

العطاء الرقمي
Attaa Digital



Cloud Security



Dalal Alharthi

Twitter: [DalalHarthi](https://twitter.com/DalalHarthi)

Introduction

In this talk, I will talk about cloud and containers security in organization. I will be addressing the following questions:

- Why do organizations migrate to cloud?
- How to ensure the security of our cloud environment?
- How to ensure the security of our containers?
- Why shift-lefting?
- What are the important documentations that I need to develop?
- On a personal level, how to ensure the security of our data in the cloud?

Cloud Providers



Why Cloud Computing?

Pay as you go

Easy maintenance

Availability

Automation

Large network access

Scalability

On-demand self services

Security

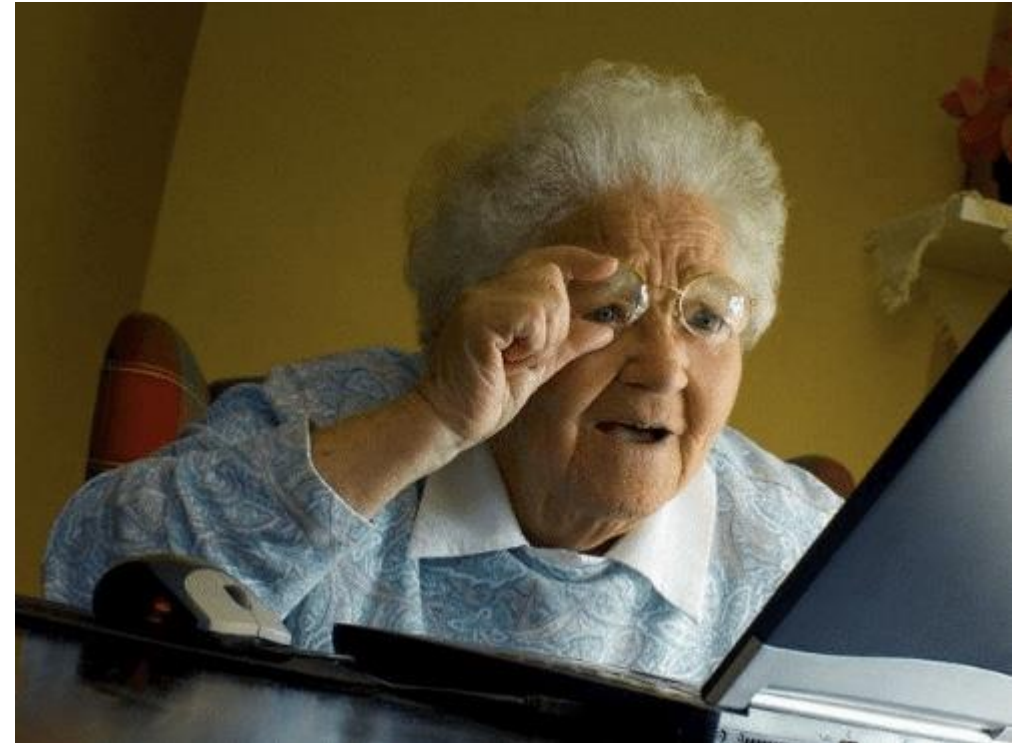
Shared
Responsibility
Model

What is the Shared Responsibility Model?

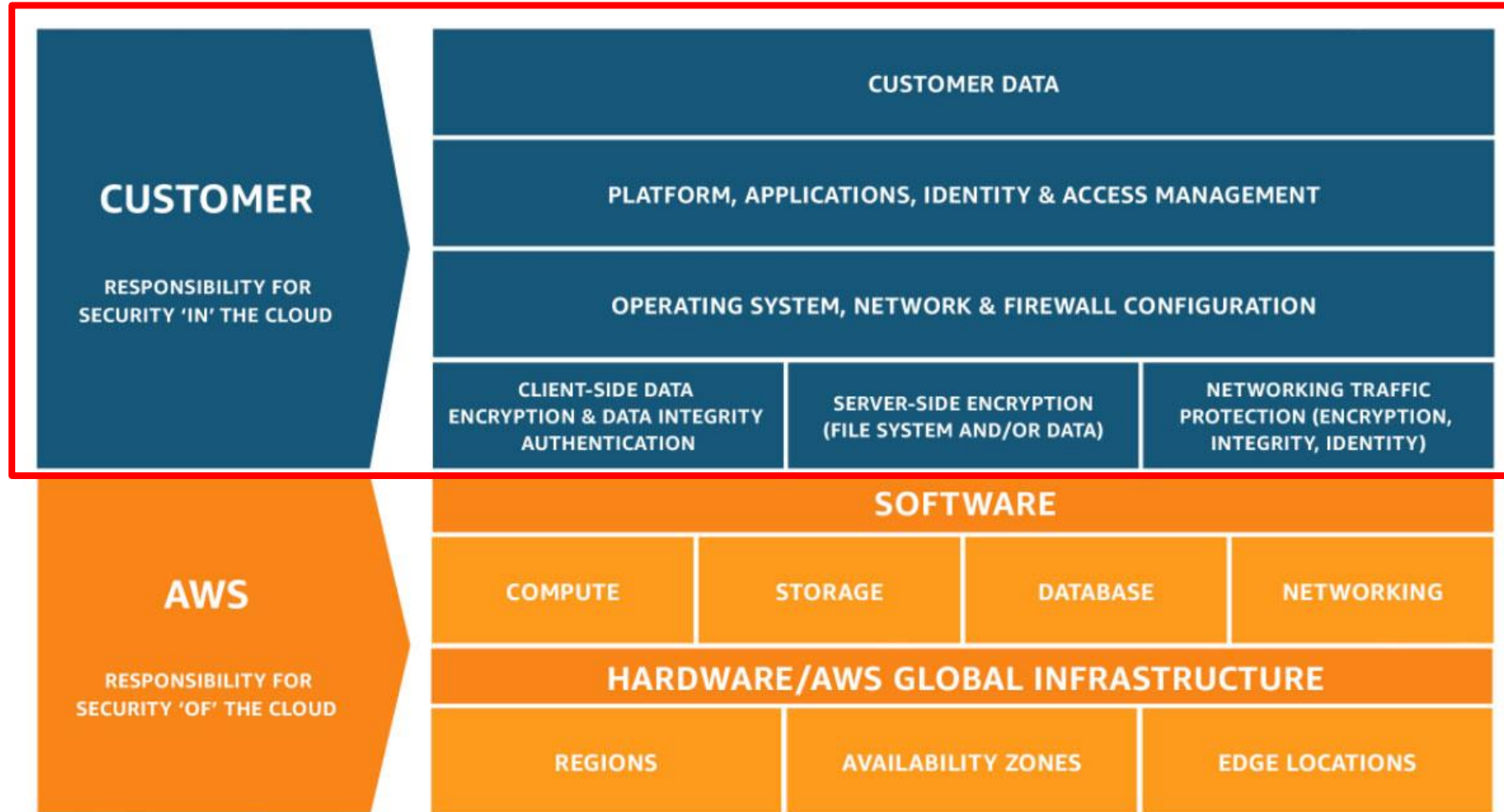
Your grandma was reading about this 'cloud' thing!

She read something about 'shared responsibility model' and asked you about it!

How do you explain it?

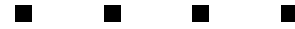


Shared Responsibility Model in the Cloud



HOW?!

Cloud Security Tools



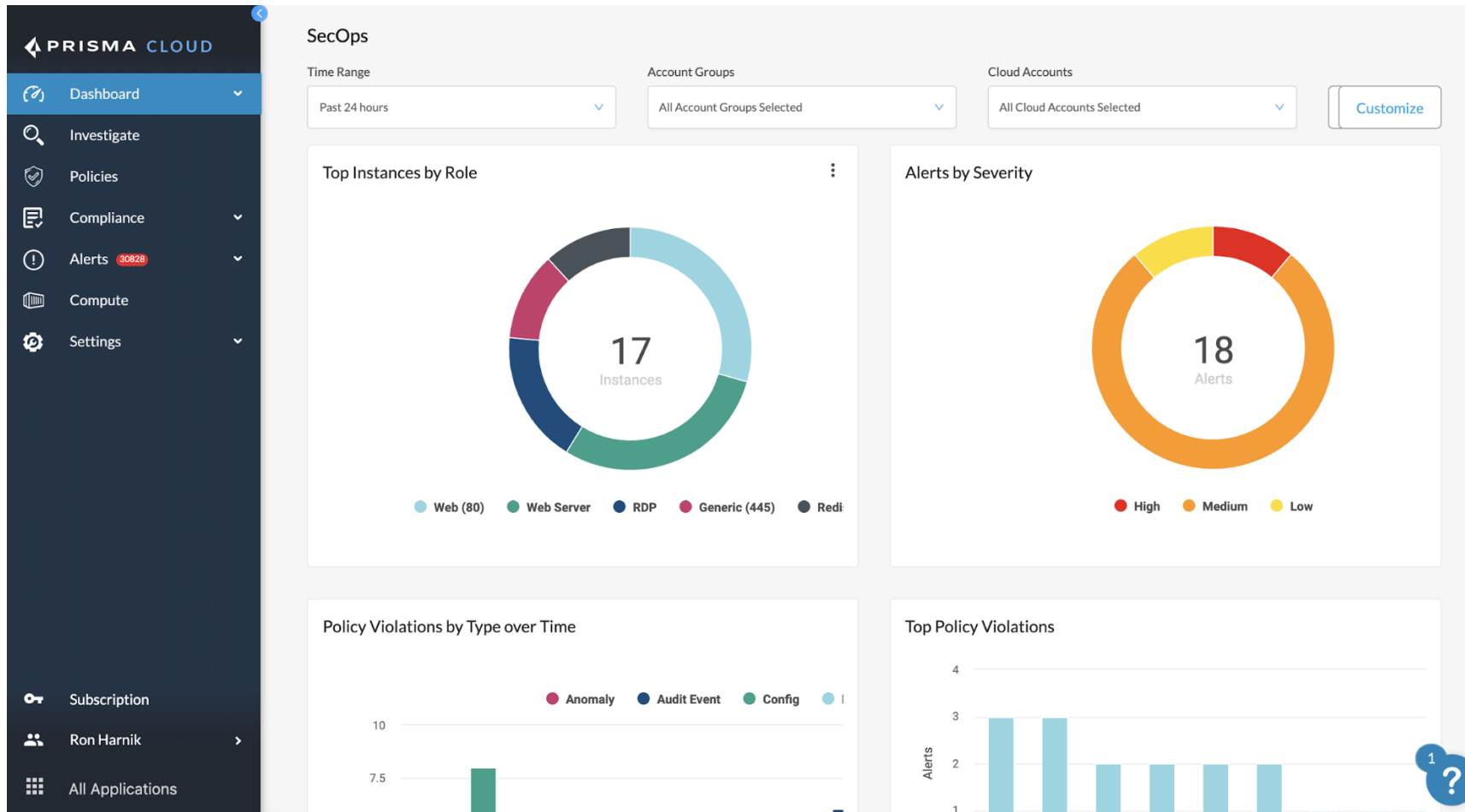
Prisma Cloud – Cloud Compliance Tool

- All security standard policies are predefined.
- You can define your own customized policies.
- Read permission? Read/Write permission?
- Alerts?
- Reports?
- RQL?
- Compute tap?
- Scan/Remediate vulnerabilities in each container.
- Compliance status?

RedLock

 **Twistlock**

Prisma Cloud – Cloud Compliance Tool



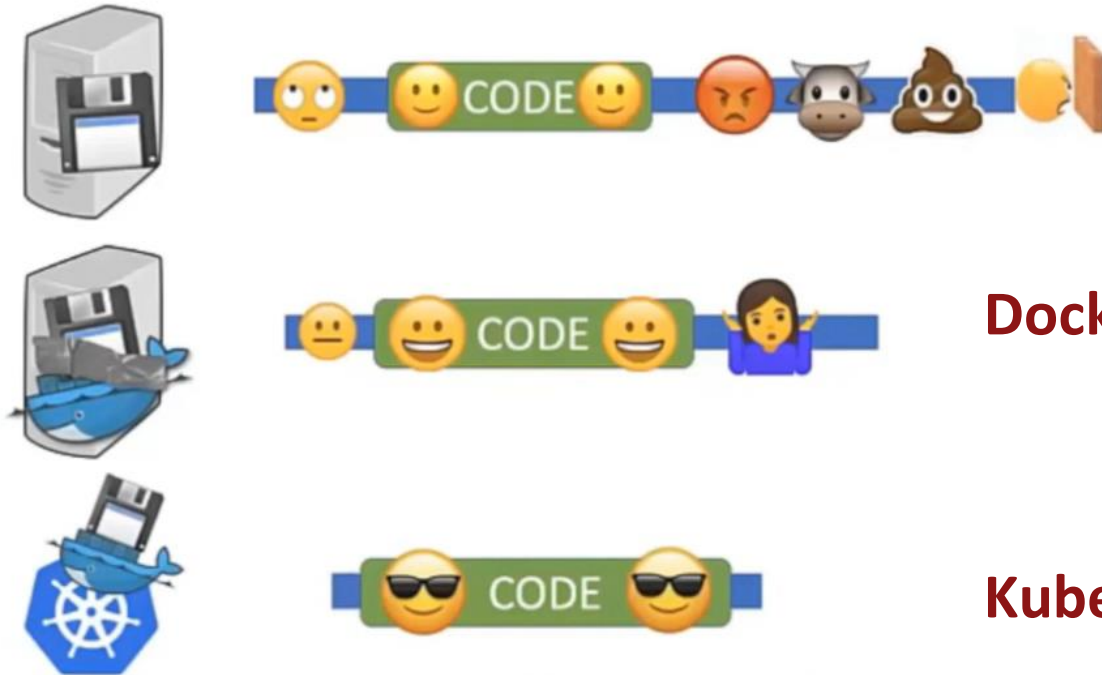


Containers

- Why do software developers always say, '**it works on my machine**'?
- This is not an issue anymore with containers.. i.e., Docker. We put the code as it is in that container.
- When we containerize it, it's portable. But it's microservices!



Why do Devs and Ops people like k8s?



Docker → portable microservices

Kubernetes → communication part 😊

Prisma Cloud – Containers Security

The screenshot displays the Prisma Cloud interface for container security. The main area shows a network diagram of namespaces within the 'twistlock' namespace. The namespaces are interconnected and color-coded by vulnerability status: red for high severity and green for low severity. The namespaces shown are:

- catalogue-db:0.3.0 (catalogue-db)
- catalogue:0.3.5 (catalogue)
- front-end:0.3.12 (front-end)
- mongo:latest (orders-db)
- mongo:latest (orders-db)
- cars:0.4.8 (cars)
- user:0.4.7 (user)
- orders:0.4.7 (orders)
- shipping:0.4.8 (shipping)
- user-db:0.4.0 (user-db)
- payment:0.4.3 (payment)

The sidebar on the left contains navigation options: Radar, Defend (Firewalls, Runtime, Vulnerabilities, Compliance, Access), Monitor (Events, Runtime, Vulnerabilities, Compliance), and Manage. The bottom left shows 'About Enterprise 19.10.459' and a 'Containers' button.

The right sidebar provides a summary of security metrics:

- Deployed Defenders:** 4 Container Defenders, 0 Host Defenders, 0 Serverless Defenders, 0 RASP Defenders.
- Number of incidents:** A line graph showing incidents over the last week (Oct 28 to Oct 29).
- Impacted images:** Compliance and Vulnerabilities status.
- Impacted containers:** Compliance and Vulnerabilities status.
- Impacted hosts:** Compliance and Vulnerabilities status.
- Impacted functions:** Compliance and Vulnerabilities status.

A 'Refresh' button is located at the bottom right of the main diagram area.

Shift-Left

Shift-left to secure the entire app lifecycle.

Build

Images & Functions

Infrastructure-as-Code

Deploy

Registries and Repos

Infrastructure-as-Code

Run


VMs, containers, serverless

IaaS, PaaS, Network, Storage

Datacenter & Infrastructure



Benefits of Shift-Lefting

- 1) Insecure resources and apps don't get deployed in the first place.
 - 2) Saves round trip on security issue resolution between DevOps and security team.
- 



Important Documentations!

**Cloud
Security
Controls**




**Incident
Response
Runbook**





Document: Cloud Security Controls

- Developers need to know about security controls.
 - This document shall address security controls for your cloud environment.
 - Three main categories:
 1. Identity and Access Management (IAM)
 2. Data logging/monitoring
 3. Infrastructure
- 

Document: Incident Response Runbook

- Different scenarios...
 1. Unauthorized changes to network configuration or resources
 2. Credentials (access key ID and secret access key) that were mistakenly exposed publicly due to developer misconfiguration
 3. Sensitive content that was mistakenly made publicly-accessible by developer misconfiguration
 4. Isolation of a server that has malware
 5. Ransomware?

Document: Incident Response Runbook

- Different scenarios...
 1. Write those scenarios.
 2. Write your response to each one of them.
 3. Address the contact information for the incident response team.
 4. Who is going to keep track of all the changes made in an event of a security incident?
 5. Test your plan!
 6. Automate it!



Ok.. What does cloud security mean on a personal level?

- Strong/complicated password?
- Rotate it periodically.
- Use Secret Management tool.
- Enable MFA.
- Recovery code?
- Security questions?
- Ensure the accuracy of your profile information.
- Check your logged in devices 😊
- Backup?





Thank you...

Dalal Alharthi
Twitter [@DalalHarthi](https://twitter.com/DalalHarthi)

