Transitioning to the Mesh

Kevin Paige
CISO, Flexport

flexport.

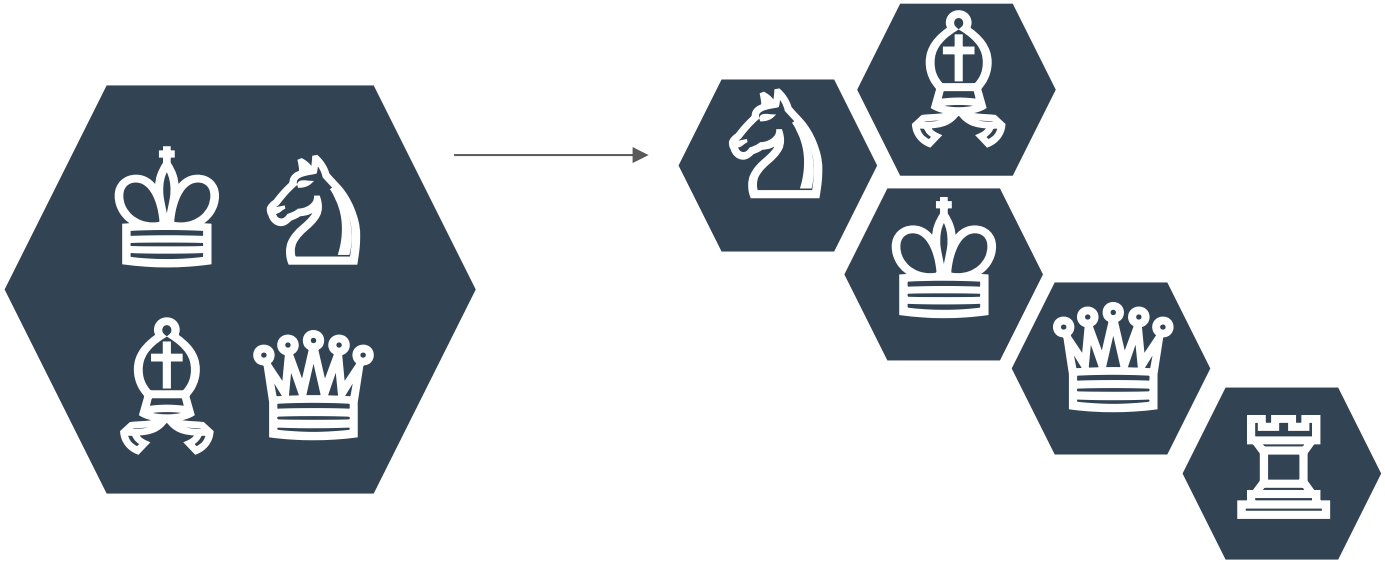
Flexport

Flexport is a freight forwarding company that makes global trade easier and more accessible.

We serve >10,000 clients in more than 200 countries with services enabled by a cloud software and data analytics platform.

We're an international business adhering to complex regulatory requirements.

Monolith to microservices



Microservices enable agility

But with distributed services you have to figure out how to manage and secure those services and workloads in different environments.

What is a service mesh?

- A service mesh is a layer of infrastructure that controls communication between services.
- A service mesh gives you a way to control networking issues outside of the application, decoupling ops from development.
- Service mesh is like a software-based network that helps you secure services and solve the networking problems that arise when services need to communicate.

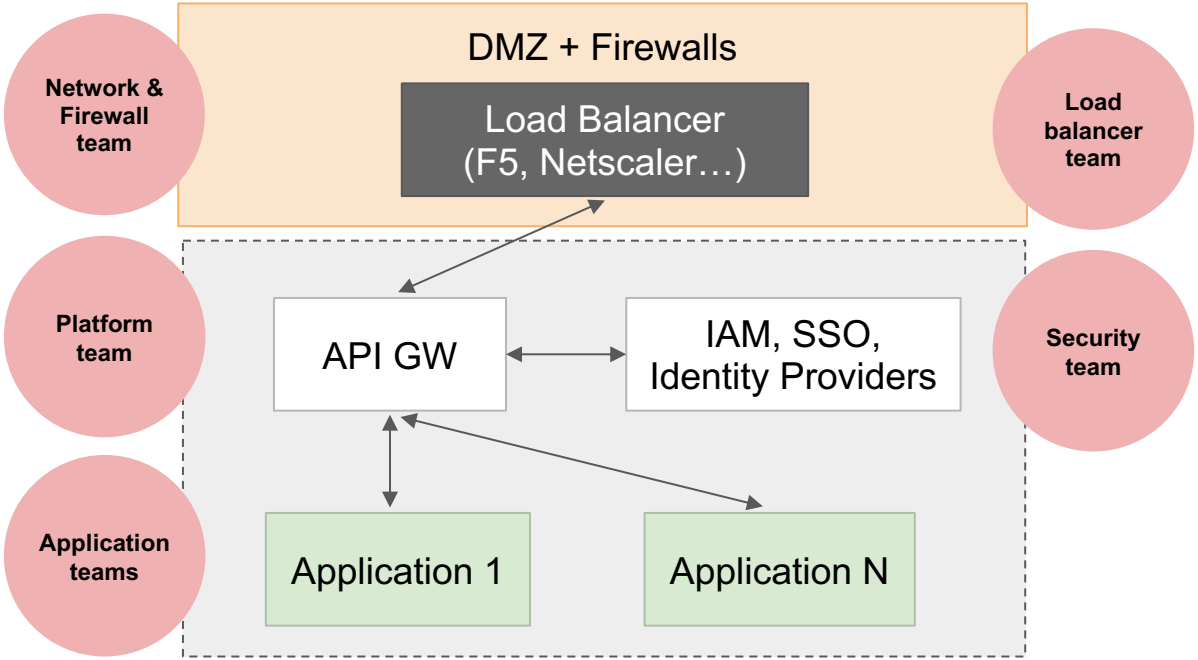
Addressing complexity

With a monolith, you have simplicity.
You get complexity with microservices that you can address with a service mesh.

Traditional networking vs. service mesh

- How do you get observability of all your services?
- How do you deal with multi-cluster protocols?
- How do you get consistent policies?
- How do you get ingress capabilities?
- How do you get zero trust – a mechanism with which you can apply dynamic policies?

A typical organization's security infra



Why a firewall mindset isn't sufficient?

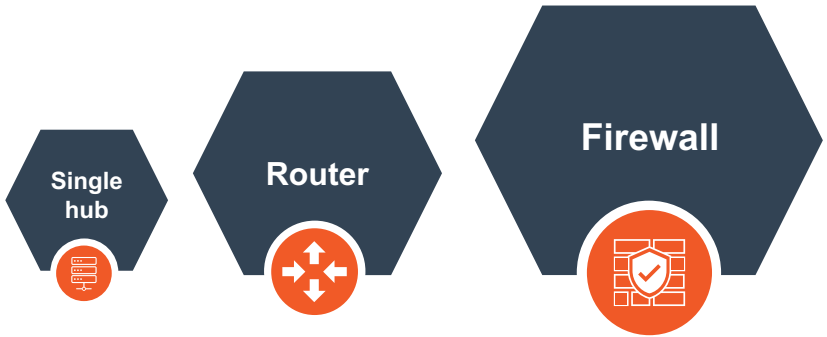
- When you have a singular system you're protecting, it's kind of easy to manage firewall rules. What if you have hundreds or thousands of services?
- With microservices, you start to have lots of firewalls, and services that are not all inside one building or one network.
- We had requirements like needing to have all these services encrypted, end-to-end.
- At Flexport, we realized that service mesh is what we were missing. This is what we needed to be effective.

The challenge of transitioning (1 of 3)

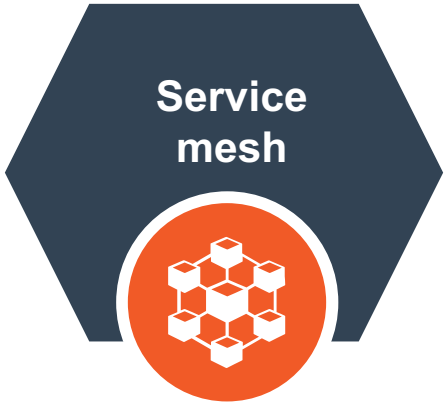
How do you get to a spot where you're using micro-segmentation and good security capabilities to secure traffic end-to-end, handle multiple protocols, make networking easier because now developers have to handle networking? How do you manage access rules in a dynamic environment? How do you make all that happen in a secure way, enabling speed, and providing guardrails?

The challenge of transitioning (2 of 3)

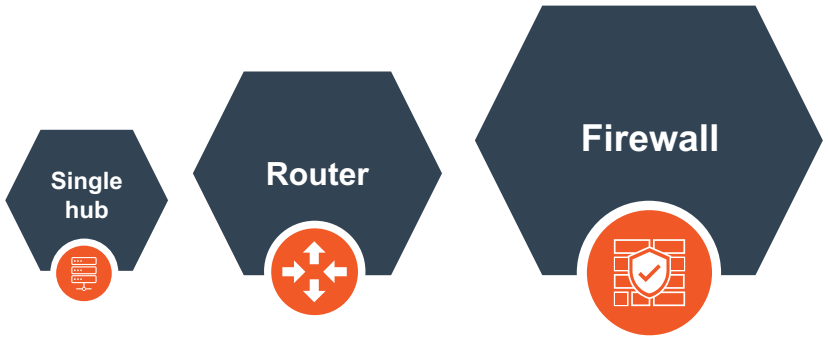
How do you get to a spot where you're using micro-segmentation and good security capabilities to secure traffic end-to-end, handle multiple protocols, make networking easier because now developers have to handle networking? How do you manage access rules in a dynamic environment? How do you make all that happen in a secure way, enabling speed, and providing guardrails?



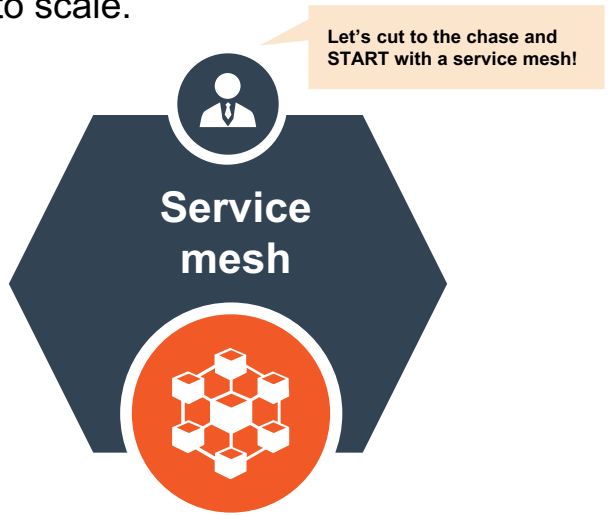
And how do you get the mindset in your organization to make the transition?



The challenge of transitioning (3 of 3)



Having learned from previous mistakes, I initiated conversations about the pitfalls and problems we were going to have as we continued to scale.



Transitioning to mesh

Evaluating

Our infrastructure ops teams did some research and saw that Istio would be a good fit

Security considerations

We realized we'd need to solve for security requirements like certificate management, better tracing, and access control for ingress and egress authentication.

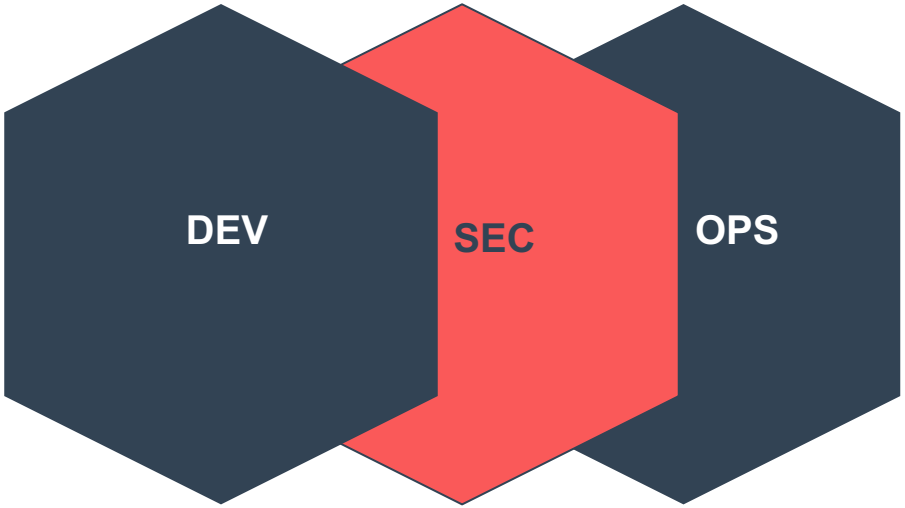
Development and Staging

We're now at the stage where we're kicking the tires, because you can't think of all the issues you might have until you try it.

Production

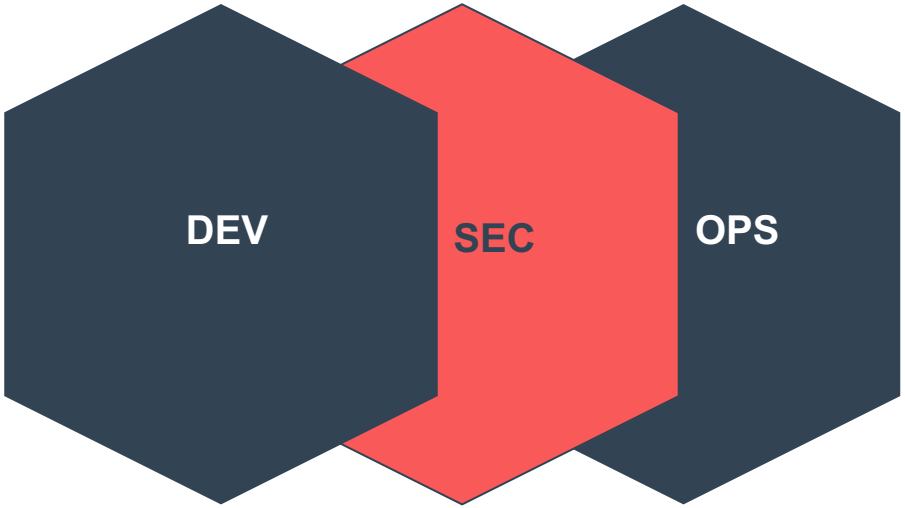
...We're not in production yet, but this would be the next step.

Transitioning to mesh: DevSecOps



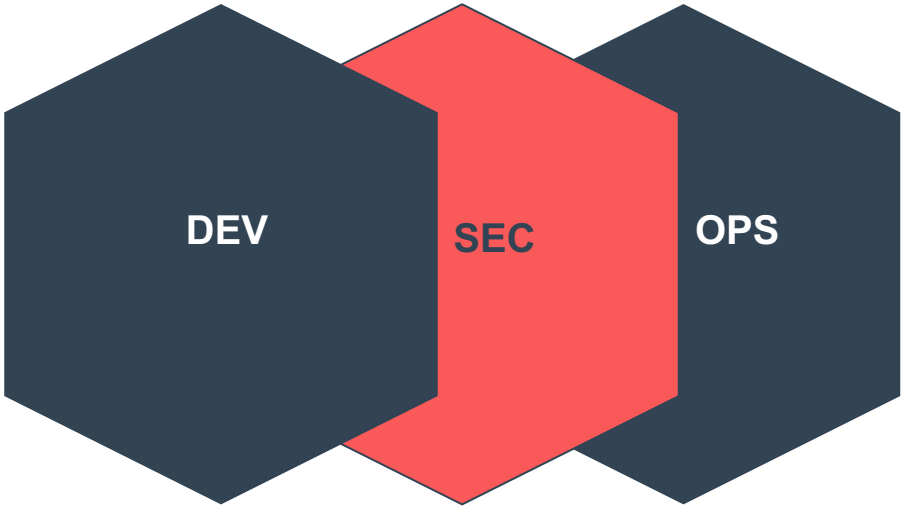
The move to a service mesh is an approach where the teams are working closer together, with a similar goal and tools, but with checks and balances and separation of duties still in place.

Transitioning to mesh



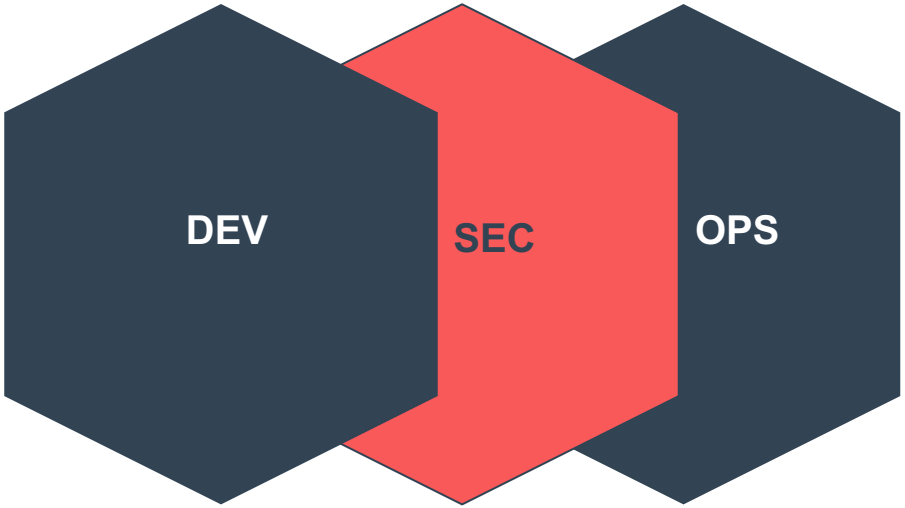
Bringing those teams together require **training and collaboration**.
It requires a **cultural mindset** change.

Transitioning to mesh



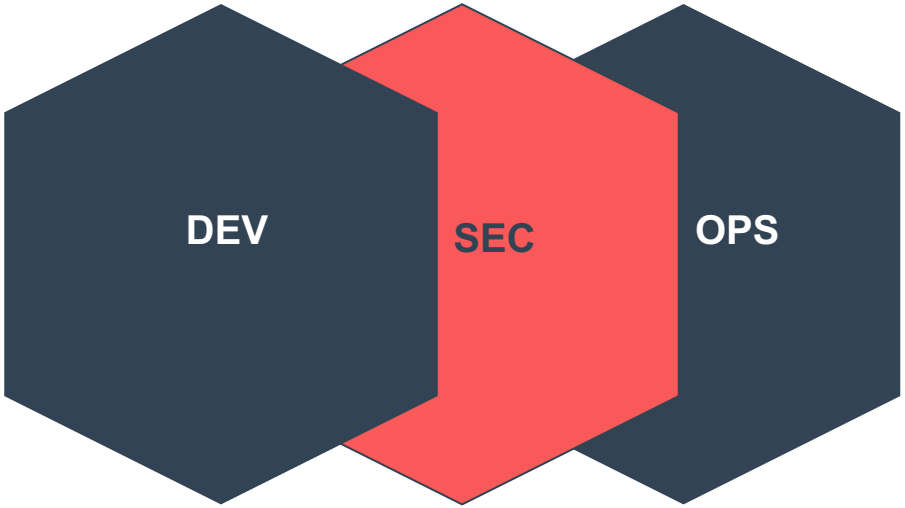
You need to be clear about permissions, roles and responsibilities, SLAs.

Transitioning to mesh



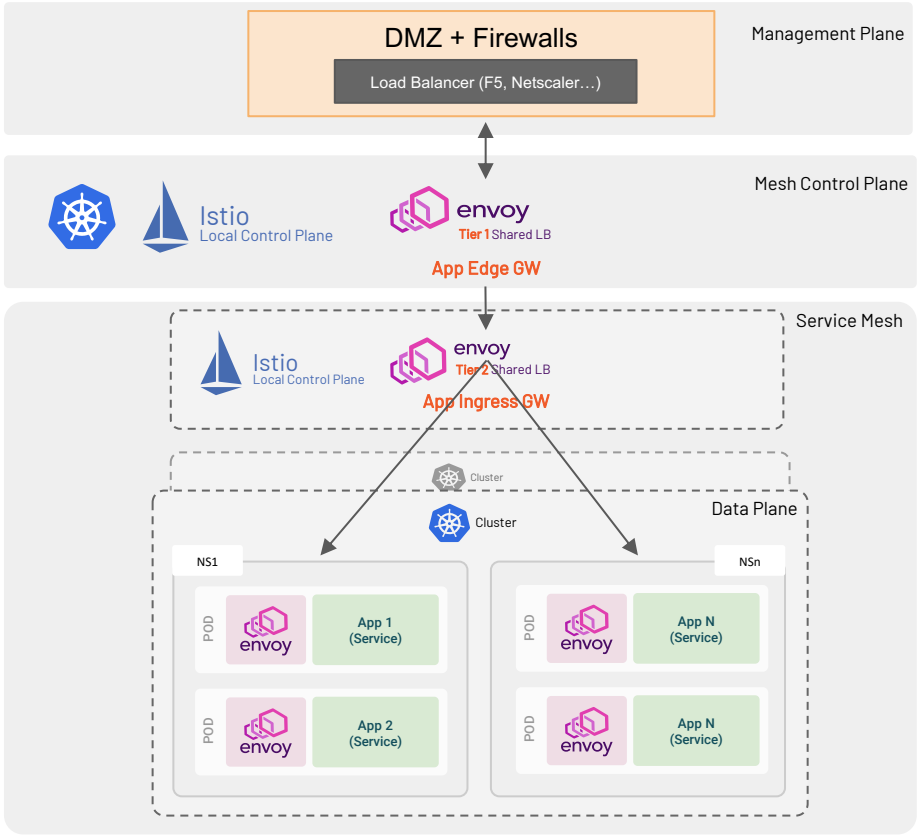
When we moved to a service-based, microservices model, it was about moving faster. Security probably took a back seat. But **security can take an equal seat when it comes to networking.**

Transitioning to mesh

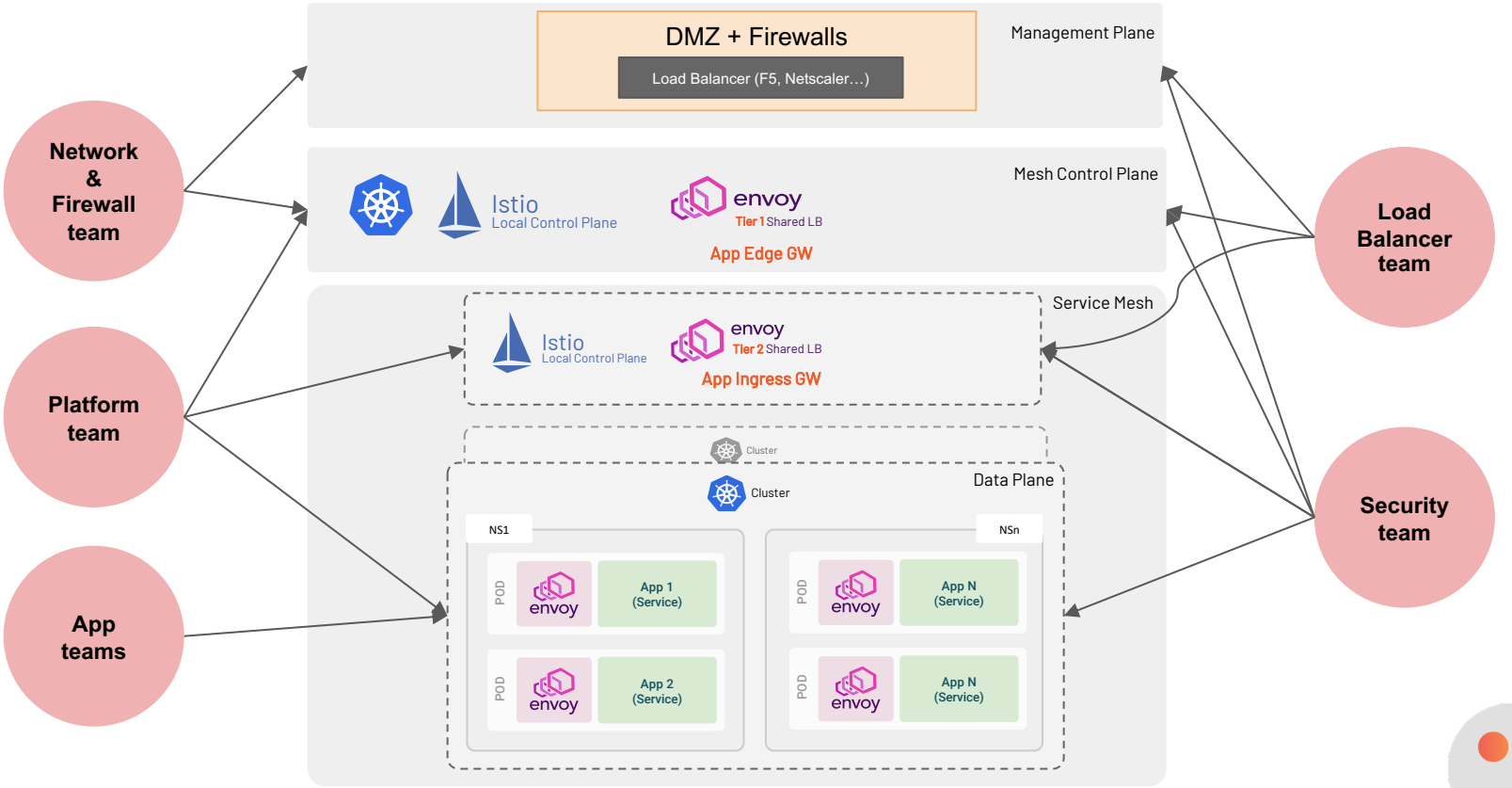


The mesh helps you accomplish the networking, connectivity, and security you need so you can **keep deploying services faster**. You provide clear communication paths to services that can **grow and scale in a distributed way**.

Mapping the mesh: traffic flow



Mapping the mesh: team ownership



Government considerations

- Defense-in-Depth-”in-Depth”
- The perimeter has no walls
- Asset Management the ephemeral way
- Identity is the new Firewall

The impact of a service mesh

Increased security: encryption, authentication, ability to manage ingress and egress

DevSecOps agility: collaboration between infra, security, and development teams

Unified observability of all services through a centralized plane

Key takeaways

Service mesh addresses the complexity of microservices architecture

DevSecOps approach helps you go faster.

Security doesn’t have to take a back seat to speed.