# Embracing the Future: The Effortless Mutual TLS and Traffic Control Without Sidecars

Showing results for house ***construction*** roles
Search instead for house constrction roles

# From sources across the web

- Architect
- Construction Manager
- Engineer
- Project Manager
- Construction
- Plumber
- Roofer
- Structural engineer
- Carpenter
- Construction scheduling
- Electrician
- Estimator
- Interior designer
- Plasterer
- Building inspectors
- Cabinetmaker
- Heavy equipment
- Design
- HVAC Installer
- Safety Manager
- Subcontractors
- Superintendent
- Surveyor
- Tile Setter

Showing results for house ***construction*** roles
Search instead for house constrction roles

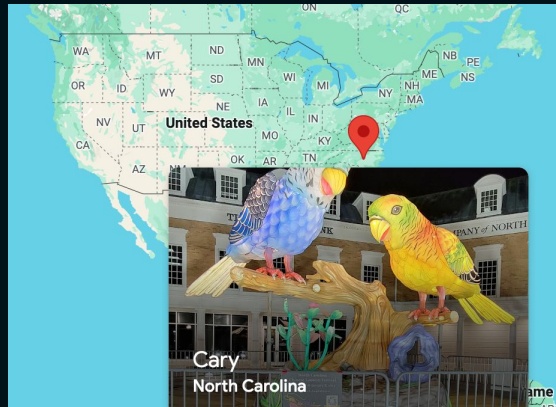
# From sources across the web

- Architect
- Project Manager
- Roofer
- Construction scheduling
- Interior designer
- Cabinetmaker
- HVAC Installer
- Superintendent
- Construction Manager
- Construction
- Structural engineer
- Electrician
- Plasterer
- Heavy equipment
- Safety Manager
- Surveyor
- Engineer
- Plumber
- Carpenter
- Estimator
- Building inspectors
- Design
- Subcontractors
- Tile Setter

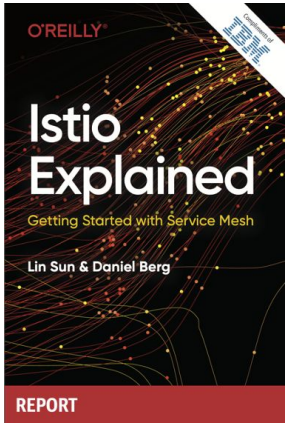
# Lin Sun

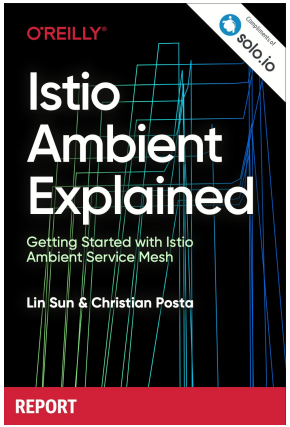
Head of Open Source

solo.io

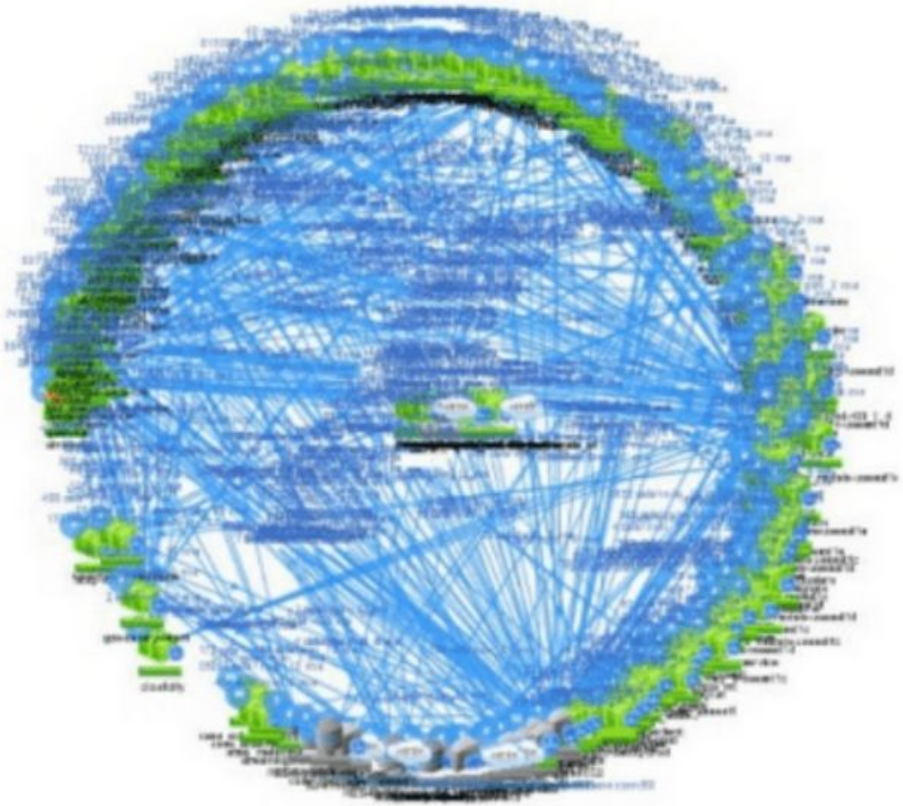



207
IBM Patents


O'REILLY
Istio
Explained
Getting Started with Service Mesh
Lin Sun & Daniel Berg
REPORT


O'REILLY
Istio
Ambient
Explained
Getting Started with Istio
Ambient Service Mesh
Lin Sun & Christian Posta
REPORT

# Problems



  Source: https://www.divante.com/blog/10-companies-that-implemented-the-microservice-architecture-and-paved-the-way-for-others

# Show Me Your Hand

# What is a Service Mesh?

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

# Service Mesh Evolution


envoy

Source: https://landscape.cncf.io/

# Happy Sidecars Users

*"We decided to just try out Istio to see how it would go, and we ended up delivering in the space of about a week – more than we had done in the last four months trying to roll it ourselves."*

AutoTrader

Learn more

*"Istio's extensibility, broad feature support and scalability make it a great choice for Airbnb."*

airbnb

Learn more

*"We've used Istio since 1.3 and we've seen every version become incrementally better. We've seen it become easier to use, use less resources, and get easier to install."*

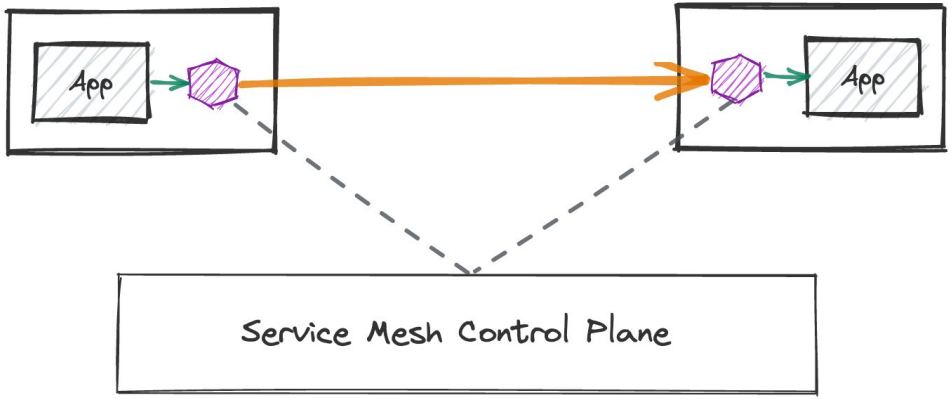
splunk>

Learn more

# Sidecar Challenge

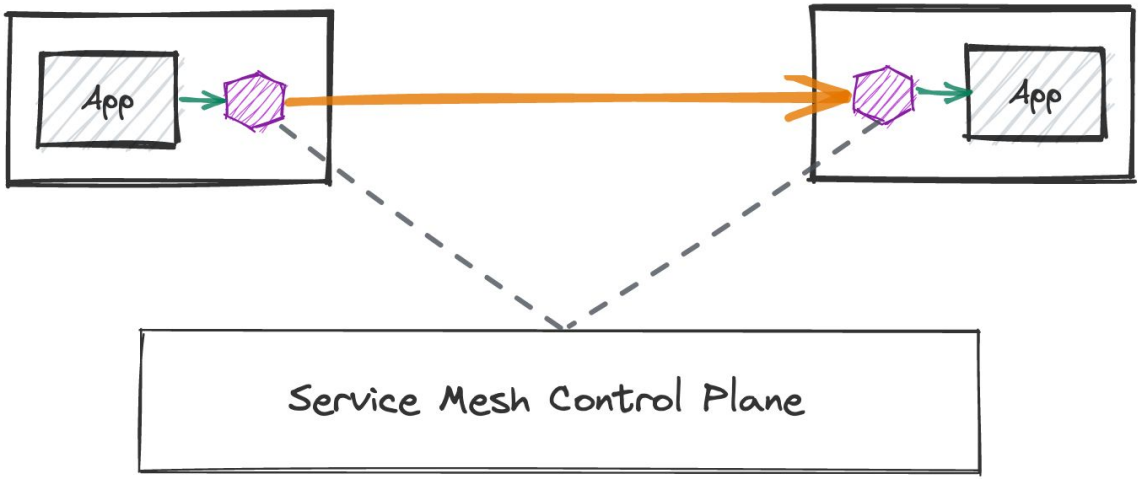
# Challenges With Sidecars - Transparency

- Require injection of sidecars
  - You may already have an init container for your application pod
- Startup/shutdown sequences between app containers and sidecars
- Sidecar upgrade requires restarting of applications
- Jobs? Server-send-first protocols?



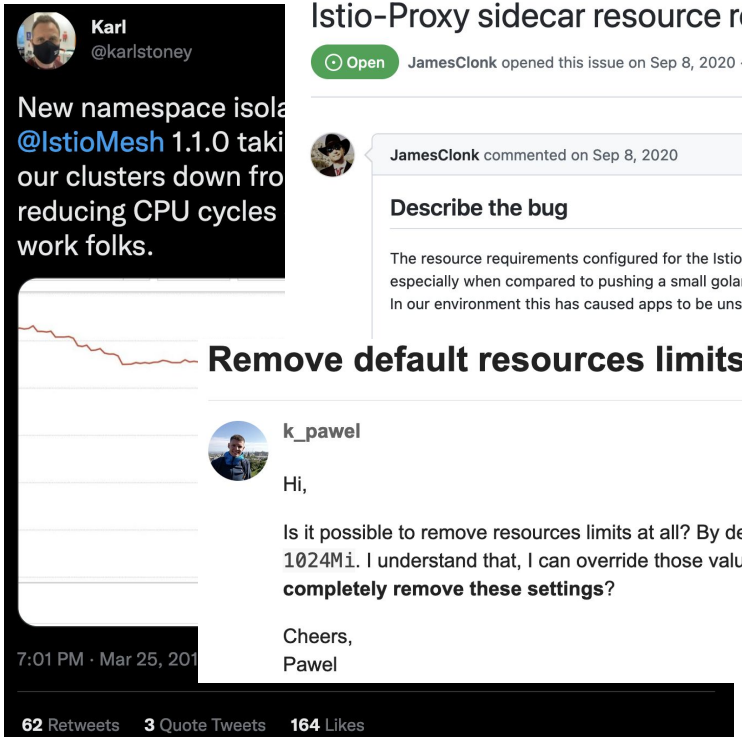
# Challenges With Sidecars - Incremental Adoption

- Yes you can adopt one feature at a time
- Many users adopt service mesh because of mTLS among applications
- All-or-nothing injection of sidecars



# Other Challenges With Sidecars

- Security
- Overprovision resources

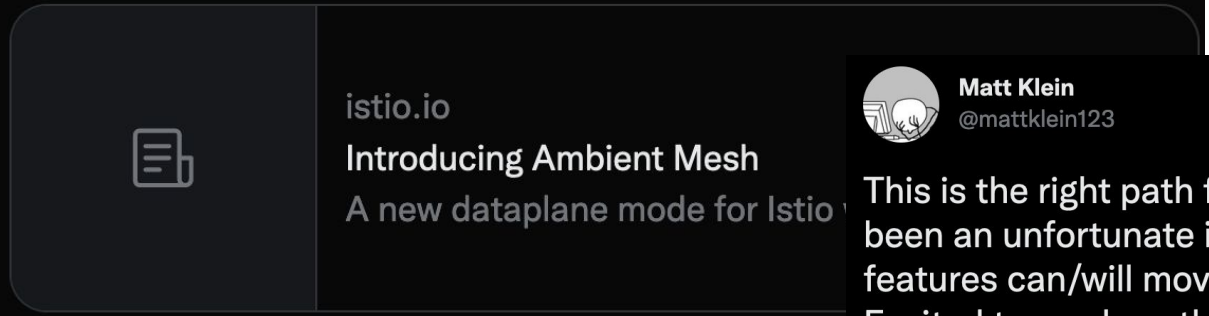


# Istio Ambient

You Retweeted

**Istio** @IstioMesh · Sep 7

Very special day for the Istio community, check out Istio ambient mesh - a new dataplane mode for Istio without sidecars:




9 135 266

**Matt Klein**
@mattklein123

This is the right path forward. Sidecars have always been an unfortunate implementation detail. Mesh features can/will move into the underlying infra. Excited to see how this evolves and very excited to see Envoy further abstracted from the average user.

> **Istio** @IstioMesh · Sep 7
> Very special day for the Istio community, check out Istio ambient mesh - a new dataplane mode for Istio without sidecars: istio.io/latest/blog/20...

4:18 AM · Sep 8, 2022 · Twitter for Android

**31** Retweets **2** Quote Tweets **172** Likes

solo.io

# Introducing Ambient Mesh

## A new dataplane mode for Istio without sidecars.

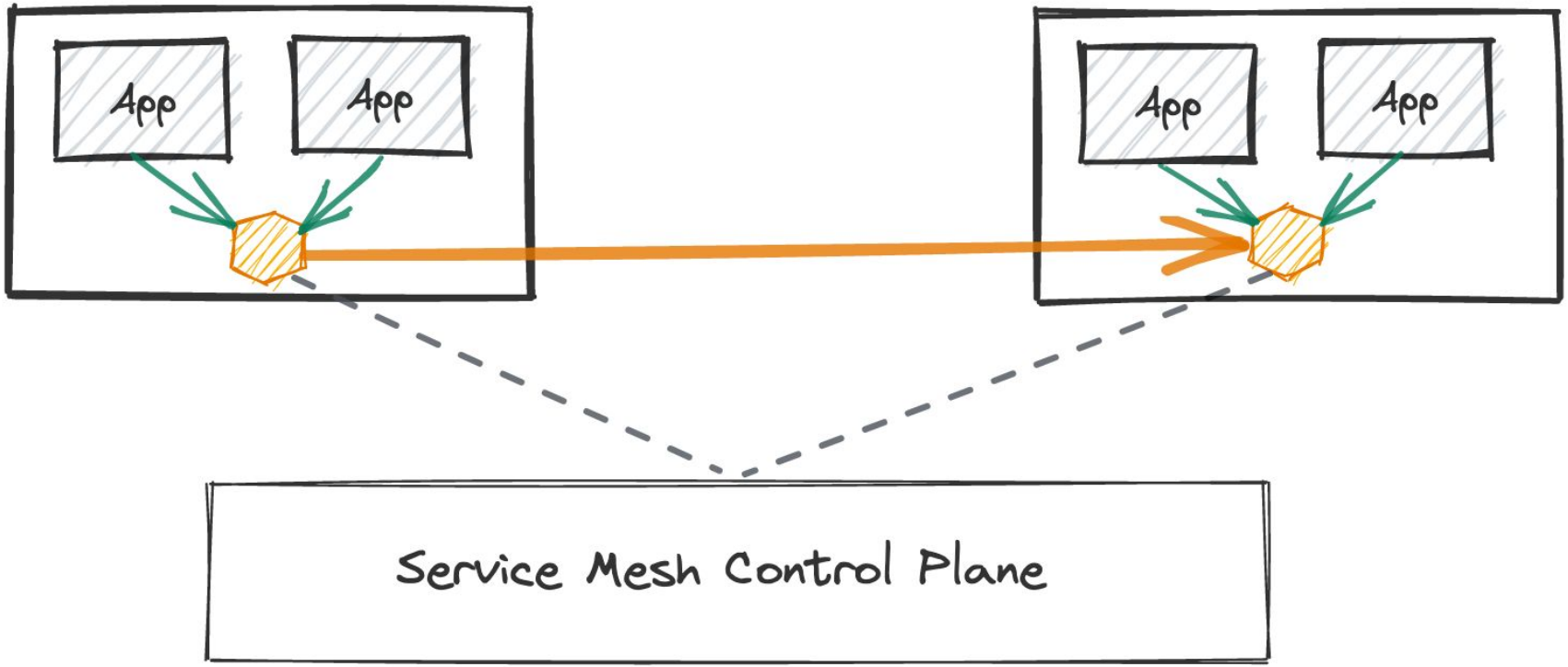
Sep 7, 2022 | By John Howard - Google, Ethan J. Jackson - Google, Yuval Kohavi - Solo.io, Idit Levine - Solo.io, Justin Pettit - Google, Lin Sun - Solo.io


https://istio.io/latest/blog/2022/introducing-ambient-mesh/

# Istio Ambient Mesh Architecture

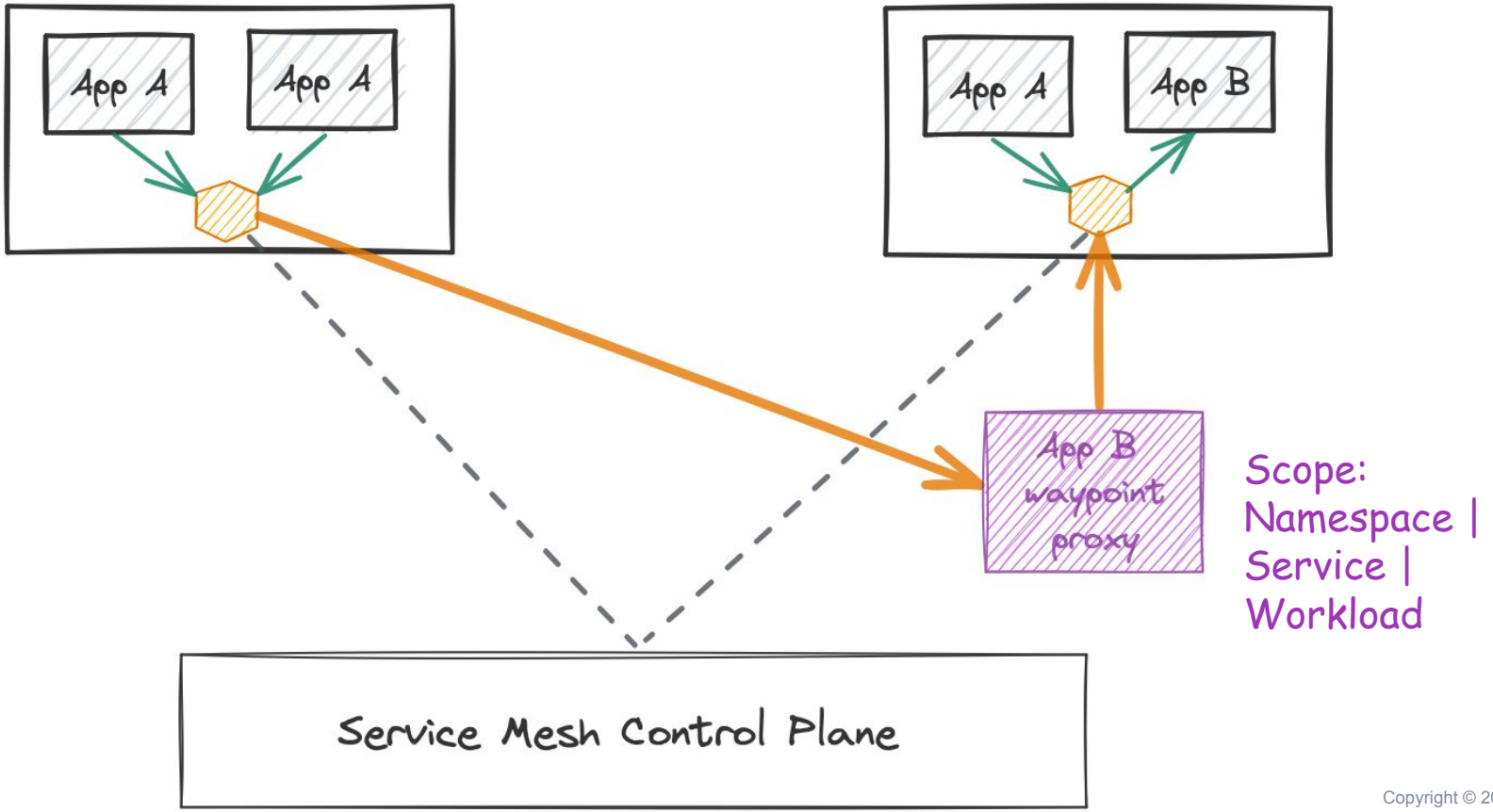
# Node Agent

# Secure Overlay Layer



# Gateway

# L7 Processing Layer



# Slicing the Layers

| | |
|---|---|
| Secure Overlay Layer | Streamlined, low resource, high performance with zero trust<br>• **Traffic Mgmt:** TCP Routing<br>• **Security:** mTLS tunneling, Simple authorization policies<br>• **Observability:** TCP metrics & logging |
| L7 Processing Layer | All features of the Secure Overlay plus…<br>• **Traffic Mgmt:** HTTP routing & load balancing, Circuit breaking, Rate limiting, Fault injection, Retry, Timeouts, …<br>• **Security:** Rich authorization policies<br>• **Observability:** HTTP metrics, Access Logging, Tracing |

# Why 2 layers architecture?

# Is Envoy Designed for Multi-Tenancy?

**Louis Ryan**
@louiscryan

I think every #servicemesh would love to reduce it's TCO and #proxyless seems attractive but there's a huge catch.

Uncontrolled L7 config in a multi-tenant proxy is an outage 💣 & noisy-neighbor 📢😭 factory. @IstioMesh and others don't do this for a very good reason.


**Matt Klein** @mattklein123 · May 6, 2022

We have actually put some thought into what tenant accounting would look like in envoy. I think it's possible to do reasonably accurately, but I agree with the general sentiment that the complexity is probably not worth it.

1 6

# Design Ambient for Scale

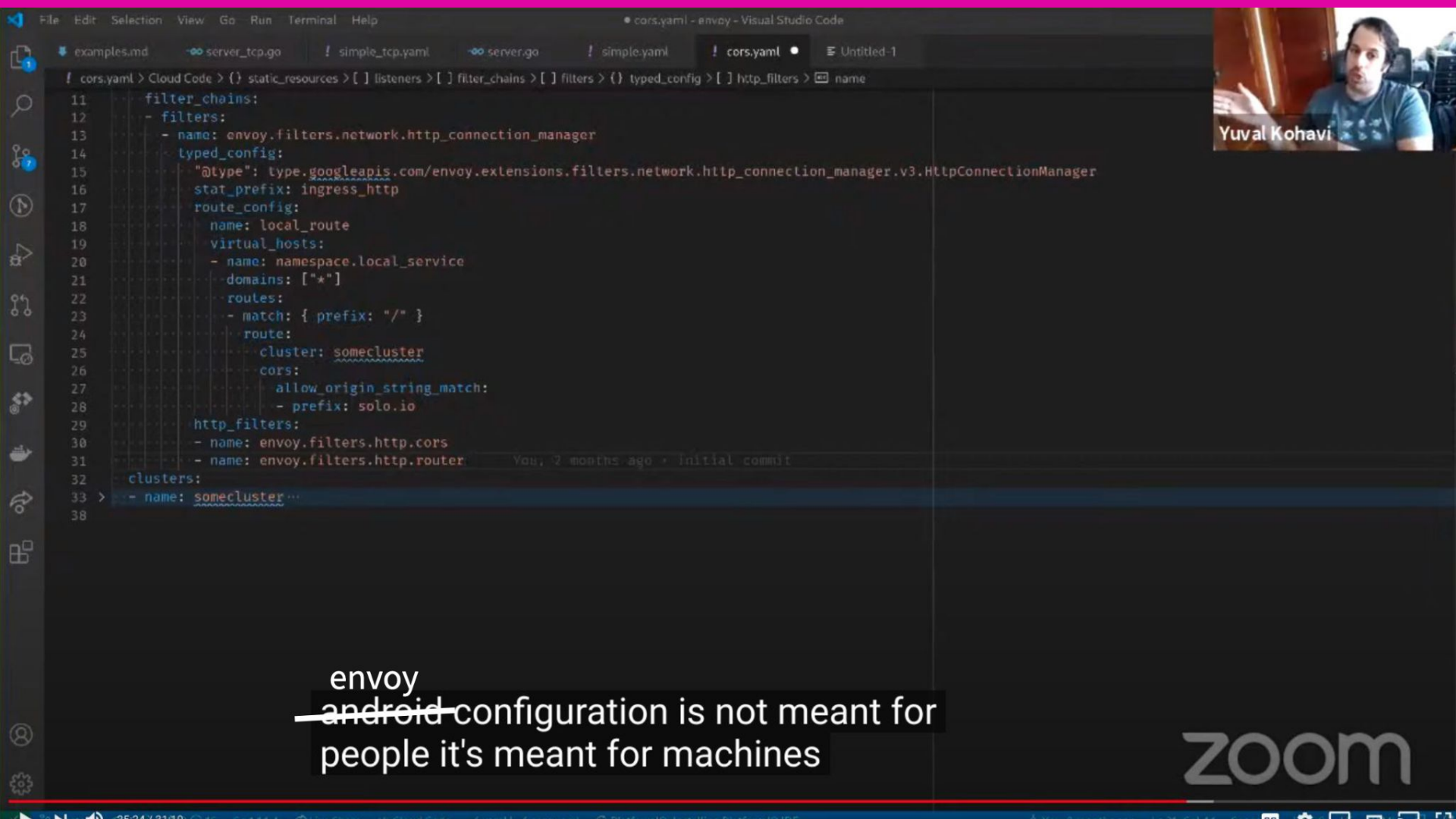
# Pre-programmed Envoy Proxy

Envoy proxy executes the configuration


Very large xDS configurations

Istiod generates Envoy configurations

Istiod


File Edit Selection View Go Run Terminal Help
cors.yaml - envoy - Visual Studio Code
examples.md
server_tcp.go
simple_tcp.yaml
server.go
simple.yaml
cors.yaml
Untitled-1
cors.yaml > Cloud Code > {} static_resources > [ ] listeners > [ ] filter_chains > [ ] filters > {} typed_config > [ ] http_filters > name
filter_chains:
- filters:
- name: envoy.filters.network.http_connection_manager
typed_config:
"@type": type.googleapis.com/envoy.extensions.filters.network.http_connection_manager.v3.HttpConnectionManager
stat_prefix: ingress_http
route_config:
name: local_route
virtual_hosts:
- name: namespace.local_service
domains: ["*"]
routes:
- match: { prefix: "/" }
route:
cluster: somecluster
cors:
allow_origin_string_match:
- prefix: solo.io
http_filters:
- name: envoy.filters.http.cors
- name: envoy.filters.http.router
You, 2 months ago • Initial commit
clusters:
- name: somecluster
Yuval Kohavi
envoy
~~android~~ configuration is not meant for
people it's meant for machines
zoom

Screenshot from Rob Salmond's IstioCon 2021 talk - https://events.istio.io/istiocon-2021/sessions/what-envoy-hears-when-istio-speaks/

# View the Ztunnel Configurations

```
{
  "workloads": {
    "10.244.2.8": {
      "workloadIp": "10.244.2.8",
      "protocol": "TCP",
      "name": "helloworld-v1-cross-node-55446d46d8-ntdbk",
      "namespace": "default",
      "serviceAccount": "helloworld",
      "workloadName": "helloworld-v1-cross-node",
      "workloadType": "deployment",
      "canonicalName": "helloworld",
      "canonicalRevision": "v1",
      "node": "ambient-worker2",
      "authorizationPolicies": [],
      "status": "Healthy"
    }
  }
}
```

kubectl label namepace istio.io/dataplane-mode=ambient

HBONE

default/hw-viewer

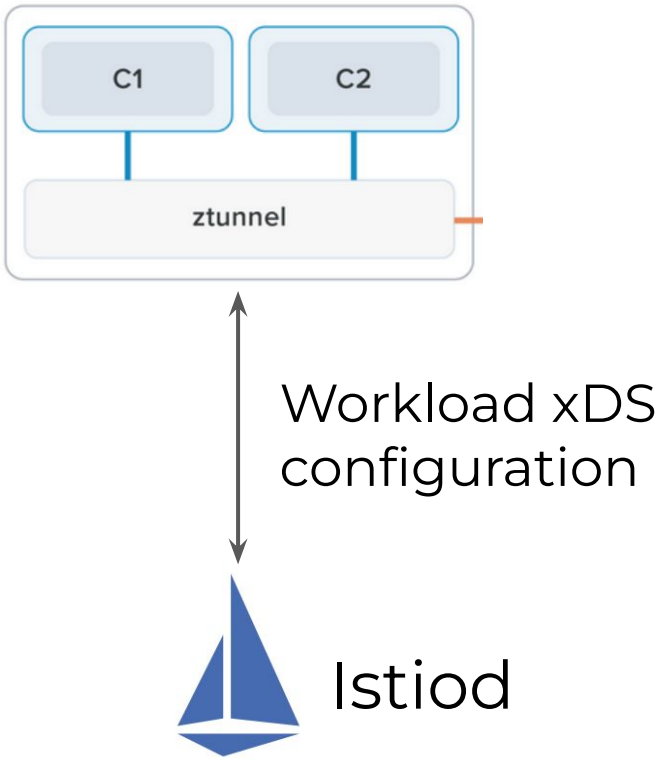
```
{
  "policies": {
    "default/hw-viewer": {
      "name": "hw-viewer",
      "namespace": "default",
      "scope": "WorkloadSelector",
      "action": "Allow",
      "groups": [[[{
        "principals": [{"Exact": "cluster.local/ns/default/sa/sleep"}]
      }]]]
    }
  }
  ...
}
```

# Much Simplified Workload xDS Configuration

Simple to read and debug

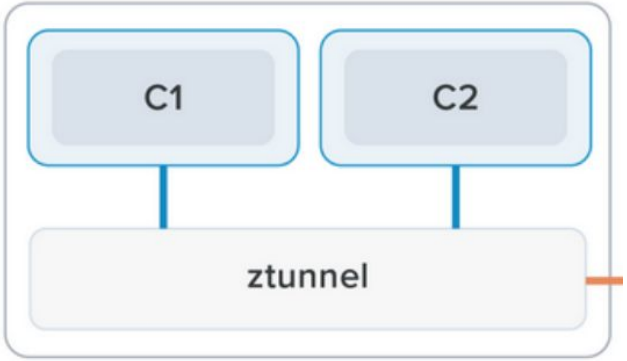
Less resources from Istiod to generate the xDS configuration

Reduced network cost between ztunnel and Istiod



# Ztunnel Implementation

- GoLang
- C++
- Rust
  - High performance and low resource utilization
  - Battle tested rich libraries (Tokio and Hyper)
  - Can support work stealing easily via its Tokio library



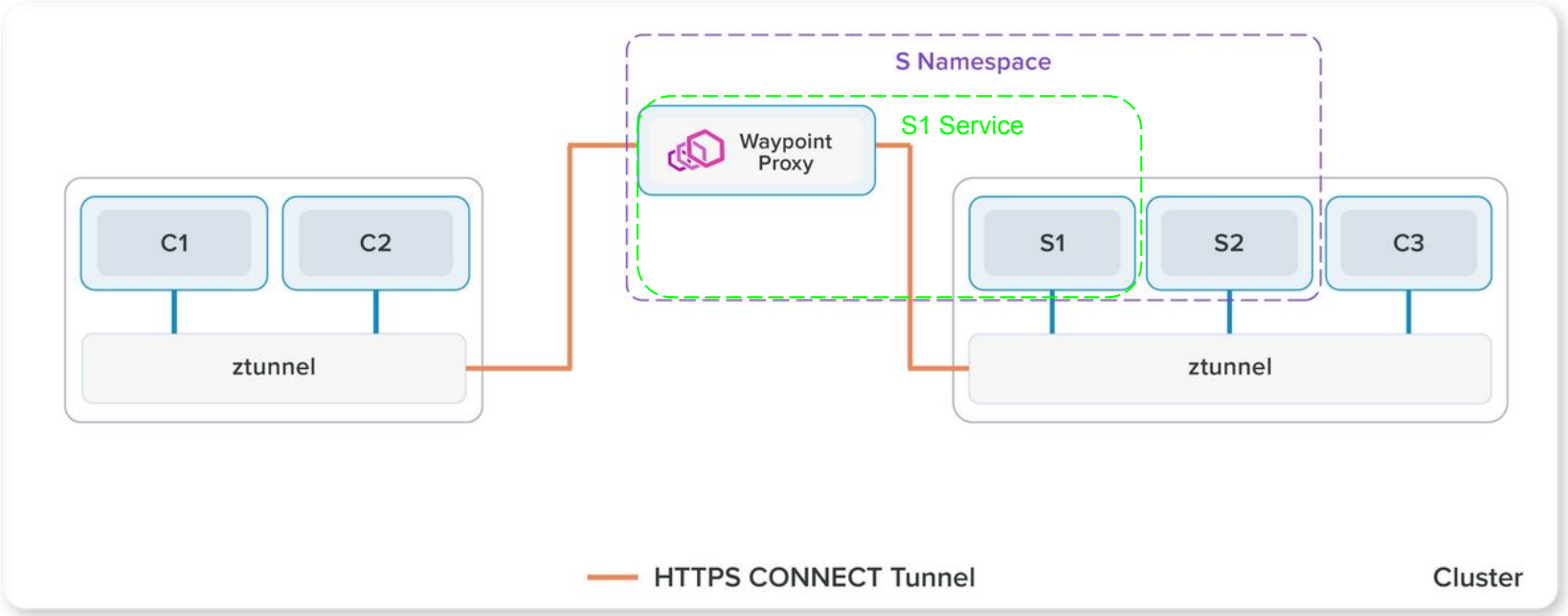

**howardjohn** @_howardjohn · Aug 24

The largest Kubernetes cluster size I have seen discussed is 150k Pods (and even that I believe is theoretical), so I setup Istio ambient on a *200k pod*, 14k service cluster.

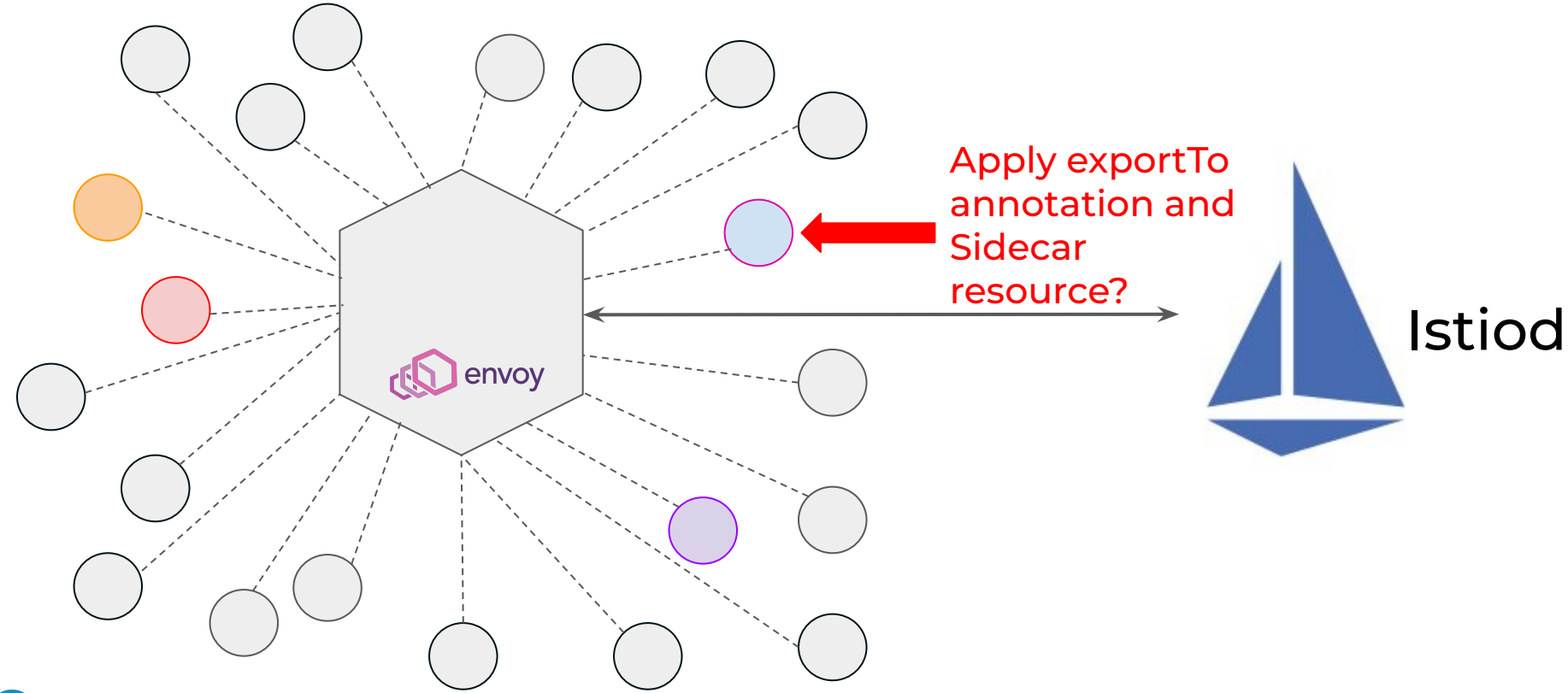
Ztunnel comes in at just under 500mb RAM and starts up in just over 1s.

5 15 58 9,668

# Waypoint Architecture



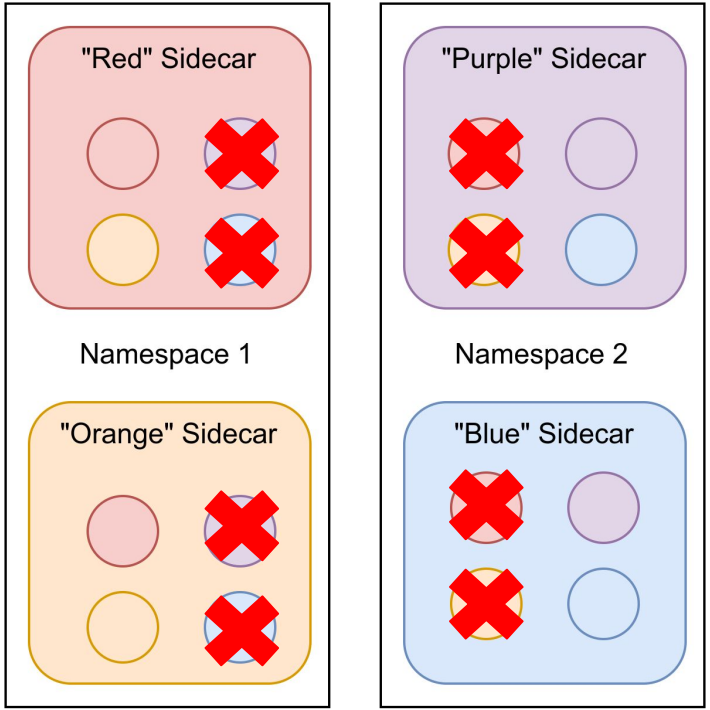
# Back to the Drawing Board



# Sidecar Config

## Service Producer

```
apiVersion: v1
kind: Service
metadata:
 name: red
 annotations:
  networking.istio.io/exportTo:
".,istio-ingress"
spec:
 selector:
   app: red
 ports:
 - name: http
   protocol: TCP
   port: 8080
   targetPort: 8080
```

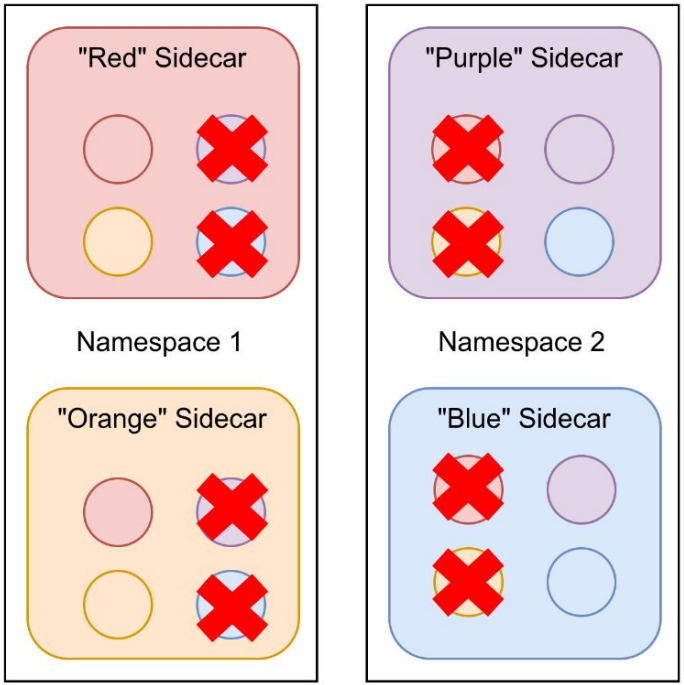



## Service Consumer

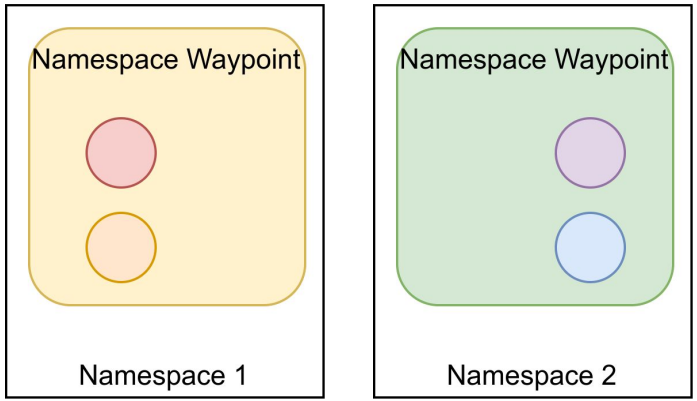
```
apiVersion:
networking.istio.io/v1beta1
kind: Sidecar
metadata:
 name: default
spec:
 egress:
 - hosts:
   - "namespace-1/*"
   port:
     number: 8080
     protocol: HTTP
     name: egresshttp
 - hosts:
   - "istio-system/*"
```

solo.io

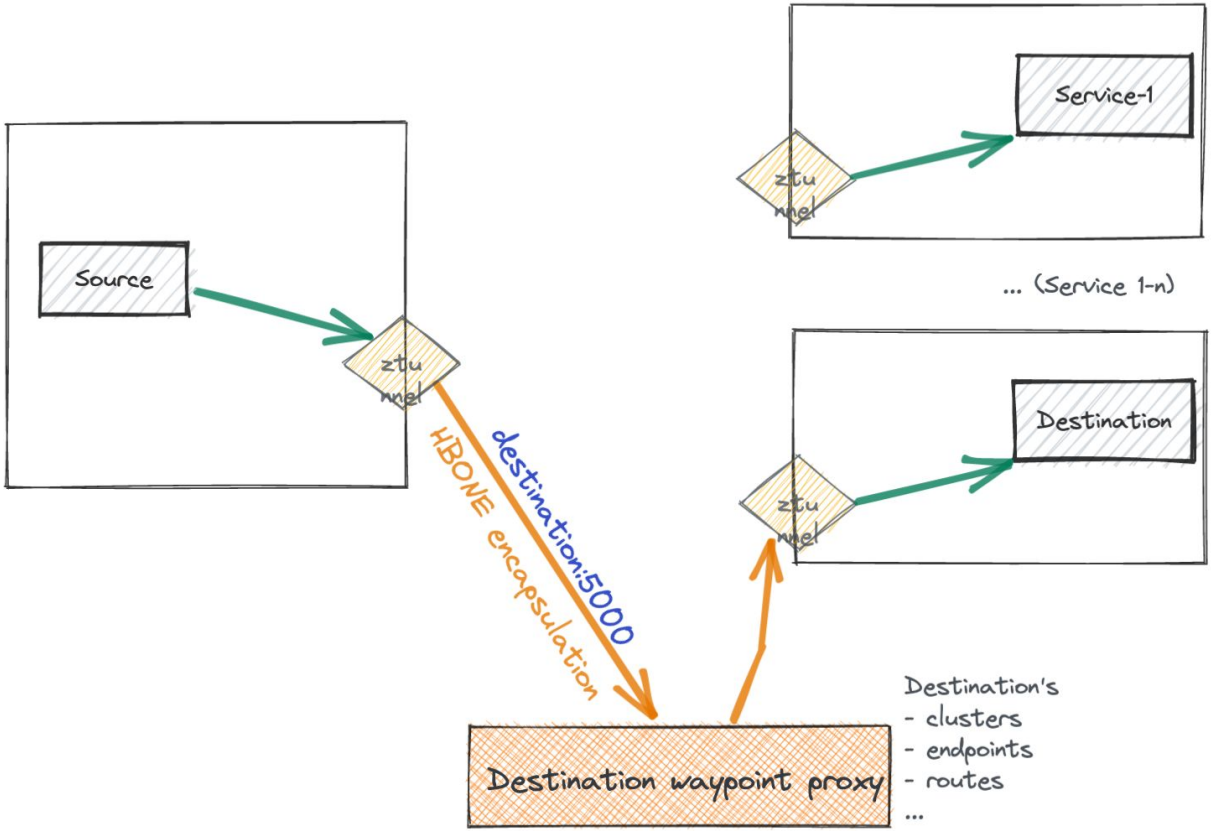
# Simplification for Waypoint




Do we require users to configure exportTo and Sidecar resource for waypoint?

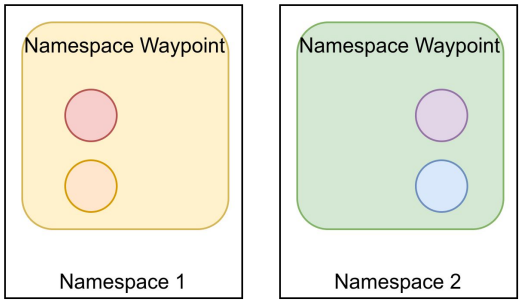


# Destination-Only Waypoint




Eliminate the need for exportTo and Sidecar resources waypoint.

# Waypoint Configuration By Default




Each namespace scales to 25 deployments with 10 pods each and each waypoint deployment with 2 pods

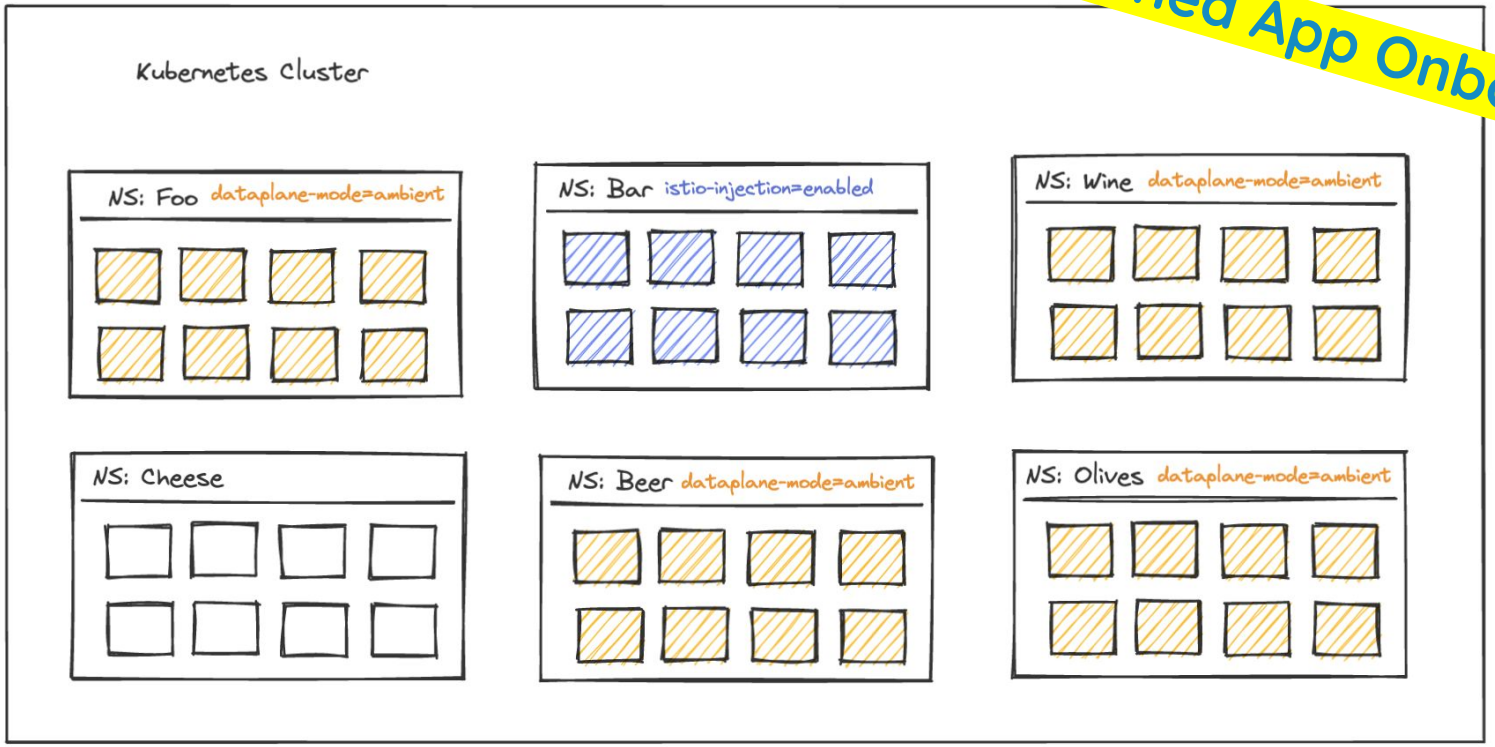
| Config Distribution | Namespace 1 | Namespace 2 | Total |
|---|---|---|---|
| Sidecars | 25 configurations * 250 sidecars | 25 configurations * 250 sidecars | 12500 |
| Waypoints | 25 configurations * 2 waypoints | 25 configurations * 2 waypoints | 100 |
| Waypoints / Sidecars | 0.8% | 0.8% | 0.8% |

CPU/Memory/Network Bandwidth

# UX experience

# Including Applications in Ambient

Simplified App Onboarding




*kubectl label namespace foo istio.io/dataplane-mode=ambient*

# App Requirements Eliminated

Simplified App Onboarding

- Jobs
- Application UID 1337
- NET_ADMIN and NET_RAW capabilities
- Ports used by Istio proxy (15000, 15001, 15004, 15006 etc)
- Server-send-first protocols
- Better support for calling pod IP directly

Reference:
https://istio.io/latest/docs/ops/deployment/requirements/#pod-requirements

# Ambient Cost Saving Analysis

| | Reserved vCPU | Reserved Memory GB | # of nodes estimated (n2-standard-16) | Cost / Month |
|---|---|---|---|---|
| **Baseline** | 165 | 115 | 12 | $6319.46 |
| **Sidecars** | 210 | 174 | 15 | $8591.34 |
| **Ambient (sidecarless)** | 174 | 148 | 12 | $6319.46 |
| **Ambient + Waypoint Proxy** | 184 | 161 | 13 | $7455.40 |

solo.io

From https://github.com/solo-io/service-mesh-for-less-blog using Google cloud pricing calculator

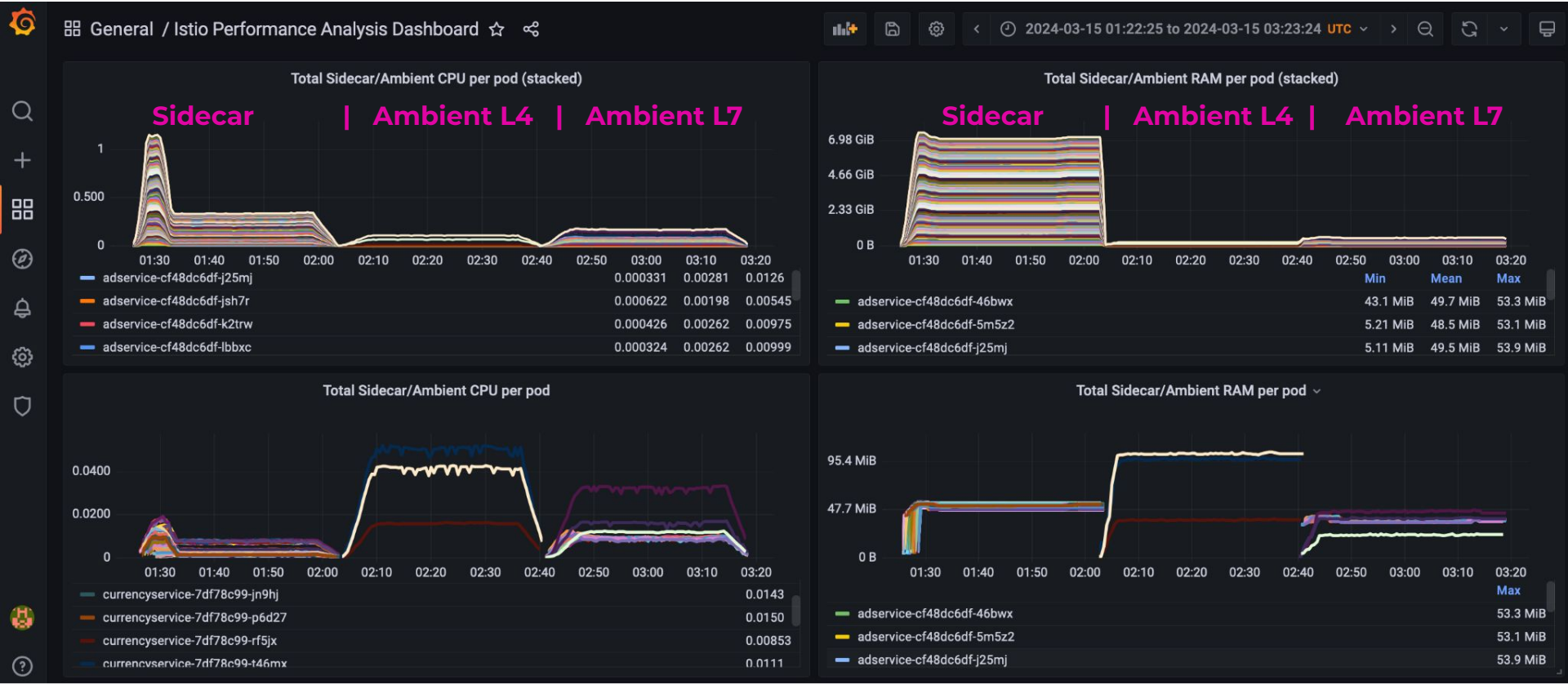
**“The introduction of Istio's ambient mode has significantly simplified management and reduced the size of our Kubernetes cluster nodes by approximately 20%.”**

**Saarko Eilers**, Infrastructure Operations Manager at EISST International Ltd

# Grafana dashboard


~150 services, ~150 pods across 12 namespaces

# Grafana dashboard



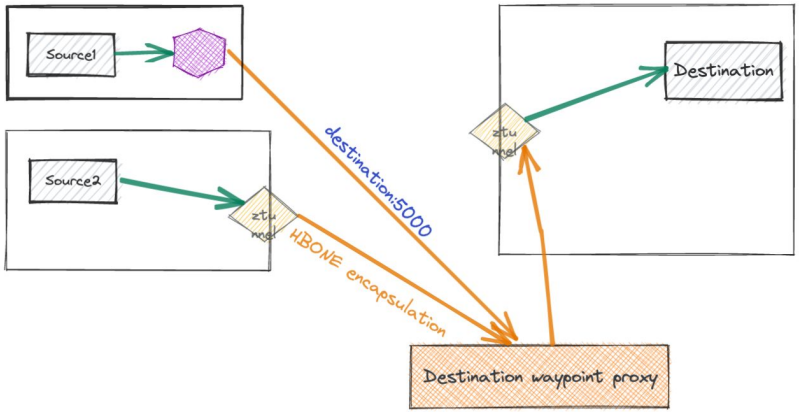

~150 services, ~150 pods across 12 namespaces

# Demo

# What about sidecars?

# What About Sidecars

- Sidecars are here to stay!
- Source side specific configuration

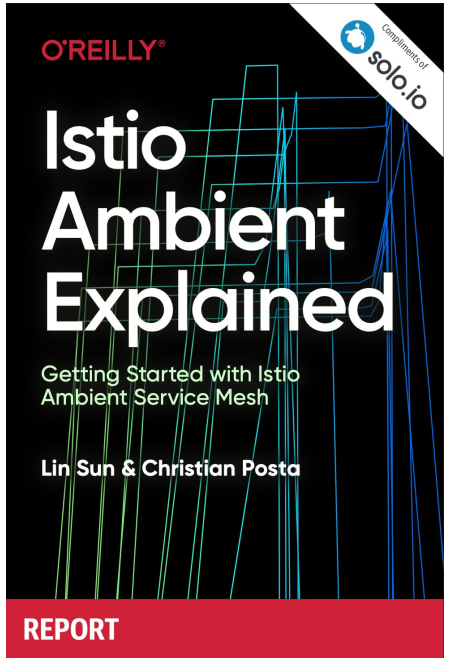


# Summary

- Sidecar-less Istio (ambient) is the new data plane mode.
- Ztunnel and Waypoint are designed to scale with minimal configurations.
- Ambient is designed to simplify mTLS and many other mesh functions.

# Call To Action

- Try Istio ambient 1.22
- Engage with us in Istio community
  - Slack (#ambient channel)
  - GitHub



# More Resources

- Get started with ambient
- Understand Istio CNI for ambient
- Ambient's architecture guide
- eBPF for service mesh?

FREE Ambient tutorial with environment