# Istio Day

NORTH AMERICA

Istio Day
NORTH AMERICA

# Vanishing Point

## Reimagining the Meaning of a Mesh

*Justin Pettit, Google*
*Mitch Connors, Microsoft*

# What is a Service Mesh?

ServiceMeshCon 2019

# Title

Istio Day NORTH AMERICA

**November 12, 2024**
**Salt Lake City**

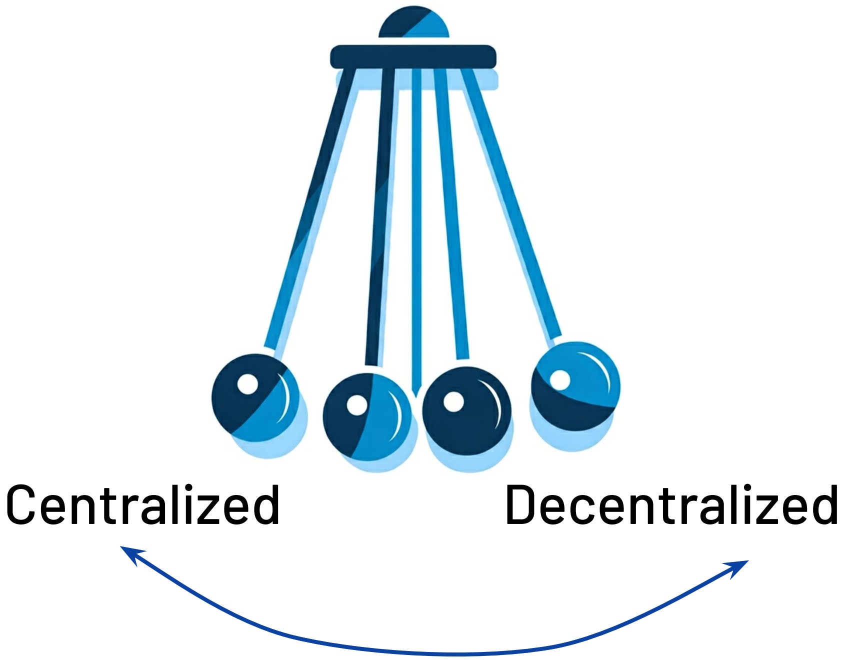
**Mitch Connors**
Software Engineer
*Microsoft*

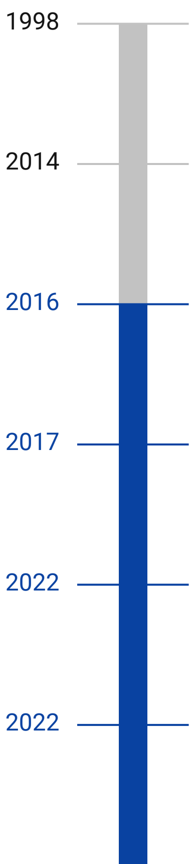
**Justin Pettit**
Software Engineer
*Google*

## Agenda

- What is a Service Mesh?
- The evolution of the Service Mesh
- The role of infrastructure
- A truly Ambient Mesh
- Other Vanishing Acts
- What is a Service Mesh?

# The Evolution of the Service Mesh





1998 **BIG-IP**

Centralized Hardware Proxy providing L7 routing and load balancing

2014 **Spring Boot**

Decentralized Software Proxy integrated at the library level

2016 **Linkerd 1.0**

Partially Centralized Software Proxy for Kubernetes, running one proxy per node.

2017 **Istio**

Decentralized Software Proxy for Kubernetes running one proxy per pod.

2022 **Cilium Service Mesh**

Partially centralized kernel proxy, running one per node

2022 **Istio Ambient Mode**

Hybrid Software Proxy for Kubernetes, combining per-node and per-app semantics

# The Role of Infrastructure

- Infrastructure is critical, but you don’t want to spend much time thinking about it
- Any time you spend thinking about it is a probably a bad day
- Needs to work well, and it’s not always immediately obvious if it has flaws
- Service mesh has not always lived up to the best view to infrastructure

# am·bi·ent

/ˈambēənt/

*adjective*

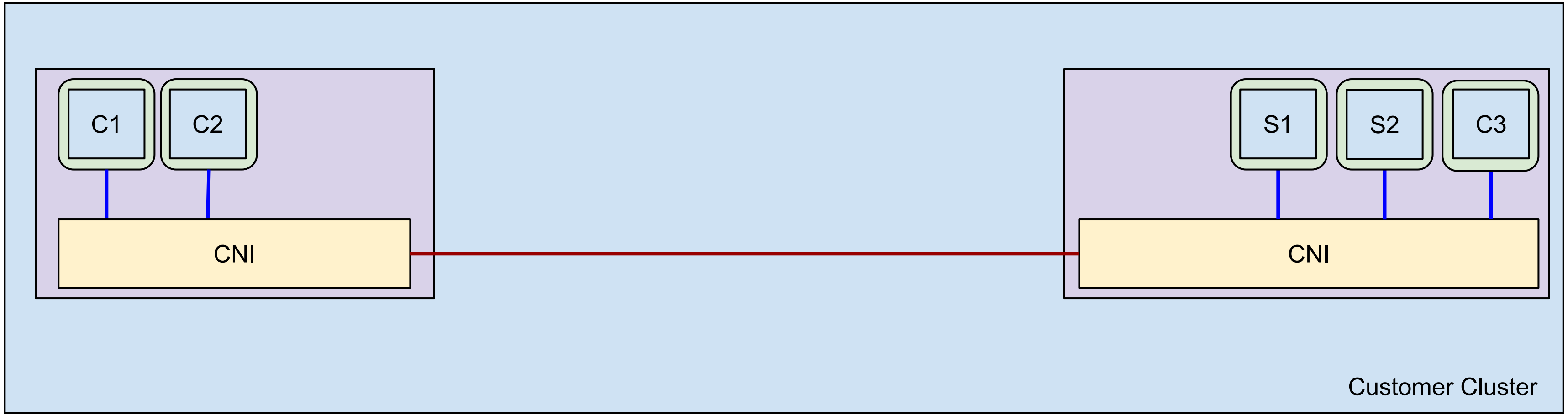
existing in the surrounding area

# Imagining a Truly Ambient Mesh

- Benefits of ambient mesh have been well covered
  - Savings of 90-98% in Memory and CPU Allocations
  - Reduced management complexity
  - Less invasive to workloads
- The reference implementation still requires an additional set of components that must be managed....can it be made even more *ambient*?

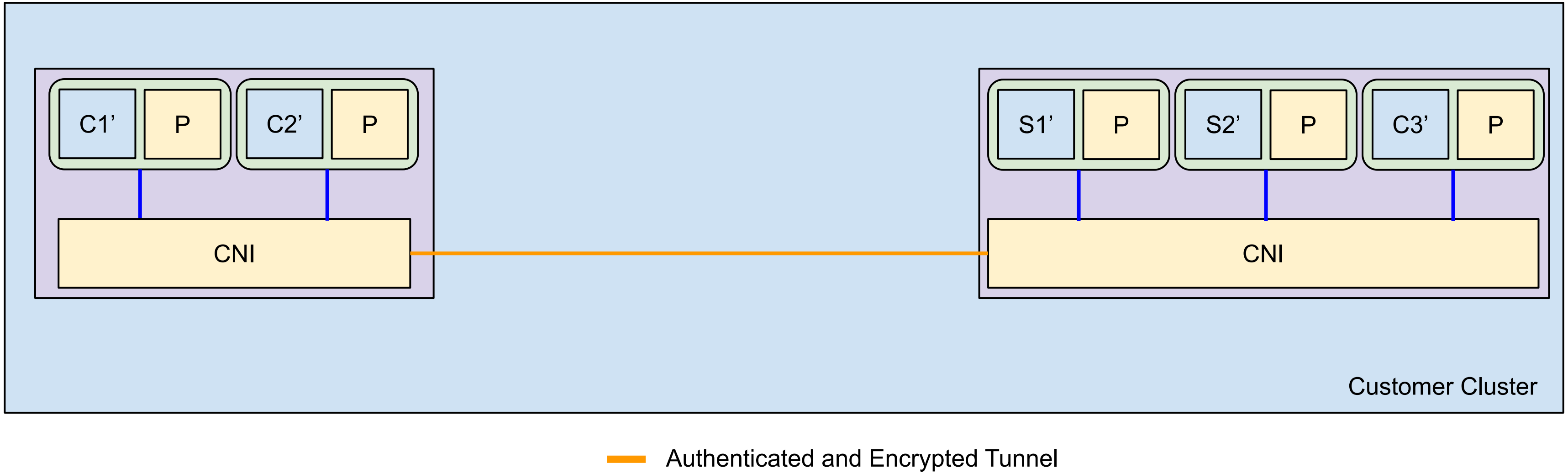
# Traditional Kubernetes Network

Istio Day
NORTH AMERICA



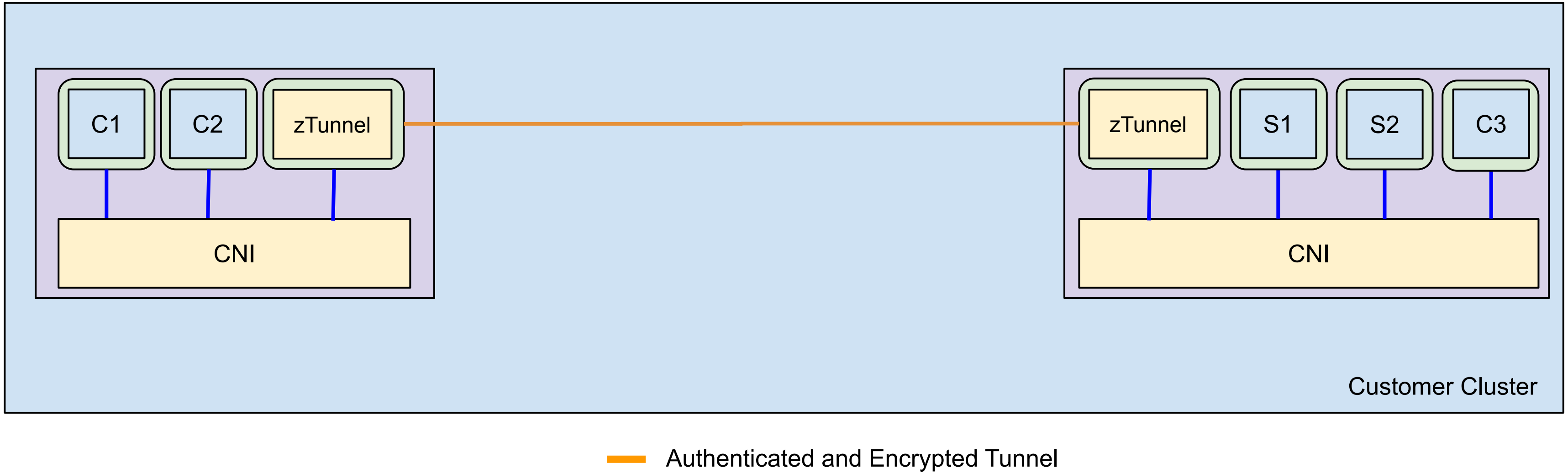
🟥 Plain Text Traffic

# Istio Sidecars

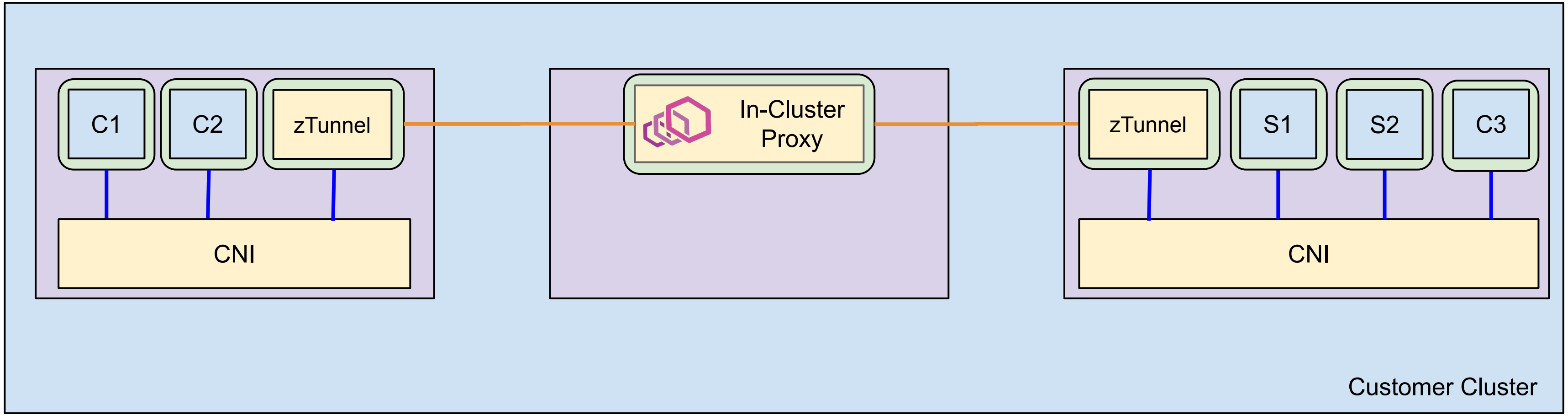


# Ambient Mesh Reference Architecture

Istio Day NORTH AMERICA



# Ambient Mesh Reference Architecture



C1

C2

zTunnel

CNI

In-Cluster Proxy

zTunnel

S1

S2

C3

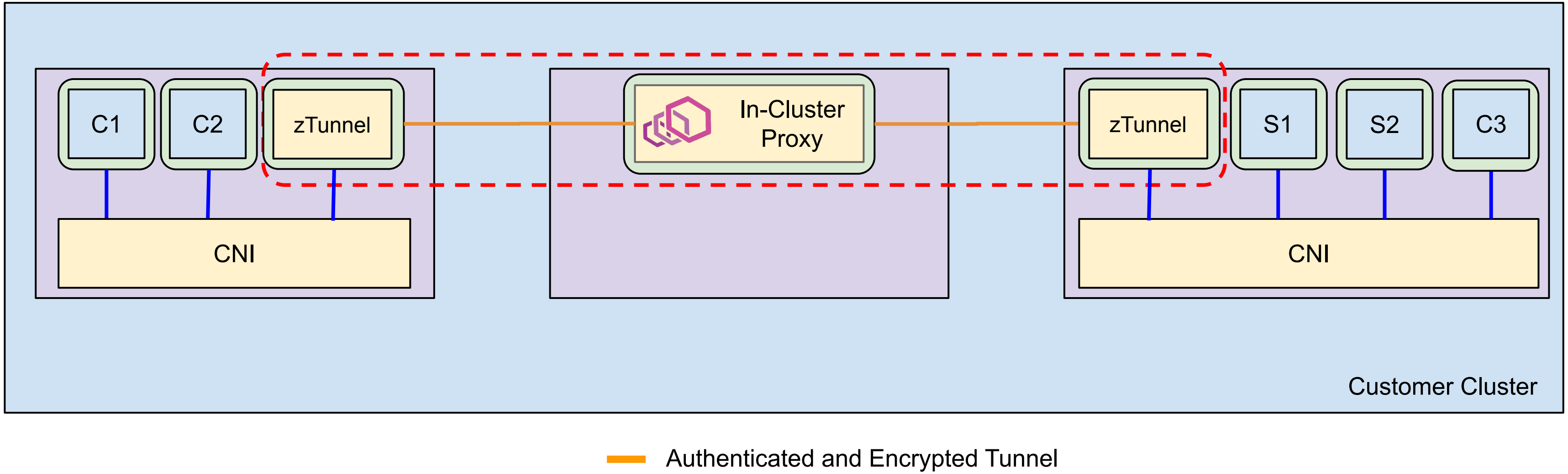
CNI

Customer Cluster

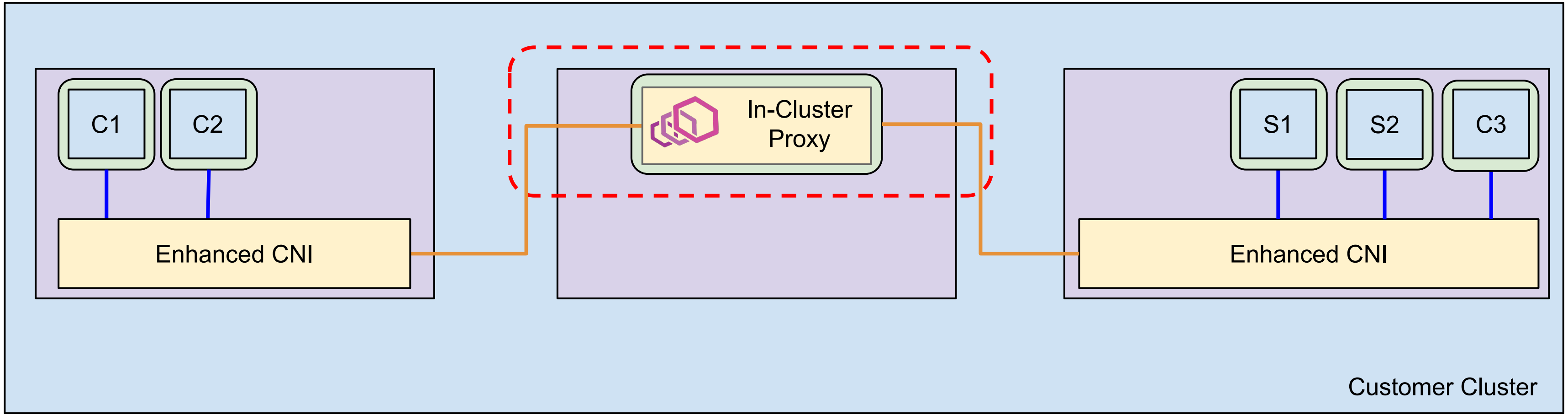
🟧 Authenticated and Encrypted Tunnel

# Ambient Mesh Reference Architecture

Istio Day
NORTH AMERICA

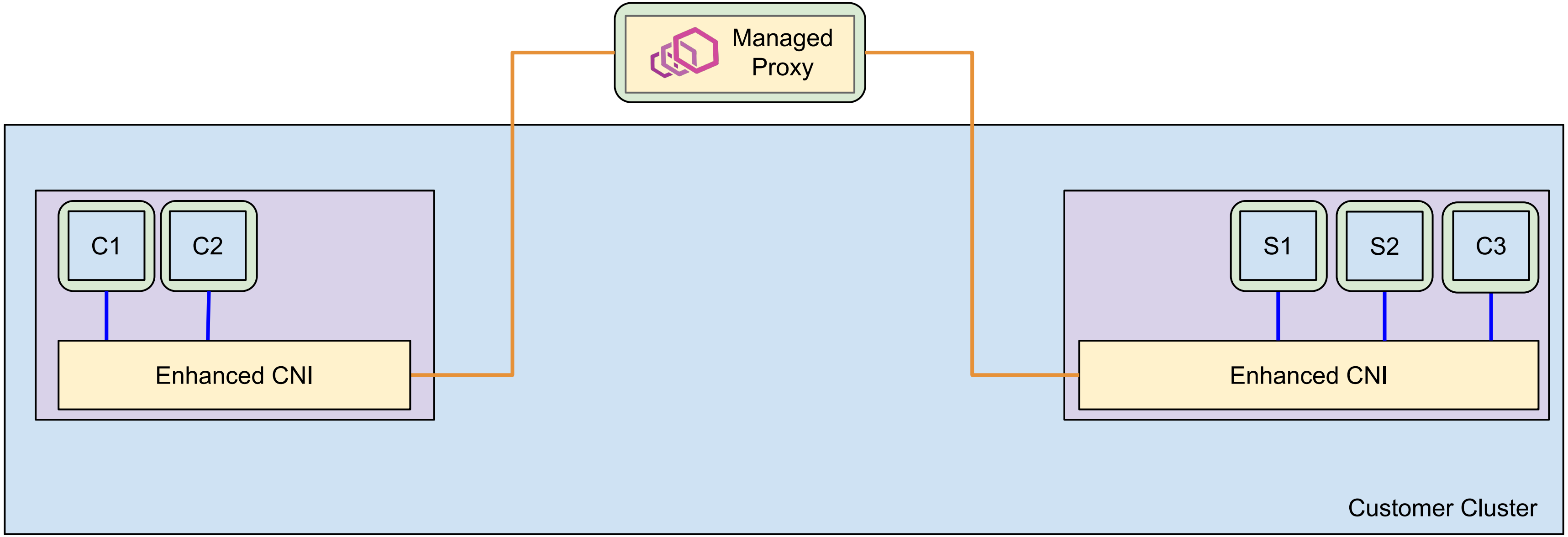


# Ambient Mesh with Enhanced CNI



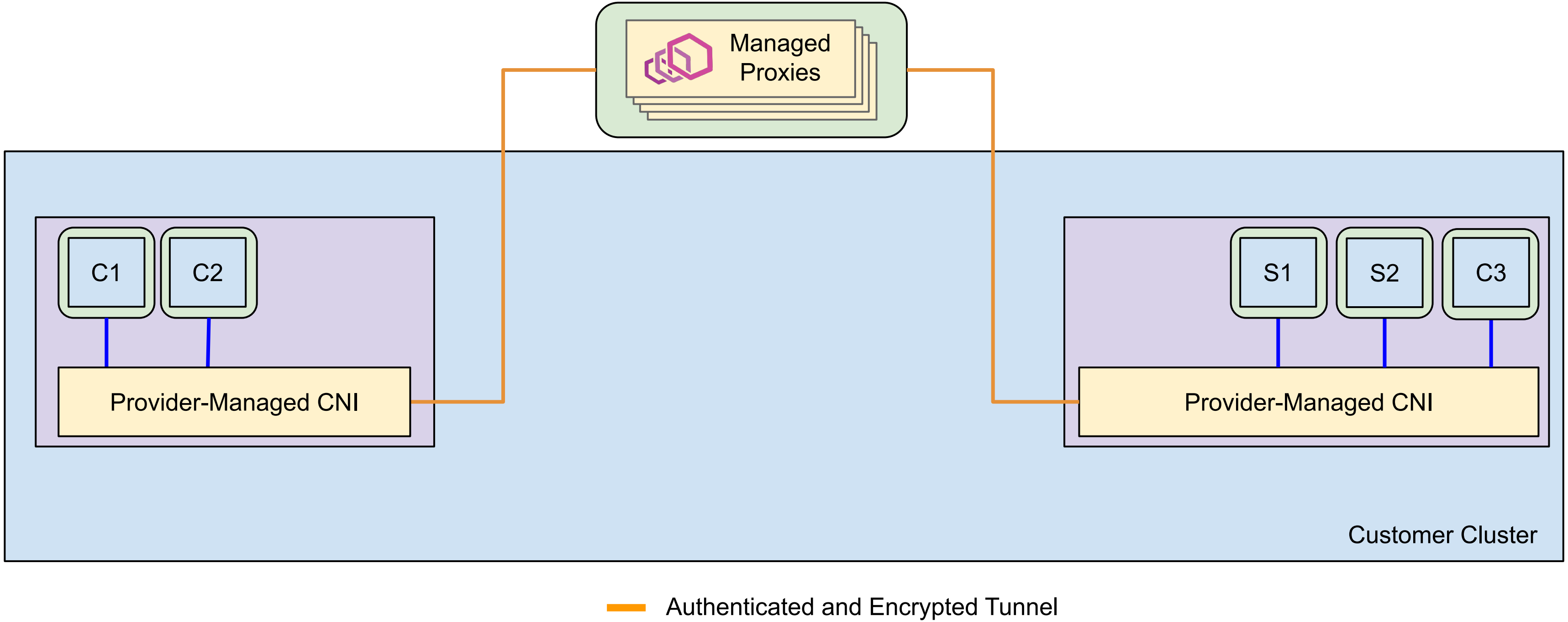
🟧 Authenticated and Encrypted Tunnel

# Ambient Mesh with Managed Proxy

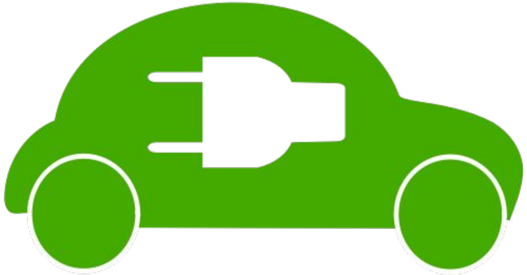


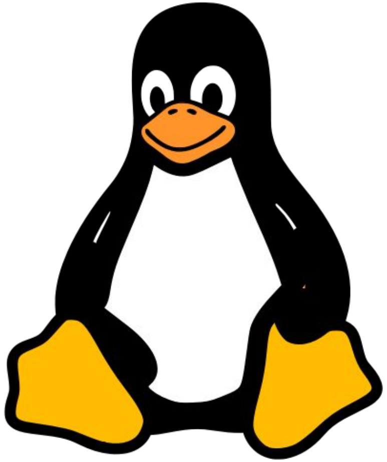
▬ Authenticated and Encrypted Tunnel

# Ambient Mesh with Provider-Managed Mesh



# Other Vanishing Acts





# What is a Service Mesh?

serv·ice mesh

*noun*

A set of APIs that consistently drive networking functionality across a variety of environments.

A good service mesh causes infrastructure to vanish.

Istio Day
NORTH AMERICA

# Thank You!

*Justin Pettit, Google*
*Mitch Connors, Microsoft*

# Abstract:

Ambient mesh introduces a new service mesh architecture without sidecars, but more than that, it gives us a way of thinking about the mesh as a set of API-driven network capabilities, distinct from the infrastructure used as an implementation. What if your mesh was truly ambient - if it was available and functional anywhere you have a network? This talk will show the state of the art of making Istio's implementation details - the ztunnel L4 secure overlay and the L7 waypoint proxy - vanish into the cloud infrastructure. We'll cover our efforts to standardize Istio's Ambient Mesh interfaces to allow alternative implementations that can leverage existing infrastructure, requiring fewer components, and less management overhead. We'll imagine alternative waypoint proxy implementations, such as managed load balancers, and non-Envoy proxies, and we'll discuss how adjacent projects like Cilium CNI are vanishing into the infrastructure, and how these parallel efforts align with one another.