

Istio: Zero Trust Communication Security for Production Services

Tao Li 11/15/2018

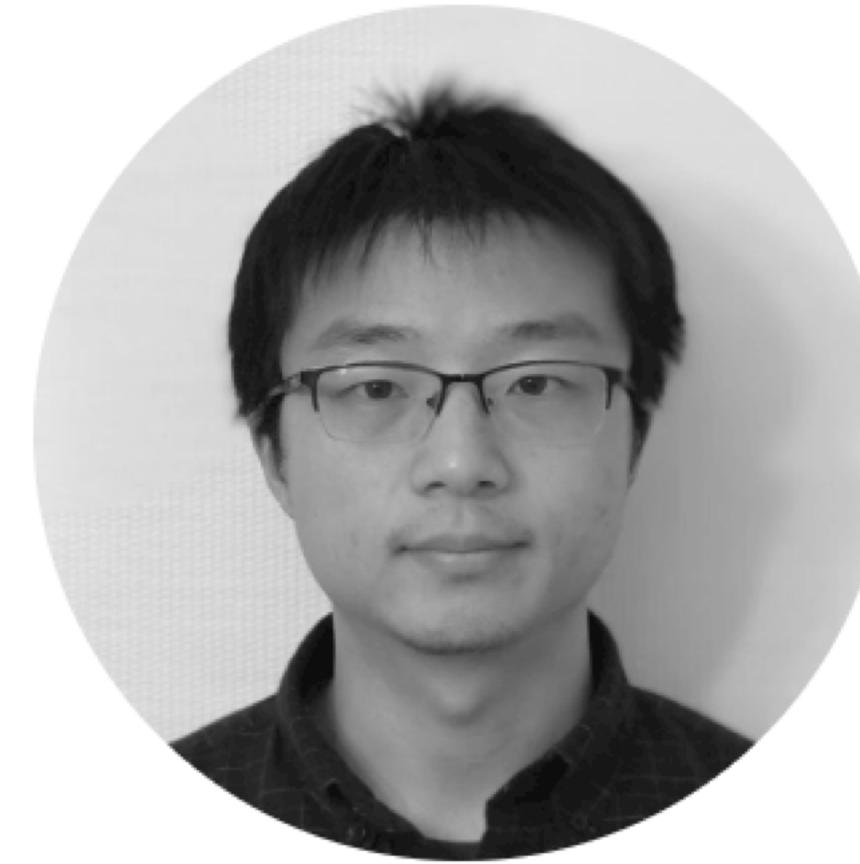


Takeaway: What
are you going to
learn today?

Google Cloud and Istio give
you the tools to help you
secure your production
environment like Google.

Also: what's Istio security?

Who am I?



Dr. Tao Li  Google Cloud

Staff Software Engineer
Tech Lead of Istio Security

Email: lita@google.com

Github: [wattli](#)

Linkedin: [tao-li-1a447935](#)

Emerging trends
driven by need for
agility, speed, cost,
data volumes ...



Containers + microservices



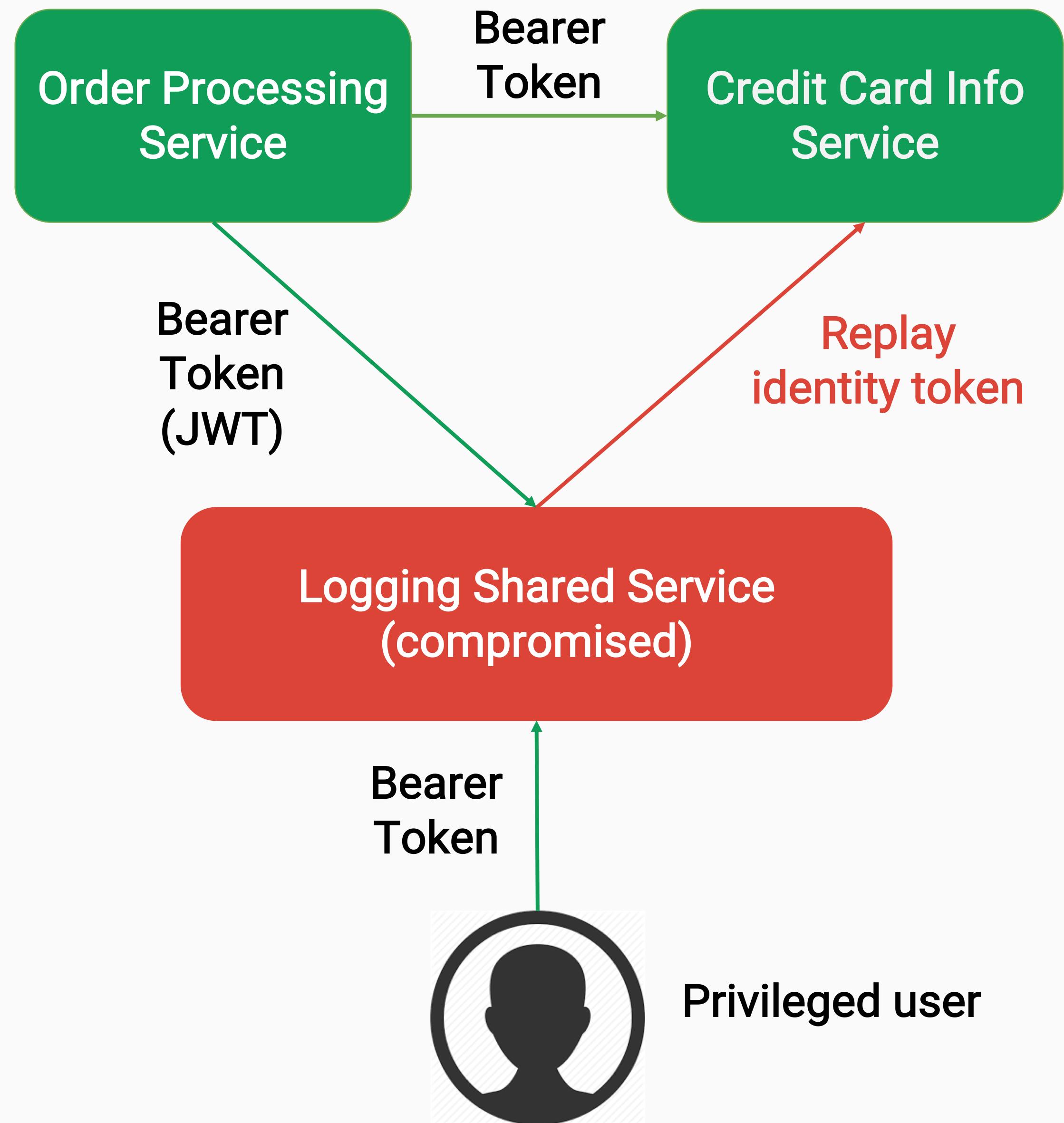
Public cloud, multi-cloud and
hybrid architectures



Heterogeneous app stacks -
languages, PaaS, OSS

How does it impact security?

- Significantly greater surface area to attack within the network if the perimeter is breached.
- Compromise of shared services enables replay attacks.
- Higher risk of indirect unauthorized access using stolen identities or by malicious insiders.



Mitigating risk in modern production environments

The zero trust security model for communication security

1. Assume threat already exists within the network

A peer (service or client) should not be trusted just because it is in the same network even if the client presents valid application level credentials.

2. Ensure every service has its own firewall (micro-perimeter)

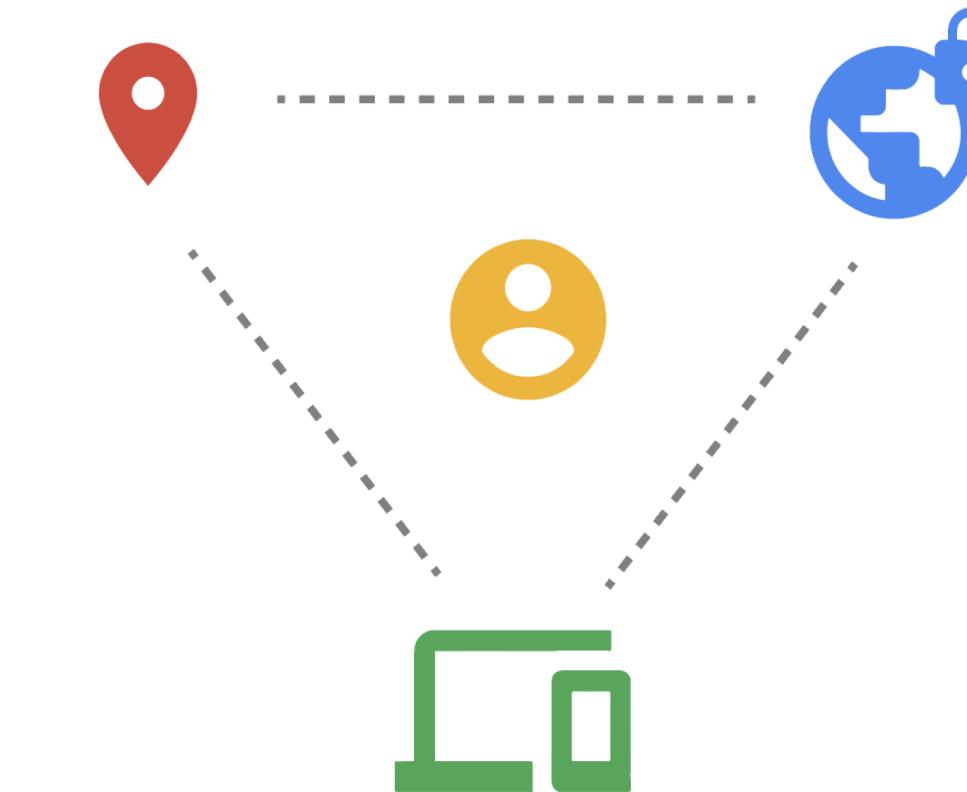
All access - human or programmatic - to production services should be strongly authenticated, authorized and encrypted.

3. Enable central administration and monitoring

Security teams should be able to understand the overall security posture and manage mandatory security policies across all services.

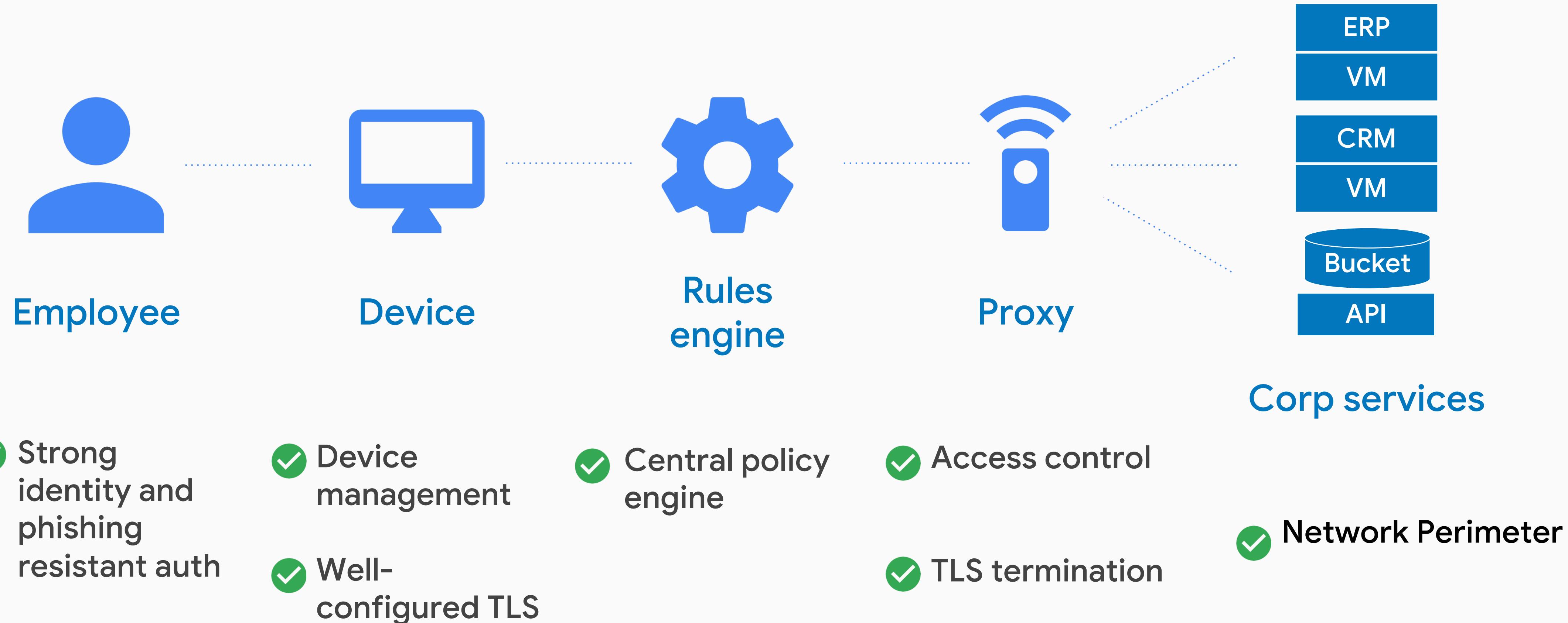
Google has adopted such a posture for many years ...

BeyondCorp



Application Layer Transport Security

BeyondCorp

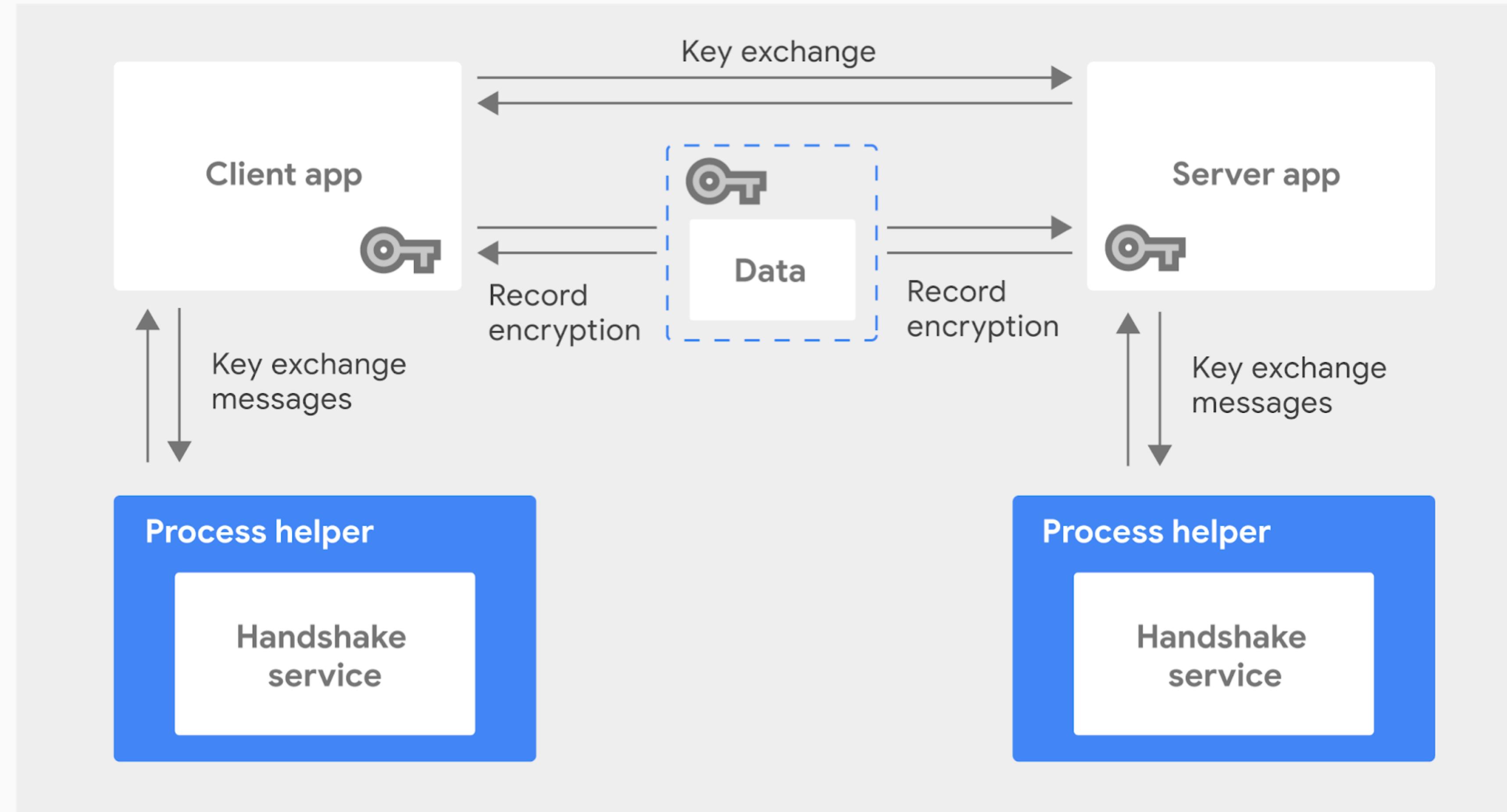


Application Layer Transport Security (ALTS)



- Transport security based on **strong peer authentication and encryption in transit**
- Optimized for **service to service interactions** in Google's production environment
- **Transparent** from application code

How does ALTS work?



But how do you implement
a similar posture
at scale
while retaining
the deployment agility and
stack heterogeneity
enabled by modern production environments ?

... drum roll ...

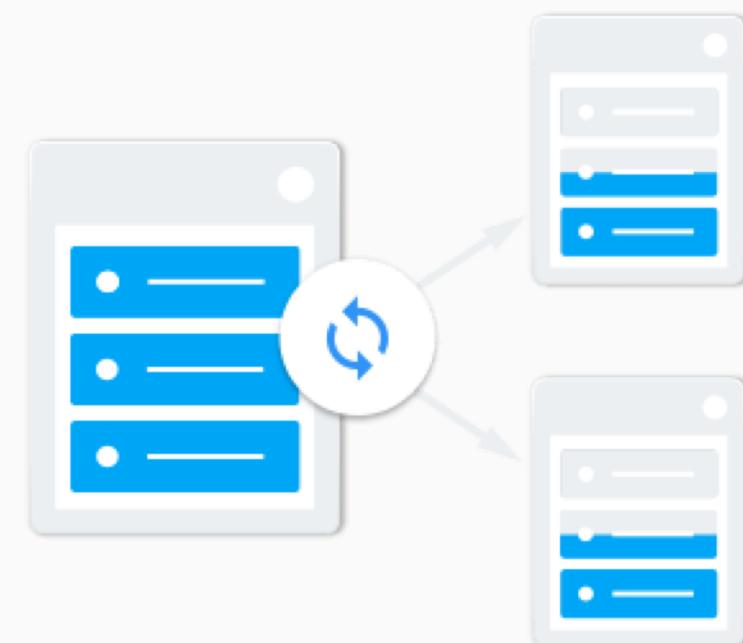
Istio is an open services platform
that incorporates the
principles and learnings
from securing Google's production
with technologies like ALTS.

What does Istio do?



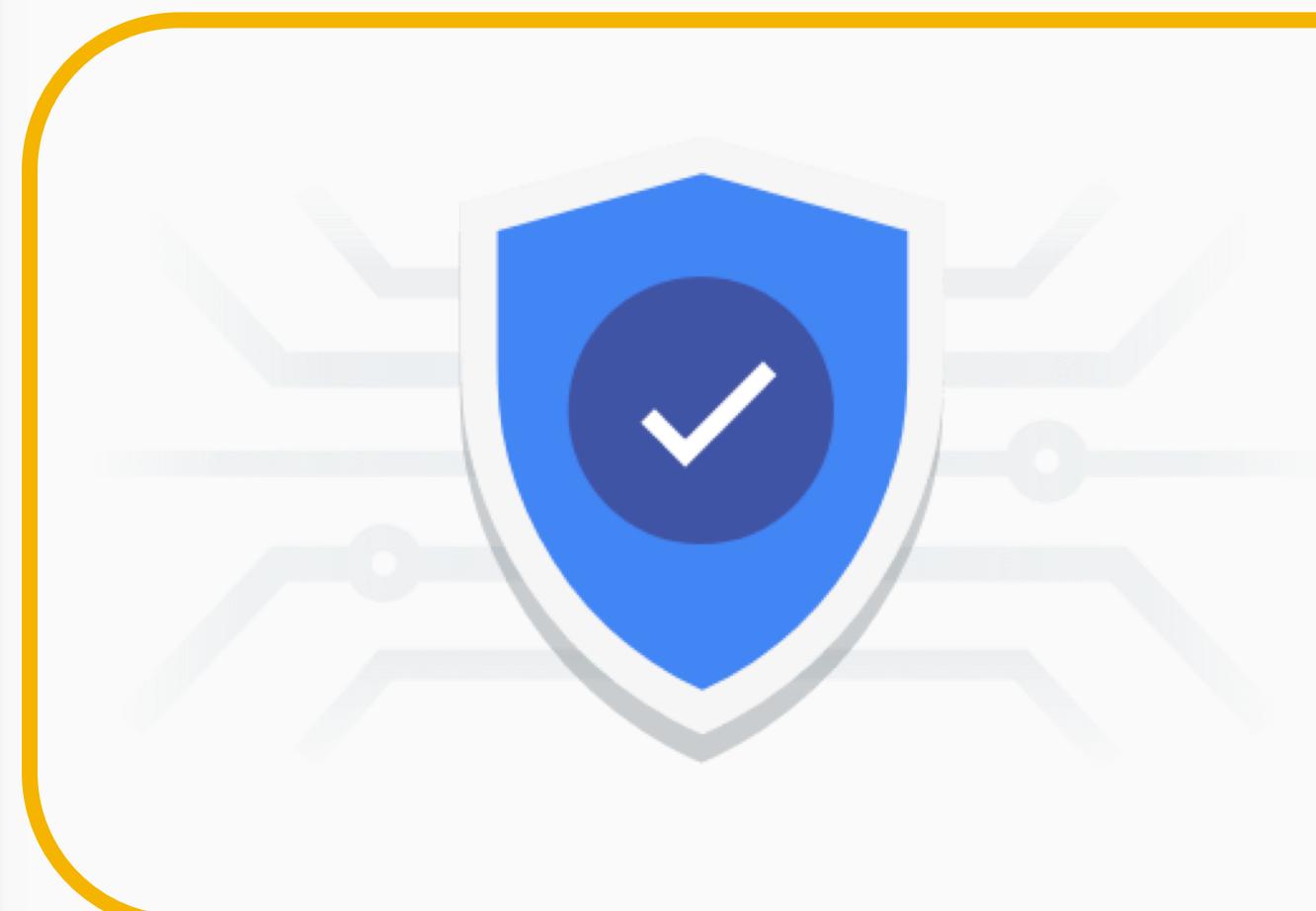
Observability

Latency, errors, dependencies, tracing



Control

L7 load-balancing, rate limiting, safe rollouts of new versions



Security

Encryption, strong authentication, authorization

What can you do with Istio security?

- Enable mTLS for authentication and encryption.
- Authorize access based on service identity or any channel attribute.
- Configure finer grained RPC-level access control for REST and gRPC.

Why do we support mTLS via Istio?

**Policy driven encryption in transit
with no code changes**

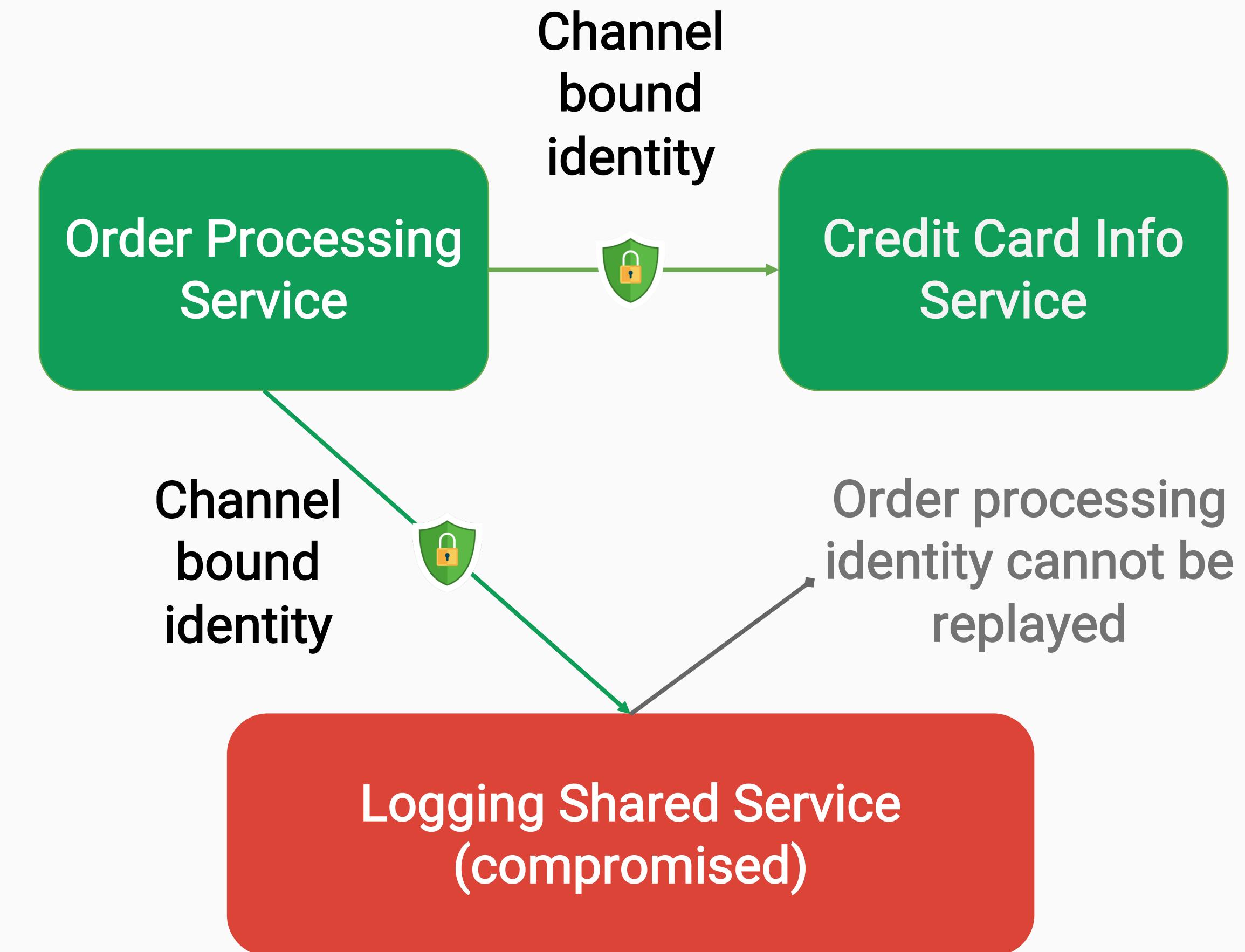
... but that's only the obvious value ...

... the real value is strong authentication

Peers are authenticated using non-replayable service identities bound to the TLS channel.

Similar to ALTS, Istio strongly authenticates the workload identity and not the host.

End user or application level identity is propagated as a bearer token across service “hops”.



Service Authorization

Istio enables identity and context aware network security policy enforcement.

Policies based on service identities are resilient to redeployment of peers.

REST / gRPC: Finer grained access control and ability to reason about both peer and end user identity.

| Layer | Policy Input | Applicability |
|----------------------|---|---------------------------|
| Application (future) | Declarative resource model | First party applications. |
| API (RPC) | Operations: URI, verbs JWT Claims: End User Id | HTTP / REST gRPC |
| Channel | Service identity (Cert) IP Context: K8S Namespace | TCP based protocols |

Centralized Monitoring



Consistent visibility
of security posture
over heterogeneous
application stacks
and deployment
platforms.



Demo Agenda

Policy based mTLS enablement

Enforce strong peer authentication + encryption.

End-user identity verification

Assert that client is acting on behalf of an authenticated end user.

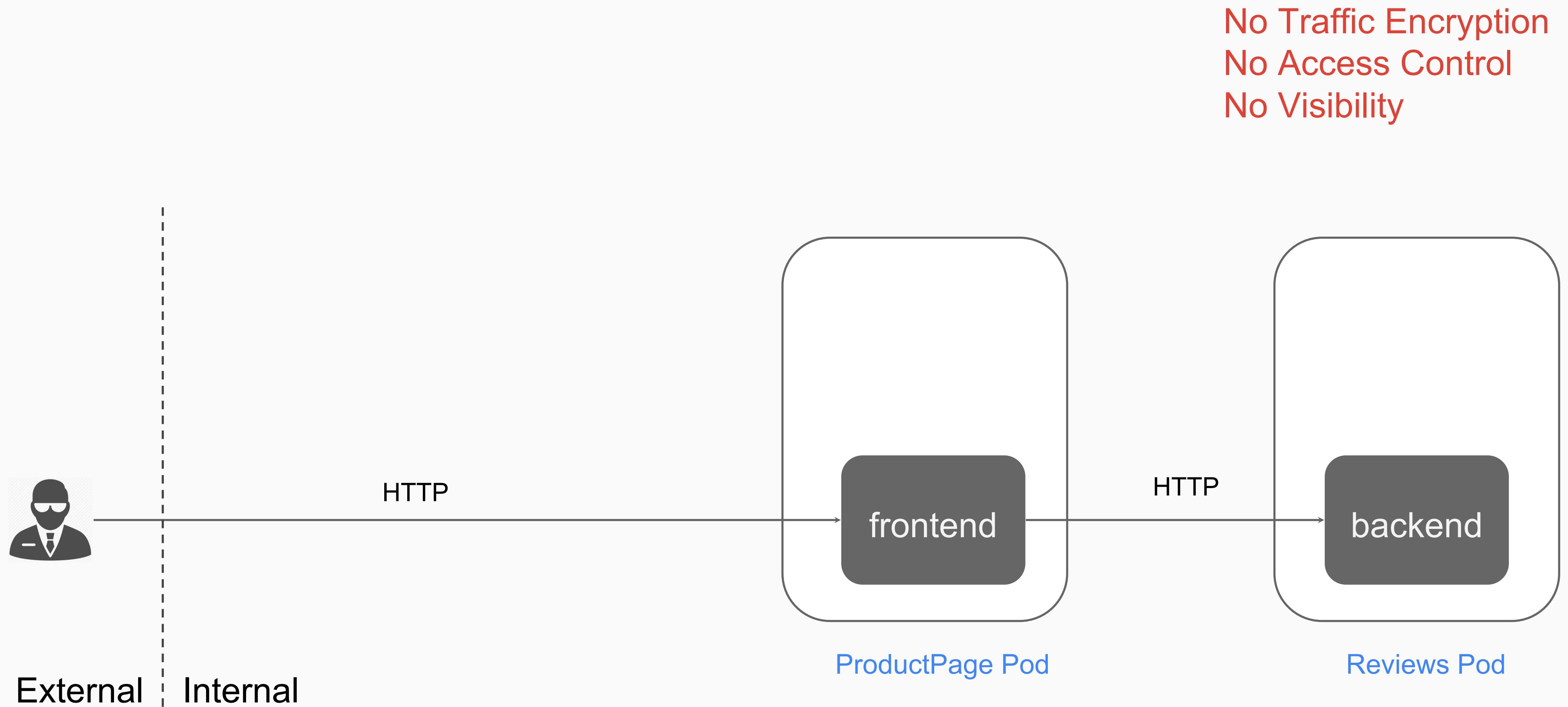
Peer identity based Authorization

Deny non-whitelisted services even with the right application level credentials (bearer token).

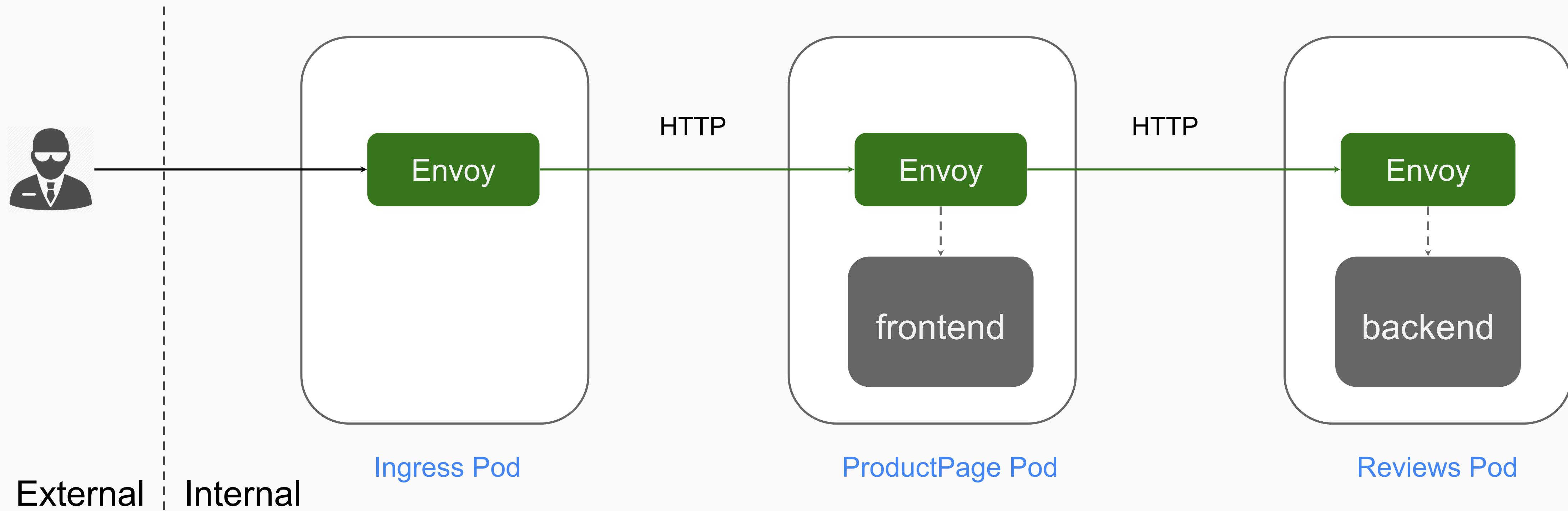
Monitoring

Centrally manage and monitor all communication.

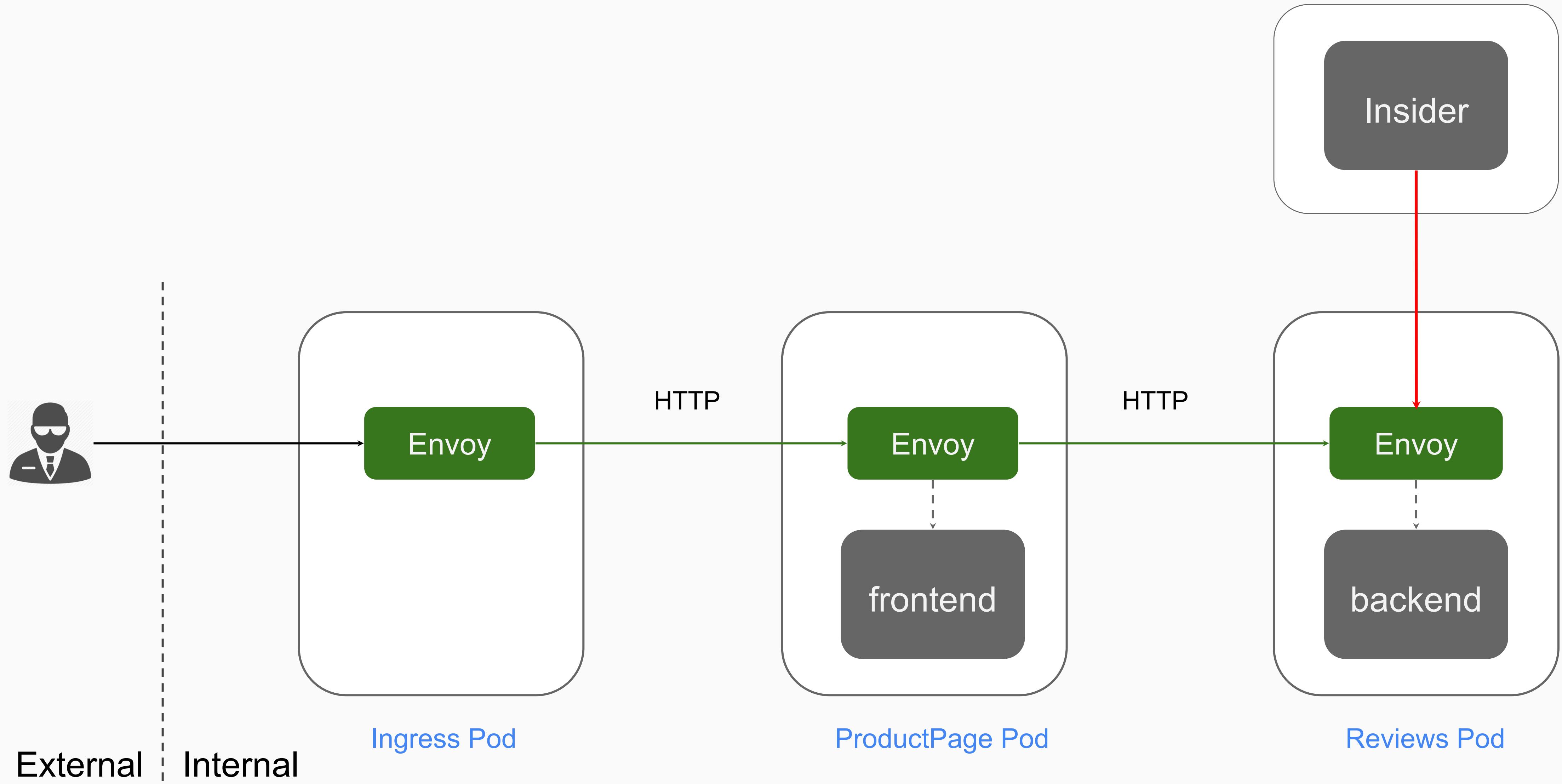
Two-Tier Example



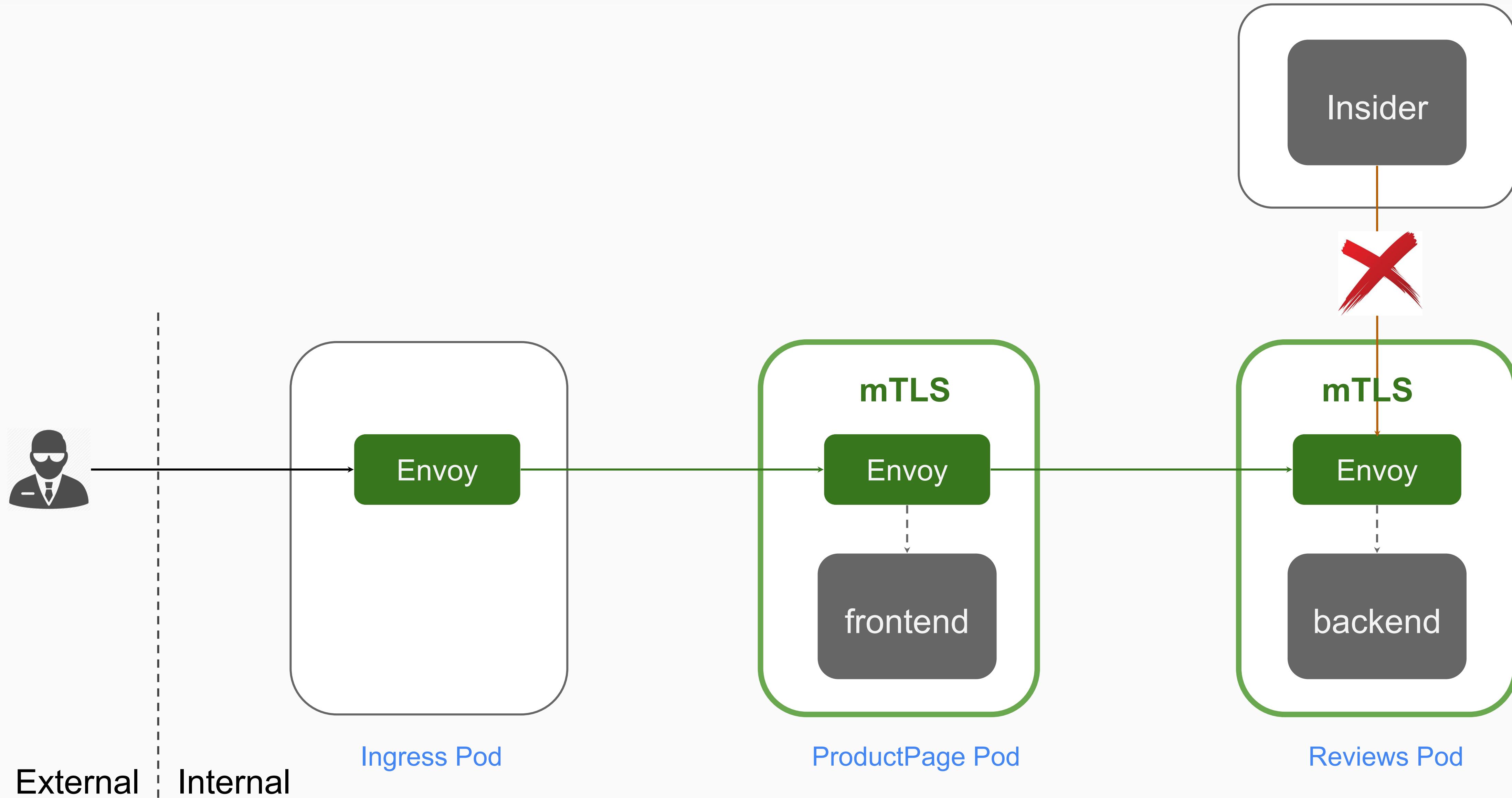
Istio without mTLS



Istio without mTLS

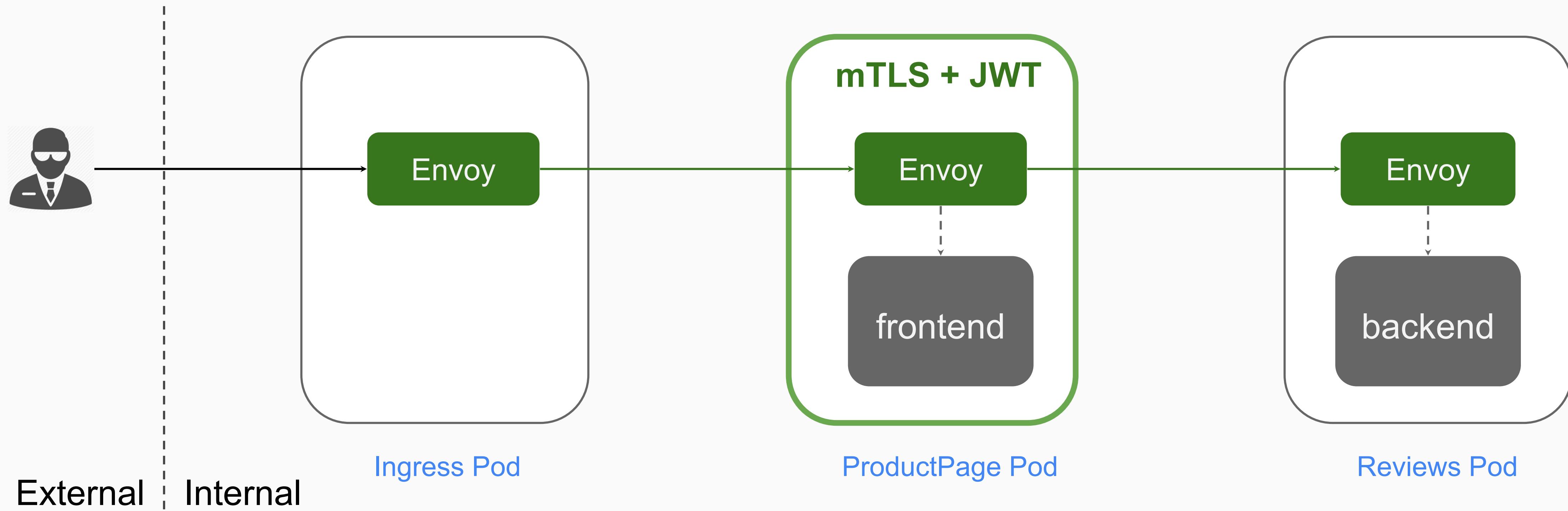


Istio with mTLS: Can only access with valid key/cert

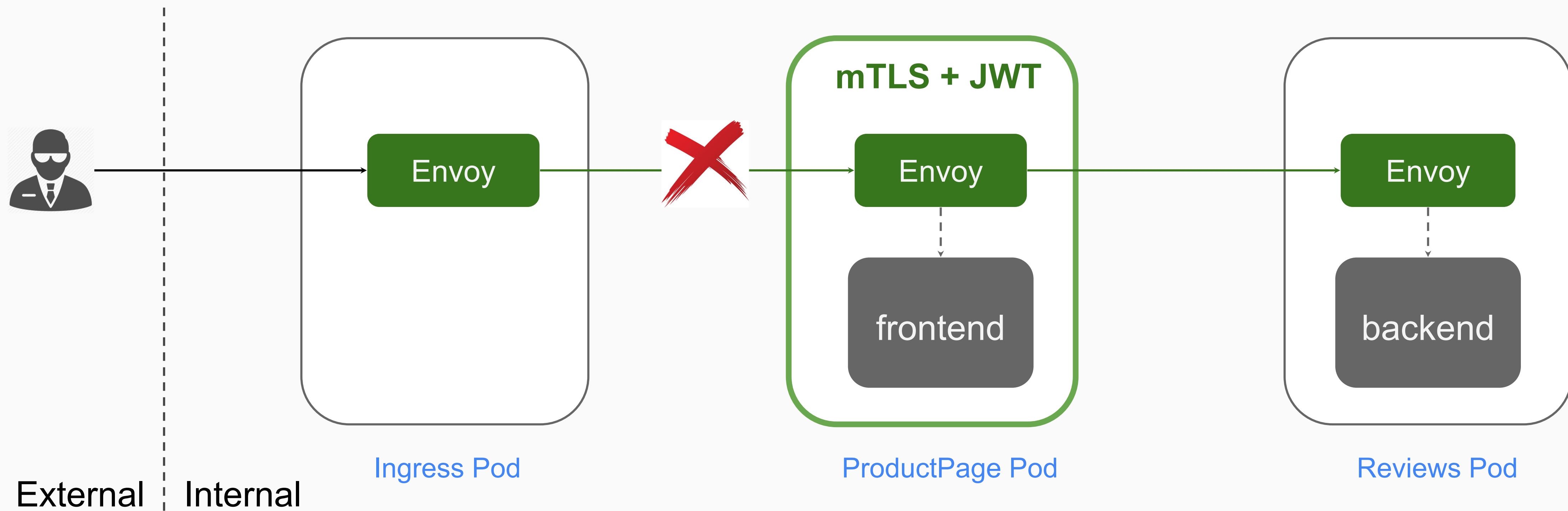


JWT Token Access

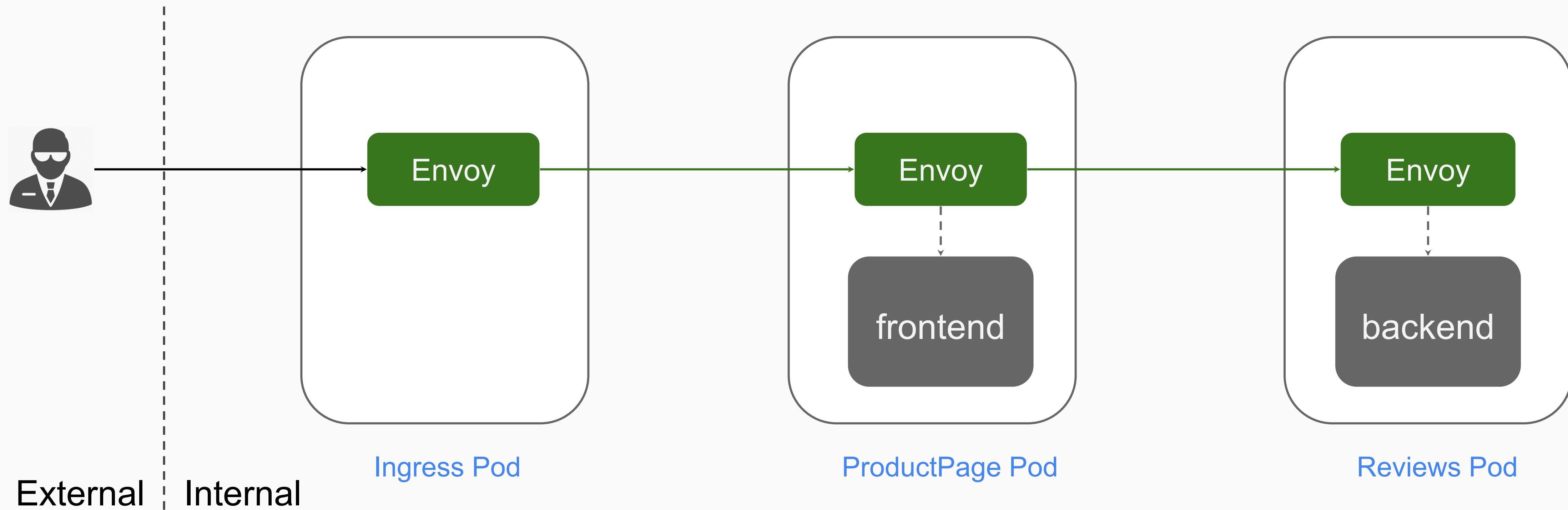
Frontend expects 2 credentials



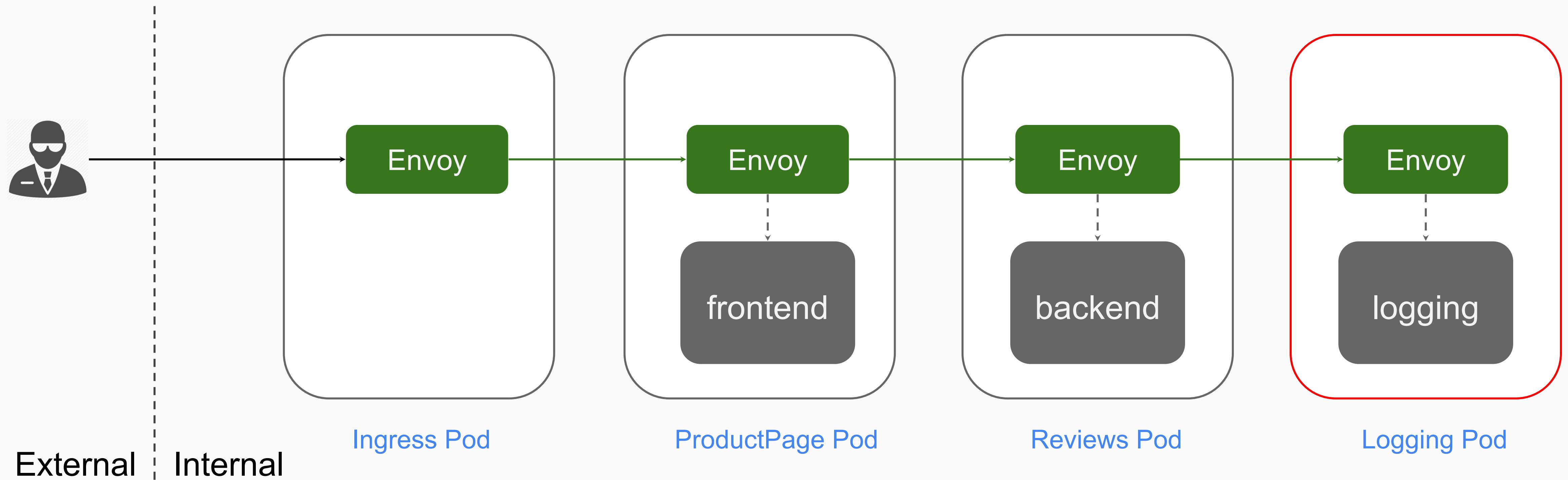
JWT Token Validation



Istio Authorization



Istio Authorization



How to engage with Istio Security

Users

Try out Istio on Google Cloud



<https://cloud.google.com/istio>

Join the Istio user group

groups.google.com/forum/#!forum/istio-users

Participate or ask questions

istio.rocket.chat

ISTIO WITH GOOGLE

Use Istio with Google to connect, monitor, and secure services

[VIEW DOCUMENTATION](#)

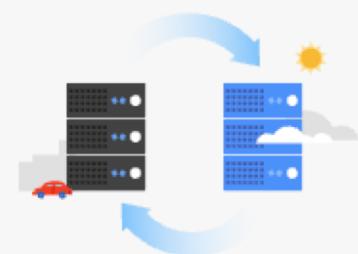
[CONTACT US](#)

Microservices Simplified

Istio is an open source service mesh that provides a uniform way to connect, monitor and secure services. The trend toward microservices and containerization is leading to more complicated applications that are difficult to secure and monitor.



At Google, we have been developing and deploying microservices for over 15 years, and have helped build Istio to transparently take care of these issues so your developers don't have to. Istio supports managing traffic flows between microservices, enforcing access policies and aggregating telemetry data, without changing your code.



Hybrid Cloud workloads with Istio

Istio on Google Kubernetes Engine is the best way to securely control traffic flows across any Kubernetes or microservice environments in a scalable way. With Istio, Google helps you connect your on-prem and cloud workloads, and manage them holistically, without requiring changes in the application software. Get started today on [Kubernetes Engine](#) and with [Compute Engine](#).



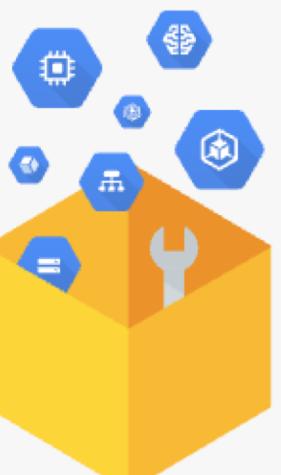
Secure Service Calls

Istio transparently adds mutual TLS to all service calls. This enables strong encryption and authentication across all of your services deployed both in Google Kubernetes Engine and Google Compute Engine.



Deeper insights across services

Istio delivers deep insight into your system running on Google Cloud by collecting tracing, monitoring and logging information on every service in your mesh.



Build to Simplify DevOps

Istio provides dynamic, config-based routing for all of your service calls, empowering the operations team with a flexible set of tools so they can leverage:

- ✓ Canary services
- ✓ Versioning
- ✓ Blue/green deployments
- ✓ Content-based routing

This enables faster and more predictable roll-outs, while ensuring higher uptime for your services.

How to engage with Istio Security

Developers

- Code contribution on github.com/istio/
- Sign up for Istio security groups.google.com/forum/#!forum/istio-security
- Join the Istio security community meetings (istio.zoom.us/j/117159906) bi-weekly on Wednesdays from 11am-12pm PST
- Sign up for Istio dev groups.google.com/forum/#!forum/istio-dev
- Join the wider Istio community meetings (zoom.us/j/986657835) bi-weekly on Thursdays from 11am-12pm PST

Questions?