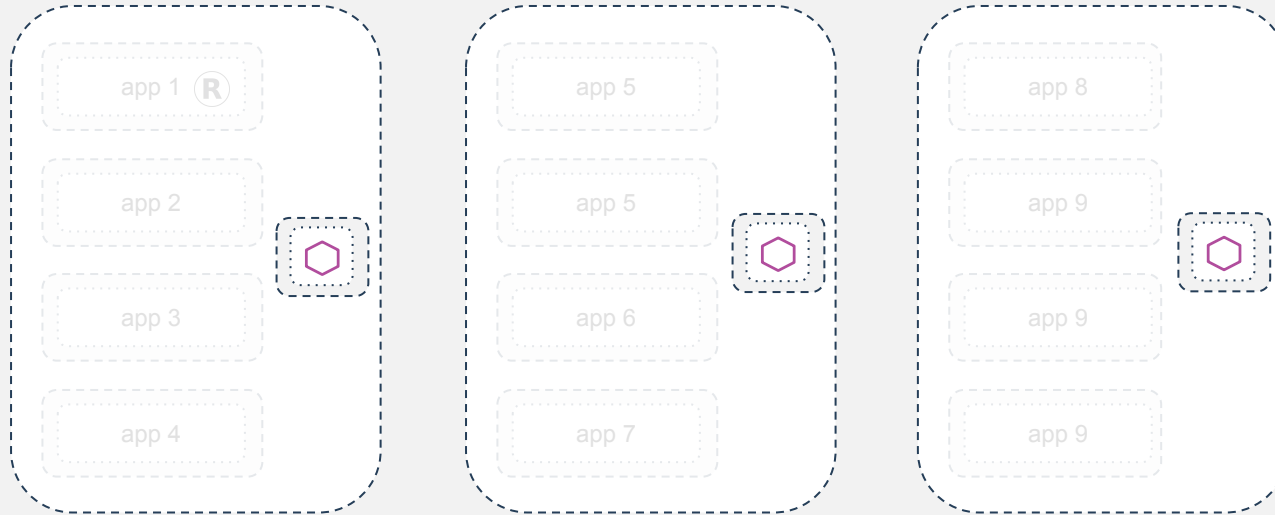
- uProxy is L4 vs L7
- uProxy can use acceleration in OS (eBPF)

Zero Trust Security

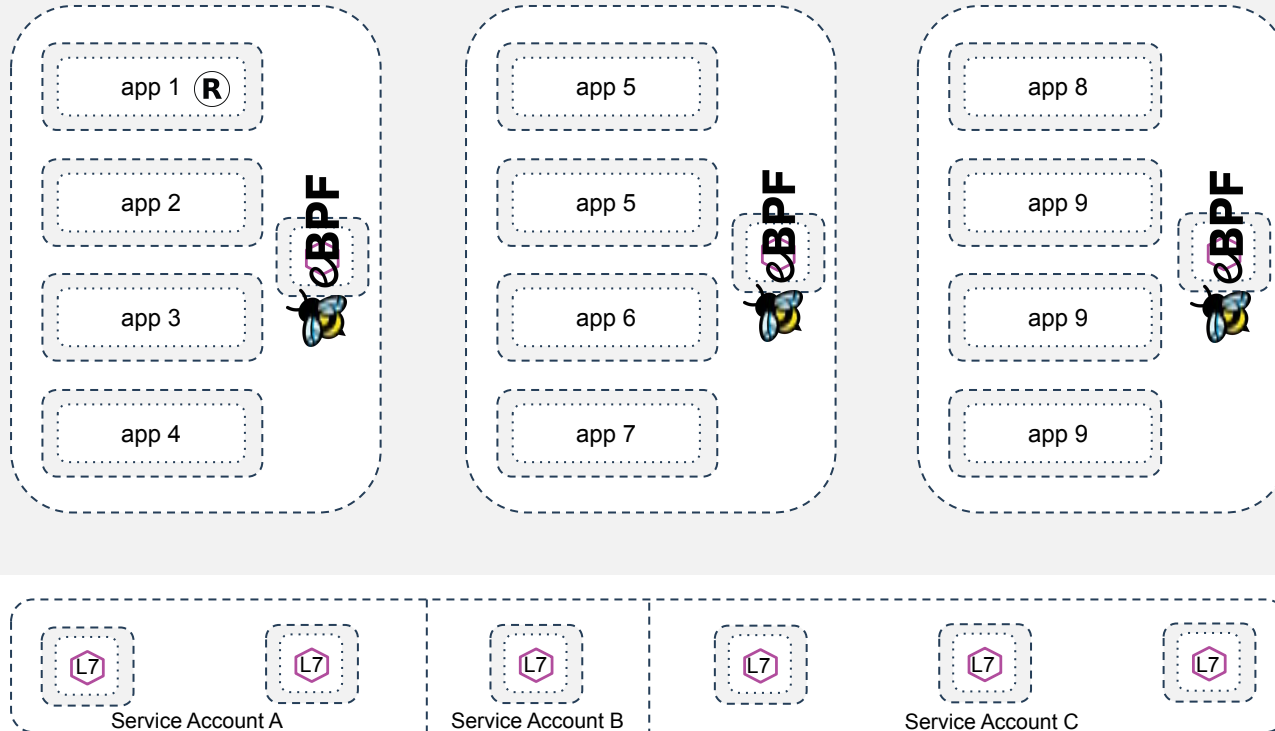


What's next?

Istio ambient



Istio ambient



Additional Resources - Istio Ambient Mesh

- [Introducing Istio Ambient Mesh](#) - Istio.io blog
- [Getting Started with Istio Ambient Mesh](#) - Istio.io blog
- [Istio Ambient Mesh - Security Deep Dive](#) - Istio.io blog
- [Istio Ambient Mesh](#) - demo video
- [Istio Ambient Mesh - Hands On Training & Certification](#) [FREE] - Solo.io Academy
- [Introducing Istio Ambient Mesh](#) - Solo.io blog
- [What Istio Ambient Mesh means for your Wallet](#) - Solo.io blog
- [Istio Ambient Mesh discussion](#) - The Cloudcast (podcast)

Thank You 🙏

Connect for more details: [@ghumare64](#)



Demo

Thank You!



solo.io



Who am I?

Rohit Ghumare

I am Developer Advocate, GDE for Google Cloud

Communities:

- Keep Up
- DevOps Community
- Developer Relations Community
- Cloud native Thane
- GDG Cloud Mumbai
- KCD Mumbai

Connect with me:

Twitter: [@ghumare64](https://twitter.com/ghumare64)

LinkedIn: [/in/rohit-ghumare](https://in.linkedin.com/in/rohit-ghumare)

Portfolio: bento.me/rohitghumare