



OPEN WEB APPLICATION SECURITY PROJECT

Pentesting AWS

Anand Varia

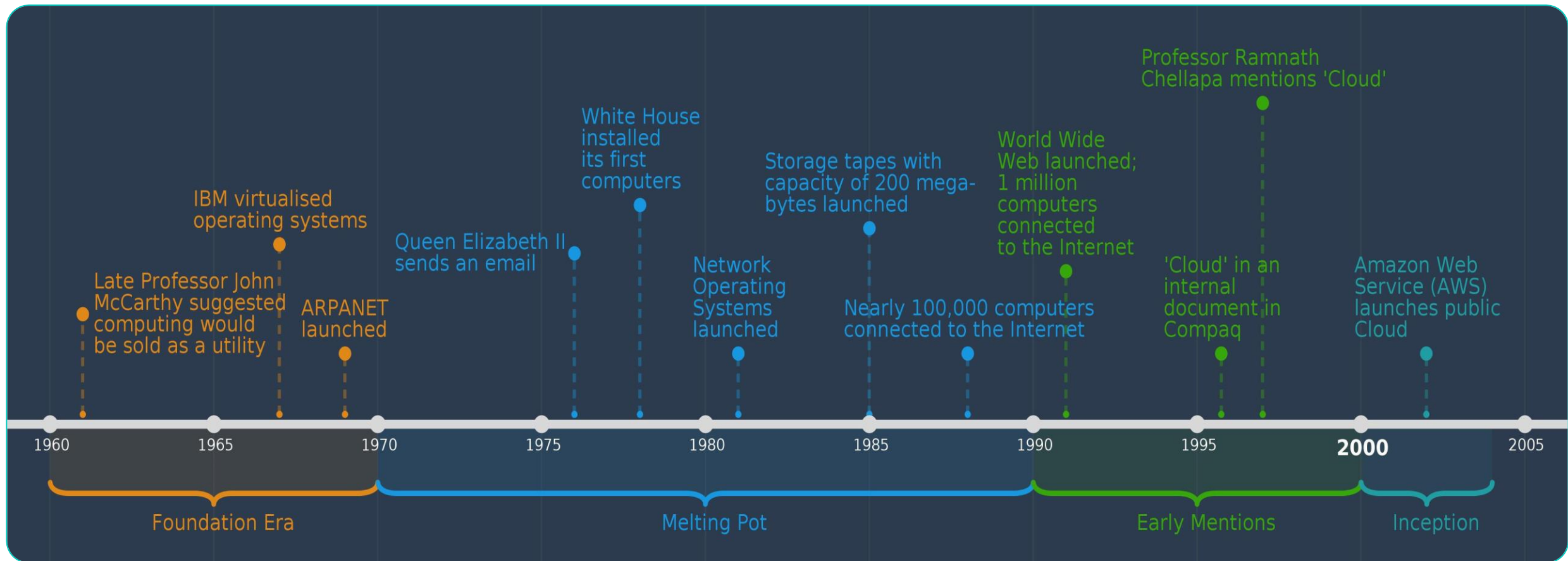
Disclaimer

- I am **NOT** being compensated by AWS or my employer to give this talk. I am expressing my own opinions here.
- I'm sharing what I have learned. There are many others who know more about AWS than I do.

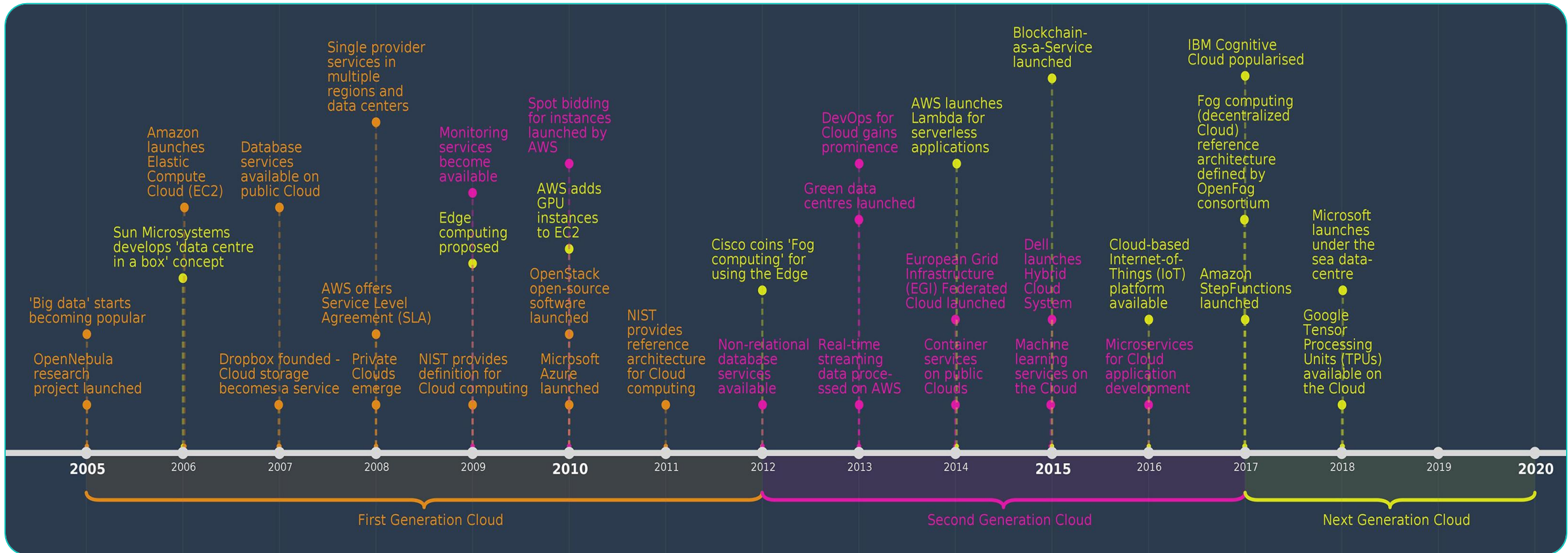
Agenda ~ 45 mins

- Evolution of Cloud
- About AWS
- Key AWS concepts
- Cloud Breaches
- Demo - Scenario 1
- Demo - Scenario 2
- Using AWS to secure AWS
- QnA

Evolution of cloud



Evolution of cloud



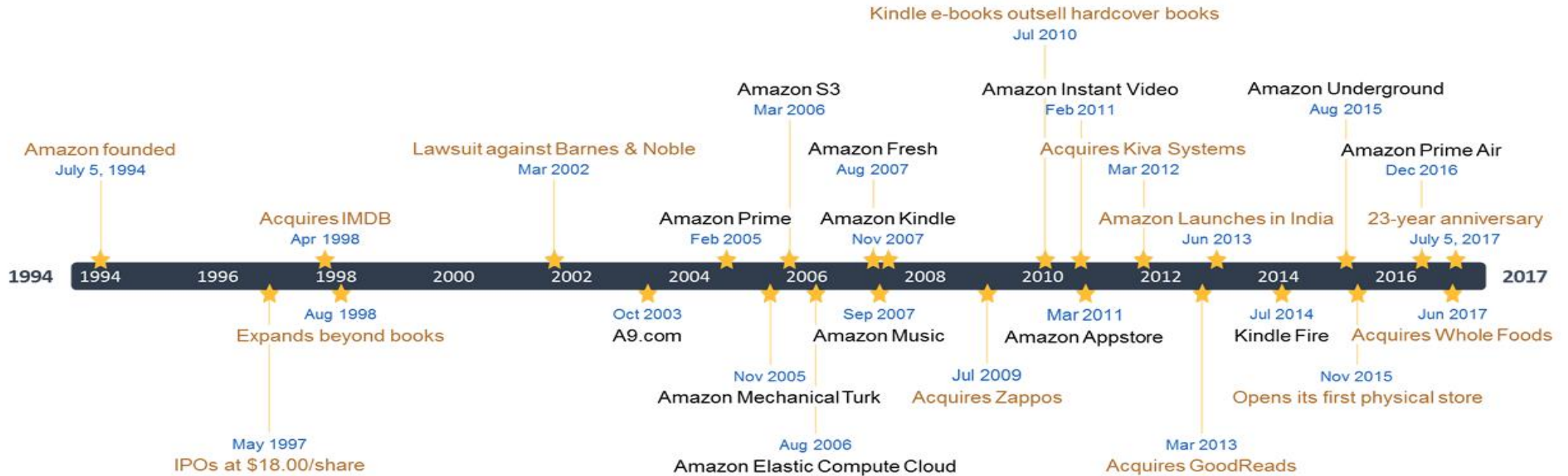
Evolution of Amazon



All ▾



★ Company milestones ★ Product launches



Office **TIMELINE**

What is Cloud?



About AWS

- Amazon **W**eb **S**ervices
- Here services are terms used for various products it is offering like S3, EC2, RDS, Lamda, Polly, SNS, SQS etc.
- There are 150+ services and are being added frequently

The screenshot displays the AWS Management Console interface. At the top, there is a navigation bar with the AWS logo and several service icons: Services, Resource Groups, EC2, VPC, IAM, S3, and RDS. The main heading is "AWS Management Console". Below this, there is a section for "AWS services" with a "Find Services" search bar. The search bar contains the text "Example: Relational Database Service, database, RDS". Below the search bar, there is a section for "Recently visited services" which includes links to EC2, Config, Inspector, and Artifact. The main section is titled "All services" and is organized into several columns of service categories:

- Compute**: EC2, Lightsail, ECR, ECS, EKS, Lambda, Batch, Elastic Beanstalk, Serverless Application Repository
- Storage**: S3, EFS, FSx, S3 Glacier, Storage Gateway, AWS Backup
- Database**: RDS, DynamoDB
- Developer Tools**: CodeStar, CodeCommit, CodeBuild, CodeDeploy, CodePipeline, Cloud9, X-Ray
- Robotics**: AWS RoboMaker
- Blockchain**: Amazon Managed Blockchain
- Satellite**: Ground Station
- Management & Governance**: AWS Organizations, CloudWatch, AWS Audit, etc.
- Machine Learning**: Amazon SageMaker, Amazon Comprehend, AWS DeepLens, Amazon Lex, Machine Learning, Amazon Polly, Rekognition, Amazon Transcribe, Amazon Translate, Amazon Personalize, Amazon Forecast, Amazon Textract, AWS DeepRacer
- Analytics**: Athena, EMR, CloudSearch, Elasticsearch Service, Kinesis, QuickSight
- Mobile**: AWS Amplify, Mobile Hub, AWS AppSync, Device Farm
- AR & VR**: Amazon Sumerian
- Application Integration**: Step Functions, Amazon EventBridge, Amazon MQ, Simple Notification Service, Simple Queue Service, SWF
- Customer Engagement**: Amazon Connect, Pinpoint, Simple Email Service

Definitions : Regions & AZ's

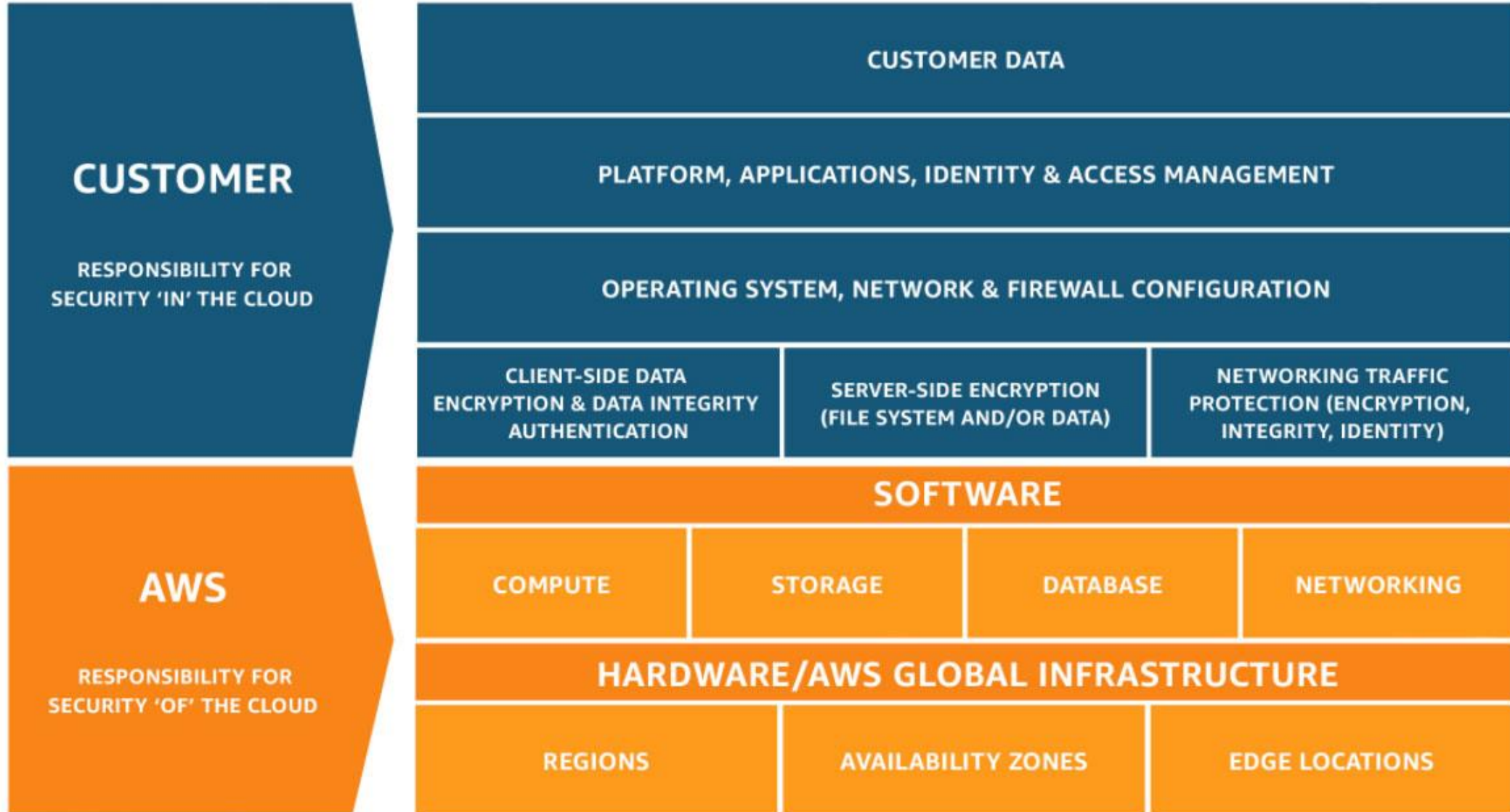
Region: A geographical area designed to be isolated from all other Regions

- Isolated for fault tolerance and stability
- AWS has Global Services (like IAM) that apply to all Regions
- AWS also has Region-based Services

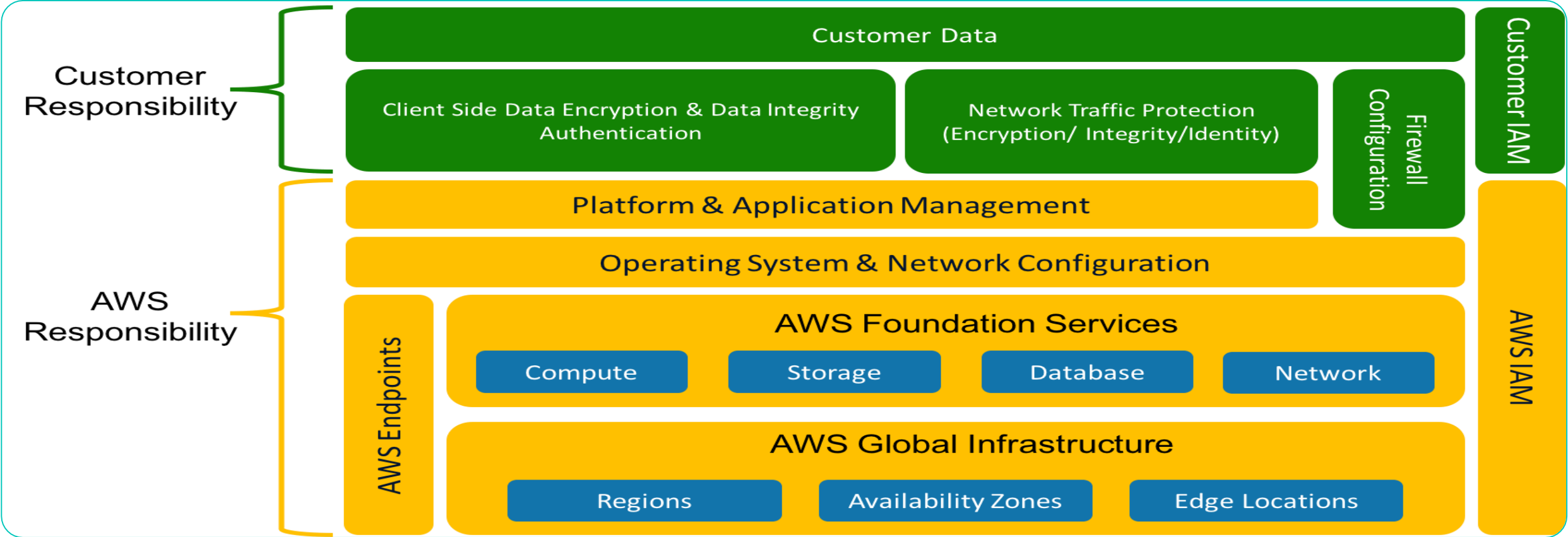
Availability Zones are separate locations within the Region

Site: <https://infrastructure.aws/>

About AWS : Shared Responsibility Model

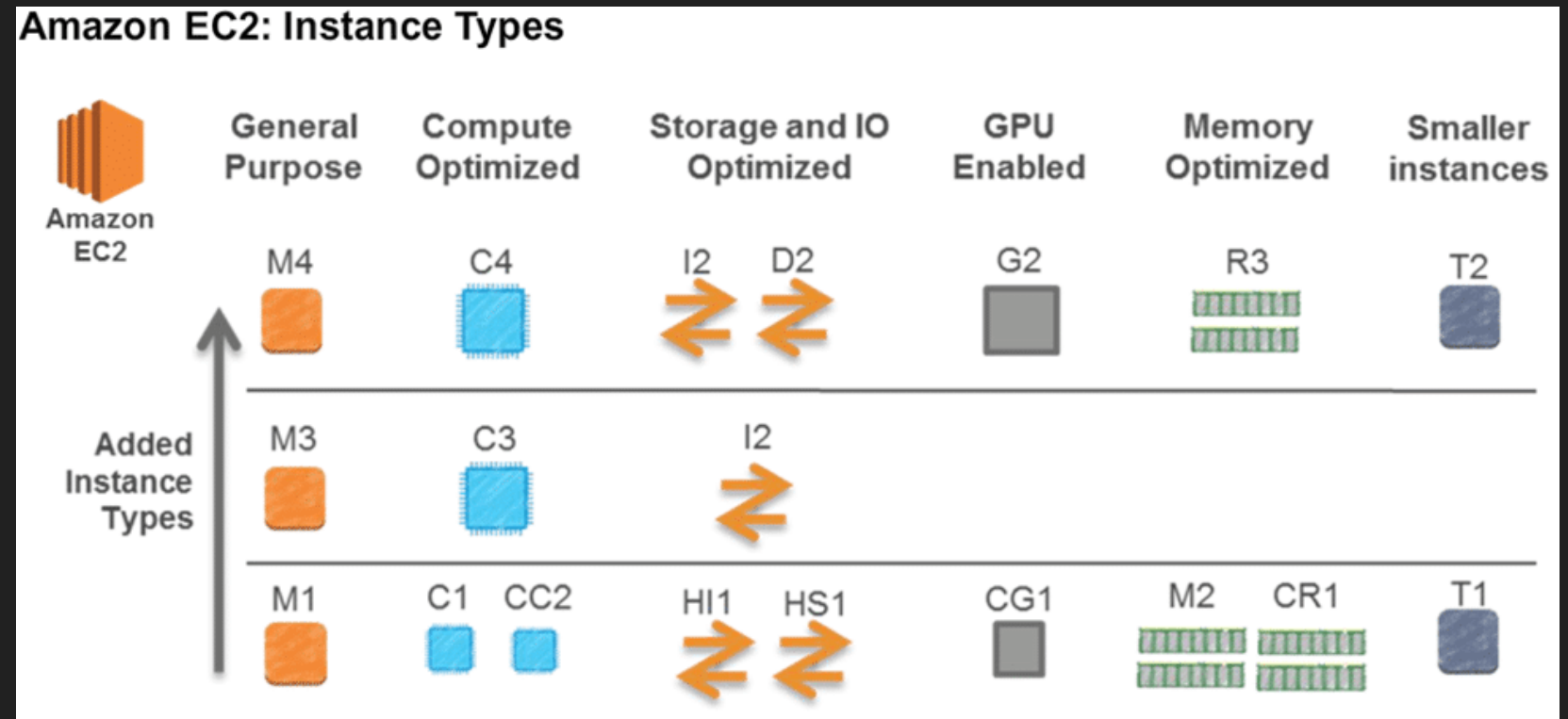


About AWS : Shared Responsibility Model



Key Services : Elastic Cloud Compute(EC2)

- EC2 instances are traditional virtual servers present on cloud
- **AMI:** Amazon Machine Image : Golden images to create Instances
- There are **Security Groups, Auto scaling groups, Elastic Ips.**



Key Services : VPCs, Security Groups

- **Security Groups** are individual enclaves bordered with stateful firewalls
 - Can specify separate (or even multiple) Security Groups for each host
 - Filtering rules can be set up for inbound and outbound traffic
 - Can specify allowed source/destination IPs and ports
 - If not otherwise specified, all outbound traffic is permitted
 - Implicit DENY of all traffic not explicitly ALLOWed
- **VPCs** are like VLANs, a private network
- **VPC Endpoints** : VPC Endpoints allow private connections between the AWS back-end and your VPC

Key Services : Simple Storage Service S3

- S3 is a Object based storage service where you can practically store unlimited files
- They have a bad reputation because, people leave them world readable

STORAGE CLASSES

CLASS	AVAILABILITY ZONES	DURABILITY	RESILIENT TO 1 AZ FAILURE
STANDARD and INFREQUENT ACCESS	1, 2, 3 or more	11 NINES	RESILIENT TO 1 AZ FAILURE
1-ZONE INFREQUENT ACCESS	1, 2, 3	11 NINES	NOT RESILIENT TO AZ FAILURE

99.5% /YR AVAILABILITY

STORAGE CLASS TRANSITIONS

```

    graph TD
      S[STANDARD] -- "128 KB obj Size Minimum" --> IA[1-ZONE IA]
      S -- "30 day minimum stay/charge" --> IA
      S -- "Cost to retrieve from IA storage $10/TB" --> IA
      S -- "Long-term Storage" --> G[GLACIER]
      IA -- "90 day minimum stay/charge" --> G
      IA -- "40KB added to each obj for metadata" --> G
      IA -- "30 day minimum stay/charge" --> IA
  
```

SERVER SIDE ENCRYPTION

AES-256 master key rotation	AWS managed KEYS (audit trail)	KMS managed KEYS (more security controls)	SELF managed KEYS (you own it!)
-----------------------------	---------------------------------------	--	--

QUERY IN PLACE

AMAZON S3 OBJECT STORAGE

Cost: \$2/TB scanned / 70% returned (Standard Storage), \$10/TB scanned / 1% returned (IA Storage)

S3 SELECT: Retrieve subset of data, Use simple SQL

OBJECT LOCKING (NEW)

PREVENT OBJECT DELETION

GOVERNANCE: CAN'T DELETE TIL DATE

COMPLIANCE: NEVER DELETE (EVER)

👤 jerry@lucidchart 🐦 @awsgeek

REQUESTS (\$/USD per 1000,000 requests)

	GET	POST	PUT	COPY	LIST	SELECT	other
Standard	0.4	5.0	5.0	5.0	5.0	0.4	0.4
Infrequent Access	1.0	10.0	10.0	10.0	1.0	1.0	1.0
1-Zone IA	1.0	10.0	10.0	10.0	1.0	1.0	1.0

Storage class transitions: 1¢ per 1,000 objects
Transition to Glacier: 5¢ per 1,000 objects

STORAGE

TB	Cost	per GB/Mo
[0, 50]	2.3¢	
[51, 500]	2.2¢	
[501, ∞]	2.1¢	
INFREQUENT ACCESS	1.25¢	
STD 1-ZONE	1.0¢	
GLACIER	0.4¢	

DATA TRANSFER

AMAZON CLOUDFRONT GLOBAL CDN

internet → S3 → internet

FREE (to 5.0¢ GB), 5.0¢ to 9.0¢ GB, 2.0¢ GB

OTHER AWS REGION

Key Services : CloudTrail vs CloudWatch

- **CloudTrail** is a webservice recording all the API activity, where as **CloudWatch** is monitoring service for aws resources and applications.
- **CloudTrail/Watch** gets enabled by default, for CloudWatch supports certain services and basic monitoring is free, for detailed one you will need to pay
- **CloudTrail** helps you in ensure compliance & regulatory requirements, **CloudWatch** logs details which provides information on what happens with data.
- **CloudTrail** : Deliver events within 15mins of API Call
- **CloudWatch** : for basic monitoring delivers data in 5 mins, for detailed monitoring 1 mins.

Key Services : Identity & Access Management



<https://www.cloudberrylab.com/resources/wp-content/uploads/2018/10/scheme-2-768x406.png>

- Not granting access to any services, user will be allowed to stare at the screen

Key Services : Identity & Access Management

Create policy 1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON [Import managed policy](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "s3:ListAllMyBuckets",
7       "Resource": "arn:aws:s3:::confidential-data"
8     },
9     {
10      "Effect": "Allow",
11      "Action": "s3:GetObject",
12      "Resource": "arn:aws:s3:::confidential-data/*"
13    }
14  ]
15 }
```

IAM Policy

IAM Statement

IAM Statement

Key Services : More Services

- **Tag**: a metadata key (value is optional) that can be attached to AWS resources.
 - Limit access to resources based on Tags:
“`Secrets manager:ResourceTag/Project`”: “`${aws:PrincipalTag/Project}`”
- **API Access : AWS CLI, AWS Provided Libraries**
 - **Access Key ID**
 - **Secret Access Key**
- **Cloud Formation** : “Infrastructure as a code” , another example is “Terraform”

Common Failures : Accessible API Keys, Excessive Permissions

- Your AWS API keys allow people to impersonate you, get access to your resources, and use your AWS account to mine for bitcoin.
- There are tools like truffleHog and git-secrets are available to audit any GitHub repositories to find AWS Keys, passwords, and other sensitive data.
- Public buckets: not even once, Until authorized by management
- Use bucket lifecycles for data retention.
- “Authenticated Users” group means anyone who has logged in to **any** AWS account, not just yours!
- Set your S3 buckets to be encrypted by default. It has zero impact on your workflow and makes your auditors happy.
- While encrypting take care of “Old Data” and all previous versions

“Demo”

Demo -1 Poorly configured S3 buckets

flAWS.cloud

Demo -2 Poorly configured IAM Policies

Excessive permission can lead to ...

Demo – 3 misconfigured EC2 instance

Who can access “meta-data”

Cloud Breaches

Former AWS Engineer Arrested as Capital One Admits Massive Data Breach

Over 540 million Facebook records found on exposed AWS servers

Leak originated at two third-party companies that had collected Facebook data on their own servers.



By Catalin Cimpanu for Zero Day | April 3, 2019 -- 18:32 GMT (00:02 IST) | Topic: Security

AWS Data Leaks Persist

In addition to the aforementioned Microsoft data leak, several Amazon Web Services (AWS) data leaks recently were discovered, including:

- **Alteryx:** [Misconfigured AWS cloud storage](#), exposing personal information from 123 million U.S. households.
- **Verizon:** Suffered two AWS-related leaks: a [Verizon Wireless leak](#) and a second exposure in which [14 million Verizon records were leaked](#).
- **Time Warner Cable:** [Leaked 4 million customer records](#).
- **WWE:** [Exposed 3 million customer records](#).

JUN 28, 2019

Ford, TD Bank Affected by Cloud Data Breach

BY CHRIS BRUNAU

Cybersecurity

by Dan Kobialka • May 1, 2019

An unprotected [Microsoft](#) cloud server database has exposed sensitive data from more than 80 million American households, hackers Noam Rotem and Ran Locar told [vpnMentor](#). Microsoft has notified the database owner, and the database has been removed.

Cloud Breach – Capital One

- On July 29th, a story broke about a hacker who extracted data from CapitalOne's infrastructure, Credit card application data from 2005-2019 was taken.
- There were 140,000 Social Security Numbers and 80,000 bank numbers included in this data.
- The source of the data was an S3 bucket, but this was not a public S3 bucket.

Facts : WAF IAM role from accessible ec2 instance with having access "sync" S3 buckets

- The report to the Law enforcement agency contains details about WAF IAM role being used to infiltrate the data from an EC2 instance

Cloud Breach – EBS Public Snapshots

- At **DEFCON**, *Ben Morris* from Bishop Fox announced that he had discovered that many Elastic Block Store (EBS) snapshots are set to public.
 - Elastic Block Store is a virtual hard drive for your EC2 Instances.
 - Backups of these virtual hard drives are done via Snapshots.
- If Snapshots are in Public mode, they are open to everyone.
- Anything that might be on your system might be in an EBS Snapshot (Code, AWS Keys, log data, company confidential information).
- You can audit your snapshots to figure out if they're Public or not via the Console or the AWS CLI, or set up AWS Config rules to audit and enforce Private snapshots

Using AWS to secure AWS

- Make use of **Trusted Advisor** at least for public S3, any to any traffic present in **SG**.
- Make separate accounts for infrastructure like **Production, SIT, UAT , Staging, Test, Hacking etc.,**
- Make use of **AWS Organizations , AWS Control Tower**
- **Least Privileges, IAM Hygiene, Restricted IAM Roles**
- Make use of **AWS Systems Manager**
- Make use of **AWS Config, Amazon Macie as well as Guard Duty**
- **Do not rely on your bill** to know which resources you are/were using. Have **inventory**

References

- For demo purpose I have used the following:
 - <http://flAWS.cloud>
 - Cloudgoat by Rhino security labs
- Tools reference link:
 - <https://github.com/0xVariable/AWS-Security-Tools>

Questions?



Thank you !

Email : anandjvaria@gmail.com