
KubeCon
CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022
TiKV
TiKV
HELM

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Istio Today and Tomorrow
Sidecars and Beyond

Lin Sun, Solo.io
Mitch Connors, Google

#KubeCon @linsun_unc @mitchashimself

Lin Sun

Director of Open Source, Solo.io

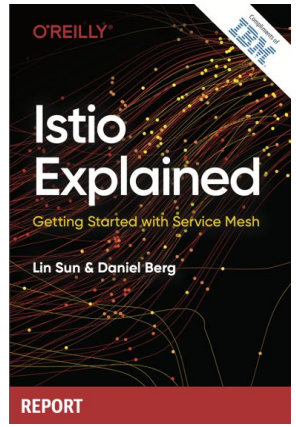
@linsun_unc

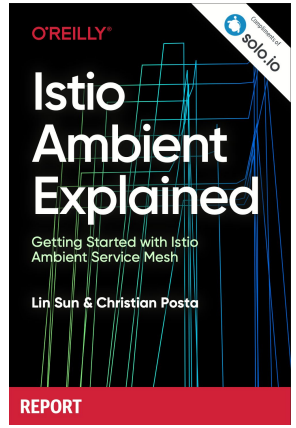
lin.sun@solo.io

linkedin.com/pub/lin-sun/1/…

6500+ contributions

TOC & Steering Member





Ambassador

Title

KubeCon CloudNativeCon North America 2022

Mitch Connors

Software Engineer, Google

@mitchashimself

@therealmitchconnors

linkedin.com/mitchconnors

Joined 2018

TOC Member

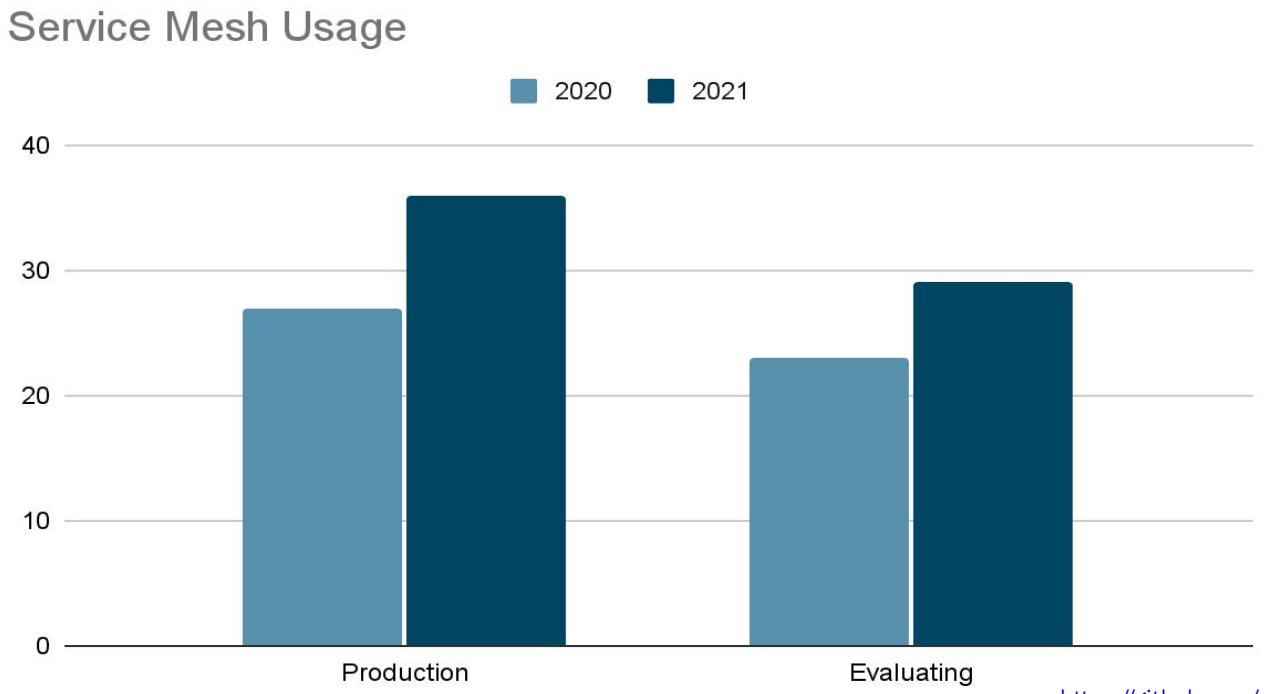
1x16,500 Line Contribution

Kubernetes Podcast from Google

Episode #177

Service Mesh Usage

Service Mesh production usage rose from 27% to 36% from 2020 to 2021 based on CNCF Annual Survey results.



https://github.com/cncf/surveys/tree/main/cloudnative

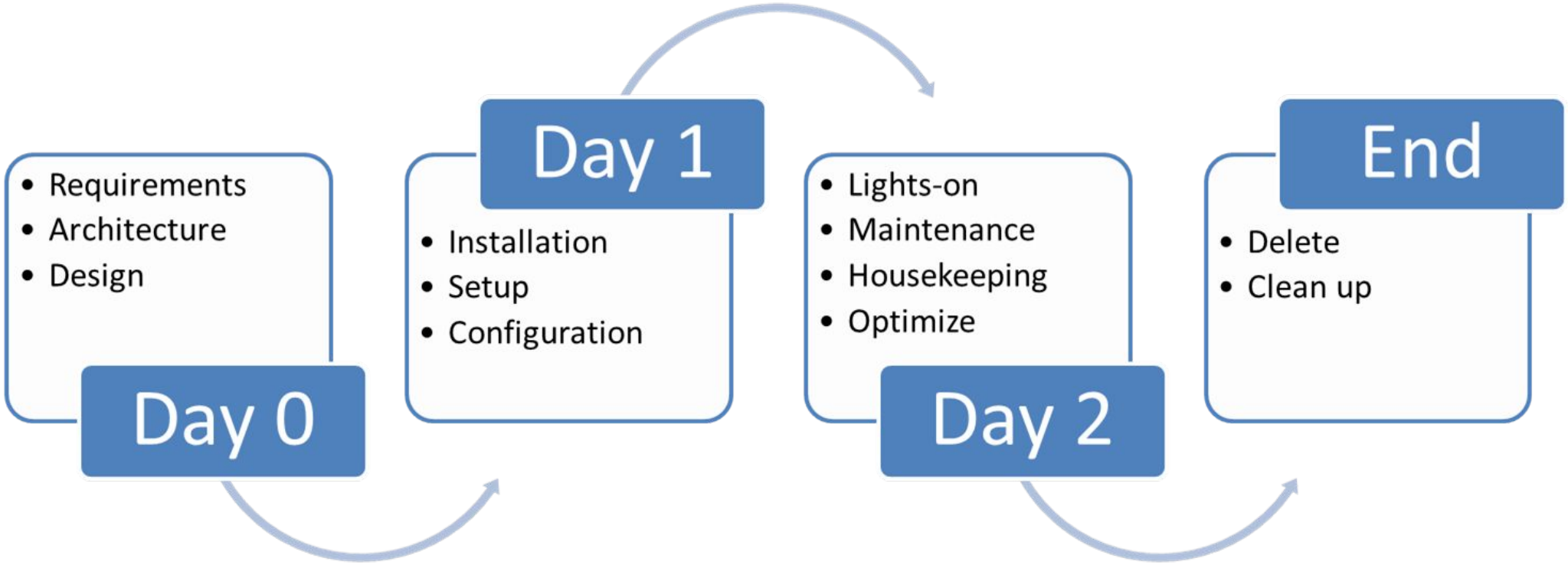
The Istio Community

- 397 Community Members (and growing)!
- 50 Maintainers
- 7 Working Groups (15 Leads)
- 435 Contributing Developers
- 124 Contributing Companies

Looking Back: Roadmap Check In

- Stabilize & Refine Istio's API Surface
- Improving Upgrades and Troubleshooting
- Improved Extensibility
- Expanding Istio's Reach
- Security Hardening
- Upgrade Automation

Day 2 Operations



https://dzone.com/articles/defining-day-2-operations

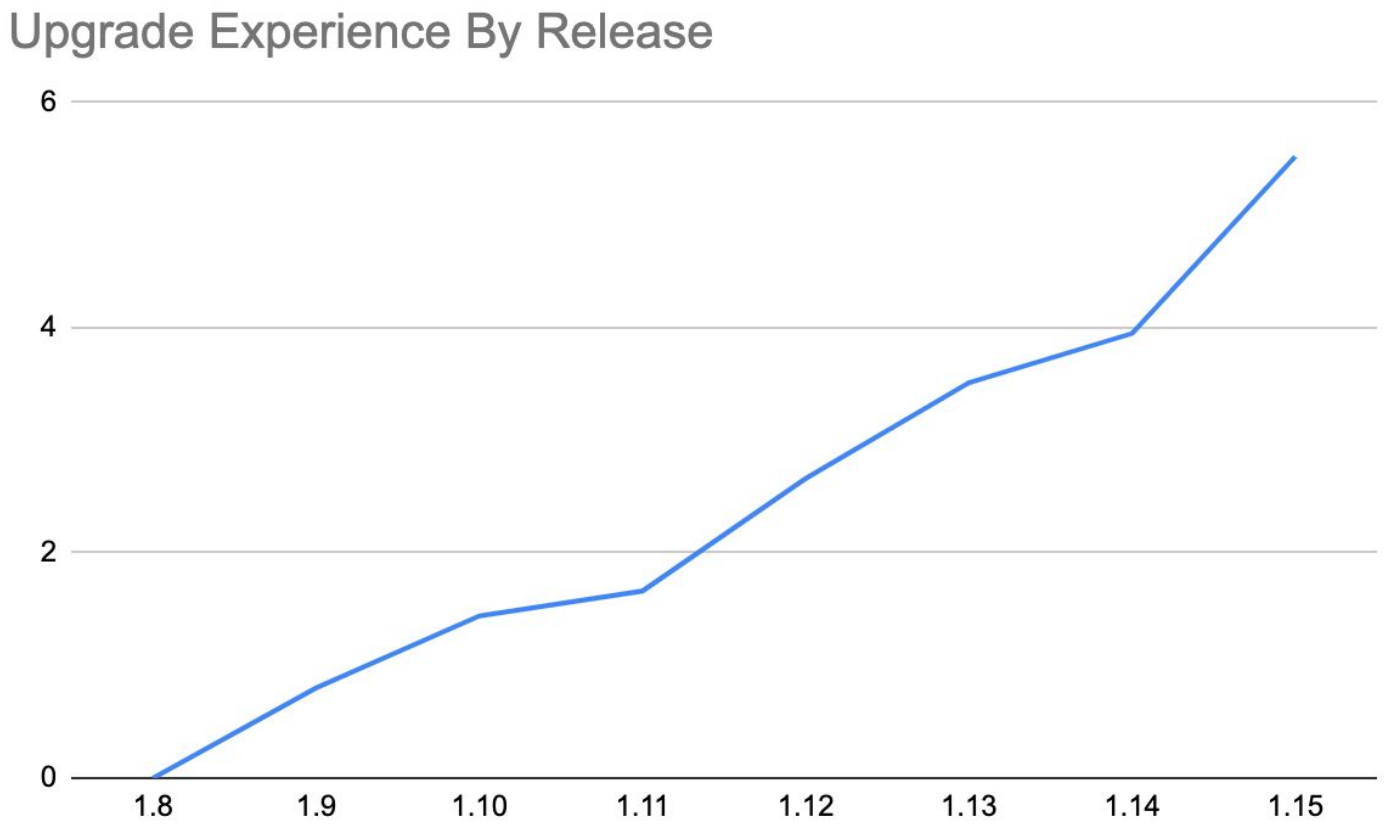
How Have We Done?

Stabilizing APIs

- 1.13
  - WorkloadGroup -> Beta
  - Authz Dry Run -> Alpha
- 1.15
  - Istioctl Uninstall -> Beta
- 1.16 (ETA November)
  - JWT Claim Based Routing -> Alpha
  - External Authz -> Beta

How Have We Done?

Improved Upgrades



How Have We Done?

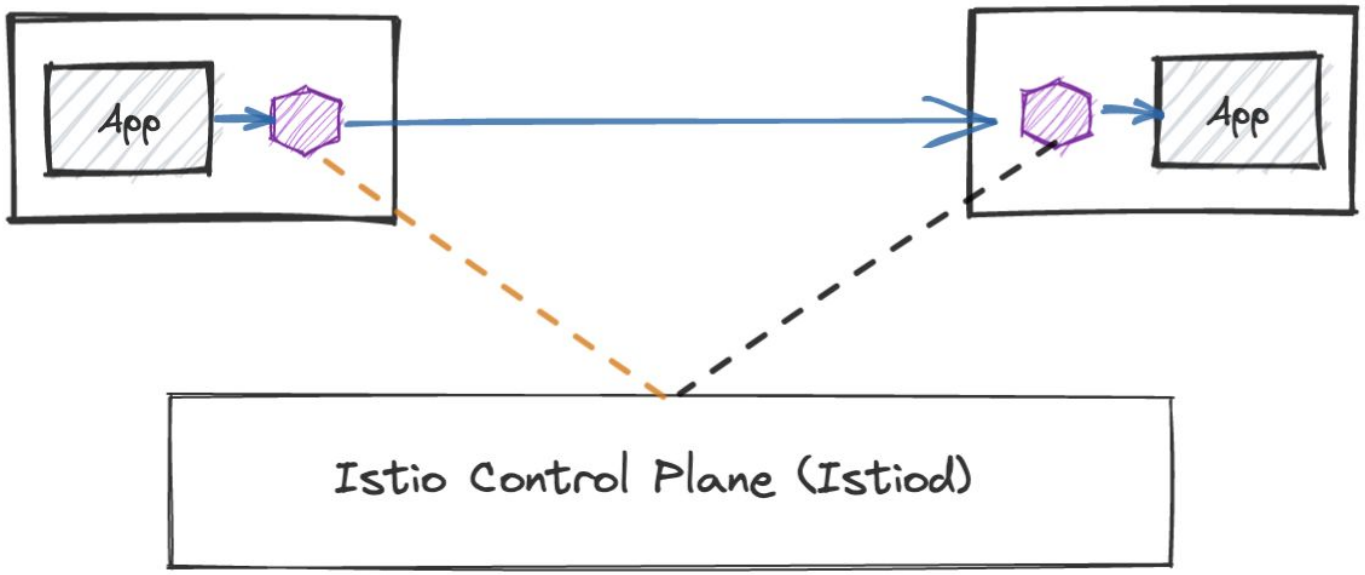
Other Progress

- Custom Auth
- ARM Support
- SBOMs for 1.13+, headed for SLSA 1
- Flux Upgrade Integration

One More Thing…

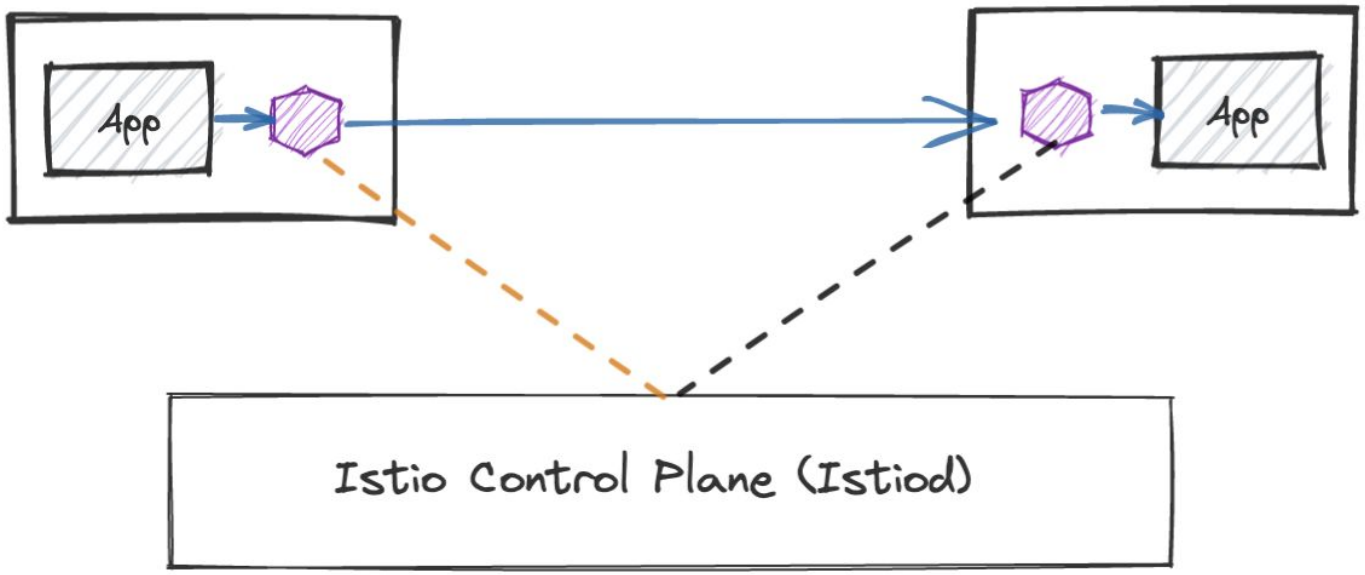
Challenges With Sidecars - Transparency

- Require injection of sidecars
- 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
- Most users adopt service mesh because of mTLS among applications
- All-or-nothing injection of sidecars
  - Overprovision of resources



Ambient Mesh Announced!

KubeCon CloudNativeCon North America 2022

Sep 7, 2022

Ambient Mesh Security Deep Dive

Digging into the security implications of the recently announced Istio ambient mesh, a sidecar-less data plane for Istio.

By Ethan Jackson - Google, Yuval Kohavi - Solo.io, Justin Pettit - Google, Christian Posta - Solo.io

---

Sep 7, 2022

Get Started with Istio Ambient Mesh

Step by step guide to get started with Istio ambient mesh.

By Lin Sun - Solo.io, John Howard - Google

Sidecar-less

Sep 7, 2022

Introducing Ambient Mesh

A new dataplane mode for Istio without sidecars.

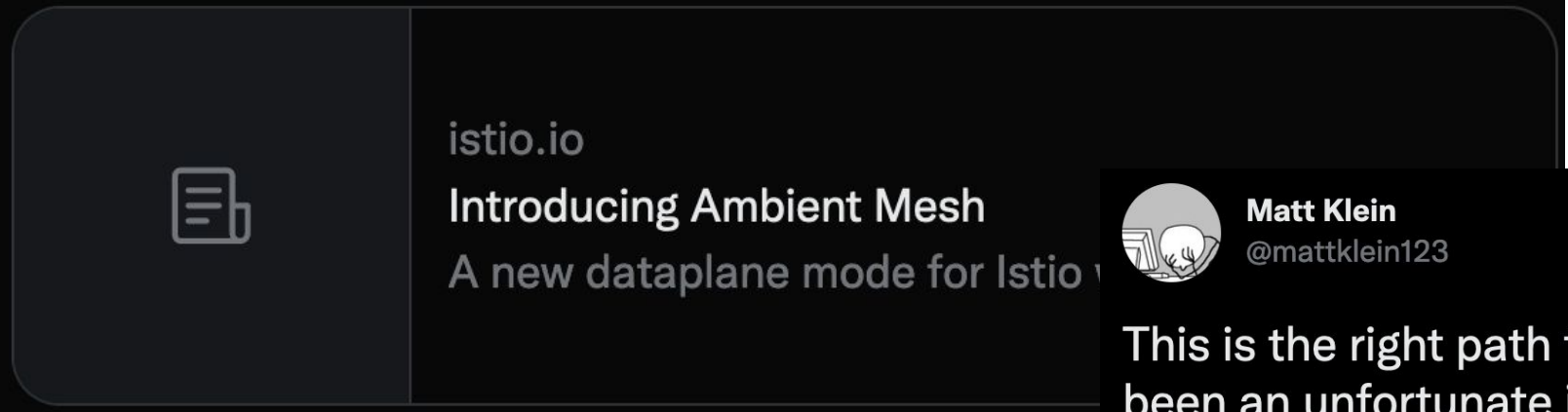
By John Howard - Google, Ethan J. Jackson - Google, Yuval Kohavi - Solo.io, Idit Levine - Solo.io, Justin Pettit - Google, Lin Sun - Solo.io

Istio

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.

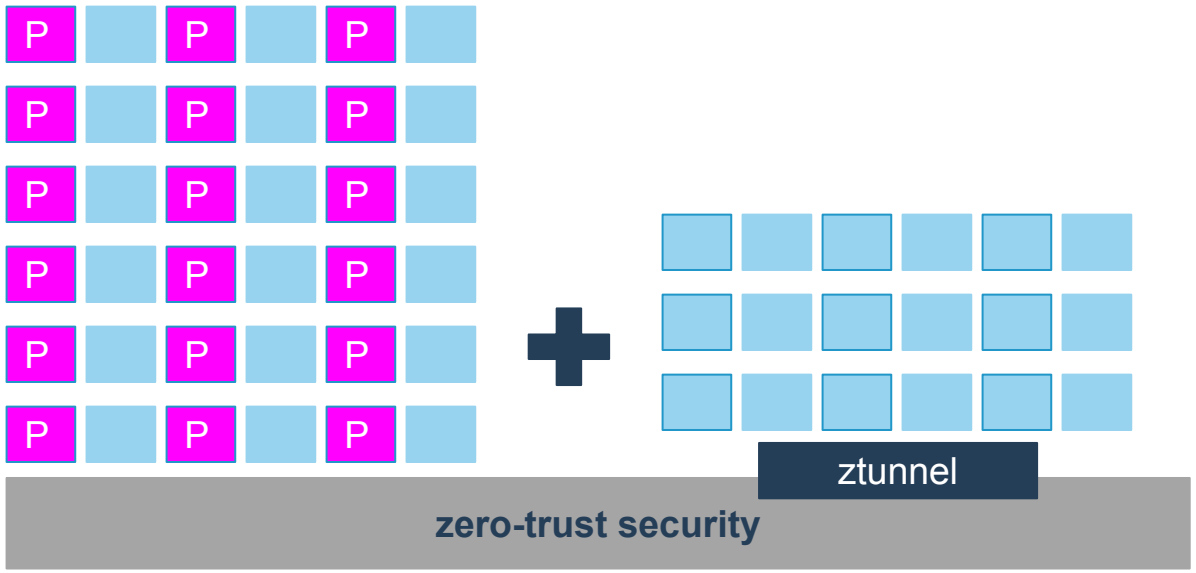
> **Istio** @IstioMesh · Sep 7
> Very special day for the Istio community, check out Istio ambient mesh - a new dataplane mode for Istio without sidecars: istio.io/latest/blog/20...

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

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

What is Istio Ambient Mesh?

Introduce per-node architecture ***only*** for
secure overlay layer



Istio Sidecar Data Plane
1 Pod/Container = 1 Proxy

Ambient Mesh Data Plane
1 Node = 1 ztunnel

Business Owner

- Reduced Compute Cost

Platform Team

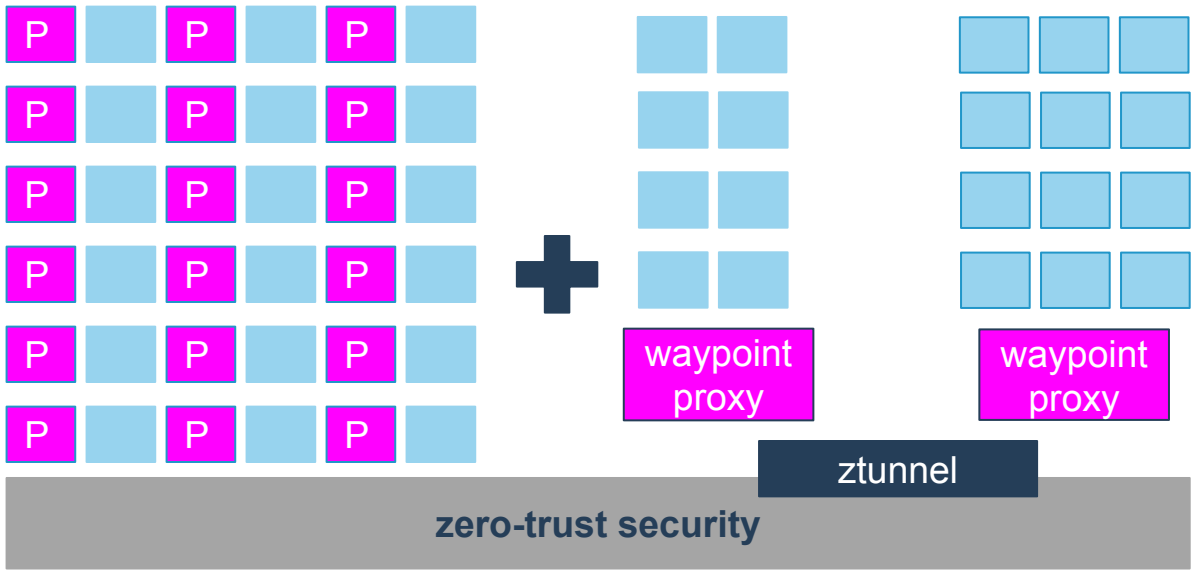
- Simplified Operations
- Reduced Maintenance

Application Team

- Mesh is transparent to Apps
- Applications won't break

What is Istio Ambient Mesh?

Introduce proxy per-service account architecture for
L7 processing layer



Istio Sidecar Data Plane
1 Pod/Container = 1 Proxy

Ambient Mesh Data Plane
1 Service Account/Namespace = 1 Waypoint Proxy

Business Owner

- Reduced Compute Cost

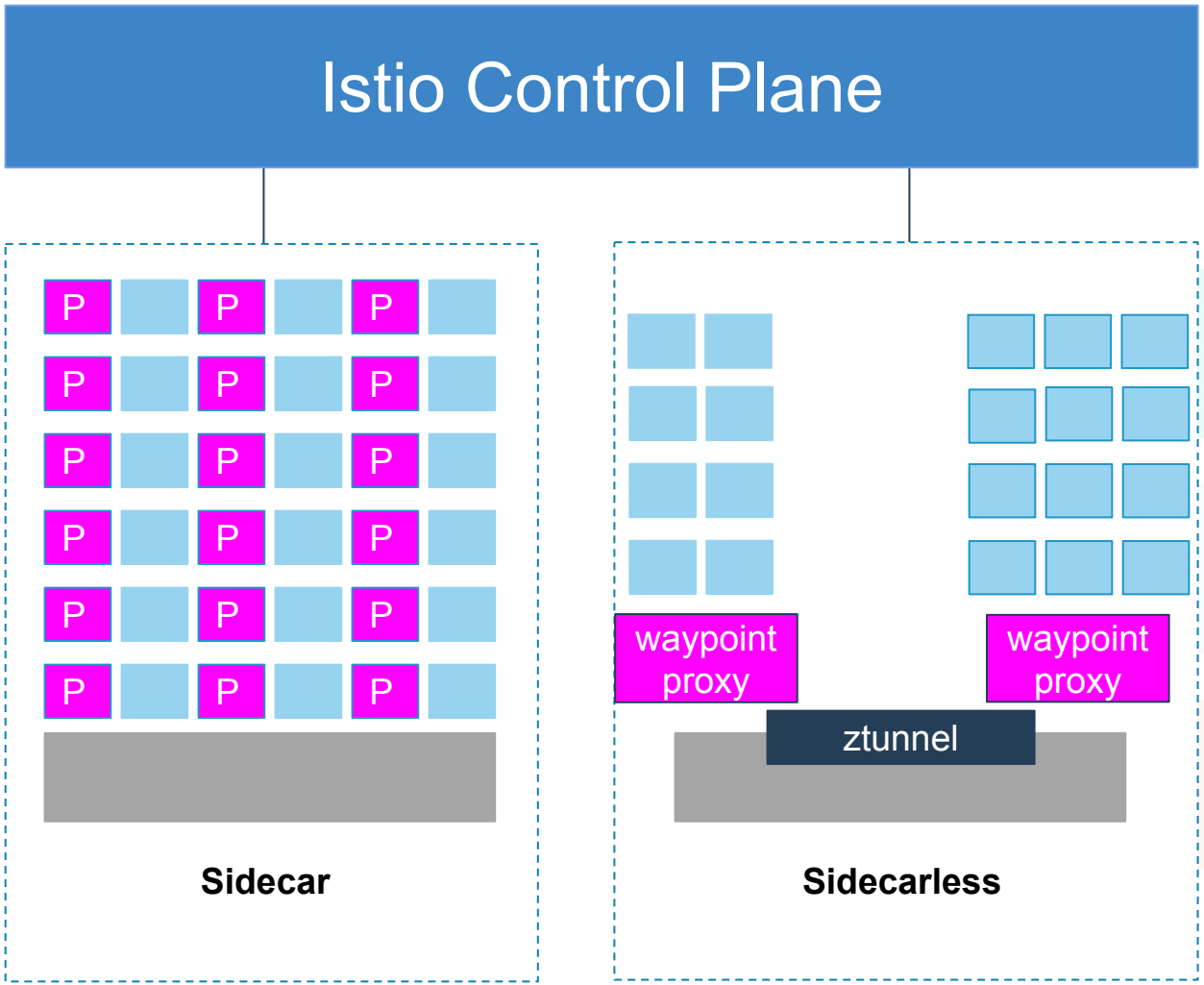
Platform Team

- Simplified Operations
- Reduced Maintenance

Application Team

- Mesh is transparent to Apps
- Applications won't break

Sidecar & Sidecarless Co-exist!



Cost Flexibility

Operational Flexibility

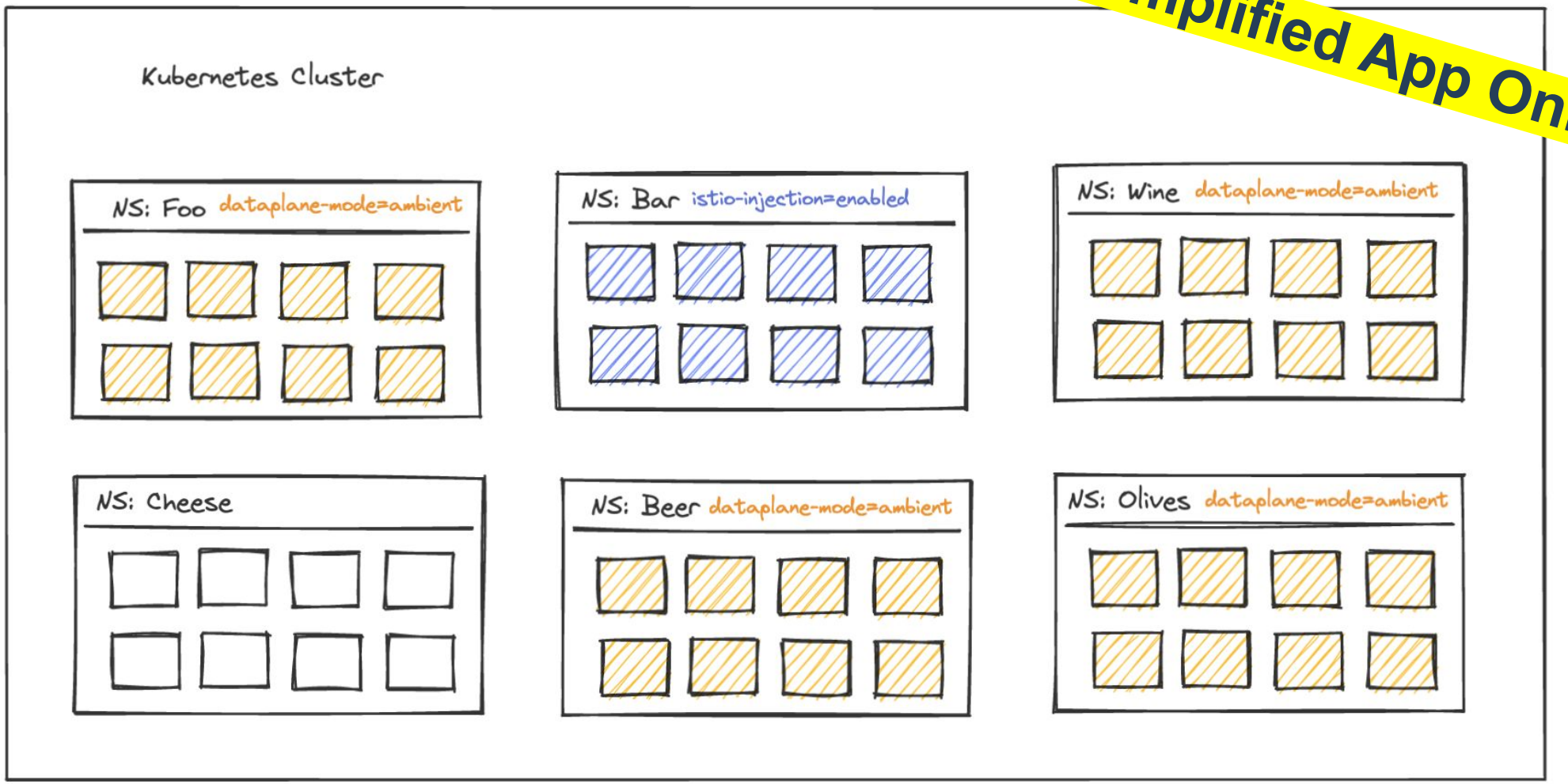
Performance Flexibility

Install Ambient

- Ambient profile
  - istioctl
  - Istio operator controller
  - Helm (?)
- We expect **ambient** profile becomes the **default** profile in Istio when it is production ready.
- What is installed?
  - Istio CNI plugin (required component for ambient, as DaemonSet)
  - ztunnel (as DaemonSet)
  - Istiod
  - Istio ingress gateway

Including Applications in Ambient

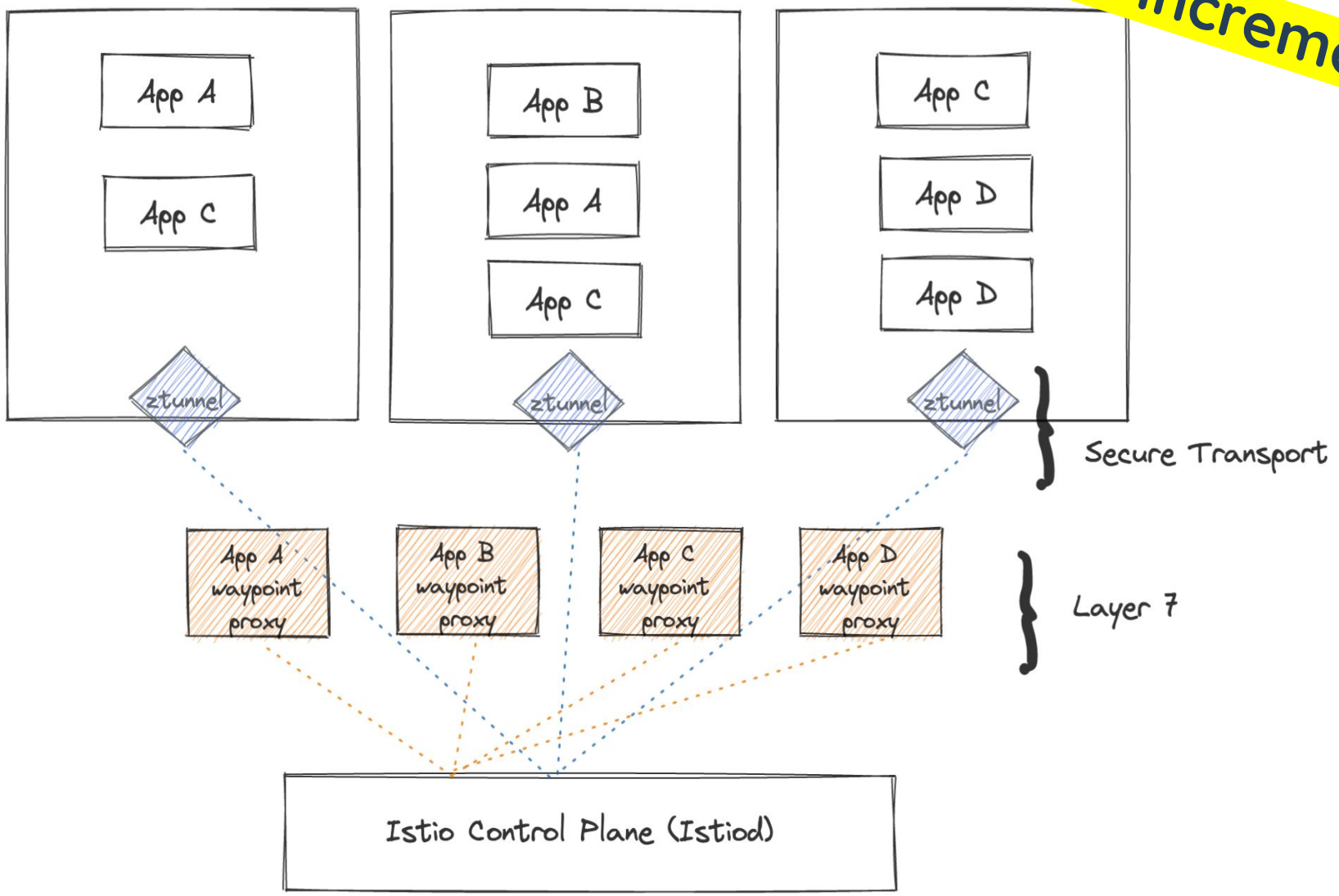
Simplified App Onboarding



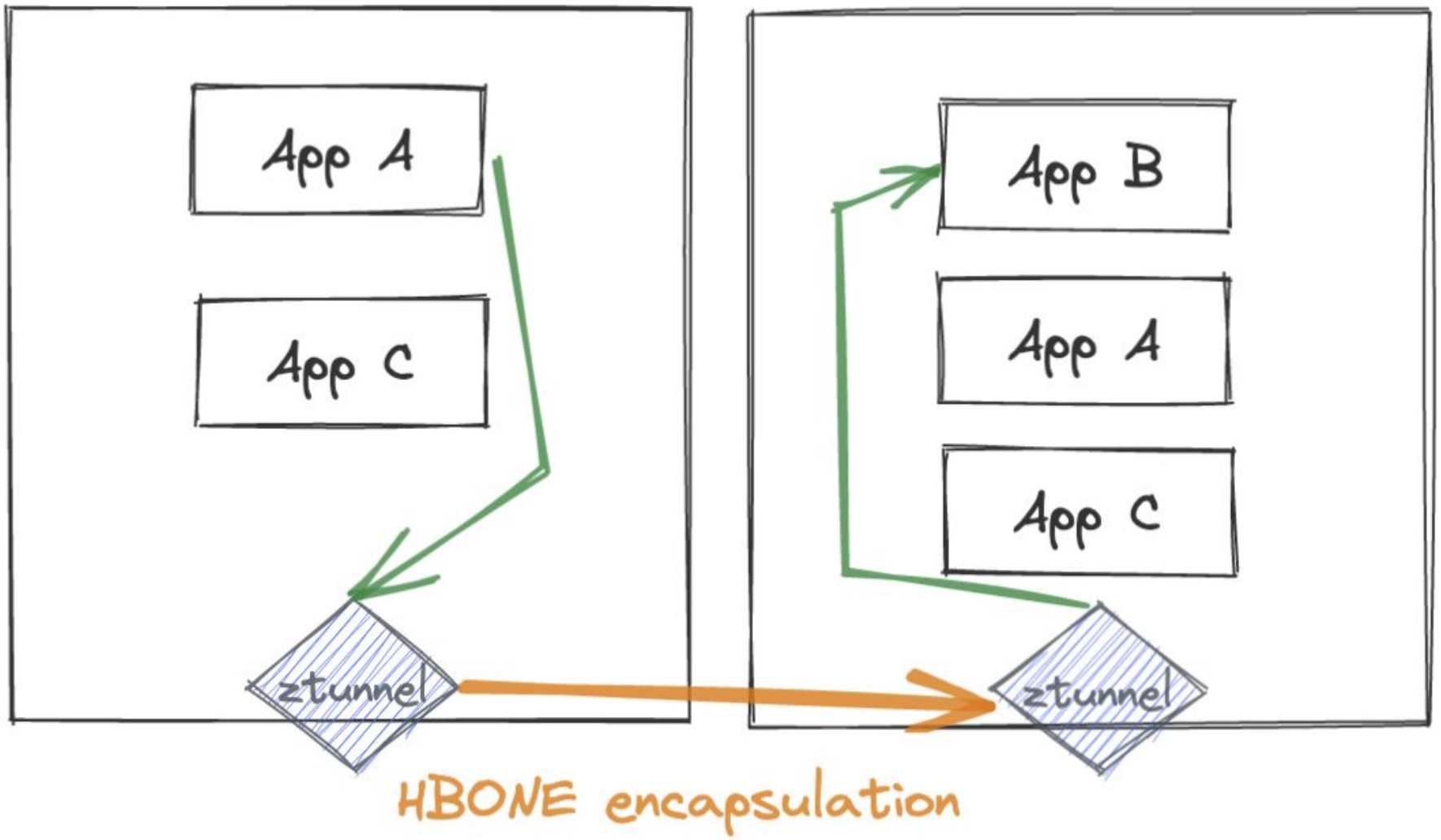
kubectl label namespace foo istio.io/dataplane-mode=ambient

Ambient Architecture - Two Layers

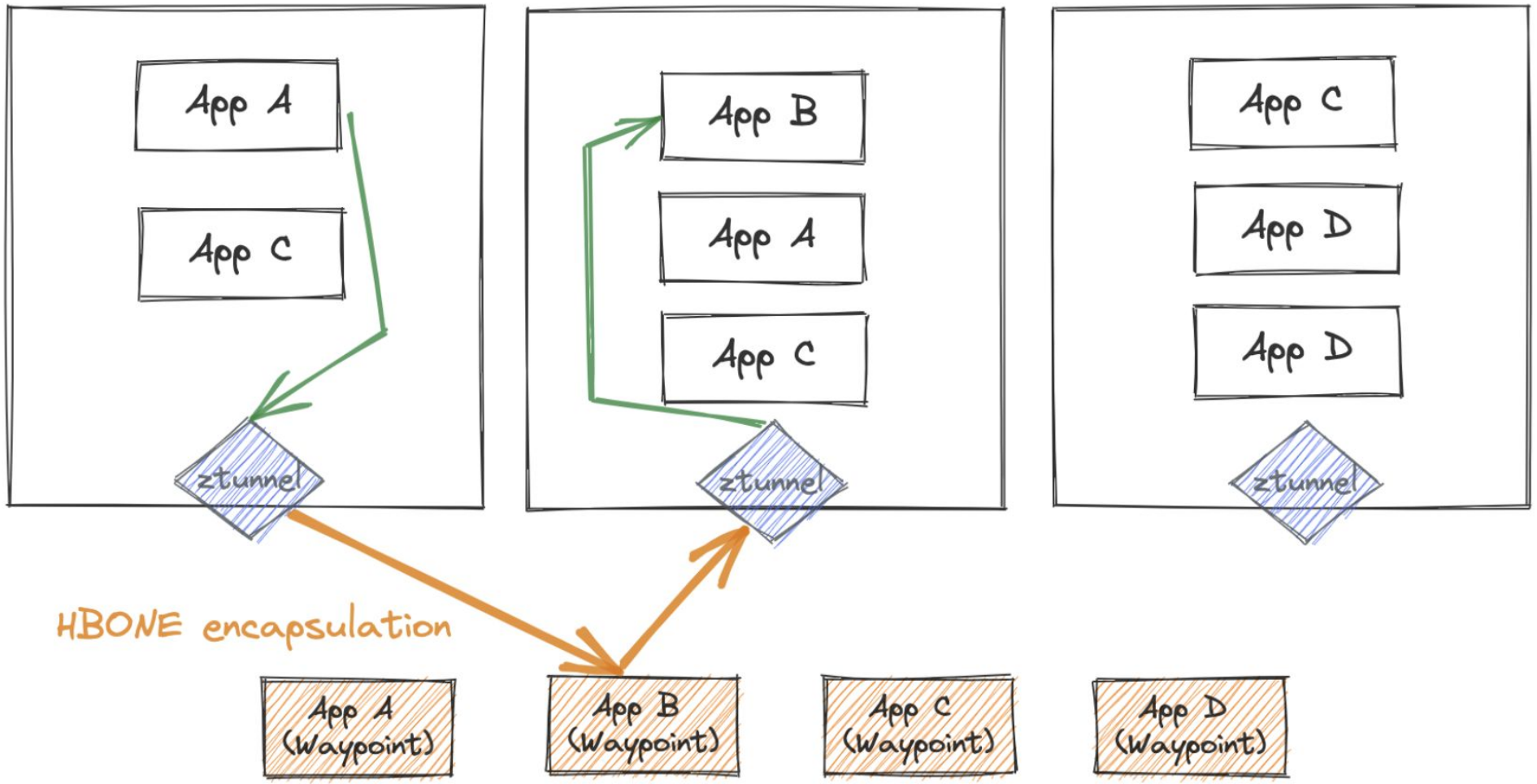
Better Incremental Adoption



Ambient Architecture - Secure Overlay Layer



Ambient Architecture - L7 Processing Layer



Each namespace/identity has its own L7 proxies; no multi-tenant proxies

Better Incremental Adoption

L7 Processing Layer

All features of the Secure Overlay plus…

- **Traffic Mgmt:** HTTP routing & load balancing, Circuit breaking, Rate limiting, Fault injection, Retry, Timeouts, …
- **Security:** Rich authorization policies
- **Observability:** HTTP metrics, Access Logging, Tracing

Secure Overlay Layer

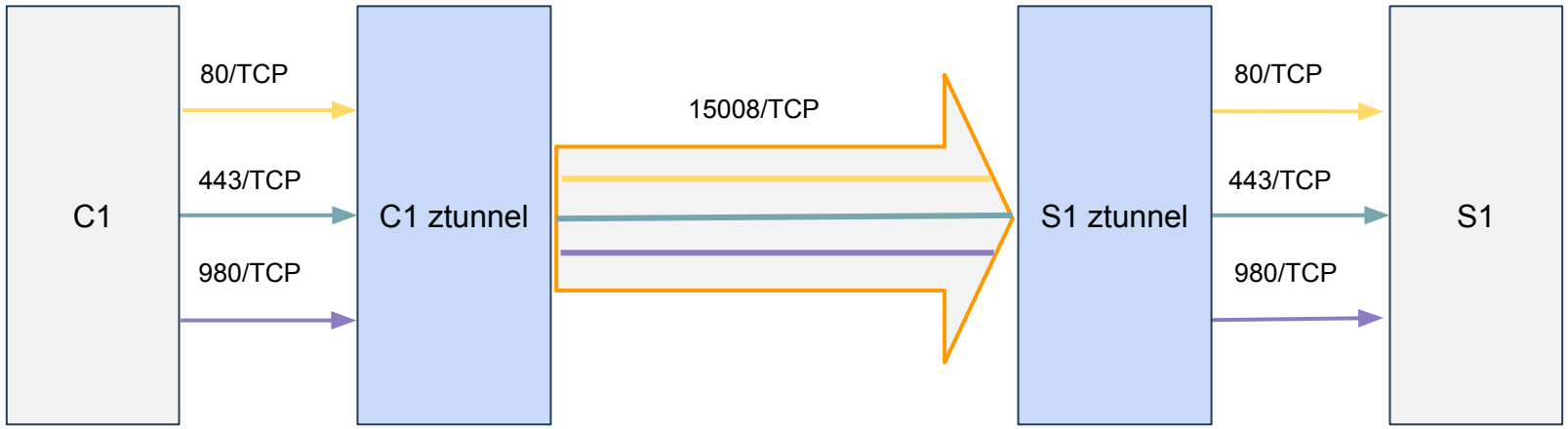
Streamlined, low resource, high performance with zero trust

- **Traffic Mgmt:** TCP Routing
- **Security:** mTLS tunneling, Simple authorization policies
- **Observability:** TCP metrics & logging

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

HTTP Based Overlay Network (HBONE)

- All traffic tunneled through a single mTLS connection using HTTP Connect
  - Per source and destination service accounts pair
  - Fixes server-speaks-first protocols for Permissive mTLS
  - Amortizes cost of mTLS handshakes over multiple connections
  - Doesn't require sniffing or metadata exchange hacks
  - Simplifies network policies, since Istio will use a single port
- Decouple mTLS encryption from the application



Security

- **Multi-tenancy: Secure overlay layer**
  - Not designed to be extensible
  - Minimal CVEs from L4 Envoy today
  - Ztunnel can only send CSR for co-located pods - lower blast radius if compromised.
- **Not Multi-tenancy: L7 processing layer**
  - Designed to be extensible, for example Wasm extensions
  - Eliminate noisy neighbor, cost attribution issues with multi-tenancy L7 Envoy (Cilium service mesh)
- What if your **application is compromised**?

KubeCon | CloudNativeCon North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Thank You!

Please scan the QR Code above to leave feedback on this session

#KubeCon @linsun_unc @mitchashimself