How to Protect your Information with Encryption and Automated Security Remediation on AWS

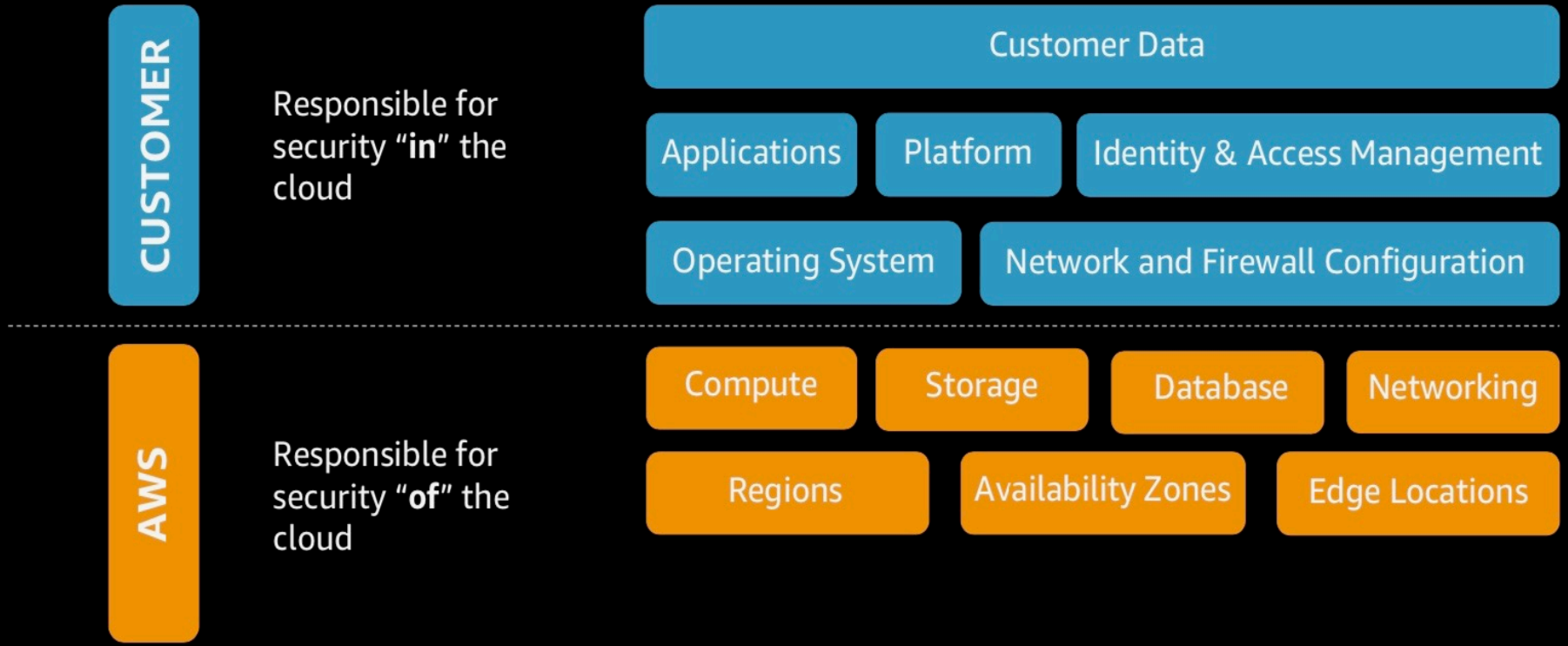
Liliya Frye
Cloud Security Specialist
LiliyaFrye@gmail.com

Agenda

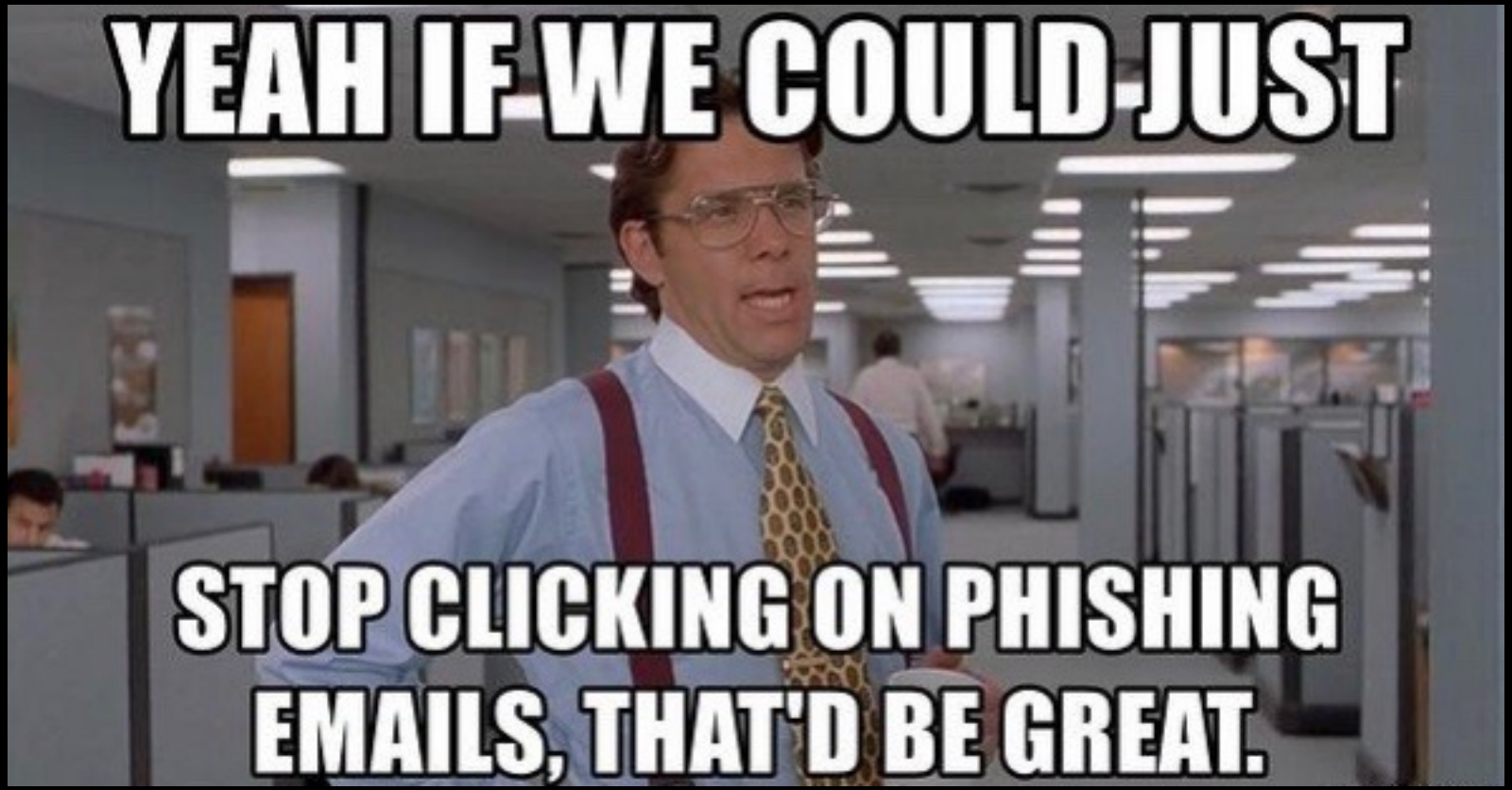
- AWS Shared Responsibility Model
- AWS Global Infrastructure
- AWS Security Solutions
- Protecting your Data with Encryption
- Incident Response
- AWS Config Rules Automated Security Remediation
- Solution


CYBER SECURITY
IT'S KIND OF A BIG DEAL

Shared responsibility model



Conduct Regular Security Awareness Inside Your Company




WHAT IF I TOLD YOU
"THE CLOUD" IS JUST
SOMEONE ELSE'S COMPUTER.

AWS global infrastructure

22 Regions – **69** Availability Zones – **169** Network PoPs

Regions & Number of Availability Zones

AWS GovCloud (US)
US-East (3)
US-West(3)

US West
Oregon (3)
Northern California (3)

US East
Northern Virginia (6)
Ohio (3)

Canada
Central (2)

South America
Sao Paulo (3)

EU
Ireland (3)
Frankfurt (3)
London (3)
Paris (3)
Stockholm (3)

Asia Pacific
Bahrain (3)
Hong Kong (3)
Mumbai (2)
Osaka (1)
Singapore (3)
Sydney (3)
Seoul (2)
Tokyo (4)

China
Beijing (3)
Ningxia (3)

Announced Regions: Cape Town, Jakarta, and Milan

AWS security solutions

Identity and access management

- AWS Identity and Access Management (IAM)
- AWS Organizations
- Amazon Cognito
- AWS Directory Service
- AWS Secrets Manager
- AWS Single Sign-On

Detective control

- AWS CloudTrail
- AWS Config
- Amazon CloudWatch
- Amazon GuardDuty
- VPC Flow Logs

Infrastructure security

- AWS Systems Manager
- AWS Shield
- AWS WAF – Web application firewall
- AWS Firewall Manager
- Amazon Inspector
- Amazon Virtual Private Cloud (Amazon VPC)

Data protection

- AWS Key Management Service (AWS KMS)
- AWS CloudHSM
- Amazon Macie
- AWS Certificate Manager (ACM)
- Server-side encryption

Incident response

- AWS Config Rules
- AWS Lambda

Identity and access management

Define, enforce, and audit user permissions across AWS services, actions, and resources.

AWS Identity and Access Management (IAM)
Securely control access to AWS services and resources

AWS Organizations
Leverage policy-based management for multiple AWS accounts

Amazon Cognito
Add user sign-up, sign-in, and access control to your web and mobile apps

AWS Directory Service
Use Managed Microsoft Active Directory in the AWS Cloud

AWS Secrets Manager
Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycles

AWS Single Sign-On
Centrally manage single sign-on (SSO) access to multiple AWS accounts and business applications

Detective control

Gain the visibility you need to spot issues before they impact the business; further, improve your security posture and reduce the risk profile of your environment.

AWS CloudTrail

Enable governance, compliance, and operational/risk auditing of your AWS account

AWS Config

Record and evaluate configurations of your AWS resources; enable compliance auditing, security analysis, resource change tracking, and troubleshooting

Amazon CloudWatch

Monitor AWS Cloud resources and your applications on AWS to collect metrics, monitor log files, set alarms, and automatically react to changes

Amazon GuardDuty

Employ intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads

VPC Flow Logs

Capture information about the IP traffic going to and from network interfaces in your VPC; flow log data is stored using Amazon CloudWatch Logs

Infrastructure security

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS.

AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure operating systems

AWS Shield

Make use of this managed DDoS protection service, which safeguards web applications running on AWS

AWS WAF – Web application firewall

Protect your web applications from common web exploits, ensuring availability and security

AWS Firewall Manager

Centrally configure and manage AWS WAF rules across accounts and applications

Amazon Inspector

Employ automation of security assessments to help improve the security and compliance of applications deployed on AWS

Amazon Virtual Private Cloud (Amazon VPC)

Provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define

Data protection

In addition to using our automatic data encryption and management services, employ more features for data protection.

AWS Key Management Service (AWS KMS)

Easily create and control the keys used to encrypt your data

AWS CloudHSM

Use a managed hardware security module (HSM) in the AWS Cloud

Amazon Macie

Use this machine learning-powered security service to discover, classify, and protect sensitive data

AWS Certificate Manager (ACM)

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services

Server-Side Encryption

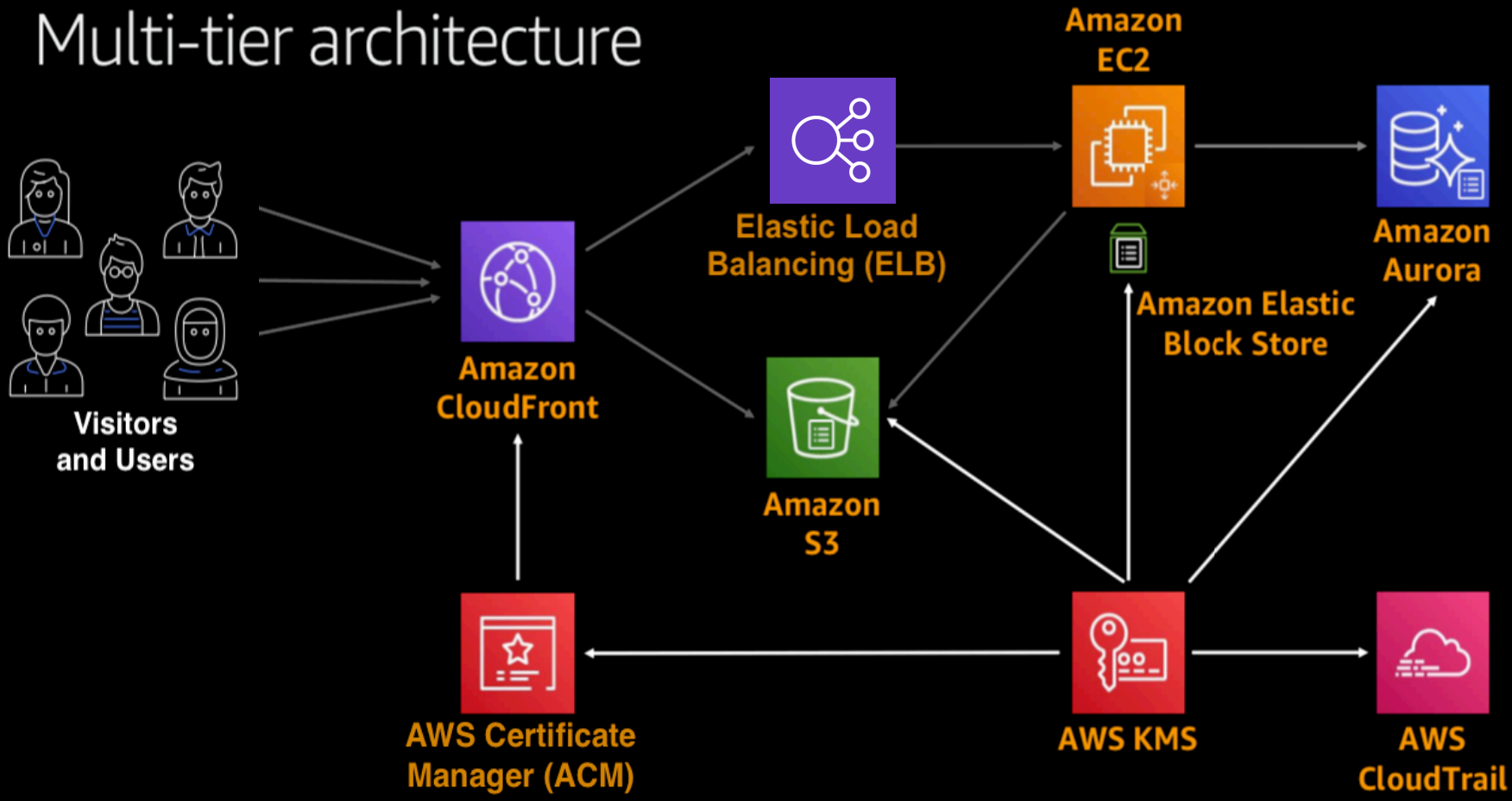
Take advantage of flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys

Benefits of protecting your data with encryption

- Provides security for data at all times
- Encrypted data maintains integrity
- Reduces incident risks
- Protects privacy
- Protects data across devices
- Keeps you ahead of competitors
- Encryption is part of Compliance (SOC, PCI, ISO, HIPAA, FIPS, DoD SRG, FedRAMP, SEC, CJIS, etc.)

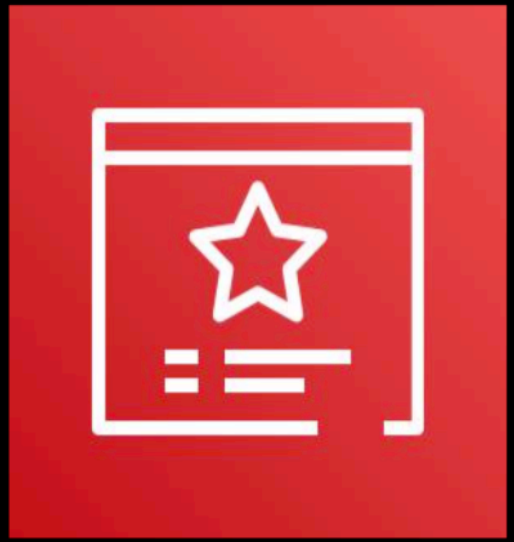
So how do we protect information?

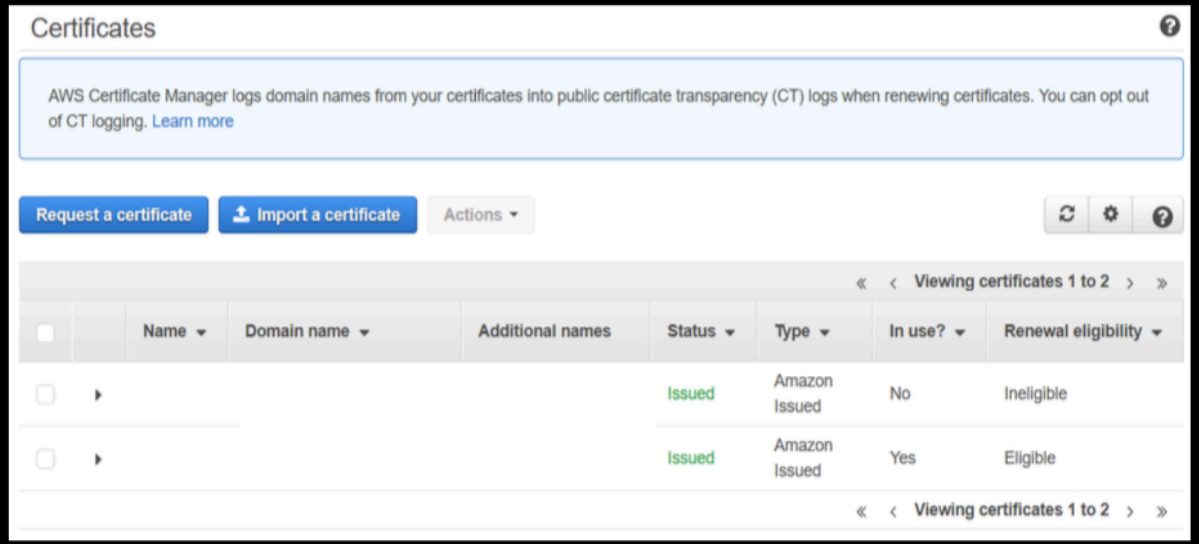
Multi-tier architecture



AWS Certificate Manager (ACM)

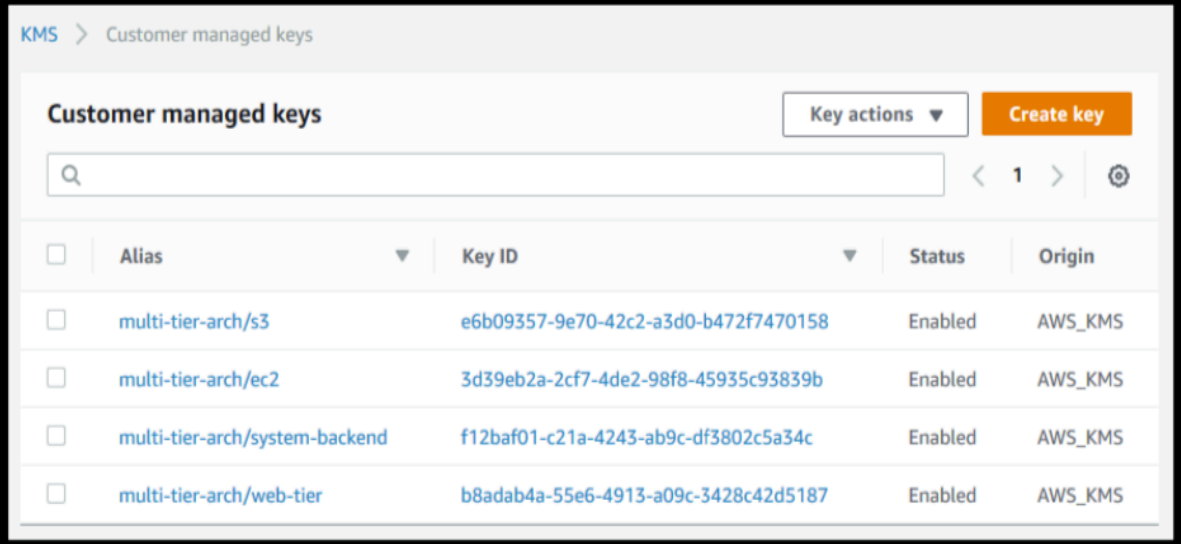
ACM makes it easy to provision, manage, and deploy public and private SSL/TLS certificates





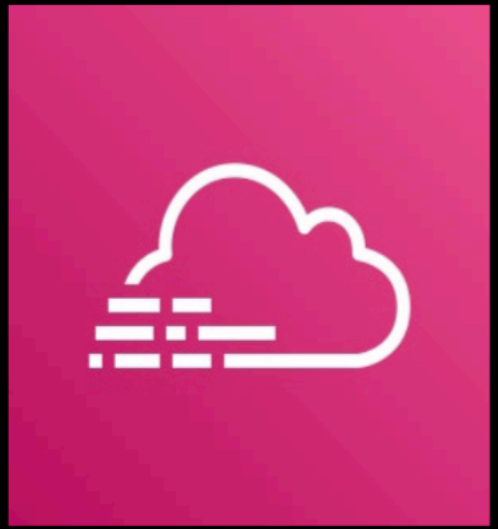
AWS Key Management Service (AWS KMS)

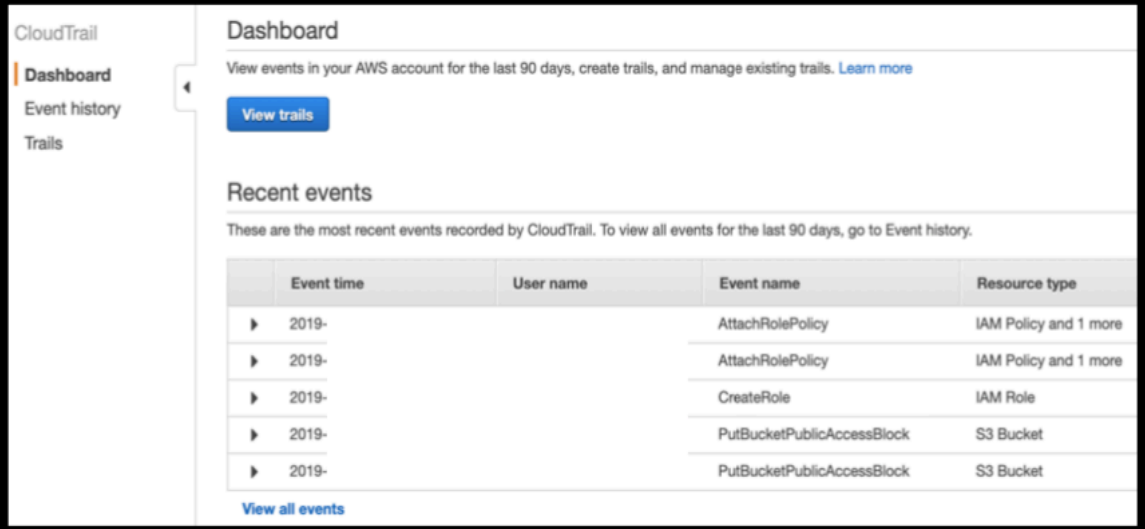
AWS KMS makes it easy to create and manage keys and control the use of encryption

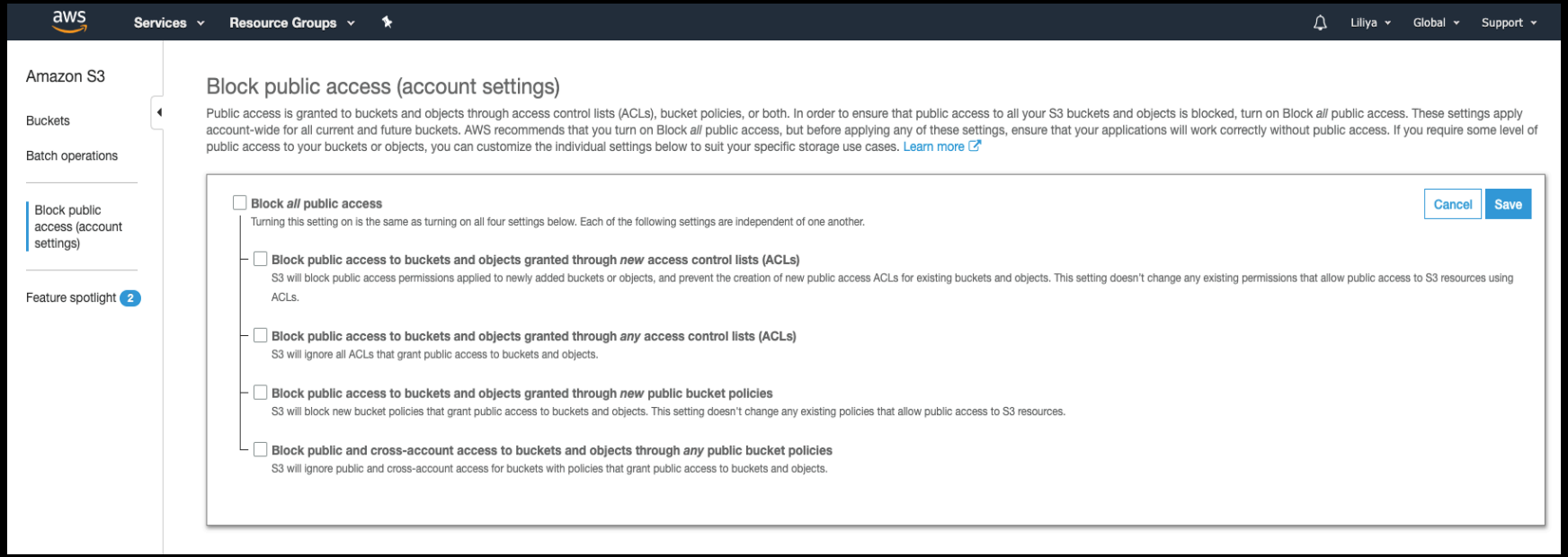


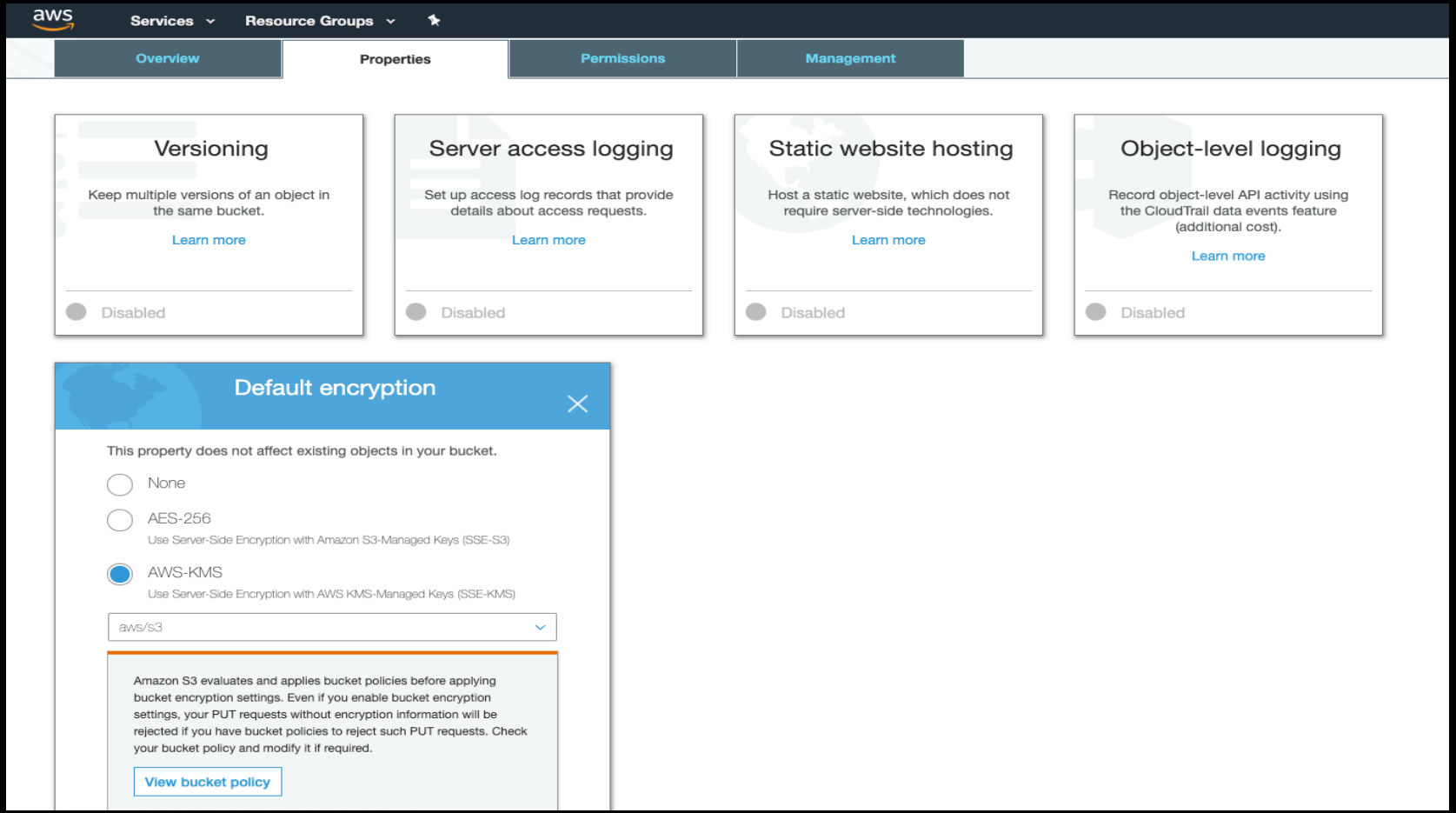
AWS CloudTrail

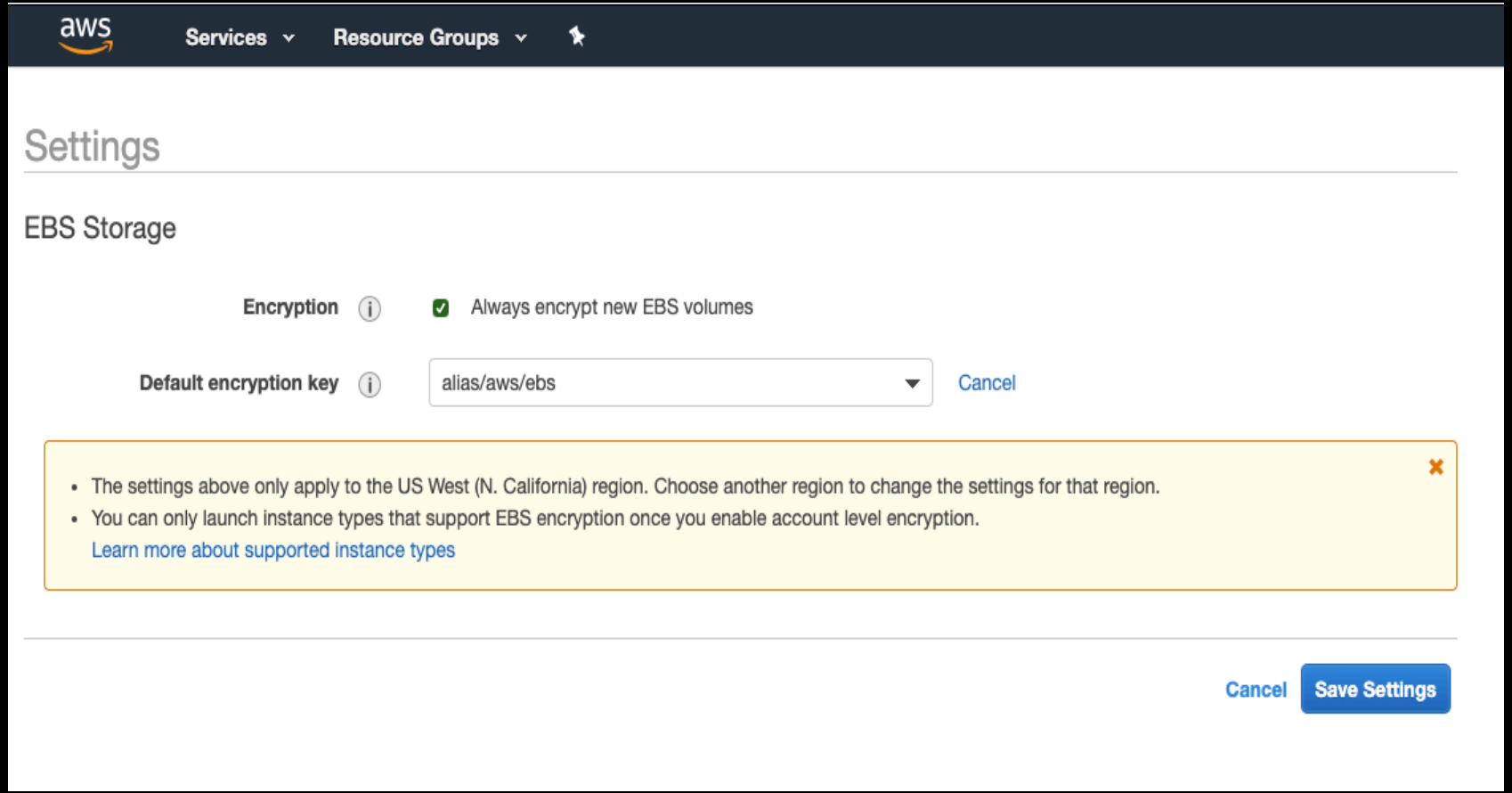
Service that records AWS API calls for your account and delivers logs






aws
Services
Resource Groups
Liliya
Global
Support
Amazon S3
Buckets
Batch operations
Block public access (account settings)
Feature spotlight 2
Block public access (account settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply account-wide for all current and future buckets. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Cancel
Save
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket policies
S3 will block new bucket policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket policies
S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.


aws
Services
Resource Groups
Overview
Properties
Permissions
Management
Versioning
Keep multiple versions of an object in the same bucket.
Learn more
Disabled
Server access logging
Set up access log records that provide details about access requests.
Learn more
Disabled
Static website hosting
Host a static website, which does not require server-side technologies.
Learn more
Disabled
Object-level logging
Record object-level API activity using the CloudTrail data events feature (additional cost).
Learn more
Disabled
Default encryption
This property does not affect existing objects in your bucket.
None
AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)
aws/s3
Amazon S3 evaluates and applies bucket policies before applying bucket encryption settings. Even if you enable bucket encryption settings, your PUT requests without encryption information will be rejected if you have bucket policies to reject such PUT requests. Check your bucket policy and modify it if required.
View bucket policy


aws
Services
Resource Groups
Settings
EBS Storage
Encryption
Always encrypt new EBS volumes
Default encryption key
alias/aws/ebs
Cancel
The settings above only apply to the US West (N. California) region. Choose another region to change the settings for that region.
You can only launch instance types that support EBS encryption once you enable account level encryption.
Learn more about supported instance types
Cancel
Save Settings

Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides these tools to automate aspects of this best practice.

AWS Config Rules

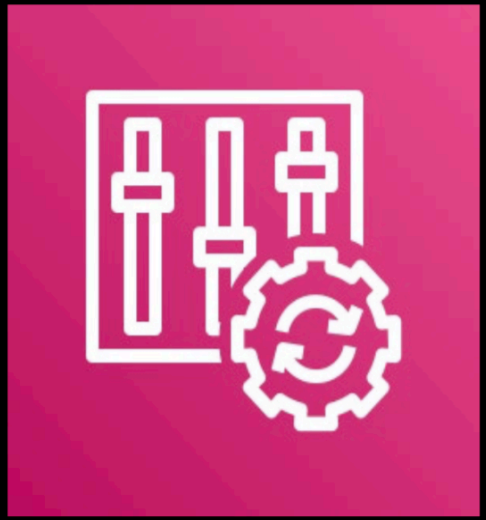
Create rules that automatically take action in response to changes in your environment, such as isolating resources, enriching events with additional data, or restoring configuration to a known good state

AWS Lambda

Use our serverless compute service to run code without provisioning or managing servers so you can scale your programmed, automated response to incidents

AWS Config

Assess, audit, and evaluate the configurations of your AWS resources



Automatic emails sent to security teams, when compliance rules fail in the real time

AWS Config Rules remediation

AWS Config now includes remediation capability with AWS Config Rules. This feature gives you the ability to associate and execute remediation actions with rules in AWS Config to address noncompliant resources. You can choose from a list of available remediation actions.

Just choose the remediation action you want to associate from a prepopulated list, or create your own custom remediation actions using AWS Systems Manager Automation documents.

Set up AWS Config

- Step 1: Settings
- **Step 2: Rules**
- Step 3: Review

AWS Config rules

75 Predefined Rules

AWS Config can check the configuration of your resources against rules that you define. Choose one or more of the following rules to get started. After setting up AWS Config, you can customize these rules, set up other rules provided by AWS Config, or create your own rules.

Learn more about AWS Config rules and pricing details.

Filter by rule name, label or description

« ‹ **Viewing 1 - 9 of 75 AWS managed rules** › »

Select all 75 | Clear all

acm-certificate-expiration-check

Checks whether ACM Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed.

ACM

alb-http-to-https-redirection-check

Checks whether HTTP to HTTPS redirection is configured on all HTTP listeners of Application Load Balancers. The rule is NON_COMPLIANT if one or more HTTP

EC2 . ELB

api-gw-cache-enabled-and-encrypted

Checks that all methods in Amazon API Gateway stages have cache enabled and cache encrypted. The rule is NON_COMPLIANT if any method in Amazon

API Gateway . REST API

autoscaling-group-elb-healthcheck-re...

Checks whether your Auto Scaling groups that are associated with a load balancer are using Elastic Load Balancing health checks.

AutoScaling

cloud-trail-cloud-watch-logs-enabled

Checks whether AWS CloudTrail trails are configured to send logs to Amazon CloudWatch logs. The trail is non-compliant if the CloudWatchLogsLogGroupArn property

CloudTrail . Periodic

cloud-trail-encryption-enabled

Checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The

CloudTrail . Periodic

cloud-trail-log-file-validation-enabled

Checks whether AWS CloudTrail creates a signed digest file with logs. AWS recommends that the file validation must be enabled on all trails. The rule is noncompliant

CloudTrail . Periodic

cloudformation-stack-notification-check

Checks whether your CloudFormation stacks are sending event notifications to an SNS topic. Optionally checks whether specified SNS topics are used.

CloudFormation

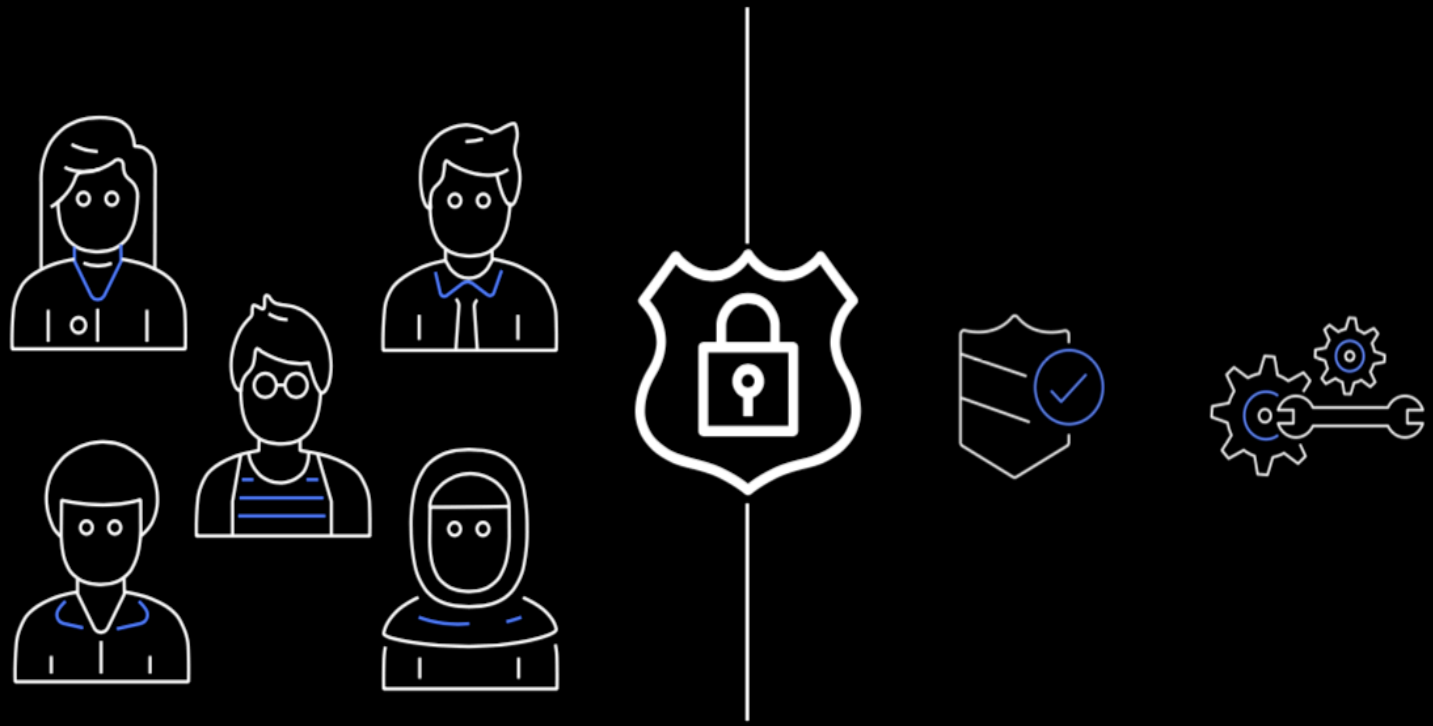
cloudtrail-enabled

Checks whether AWS CloudTrail is enabled in your AWS account.

CloudTrail . Periodic

You can customize these rules and add other rules after completing the setup process.

Keep humans away from your security and scaling



Benefits of automating your security remediation

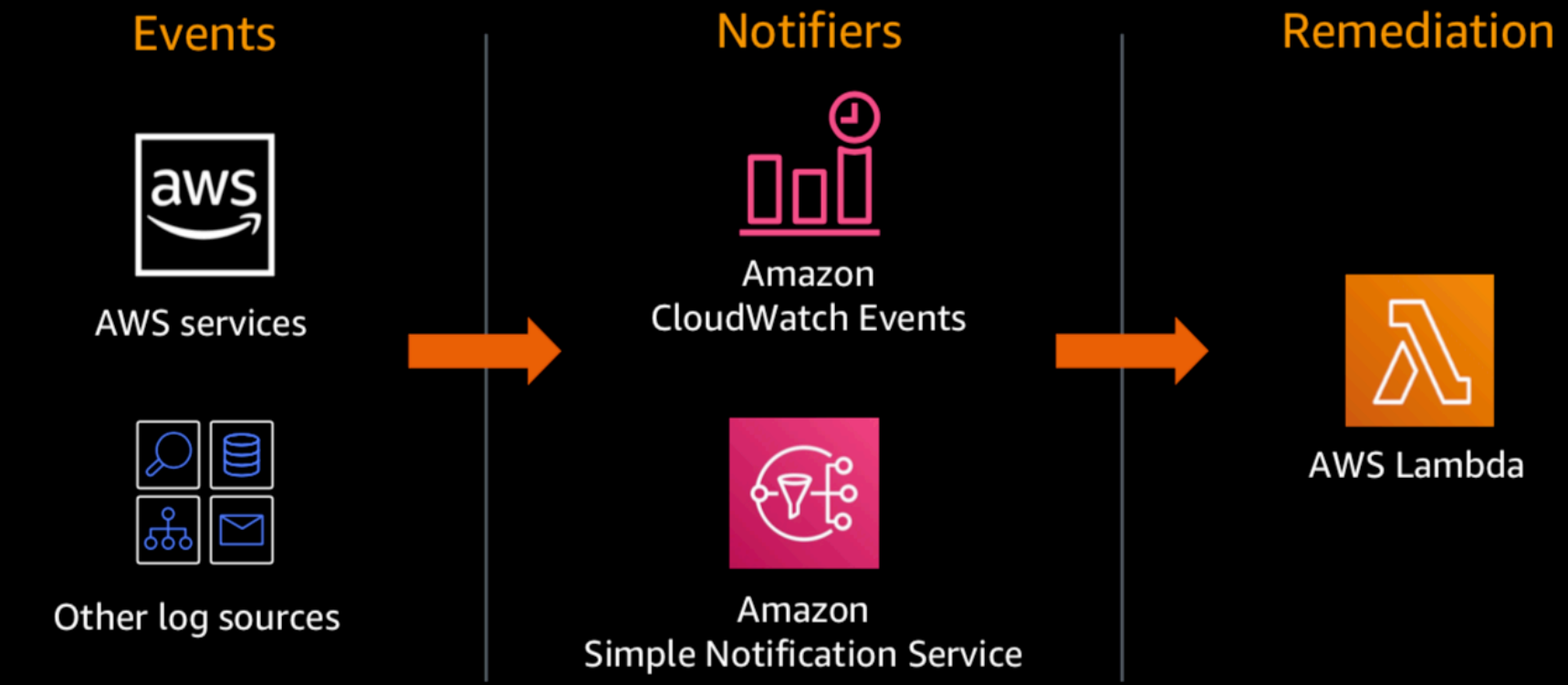
- Automation removes the potential for human error
- It works around the clock, and on weekends and holidays
- Automation enables a self-healing environment
- Multiple incidents can be responded to in parallel
- It allows DevSecOps and other teams to better utilize their time for high-level security tasks

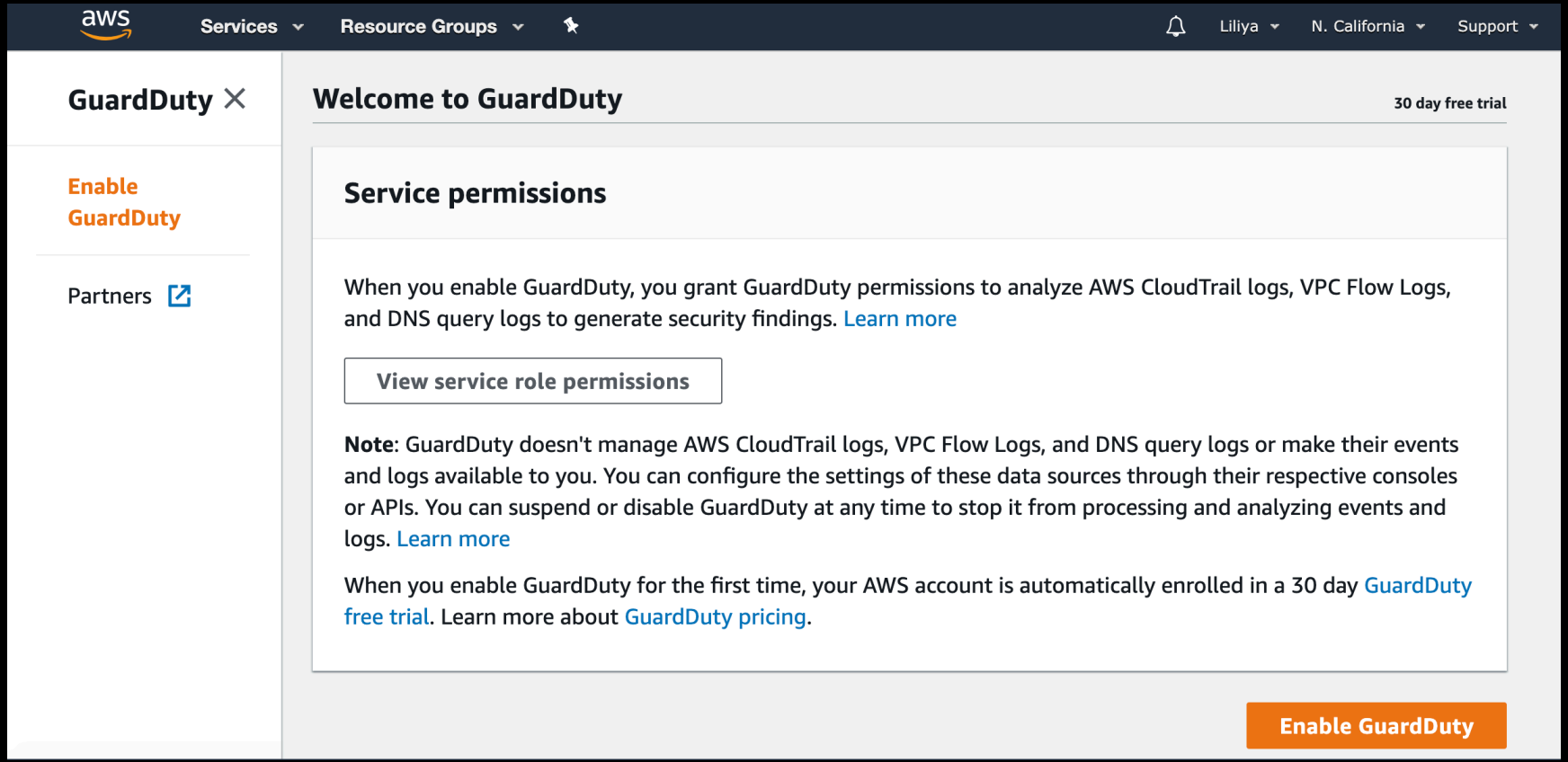
How do we scale security?

- Invest in end-to-end automation via pipelines
- Code and containers builds
- Security via DevSecOps
- Deployments

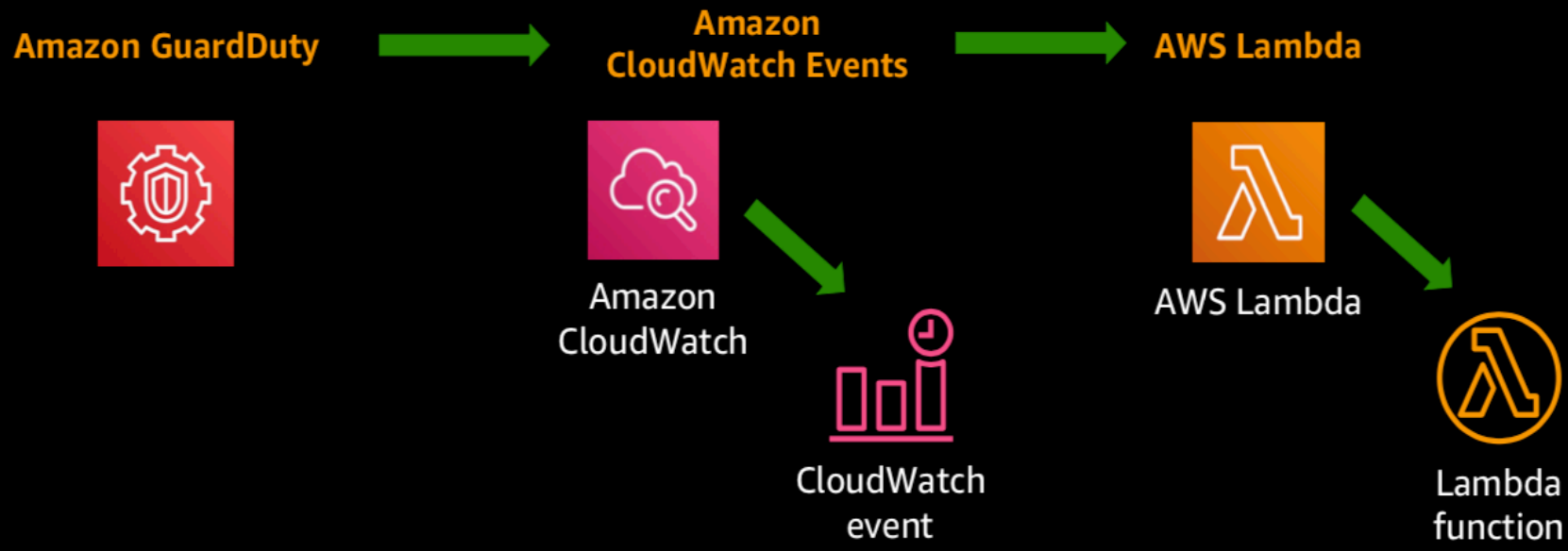
Make it fast and easy for your team to do the right thing. Because if you don't, people will often just go around the rules/restrictions to get their work done.

Build repeatable serverless automation patterns

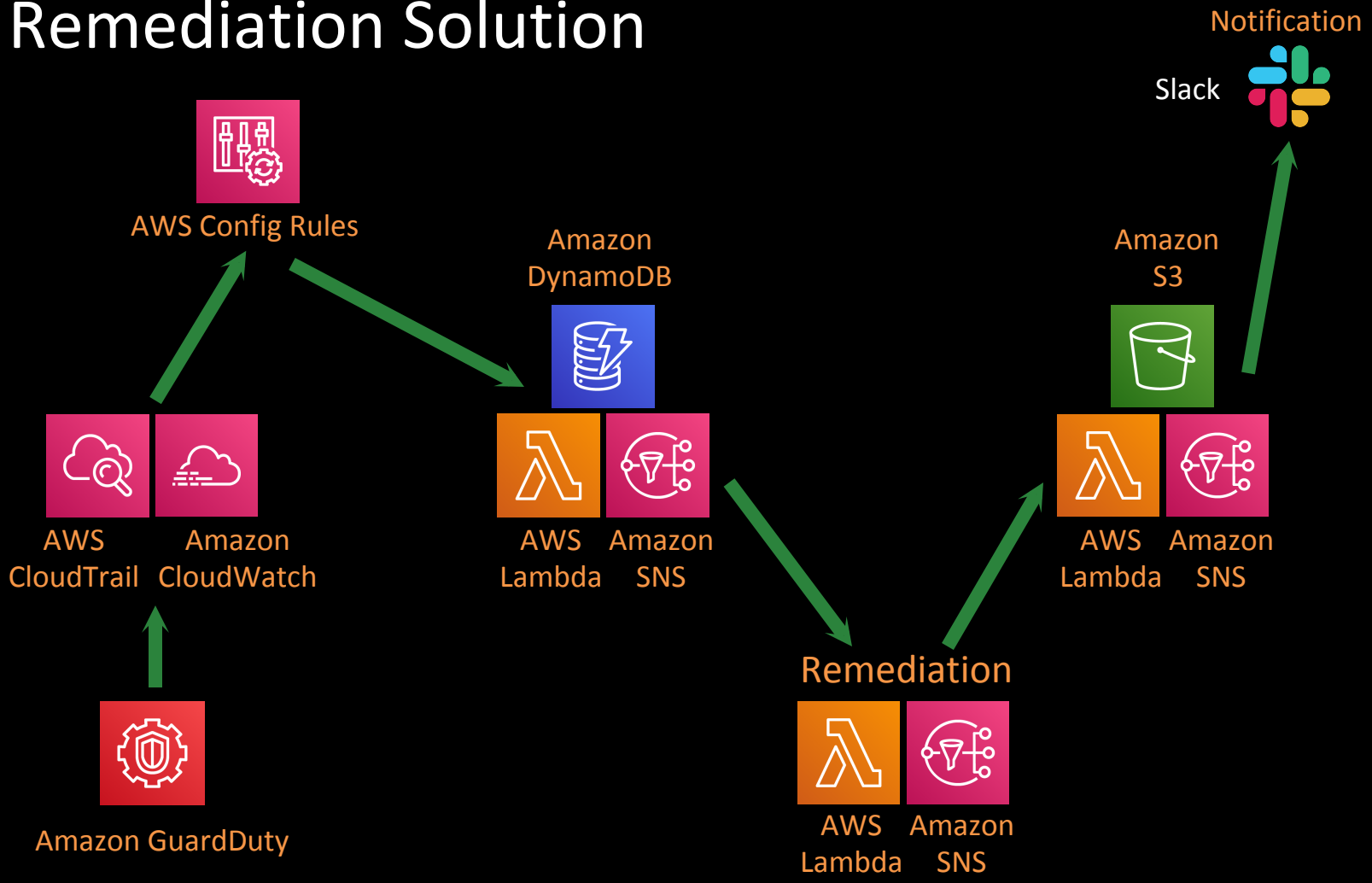



aws
Services
Resource Groups
Liliya
N. California
Support
GuardDuty
Enable GuardDuty
Partners
Welcome to GuardDuty
30 day free trial
Service permissions
When you enable GuardDuty, you grant GuardDuty permissions to analyze AWS CloudTrail logs, VPC Flow Logs, and DNS query logs to generate security findings. Learn more
View service role permissions
Note: GuardDuty doesn't manage AWS CloudTrail logs, VPC Flow Logs, and DNS query logs or make their events and logs available to you. You can configure the settings of these data sources through their respective consoles or APIs. You can suspend or disable GuardDuty at any time to stop it from processing and analyzing events and logs. Learn more
When you enable GuardDuty for the first time, your AWS account is automatically enrolled in a 30 day GuardDuty free trial. Learn more about GuardDuty pricing.
Enable GuardDuty

Automate with integrated services



Remediation Solution



Outcomes

Drastically improved coverage

Significant reduction in time to remediate

Increased transparency, more engaged delivery teams

Scalability with extremely low operating costs

AWS Config Pricing

You pay $0.003 per configuration item recorded in your AWS account per AWS Region. A configuration item is recorded whenever a resource undergoes a configuration change or a relationship change. A relationship defines how a resource is related to other AWS resources within an AWS account. You can stop recording configuration items at any time and still continue to access the previously recorded configuration items.

AWS Config rules

Effective August 1, 2019, you are charged based on the number of AWS Config rules evaluations recorded, instead of the number of active rules in your account per region. A rule evaluation is recorded every time a resource is evaluated for compliance against an AWS Config rule.

AWS Config rules evaluations	**Price**
First 100,000 rule evaluations	$0.001 per rule evaluation per region
Next 400,000 rule evaluations (100,001-500,000)	$0.0008 per rule evaluation per region
500,001 rule evaluations and more	$0.0005 per rule evaluation per region

Pricing example

Let's assume you have the following usage in US East (N.Virginia) Region in a given month.

10,000 Configuration items recorded across various resource types

100 Config rules- with 60 active rules in the month.

- 50 Config rules that invoked 500 rule evaluations each
- 9 Config rules that invoked 1000 rule evaluations each
- 1 Config rule that invoked 10,000 rule evaluations

Total Config Bill

$74 = (10,000 * $0.003) + ((50 * 500)+(9 * 1000) + (1 * 10,000) * $0.001)

Solution

- Block public access to your S3 buckets and objects with Amazon S3 Block Public Access and turn ON encryption for your S3 buckets
- Turn ON default encryption for your new Amazon EBS volumes
- Enable AWS detective security controls today: AWS CloudTrail, AWS Config, Amazon GuardDuty
- Enable detective controls that map to your organization's cloud/IT security policy to detect compliance in real time (AWS Config rules).
- Configure alerts to be sent via the most appropriate channel to get to your DevSecOps team as fast as possible. Integrate to existing workflow management tools. (JIRA, Slack, email, SMS, API)
- Automate the response to security events to scale your DevSecOps team!

Thank you

Resources:
https://aws.amazon.com/whitepapers/
https://aws.amazon.com/about-aws/global-infrastructure/
https://aws.amazon.com/mp/Security_Solutions_Overview/
https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html
https://docs.aws.amazon.com/config/latest/developerguide/remediation.html
https://aws.amazon.com/config/pricing/

Let’s all continue to work together to make the cloud ecosystem the most advanced and secure in the world.

Stay safe and secure!