Сеть и безопасность в Tanzu в наземных и облачных средах

Mariia Bocharova
VMware Solution Engineer

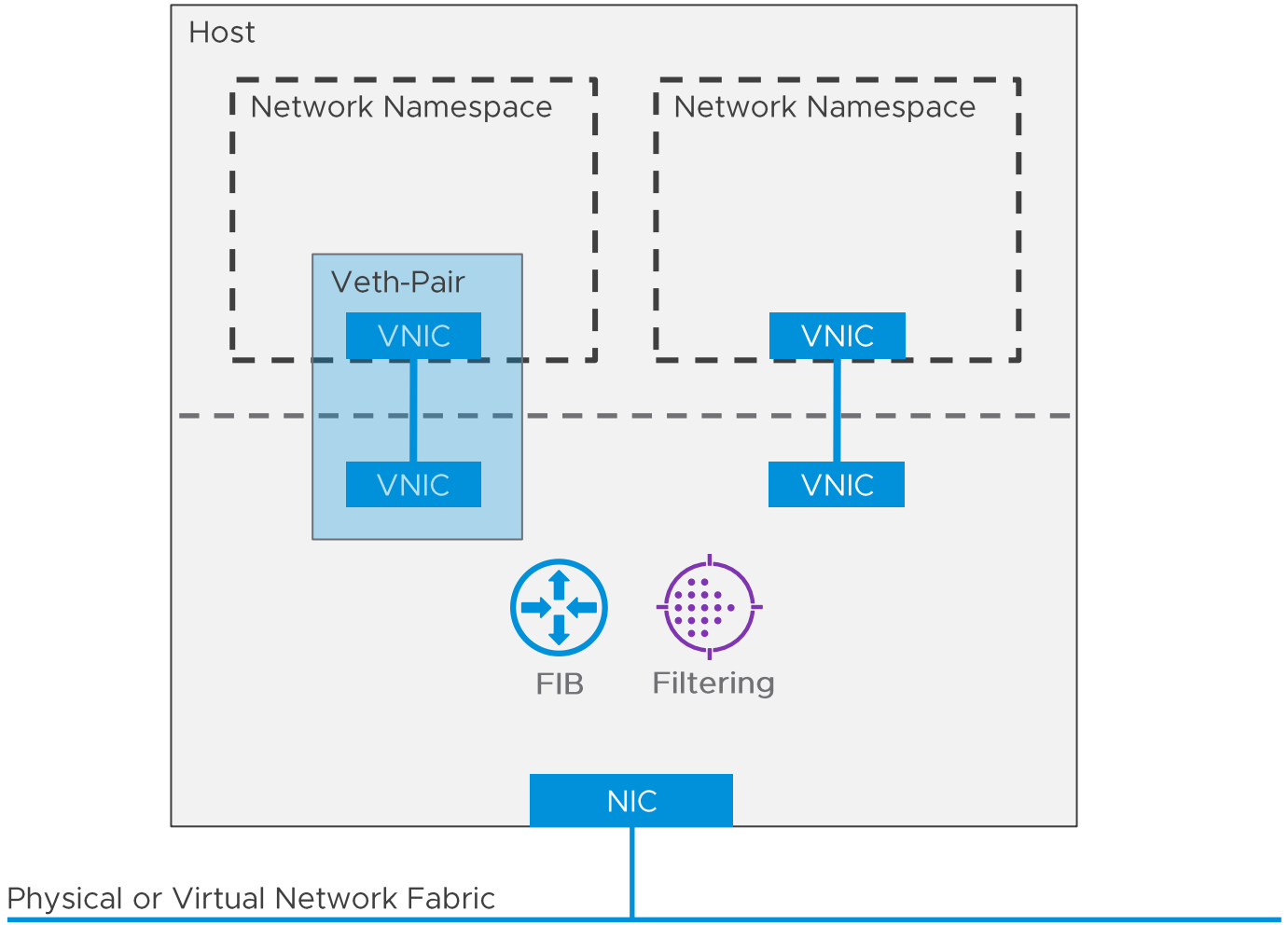
June 2023

Kubernetes Networking

A quick review

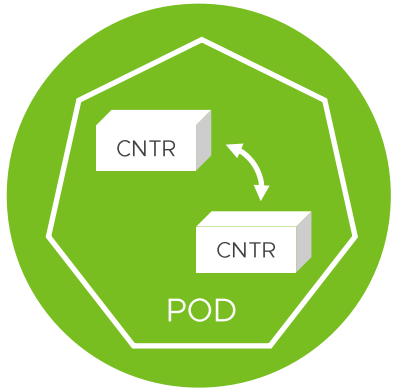
The Network Namespace

Container Networking Demystified

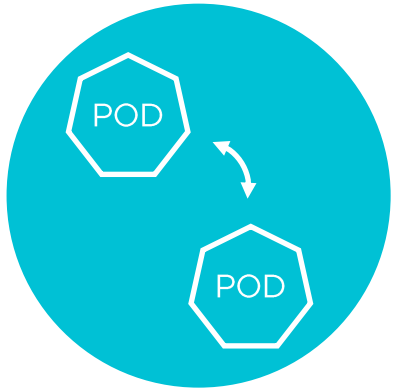


Kubernetes Cluster Networking

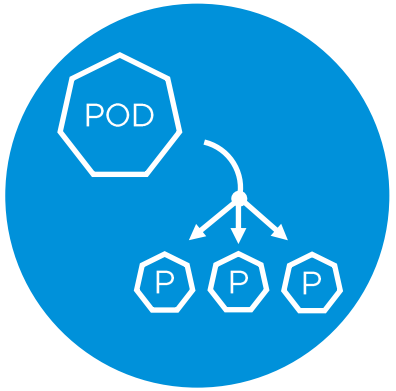
Four connectivity scenarios must be enabled by network plugin.



Container
-to-
Container



Pod
-to-
Pod

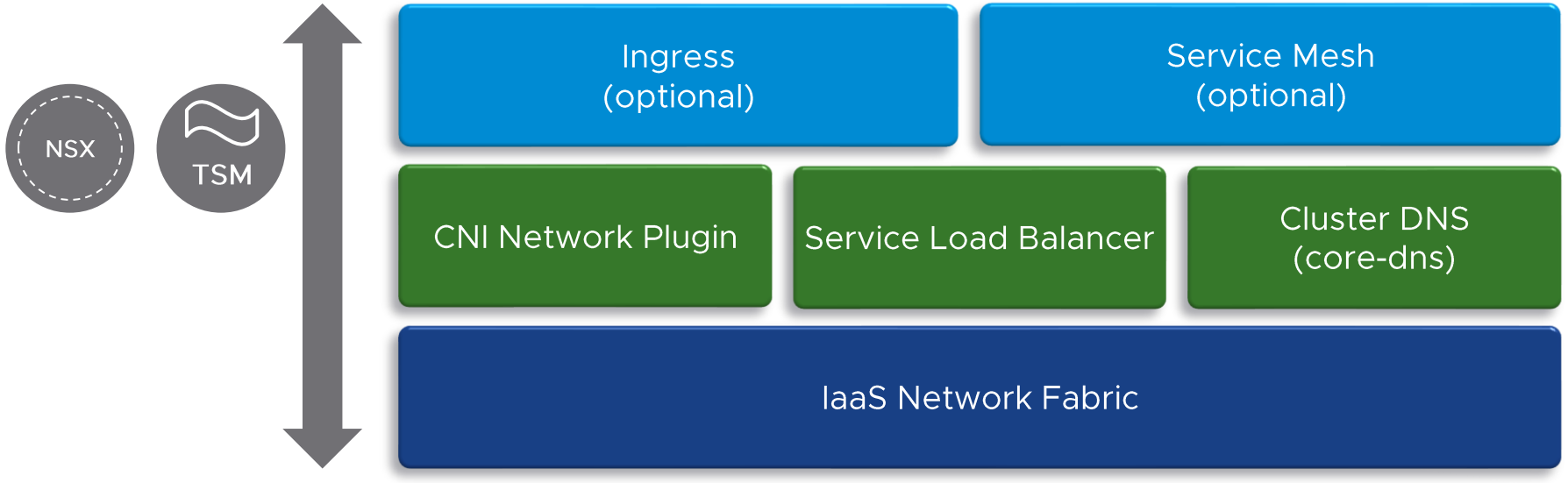


Pod
-to-
Service

External
-to-
Service

Kubernetes Networking in Layers

Separating network concerns



ANTREA

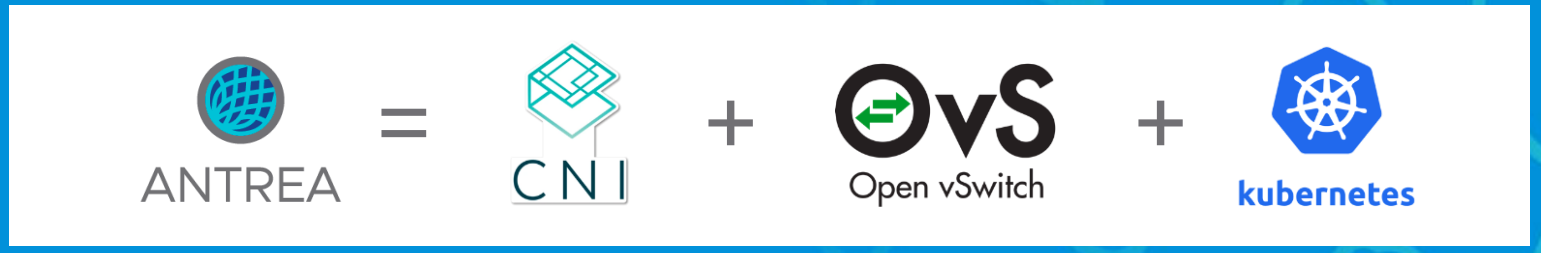
https://antrea.io

https://github.com/vmware-tanzu/antrea

@ProjectAntrea

Kubernetes Slack – #antrea

Project Antrea is an open source CNI network plugin providing pod connectivity and network policy enforcement with Open vSwitch in Kubernetes.



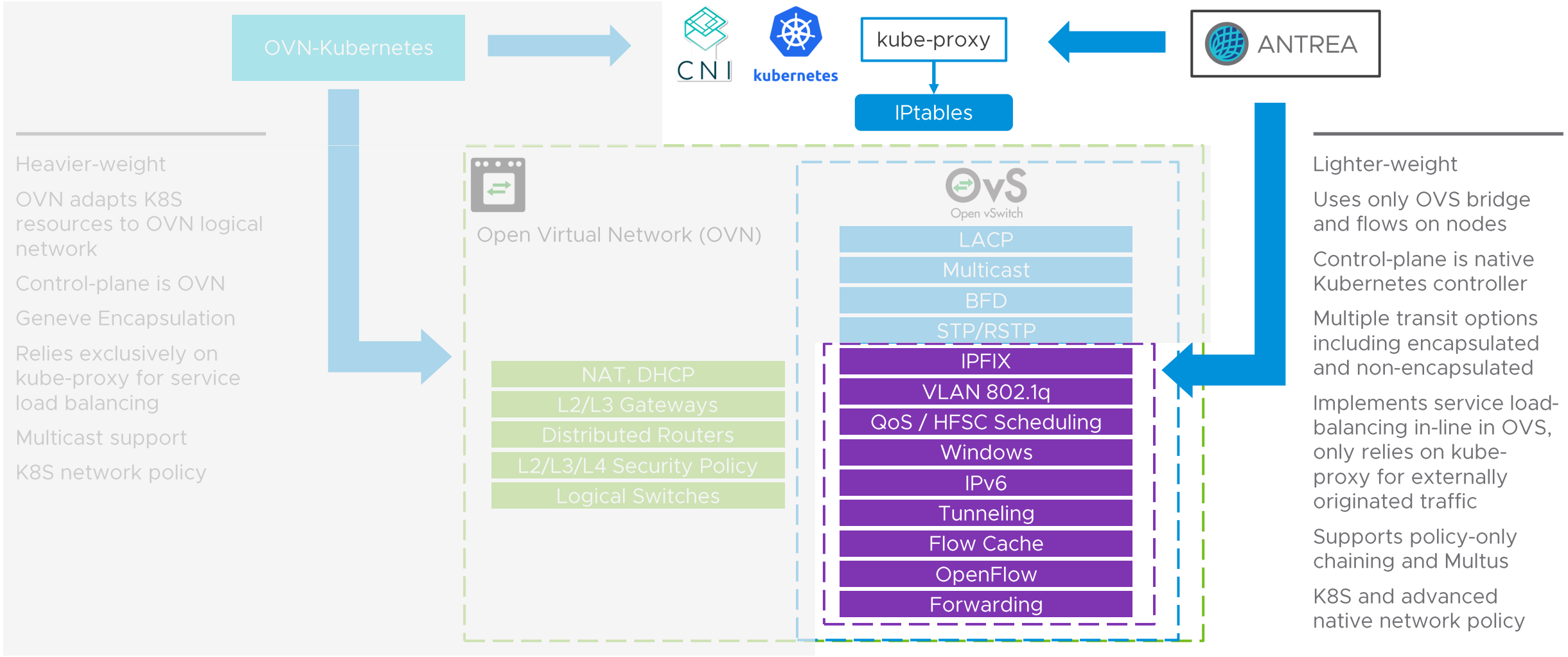
689
GitHub Stars

116
GitHub Forks

31
Contributors

OVN vs Antrea

Antrea is a lightweight utilization of OVS for Kubernetes pod networking



Heavier-weight

OVN adapts K8S resources to OVN logical network

Control-plane is OVN

Geneve Encapsulation

Relies exclusively on kube-proxy for service load balancing

Multicast support

K8S network policy

Lighter-weight

Uses only OVS bridge and flows on nodes

Control-plane is native Kubernetes controller

Multiple transit options including encapsulated and non-encapsulated

Implements service load-balancing in-line in OVS, only relies on kube-proxy for externally originated traffic

Supports policy-only chaining and Multus

K8S and advanced native network policy

Project Antrea

Extending NSX management to everywhere Kubernetes runs.

ANTREA = CNI + OvS Open vSwitch + kubernetes

Runs Everywhere K8S Runs

Very easy to start with – single line install using kubectl commands

Supports multiple OS, Compute Platforms, Clouds and Simulators where K8S runs.

Can run in public clouds – DIY and managed K8S.

Community Driven

Open source and easily available.

Active community with contributors participating in CNCF and K8S network SIGs.

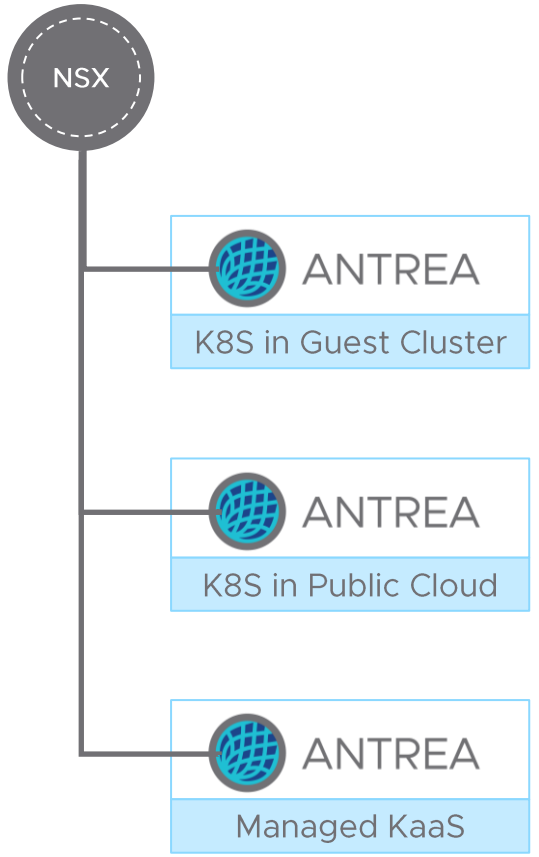
Very easy to start – single line install using kubectl command.

Extensible and Scalable

Extensibility allows for easy addition of new features.

Scales better for large number of K8S clusters.

Connection to NSX-T for visibility and global policy distribution.



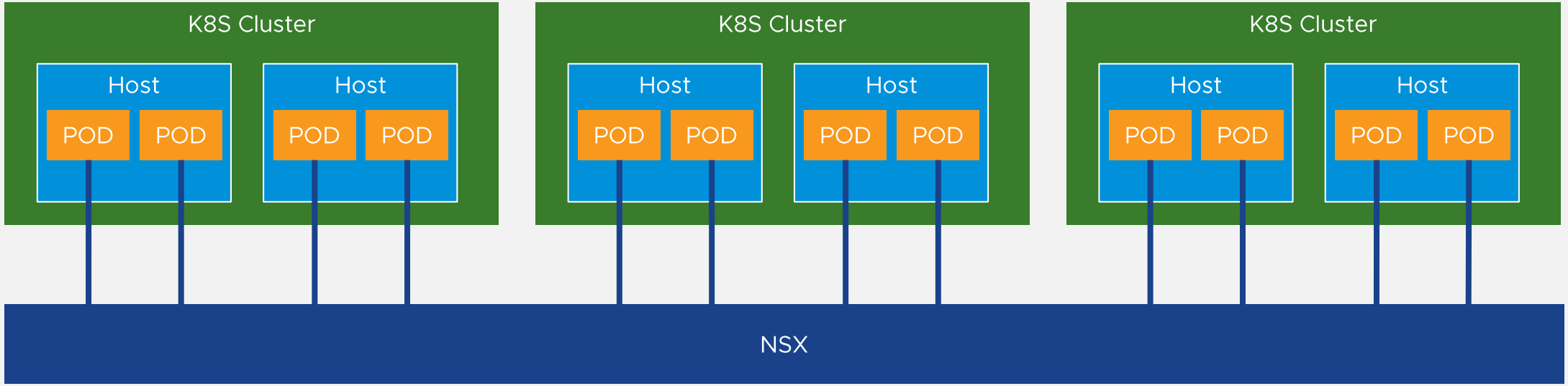

```
kubectl apply -f https://github.com/vmware-tanzu/antrea/releases/download/v0.8.0/antrea.yml
```

Scale Out with NCP

NSX used as pod data plane

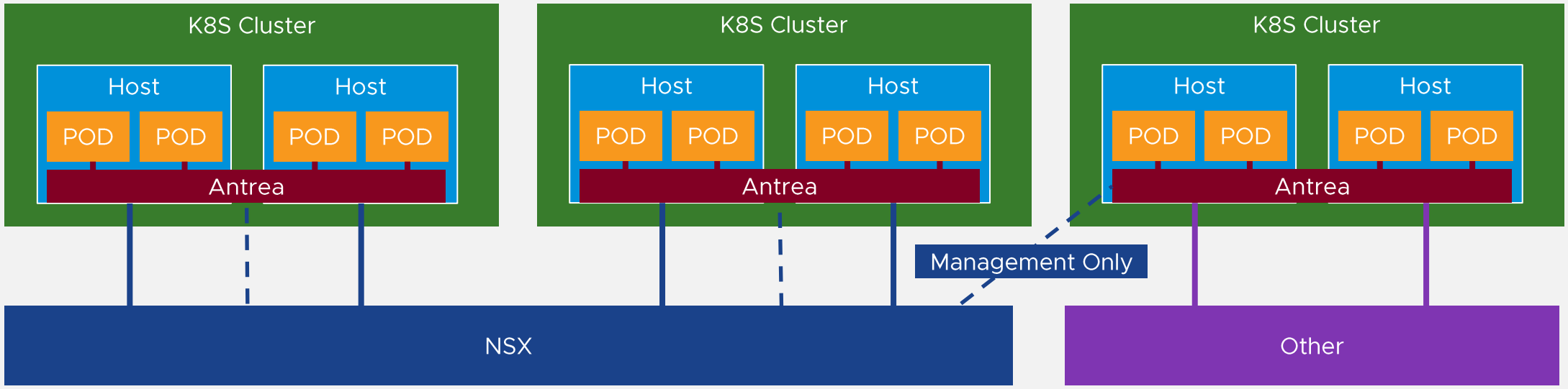
Pod network interface is NSX port

Monolithic data plane as clusters, hosts, and pods scale.



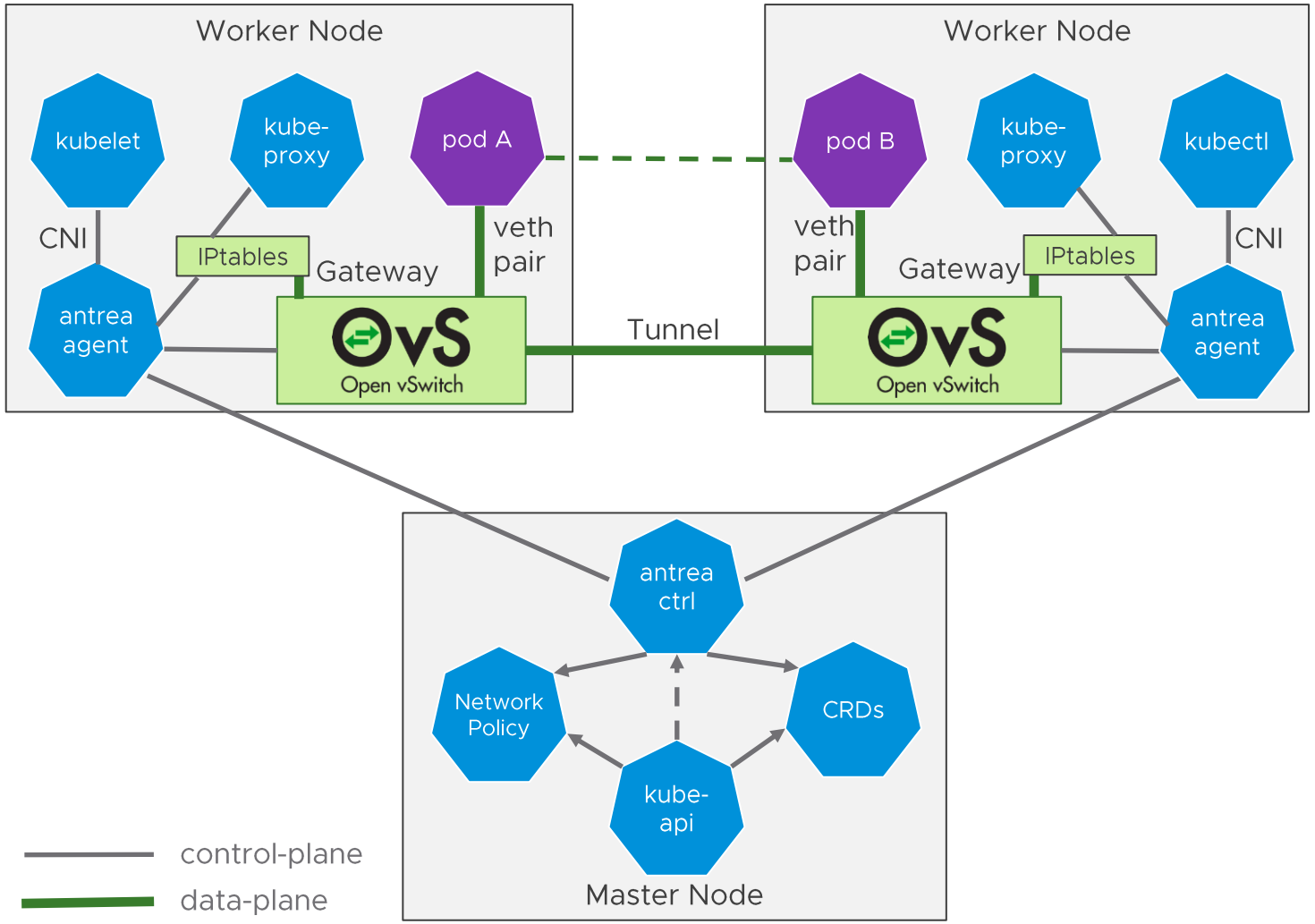
Scale Out with Antrea

Antrea creates autonomous data plane for K8S clusters – only host is connected to NSX
NSX not responsible for policy enforcement or transit – efficient scale out
Antrea also works in non-NSX environments
NSX will be able to manage policy distribution and visibility in NSX Inferno



Project Antrea Architecture

Open vSwitch provides a flexible and performant data plane.



Supports K8S cluster networking

Antrea Agent

- Manages Pod network interfaces and OVS bridge.
- Creates overlay tunnels across Nodes.
- Implements NetworkPolicies with OVS.

Antrea Controller

- Computes K8s NetworkPolicies and publishes the results to Antrea Agents.

Open vSwitch as dataplane

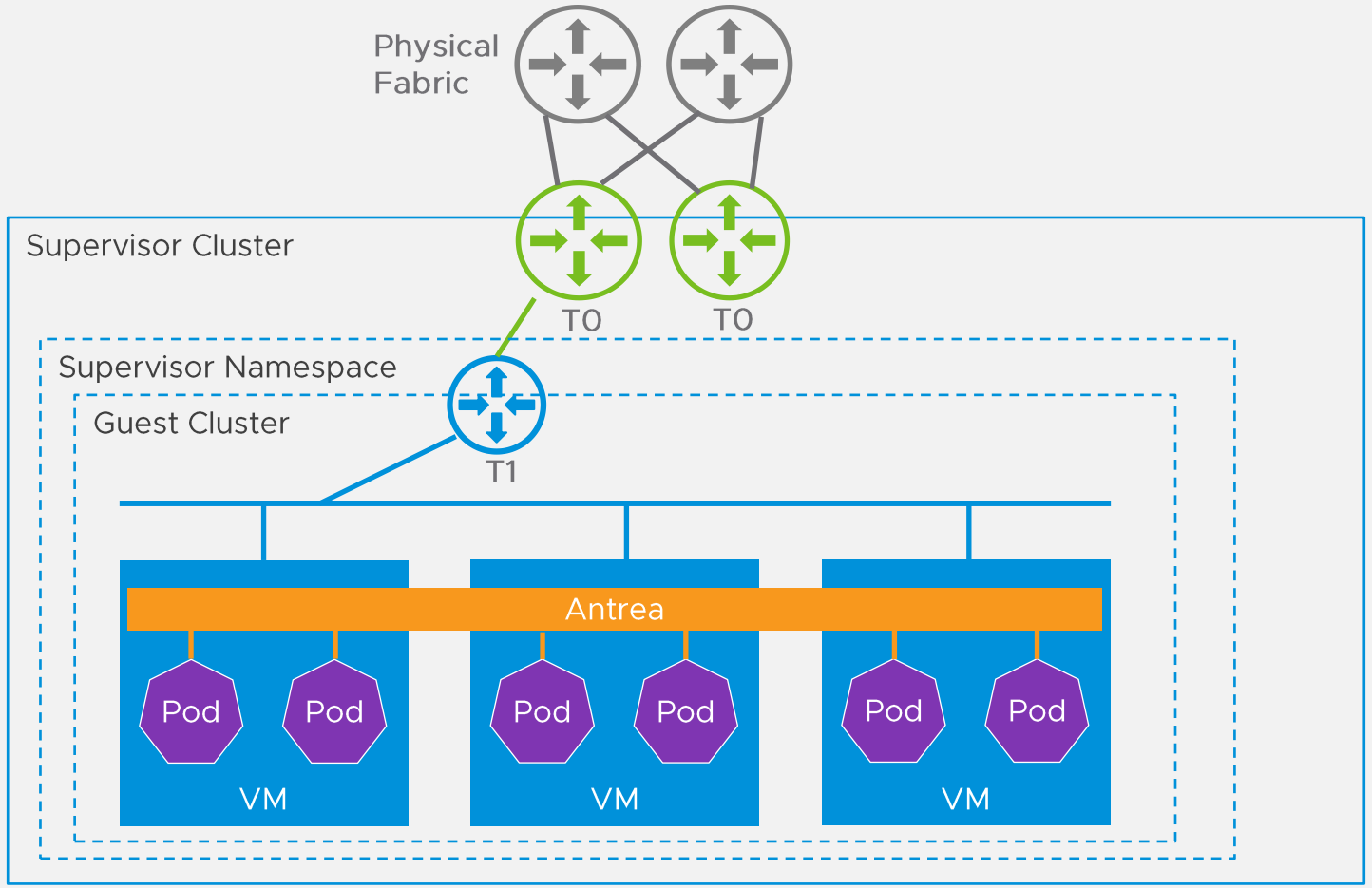
- Antrea Agent programs Open vSwitch with OpenFlow flows.
- Geneve, VXLAN, GRE, or STT tunnel between nodes
- Also supports policy-only and no-encap modes

Built with K8S technologies

- Leverages K8S and K8S solutions for API, UI, deployment, control plane, and CLI.
- Antrea Controller and Agent are based on K8S controller and apiserver libs.

Guest Cluster with Antrea Encapsulated

NSXT encapsulation between nodes, any number of VM subnets



Guest cluster has isolated L2 segment in NSX

VM-to-VM traffic encapsulated by NSX

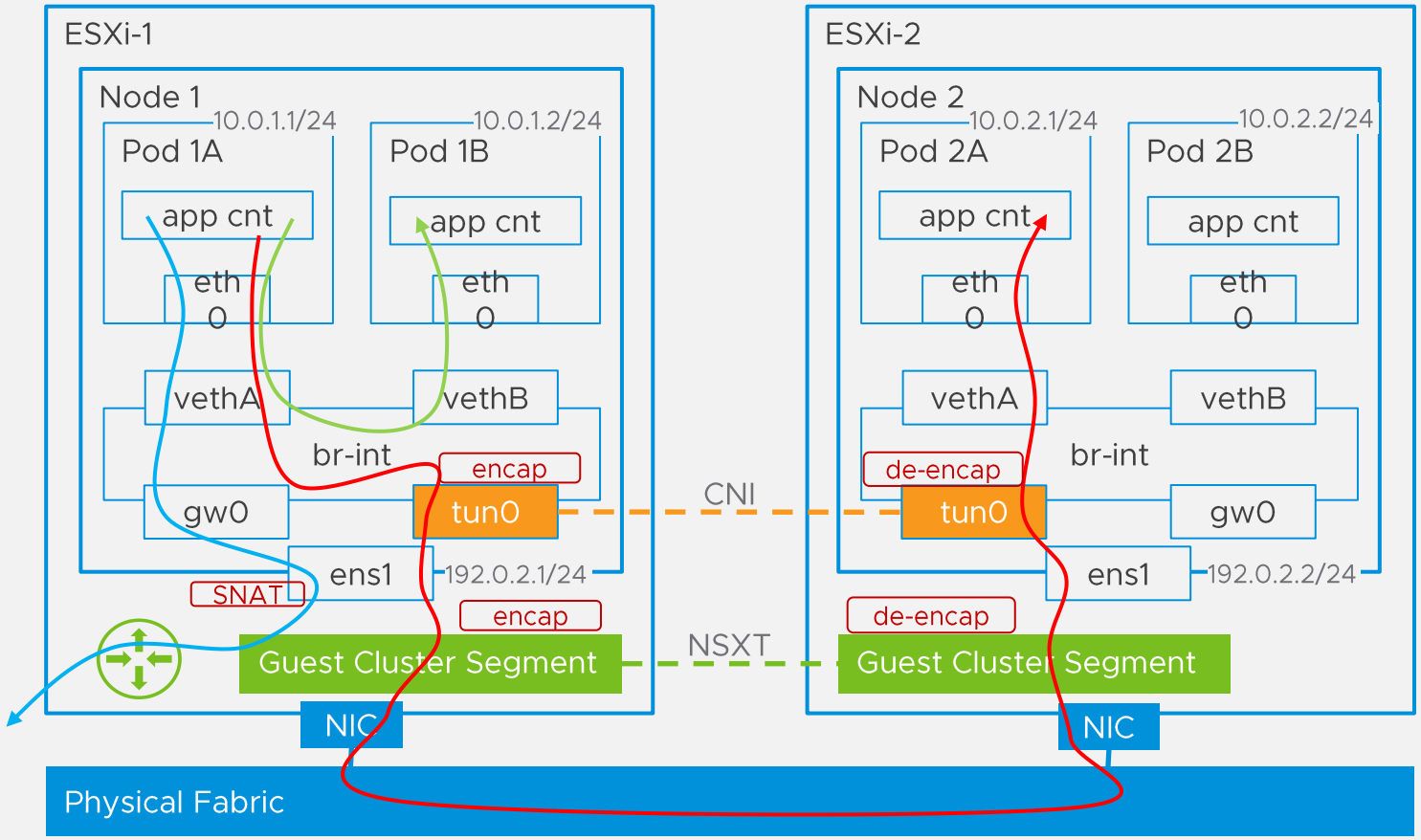
Antrea data plane is autonomous and not controlled by NSX

Pod-to-pod traffic encapsulated between VMs (Geneve or VXLAN)

Network Policy enforced by Antrea

Guest Cluster with Antrea Encapsulated

NSXT encapsulation between nodes, any number of VM subnets



Intra-Node Pod-to-Pod Traffic

Inter-Node Pod-to-Pod Traffic

Traffic to external / Node network

Intra-Node Traffic

- Does not leave the OVS bridge.

Inter-Node Traffic

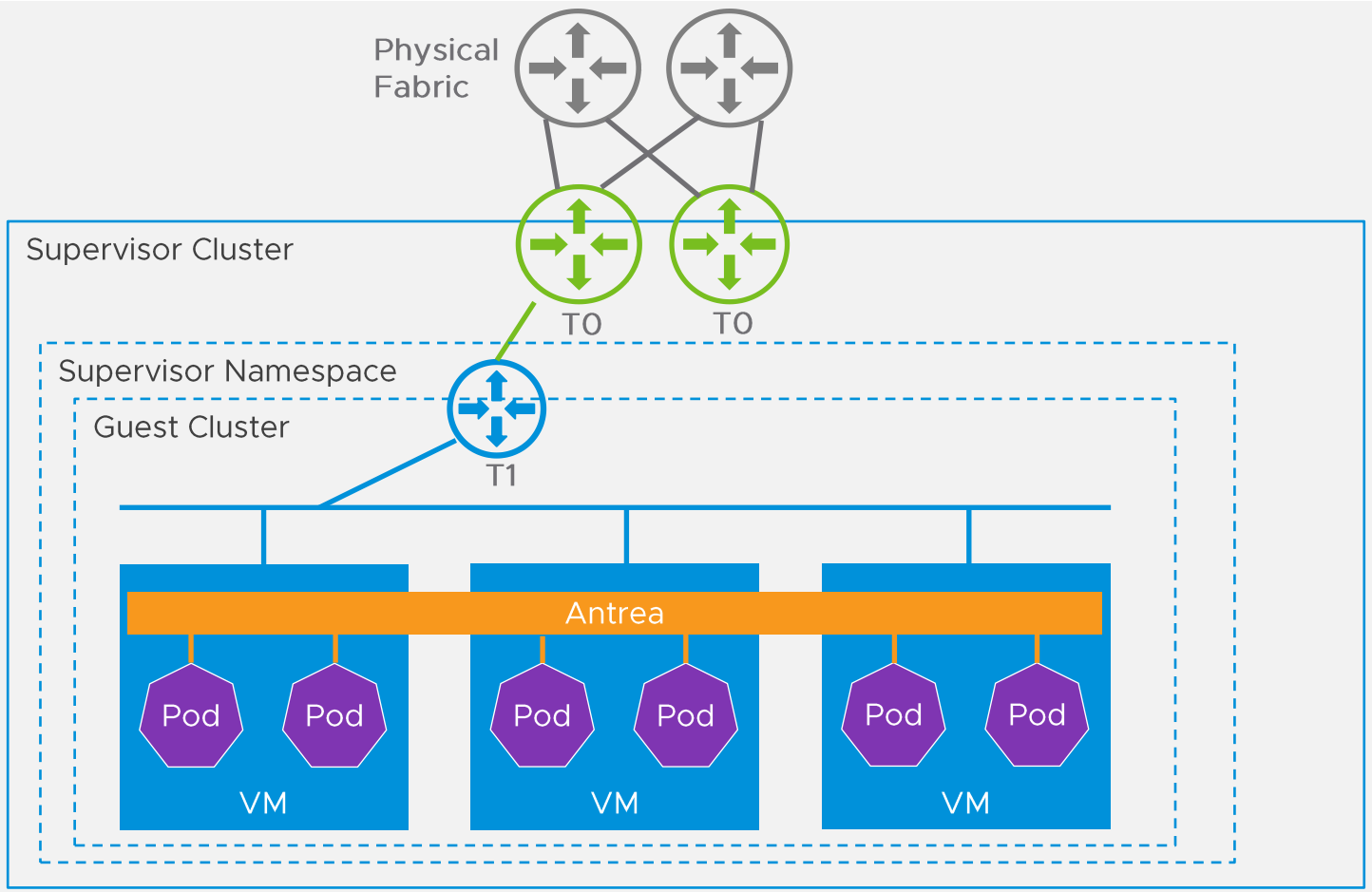
- Transmitted to the destination node via overlay tunnels.
- OVS flow based tunneling

Traffic from a Pod to external network or another Node

- SNAT to the Node IP (by an iptables rule)

Guest Cluster with Antrea Non-Encapsulated

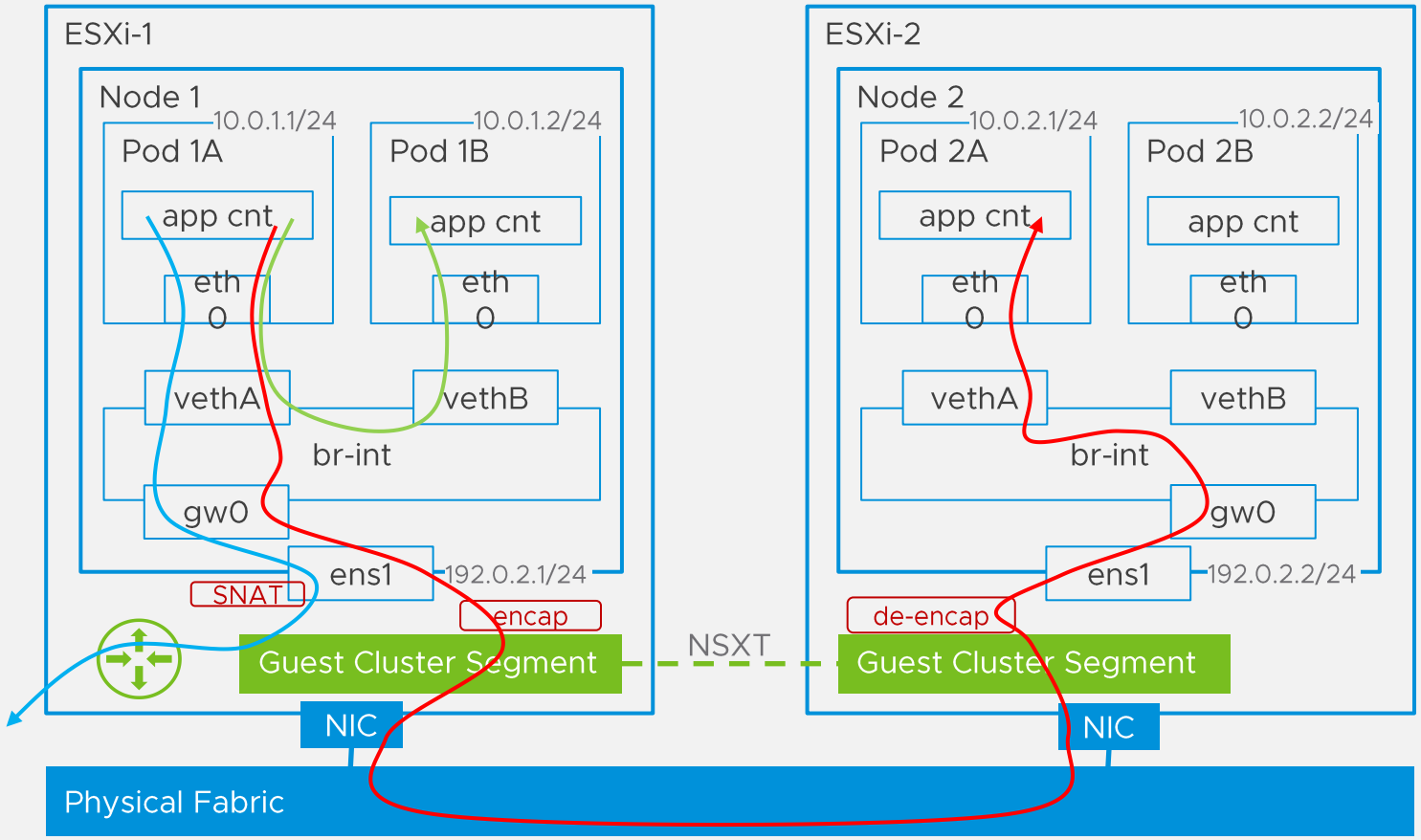
NSXT encapsulation between nodes, single large subnet



Pod-to-pod traffic forwarded between VMs

Guest Cluster with Antrea Non-Encapsulated

NSXT encapsulation between nodes, single large subnet



Intra-Node Pod-to-Pod Traffic

Inter-Node Pod-to-Pod Traffic

Traffic to external / Node network

Intra-Node Traffic

- Does not leave the OVS bridge.

Inter-Node Traffic

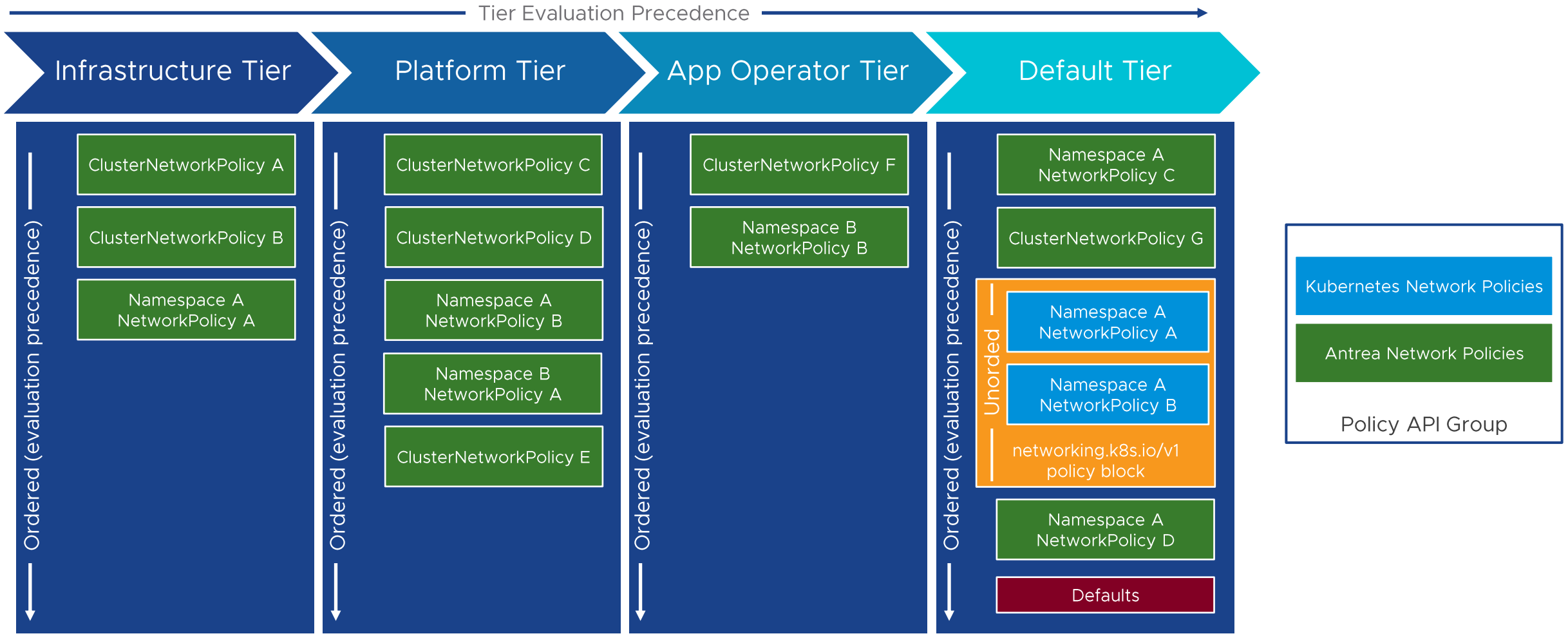
- Antrea tracks pod/node locations and updates routes
- Transmitted to the destination by forwarding

Traffic from a Pod to external network or another Node

- SNAT to the Node IP (by an iptables rule)

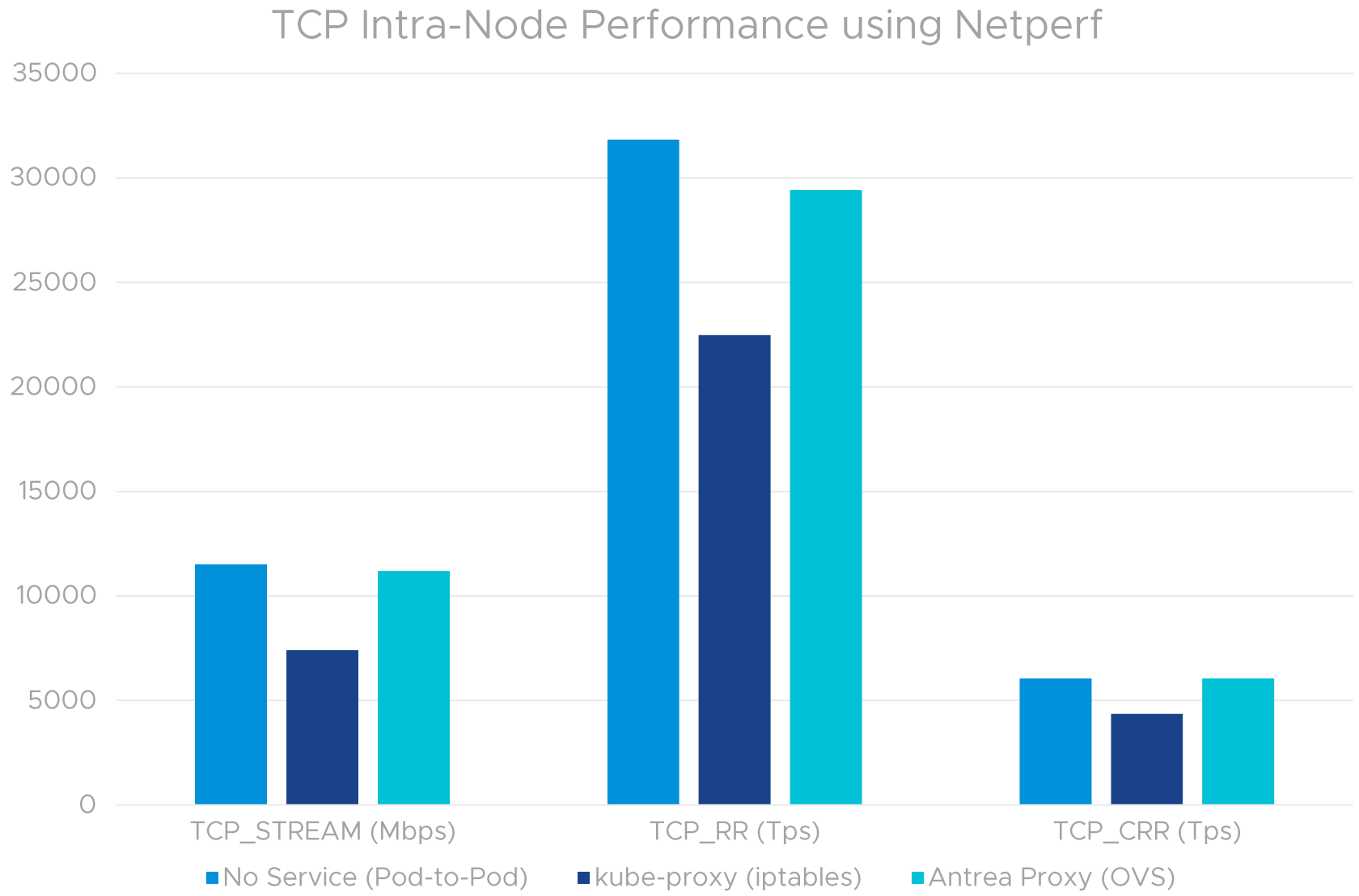
Policy Model

Antrea will allow native and Kubernetes policies to co-exist.

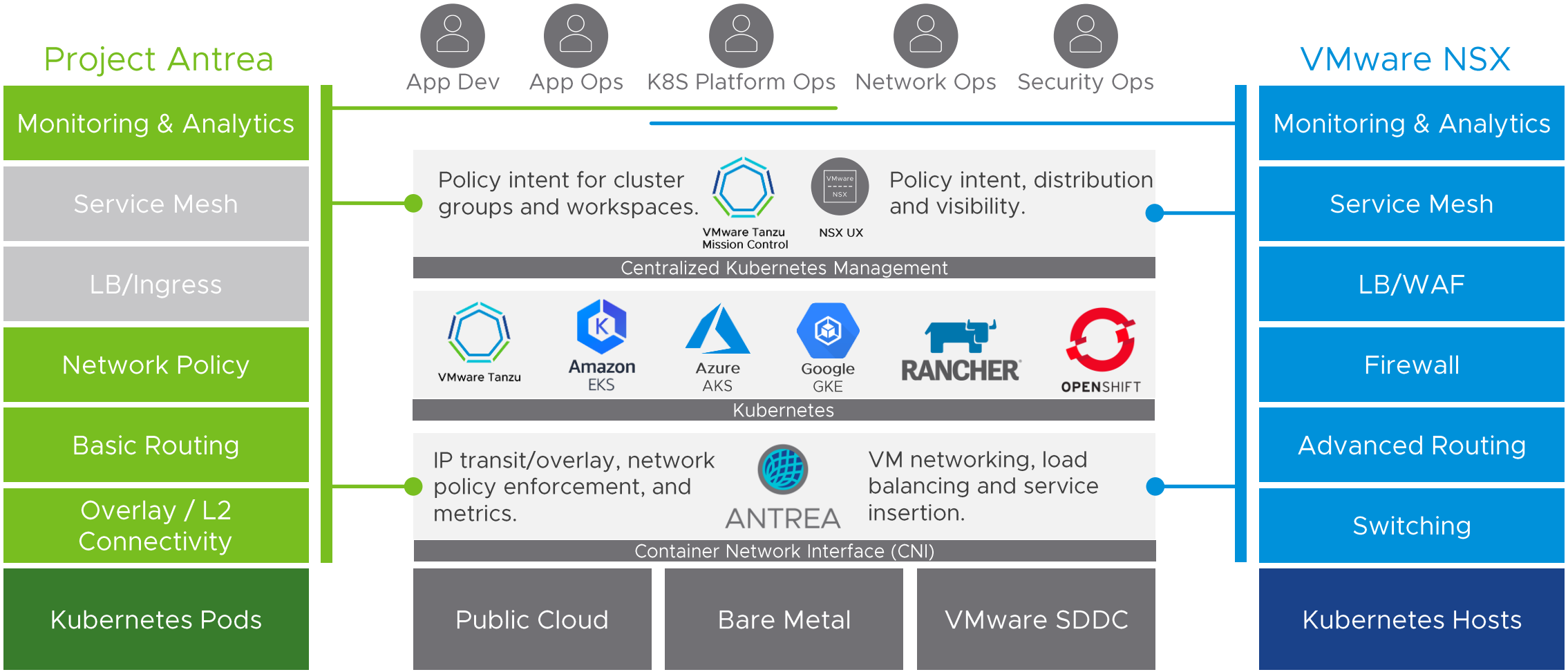


Pod-to-Service Performance

kube-proxy vs Antrea proxy



Antrea + NSX = Better Together



Tanzu Service Mesh

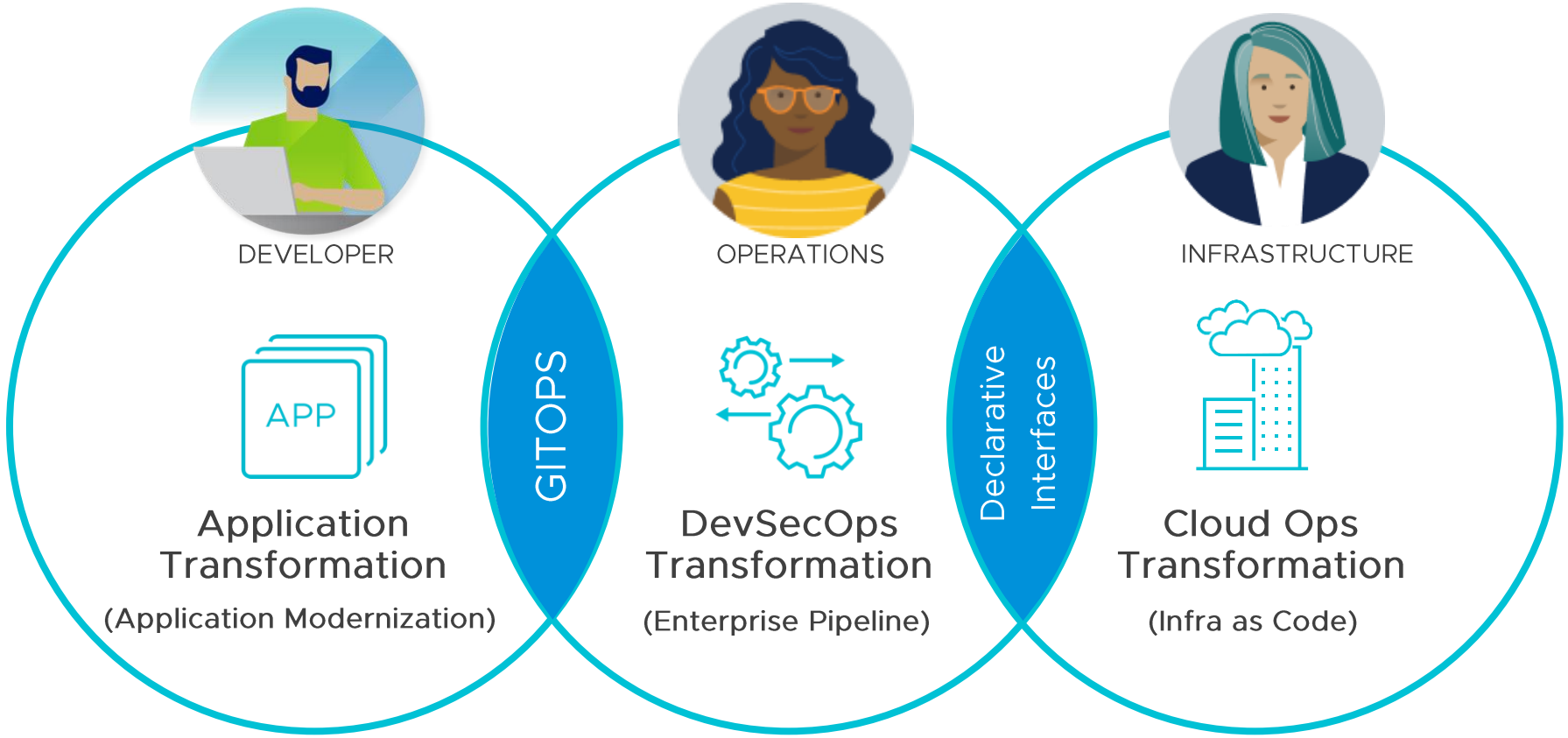
Overview

Presenter

Team

June 2022

Changing the Interactions Between Functions



Cloud-native patterns to support innovation, scaling, resiliency, and ecosystems

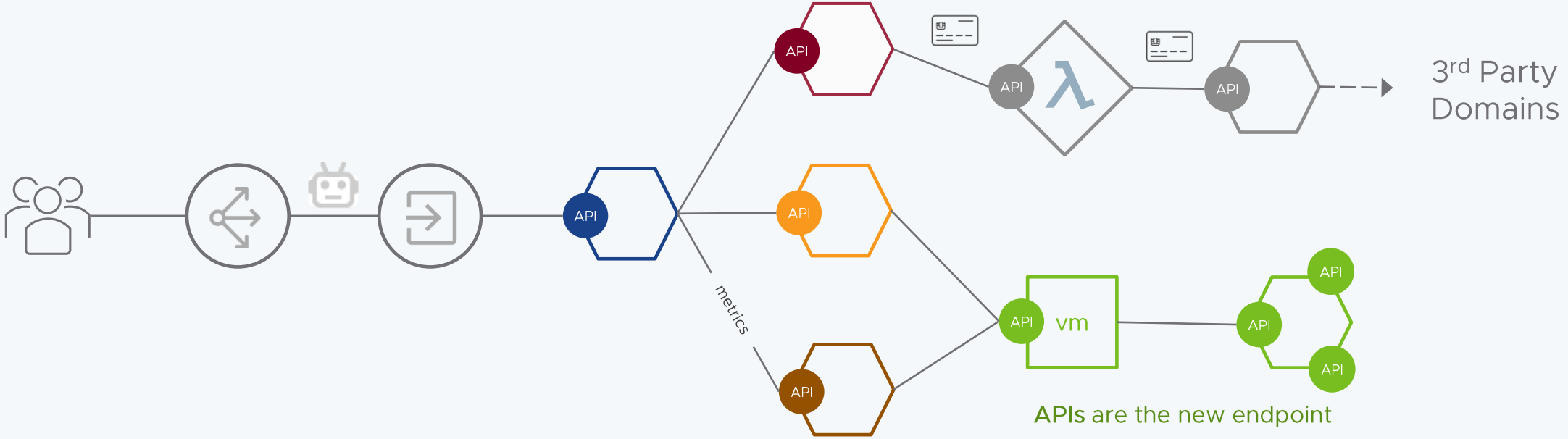
Continuously delivering high quality, more secure code to production faster and more frequently

Automation, Control and govern cost, performance and security across clusters and clouds

Modern Applications Challenges

How to consistently observe, secure, and provide compliance to cloud native apps?

Trusted Perimeter has dissolved	Explosion in # of microservices and APIs – risky blind-spots	Breaches moving deep within application layer	Extensive Reliance on 3rd parties increases risk



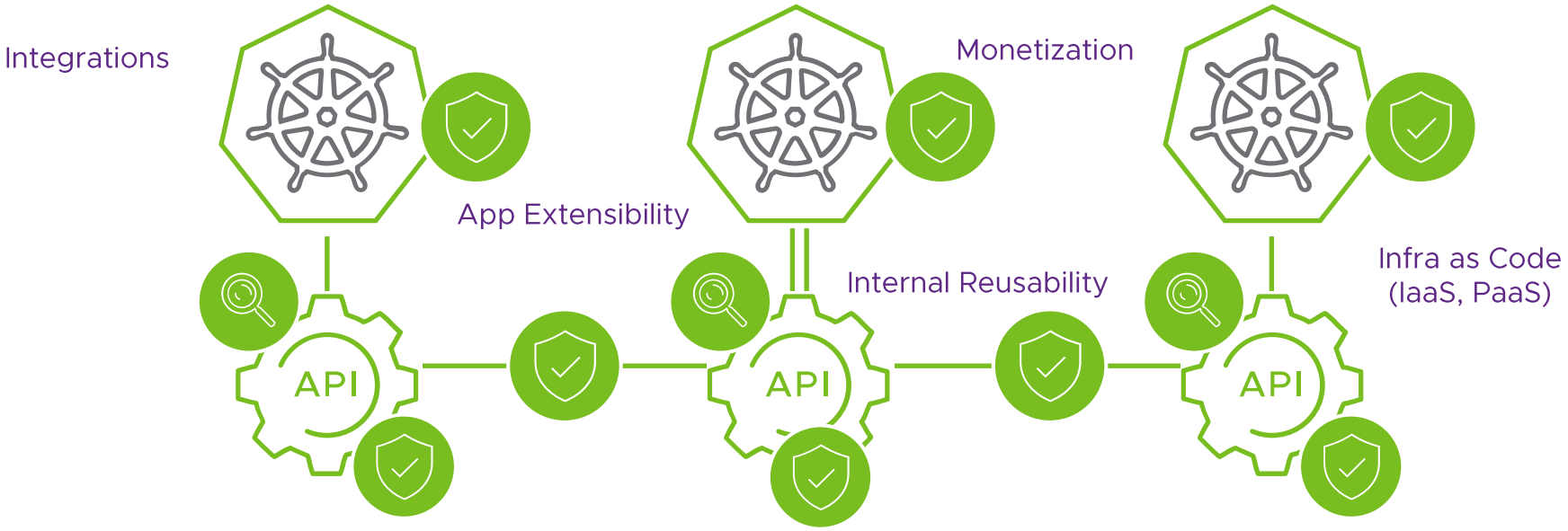
Kubernetes

Public Clouds

VMs / Monoliths

Strong Security Designed for Modern Apps

APIs are the new endpoint.

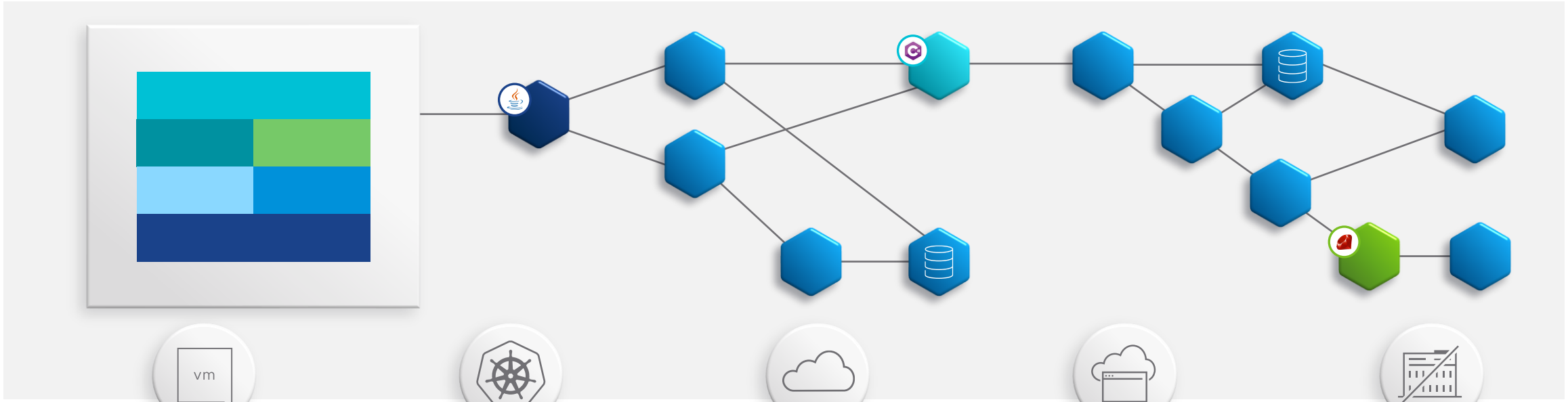


Operate within guardrails	End-to-end encryption	API Protection: WAF, API Discovery, Baseline Normal Patterns, Stop Anomalous Behavior	DLP : PII & PCI data tracking and leakage prevention

Modern Apps Secure Connectivity

Requirements: consistent visibility, control, and security for apps across any cloud

Multi-platform and multi-cloud federation | Centralized visibility and remediation | Global policies for users, services and data | Centralized security, audit, and compliance | No changes to application code



Modern Applications Bring Unique Challenges

At the Edge

How can I ensure only legitimate traffic gets in?

E-W Security

How do I ensure only the right services can talk to each other?

Across clouds, across clusters?

Container Runtime

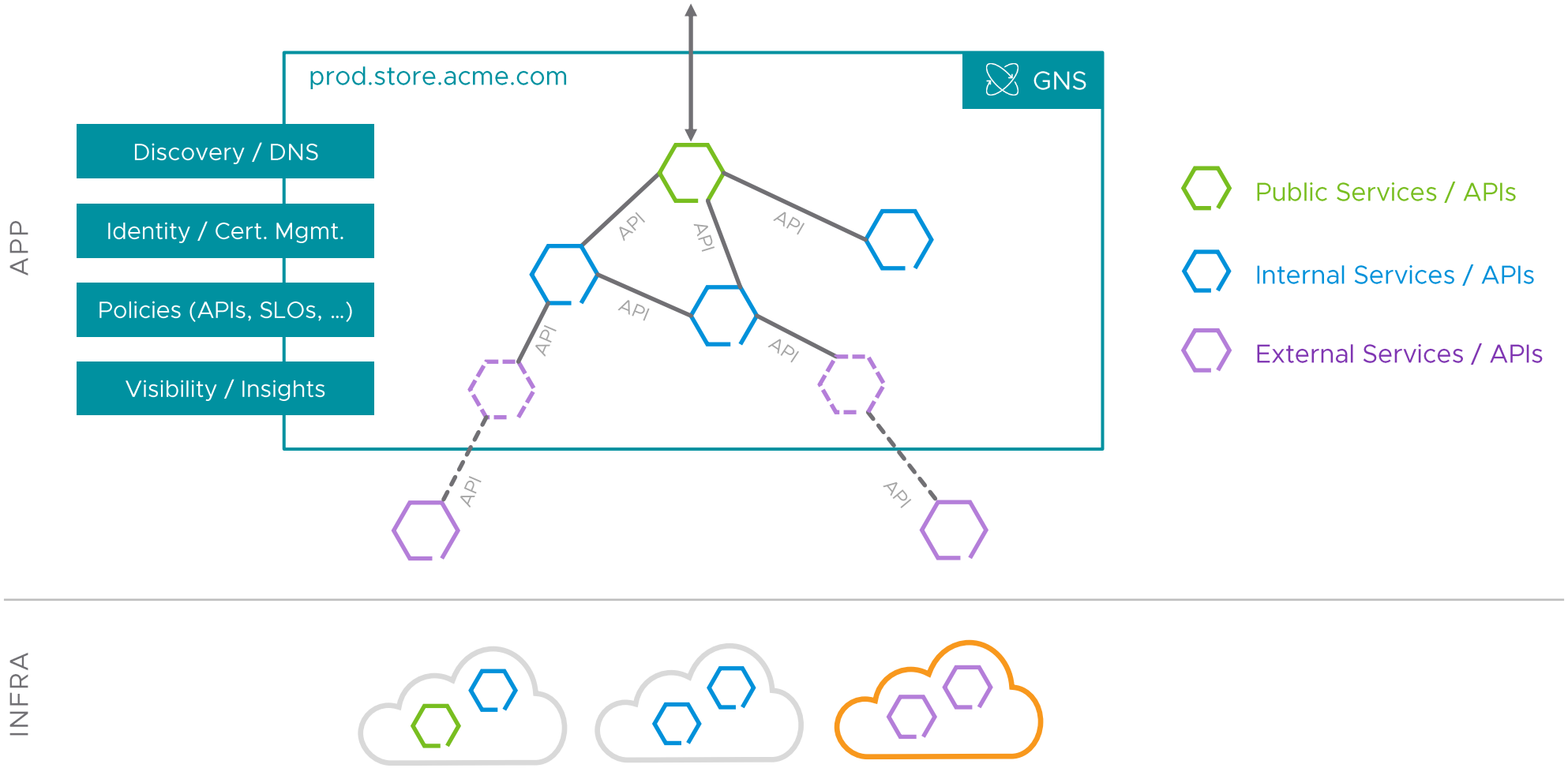
How can I ensure my containers are operating within expected guardrails?

Multiple Clouds / Platforms

vmware aws kubernetes Google Kubernetes Engine Azure

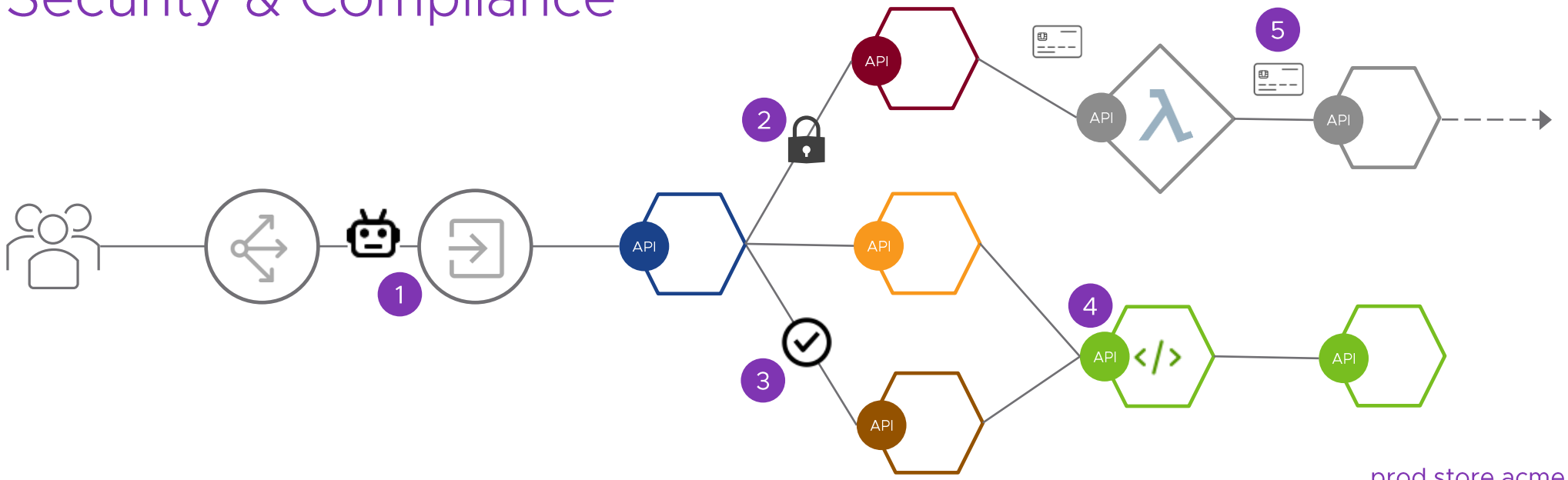
Global Namespace

End to end connectivity and security for all microservices and APIs



ZT Security & Compliance

GNS

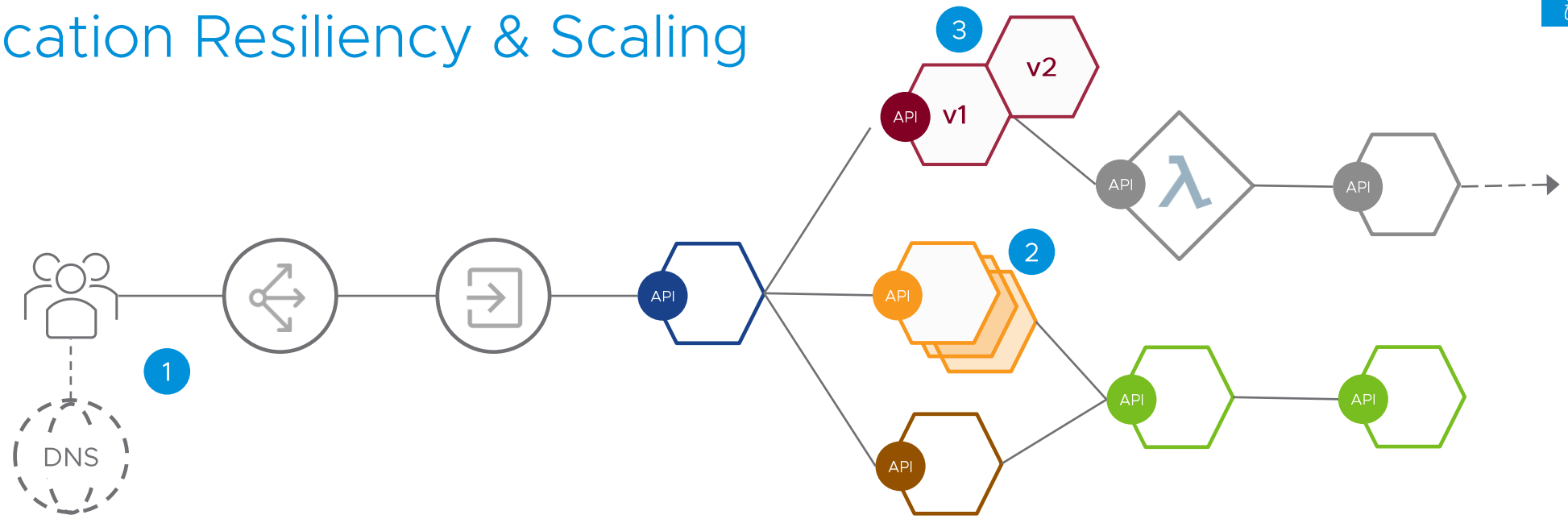


TSM Enterprise

1. K8s Ingress Security (WAF, BOT Detection, TLS, DDoS)
2. e2e mTLS Encryption for E-W
3. Least Privilege Access w/ Auditing (Users, Svcs/APIs, Data)
4. API Security (Baselining, Drift Detection, Threat Protection)
5. PII Data Tracking & DLP

Protect users, apps, and PII / sensitive data for compliance with data privacy, data protection, and data sovereignty regulations

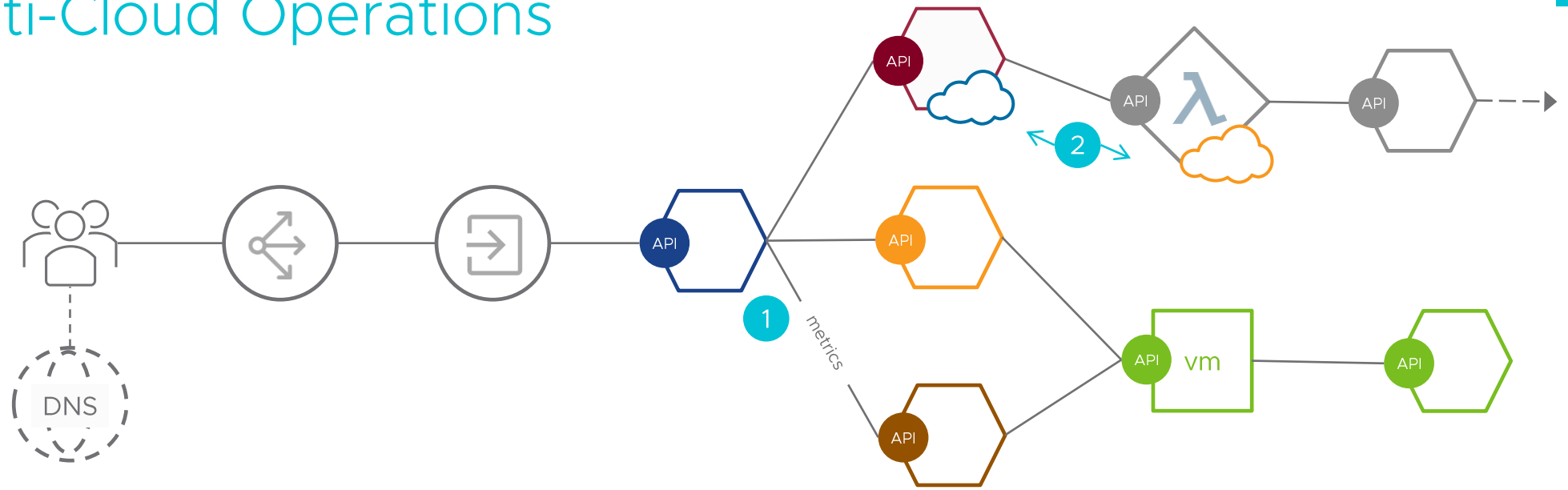
Application Resiliency & Scaling



1. GSLB (HA & Failover)
2. SLOs / SLIs Monitoring & Enforcement
3. Traffic Shifting / Progressive Upgrade

Meet service level objectives (SLOs) for compliance with application SLAs and performance targets

Multi-Cloud Operations



1. Service & API Discovery, Visibility, and Troubleshooting
2. Multi-Cloud & Multi-Runtime Connectivity (K8s, VMs, Serverless)
3. Elastic Scaling
4. Cloud Bursting
5. Declarative Config & GitOps Workflows for DevSecOps

Streamline operational agility and DevSecOps collaboration across multiple cloud environments

Top Three Takeaways

Connect, secure, scale, and operate across multiple clouds

ZT Security & Compliance

Protect PII and sensitive data for compliance with data privacy and data sovereignty regulations

Application Resiliency & Scaling

Meet service level objectives for compliance with SLAs and performance targets

Simplified Multi-Cloud Ops

Improve agility and DevSecOps collaboration across multiple cloud environments

Thank You