Security, Governance, Cost on AWS

Thomas Le Moullec. AWS Solutions Architect
September 29th 2020

Agenda

- AWS Security: Certifications & Shared Responsibility
- Identity and Access Management
- Encryption: Rest & Transit
- Configuration Management
- Cost Optimization 5 Pillars
- AWS Cost Explorer, Budget and Report
- Cost Management best practices

Security Principles

Identity and Access Management

Detection

Infrastructure Protection

Data Protection

Incident Response

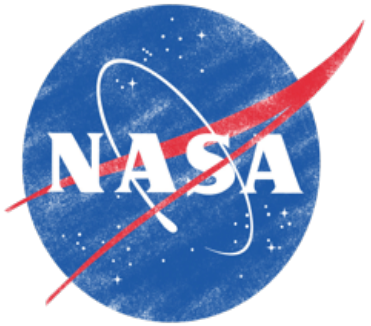
AWS – Data Privacy and Compliance

Highly Regulated industries such as Financial Services, Public Sector, Healthcare

AWS has world-class security and compliance teams working continuously on improving Security

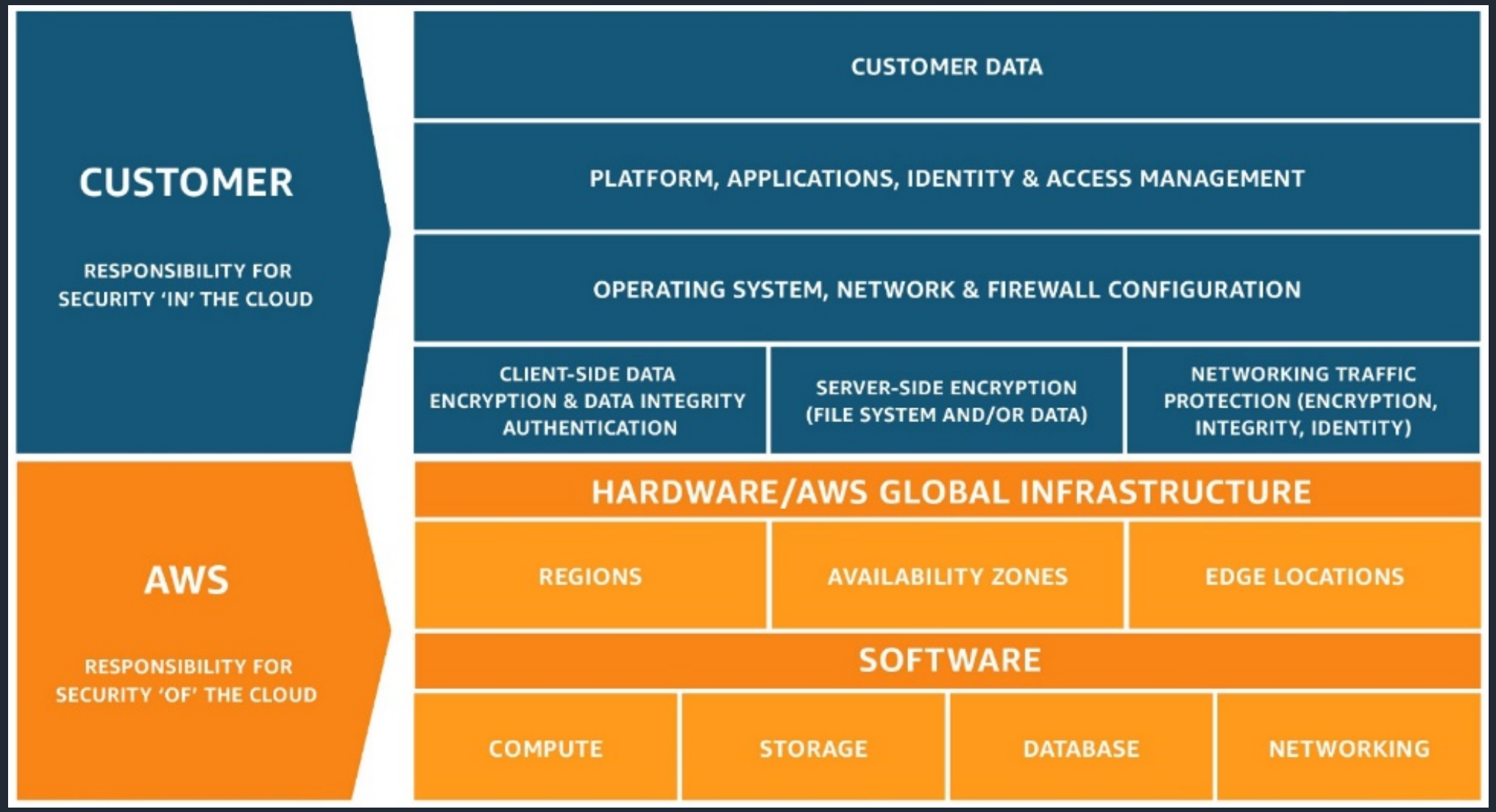
GDPR

General Data
Protection Regulation



Customers inherit best practices of policies, architecture and processes that have been built to satisfy the needs of most security sensitive customers

AWS – Shared Responsibility Model



AWS – Identity and Access Management (IAM)

IAM allows you to implement a comprehensive access control on AWS resources.

Authenticate

Credentials, MFA,
Other AWS Account

Authorize

Least Privilege with
IAM Policies

Audit

Log Allow and Deny in
Cloudtrail

AWS Principals

Do not use the root account for daily work

Root Account

Access to all, billing, Support, Console and APIs

IAM Users, Groups and Roles

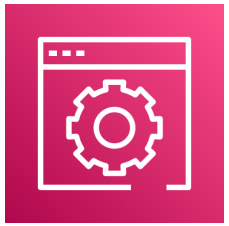
Access to some services, Support, Console and/or APIs

Temporary Credentials

Access to specific services, Console and APIs

AWS Authentication

Who are you ?



AWS Management Console

- Login with Username and Password
- Optional Multi-Factor Authentication (MFA)
- Temporary access via Signed URL

API access (CLI, SDK)

- Access with Access Key + Secret Key
- Optional Multi-Factor Authentication (MFA)
- Temporary access via request to AWS STS

AWS Authorization

Are you allowed to proceed ?

AWS Root Account

- All Access for all actions
- Always enable MFA on root account

(If MFA is on a Device, store securely the device)

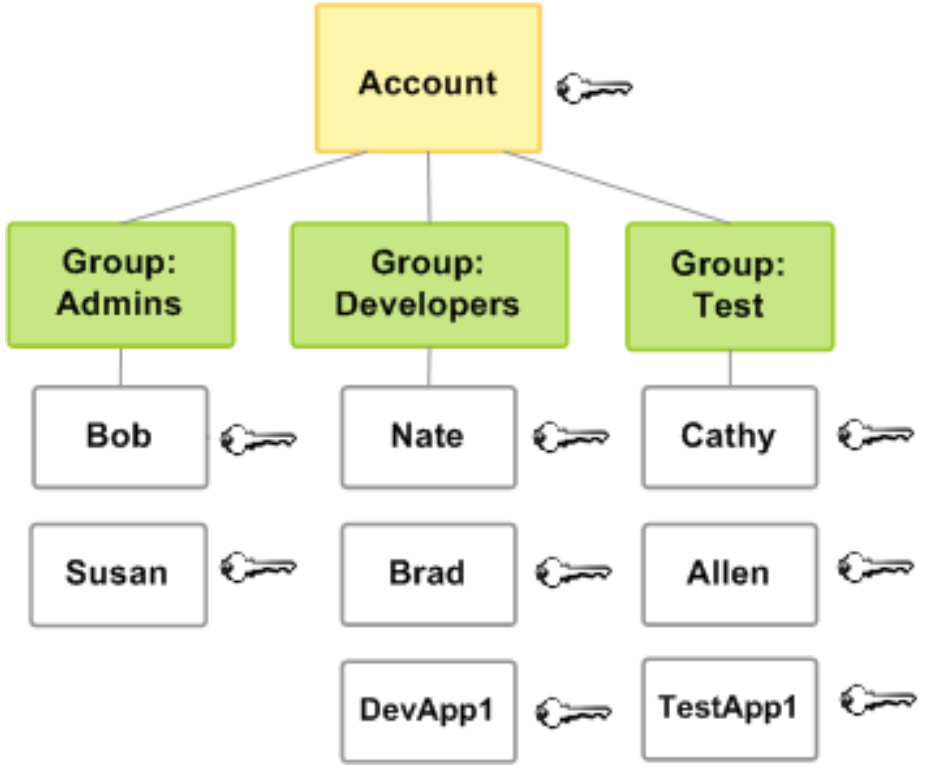
IAM Policies

- Privileges for Users, Roles, Resources level
- JSON format
- Best practice: Use the Least Priviledge
- Example:

  Action: [‘s3:Get*’]
  Effect: Allow
  Resource: ‘arn:aws:s3:::mybucket/*’

IAM – Groups and Users

- Permissions for each users
- Manage groups of users
- Give permissions directly to the group



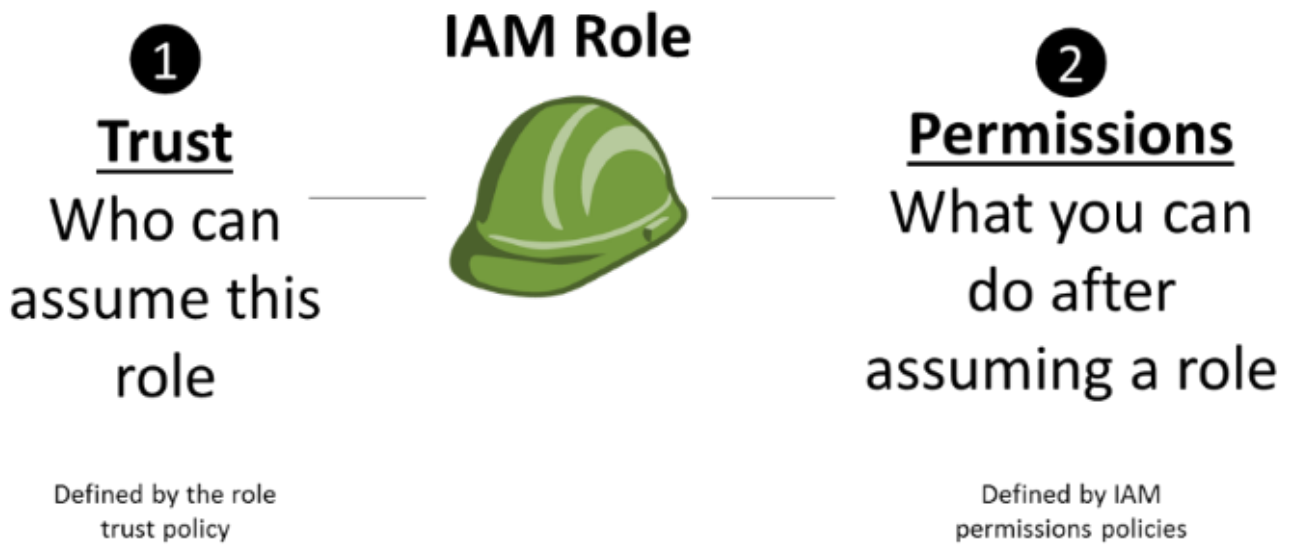
IAM – Roles

Put on a new hat and assume a new role with different permissions

Can be assumed by Users or AWS resources.

Few Examples:

- EC2 Instance accessing S3
- User creating EC2 instance
- User in another account assume the role (Prod and Test Account)



Security – Encryption at Rest

Volume
- EBS encryption - Marketplace solution - OS/Filesystems Tooling

Object
- Server Side Encryption - SSE with Customer keys - Client Side Encryption - Integrates with KMS

Database
- Integrates with KMS - Integrates with HSM - One click encryption (Redshift, DynamoDB)

AWS Secrets Manager

Leverage AWS Secrets Manager to store securely at rest credentials and secrets

Security – Encryption in Transit

HTTPS: AWS Services APIs / endpoints are offering HTTPS

SSL/TLS	VPN/IPSec	SSH
 AWS Certificate Manager	 AWS Site to Site VPN	 AWS Systems Manager
 AWS Elastic Load Balancer		

AWS Key Management Service (KMS)

AWS KMS

Managed service for encryption key creation, control, rotation and usage.
Integrates with most AWS services: S3, Redshift, RDS, EBS, Secrets Manager.
Customers can bring their keys.

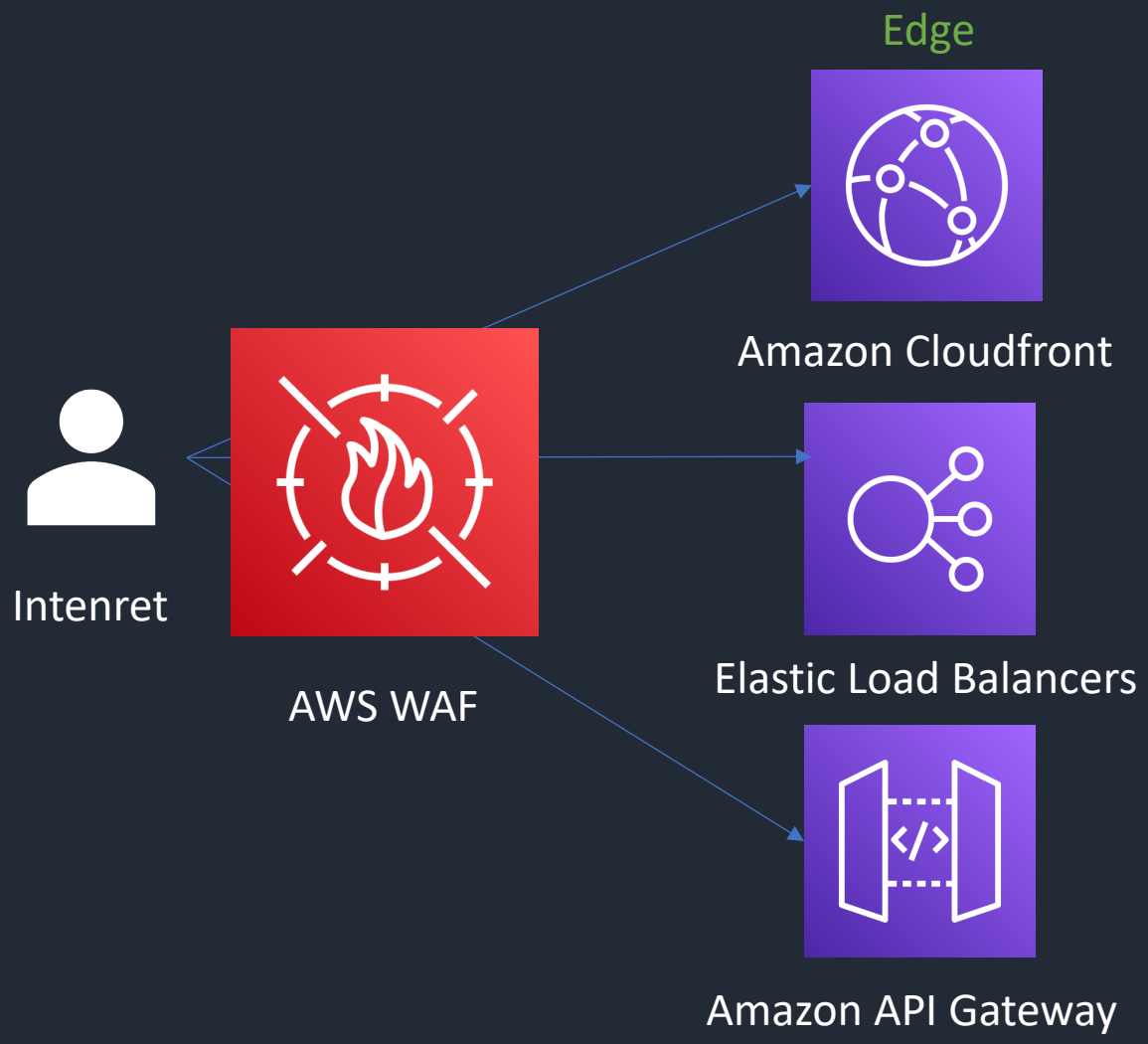
Amazon Inspector

Automated security assessment service to help improve the security and compliance of applications deployed on AWS

Amazon Inspector

- Pay for what you use : OnDemand
- Uses an optional agent for EC2
- Integrates with CI/CD
- Generates findings: Priority order by level of severity
- Rules packages include :
  - Common Vulnerabilities and Exposures (CVE),
  - Center for Internet Security (CIS) benchmarks,
  - Security Best Practices,
  - and Runtime Behavior Analysis

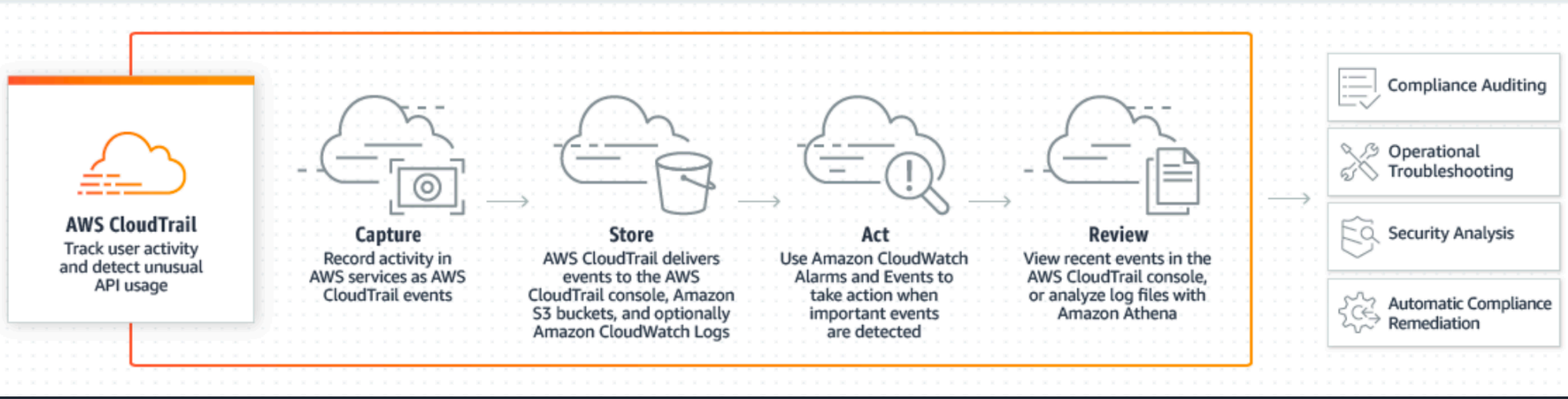
AWS Web Application Firewall - WAF



- SQL Injection & Cross Site Scripting (XSS)
- Mitigate DDoS (HTTP/HTTPS floods)
- Web Site Scraping,BOTS / Crawlers
- Create Custom Rules

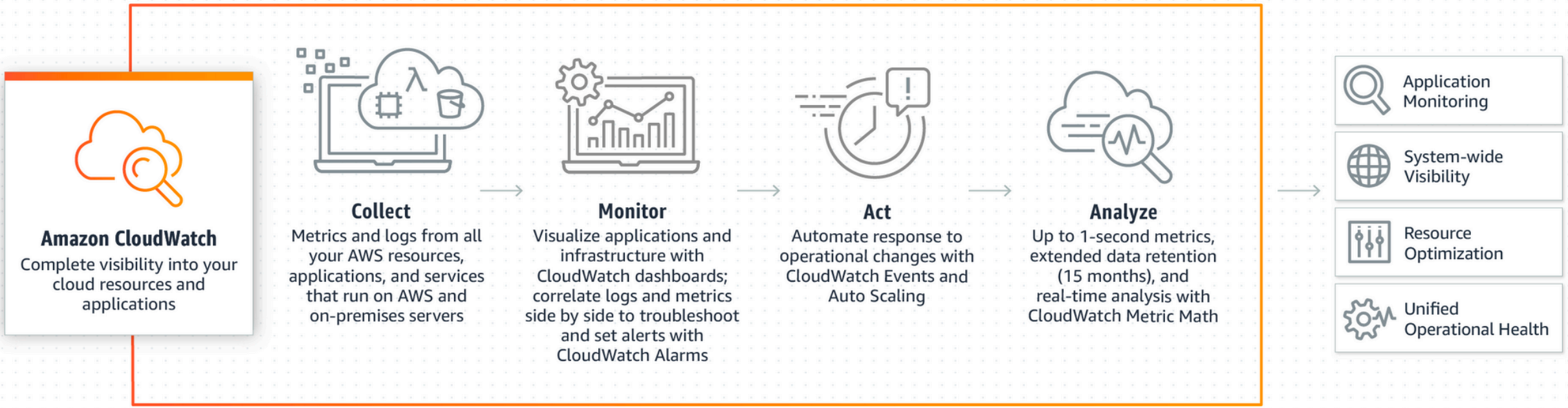
AWS Cloudtrail

API Calls report for audit and user activity tracking



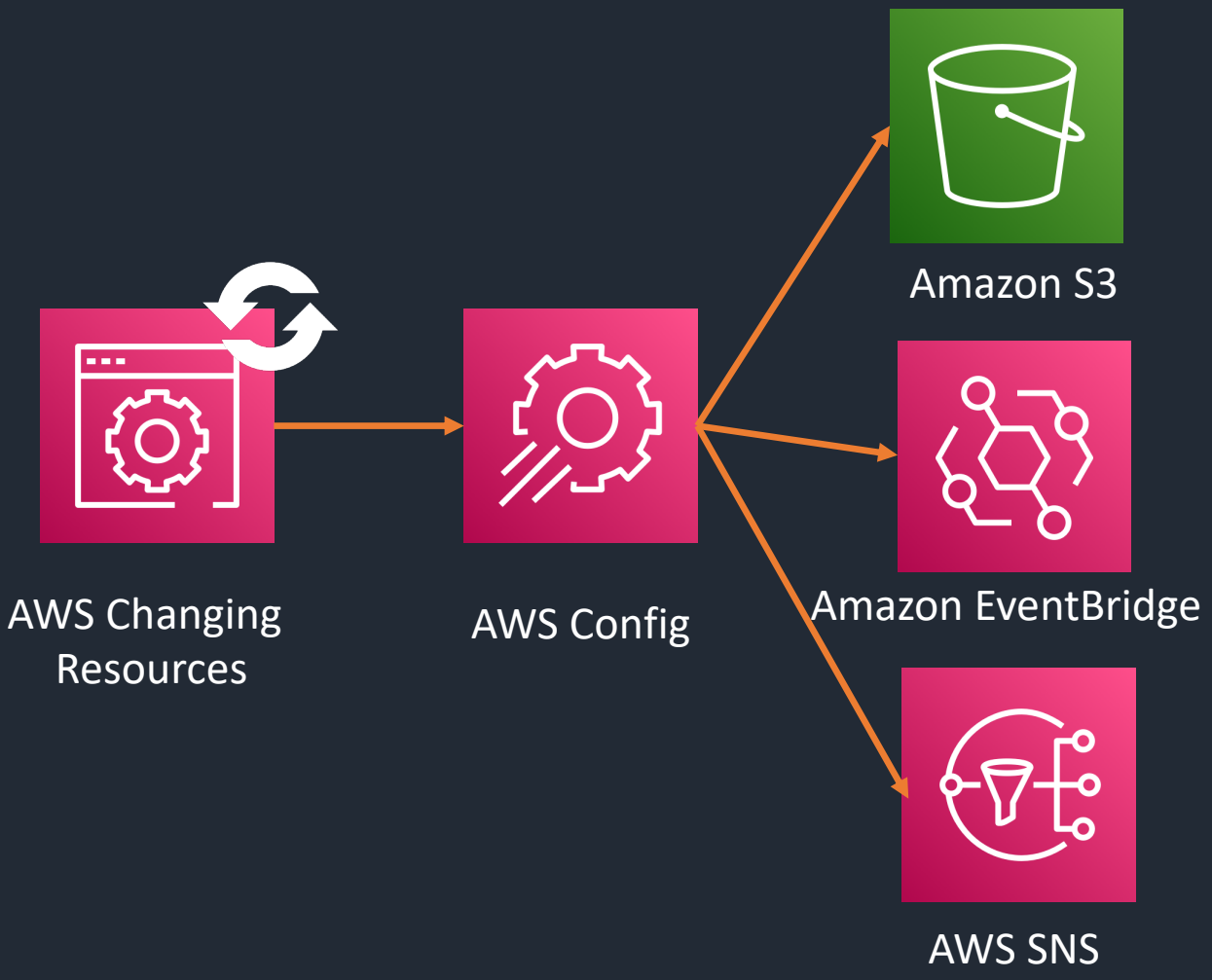
AWS Cloudwatch

Critical service to achieve a well-architected solution on AWS



AWS Config

- Security Analysis
- Audit Compliance
- Change Management
- Discovery (What exist ?)



5 Pillars of Cost Optimization

Right Sizing

Increase Elasticity

Right Pricing Model

Match Usage and Storage

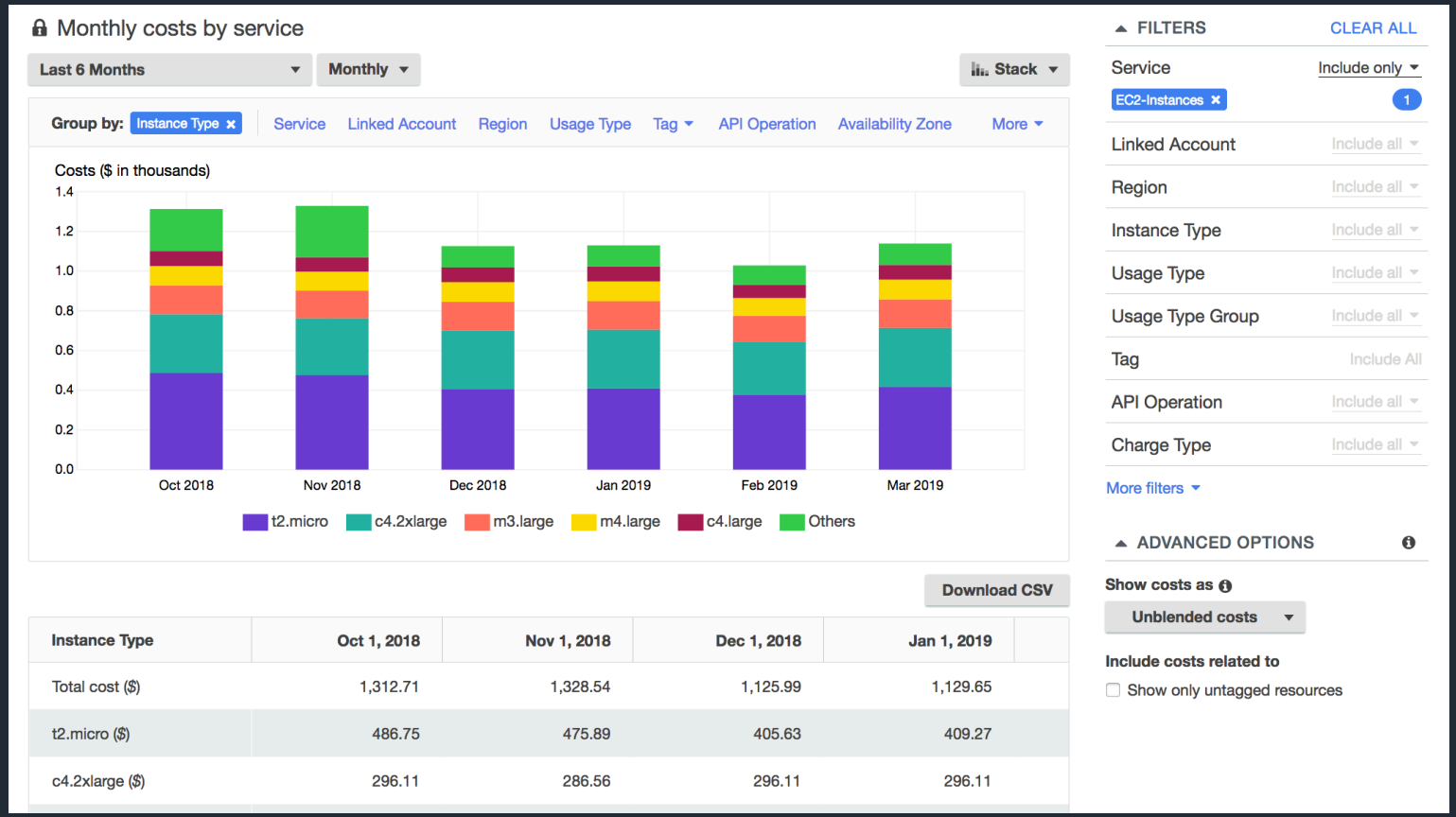
Mechanisms for Optimization

AWS Free Tier

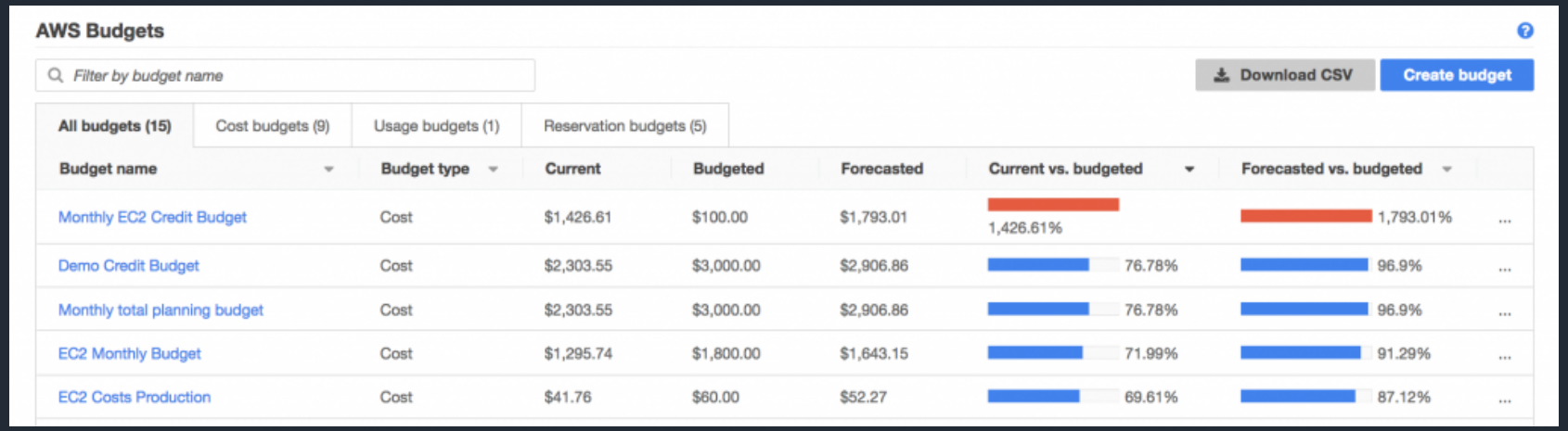
- 60+ Services
- Always Free / 12 months / Trials
- Check https://aws.amazon.com/free/

AWS Cost Explorer

- Filter, group and visualize
- Save as report for future
- Forecasting capabilities



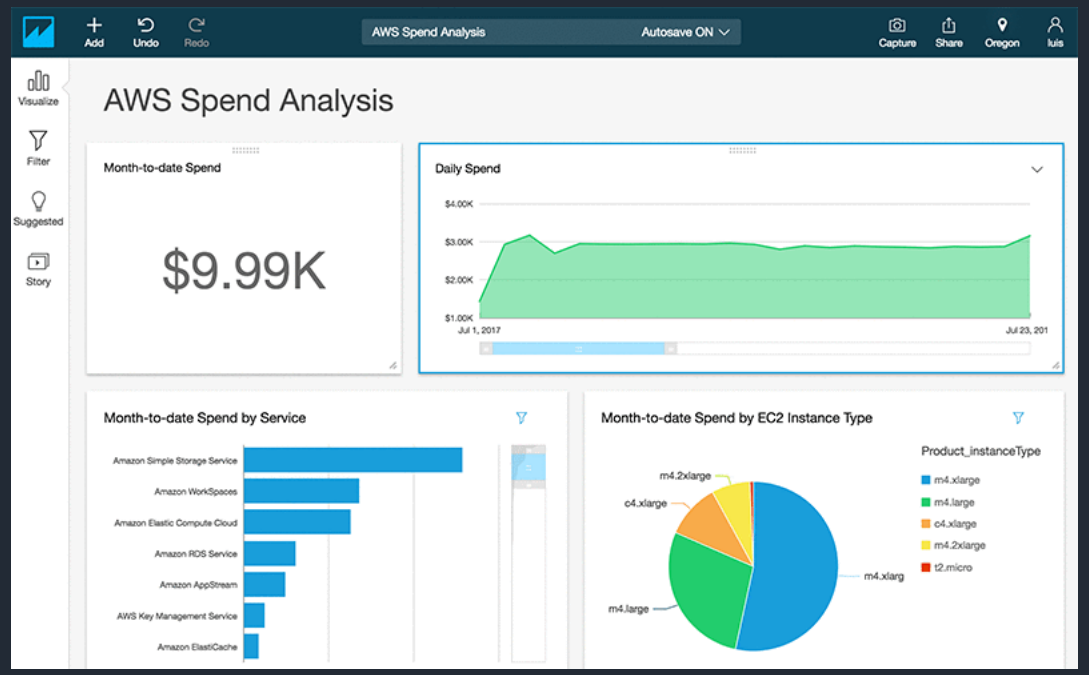
AWS Budgets



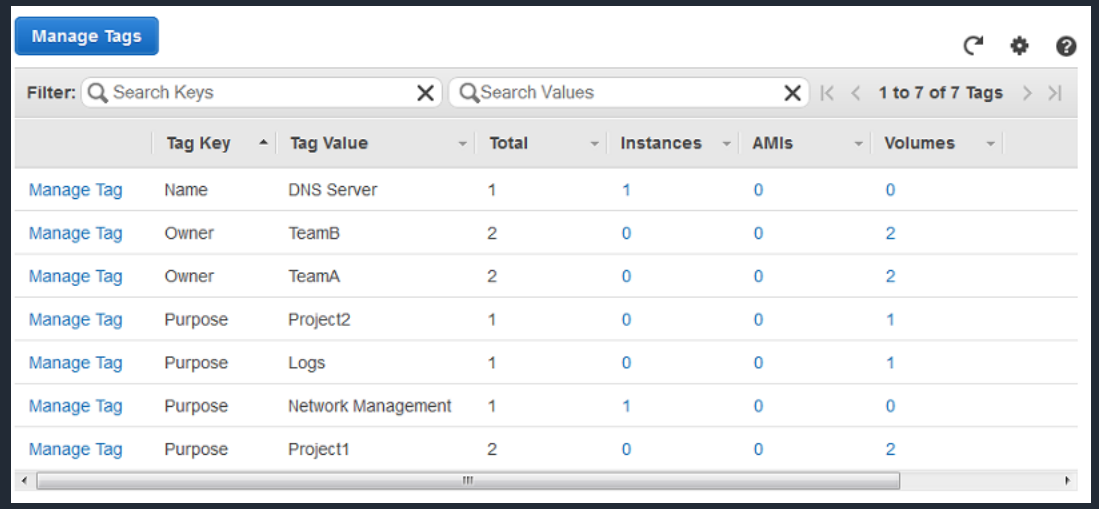
- Set Custom Budgets
- Alert when your Cost or Usage exceed (or the forecasted)
- Can send notifications (Email) or SNS with Lambda

AWS Cost Report

- Cost Report in CSV delivered to S3
- Can ingest in Database
- Can visualize with Quicksight



Cost Management – Best practices



	Tag Key	Tag Value	Total	Instances	AMIs	Volumes
Manage Tag	Name	DNS Server	1	1	0	0
Manage Tag	Owner	TeamB	2	0	0	2
Manage Tag	Owner	TeamA	2	0	0	2
Manage Tag	Purpose	Project2	1	0	0	1
Manage Tag	Purpose	Logs	1	0	0	1
Manage Tag	Purpose	Network Management	1	1	0	0
Manage Tag	Purpose	Project1	2	0	0	2

- Define and enforce cost allocation tagging(AWS Config)
- Define Metrics (Cloudwatch) and Monitor (AWS Cost Explorer)
- Setup Automation (AWS Budget, SNS, Lambda)

Thank you !

Find me on Linkedin:
Thomas LE MOULLEC