Cloud Security

C5 Forum Hawaii 2022

Sudhakar Gummadi

About HMSA

- Most experienced health plan in the state, covering more than half of Hawaii's population
- Working with employers, partners, and providers, HMSA promotes wellness; develops reliable, affordable health plans; and supports members with clear, thoughtful guidance
- Headquartered on Oahu with centers statewide to serve members
- HMSA is an independent licensee of the Blue Cross and Blue Shield Association

About Me

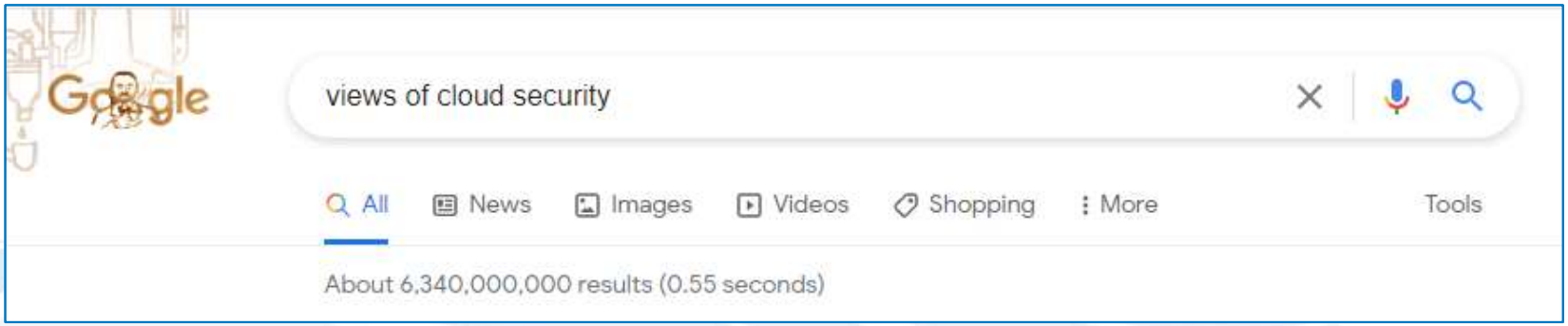
- Current role: **CISO/Privacy Officer, HMSA**
- Prior role: **Executive Advisor, Anthem Inc**
- Previously: **VP/CISO, Molina Healthcare Inc**

Cloud Security- A Split Responsibility

- Cloud Security Deployments- Public, Private and Hybrid Clouds
- Cloud Service Models- IaaS, PaaS and SaaS

- *"A shared responsibility model is a cloud security framework that dictates the security obligations of a cloud computing provider and its users to ensure* ***Accountability****"*

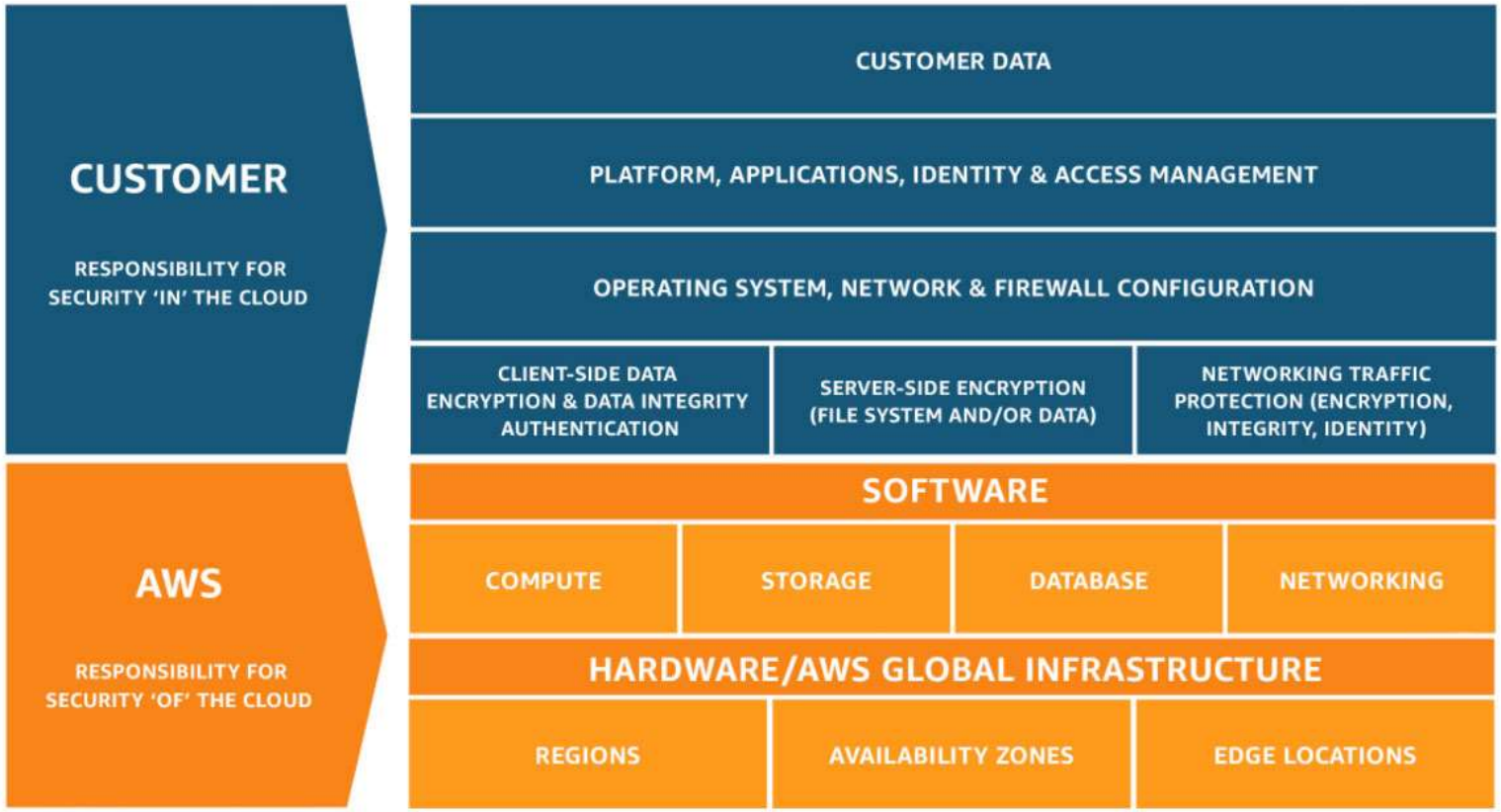
Cloud Security by Billions



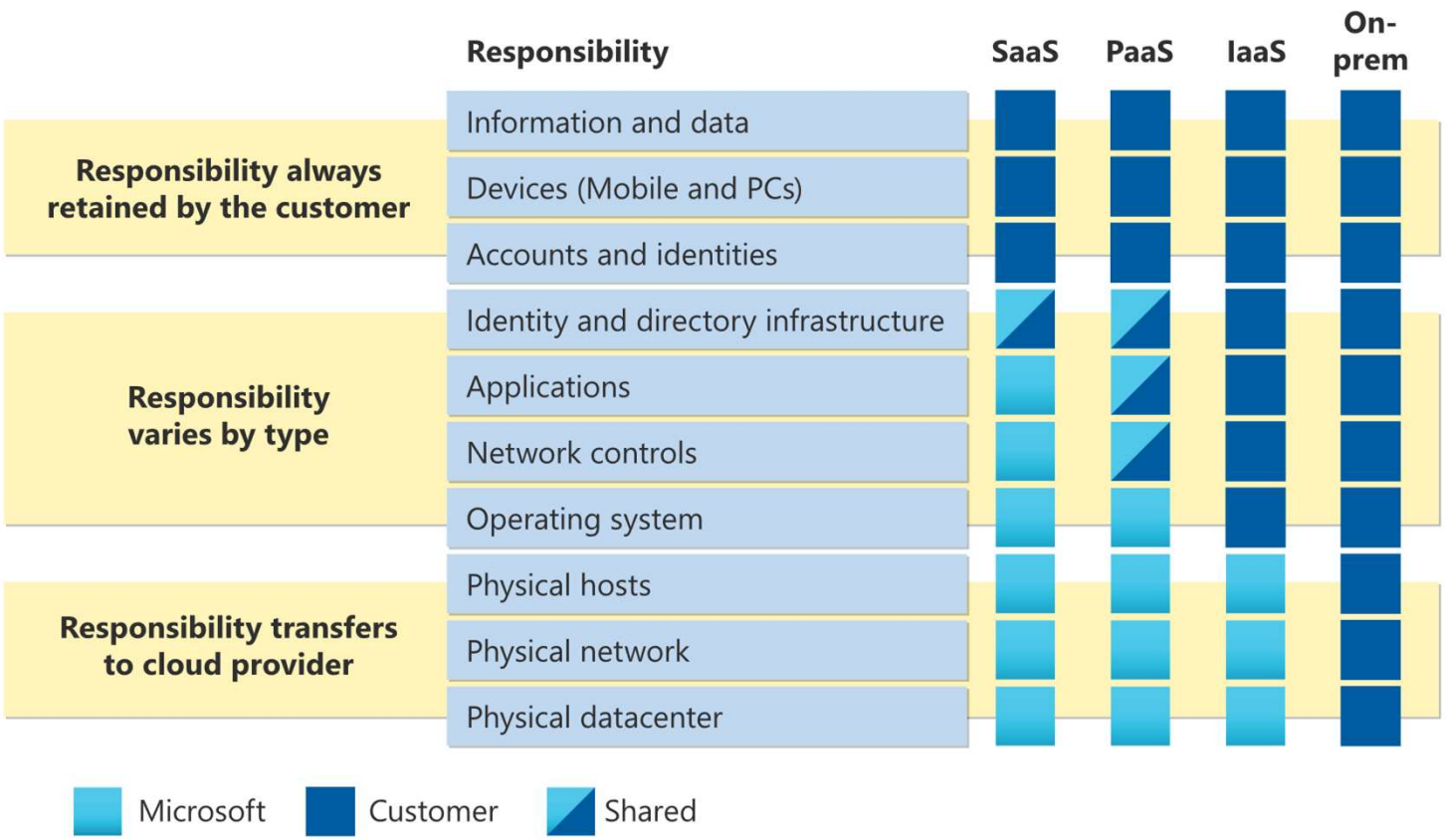
- Billions of perspectives are out there for cloud security
- Focus of this talk is back to security basics: **Accountability**
- Cloud Service Provider- *" Security of the Cloud"*
- Cloud User- Customer – *" Security in the Cloud"*

AWS Cloud

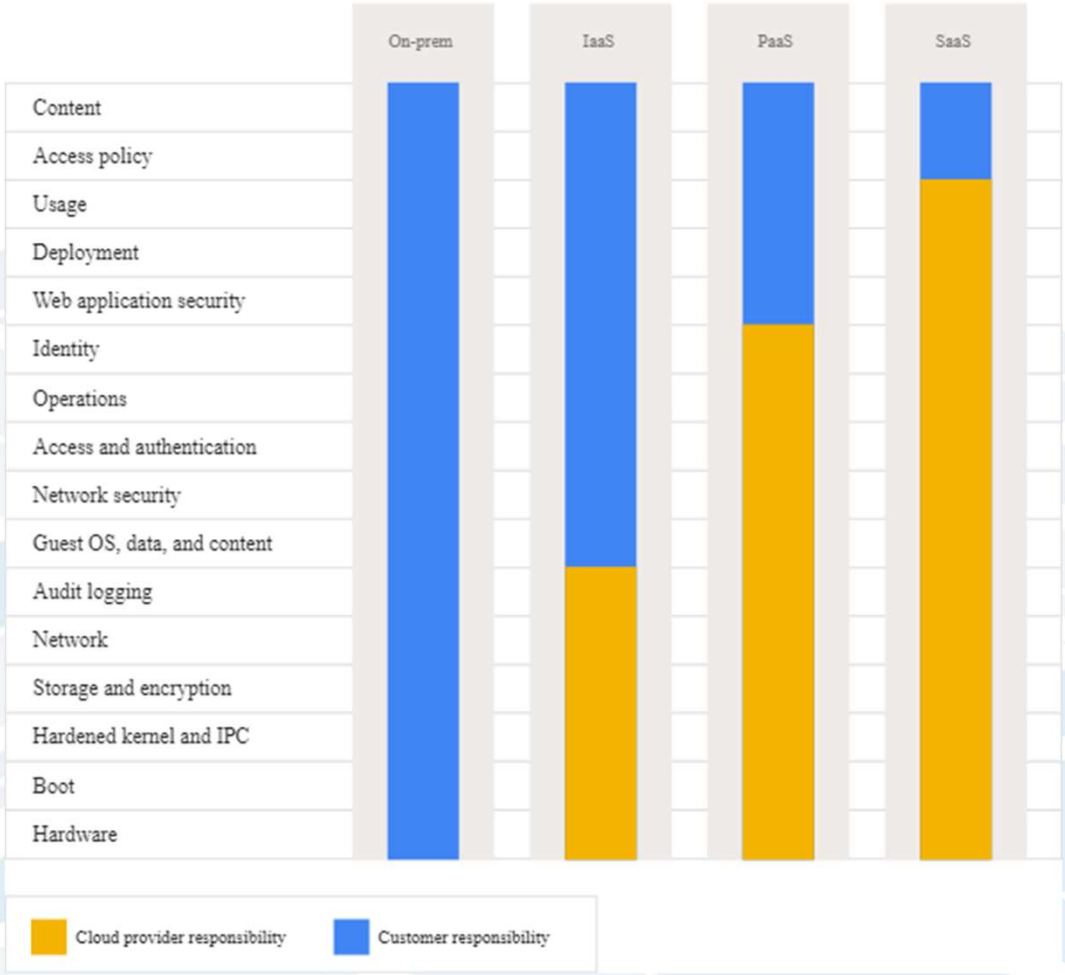
Security of the Cloud vs. Security in the Cloud



Azure Cloud


Responsibility
SaaS
PaaS
IaaS
On-prem
Responsibility always retained by the customer
Information and data
Devices (Mobile and PCs)
Accounts and identities
Responsibility varies by type
Identity and directory infrastructure
Applications
Network controls
Operating system
Responsibility transfers to cloud provider
Physical hosts
Physical network
Physical datacenter
Microsoft
Customer
Shared

Google Cloud



Shared Responsibility

Cloud Provider

- Physical layer
- Virtualization
- Provider

Divided

- Native vs. third party
- Server-based vs. serverless computing
- Network controls
- Operating systems

Tenant

- Data
- Applications
- Credentials
- Configurations
- Outside connections

Accountability Within Client Organization

People	• Cloud learning and growth first • Business leaders fully aware of cloud risk • Stakeholders “all hands on deck”
Process	• With cloud mindset • Incident response, asset management, configuration management, patching, etc.
Tools	• In cloud way and cloud speed • Continuous testing and monitoring

Accountability Across Supply Chain

- No ambiguity: Clear RACI between client, cloud provider, and third party, especially for application and data

Set and measure SLA: Security maturity or risk

- Follow the data: Deep dive on security operations and engineering
- "Trust but verify": Third-party assessment of controls
- Embrace DevSecOps.
- Identify a trusted cybersecurity partner

Q&A

Sudhakar_Gummadi@hmsa.com