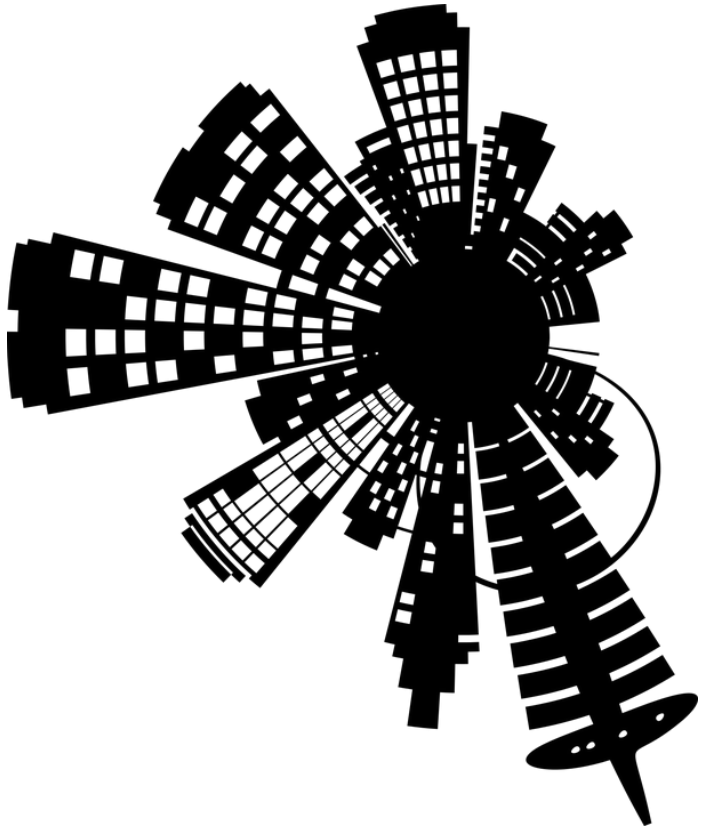
SACON International 2017

India | Bangalore | November 10 – 11 | Hotel Lalit Ashok



Architecting cloud services

Moshe Ferber
CSA Israel
@Ferbermoshe

SACON International

angalore | November 10 – 11 | Hote

ONLINECLOUDSEC.COM

The Cloud & I,
CISO challenges with the cloud

When the winds of change blow, some people build walls and others build windmills.
- Chinese Proverb

Moshe Ferber

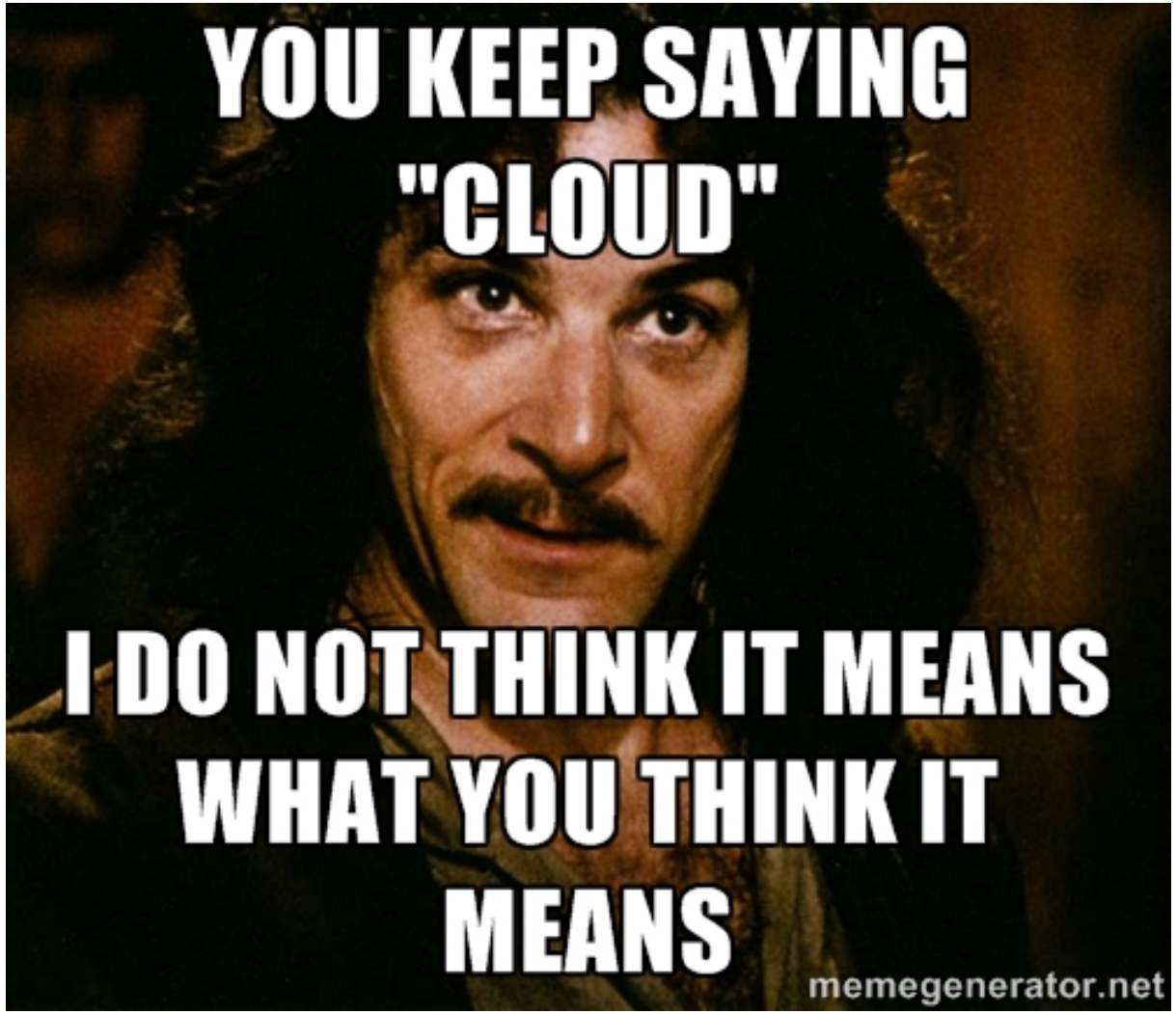
CCSK, CCSP

About myself

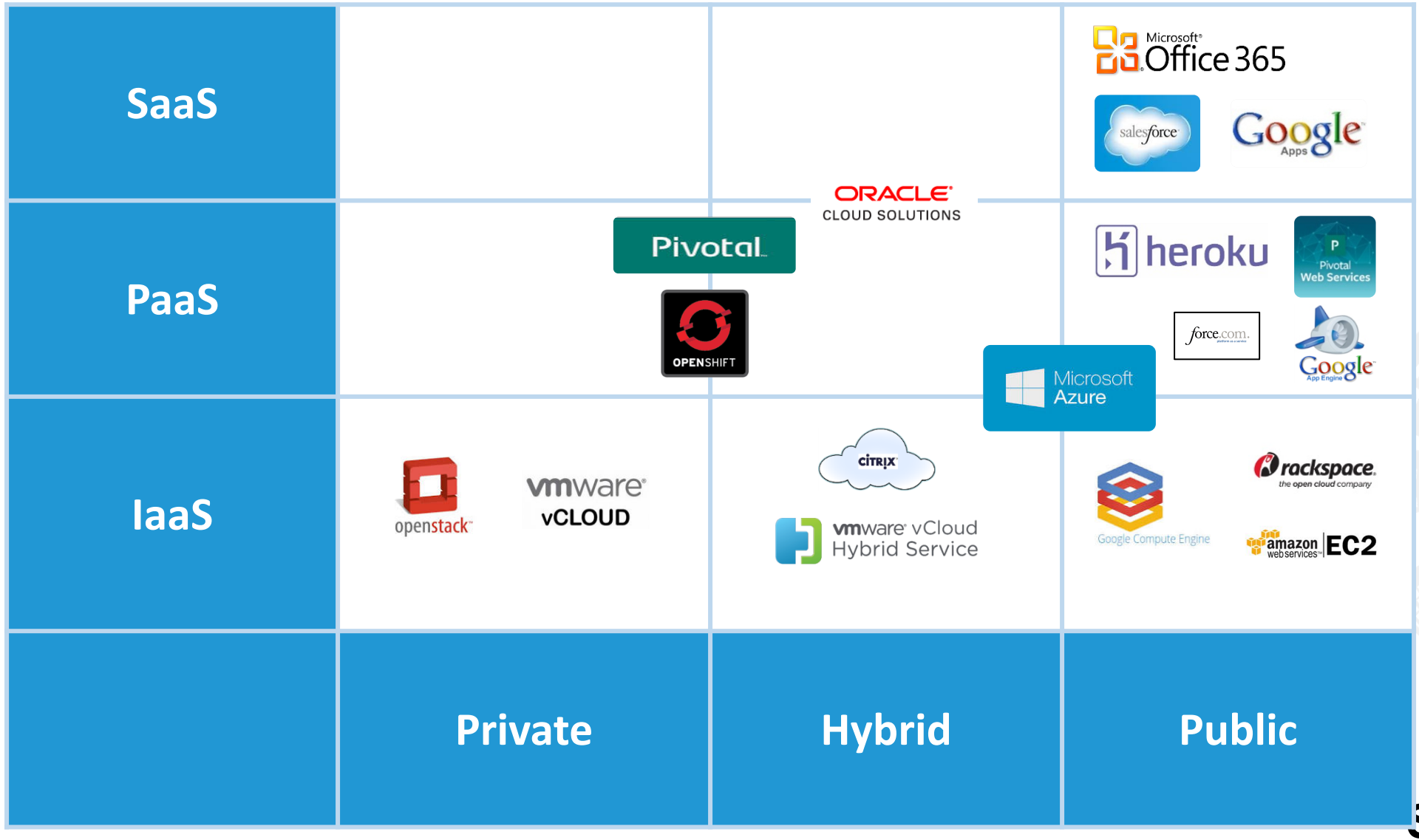
- ✓ Information security professional for over 20 years
- ✓ Founder, partner and investor at various cyber initiatives and startups
- ✓ Popular industry speaker & lecturer (DEFCON, BLACKHAT, RSA and more)
- ✓ Founding committee member for ISC2 CCSP certification.
- ✓ CCSK Certification lecturer for the Cloud Security Alliance.
- ✓ Member of the board at Macshava Tova – *Narrowing societal gaps*
- ✓ Chairman of the Board, Cloud Security Alliance, Israeli Chapter

CSAIL cloud security ISRAEL alliance℠

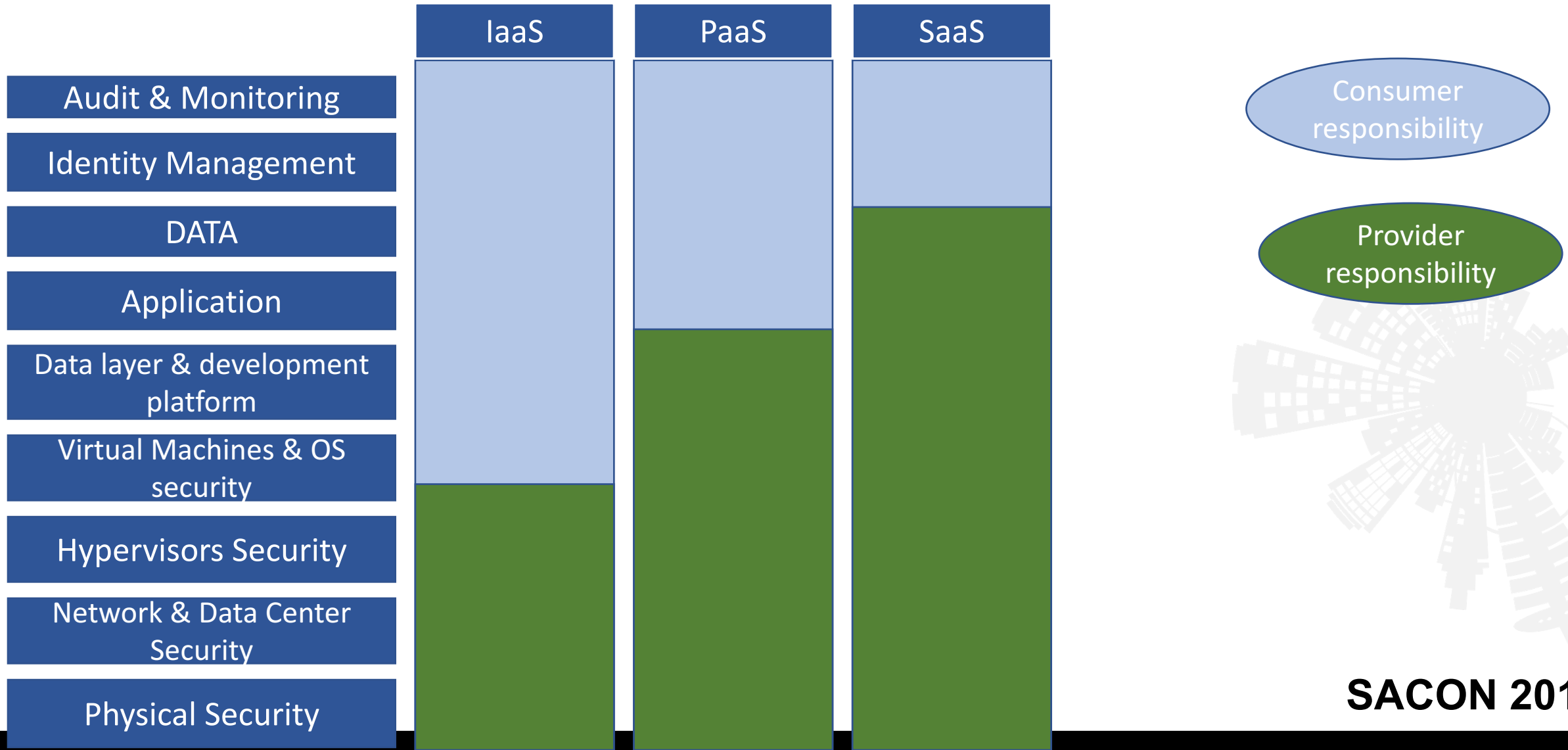
So, what is cloud?



Cloud Services are very different in nature



The shared responsibility model



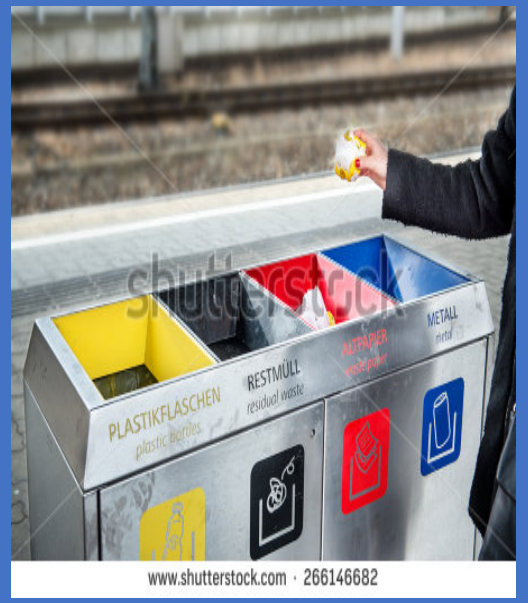
The CISO Challenge

IaaS/PaaS

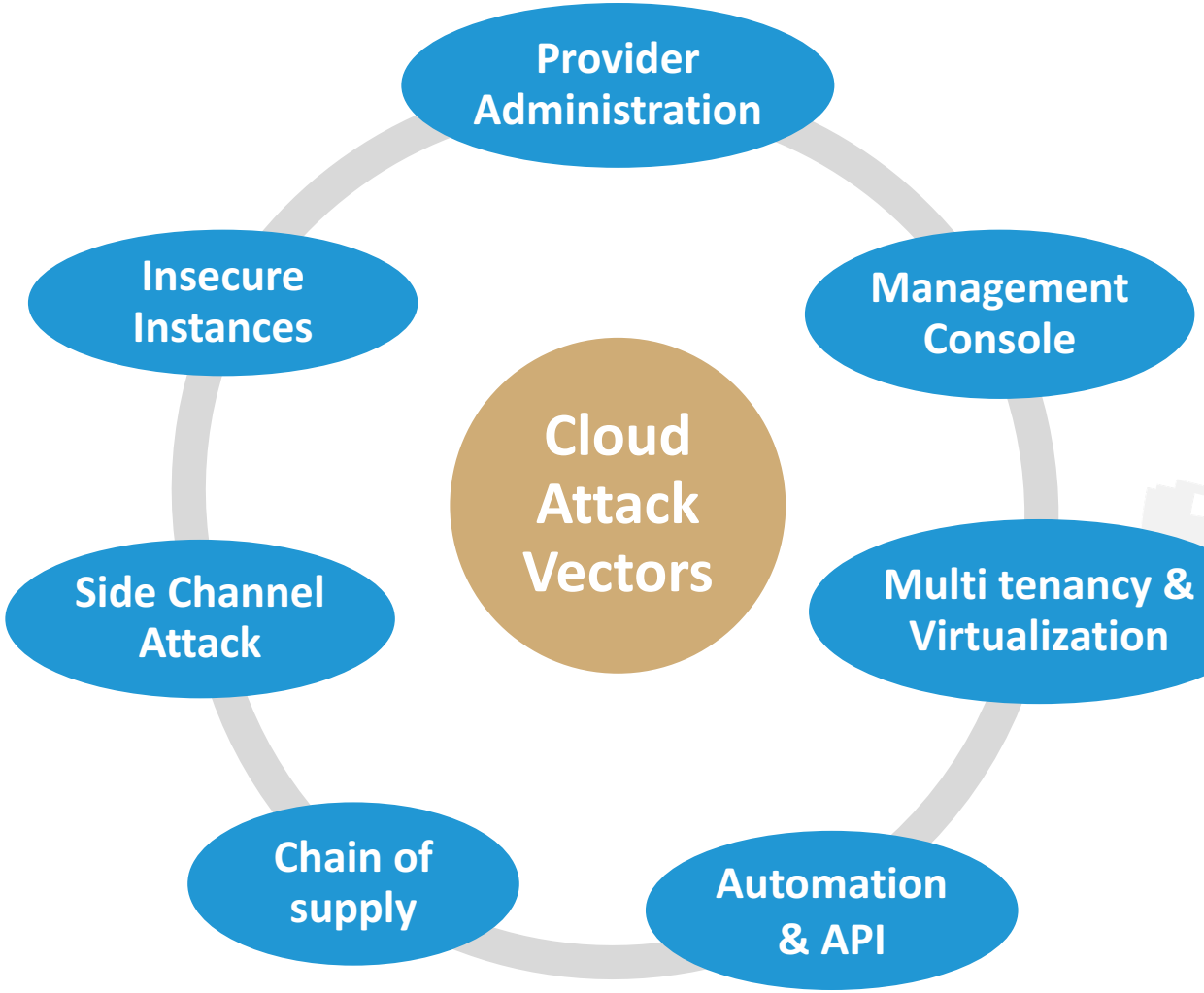
How to build secure applications

SaaS

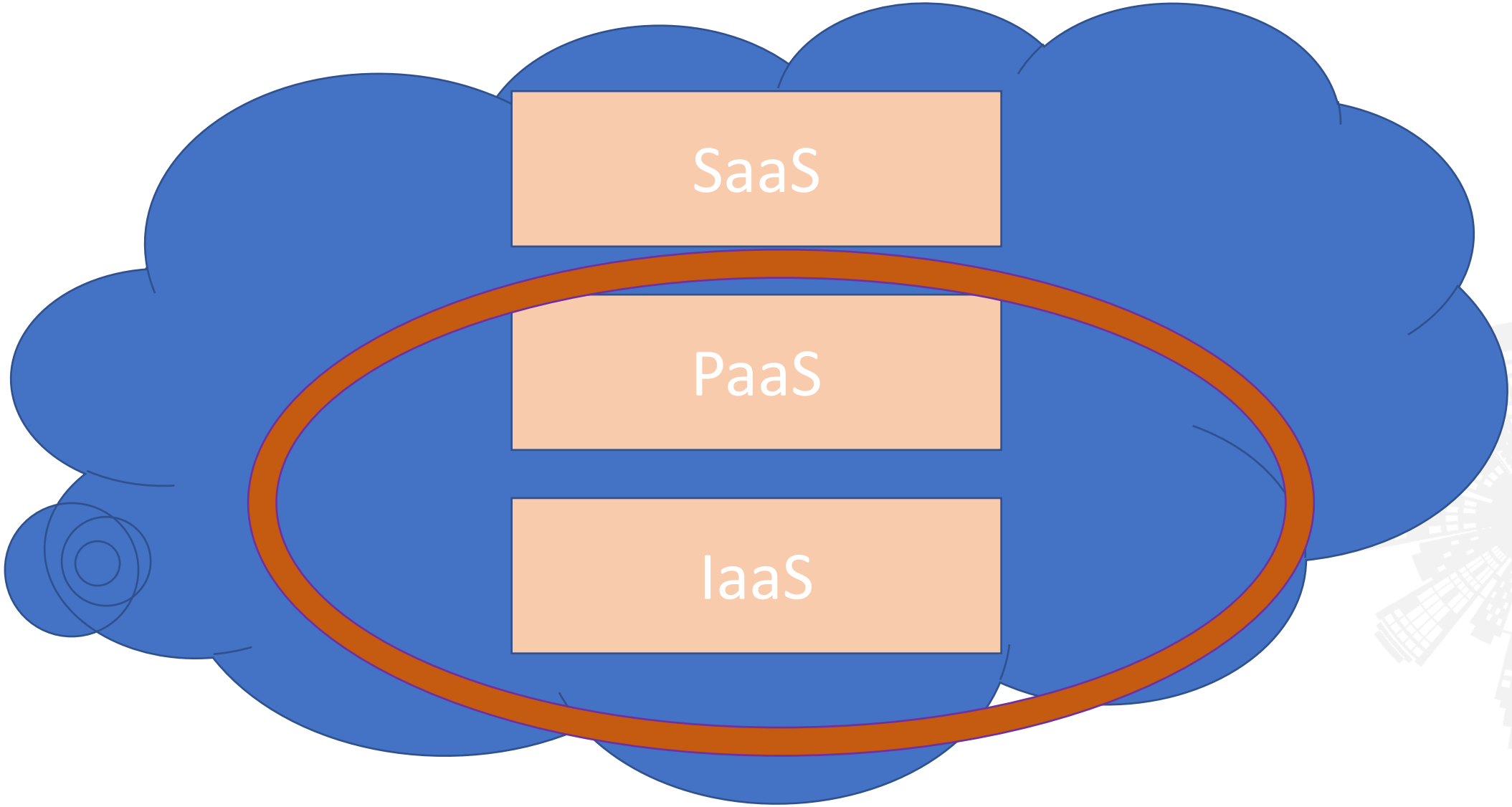
How to correctly evaluate your provider



The Challenge: Private cloud still got the same attack vectors!



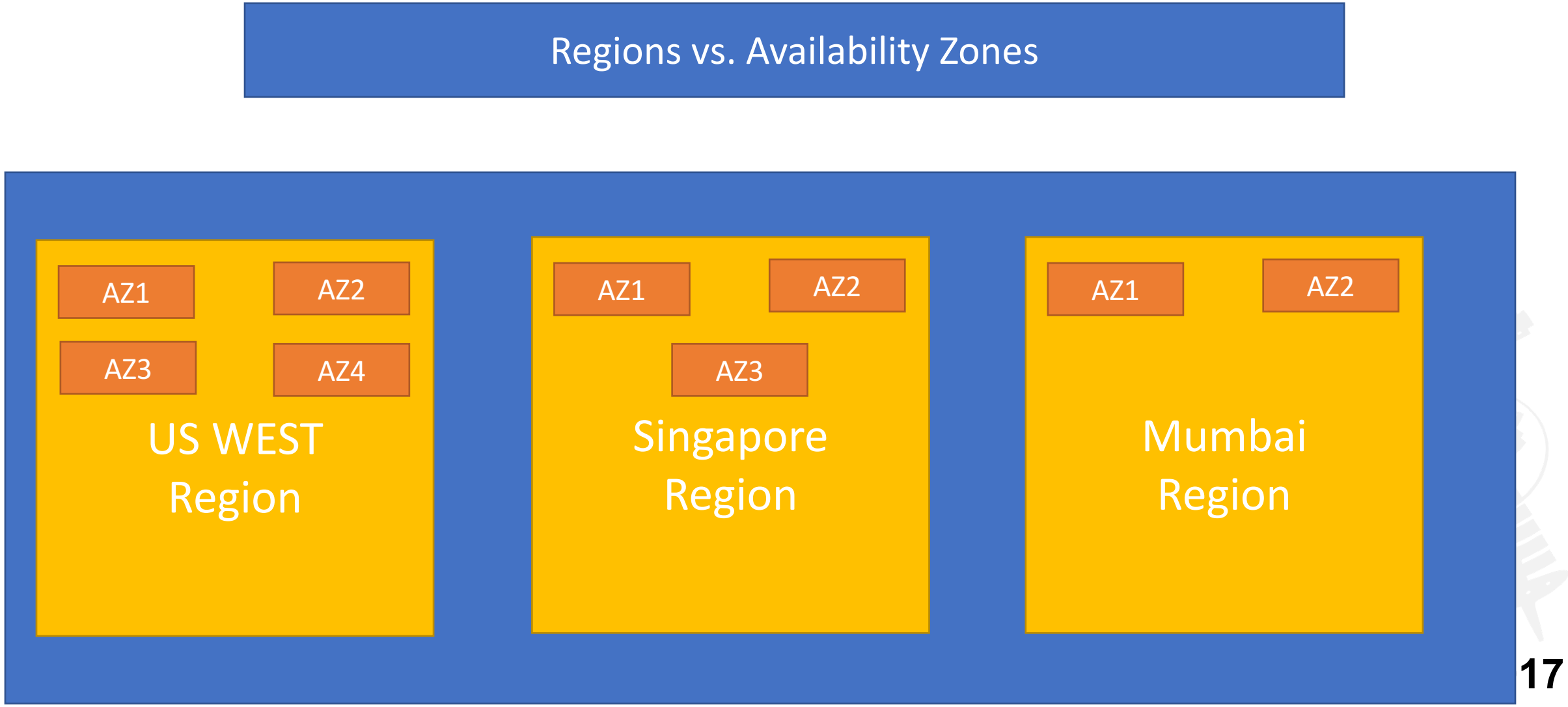
Our focus today



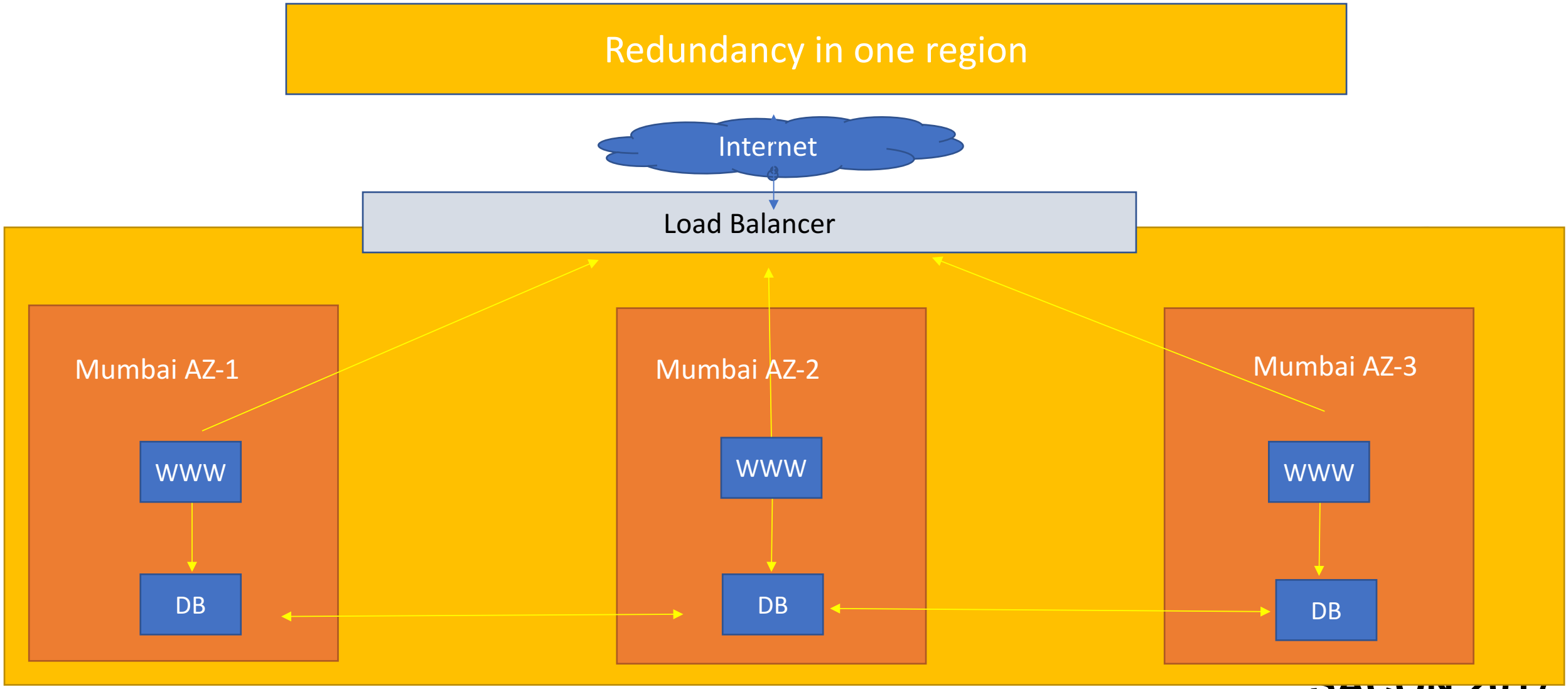
Terminology

AWS	IaaS	PaaS
Instance	Image	Snapshot
ELB	Root Account	IAM user

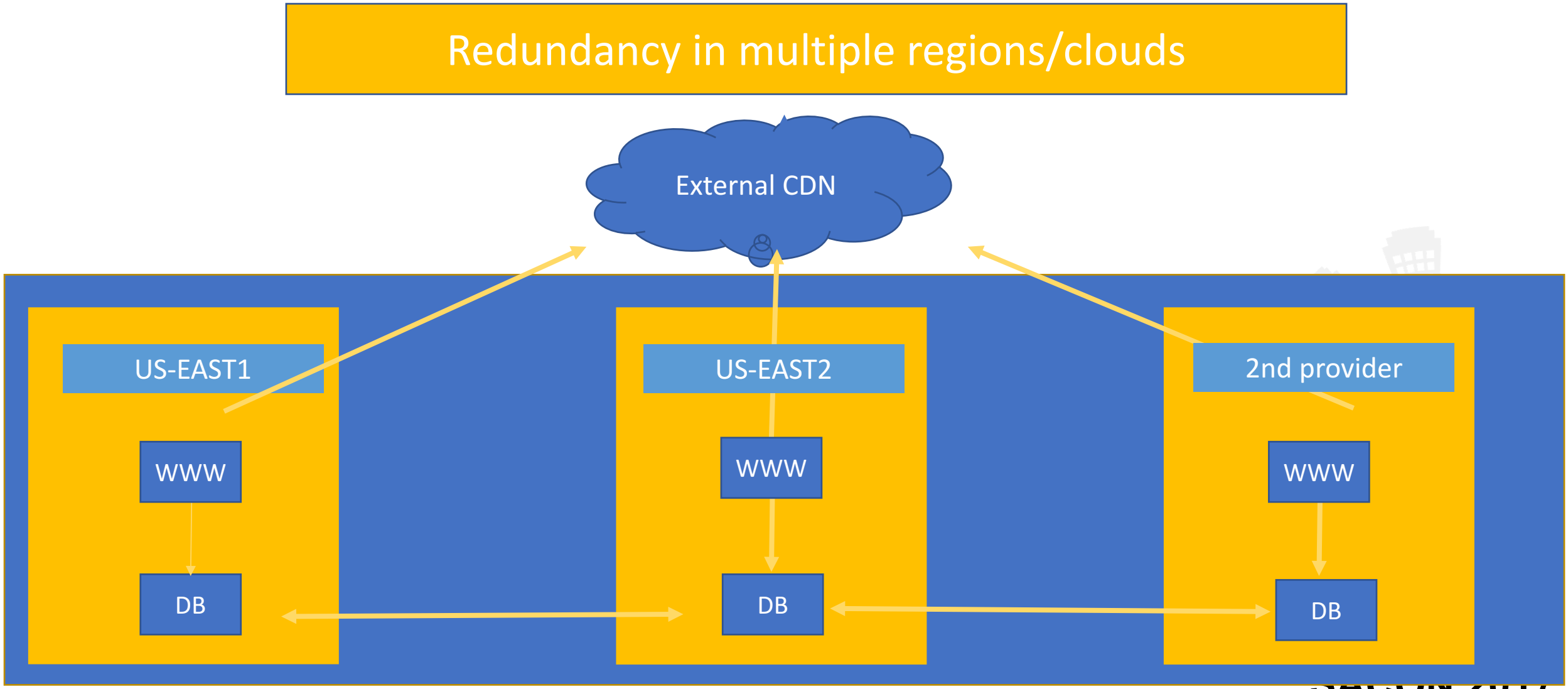
Architecting for availability



Architecting for availability

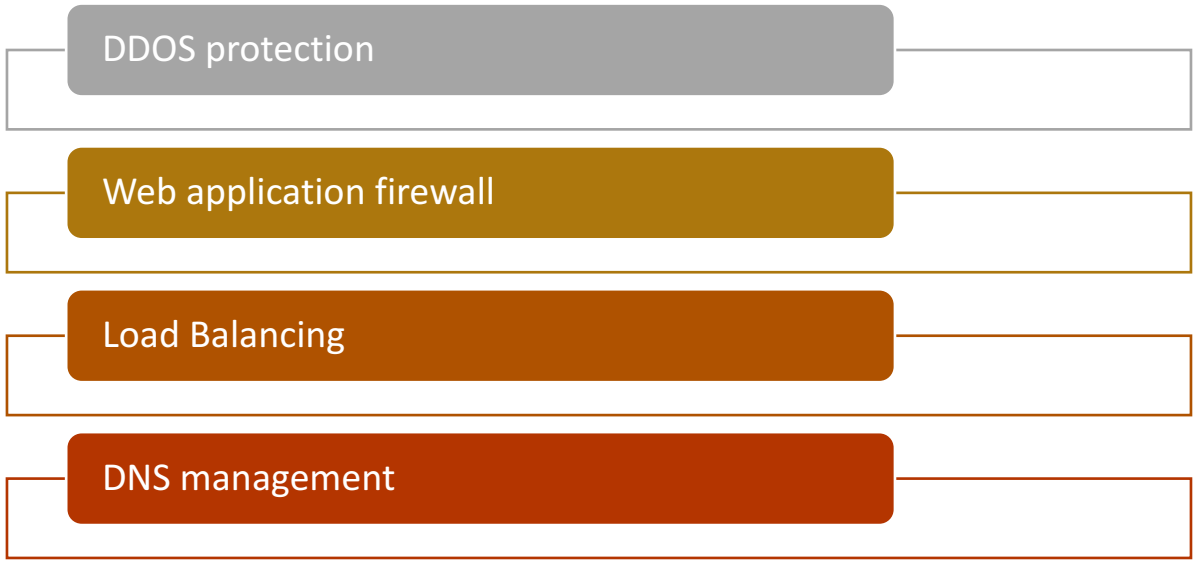


Architecting for availability



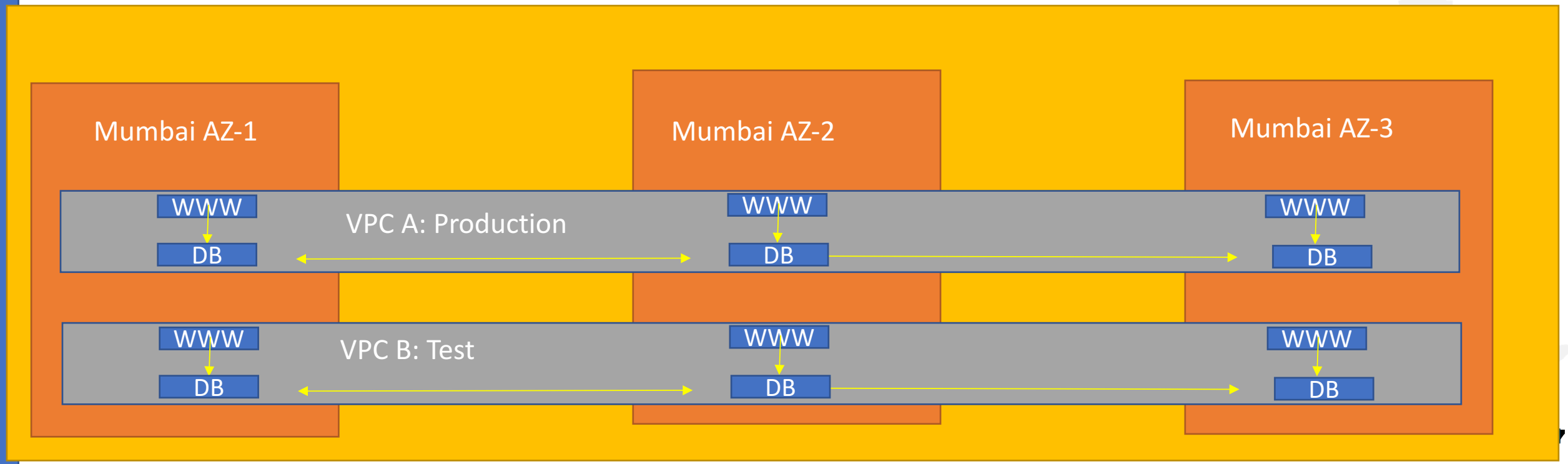
Architecting for availability

- CDN providers can add resiliency, flexibility & redundancy
- Look for vendors who can add functionality:



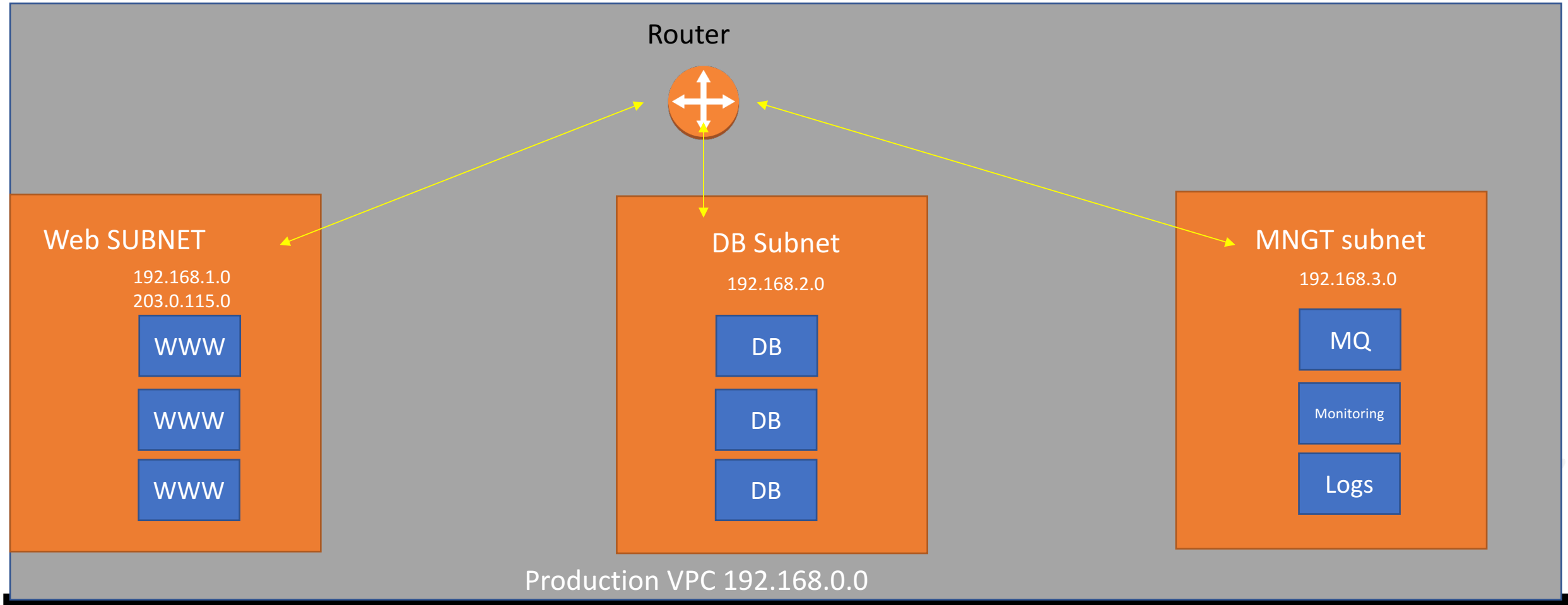
Architecting for network separation

Understanding VPC (Virtual Private Cloud) / Virtual Network



Architecting for network separation

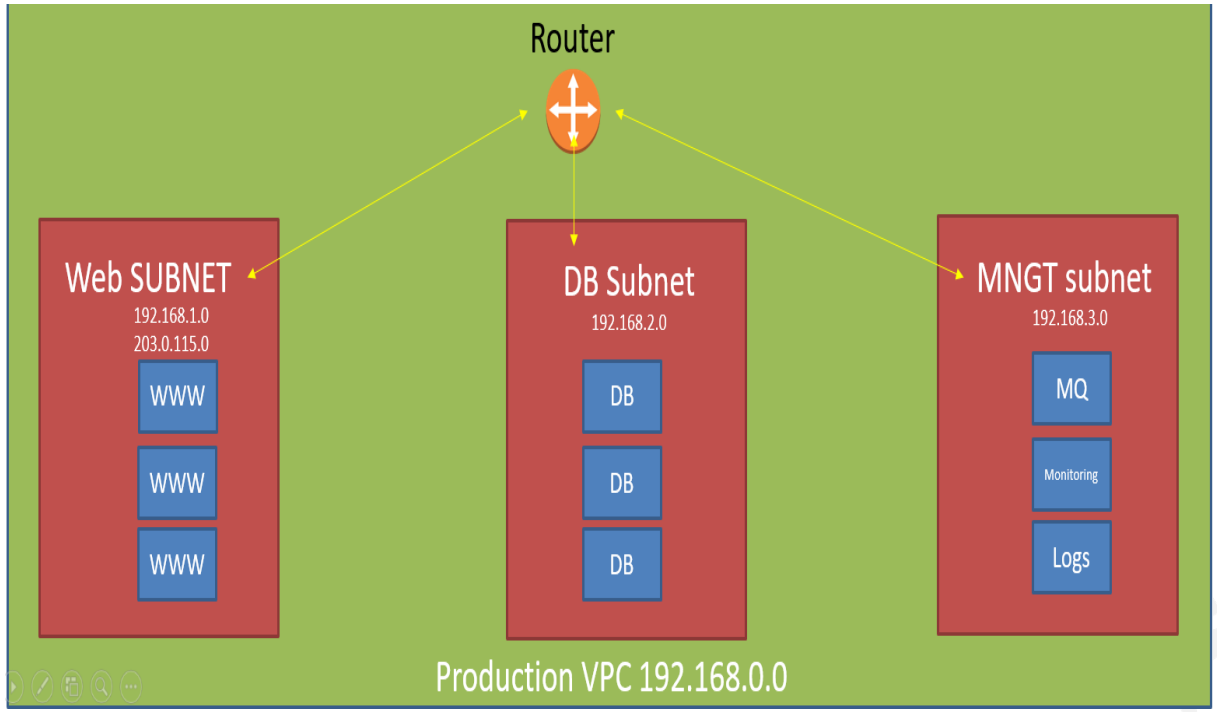
Understanding VPC (Virtual Private Cloud) / Virtual Network



Architecting for network separation

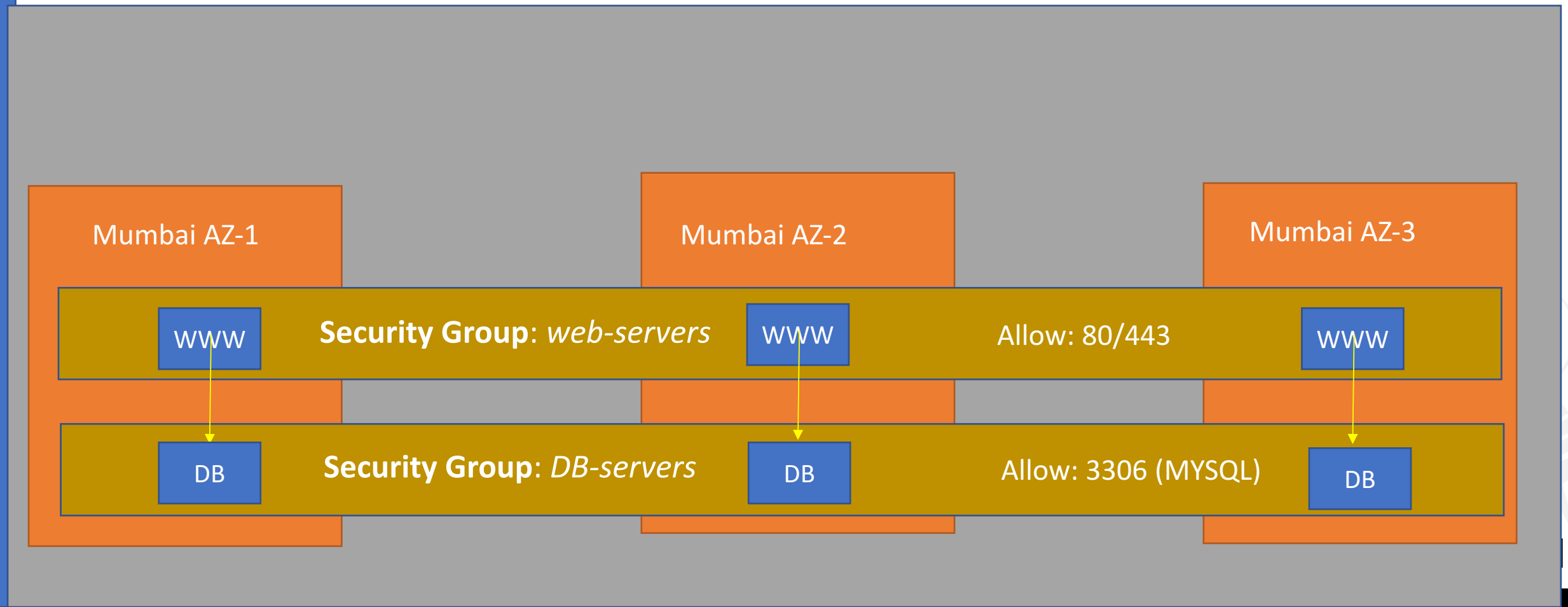
Understanding VPC (Virtual Private Cloud) / Virtual Network

VPC is logical grouping of subnets & instances, virtualizing physical data center features



Architecting for network separation

Understanding Security groups



Architecting for network separation

Additional VPC tools

NAT Gateway

Direct Connect

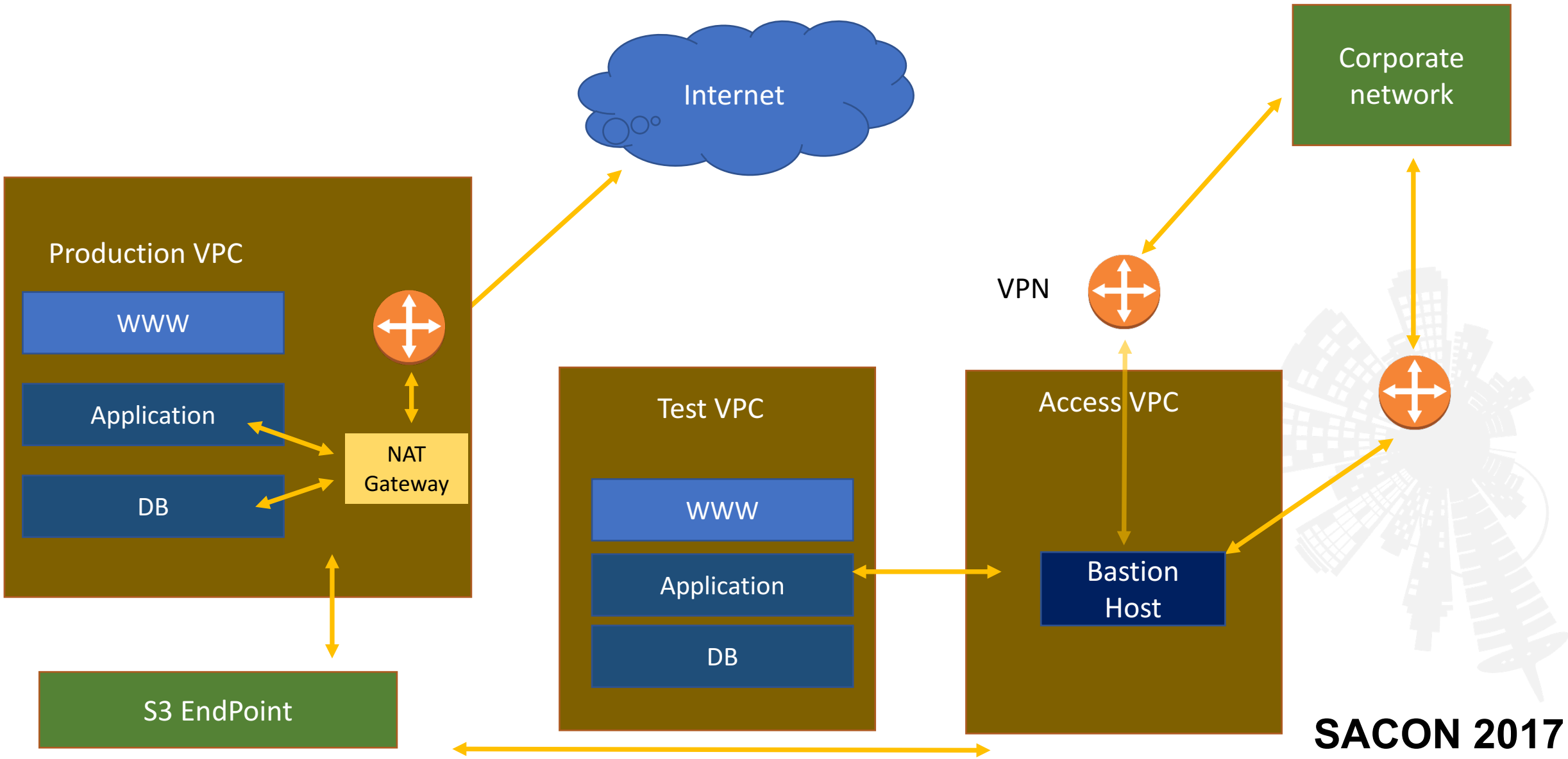
Bastion Host

VPN Gateway

Network ACLs

Flow logs

Architecting for network separation



Architecting for application separation

Web Application Firewall options

- 3rd party as a service
- Internal Provider service
- WAF Proxy inside cloud
- WAF client on web instances

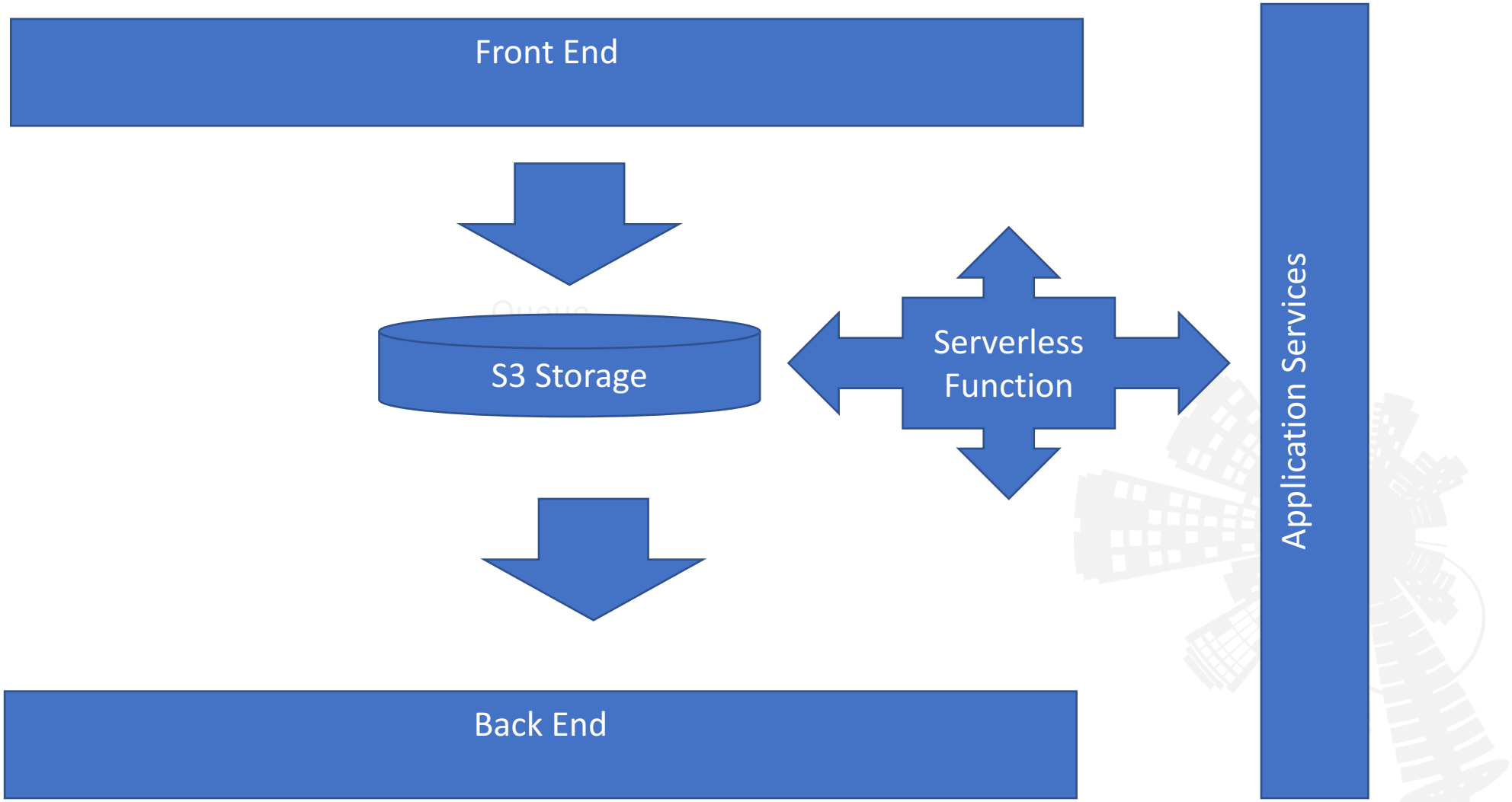
Architecting for application separation

Build application separation

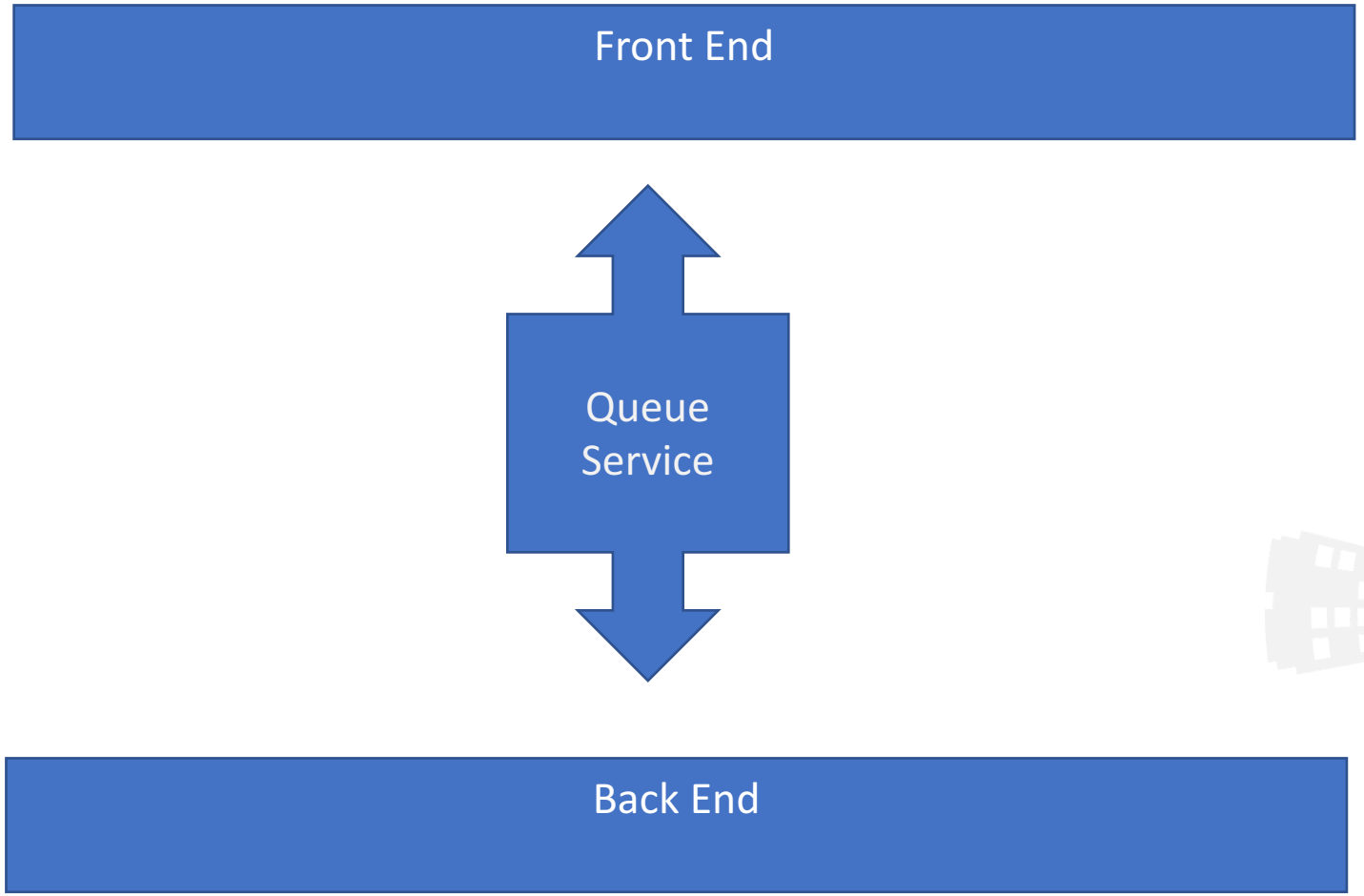
Utilize MQ services to separate application components

Use API Gateways & Serverless functions

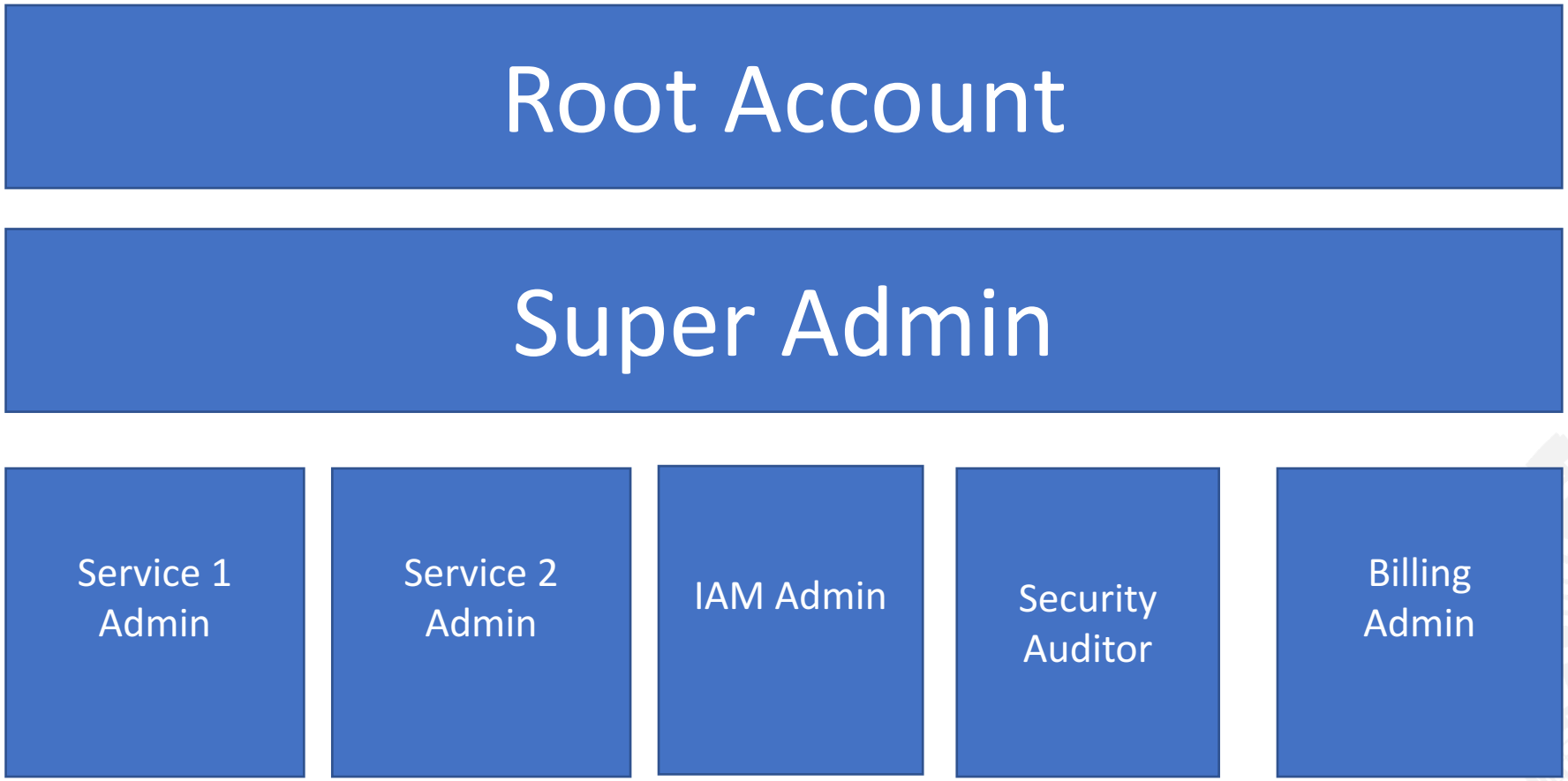
Architecting for application separation



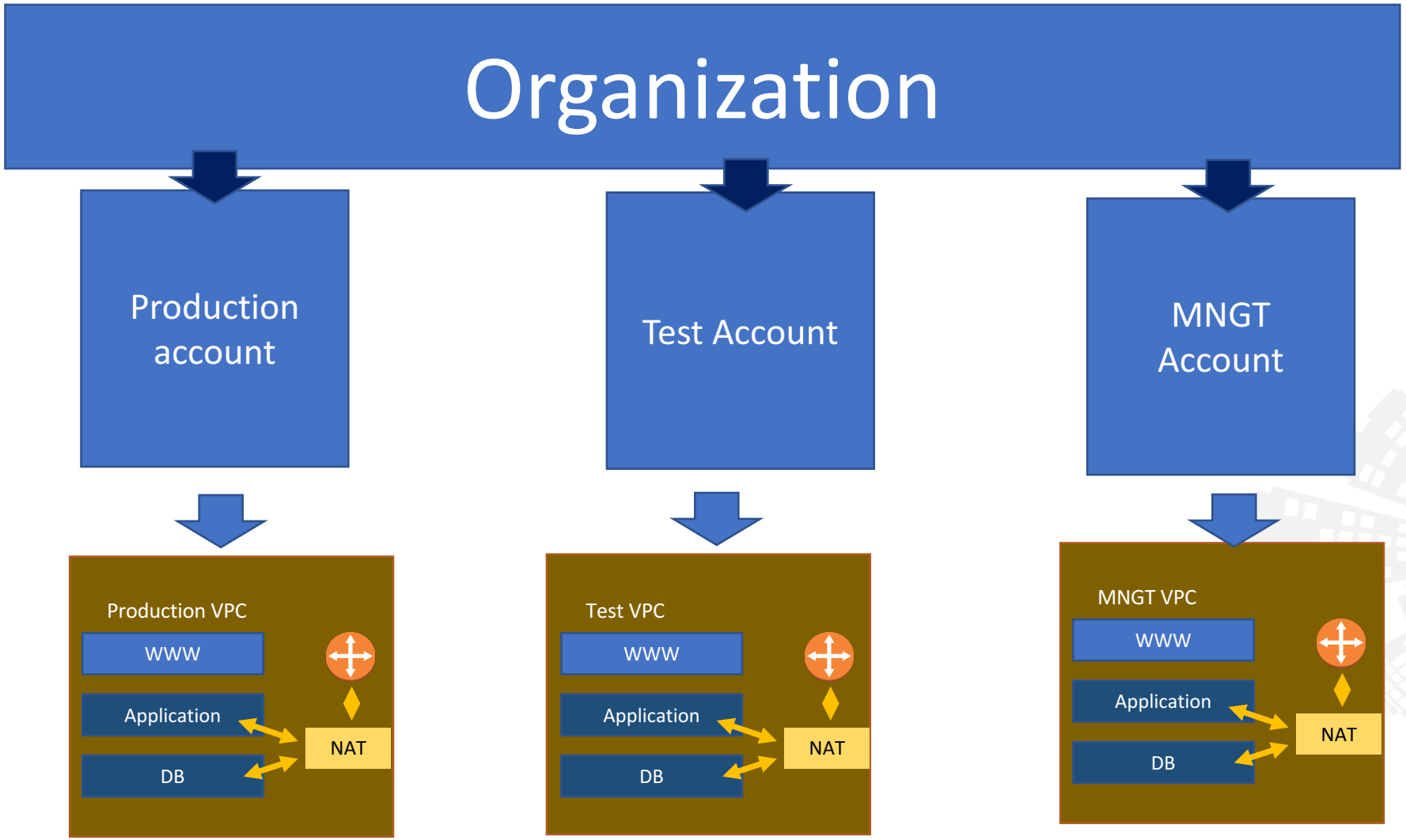
Architecting for application separation



Limiting blast Radius



Limiting blast Radius



Architecting for data security

Understanding storage options

Volume Storage

- Attached to a single instance
- Not shared, accessible only from the instance
- Useful in storing instance OS environment , application binaries , DB files and anything instances need to operate

Object Storage

- Provider managed
- Files are placed in buckets
- Versioning & meta data kept for all objects
- Files are accessible by API or HTTP
- Independent from AZ or instances dependencies
- Useful for storing static applications data, backups, source code and config files

Database service

- Provider managed
- Files are accessible by DB API
- Vary between different services: (structured, unstructured and more)
- Usually customer has no access to underlying DB infrastructure

CDN

- Cloud provider proprietary service or external 3rd party services
- Provide flexibility and resiliency
- Useful in serving static content at late latency
- Usually accompanied by additional services: WAF, DDOS protection, Load balancer…

Architecting for data security

Volume storage

Backups

- Usually snapshots
- Customer responsibility to keep snapshots inaccessible
- Don’t keep application secrets on disk

Redundancy

- Not redundant
- Access is made by a service on the instance OS (web service I.e)
- If service fails, no access

Encryption

- Storage encryption with provider service (i.e. AWS KMS, Azure keyvault)
- Or OS Level encryption software (i.e. truecrypt, bitlocker)

Architecting for data security

Object storage

Backups

- Keeps versioning system of files
- External backups are recommended (explore provider services)

Redundancy

- Availability is responsibility of the provider
- Increased availability can be achieved by replicating to other regions

Encryption

- Service side: Storage encryption with provider service (i.e. AWS KMS, Azure key vault)
- Or Client side using provider SDK

Architecting for data security

Database Storage (Database as a service)

Backups

- Automated backups are made by provider
- External exports and backups should be made periodically, just as any other database

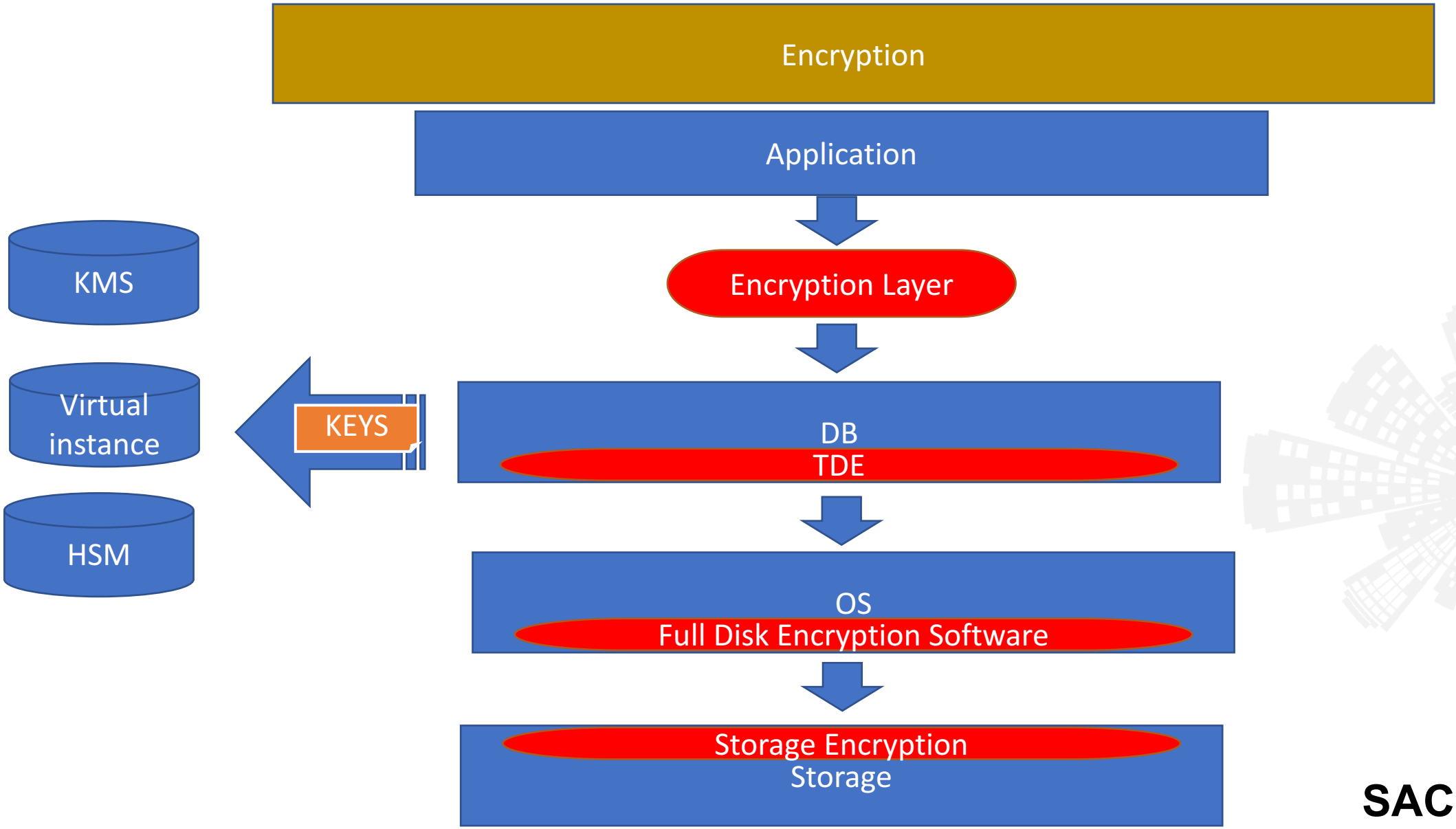
Redundancy

- Availability is responsibility of the provider but managed by customer
- Architect multiple AZ

Encryption

- Service side: Storage encryption with provider service usually at the database level
- TDE can be used here as well to encrypt at table/ column level

Architecting for data security



Questions?

KEEP IN TOUCH

ONLINECLOUDSEC.COM

Moshe Ferber

Moshe (at) onlinecloudsec.com

www.onlinecloudsec.com

@FerberMoshe

http://il.linkedin.com/in/MosheFerber

Cloud Security Course Schedule can be find at:

http://www.onlinecloudsec.com/course-schedule