JETSTACK by Venafi

From zero to hero

How platform engineers are Zero Trust rainmakers

Stephen Judd | **Chief Architect**

Conf42: Cloud Native 2023

jetstack.io

Steve Judd

Chief Architect
@
Jetstack Consult, a Venafi company

✉️ steve.judd@jetstack.io

What is Zero Trust?

> “An information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices.”
>
> — Forrester

> “An information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices.”

— Forrester

> “An information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices.”

— Forrester

Never trust

Always verify

Every time

Key principles

Principle of least privilege

Per request authentication & authorisation

Identity based

Context based

Principle
of least
privilege

Per request
authentication
&
authorisation

Identity
based

Context
based

Principle of least privilege

Per request authentication & authorisation

Identity based

Context based

Principle
of least
privilege

Per request
authentication
&
authorisation

Identity
based

Context
based

Prevent lateral movement within a network

Photo by Masaaki Komori on Unsplash

The Challenges! The Challenges!

- Machine Identity management at scale
- Policy & Role Based Access Control and enforcement
- Shift-left security: easier said than done
- Governance & oversight

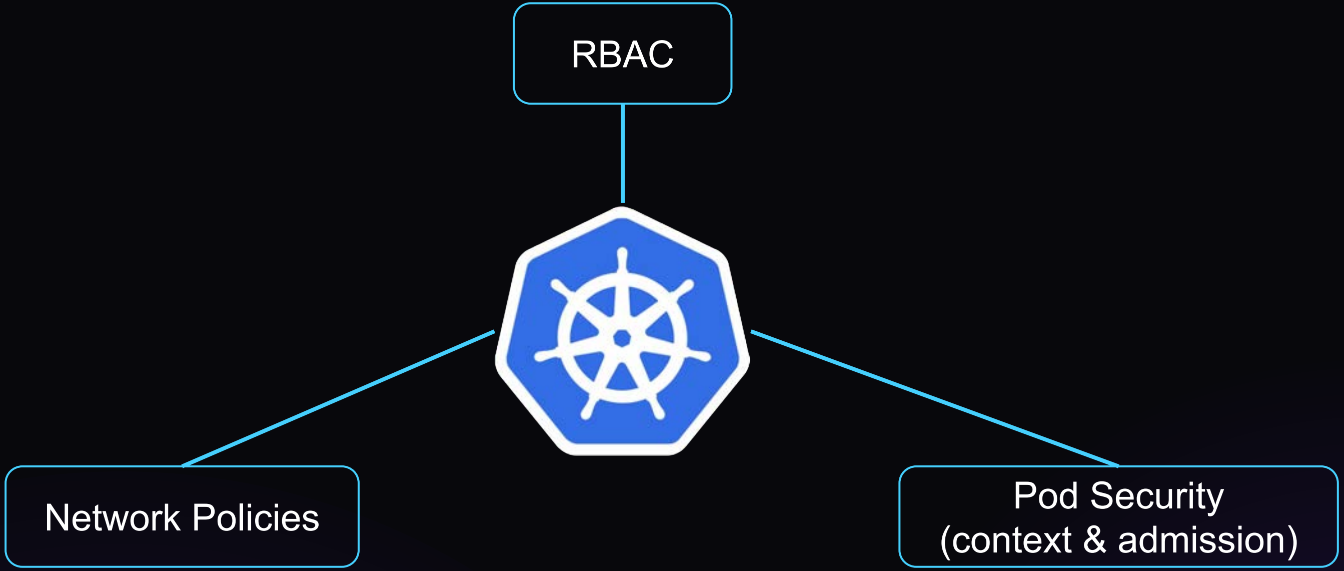
- Machine Identity management at scale
- Policy & Role Based Access Control and enforcement
- Shift-left security: easier said than done
- Governance & oversight

- Machine Identity management at scale
- Policy & Role Based Access Control and enforcement
- Shift-left security: easier said than done
- Governance & oversight

- Machine Identity management at scale
- Policy & Role Based Access Control and enforcement
- Shift-left security: easier said than done
- Governance & oversight

Solving these for a containerised world

Kubernetes native...

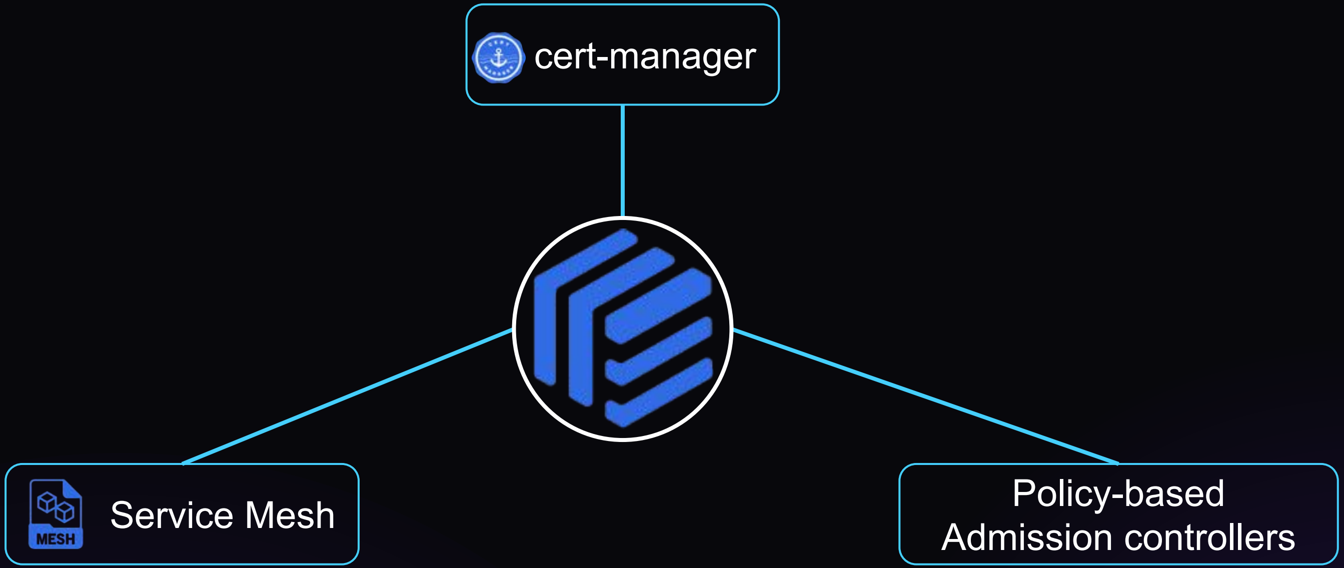


RBAC

Network Policies

Pod Security
(context & admission)

Kubernetes add-ons...



cert-manager

Service Mesh

Policy-based Admission controllers

Where does “Shift-left” fit into this?

Security teams can introduce policies but who’s responsible for implementation?

Platform Engineering

Platform Engineering

- ✓ Kubernetes expertise
- ✓ Automation know-how
- ✓ Familiarity with tooling

Onus is on the Security teams to take the lead, reach out to Platform Engineering and collaborate

JETSTACK by Venafi

Thank you! 🚀