Kata Containers

云原生服务的一块坚定基石

彭涛，蚂蚁金服

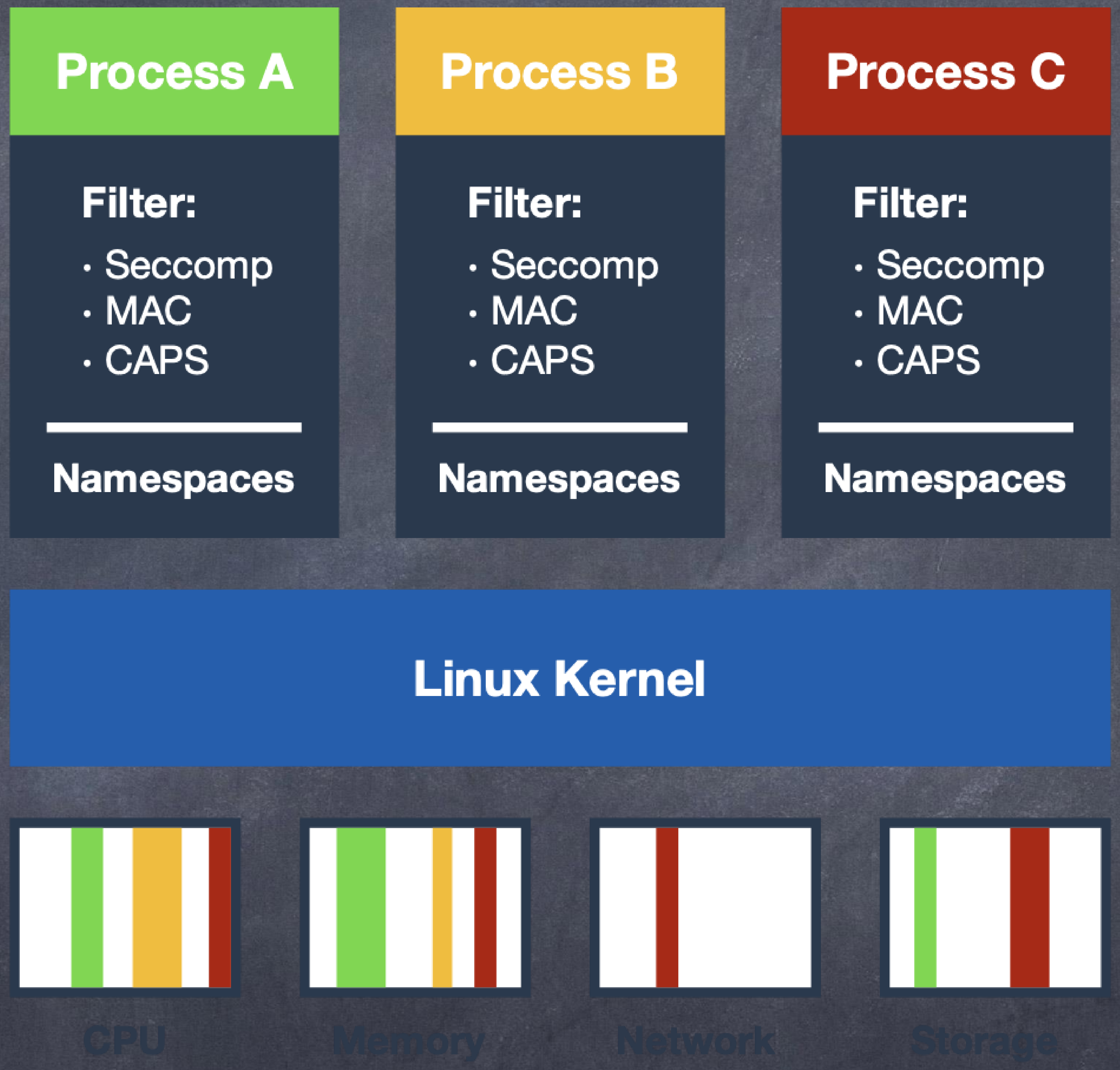
What is Kata Containers

- Kata Containers is an open source community working to
  - build a secure container runtime
  - with lightweight virtual machines
  - that feel and perform like containers
  - but provide stronger workload isolation
  - using hardware virtualization technology as a second layer of defense

katacontainers

Traditional

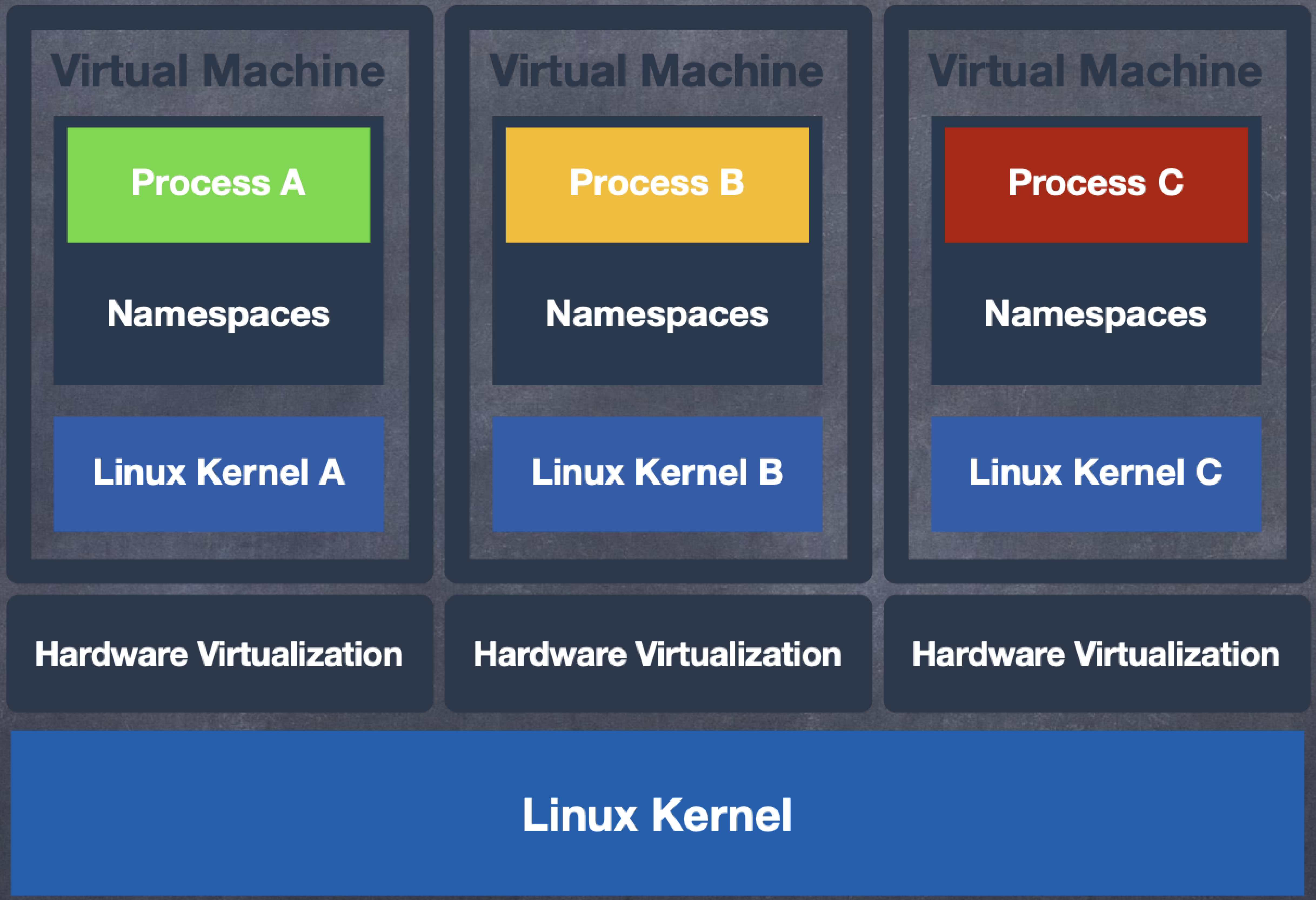
Containers: Isolation by namespaces, cgroups with shared kernel



katacontainers

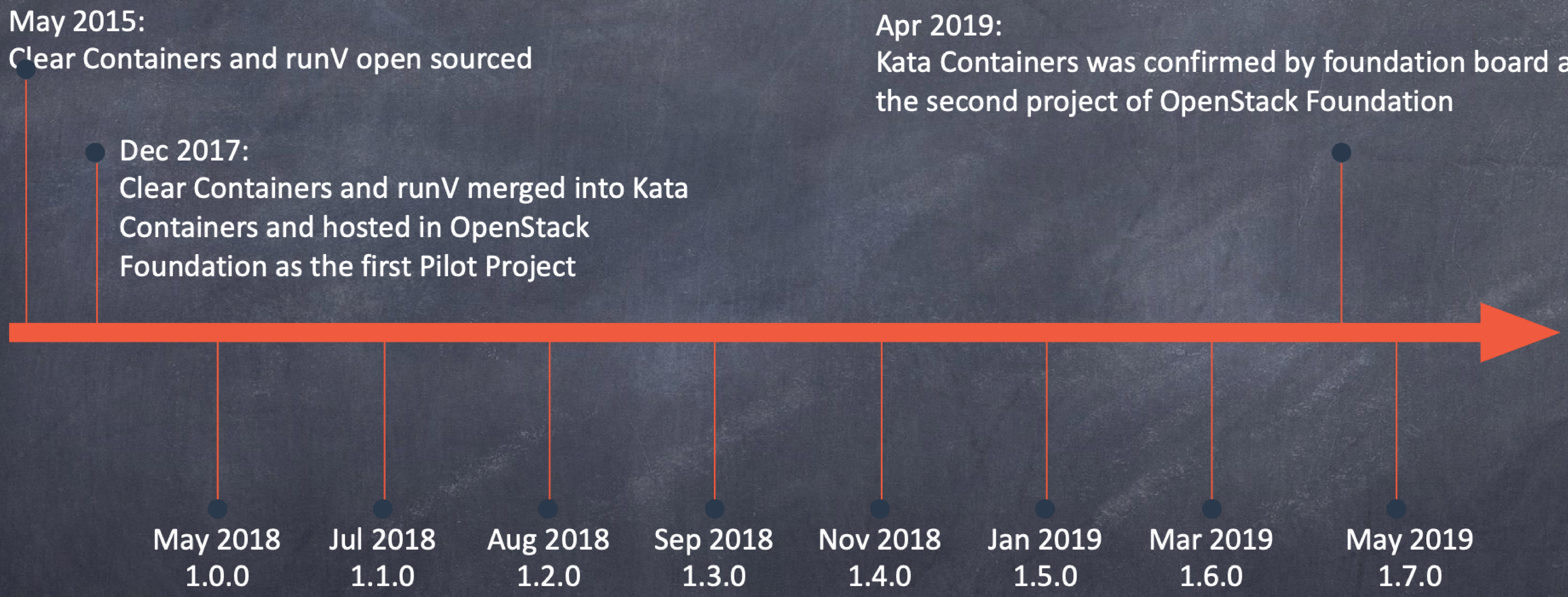
Kata Containers:

Additional isolation with a lightweight VM and individual kernels



katacontainers

Brief History



May 2015:
Clear Containers and runV open sourced

Dec 2017:
Clear Containers and runV merged into Kata Containers and hosted in OpenStack Foundation as the first Pilot Project

Apr 2019:
Kata Containers was confirmed by foundation board as the second project of OpenStack Foundation

May 2018
1.0.0

Jul 2018
1.1.0

Aug 2018
1.2.0

Sep 2018
1.3.0

Nov 2018
1.4.0

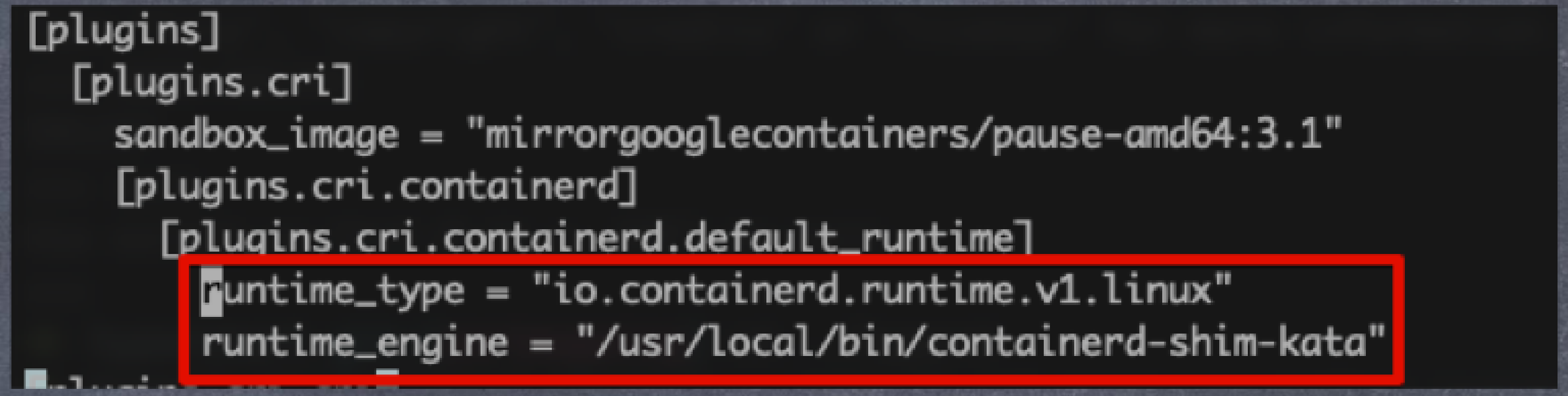
Jan 2019
1.5.0

Mar 2019
1.6.0

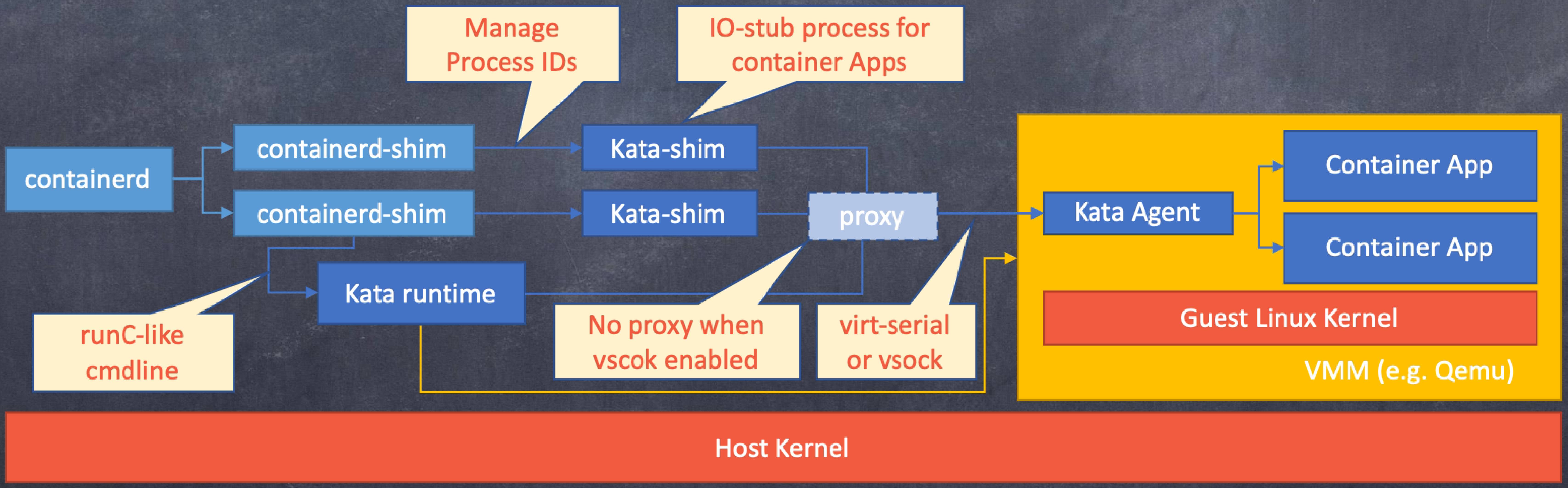
May 2019
1.7.0

Kata Containers (pre-1.5)

- It works
- But looks not so elegent…



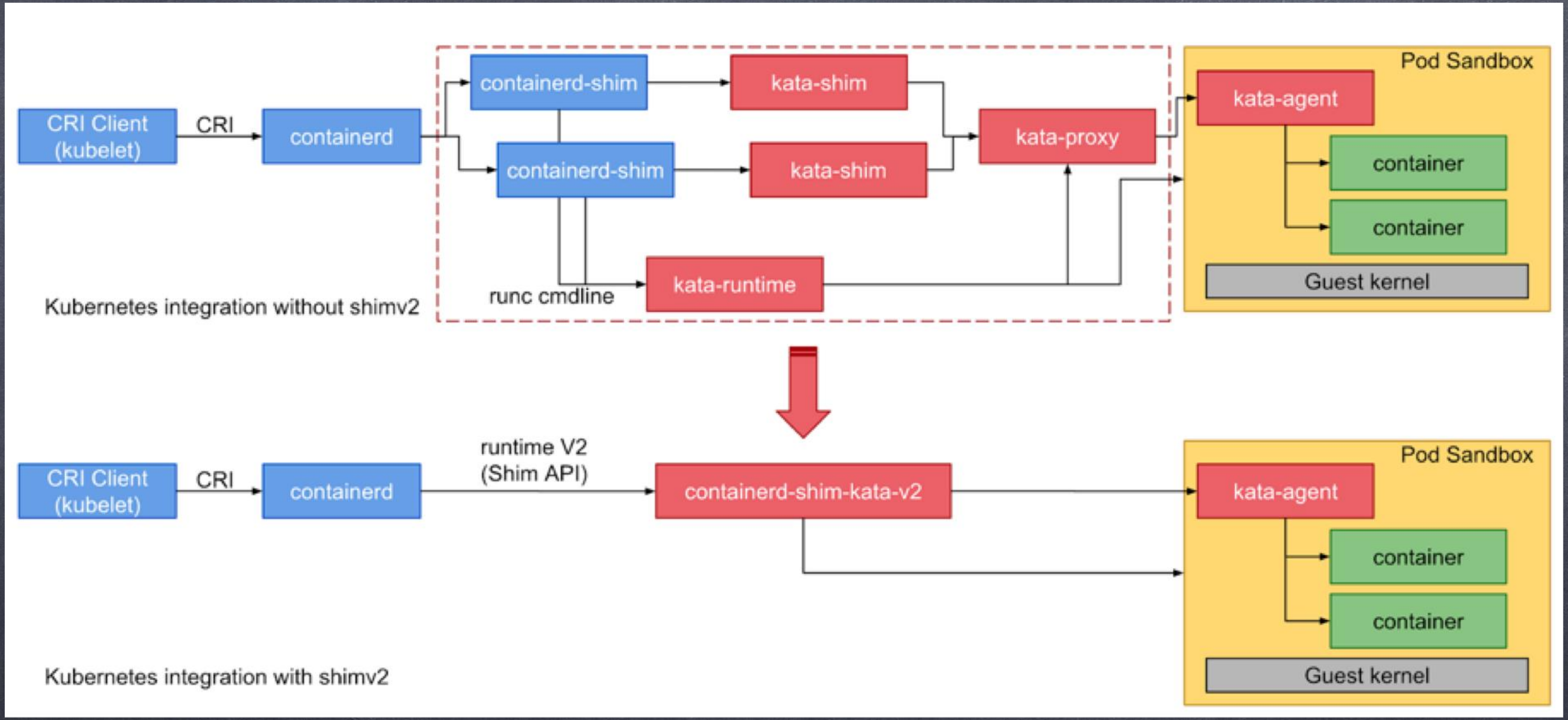
```
[plugins]
  [plugins.cri]
    sandbox_image = "mirrorgooglecontainers/pause-amd64:3.1"
    [plugins.cri.containerd]
      [plugins.cri.containerd.default_runtime]
        runtime_type = "io.containerd.runtime.v1.linux"
        runtime_engine = "/usr/local/bin/containerd-shim-kata"
```



“All problems in computer science can be solved by another level of indirection, except of course for the problem of too many indirections ”

－David Wheeler

Kata Containers w/ shim-v2



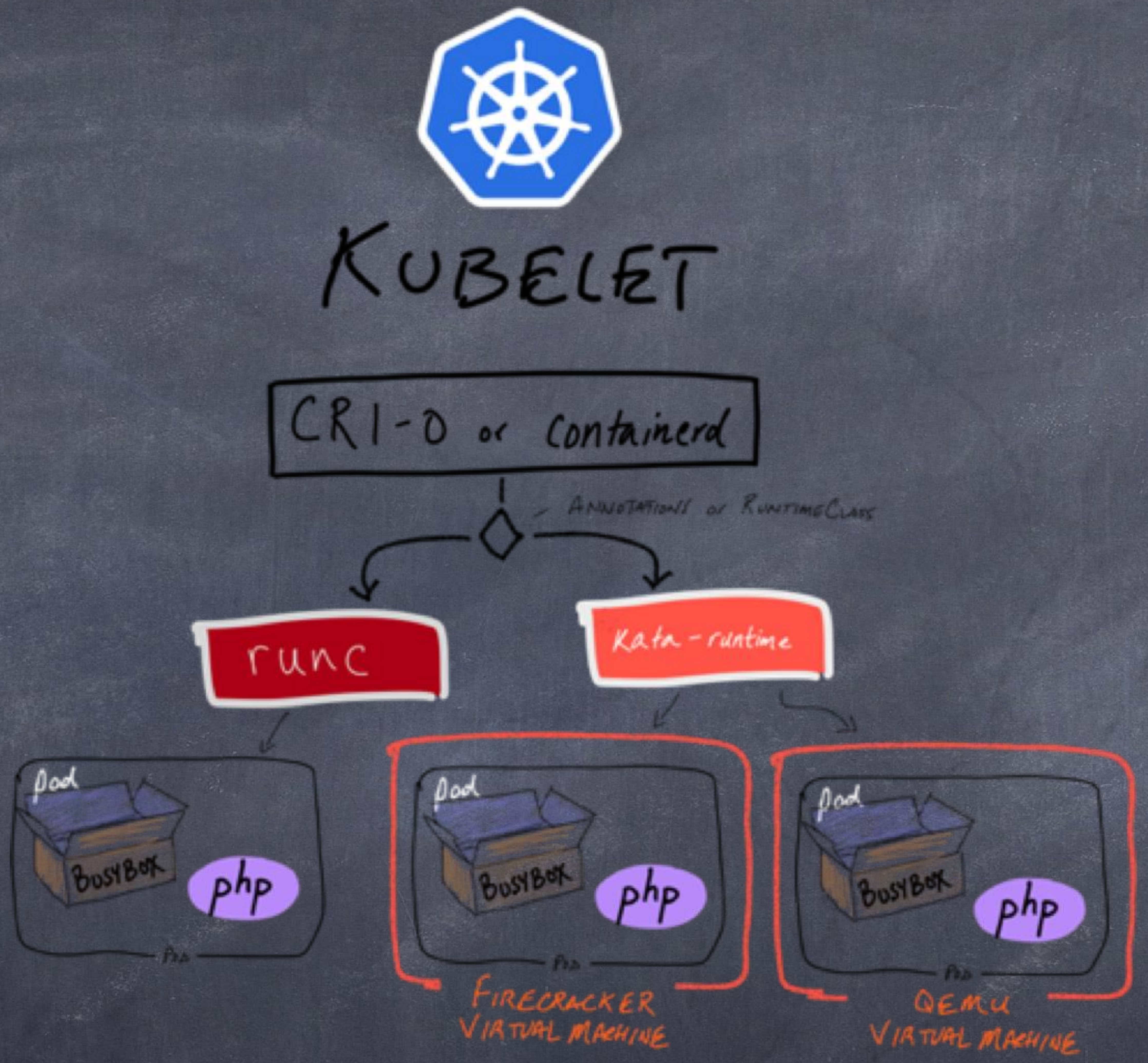
katacontainers

Firecracker

- Virtual Machine Monitor
- Open source by AWS - Nov 2018
    - vmm with minimal design, thus less memory footprint and attack surface
- Supported by Kata Containers since 1.5 release

Kubernetes RuntimeClass

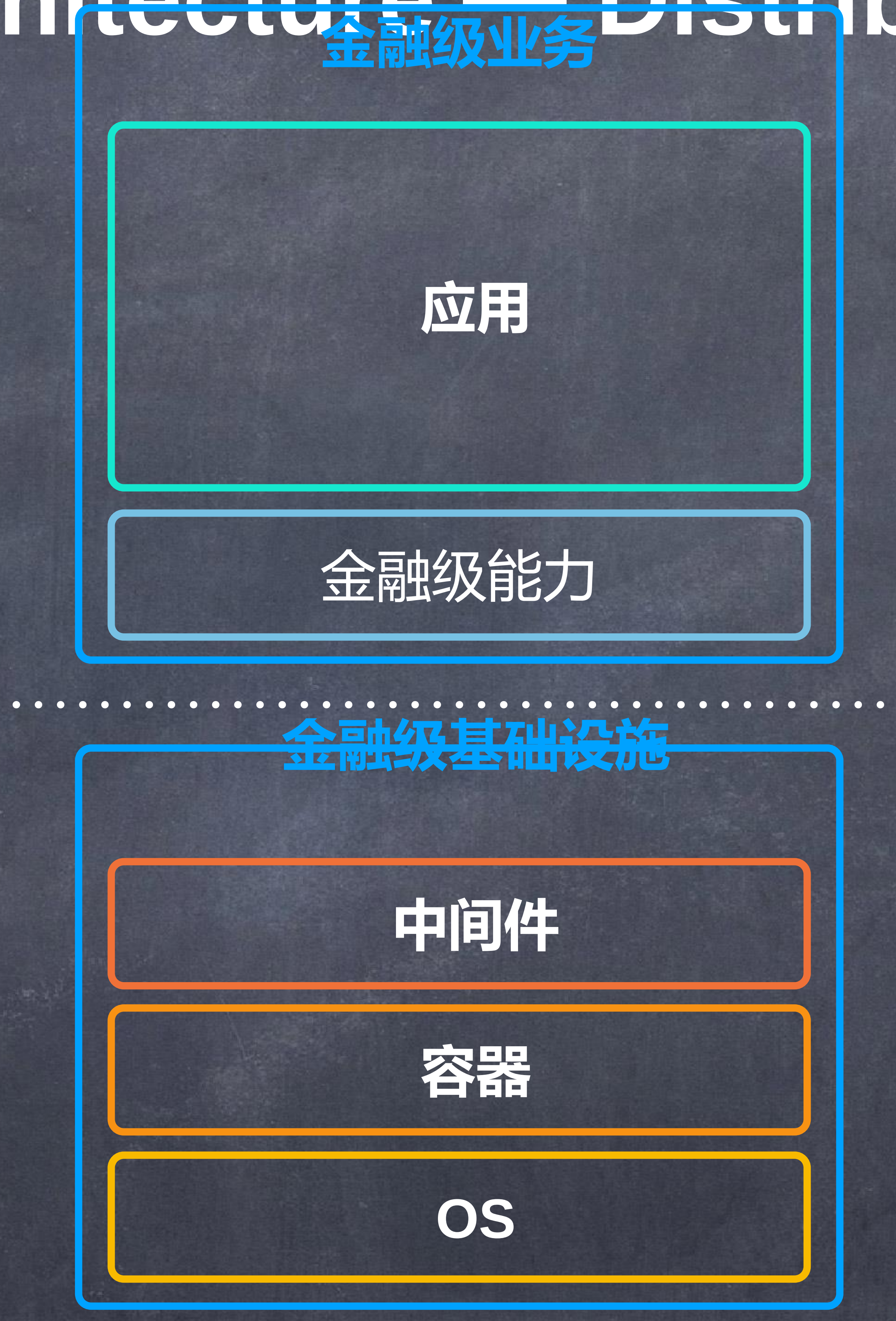
- Available since kubernetes v1.12 (beta feature since v1.14)
- Kubernetes native way to define multiple container runtimes
- Supported by CRI-O and containerd



katacontainers

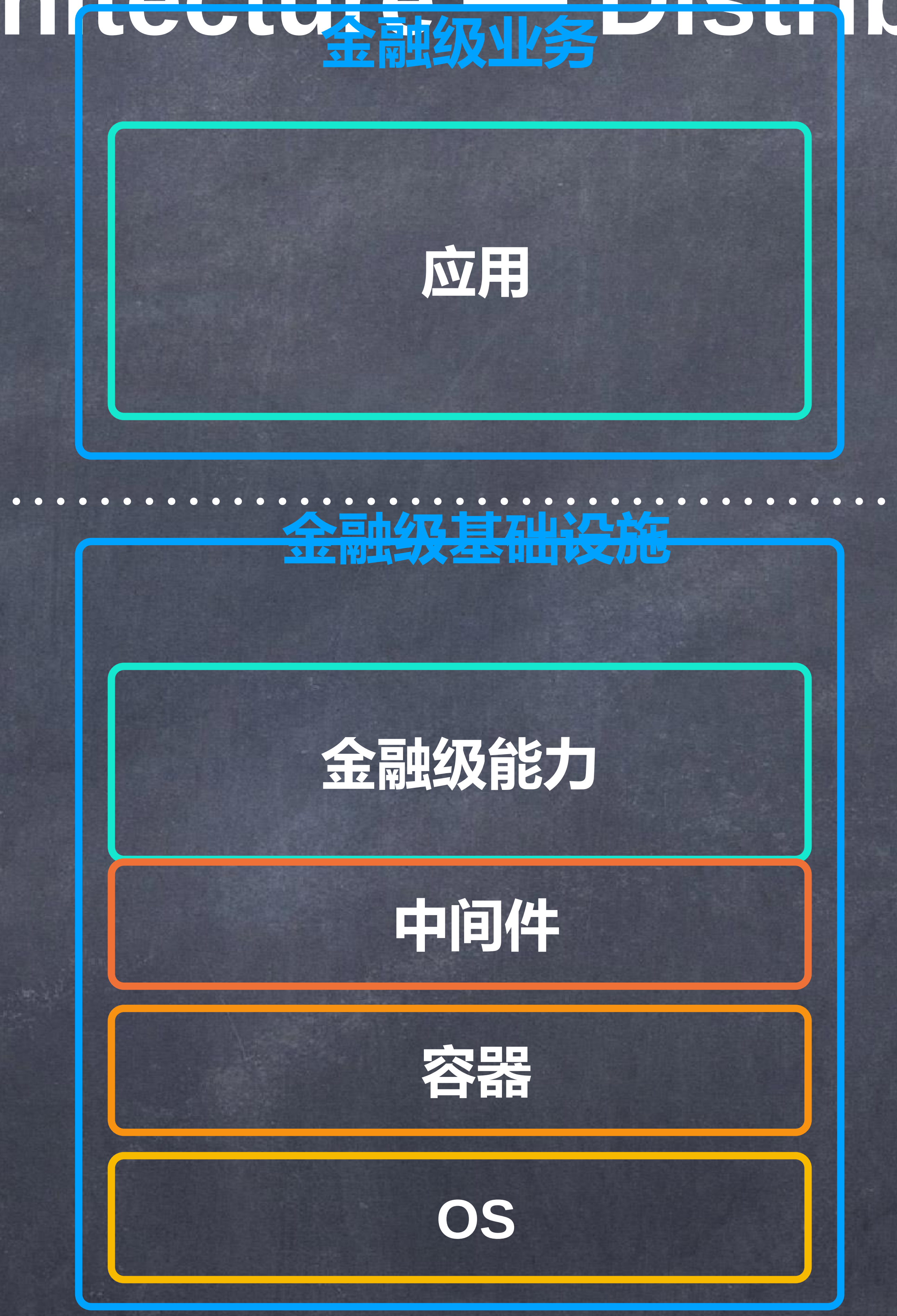
ANT FINANCIAL ♥ katacontainers

Financial Service Architecture — Distributed



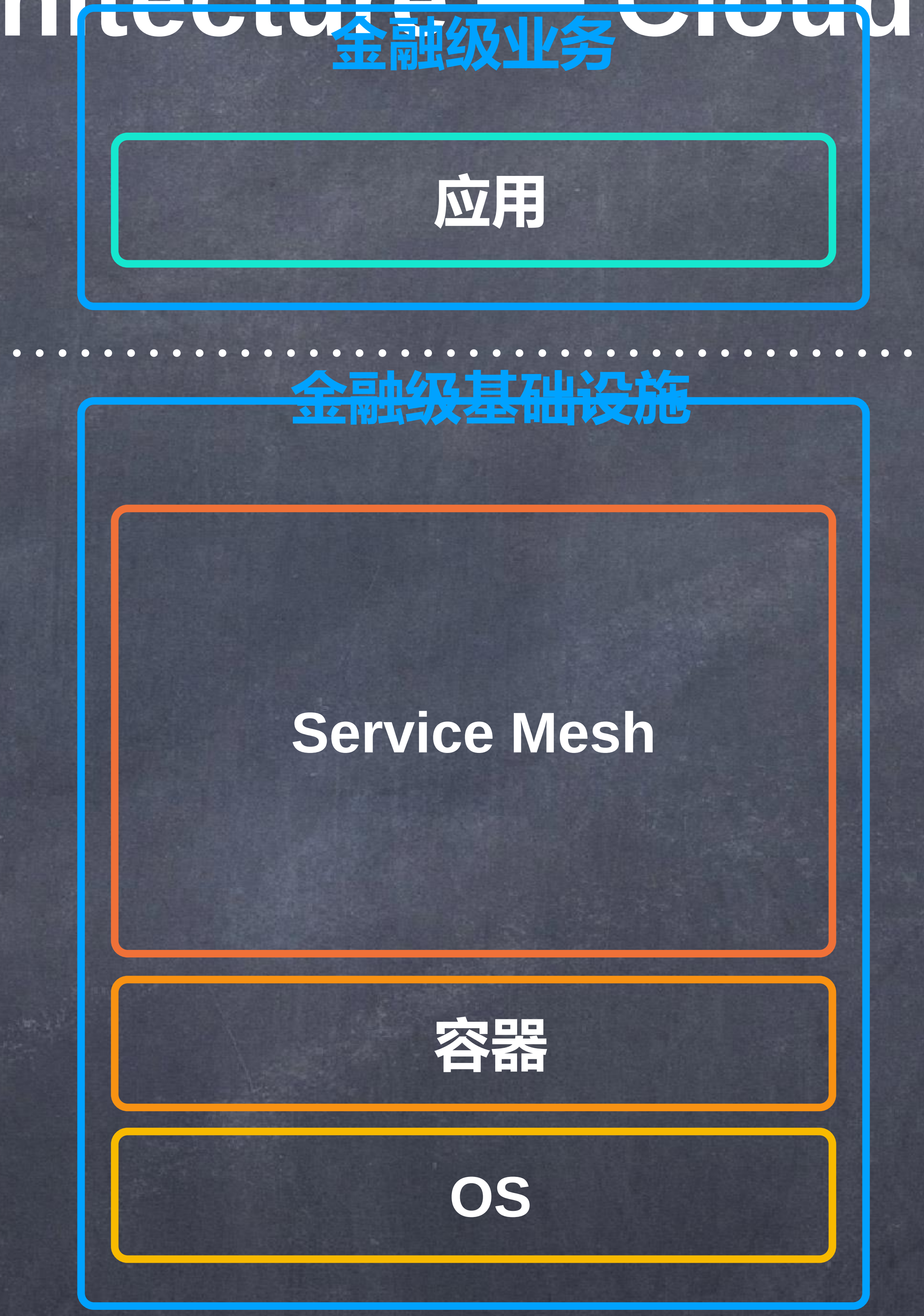
金融级分布式架构

Financial Service Architecture — Distributed



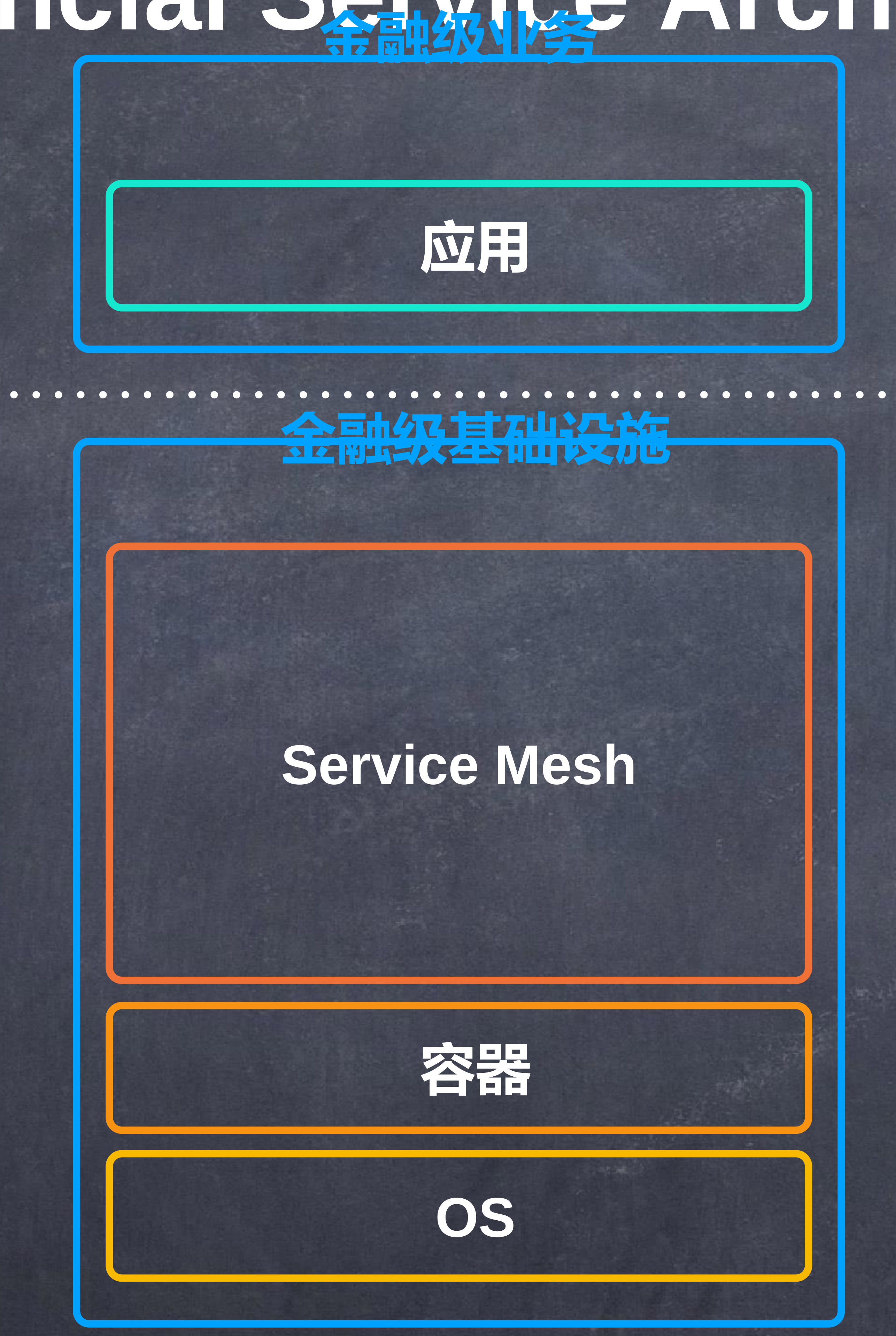
金融级分布式架构

Financial Service Architecture — Cloud Native



金融级云原生

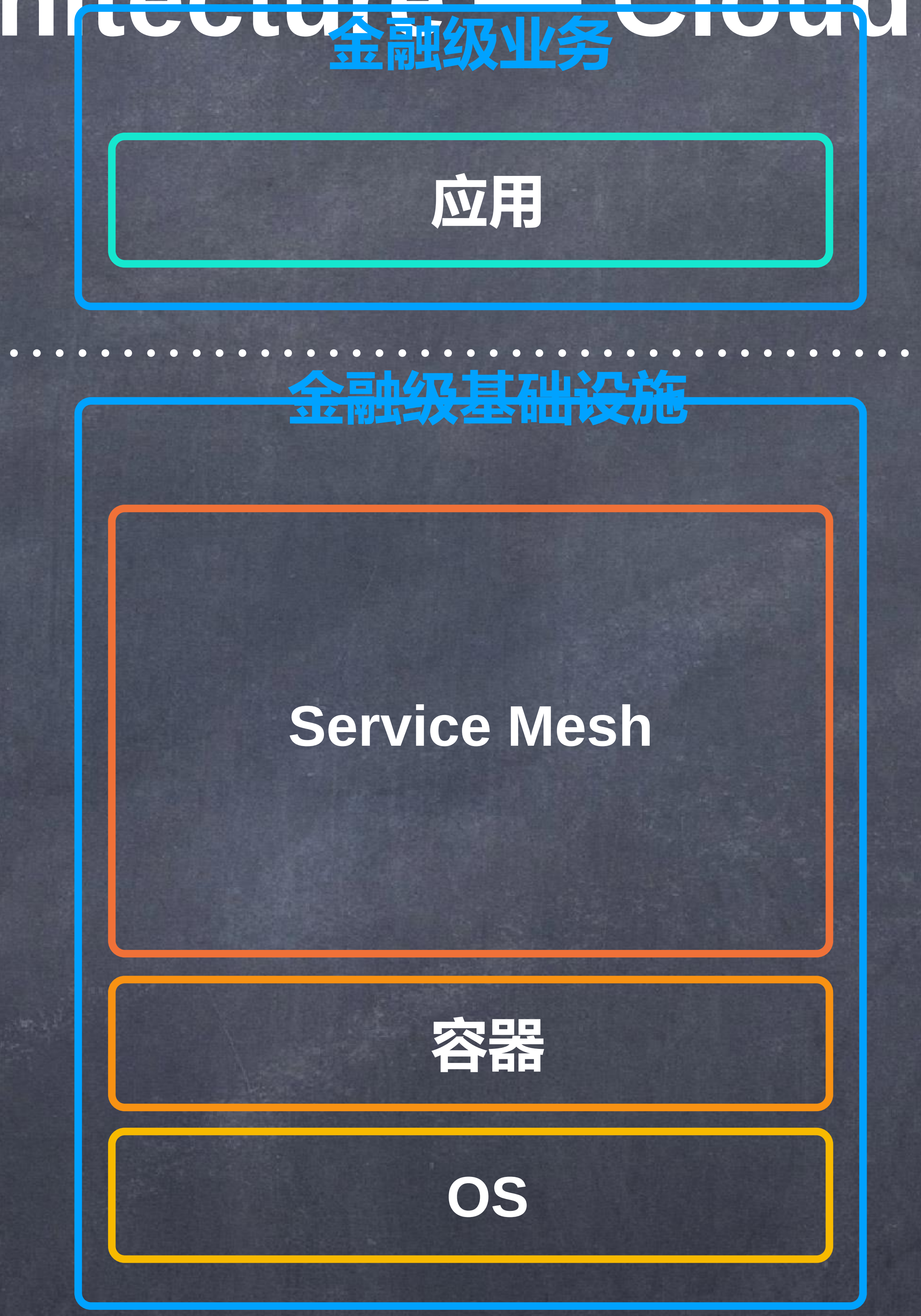
Financial Service Architecture — Cloud Native



金融级云原生

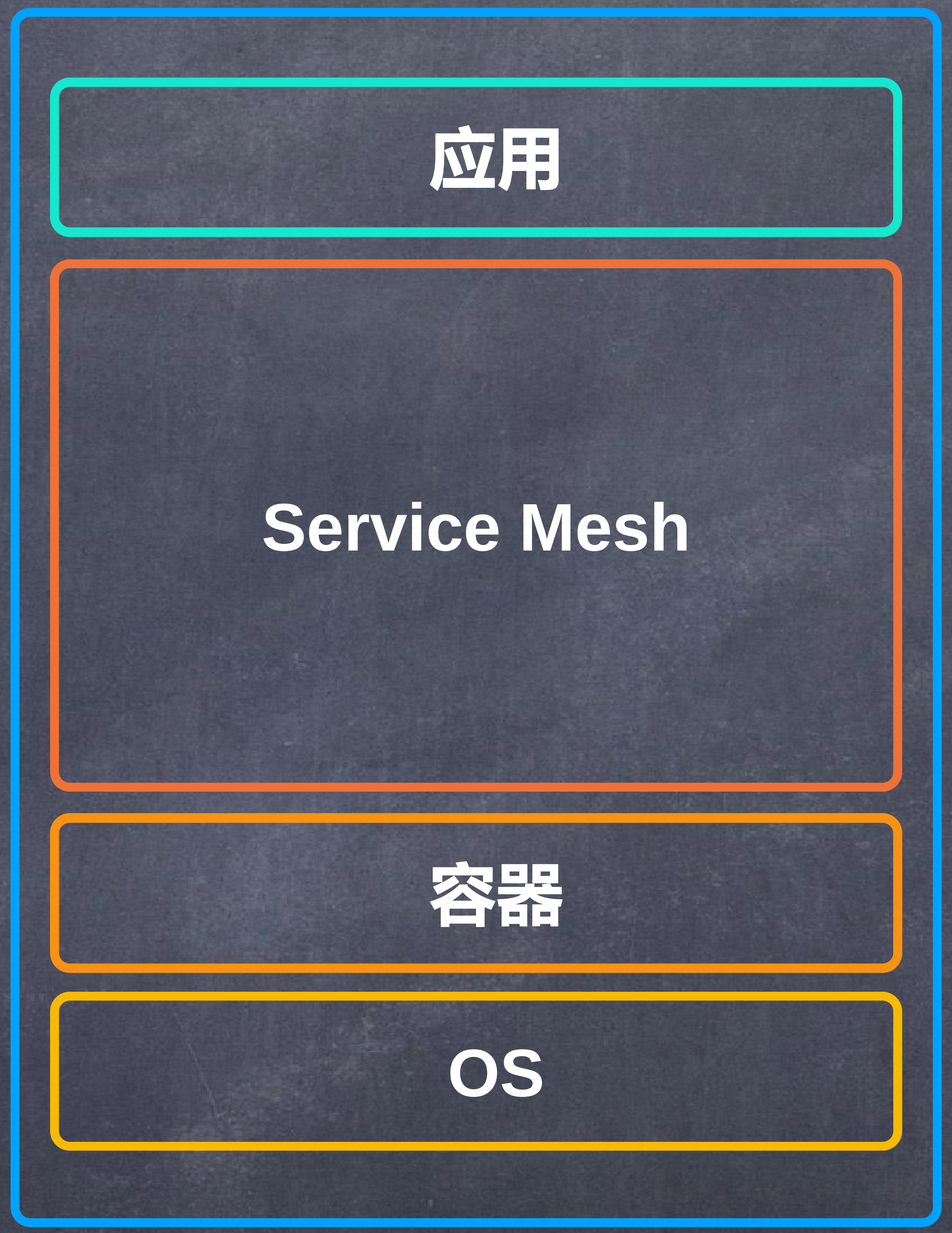
金融级分布式系统，最终将走向云原生化

Financial Service Architecture — Cloud Native



金融级云原生

Financial Service Architecture — Cloud Native



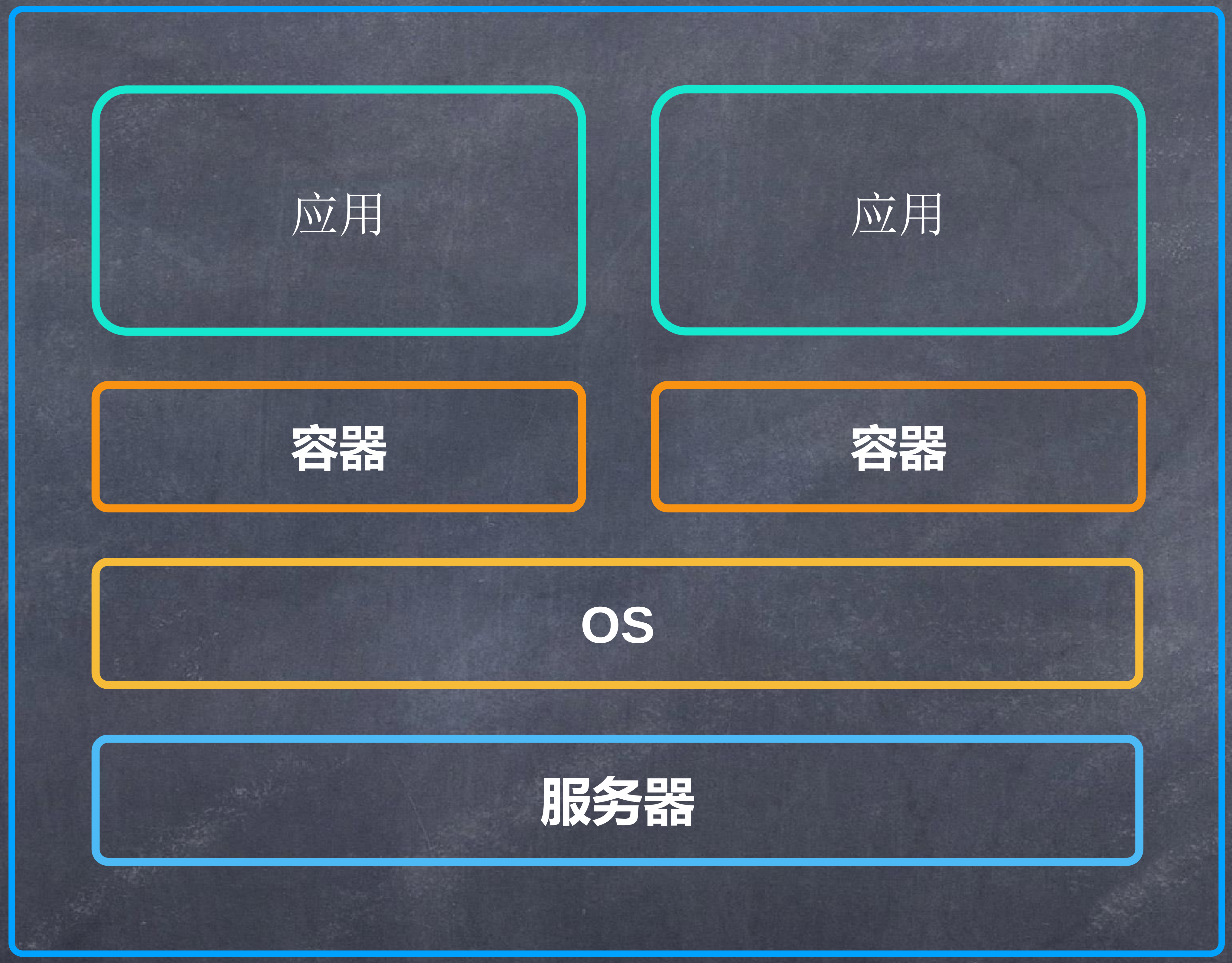
应用

Service Mesh

容器

OS

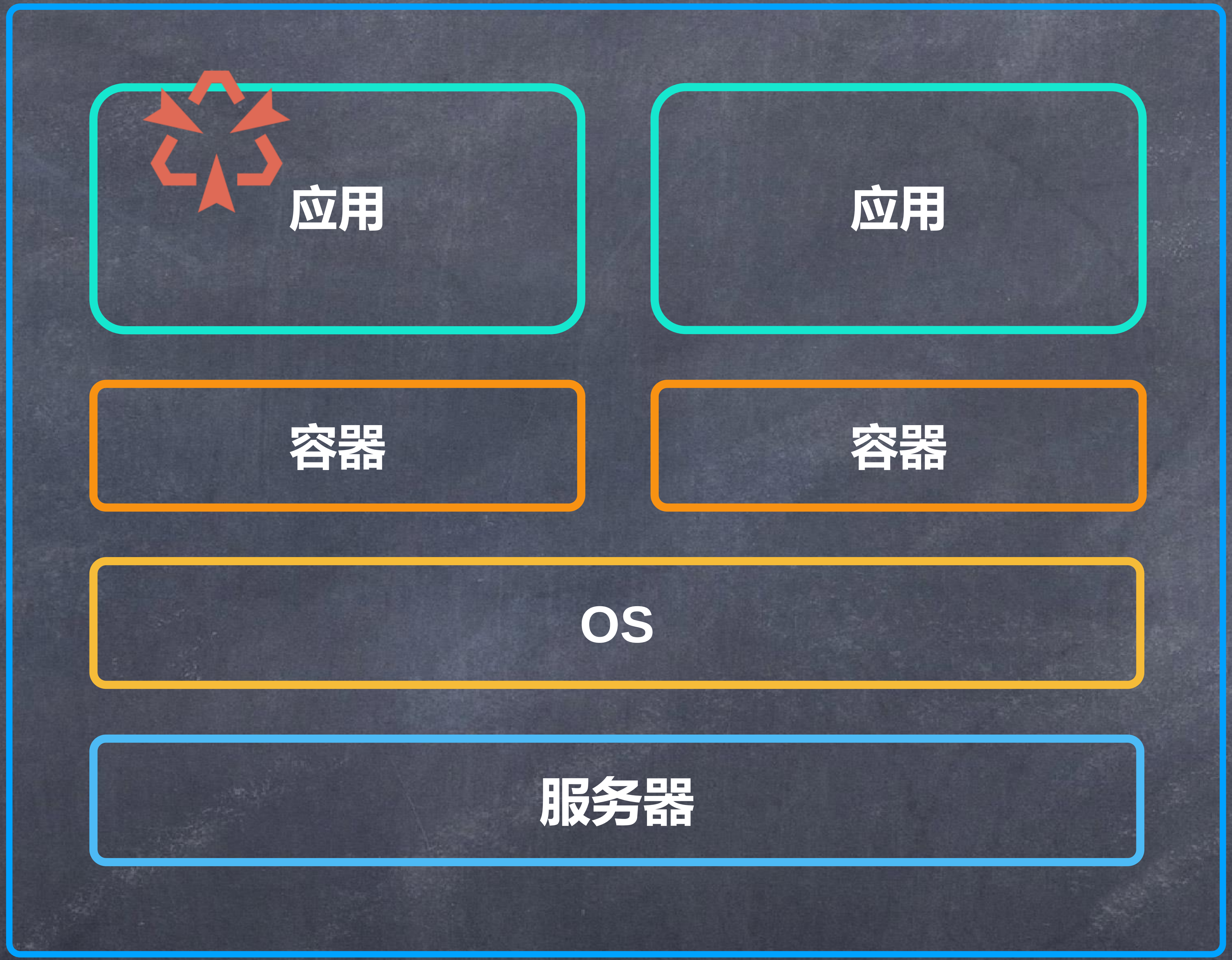
Financial Level Security with Kata



Old

katacontainers

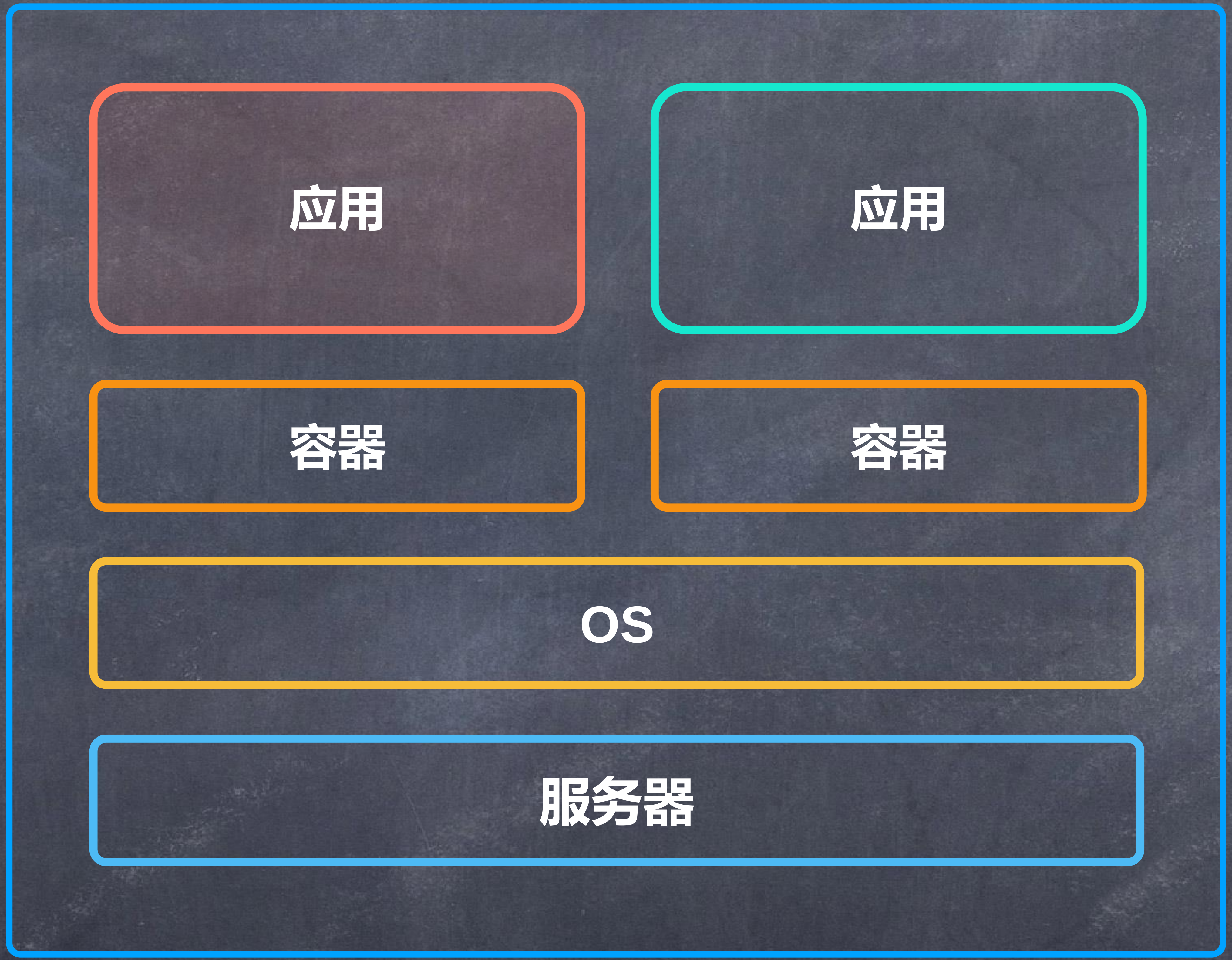
Financial Level Security with Kata



Old

katacontainers

Financial Level Security with Kata



应用

应用

容器

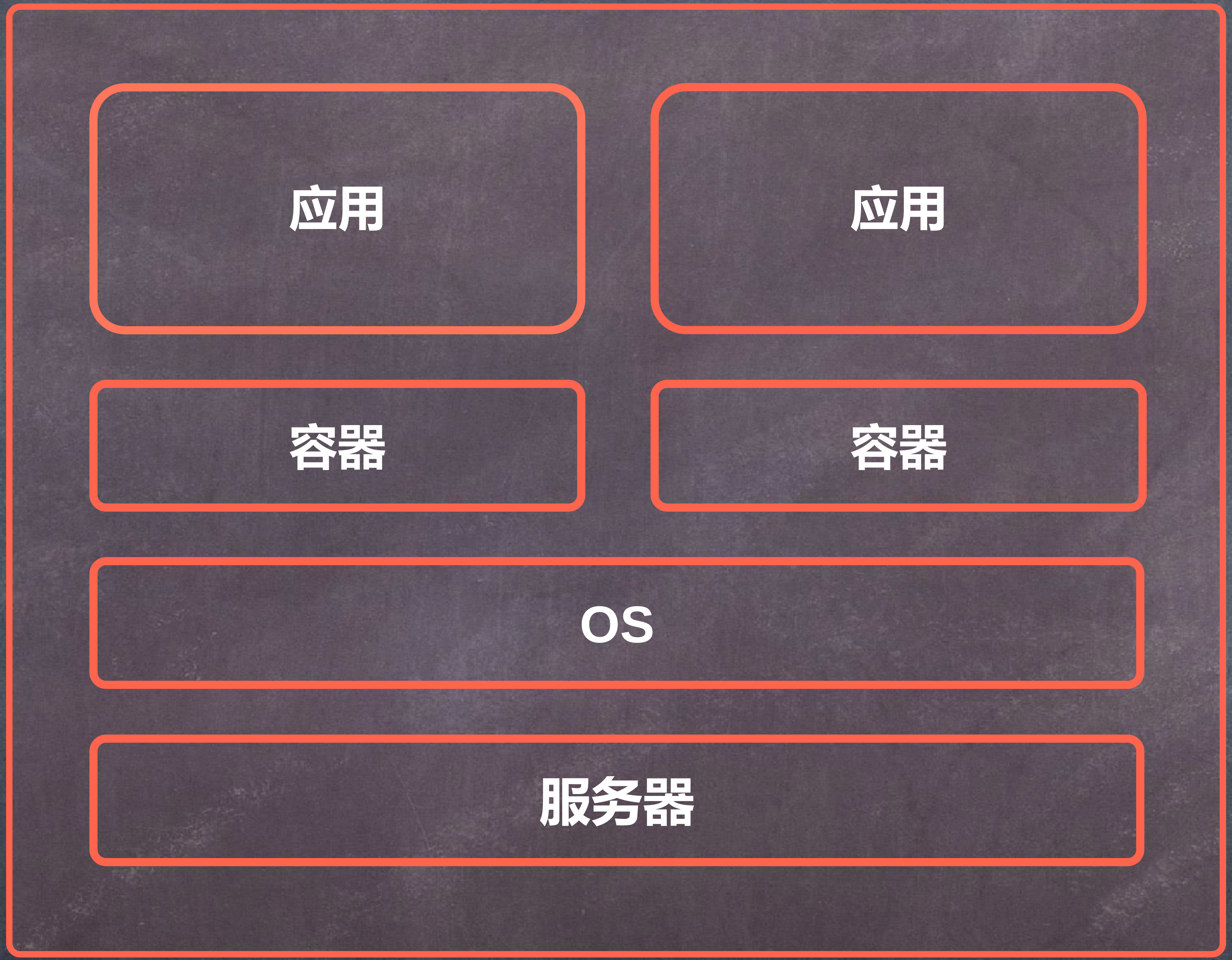
容器

OS

服务器

Old

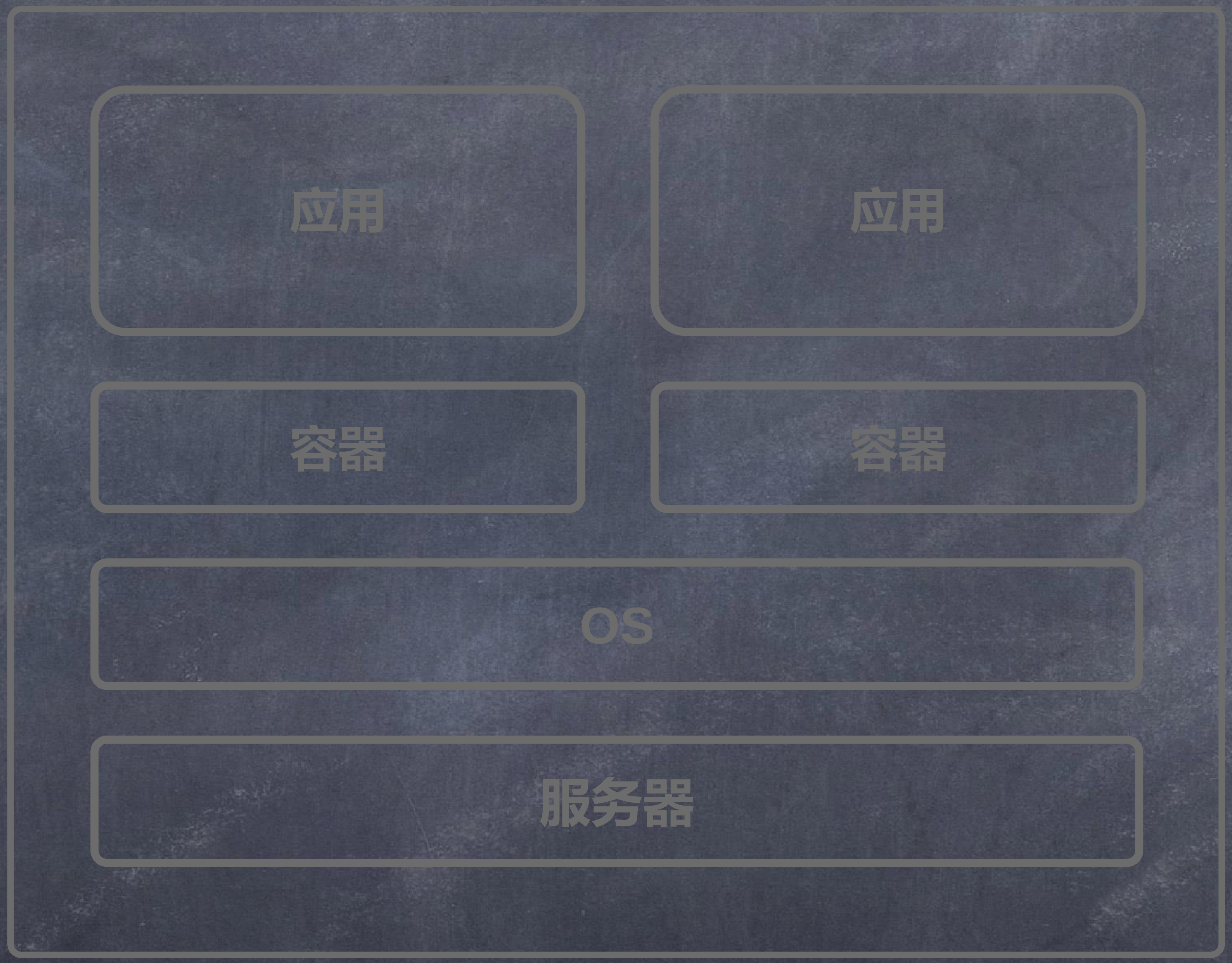
Financial Level Security with Kata



Old

katacontainers

Financial Level Security with Kata



应用 应用

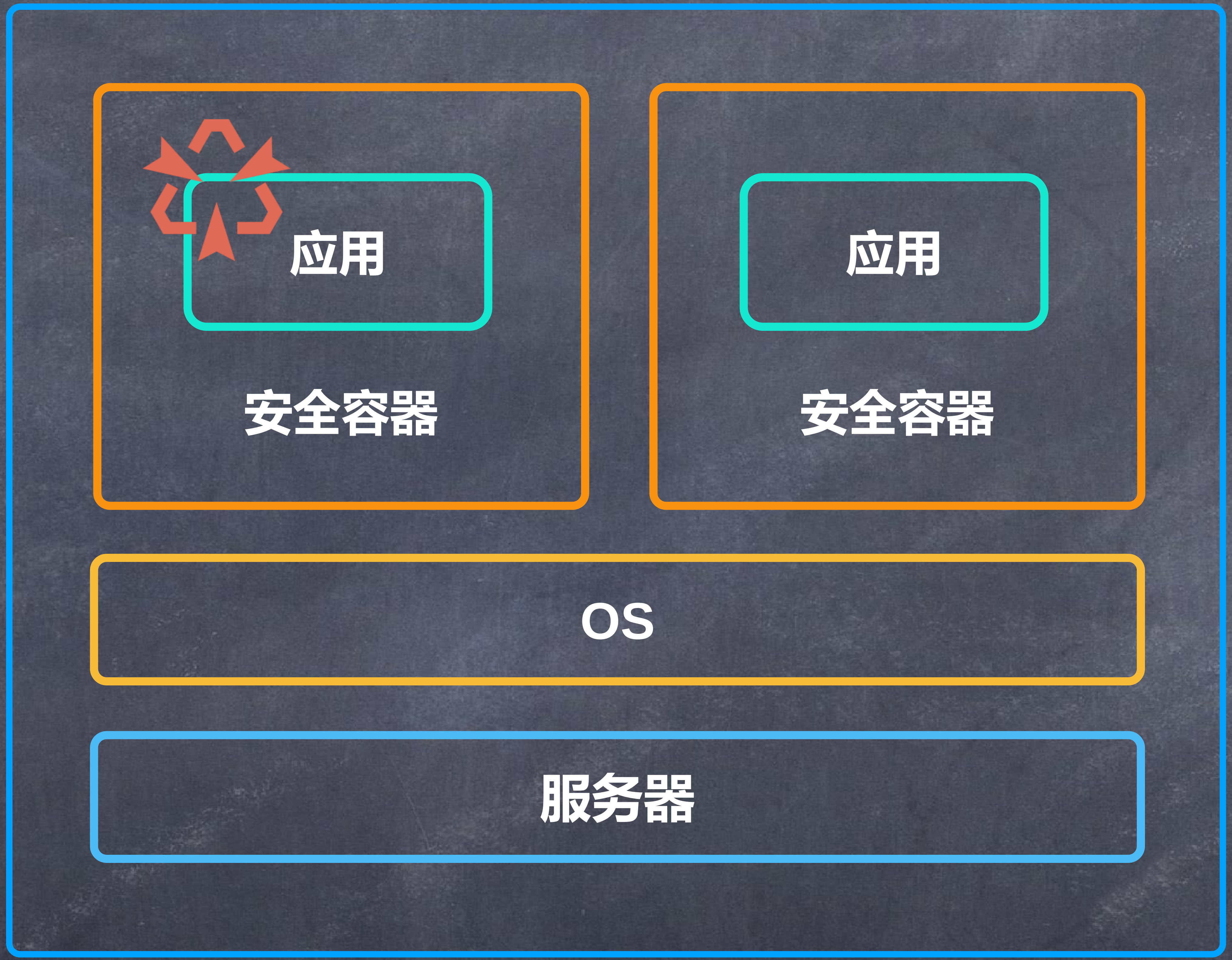
容器 容器

OS

服务器

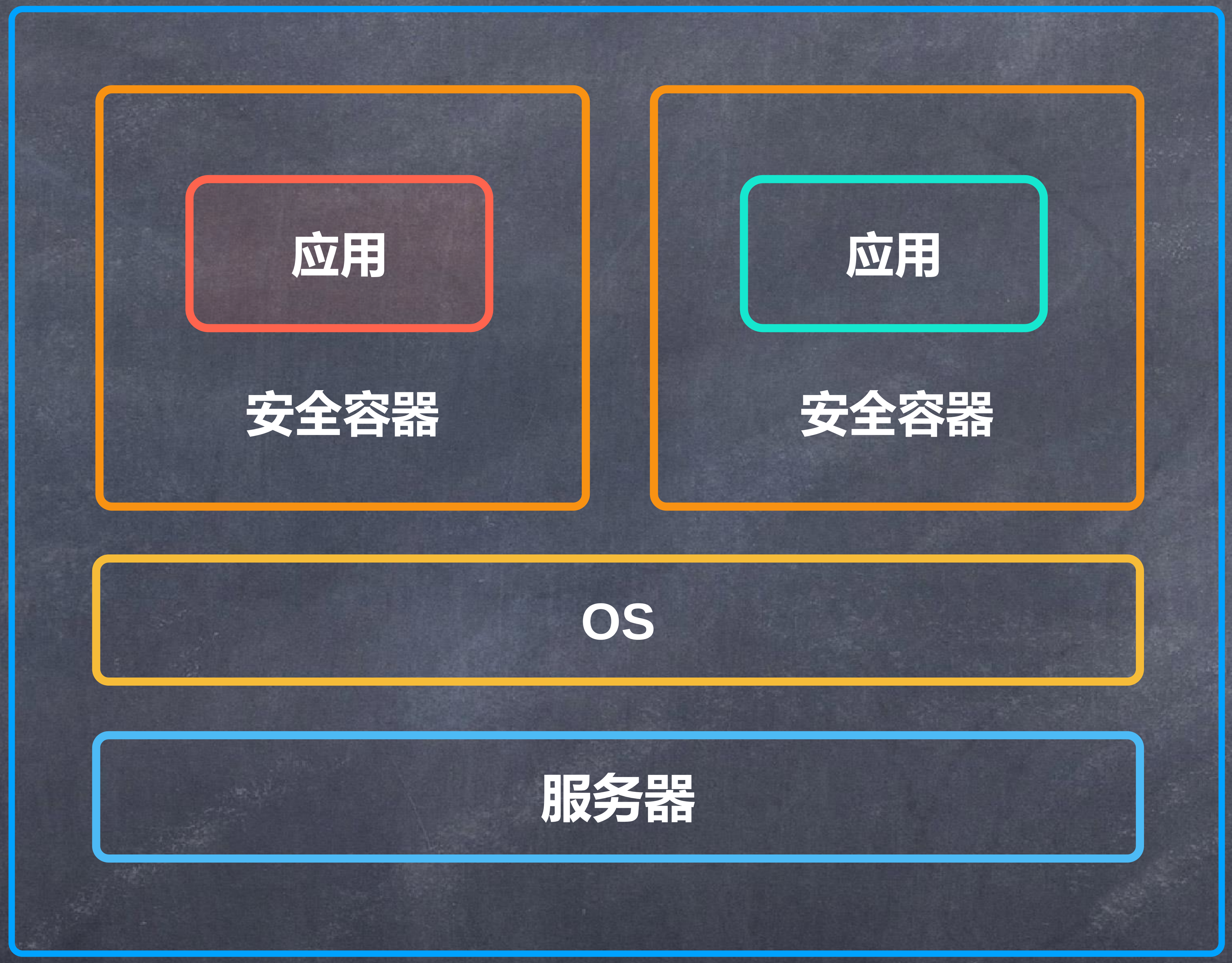
Old

Financial Level Security with Kata



New

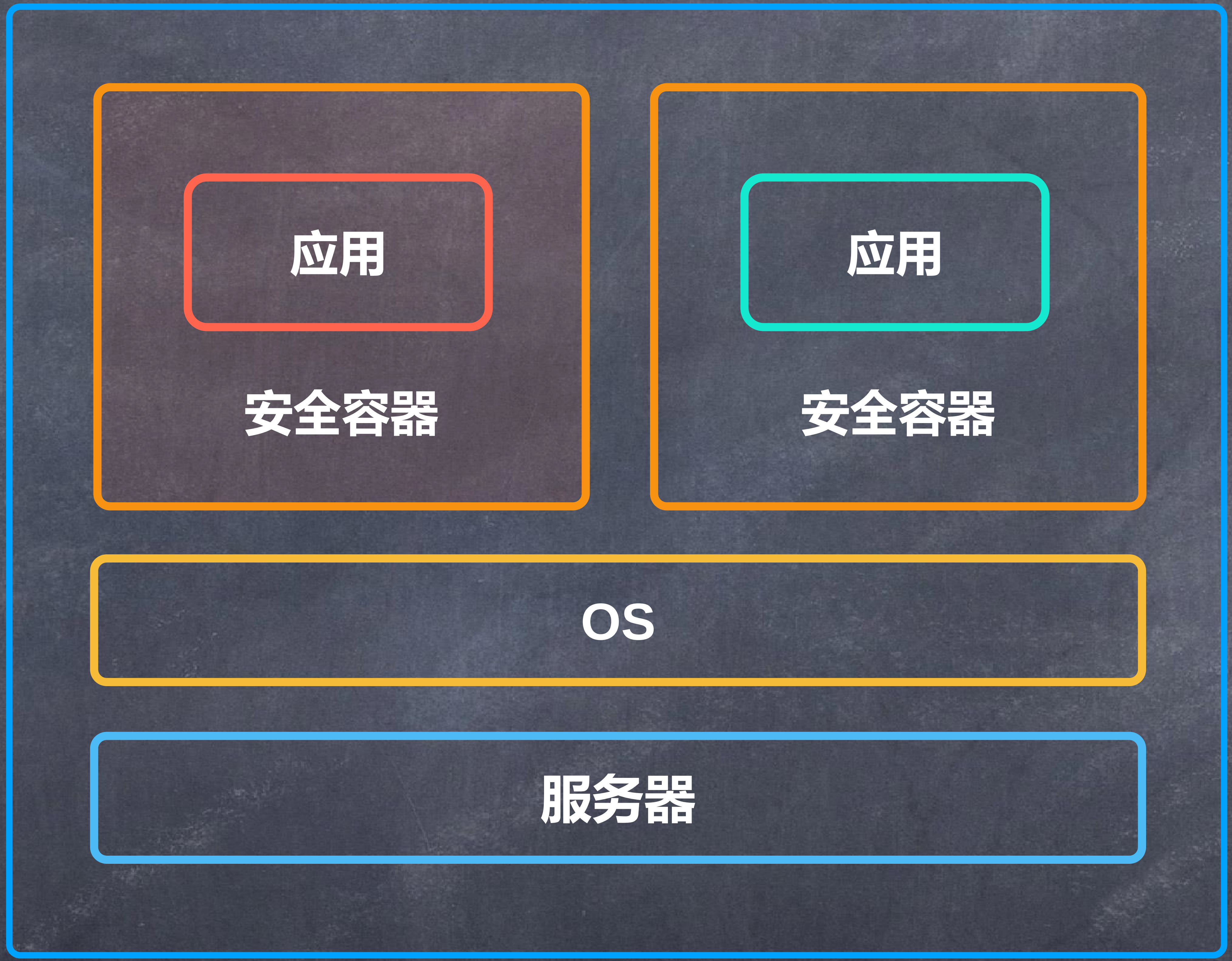
Financial Level Security with Kata



New

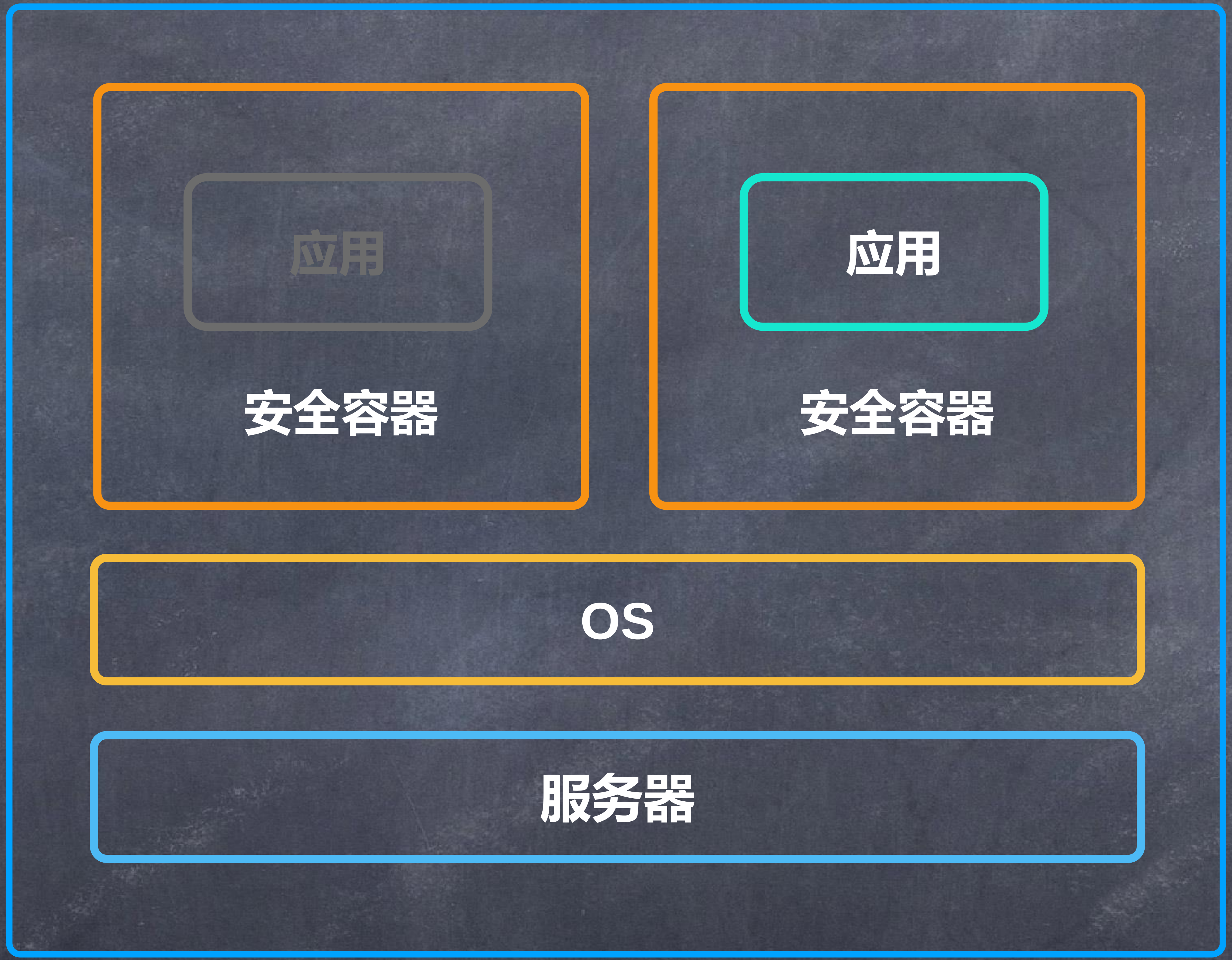
katacontainers

Financial Level Security with Kata



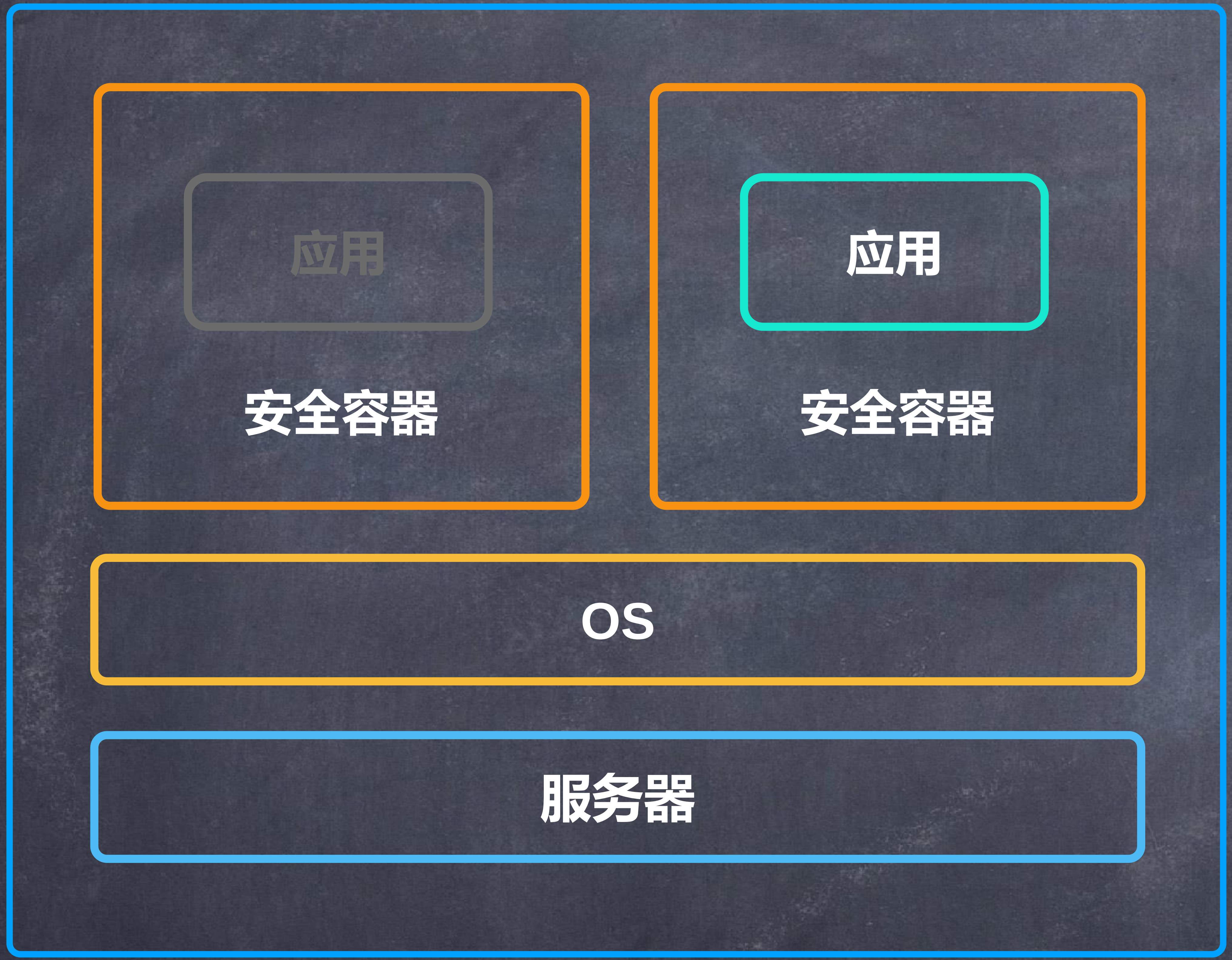
New

Financial Level Security with Kata



New

Financial Level Security with Kata



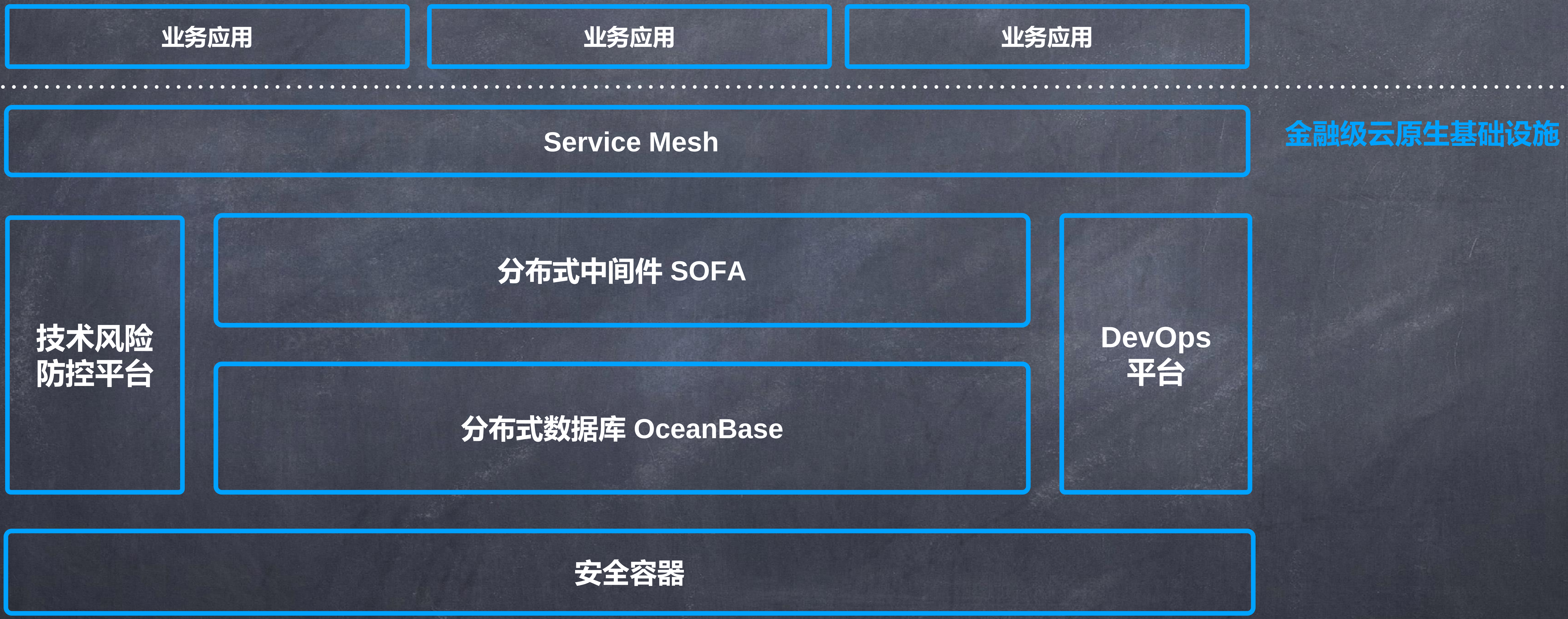
New

Kata Containers

成为OpenStack基金会旗下第一个新的顶级开放基础设施（Open Infrastructure）项目

katacontainers

Financial Cloud Native Service Architecture



katacontainers

Contribute

- https://katacontainers.io
- code/docs: https://github.com/kata-containers/
- Apache 2.0 license
- Slack: bit.ly/KataSlack
- IRC: #kata-dev@freenode
- Mailing list: kata-dev@lists.kata-containers.io

katacontainers

Future Plans

Continued enhancements around performance, security, ecosystem integration.

Short Term

- CRIO “v2 shim” support
- Tighter integration with Cilium network solutions
- virtio-fs for faster filesystem access

Medium Term

- jail/constraining hypervisor on host
- Kubernetes runtimeClass enhancements

Long Term

- Light hypervisors (rust-vmm based) support
- Virtio-mem for unified memory hotplug/unplug inside VM

- **Focus on reducing Kata complexity and enabling end users.**
- **2.0 plans underway to help address design simplification.**

Thank You