Sidecarless service mesh.

No local TCP/IP stack.

What's left?

Solo.io

With you today

Kevin Dorosh

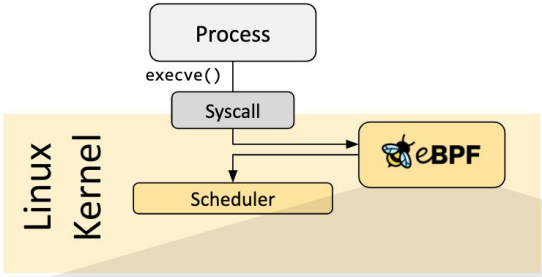
Tech Lead

Solo.io

 Copyright © 2022

solo.io

iptables & ePBF

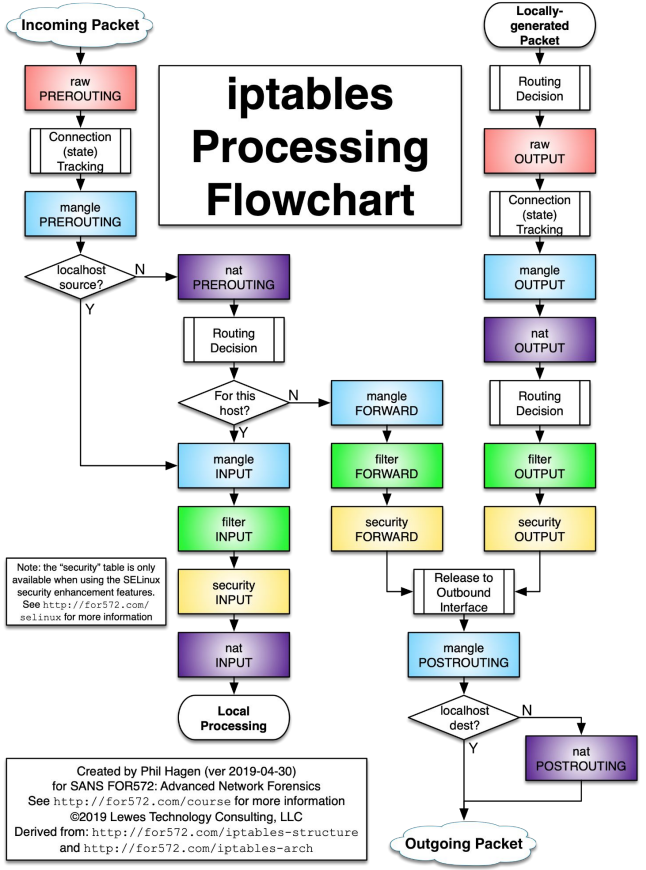



```c
int syscall__ret_execve(struct pt_regs *ctx)
{
        struct comm_event event = {
                .pid = bpf_get_current_pid_tgid() >> 32,
                .type = TYPE_RETURN,
        };

        bpf_get_current_comm(&event.comm, sizeof(event.comm));
        comm_events.perf_submit(ctx, &event, sizeof(event));

        return 0;
}
```

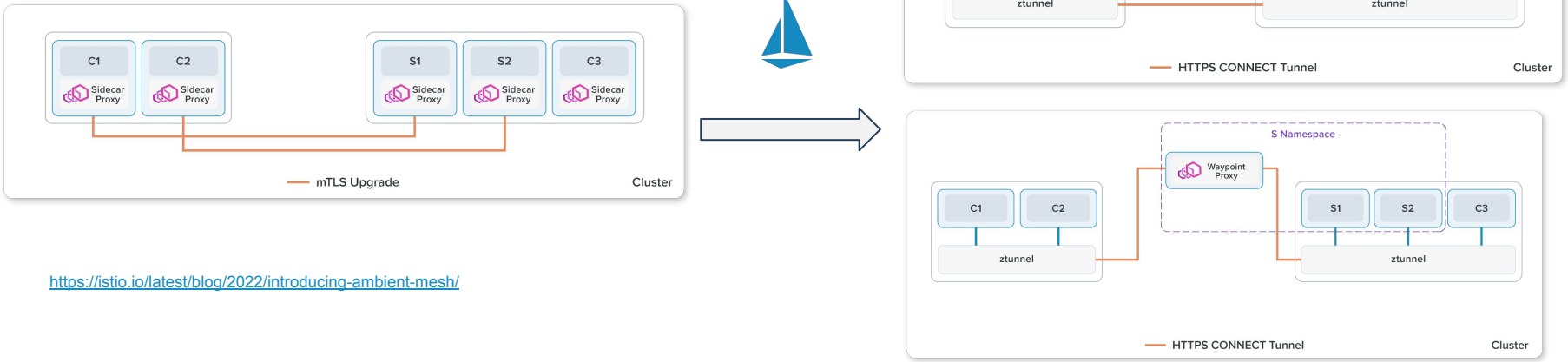
https://ebpf.io/what-is-ebpf/



solo.io

Sidecarless Architecture

- Traditional istio uses the sidecar model
- Ambient optimizes to improve performance and resource utilization
- Original src/dst IPs are preserved, so other IP-based network policy works unhindered



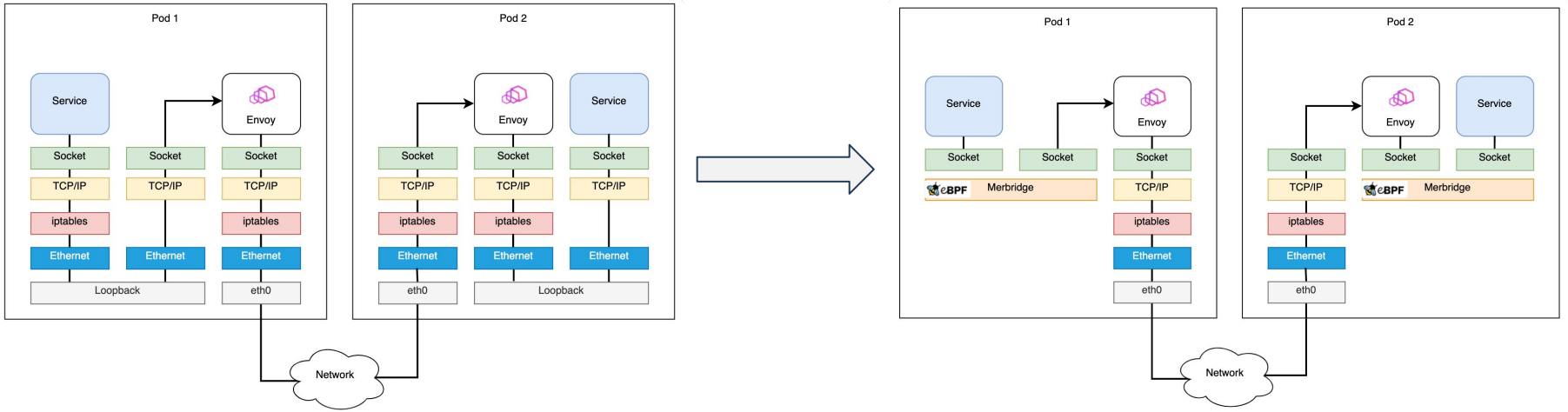
https://istio.io/latest/blog/2022/introducing-ambient-mesh/

 Copyright © 2022

solo.io

eBPF Acceleration

- Other optimizations include bypassing tcp/ip stack
- Requires linux kernel 5.7+
- Can fall back to iptables



https://istio.io/latest/blog/2022/merbridge/

 Copyright © 2022

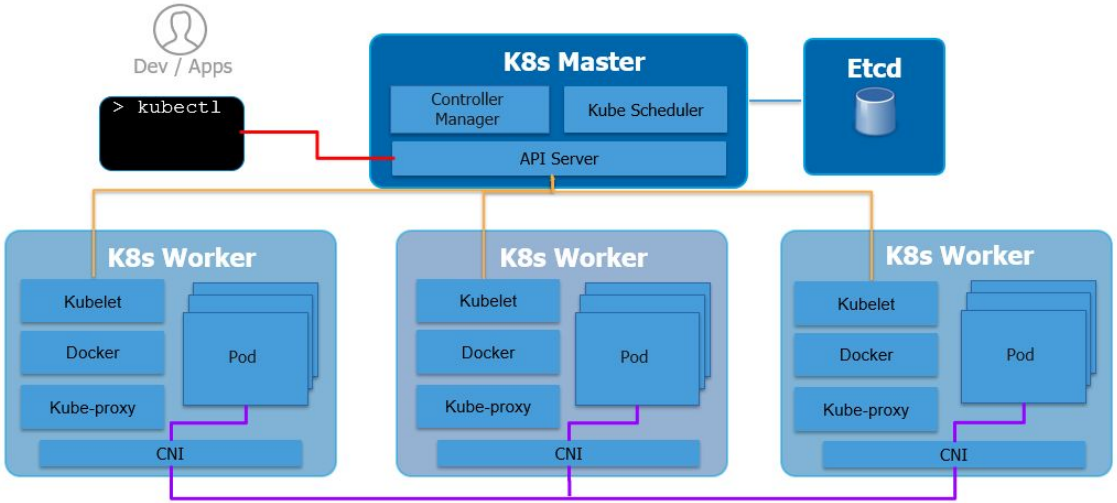
solo.io

Ambient and ePBF in “The Cloud”

- Istio-init container sets up iptables redirect
- Istio CNI can replace istio-init container
- Merbridge can replace Istio CNI

  https://github.com/merbridge/merbridge

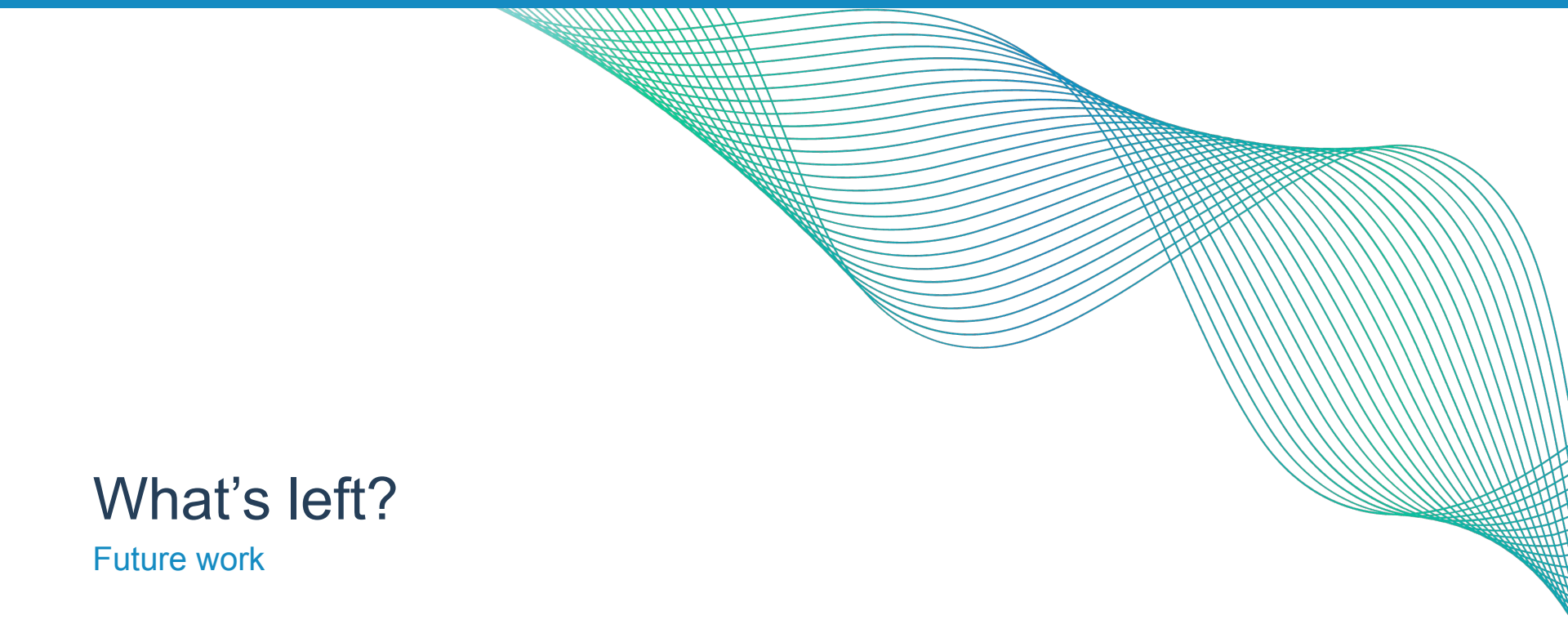
- Each CNI needs to be validated that it does not conflict with others (e.g. Calico, EKS)
- Ambient has some other platform-specific logic that needs updating (more on that later)



https://1.bp.blogspot.com/-gtwl__jkpd4/XcNPxPns2fI/AAAAAAAAC_U/Dyy3L7LgZZA_Ht8TFMDO9Hbrx_BAYyBwACLcBGAsYHQ/s1600/Kube-architecture.png

 Copyright © 2022

solo.io



What’s left?

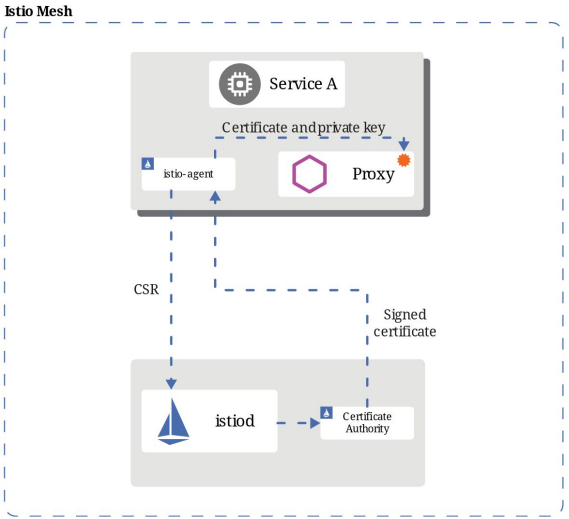
Future work

 Copyright © 2022

solo.io

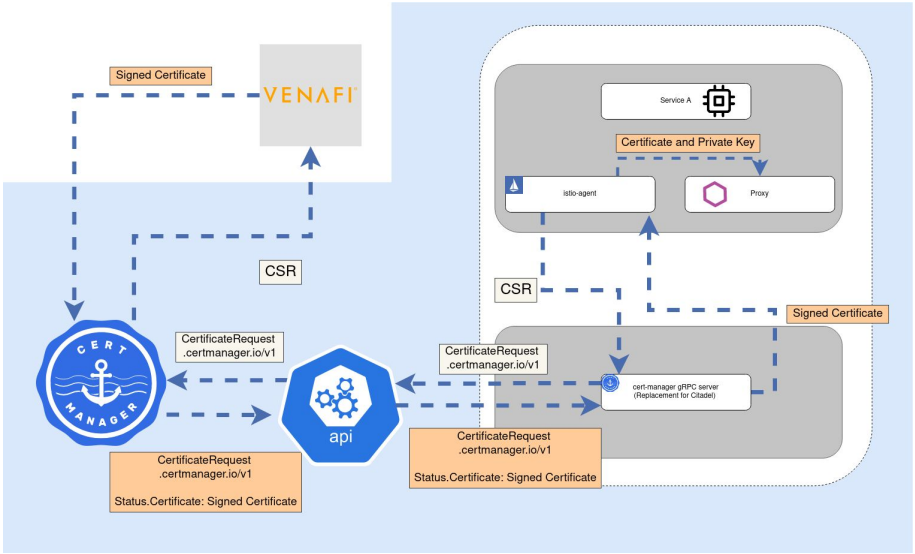
Certificate Management in Istio

- Istiod as a CA



https://istio.io/latest/docs/concepts/security/id-prov.svg

- External CA



https://www.jetstack.io/blog/cert-manager-istio-integration/

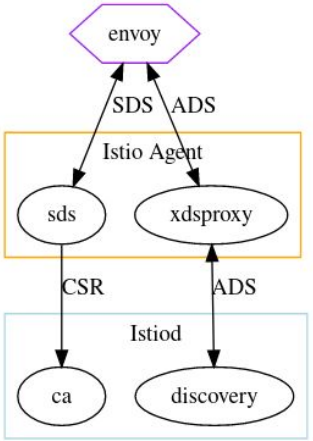
 Copyright © 2022

solo.io

k8s JWTs for Service Accounts with Istio

- A successful **`TokenRequest`** returns a JWT for a specific service account
- **`TokenReview`** authenticates a token to a user

```
curl -X "POST" "https://{kubernetes API IP}:{kubernetes API Port}/api/v1/namespaces/{namespace}/serviceaccounts/{name}/token" \
     -H 'Authorization: Bearer {your bearer token}' \
     -H 'Content-Type: application/json; charset=utf-8' \
     -d $'{}'
```



https://fossies.org/linux/istio/pkg/istio-agent/README.md

Note that istio agent is *per pod*

 Copyright © 2022

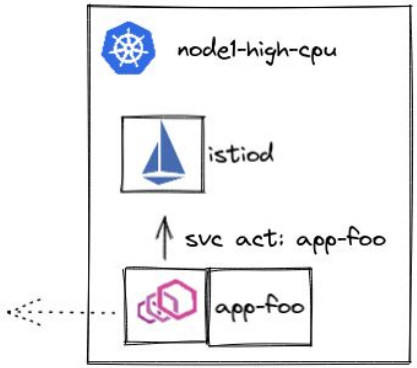
solo.io

Ambient Certificate Management in Ambient

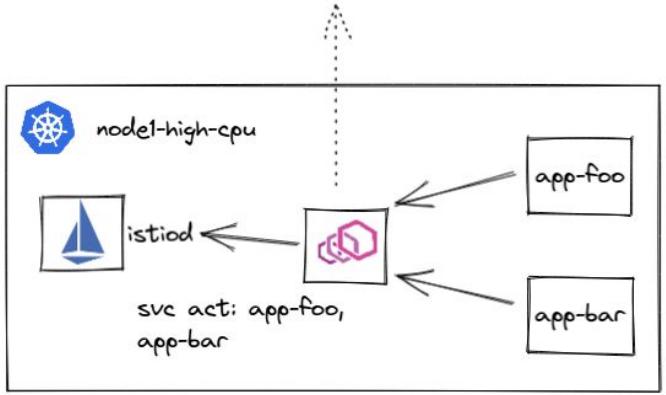
- Ztunnel (envoy here) requests mtls certs for workloads it proxies for
- To do so, impersonates kubelet
- This works, except on EKS
  - AWS IAM for kubelet authentication; no service account JWT

Amazon EKS

Sidecar Model



Ambient Model



 Copyright © 2022

solo.io

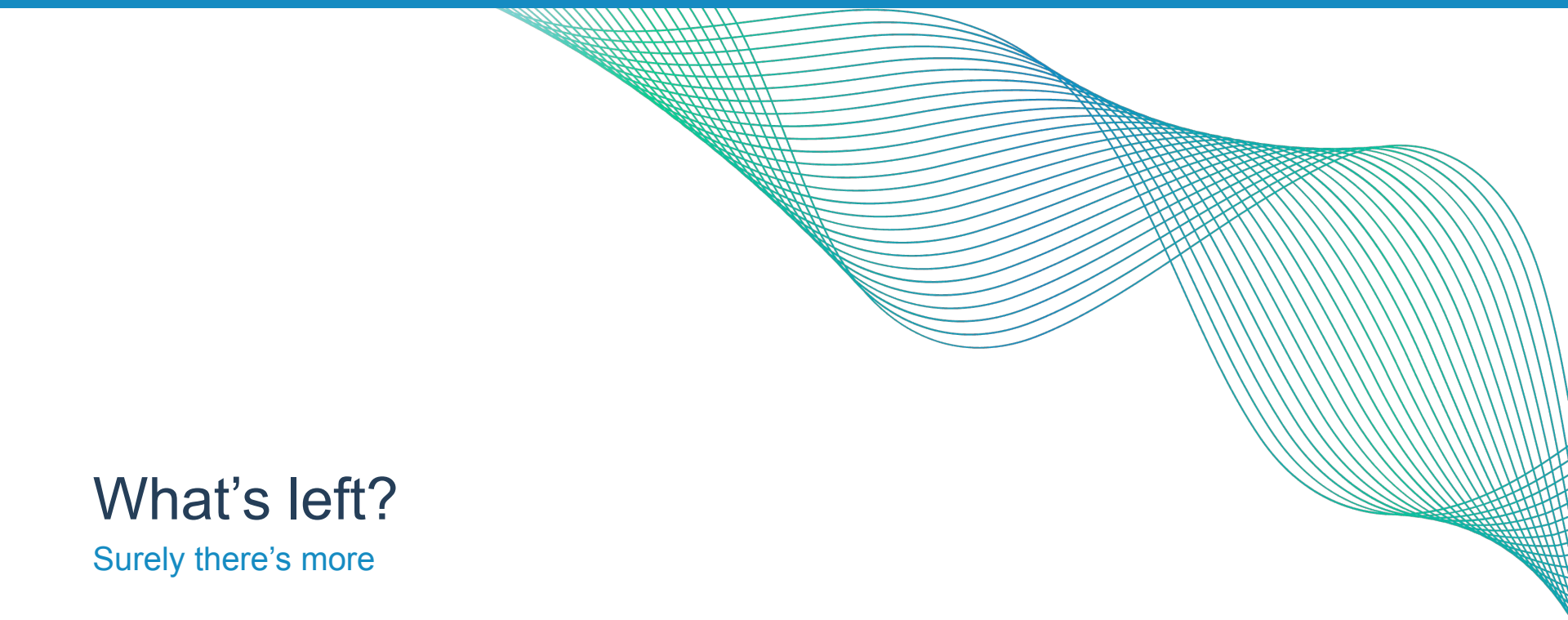
Limiting Permissions

- For now, ztunnel has cluster admin permissions on EKS so it can get certs for anything

- Istiod will be updated to watch pods on the node so no impersonation required

 Copyright © 2022

solo.io



What’s left?

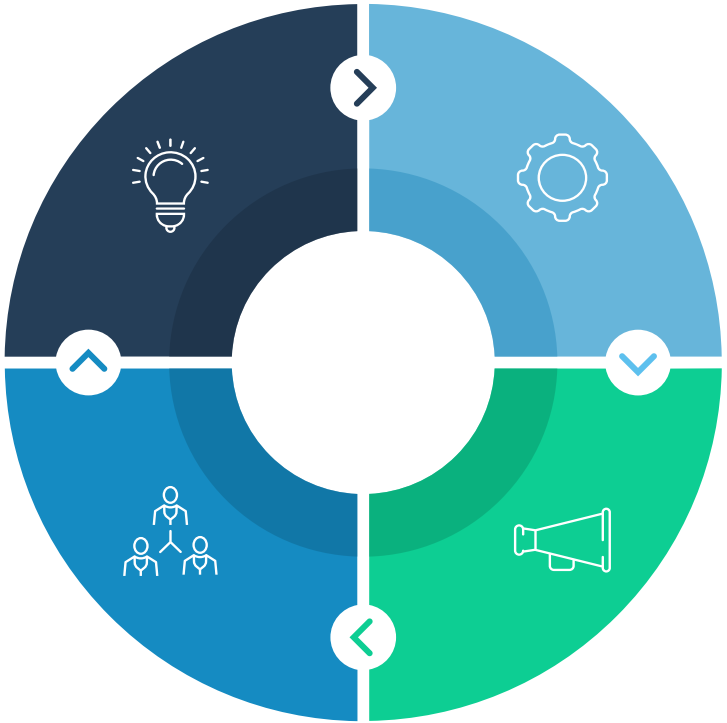
Surely there’s more

 Copyright © 2022

solo.io

The Future

HTTP/3
Envoy adds support for HTTP/3, HTTP Connect tunnel gets upgrades to masque



ZTunnel to Rust
Currently envoy. Initial benchmarks on rust proxy were faster and used far less RAM

Update Istio CA
Both for platform-specific needs (e.g. EKS) and new rust ztunnel xds api

Optimize eBPF redirect
Full istio feature set support forthcoming & support for ambient

 Copyright © 2022

solo.io

Thank You!