CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Your Cloud Security Maturity RoadMap is WRONG?

Ashish Rajan | Technical Director - Security & Identity
www.ashishrajan.com

Who am I?

- Security and Identity in Cloud
- Advisory aka Coach
- Public Speaker
- Community Builder
- Have strong opinion on Security, Coffee, Fashion

Connect on www.ashishrajan.com

Agenda

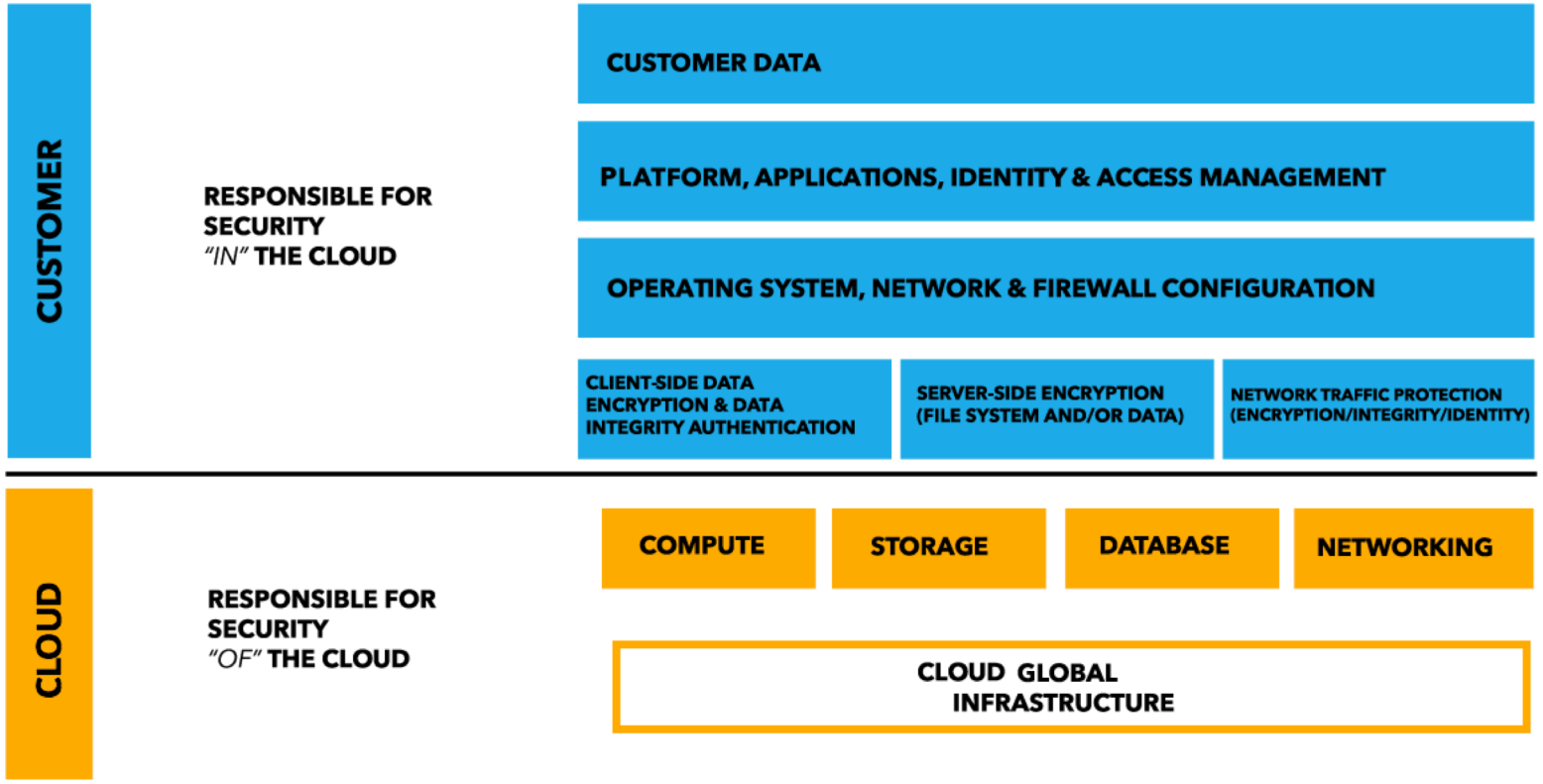
- Leveling up the security playfield
- Challenges & Risks
- Cloud Security RoadMap
- Where should you start?

Leveling up the security playfield

Shared Cloud Security Model

- Security "***in***" the Cloud
  - Consumer of Cloud

- Security "***of***" the Cloud
  - Public Cloud
  - Private Cloud



Current Security Landscape

- On-premise
- Cloud (Hybrid, multi-cloud)
- **Budget** ☹
- Containers (Kubernetes)
- Endpoints (Physical Devices)
- Security Education & Awareness
- Governance

Types of Cloud Deployments

What should be done

- *Microservices*
- *Transformed*
- *Automated*
- *Guardrails*
- *Compliant*

What really happens

- *Monolith*
- *Lift & Shift*
- *Kind of Automated*
- *Magic*
- *No visibility*

Cloud environment as a Service

Challenges & Risks

Challenges

- Everyone wants to go on the cloud but rarely want to talk security
- Network Perimeter is no longer a walled garden
- Limited budget for automation & security
- Not everything in the cloud is “transformed”
- Un-trusted on-premise assets move to cloud
- Compliance is a challenge in a cloud context

Risk

- Cloud platforms are a two-way street
- A security incident is only a line of code away
- Shadow Cloud
- Retaining talent and keeping them engaged
- Hiring “*skilled people”* with “*right behavior”* is hard!!
- “*Trusted Advisors*” are rare and few.

Cloud Security RoadMap

Cloud Security RoadMap

- Inventory
- Clean up the shed
- Pick the Path of MVP but focus on vision
- Feedback

Inventory

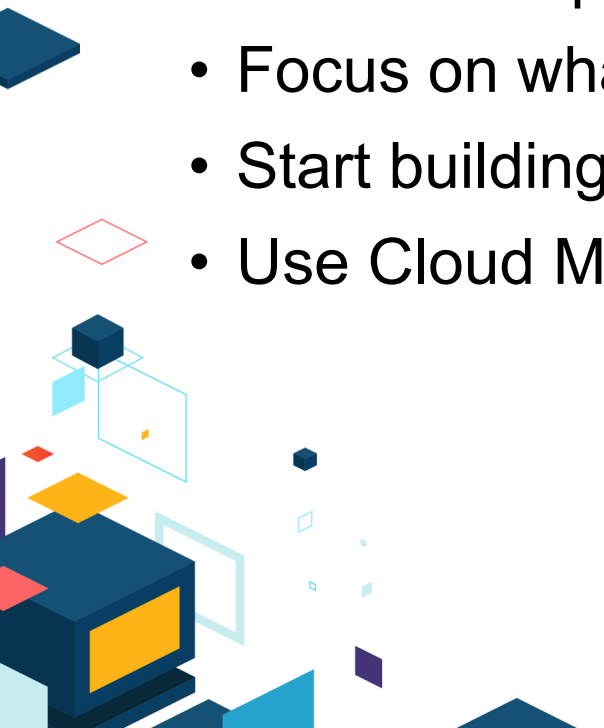
- **On-Premise**
  - Internal Network accessible to Cloud
  - Systems connected to Cloud Platform
  - Governance templates
  - Compliance inventory

Inventory

- **Cloud**
  - Identity Framework – Servers & Users
  - Access Management
  - What kind of clouds do you have?
  - DevOps Team vs App Team
  - What Applications are in the cloud?
  - Are any business critical systems on cloud?
  - Any compliance driven systems on cloud?
  - Security Team Cloud accounts

Clean up the shed

- Re-define Organisation Risk to include data points from your cloud environments
- Re-assess & save some $$ on security products that are not relevant
- Tackle Compliance – what must not go into cloud vs what can?
- Focus on what is the most valuable and business critical
- Start building relationships with DevOps, Cloud, App teams
- Use Cloud Migration projects as a security education exercise



Pick the Path

Pick the path of MVP but don’t loose focus on the vision.

- Infrastructure
- Application
- Compliance
- Governance

Pick the Path

Pick the path of MVP but don’t loose focus on the vision.

- **Infrastructure**
- **Application**
- **Compliance**
- *Governance*

Path – Infrastructure – Use Case 1

Greenfield cloud template

- Define Identity Framework
- Define process and implement environment security guardrails for Service Catalogue offered and used in the new Cloud environments
- Name resources
- Infrastructure is code with ephemeral resources but logs can be permanent
- Log the Servers, Network, Firewall, Identity, Audit into SIEM
- Integrate Patching, Vulnerability & Threat Management
- Monitor & Alert from Cloud & SIEM for security events
- Document and publish a Cloud ready Response Plan

Path – Infrastructure – Use Case 2

Cloud Environment as a Service Template

- Get involved in the Service Catalogue request process
- Identify business critical resources in the cloud
- Identify the Infrastructure, Network Connectivity, Applications
- Identify Patching, Vulnerability & Threat Management
- Identify Monitoring and Alerting available for security events
- Integrating security to identified resources
- Update and publish the cloud ready Response Plan

Path – Application – Use Case 1

Application going into a new Cloud environment

- Identify your Security Champions
- Define Security components
  - Standard OS Images, Secure Coding Practices, Segregation of Duties
- Define security integration for Supply Chain Management components
  - Code Management – Dependency, Code Security, Code Release
- Identify, supply and manage Application Security detection tools in stages
- Code Security education

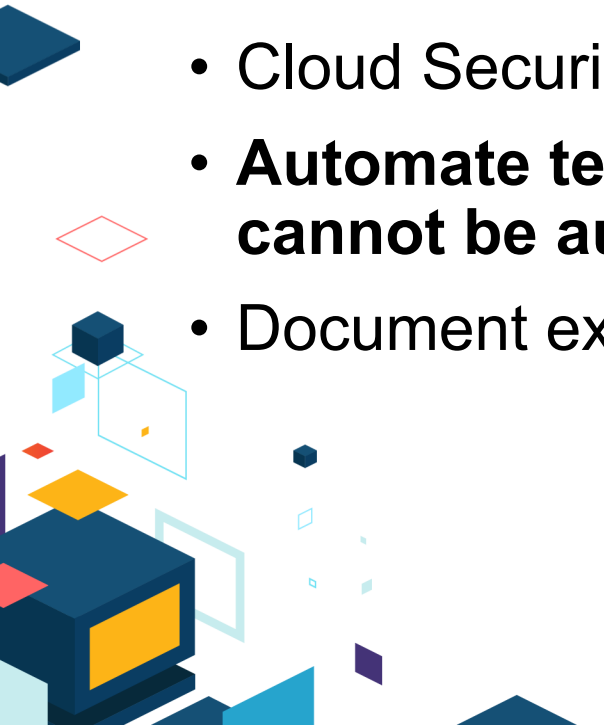
Path – Application – Use Case 2

Applications already in Cloud environments

- Identify your Security Champions
- Identify Security components
  - Standard OS Images, Secure Coding Practices, Segregation of Duties
- Identify security integration for Supply Chain Management components
  - Code Management – Dependency, Code Security, Code Release
- Identify, supply and manage Application Security detection tools in stages
- Code Security education

Path - Compliance

- Same standards but applied differently, unique per industry
- Driven by the auditor or assessor of the standard.
- Standards have not been updated to meet cloud but some security communities have started working on this
- Cloud Security Alliance, Center for Internet Security Benchmark
- **Automate technical controls and document process for controls that cannot be automated**
- Document exceptions and have governance process defined.



Feedback

- What is security in your organisation?
- Who are your customers?
- What does Security Assurance look for your company in cloud?
- Feedback, Feedback, Feedback
- Don’t be afraid to go back to the drawing board

Where should you start?

New Hire/ Upskill

- Cloud Security Architect
- Application Security
- SecOps
- DevSecOps
- Compliance in Cloud
- Trusted Partners

People who *can run it*
People who *want to learn it*

Cost of doing nothing

- Respect Legacy but *Adapt*
- Build visibility for security
- Guardrails not Metal Gates
- Automate, Automate, Automate
- Think like a security business

THANK YOU

Ashish Rajan | Technical Director – Security & Identity
www.ashishrajan.com

#cloudsec

www.cloudsec.com