Cloud Security

Chengyu Song

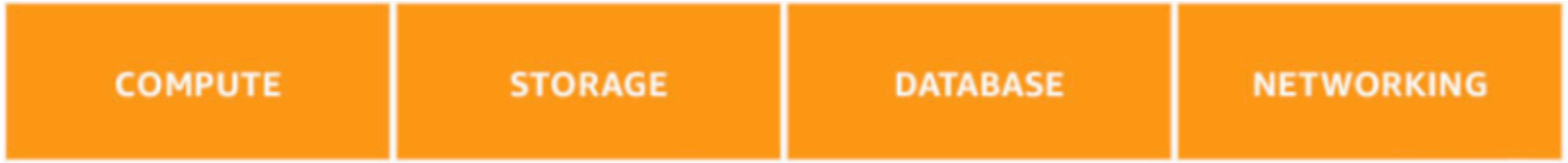
some materials are from AWS Security Whitepaper

Cloud

- What is cloud?

Cloud Computing

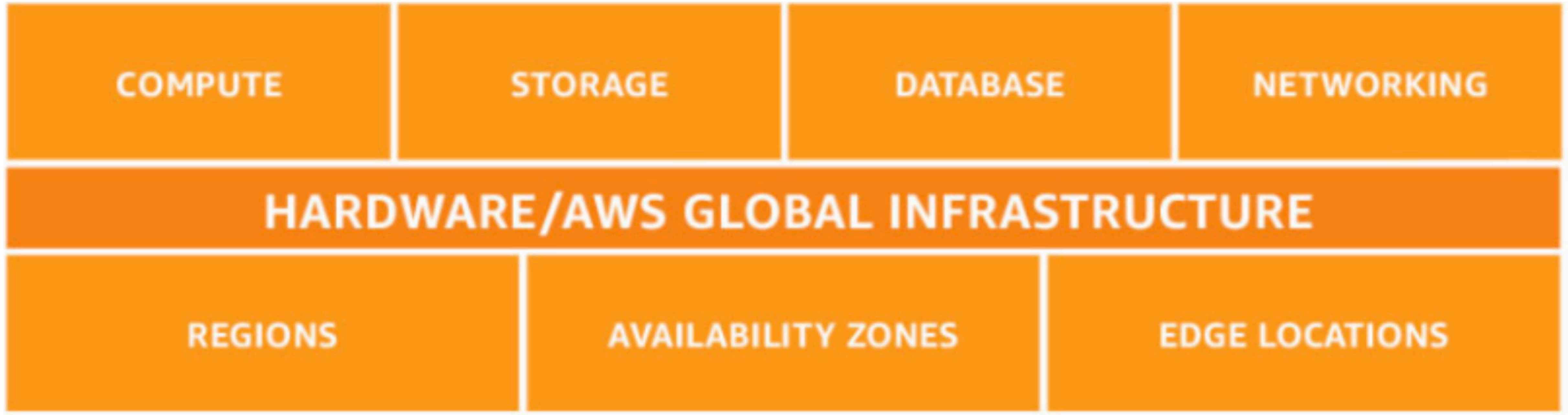
- What’s provide by the cloud?



COMPUTE STORAGE DATABASE NETWORKING

Cloud Computing

- What’s provide by the cloud?



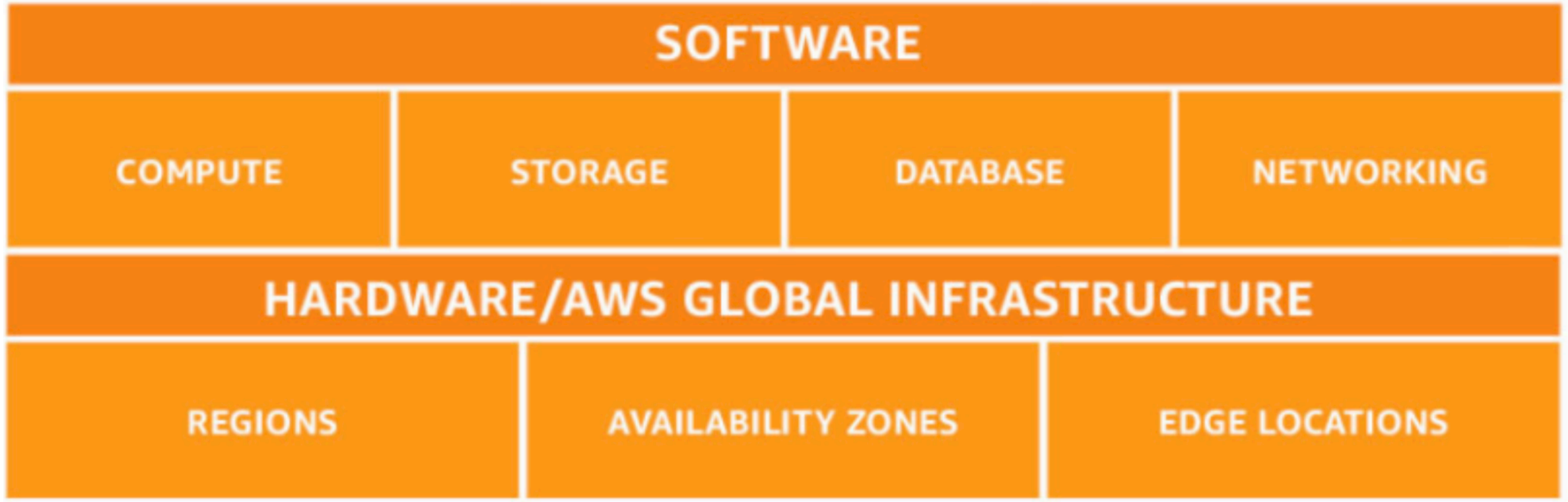
COMPUTE | STORAGE | DATABASE | NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS | AVAILABILITY ZONES | EDGE LOCATIONS

Cloud Computing

- What’s provide by the cloud?



SOFTWARE

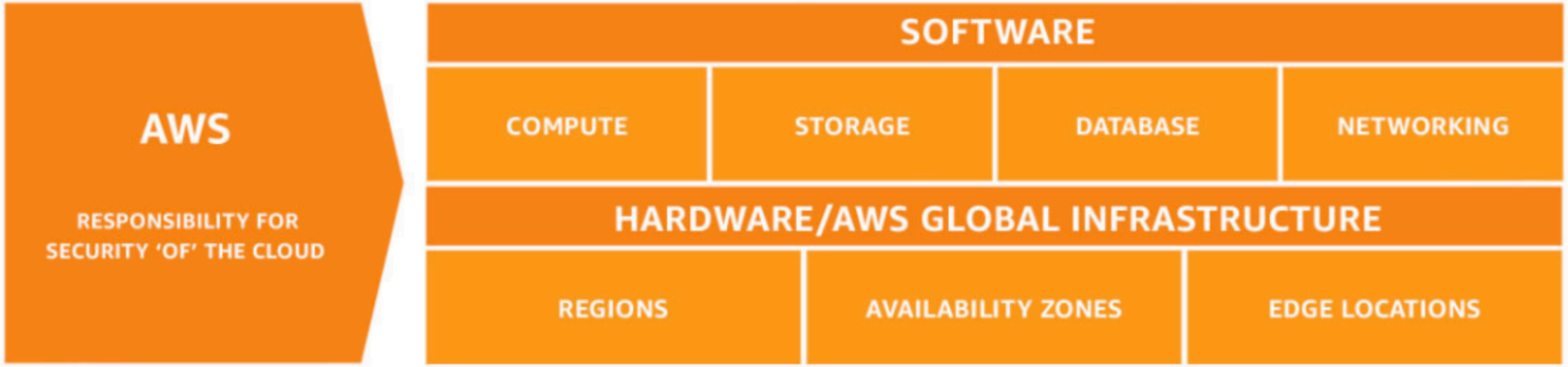
COMPUTE | STORAGE | DATABASE | NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS | AVAILABILITY ZONES | EDGE LOCATIONS

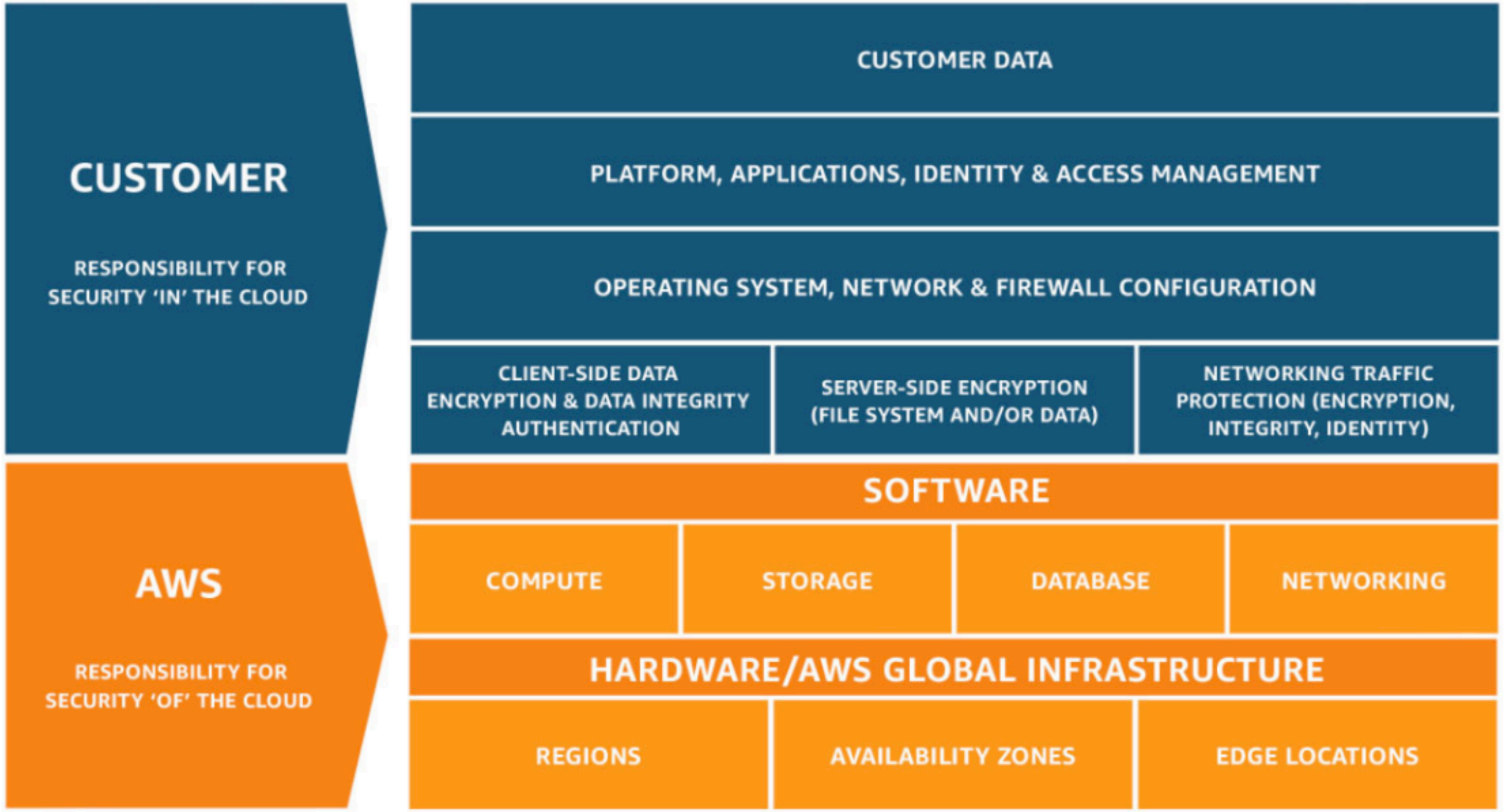
Cloud Security

- What security guarantees are provided by the cloud?



Cloud Security

- What security guarantees are **NOT** provided by the cloud?



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

What are the differences?

- Compared to on-premise infrastructure, what are the advantages and disadvantages of cloud, in terms of
  - Confidentiality
  - Integrity
  - Availability

Confidentiality

- What are the ways to guarantee confidentiality?
    - Access control (who can read)
        - Infrastructure
        - Identity (authentication)
    - Encryption
        - Key management

Integrity

- How to guarantee integrity?
    - Access control (who can write)
    - Message Authentication Code (MAC)
    - Logging and Audit

Availability

- Availability? What can go wrong?
  - DDoS, infrastructure maintenance error, power outage, storage, etc.
- How to mitigate these risks?
  - Multi-cloud, multi-region, hybrid cloud

Resources

- https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/introduction-aws-security.pdf

- https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

-

Management

- Inventory and configuration management