Microsoft

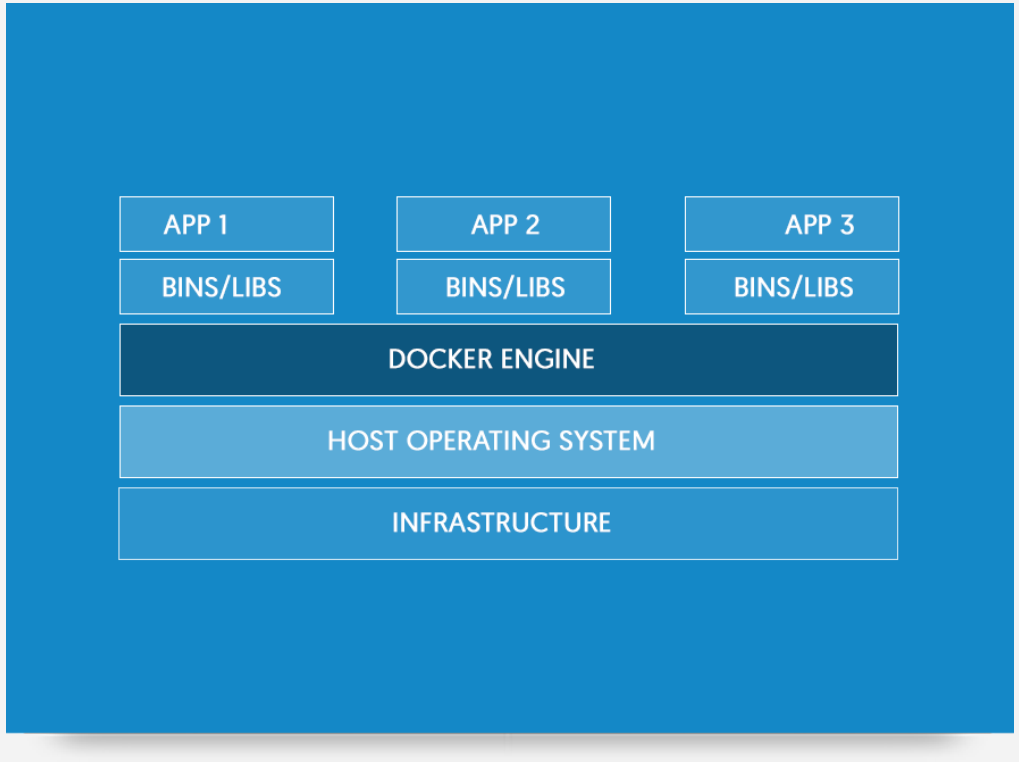
Enterprise security in the era of containers and Kubernetes

- Karthikeyan VK
- Twitter: @Karthik3030
- Blogs.karthikeyanvk.in

Microsoft

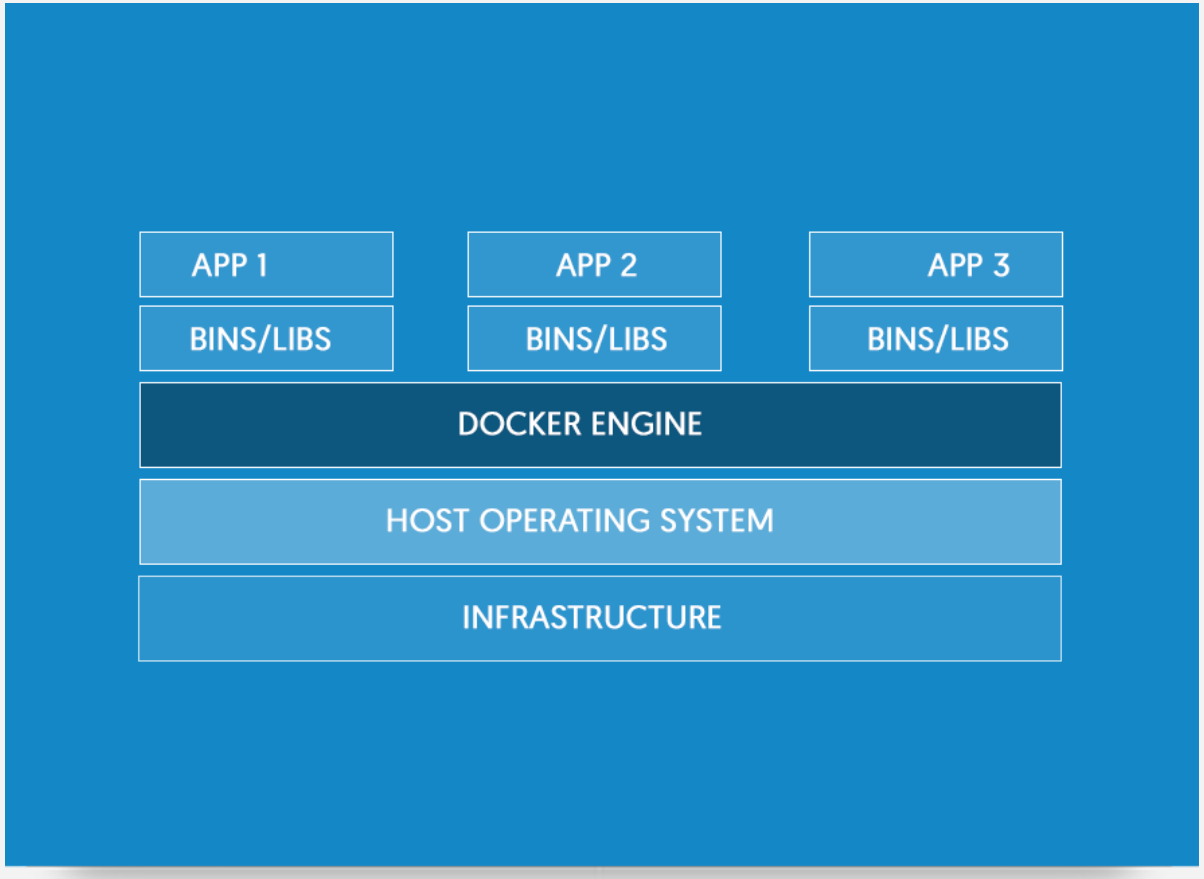
What is a Container?

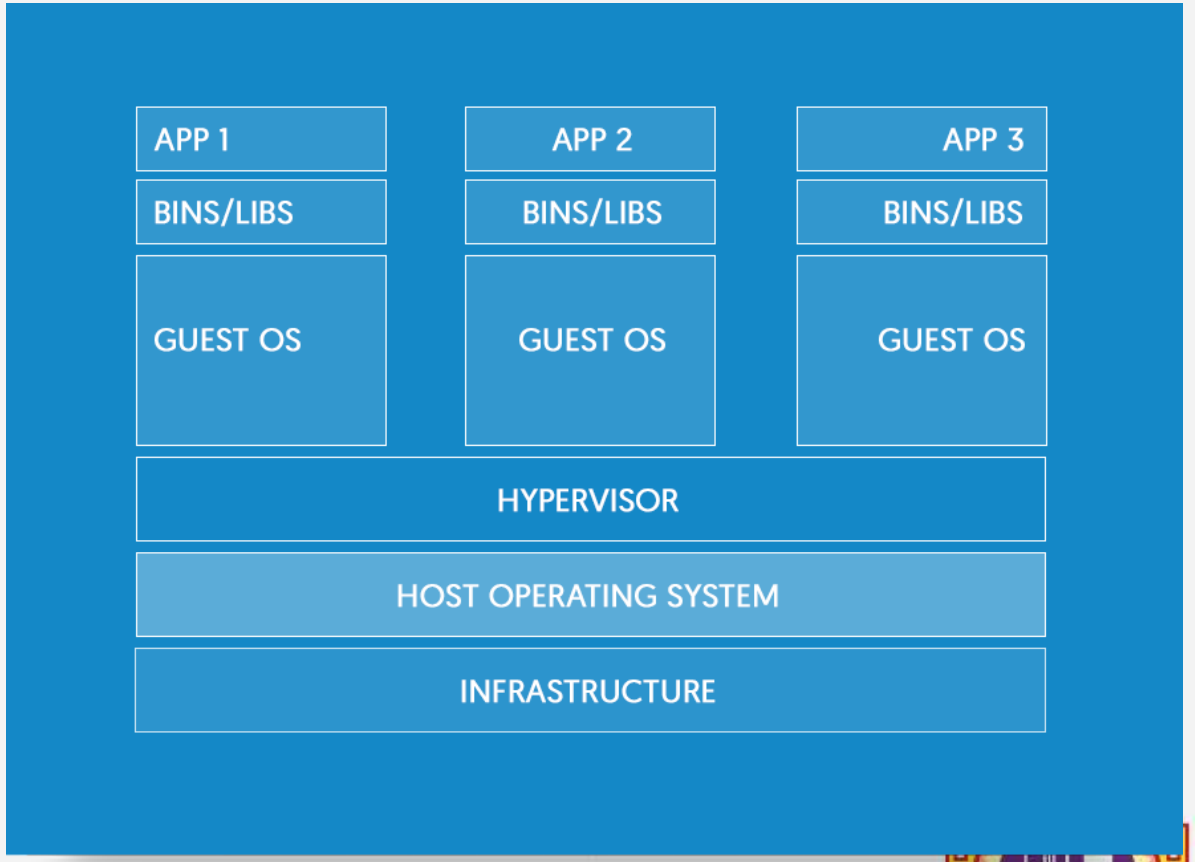
Windows Containers provide operating system virtualization that allows multiple isolated applications to be run on a single system.



Microsoft

Difference between Containers and VMs





Twitter: @Karthik3030
Blogs.karthikeyanvk.in

Microsoft

Difference between Containers and VMs

Twitter: @Karthik3030
Blogs.karthikeyanvk.in

Microsoft

Why Containers ?

Microsoft

Why Containers?

- Transforming existing applications into cloud Is Hard!
- Building Hybrid Cloud applications Is Hard!
- Think about building solutions that should be deployed in Azure, AWS & GCP at the same time

Microsoft

What is Docker ?

- Docker is an open platform for developing, shipping, and running applications

Microsoft

DEMO !!!

Microsoft

What is Kubernetes ?

- Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications.
- Orchestrator for Containers

Microsoft

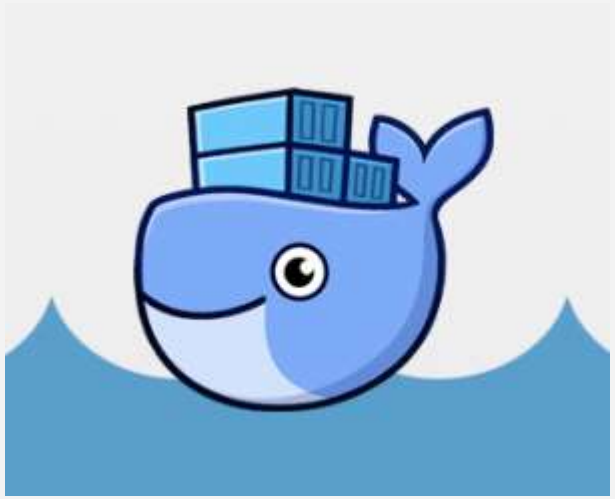
What is Kubectl ?

- Kubectl is a command line interface for running commands against Kubernetes clusters.

Microsoft

What is Pod?

- A Kubernetes pod is a group of containers that are deployed together on the same host.



Microsoft

What is Kubernetes Service?

- A Kubernetes Service is an abstraction which defines a logical *set* of Pods and a policy by which to access them

Microsoft

What is Kubernetes Replica Sets?

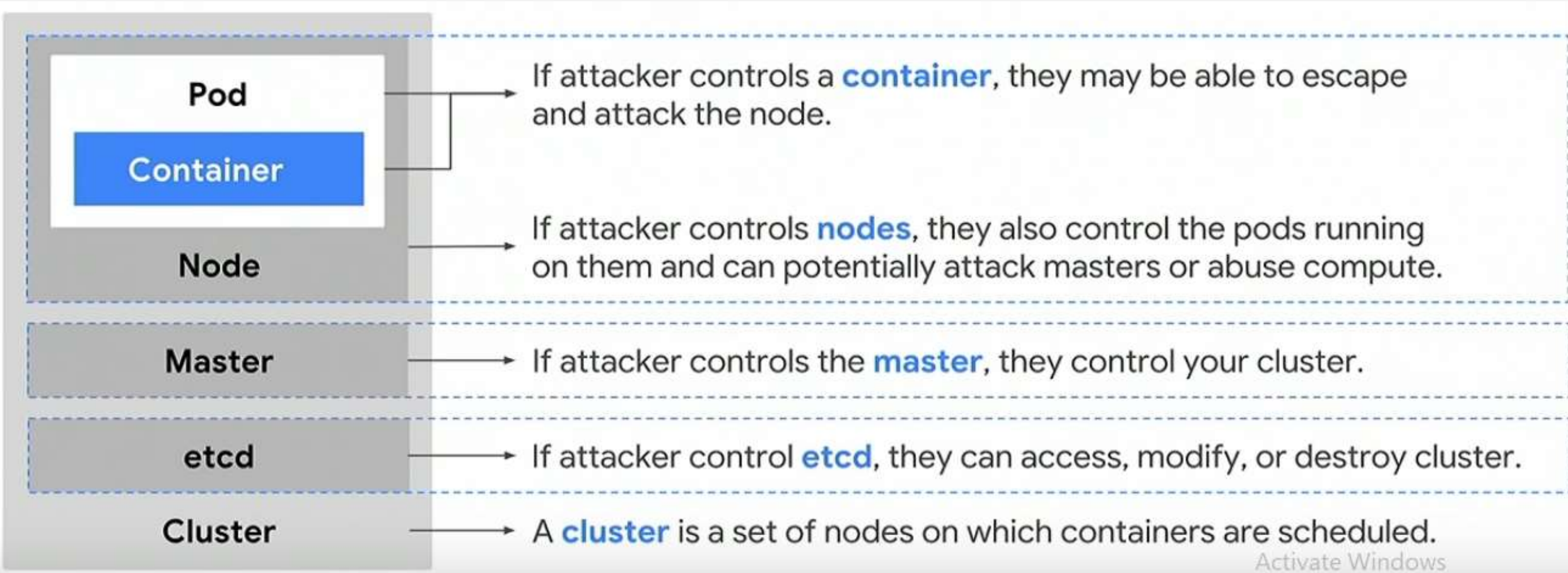
- Replica Set ensures how many replica of pod should be running. It can be considered as a replacement of **replication controller**.

Microsoft

DEMO !!!

Microsoft

Why Enterprise Level Security



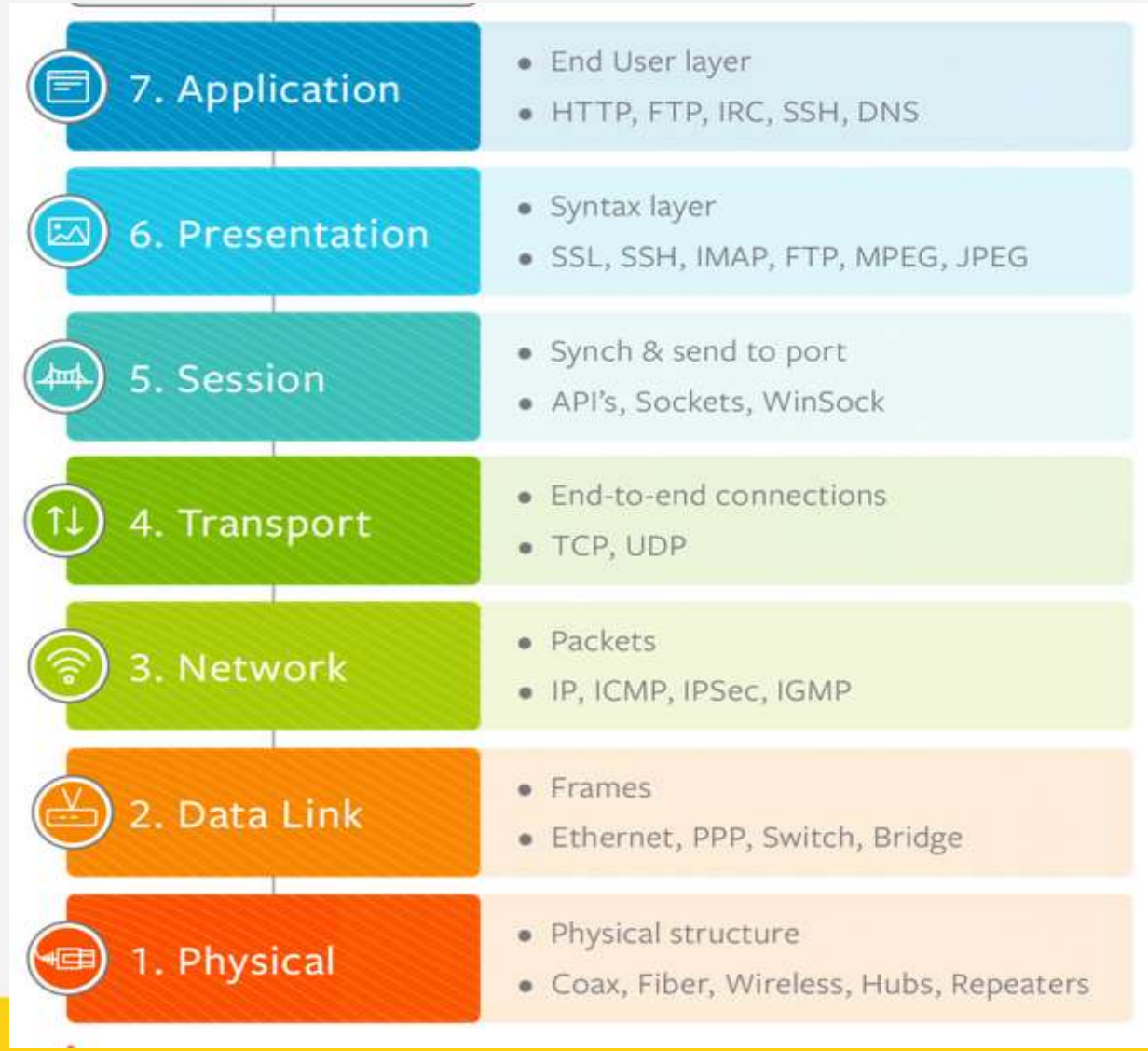
Microsoft

Enterprise Level Security Features in AKS

- Private Load Balancer
- Virtual Network
- L4 & L7 Capabilities
- Control Egress Traffic
- Control Ingress Traffic
- East-West Traffic Policies
- Whitelisting IP Addresses

Microsoft

L4 & L7 Security



Twitter: @Karthik3030
Blogs.karthikeyanvk.in

Microsoft

L4 & L7 Security

- L4 denotes TCP/UDP layer, where the network is flooded with packets of unnecessary data to enable Denial of Service Attack
- L7 Denotes Application layer, where the API call is bombarded with unnecessary GET, POST.
- Can be mitigated using application gateway or web application firewall of azure.

Microsoft

Ingress Traffic

- Traffic originating from external network
- Limit the traffic with ingress policies
- Controlled by setting which domain or which ip is allowed inside the network

Microsoft

Ingress Traffic

yaml Copy

```yaml
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: backend-policy
  namespace: development
spec:
  podSelector:
    matchLabels:
      app: webapp
      role: backend
  ingress: []
```

Microsoft

Egress Traffic

- Traffic originating from internal network to Internet
- Limit the traffic with 3rd party firewall

Microsoft

East-west Traffic

- Traffic between containers
- Think of one pod or container has been exploited.
- East-West traffic control is very important.

Microsoft

Whitelisting IP Addresses

- Control who should access
- Http routing is disabled by default
- Helps in avoiding unnecessary access and port scanning

Microsoft

DEMO !!!