Container and Kubernetes security policy design

10 critical best practices

Reza Ramezanpour

Developer Advocate
Tigera

TIGERA

Agenda

- Calico is everywhere
- Application modernization
- Container security
- Network segmentation
- Best Practices for Securing a Kubernetes Environment
- Monitoring
- DEMO

TIGERA

00

Calico is everywhere

One project to rule them all!

PROJECT CALICO

A pluggable dataplane that rocks!

CALICO CLOUD

CALICO ENTERPRISE

Standard

eBPF

Windows

VPP

PROJECT CALICO

https://projectcalico.org

@projectcalico

https://github.com/projectcalico/community

https://slack.projectcalico.org

https://discuss.projectcalico.org

9000+
Slack channel members

550+
Contributors

2,000,000+
Nodes powered by Calico every day

TIGERA

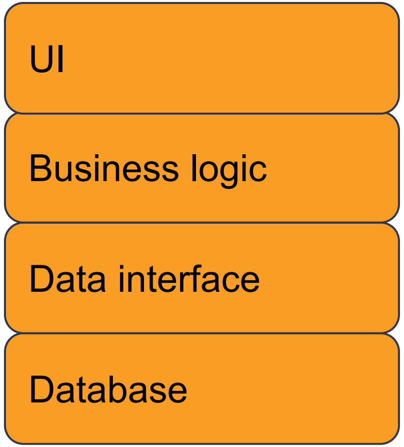
April 18-21
Meet us at booth S28

01

Application Modernization

What is Application modernization?

Physical server era



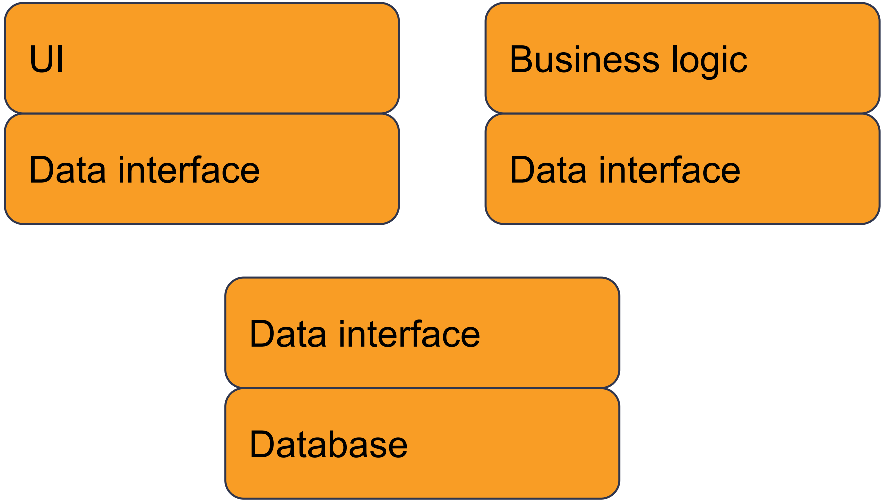
UI

Business logic

Data interface

Database

Virtualization



UI

Data interface

Business logic

Data interface

Data interface

Database

What is Application modernization?

Legacy applications

Difficult to maintain

Difficult to update

Less secure

Massive piece of software

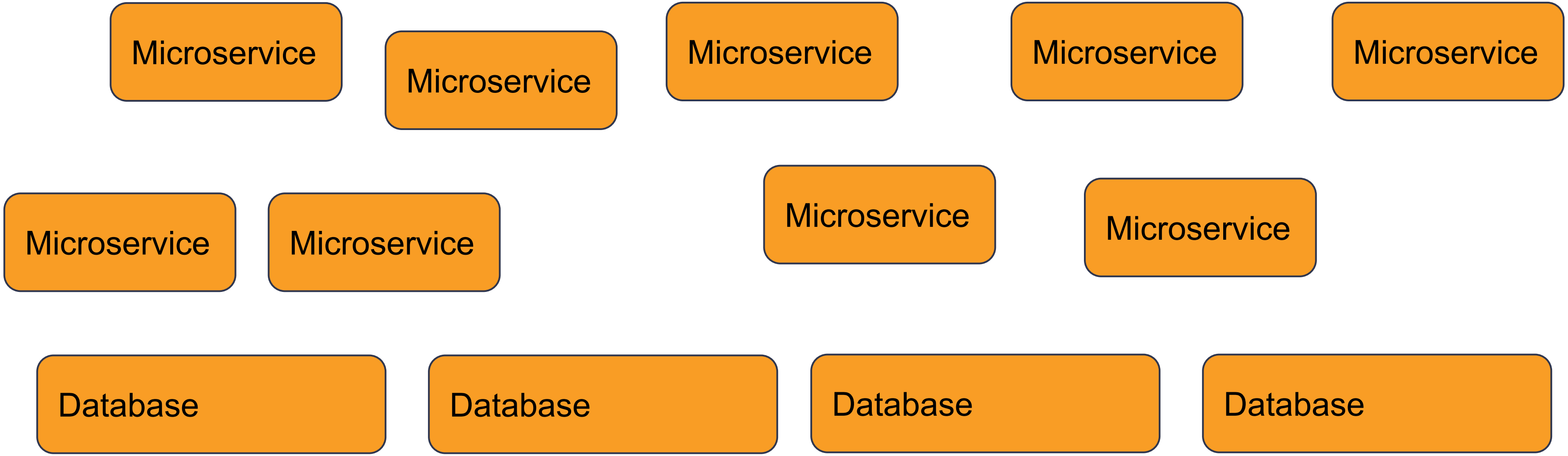
Modern application

Significant investment in people

Change in the processes

Change of technology

Cloud, cloud-native



Microservice

Microservice

Microservice

Microservice

Microservice

Microservice

Microservice

Microservice

Microservice

Database

Database

Database

Database

02

Container Security

Securing Images

- Include your application in a container image
- Include as little as possible
- Scan your images

Image registry

Public image registry

1. Large community and ecosystem
2. Ease of access
3. Wide range of images available
4. Cost-effective

Private image registry

1. Compliance
2. Privacy
3. Greater control
4. Requires configuration and maintenance
5. Can get expensive

03

Network Segmentation

Namespace

TIGERA

Segmentation tools

- Namespace
- labels
- Security policies
- Role Based Access Control (RBAC)

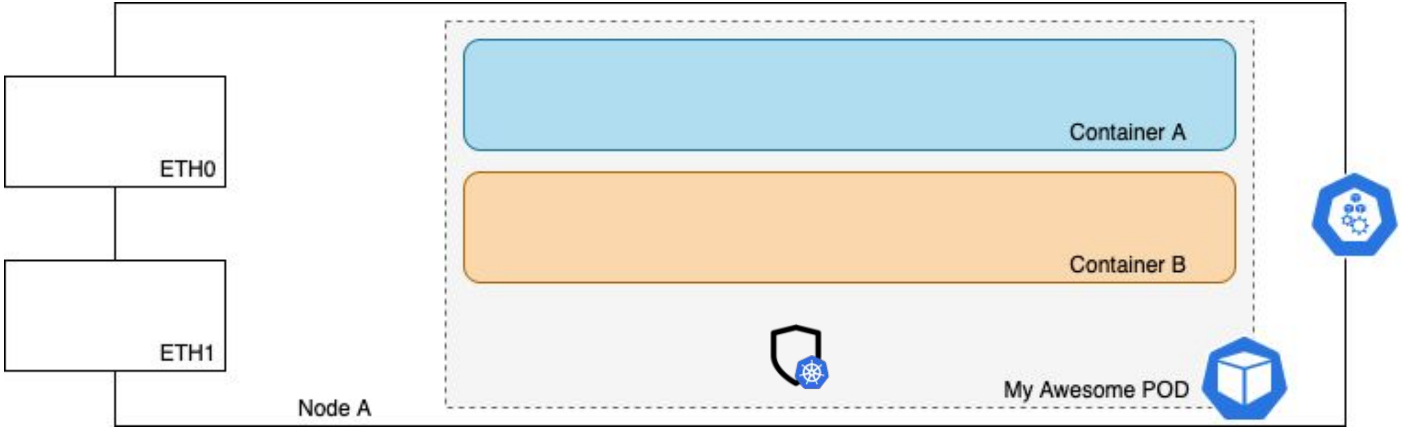
04

Best Practices for Securing a Kubernetes Environment

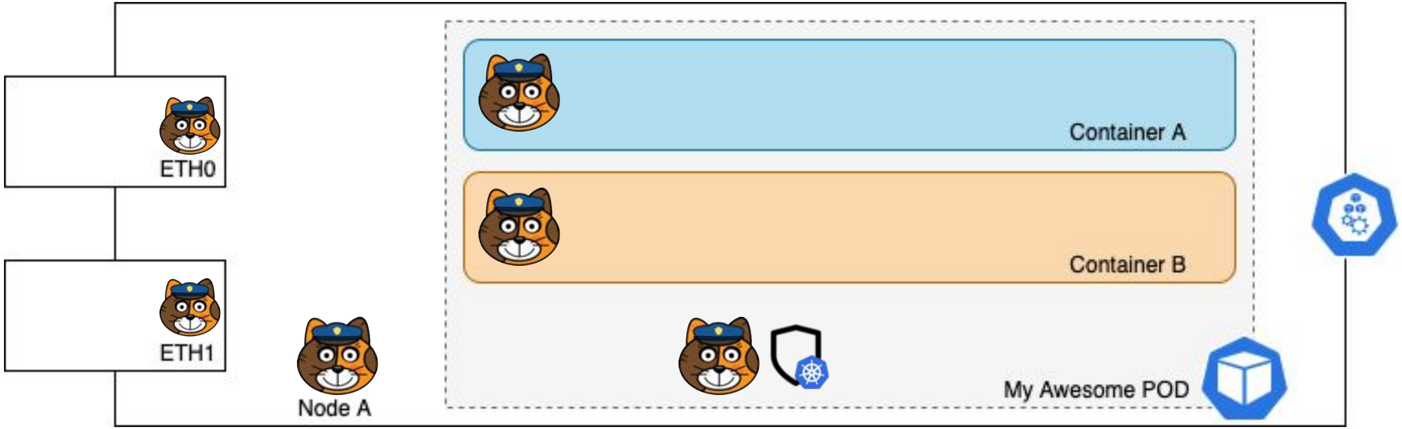
KNP, WEP, and HEP

TIGERA

Kubernetes network policy



Calico security policy

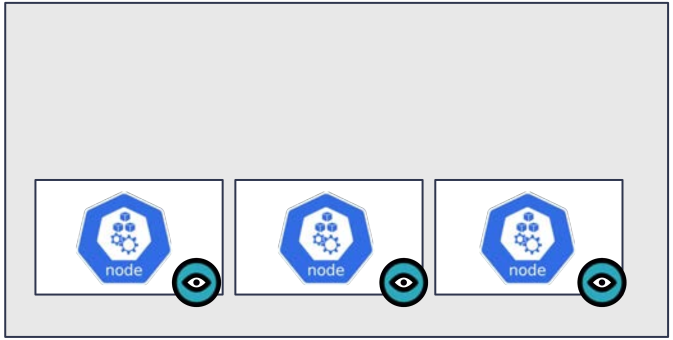


05

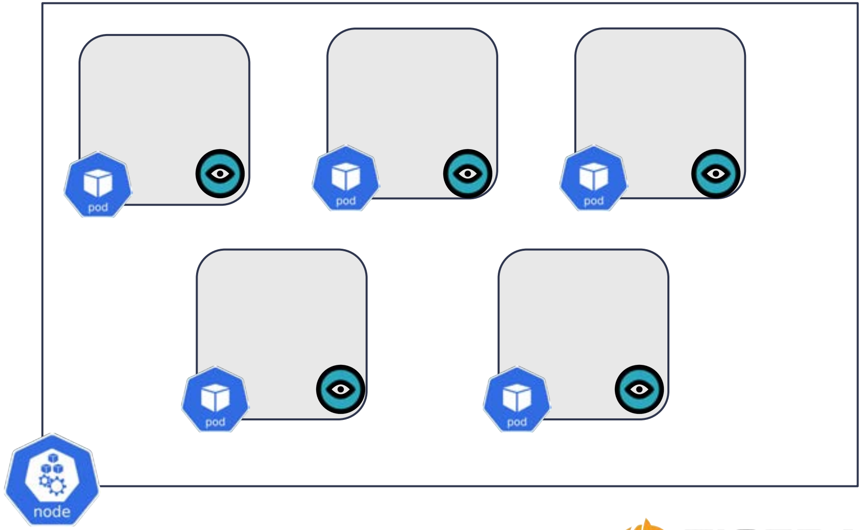
Monitoring

Methods of monitoring

Infrastructure monitoring



Application monitoring



06

DEMO

Do-It-Yourself Resources

Stuff used for the demo:

https://github.com/frozenprocess/Tigera-Presentations

When things are not working:

Github: https://github.com/frozenprocess

Twitter: https://twitter.com/fr0zenprocess

Linkedin: https://www.linkedin.com/in/rramezanpour/

April 18-21
Meet us at booth #S28