Containers should contain ...right?

Maya Kaczorowski,
Product Manager,
Security & Privacy
@MayaKaczorowski

OpenStack Summit 2018

Google Cloud

What kinds of threats are there to containers?

- privilege escalation
- credential theft
- Unpatched vulnerability
- Zero day in open source library
- DDoS
- container escape

Google Cloud

What kinds of threats are there to containers?

- privilege escalation
- credential theft
- Unpatched vulnerability
- Zero day in open source library
- DDoS
- container escape

Google Cloud

So, what is container security?

Infrastructure security

Is my infrastructure secure for developing containers?

Software supply chain

Is my container image secure to build & deploy?

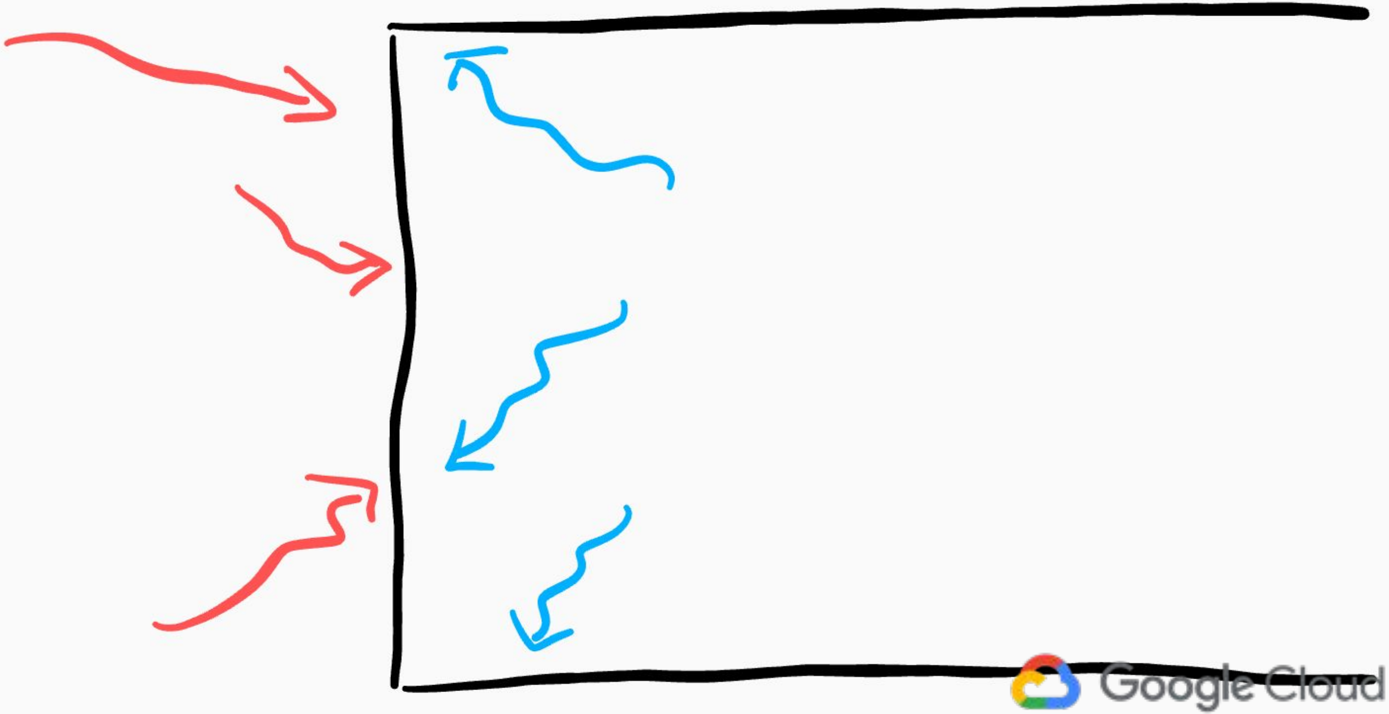
Runtime security

Is my container secure to run?

Threats

From the outside

From the inside



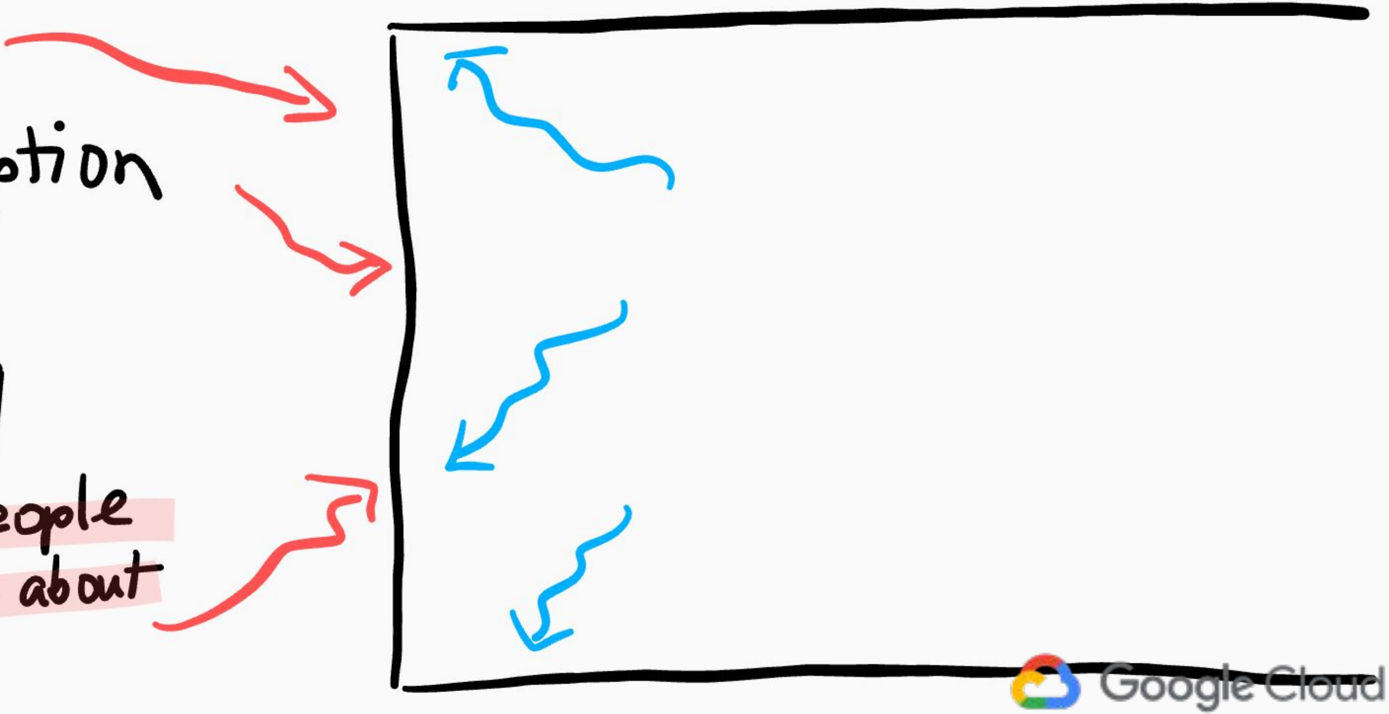
Threats

From the outside

- DDoS, disruption
- Data theft
- Cryptomining

...what most people typically think about

From the inside



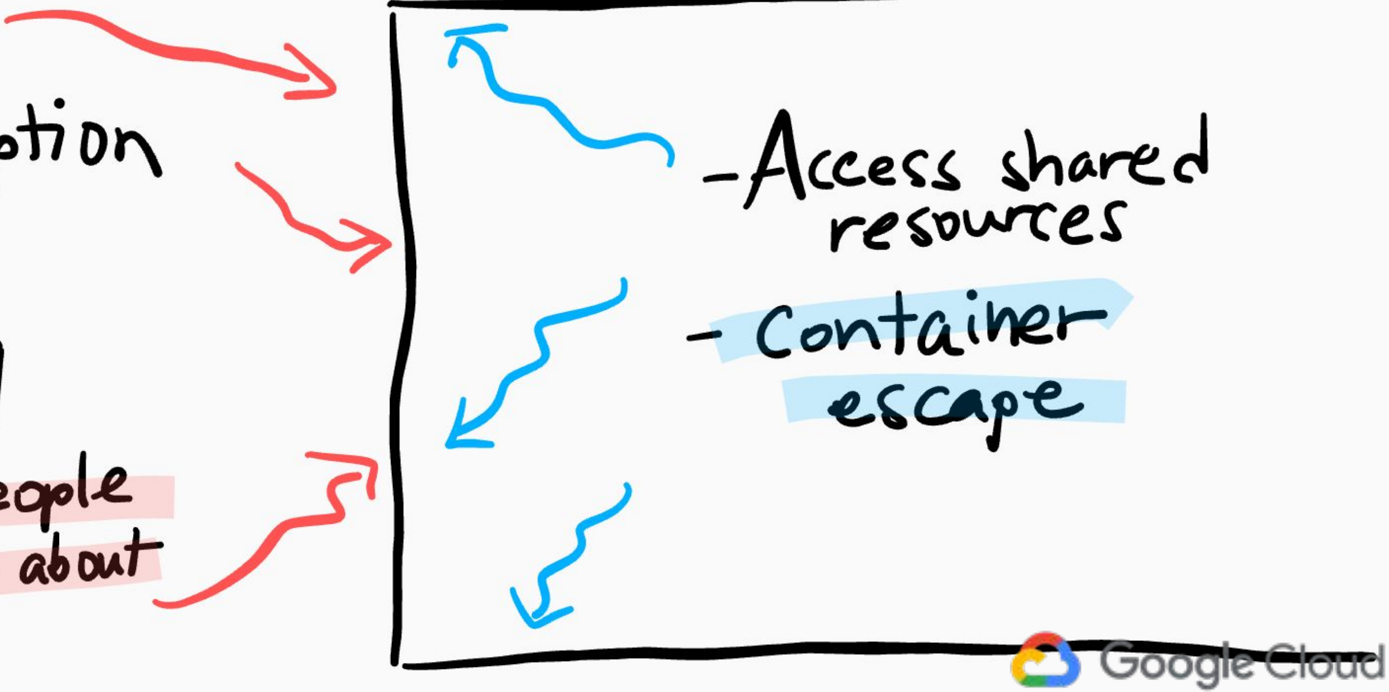
Threats

From the outside

- DDoS, disruption
- Data theft
- Cryptomining

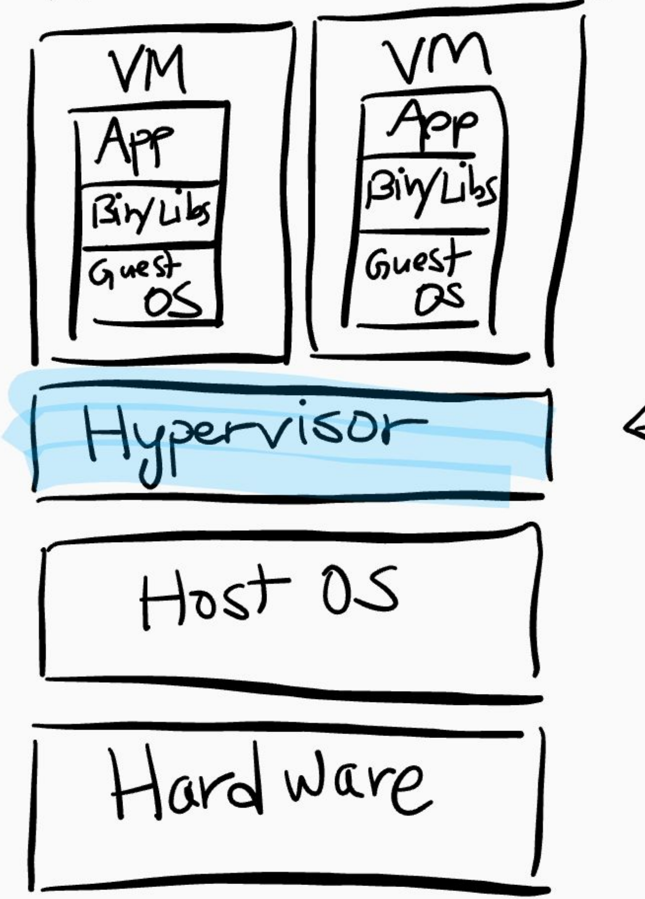
... what most people typically think about

From the inside



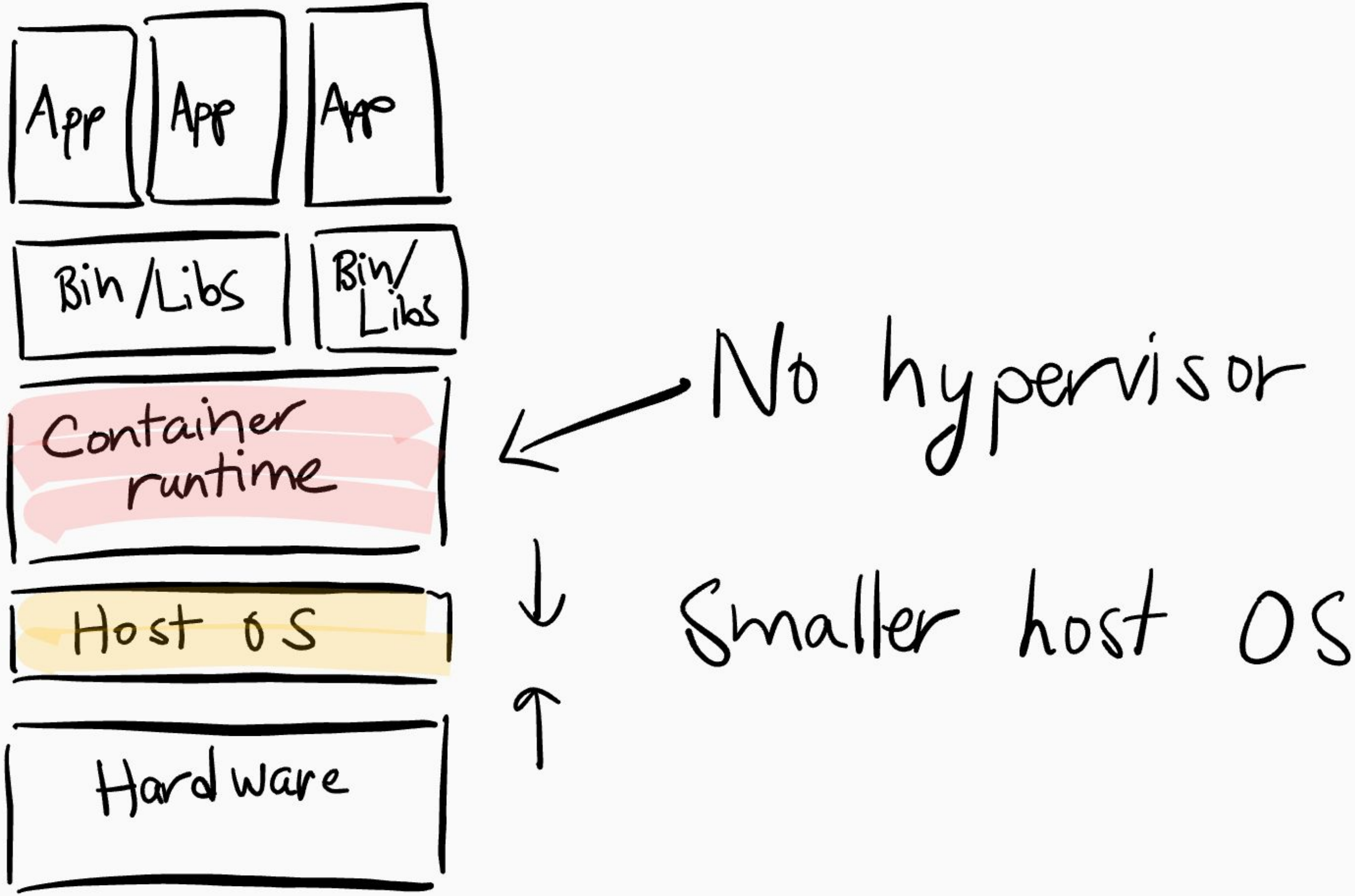
- Access shared resources
- Container escape

Virtual machine



The hypervisor isolates the virtual machines

Container


App
App
App
Bin/Libs
Bin/Libs
Container runtime
No hypervisor
Host OS
Smaller host OS
Hardware

	Virtual machine	Container
Surface of attack	Hypervisor + VMM	minimal host OS
Isolation	Software (hypervisor) + hardware (VMX/SVM)	????

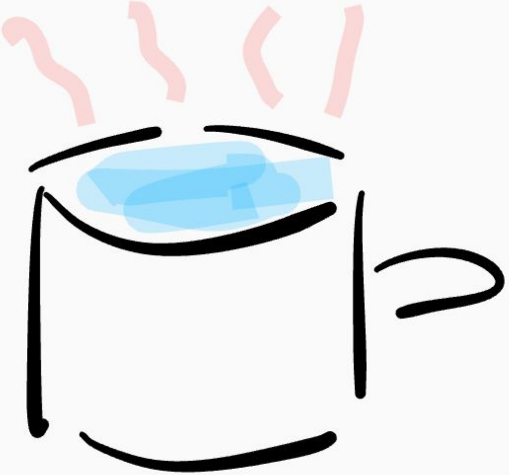
PSA:

Containers don't contain!

Google Cloud

Containers contain ...

like a cup of water



NOT a thermos

Why do I need isolation?

- *untrusted code
  - third party
  - open source
  - known bad
- *surface of attack
  - runtime daemons
- *multi-tenancy
  - public cloud
  - aaS

Trust boundary

Point at which code changes levels of trust

Security boundary

Set of controls to prevent a process from elevating its trust level

Google Cloud

Trust boundary

Point at which code changes levels of trust

Security boundary

Set of controls to prevent a process from elevating its trust level

A security boundary is how you enforce a trust boundary

Trust boundary

A process on:

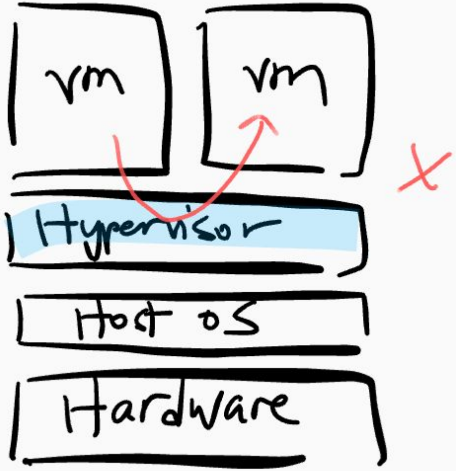
public data vs. user data

LOW TRUST

HIGH TRUST

Security boundary

Hypervisor:



Layers of isolation in Kubernetes

Network

Data

metadata

Control plane

Service account

Resource

Kernel security

Layers of isolation in Kubernetes

Network

Data

metadata

Control plane

Service account

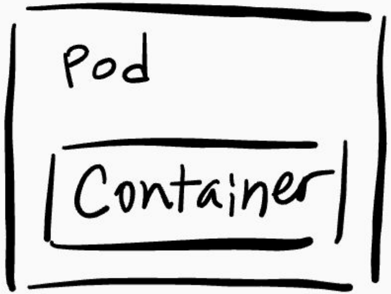
Resource ☆

Kernel security ☆ ☆ ☆

Container

Layers of isolation in Kubernetes

- Network ☆
- Data
- metadata
- Control plane
- Service account
- Resource ☆☆
- Kernel security ☆☆☆



Pod

Container

Layers of isolation in Kubernetes

Network ☆

Data

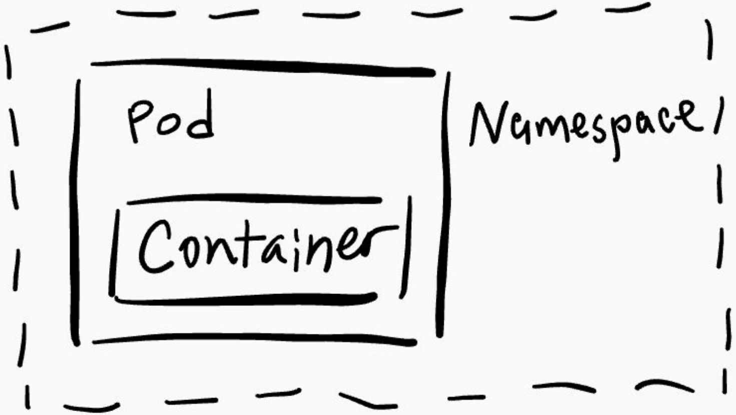
metadata

Control plane ★★

Service account ★★★

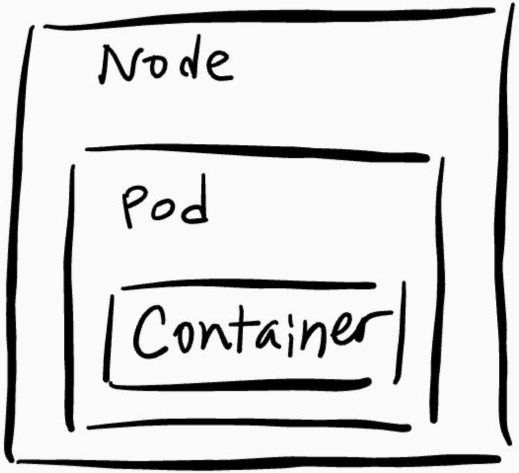
Resource ☆☆

Kernel security ☆☆☆



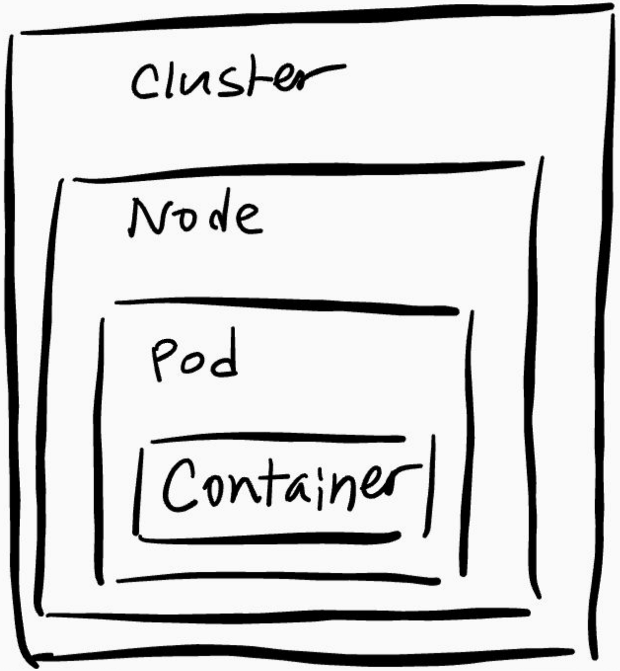
Google Cloud

Layers of isolation in Kubernetes



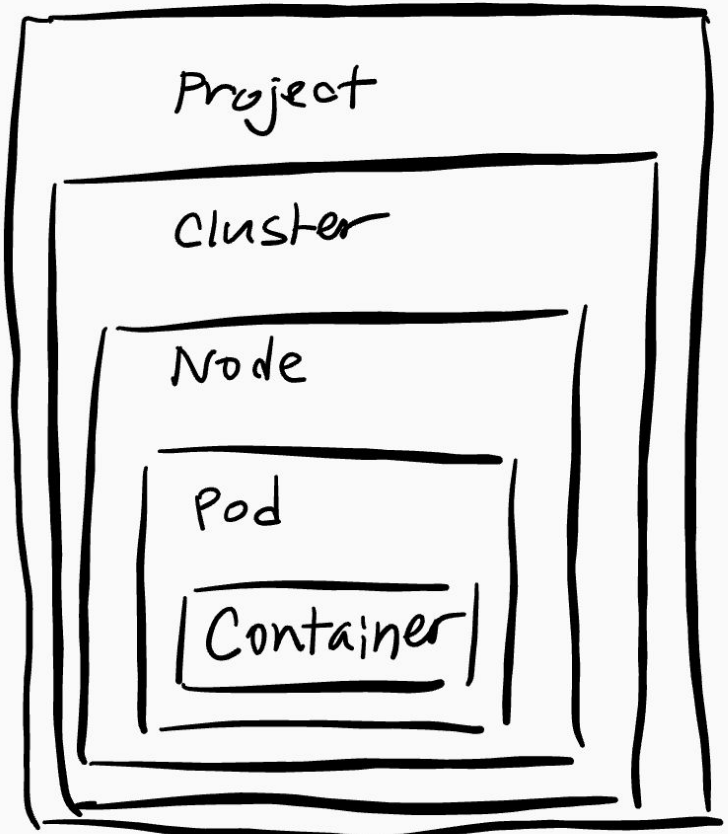
- Network ☆
- Data ☆
- metadata
- Control plane ☆☆
- Service account ☆☆☆
- Resource ☆☆☆
- Kernel security ☆☆☆

Layers of isolation in Kubernetes



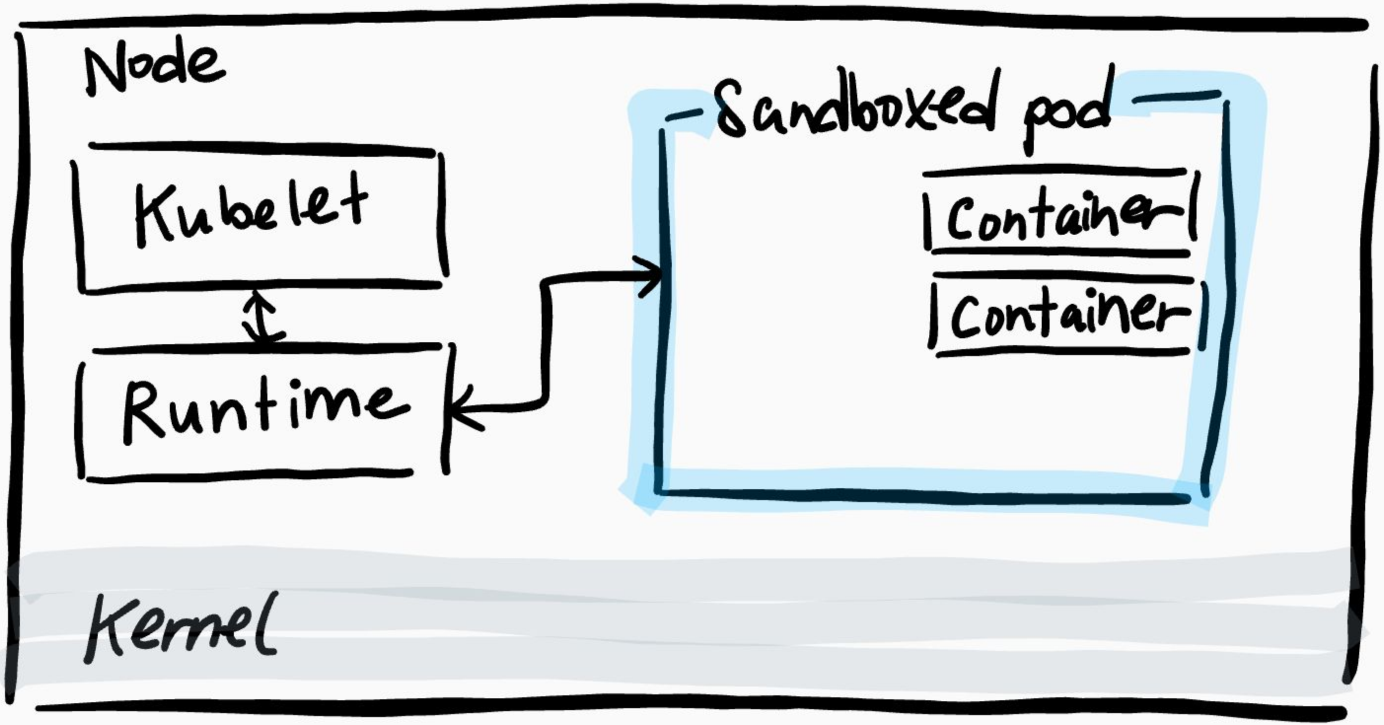
Network	☆ ★
Data	☆ ★
metadata	★ ★
Control plane	☆ ☆ ★
Service account	☆ ☆ ☆
Resource	☆ ☆ ☆
Kernel security	☆ ☆ ☆

Layers of isolation in Kubernetes



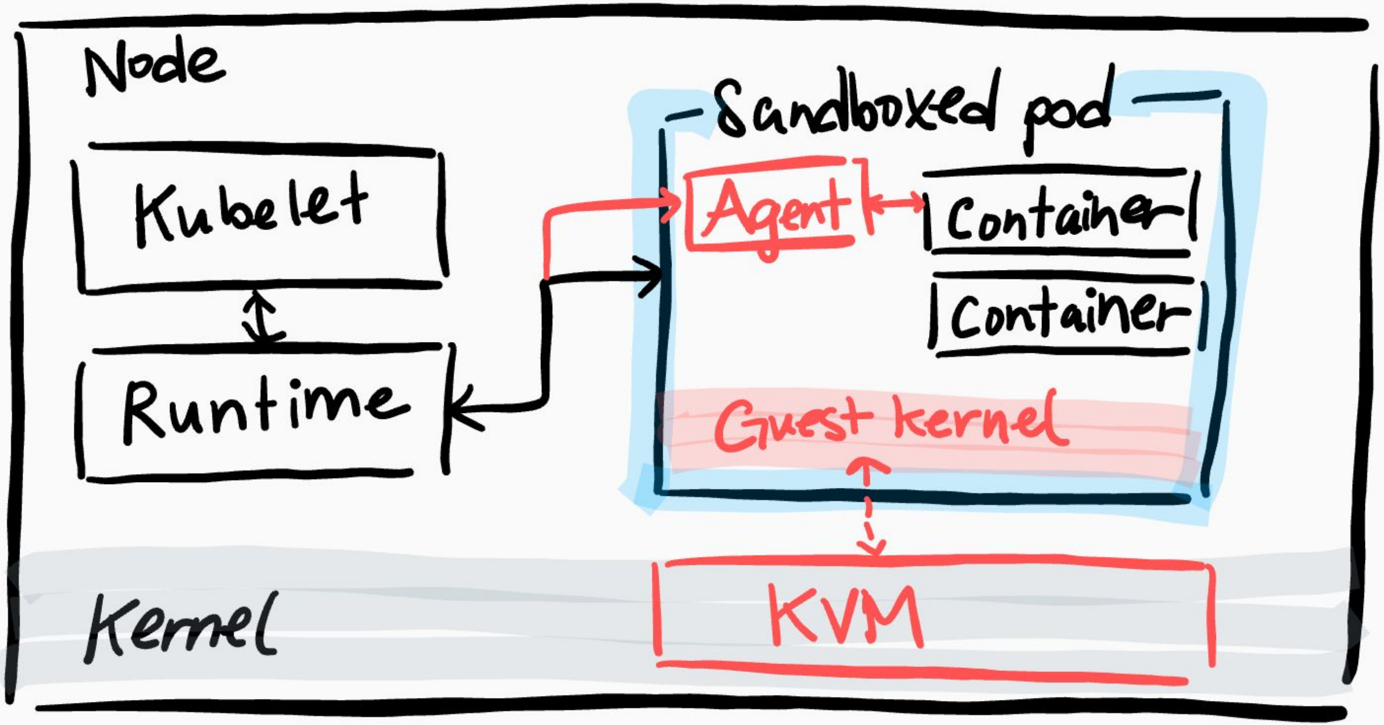
Network	☆ ☆ ★
Data	☆ ☆ ★
metadata	☆ ☆ ★
Control plane	☆ ☆ ☆
Service account	☆ ☆ ☆
Resource	☆ ☆ ☆
Kernel security	☆ ☆ ☆

What's a sandbox?



What's a sandbox?

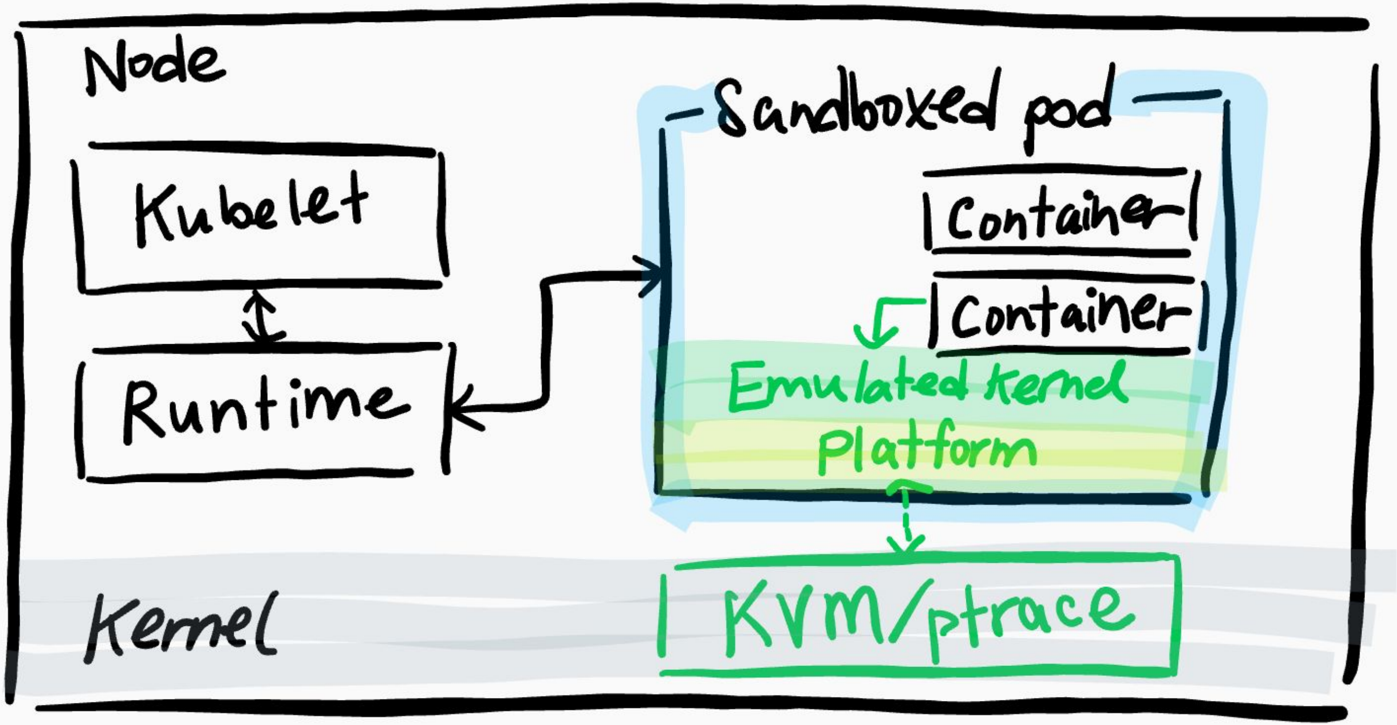
Kata container



Google Cloud

What's a sandbox?

gvisor



Google Cloud

Residual risks with sandboxes

Sandboxes don't solve all your problems!

Residual risks with sandboxes

Sandboxes don't solve all your problems!

Attacks are still possible via...

Residual risks with sandboxes

Sandboxes don't solve all your problems!

Attacks are still possible via...

- storage
- network
- daemons
- hardware

etc.

Kubernetes
is a complex system
with many attack surfaces
exposed to internal threats

Kubernetes
is a complex system
with many attack surfaces
exposed to internal threats

- Pick the right layer of isolation
- Use sandboxes to mitigate risks