How to Secure Kubernetes and Applications with Calico on AKS

Jintao Zhang

Cloud Native Team Leader
API7.ai

CalicoCon + Cloud-Native Security Summit

Sponsored by aws Red Hat SUSE

Presented by TIGERA

How to Secure Kubernetes and Applications with Calico on AKS

Jintao Zhang

CalicoCon + Cloud-Native Security Summit

Sponsored by aws Red Hat SUSE

Presented by TIGERA

How to Secure Kubernetes and Applications with Calico on AKS

Jintao Zhang
Cloud Native Team Leader
API7.ai

CalicoCon + Cloud-Native Security Summit

Sponsored by aws Red Hat SUSE

Presented by TIGERA

Who am I

- I’m Jintao
- Apache APISIX PMC
- Calico Big Cats
- Kubernetes Ingress NGINX manatainer
- Microsoft MVP
- It’s my first time CalicoCon speak

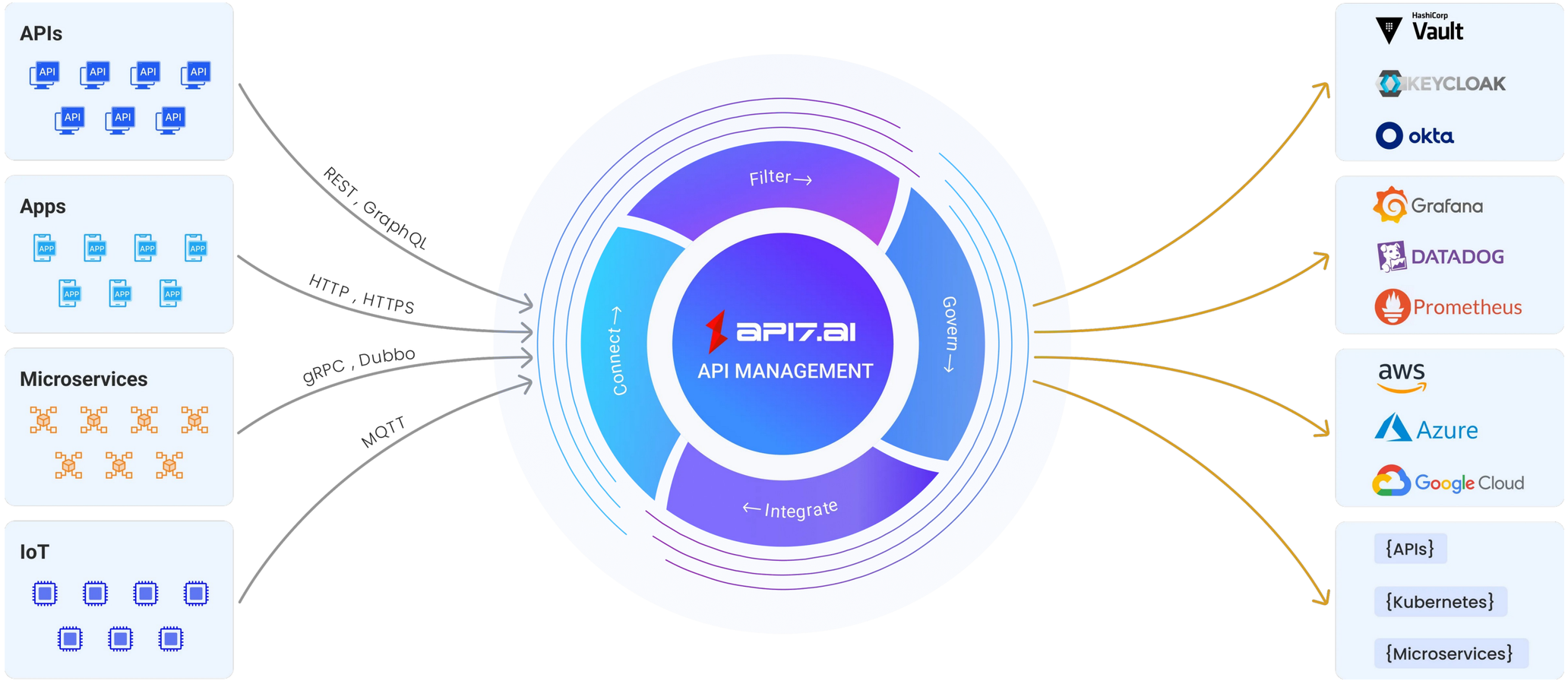
Agenda

1 - Background introduction
2 - Calico with AKS
3 - Security issues in Kubernetes
4 - How to improve security with Calico
5 - The future

About API7.ai

- Creator of Apache APISIX (2019)
- Created many open source projects
  - Apache APISIX Ingress controller
  - Service Mesh base on APISIX - Amesh

About API7.ai



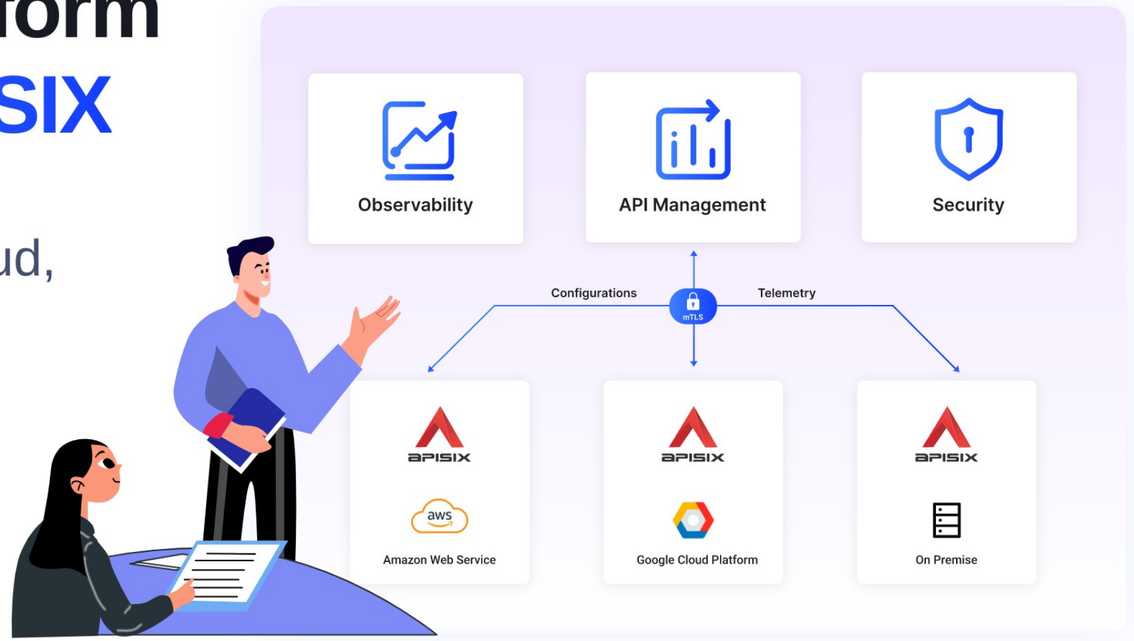
About API7 Cloud

The Centralized API Platform Powered by Apache APISIX

Manage your APIs deployed on any cloud, connect them efficiently and reliably.

Sign up for Early Access

Read Docs →



Why choose Kubernetes

- Efficient deployment and delivery of applications
- Improve overall usability
- Declarative configuration, deploy in any environment
- OSS and Ecology

Why choose Azure Kubernetes Service(AKS)

Self managed

- Advantage
  - Freer
  - Choose your own components
- Disadvantage
  - Cost
  - High availability

Hosting

- Advantage
  - Cost(free control plane)
  - Simpler
  - Built-in support for Calico
- Disadvantage
  - Component selection is limited

How Calico work with AKS

- Policy mode
  - Work with Kubenet or Azure CNI
- Networking mode
  - VXLAN mode only
  - IPIP packets are blocked

Challenges under Kubernetes

- Attack surface increases
- Supply chain attack
- Privilege escalation
- Network security

- Resource security
- Data security
- Component security
- Runtime security

Why network security is important

- Almost all attack methods rely on the network
- The network is a vector for attackers
- Data can be protected over the network(preventing transmission)
- In the system, the network is the most interactive way

How to protect network security in Kubernetes

- NetworkPolicy
  - NetworkPolicy describes what network traffic is allowed for a set of Pods
  - NetworkPolicy is namespace scope, it is not very convenient

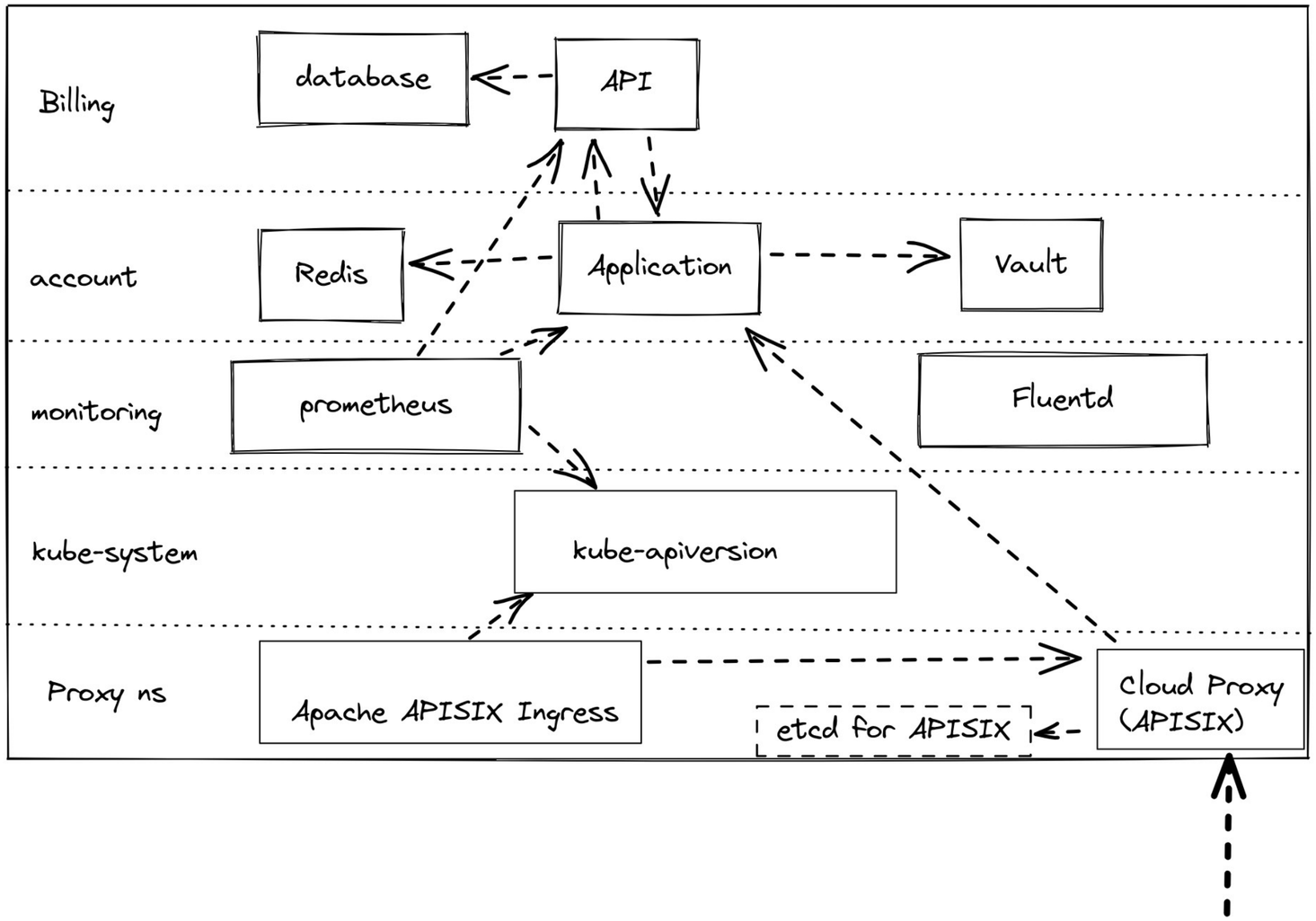
- mTLS
  - Automatic injection with tools like Istio
  - The application does it itself

How calico protects network security

- Provides two custom resources, GlobalNetworkPolicy and NetworkPolicy
  - Extends Kubernetes network policy
    - policy ordering/priority
    - deny rules
    - flexible match rules
    - can be integrated with Istio

How to apply in real scenarios

- Simplified Architecture Diagram
- Set GlobalNetworkPolicy to ensure namespace isolation
- Open for each component individually



Enable Azure Policy

- Azure Policy base on Gatekeeper v3
- Open Policy Agent (OPA)
- Strong constraints are available through Azure Policy
  - require each Deployment to contain the app label
  - Restricted images must come from private repositories

Why we choose Calico

- AKS native integration
- More powerful policy descriptions
- Active community
- Feature rich
- continuous evolution
  - eBPF dataplane

The future

- We want to try WireGuard Encryption
- Will try Calico eBPF dataplane if needed

Thanks!

mail: zhangjintao@apache.org
Twitter: @zhangjintao9020