Container and Kubernetes security policy design

best practices

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!

TIGERA

PROJECT CALICO

TIGERA

A pluggable dataplane that rocks!

Standard

eBPF

Windows

VPP

TIGERA

PROJECT CALICO

https://projectcalico.org

@projectcalico

https://github.com/projectcalico/community

https://slack.projectcalico.org

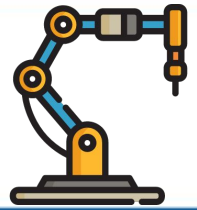
https://discuss.projectcalico.org

9000+
Slack channel members

550+
Contributors

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

TIGERA



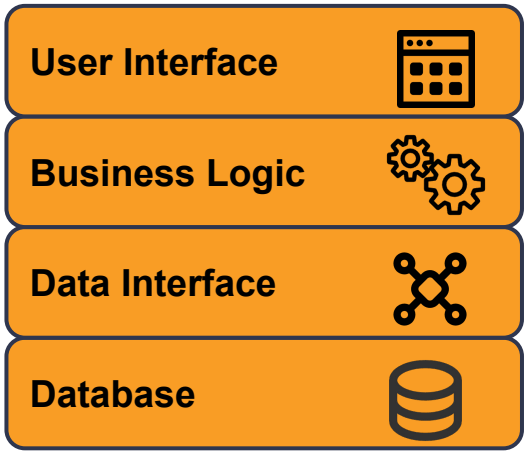
01

Application Modernization

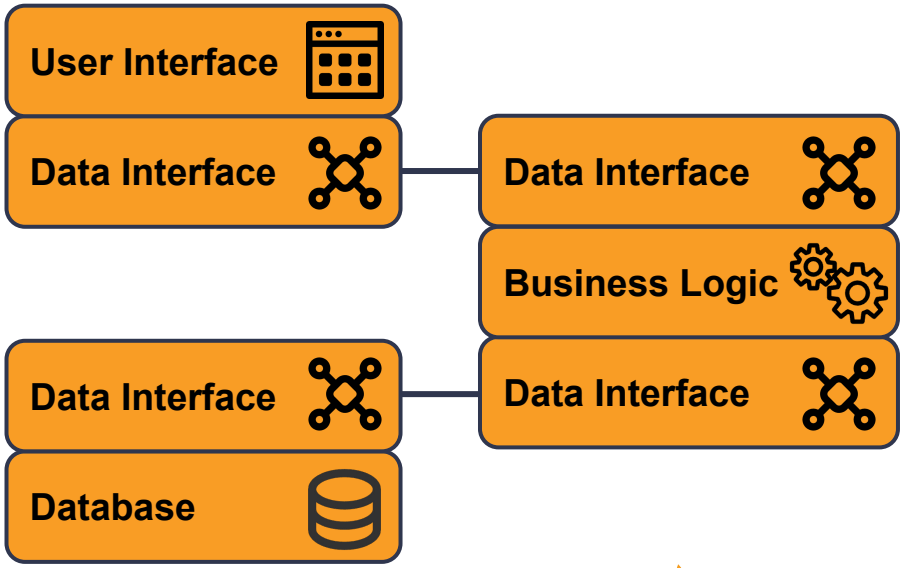
TIGERA

What is Application modernization?

Physical server era



Virtualization



What is Application modernization?

Legacy applications

Difficult to maintain

Difficult to update

Less secure

Massive piece of software

Modern application

Significant investment in people

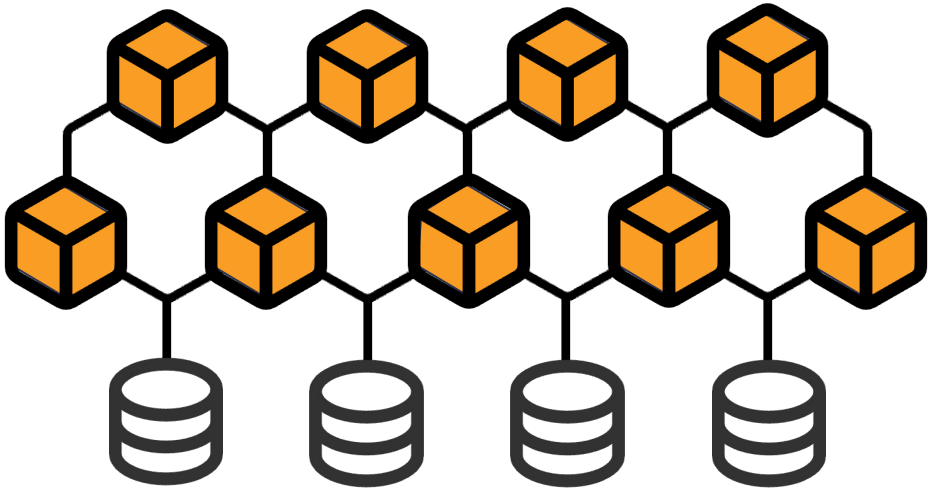
Change in the processes

Change of technology

Cloud, Cloud-Native

Microservices

Databases



02

Container Security

TIGERA

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

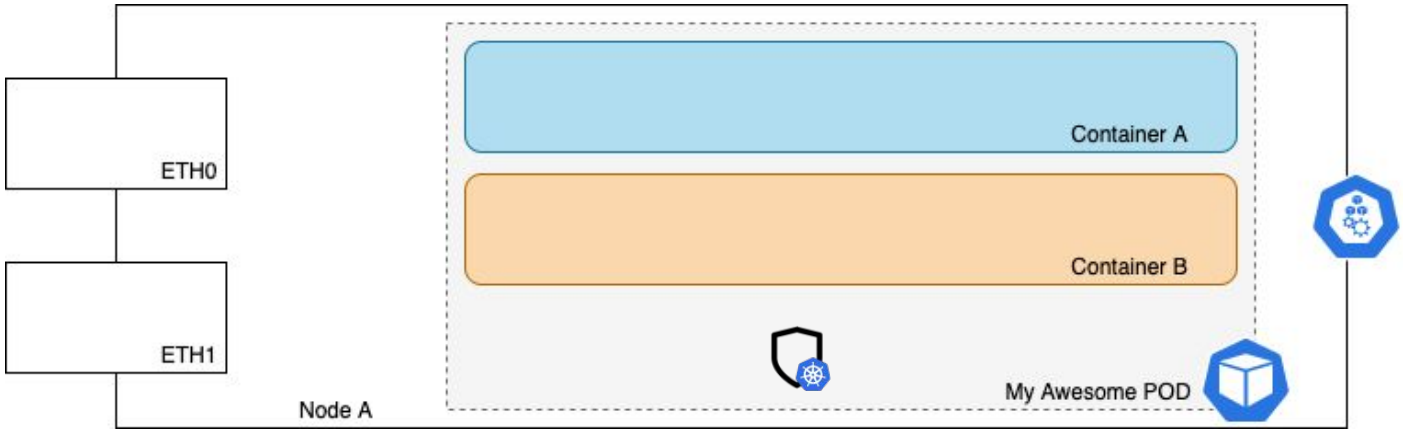
- Namespace
- Labels
- Security policies
- Role Based Access Control (RBAC)

Best Practices for Securing a Kubernetes Environment

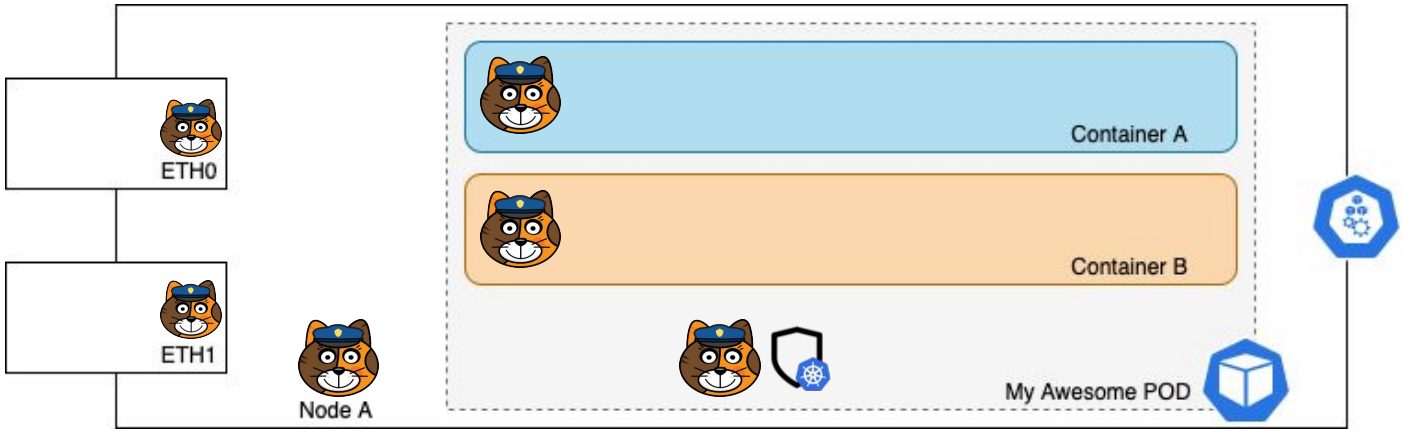
KNP, WEP, and HEP

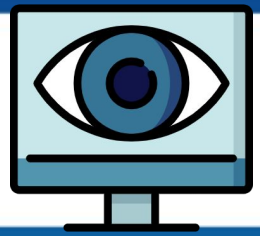
TIGERA

Kubernetes Network Policy



Calico Security Policy



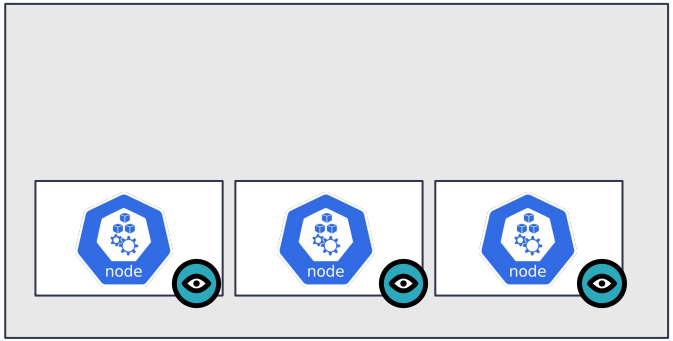


05 Monitoring

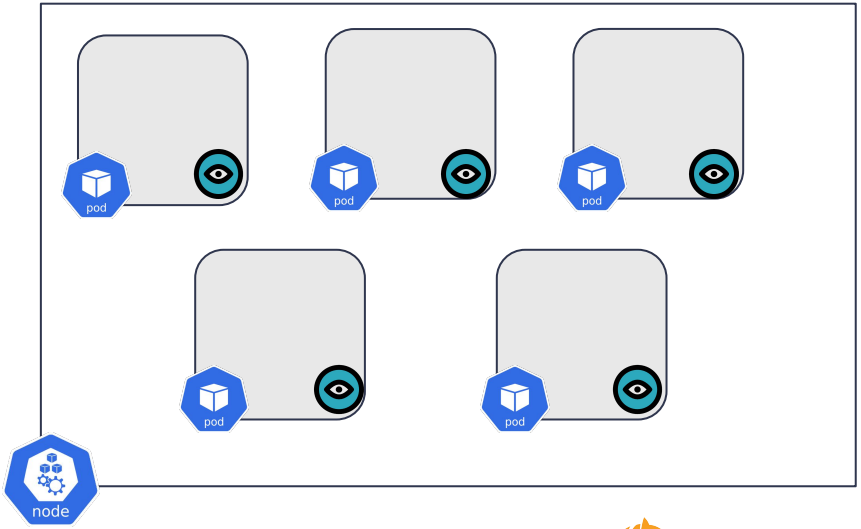
TIGERA

Methods of Monitoring

Infrastructure Monitoring



Application Monitoring



TIGERA

06

DEMO

TIGERA

Do-It-Yourself Resources

Stuff used for the demo:
https://github.com/regisftm/owasp-toronto

When things are not working:

Github: https://github.com/regisftm
Linkedin: https://www.linkedin.com/in/regismartins

Photo by Clark Young on Unsplash