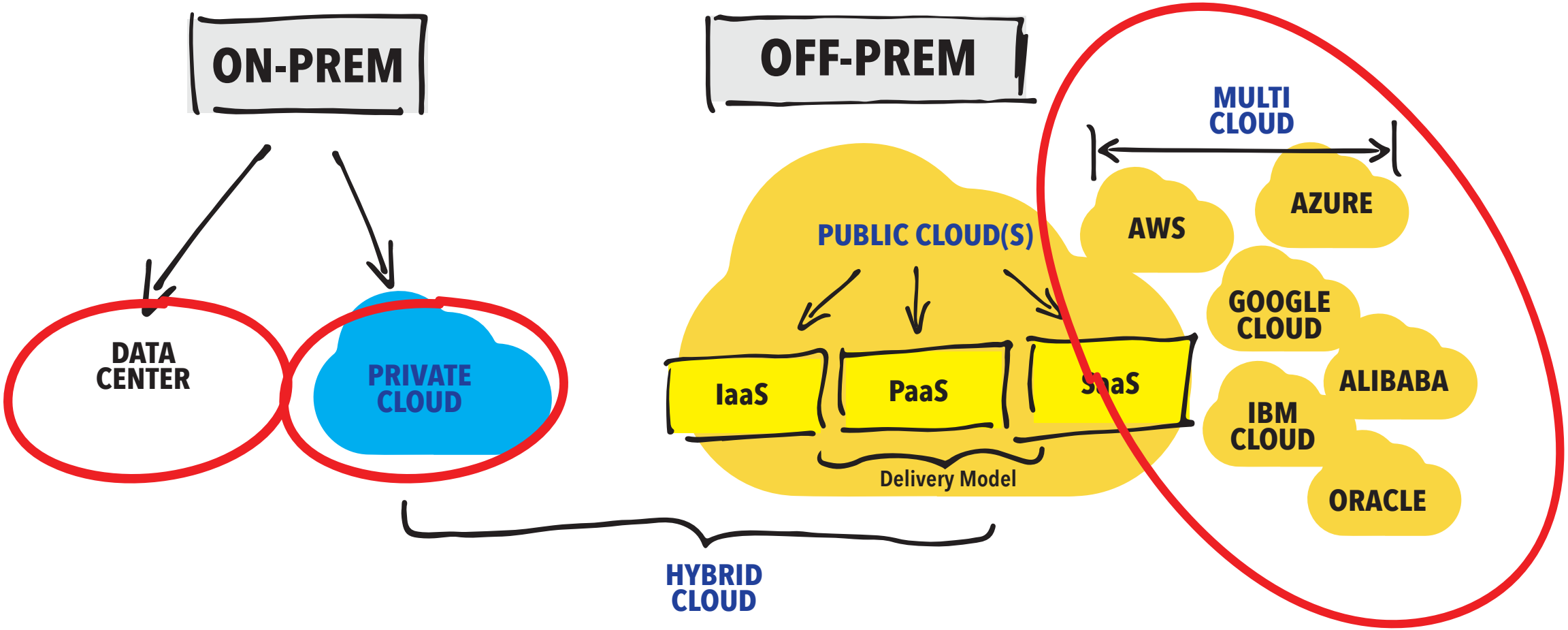
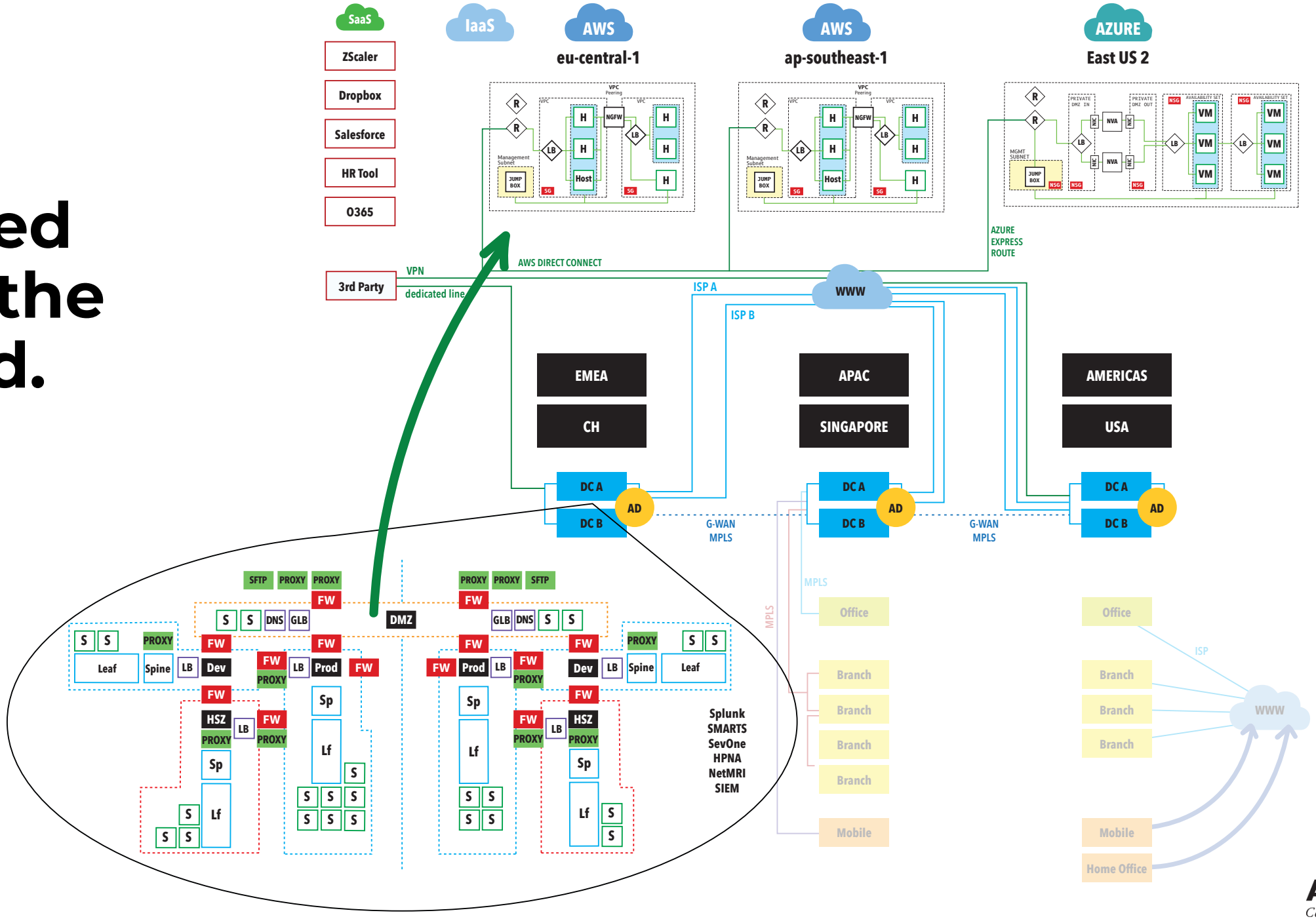
Container & Kubernetes & Serverless

Borna Cisar


ON-PREM
OFF-PREM
DATA CENTER
PRIVATE CLOUD
PUBLIC CLOUD(S)
IaaS
PaaS
SaaS
Delivery Model
MULTI CLOUD
AWS
AZURE
GOOGLE CLOUD
ALIBABA
IBM CLOUD
ORACLE
HYBRID CLOUD

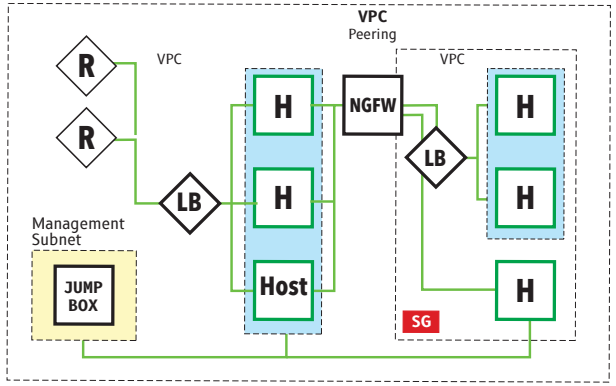
TECBITE INDUSTRIES

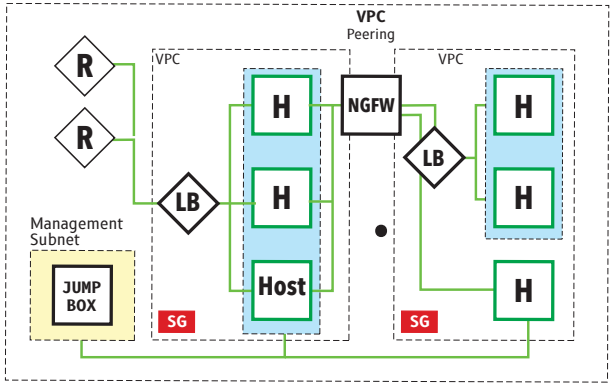
We moved into the cloud.

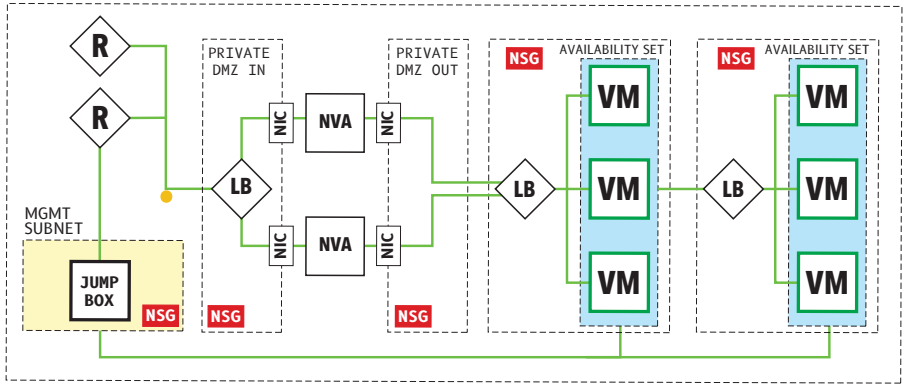


AVANTEC
Competence. Security. Trust.

We use VPCs to host our VM’s



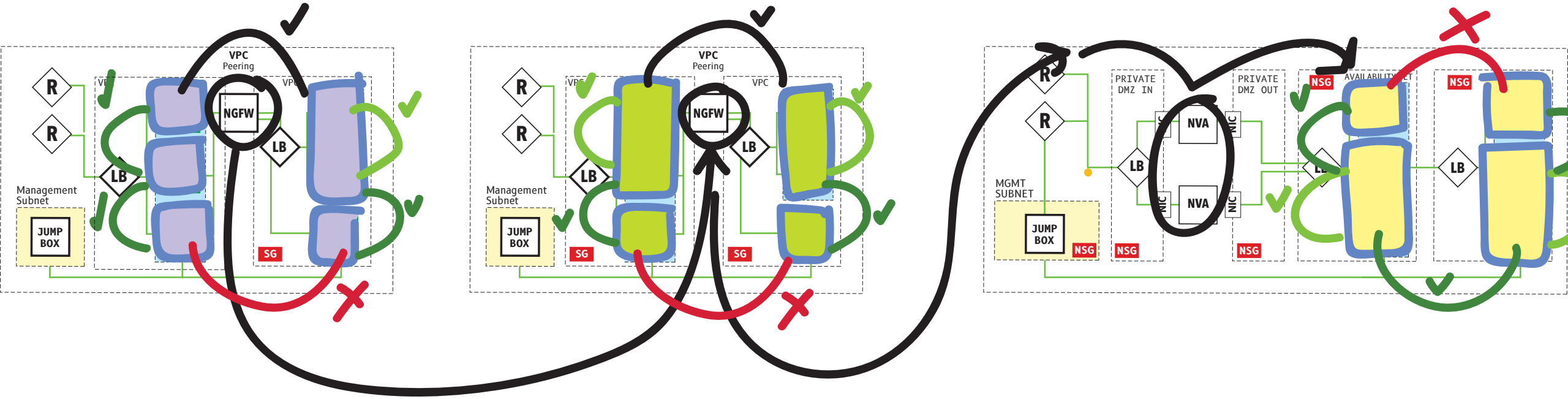




We’re elastic

AVANTEC
Competence. Security. Trust.

Still, there is lots of complexity...



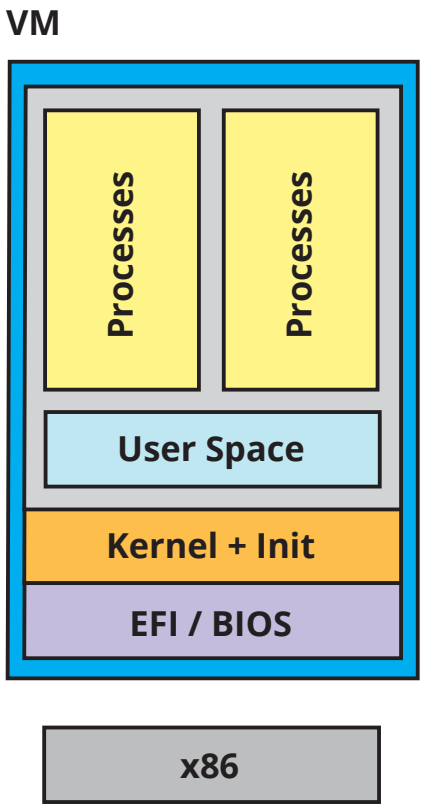
AVANTEC
Competence. Security. Trust.

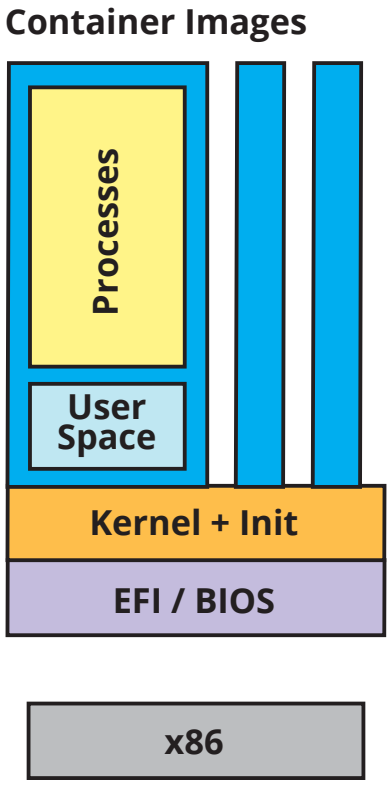
Especially, when using Multi-Cloud

And moving Apps between Clouds

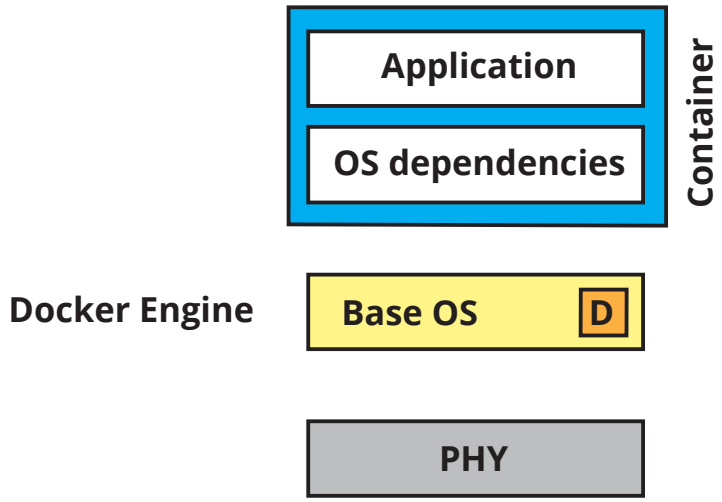
Then came the container.

What are containers?





What makes containers different?

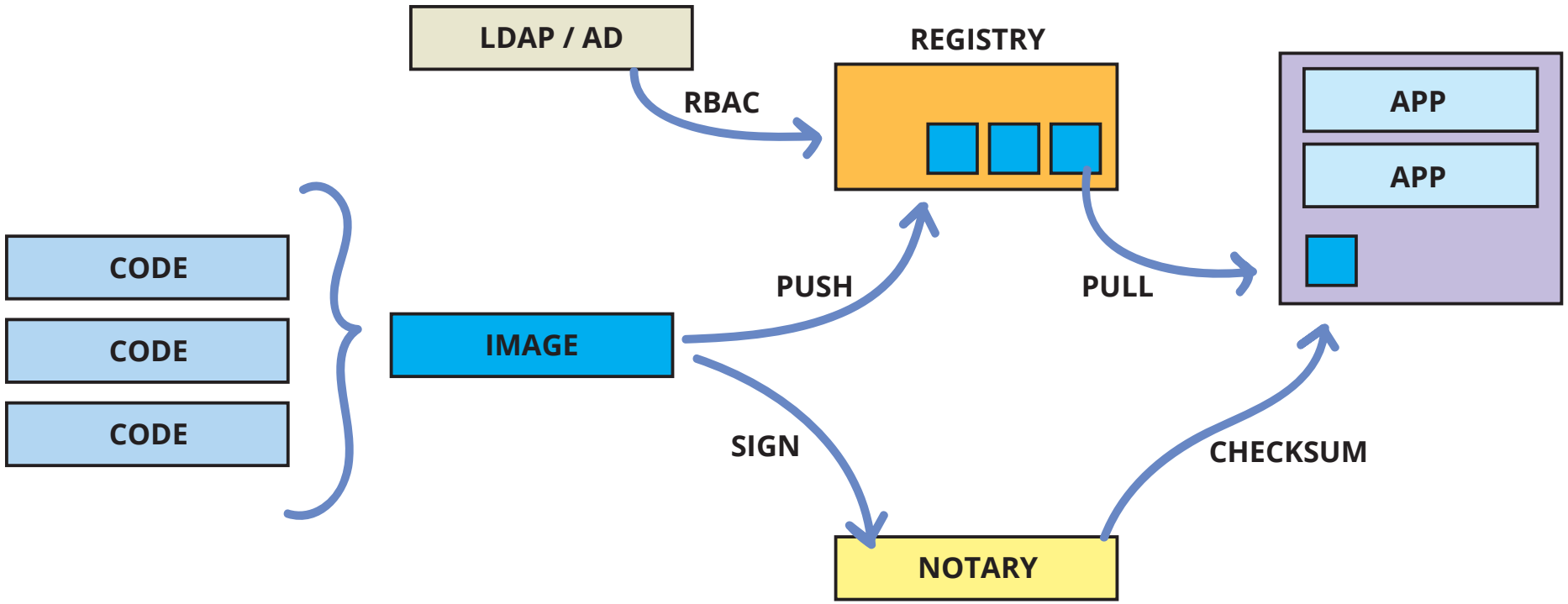


Ubuntu base container
ca. 100-120 MB
incl. user space

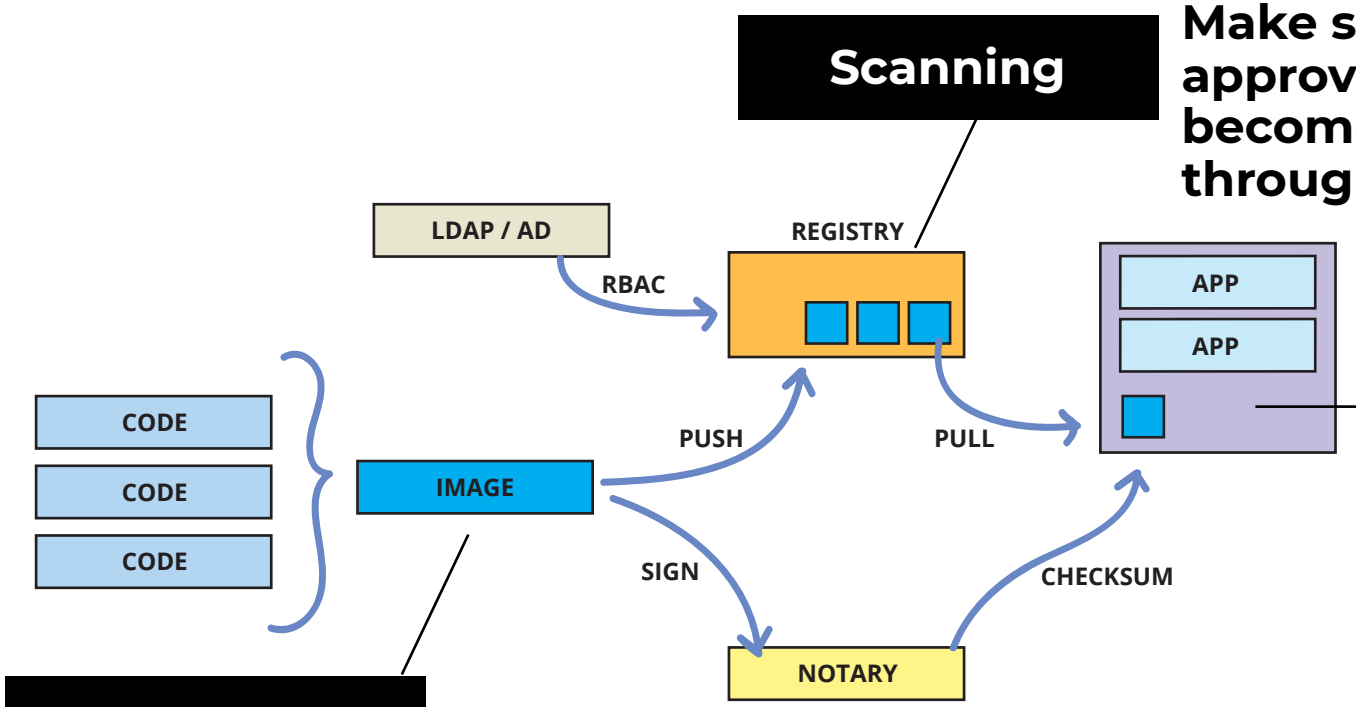
GO (Golang)
without user space
Only a few MB's

- **Size**
- **Isolation**
- **Boot time**

How to work with containers?



How to secure containers?



Scanning

Make sure that previously approved images haven't become vulnerable through new CVE's

Runtime

Runtime protection
Prevent unauthorised processes, file access, etc. (without stopping the container even)

CI/CD

Scanning

Detect known vulnerabilities (CVE)
Configuration Issues
Malware
Open-source dependency
+ Static analysis

- **RBAC**
- **Image Assurance (Policies)**

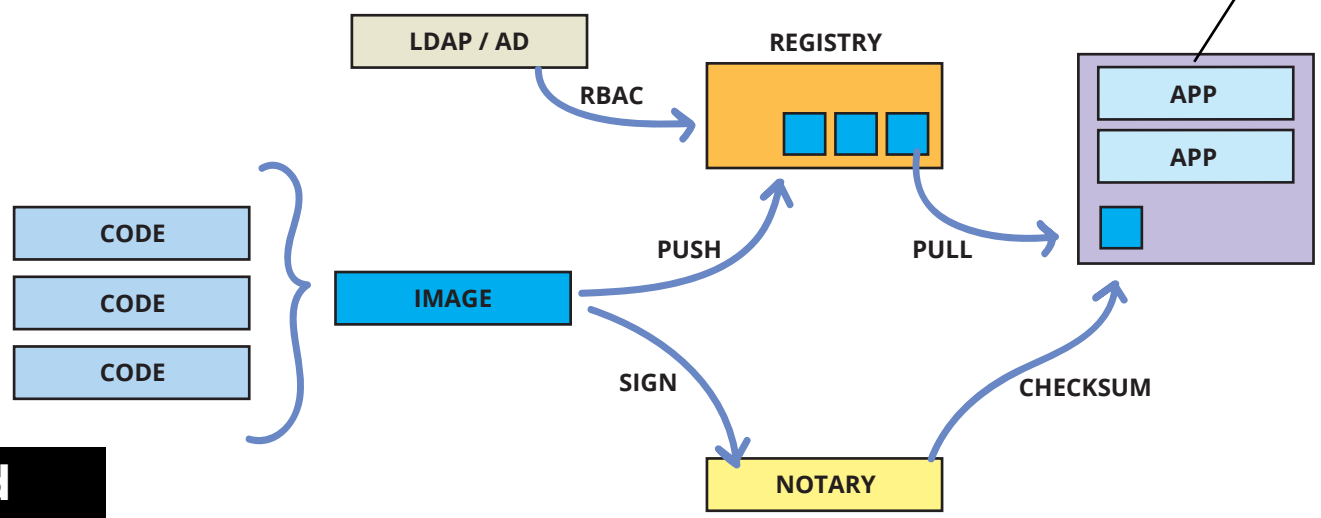
AVANTEC
Competence. Security. Trust.

How to secure containers?

- Fargate
- Azure Containers

Managed Containers

- There's no host / Cluster to manage
- Still possible to embed security controls into images during build and at deployment



Firewall

- Visualise network connections
- Automatically suggest firewall rules (whitelisting)
- Limit network traversal
- Limit attack blast radius
- Baselines

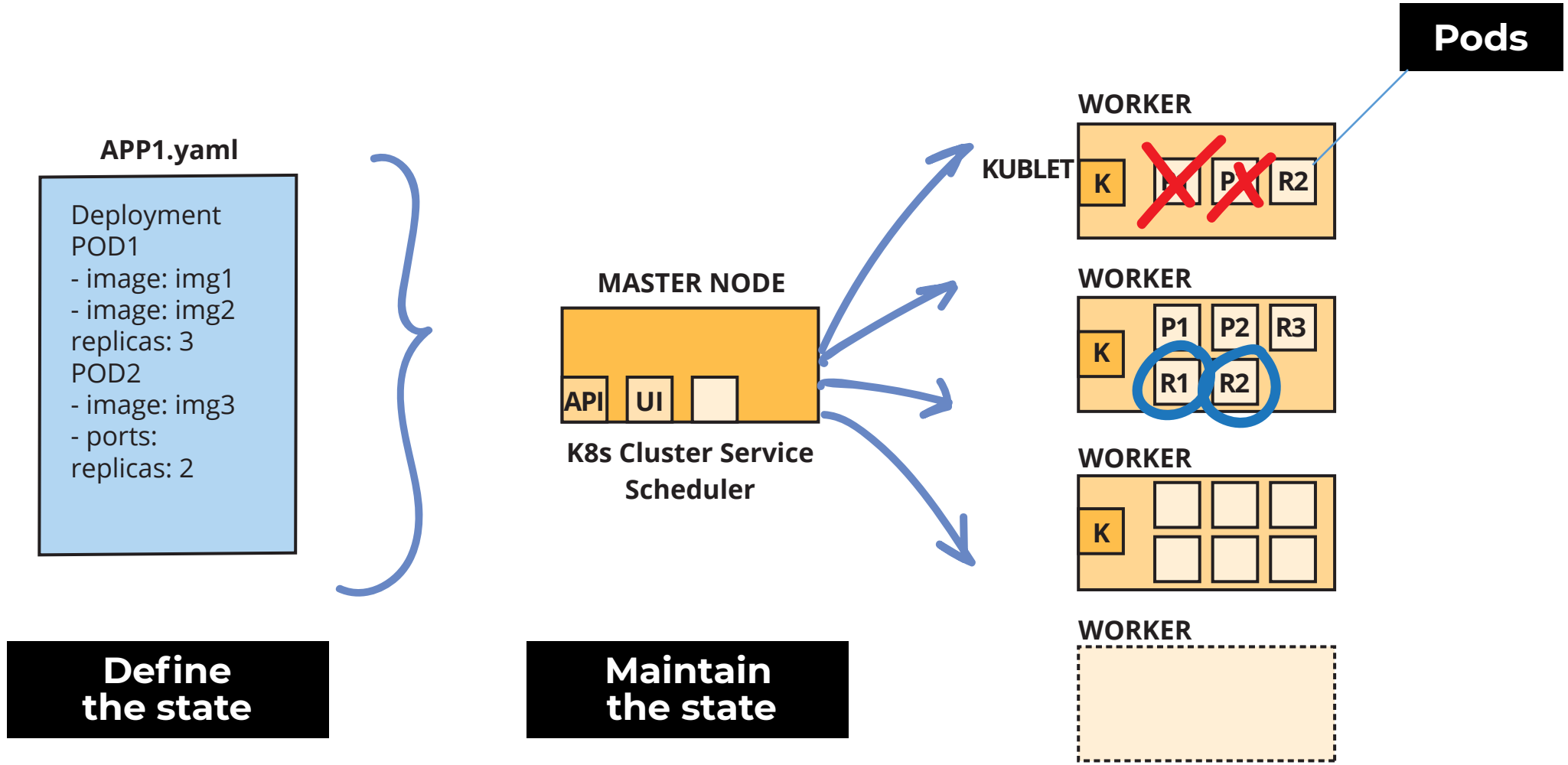
AVANTEC
Competence. Security. Trust.

OK, now we have lots and lots of containers...

And need to orchestrate them. Introducing: Kubernetes

“Desired state management”

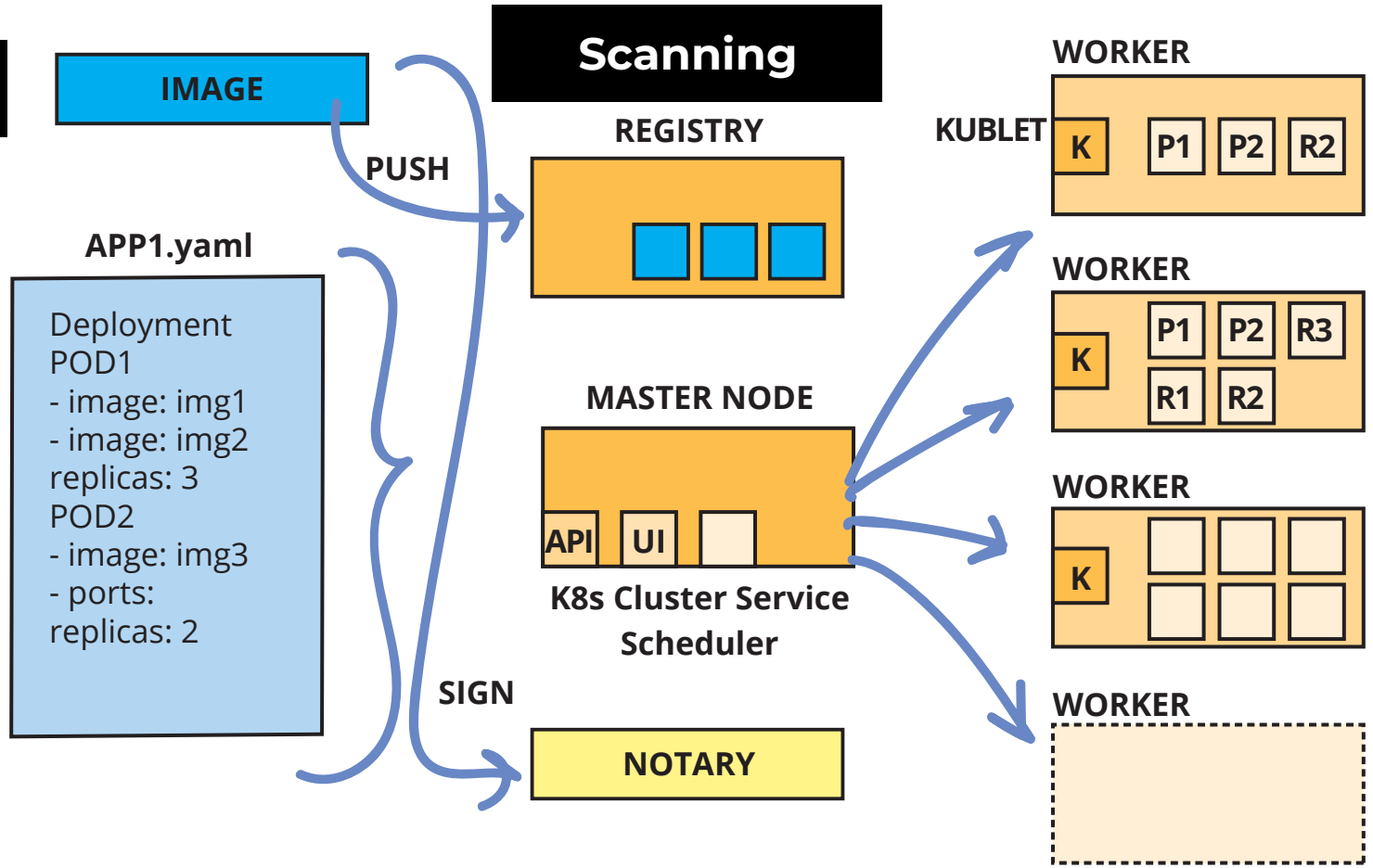
Kubernetes: Containers at scale.



OK, and is Kubernetes secure?

Scanning

- Detect known vulnerabilities (CVE)
- Configuration Issues
- Malware
- Open-source dependency



Runtime

- Monitor Pod behaviour
- Enforce assurance
- Runtime protection
- Baselining

Firewall

- Define policies during build
- Enforce during run

Logging

AVANTEC
Competence. Security. Trust.

Native & NGFW

It’s not about one or the other. Combine any cloud provider policies, such as AWS Security Groups or Azure Security Groups, or cloud platform policies, such as Kubernetes security policies, Istio API-level perimeter policy and then consolidate them.

AVANTEC
Competence. Security. Trust.

Native & NGFW

This allows users to immediately understand inbound and outbound rules as well as enforce application-aware embedded policies across cloud infrastructure and microservices.

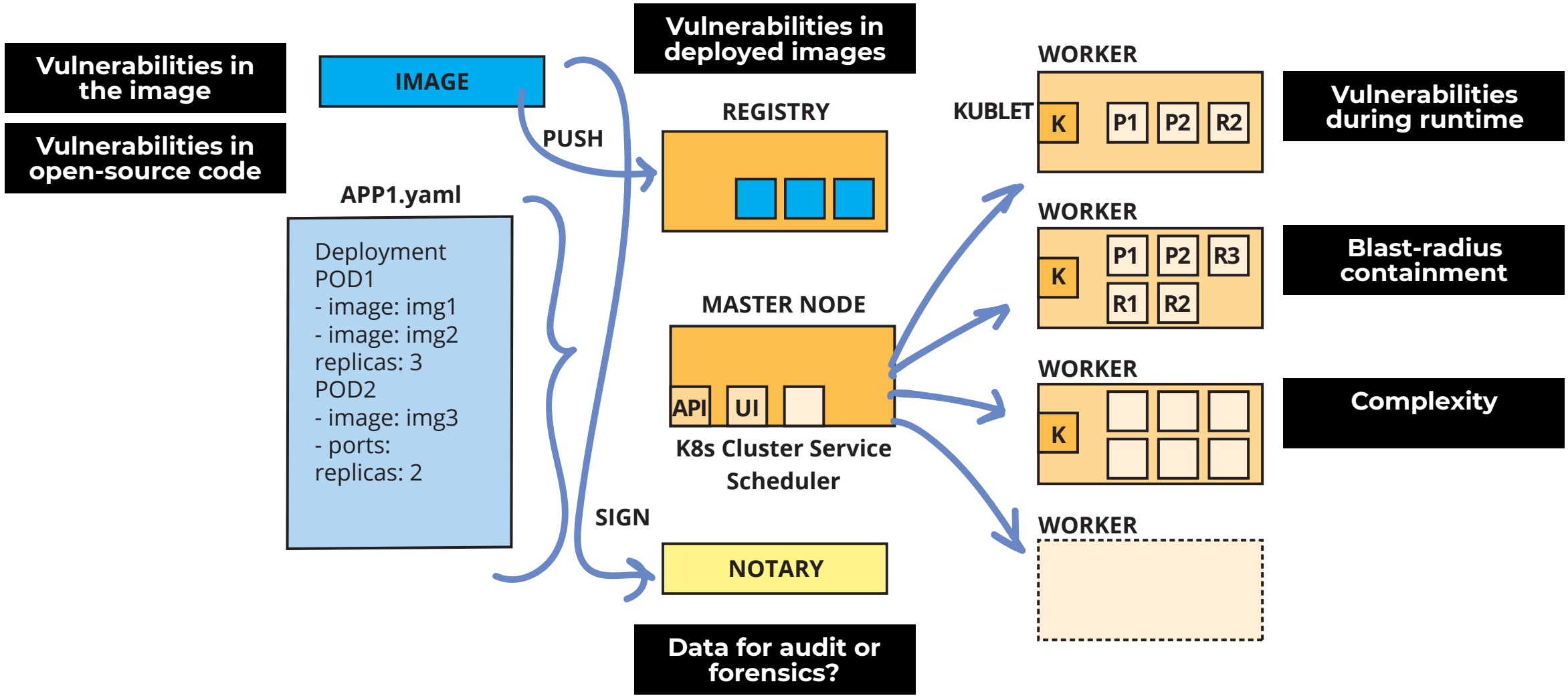
AVANTEC
Competence. Security. Trust.

Native & NGFW

- Policy simplification
- Policy unification
- Embed policy directly onto the workload
- Integrate logging and alerting with Operations / SOC

AVANTEC
Competence. Security. Trust.

What are the Risks, after all?

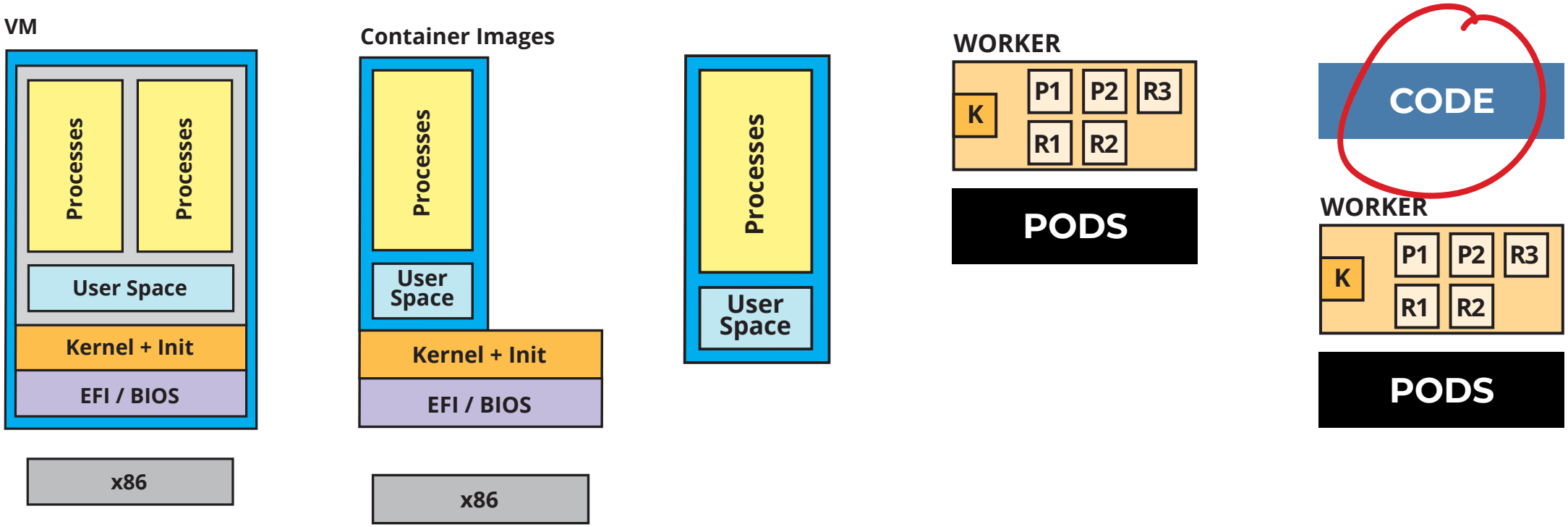


AVANTEC
Competence. Security. Trust.

Why use a Platform and not just the tools that Kubernetes offers

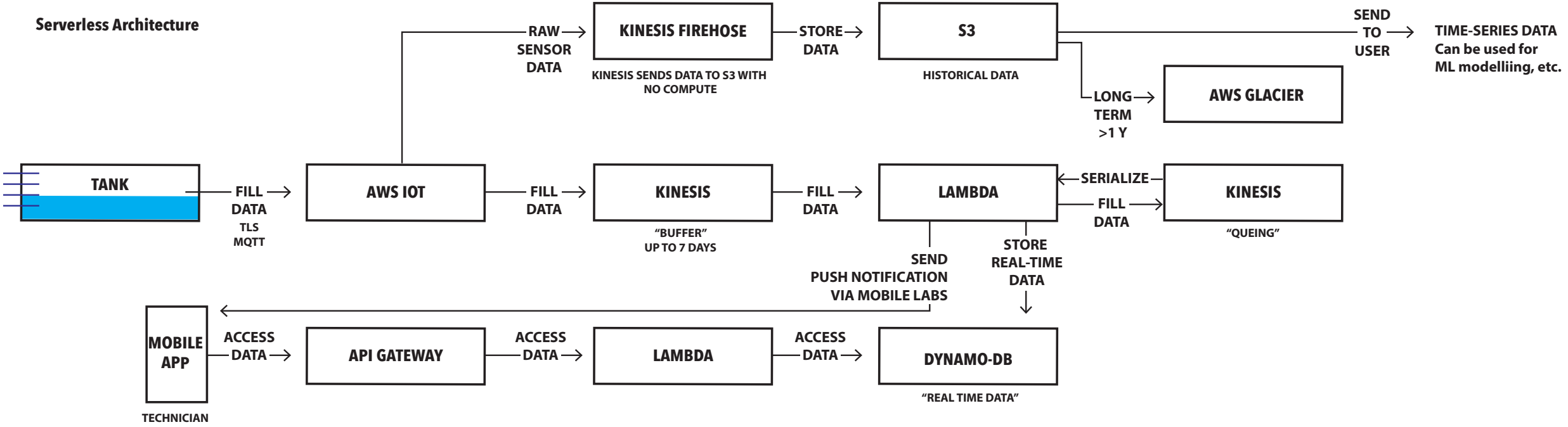
Kubernetes is open-source and most tools used with Kubernetes are open-source as well. Like Istio, Prometheus, Grafana, etc.
Do you DevOps or DevSecOps?
Container Security Platforms are ready-made and easier to use.

OK. And Serverless?



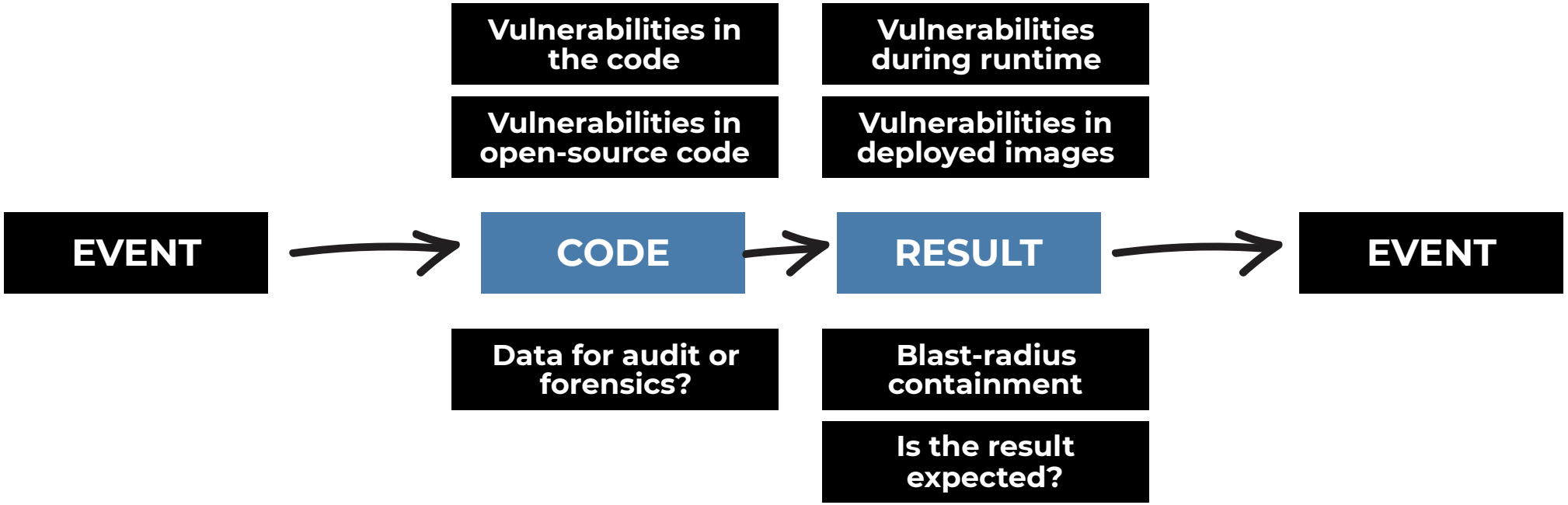
Serverless und Functions as a Service (FaaS)

Serverless Example



AVANTEC
Competence. Security. Trust.

Risks in Serverless



How to secure Serverless?

Scanning

- Detect known vulnerabilities (CVE)
- Configuration Issues
- Malware
- Open-source dependency

Runtime

- Monitor Code behaviour
- Enforce assurance
- Runtime protection
- Baselining

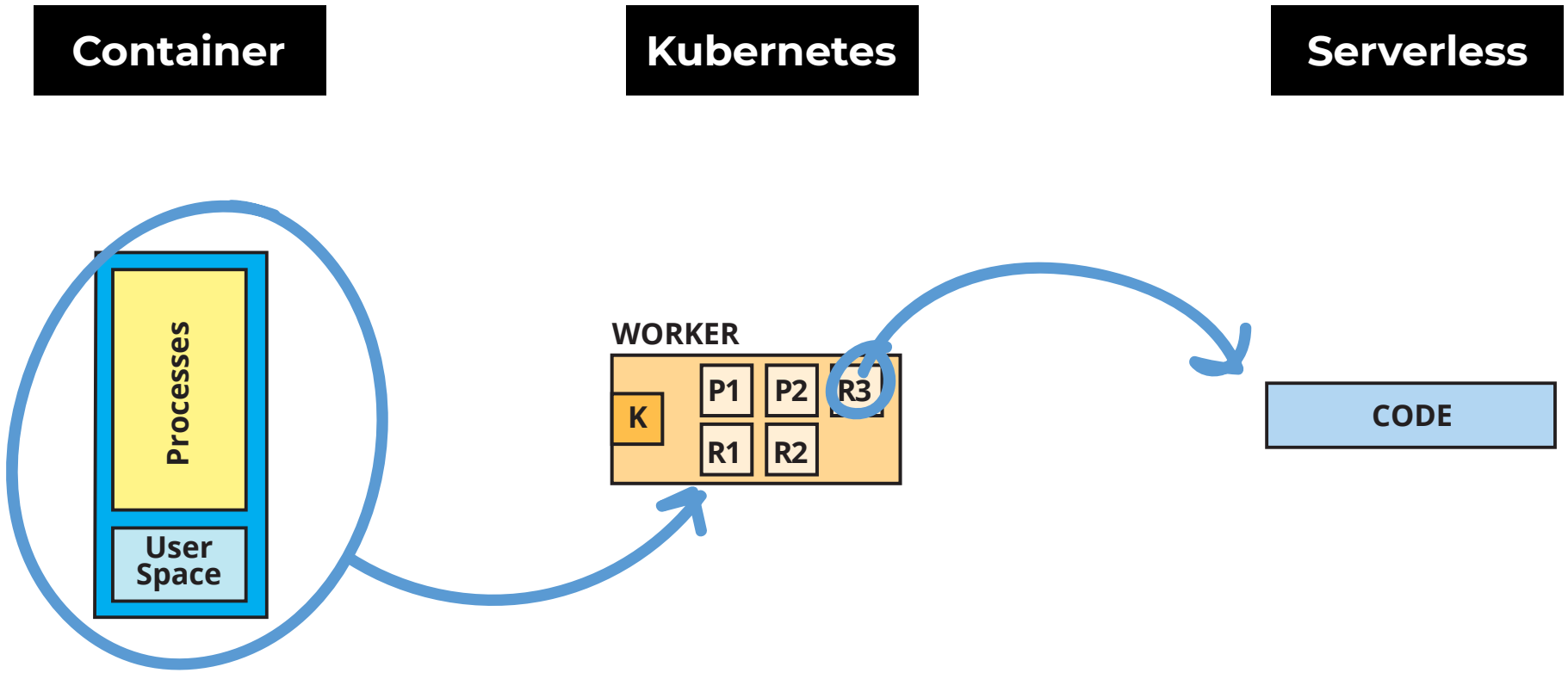
Firewall

- Define policies during build
- Enforce during run
- Embed FW in code
- Embed code in secure code

Logging

AVANTEC
Competence. Security. Trust.

Overview



Thank you

AVANTEC
Competence. Security. Trust.