Managing Cybersecurity in Public Cloud Environments

By

Vijayabharathi

About me

- Stared the journey as a Java developer before a decade.
- Running technical communities in various cities in Tamilnadu.
- Working in Infosys for last 7 years.
- Used to teach programming language to the students.
- Love travel, exploring new places, ethnography etc…
- Passionate about cybersecurity and ML
- Completed MTech in Cybersecurity
- Research areas are IoT, Blockchain security…!

Session Outline

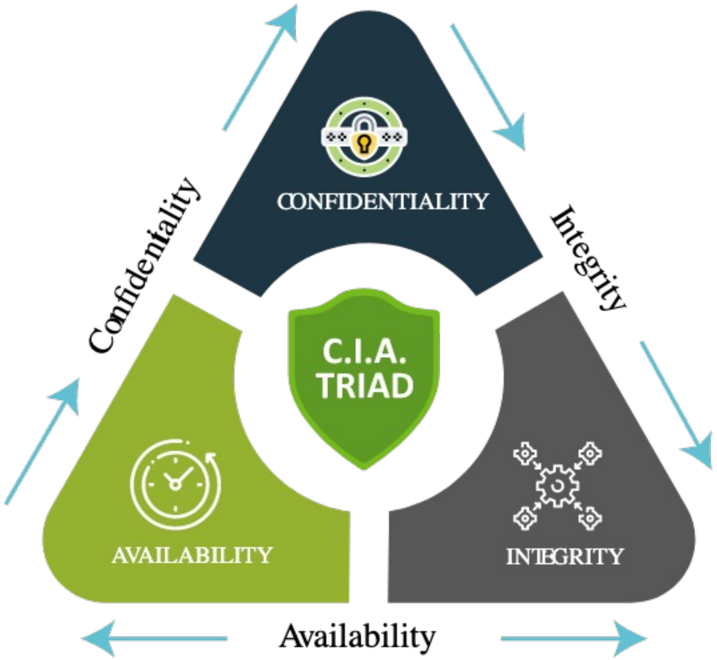
- Overview of Public Cloud Environments
- Deployment models and Shared Responsibility Model
- IAM
- Network Security
- Data Security
- Host Security
- Logging & monitoring
- Research areas

What is Cloud ?

- Infrastructure managed by service providers in a remote location
- Any type of resources can be provisioned in few clicks
- Cost effective, pay for use !
- Accessible anywhere, easy to manage…!
- Secure environment ?

What is (cyber)security ?

- To Secure or protect the Confidentiality, Integrity and availability of the data/resources in IT systems.



What is Deployment model?

IaaS

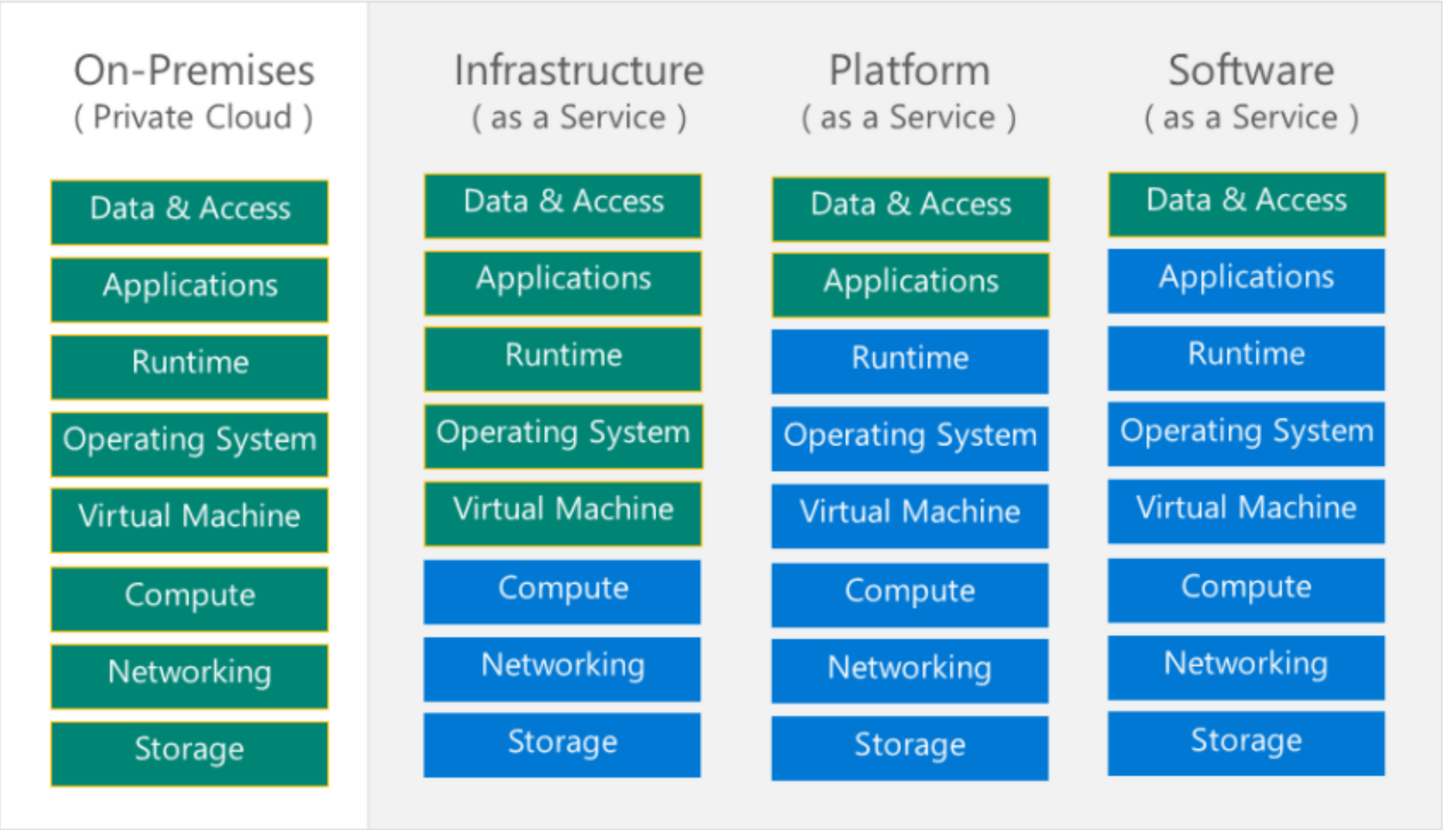
SUBIKSHA
Feels Homemade
SEMI COOKED CHAPATI
சப்பாத்தி
Made from Whole Wheat Atta, nutritious and rich source of protein and fibre.
Just Heat & Serve
NO Artificial Colors & Flavors

PaaS

SaaS

Which one is better ?

What is Shared responsibility model ?



On-Premises (Private Cloud)	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
🟩 Data & Access	🟩 Data & Access	🟩 Data & Access	🟩 Data & Access
🟩 Applications	🟩 Applications	🟩 Applications	🟦 Applications
🟩 Runtime	🟩 Runtime	🟦 Runtime	🟦 Runtime
🟩 Operating System	🟩 Operating System	🟦 Operating System	🟦 Operating System
🟩 Virtual Machine	🟩 Virtual Machine	🟦 Virtual Machine	🟦 Virtual Machine
🟩 Compute	🟦 Compute	🟦 Compute	🟦 Compute
🟩 Networking	🟦 Networking	🟦 Networking	🟦 Networking
🟩 Storage	🟦 Storage	🟦 Storage	🟦 Storage

🟩 You Manage

🟦 Cloud Provider Manages

Identity and Access Management (IAM)

- Authentication – Zero trust model
  - Multi factor authentication
  - Password less authentication
  - Bio-metric authentication
  - Password complexity & reset policies
- Authorization – principle of least privileges
  - Approval process, offboarding process
  - Periodic audit, JIT access
  - Dual admin with activity logging
  - Service/automation accounts as admin

Network Firewall & WAF

- Deny all traffic by default
- Approval process for whitelisting IP/URLs
- IDS and IPS systems
- Strict minimum allow rules

Network load balancing

- DDos protection is essential
- Primary and failover servers
- Containerized environments with auto scaling

Data Encryption

- Data should be encrypted in Rest and Transit
- We can use either symmetric or asymmetric encryption
- Should have to use the approved encryption algorithms
- Hashing and tokenization techniques are to be used during transit.
- Data logs should be audited via SIEM.
- Public access to storage should be denied.
- Data masking techniques

Replication & Data loss protection

- Enable backups in secondary region
- OS hardening
- Asset management
- Security posture score
- Vulnerability management process

Secret management

- Secrets & certificates are managed securely in the cloud
- CSP Managed keys or customer managed keys both can be used
- Key rotation is important
- Key exchange algorithms are to be followed
- Role based access control
- No one can delete the keys

Anti-Virus, VM, EDR and CSPM solutions

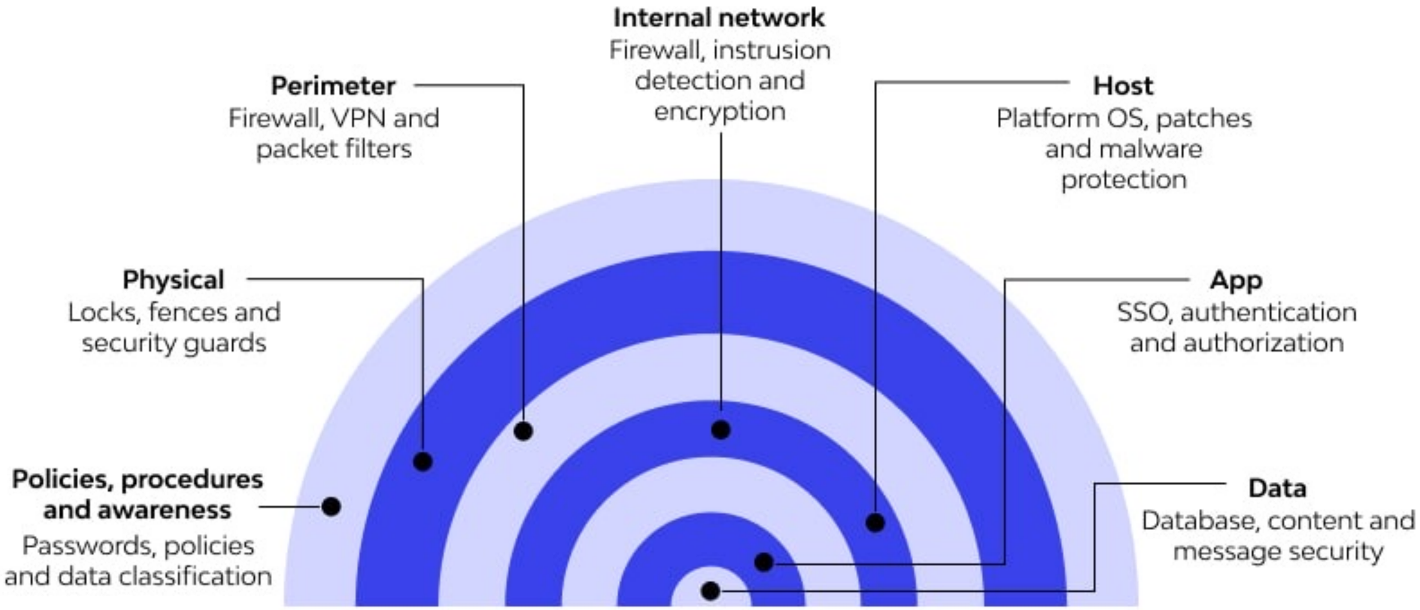
- More than one AV solution to protect the files stored
- Periodic scanning & Signature update
- Health monitoring of agents
- Automated patching schedules

Monitoring & Security Alerts in Cloud

- Analyzing the diagnostics and activities log
- Detecting suspicious activities
- Raising alerts to respective action owners
- Performing automated actions or raising incidents
- ML based algorithms to detect anomolies

SIEM – Security information and Event Management

Defense in Depth



Internal network
Firewall, instrusion detection and encryption

Perimeter
Firewall, VPN and packet filters

Host
Platform OS, patches and malware protection

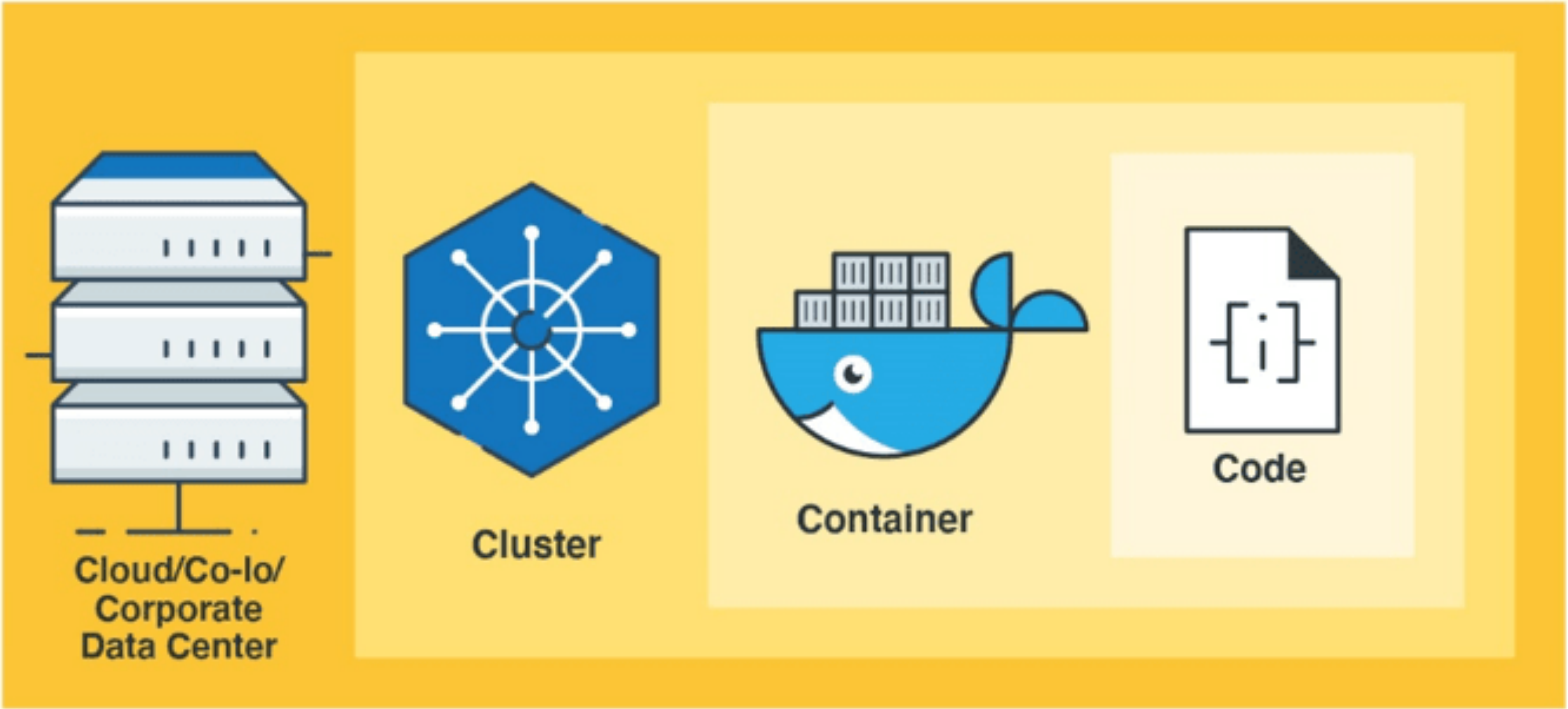
Physical
Locks, fences and security guards

App
SSO, authentication and authorization

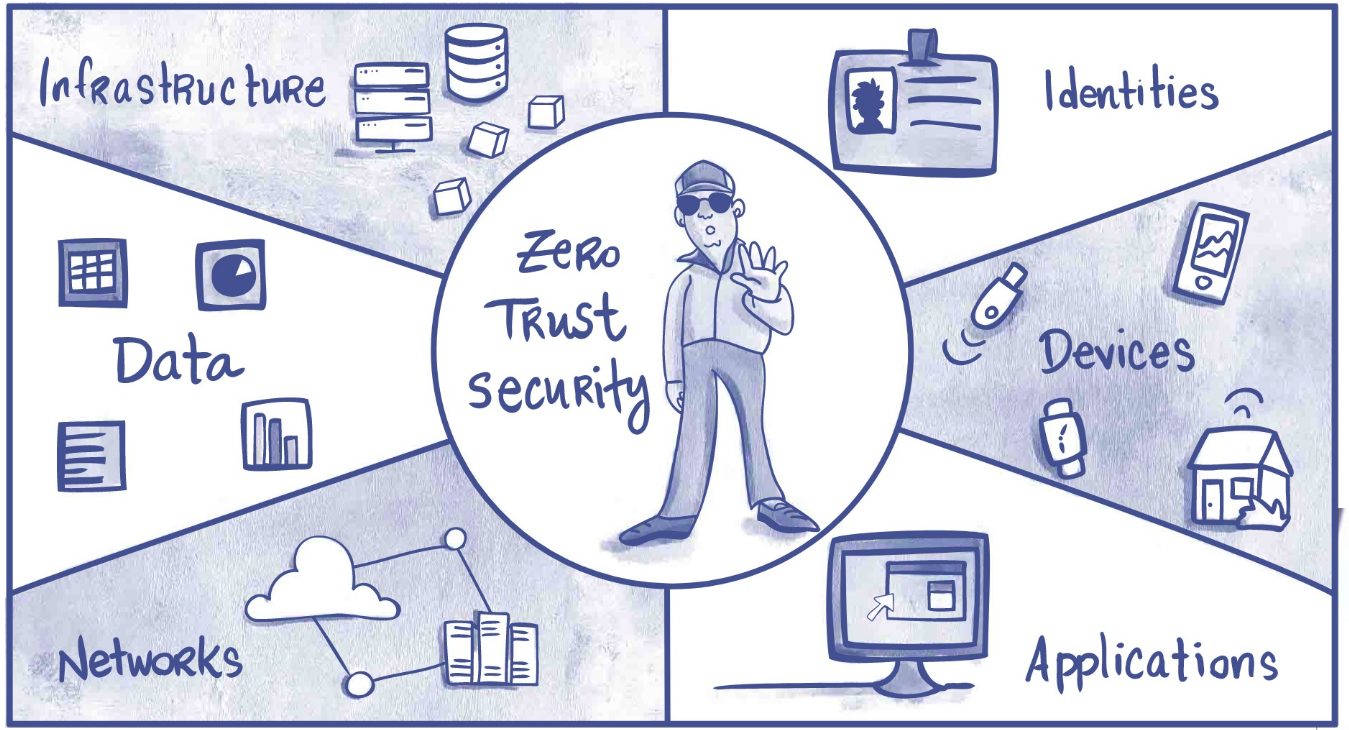
Policies, procedures and awareness
Passwords, policies and data classification

Data
Database, content and message security

We are heading towards Cloud Native Security…



Zero Trust Model



To conclude…!

- Cloud is a black box and when we don’t have control over it’s operations

Research areas are…

- Cyber threat intelligence / Malware Analysis
- Threat modelling
- IoT Security
- AI powered SIEM, SOR and SOC operations
- Zero Trust models
- Digital forensics
- Quantum cryptography
- AI security governance

Any questions… ?

Thank you !

- LinkedIn / Twitter - @ImTheVB