

# Welcome to AWS Security and Cost Management

AWS SECURITY AND COST MANAGEMENT CONCEPTS



Dev Bhosale

Principal Data & Cloud Architect

# The structure of this course

Chapter 1  
Introduction to  
AWS Security



Chapter 2  
Security  
Best Practices



Chapter 3  
Billing and  
Cost Management



# The structure of this course

Chapter 1  
Introduction to  
AWS Security



Chapter 2  
Security  
Best Practices



Chapter 3  
Billing and  
Cost Management



# The structure of this course

Chapter 1  
Introduction to  
AWS Security



Chapter 2  
Security  
Best Practices



Chapter 3  
Billing and  
Cost Management



# Prerequisites

- No technical experience needed
- A basic understanding of AWS could help

INTERACTIVE COURSE

## Introduction to AWS

[Continue](#) [Bookmark](#)

• Beginner 2 hours 12 videos 39 exercises 10,584 participants **2650 XP**

# Course Format

The screenshot shows the AWS Console Home page. At the top, there is a navigation bar with the AWS logo, a 'Services' dropdown, a search bar containing 'Search', a keyboard shortcut '[Option+S]', and account information for 'datacamp-learner-user @ 3397-1279-7442'. Below the navigation bar, the main content area has a title 'Console Home' with an 'Info' link. On the right side of the main area, there are two buttons: 'Reset to default layout' and '+ Add widgets'. The main content is divided into several sections:

- Recently visited:** A list of recently used services including S3, IAM Identity Center, AWS Billing Conductor, Secrets Manager, Trusted Advisor, Security Hub, Lambda, CloudWatch, and Certificate Manager. Each service has a small icon and a blue link.
- Applications (0):** A section titled 'Applications (0)' with an 'Info' link. It shows the region as 'US East (N. Virginia)'. It includes a dropdown for 'us-east-1 (Current Region)', a search bar for 'Find applications', and navigation arrows (< 1 >). The table headers are 'Name', 'Description', 'Region', and 'Originating account'. A message below the table says 'No applications' and 'Get started by creating an application.' with a 'Create application' button.
- Welcome to AWS:** A section with a 'Welcome to AWS' message and a 'View all services' link.
- AWS Health:** A section with an 'AWS Health' link.
- Cost and usage:** A section with a 'Cost and usage' link.

# **Let's practice!**

**AWS SECURITY AND COST MANAGEMENT CONCEPTS**

# AWS Shared Responsibility Model

AWS SECURITY AND COST MANAGEMENT CONCEPTS

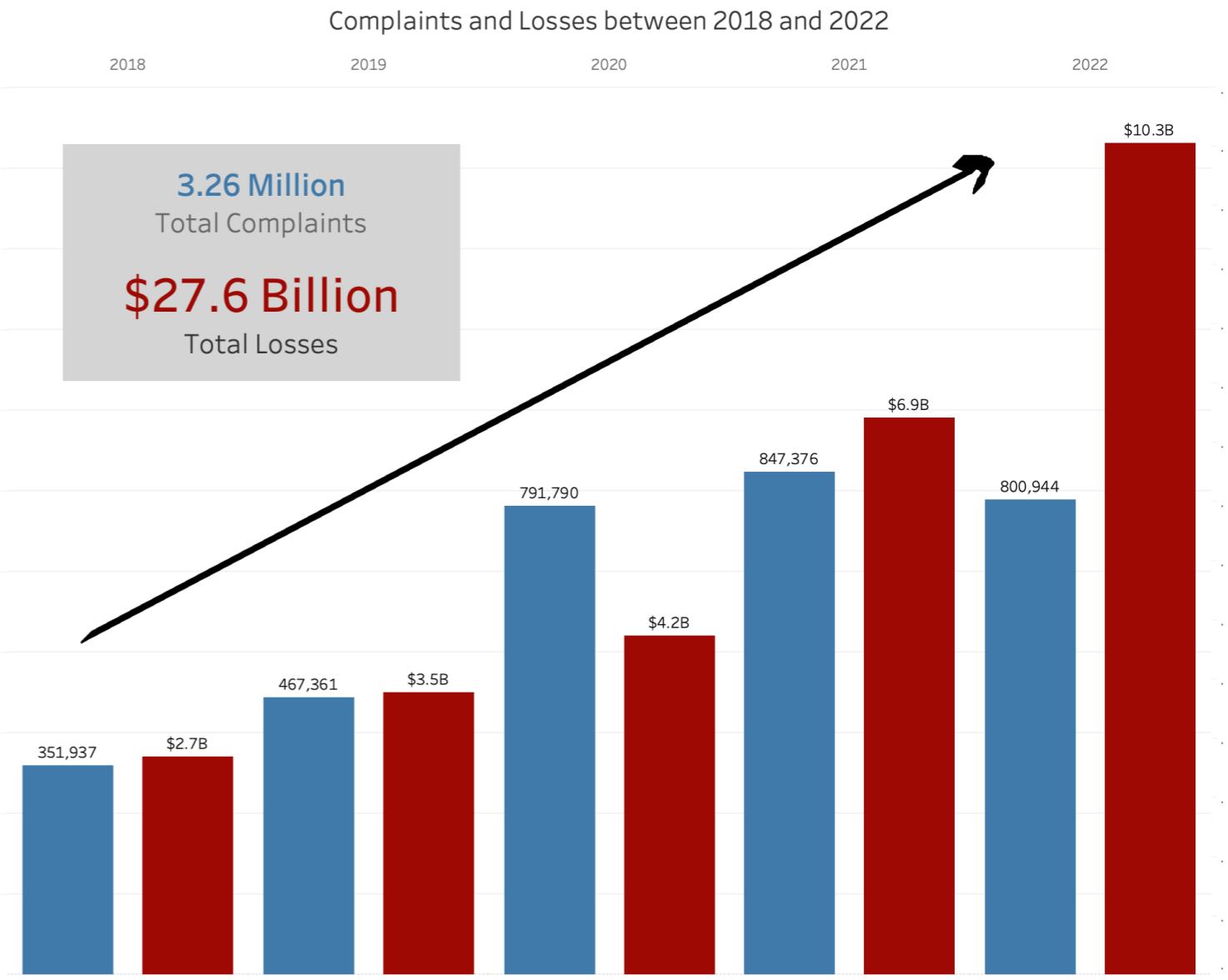


Dev Bhosale

Principal Data & Cloud Architect

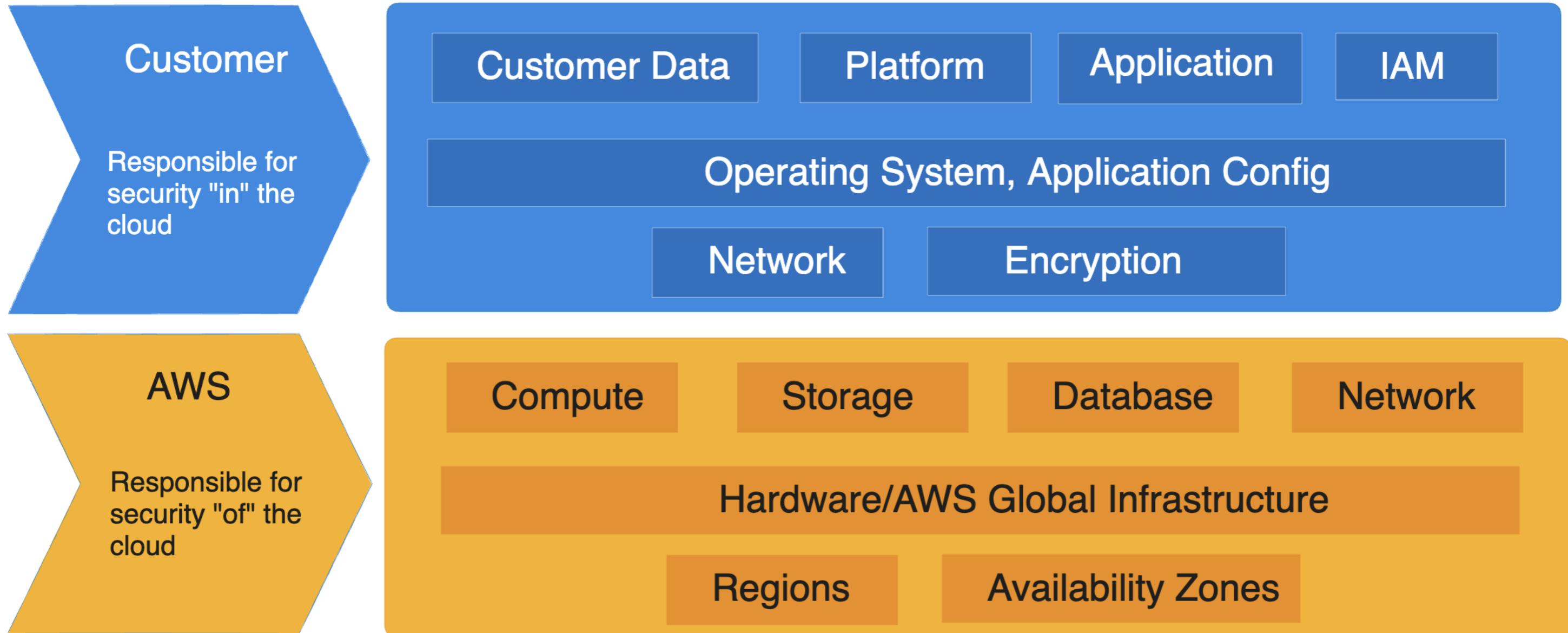
# Why cloud security is important?

- Sensitive data
- Reputation risk
- Compliance requirement
- Financial consequences



<sup>1</sup> <https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/>

# Shared responsibility model

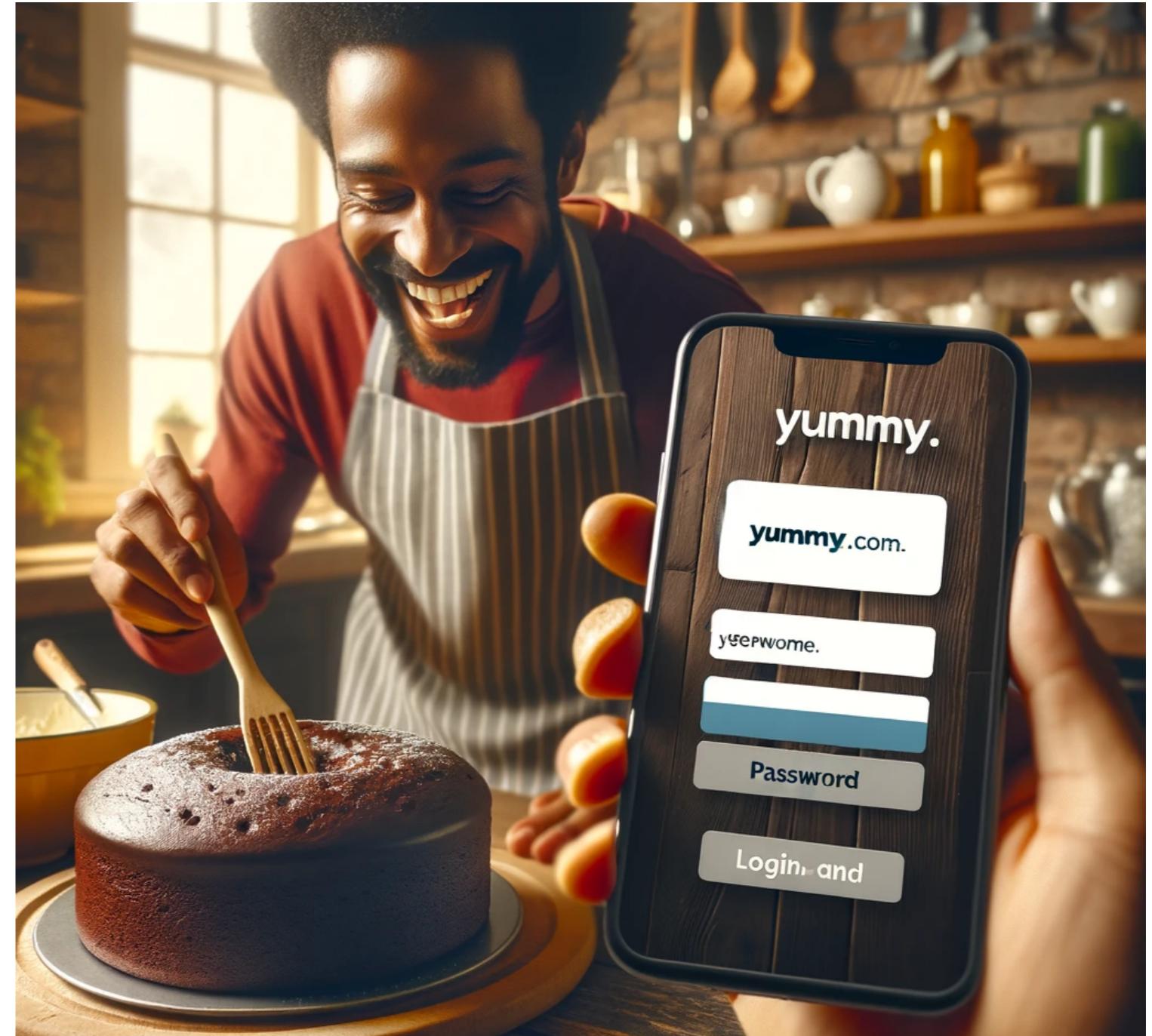


# Shared responsibility model



# Security in the cloud - Customer responsibilities

- Credentials to server
- Database access
- Application software installed on server
- Encryption keys



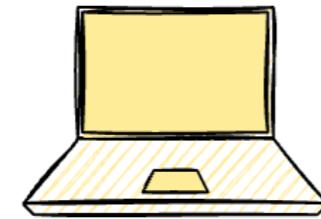
# Security of the cloud - AWS responsibilities



- Access to building and equipment
- Network connectivity
- Power backup
- Infrastructure software (e.g. routing)

# How responsibilities change?

## Servers



(EC2, etc.)

Customer Data

Server, encryption, OS Updates for servers

Network & firewall configuration

- With servers, customers are responsible for server security and updates.
- In serverless offerings such as Lambda, AWS manages server security and updates.

## Serverless



Glue



Lambda

(Glue, Lambda, etc.)

Customer Data

Network & firewall configuration

# **Let's practice!**

**AWS SECURITY AND COST MANAGEMENT CONCEPTS**

# AWS compliance and governance

AWS SECURITY AND COST MANAGEMENT CONCEPTS

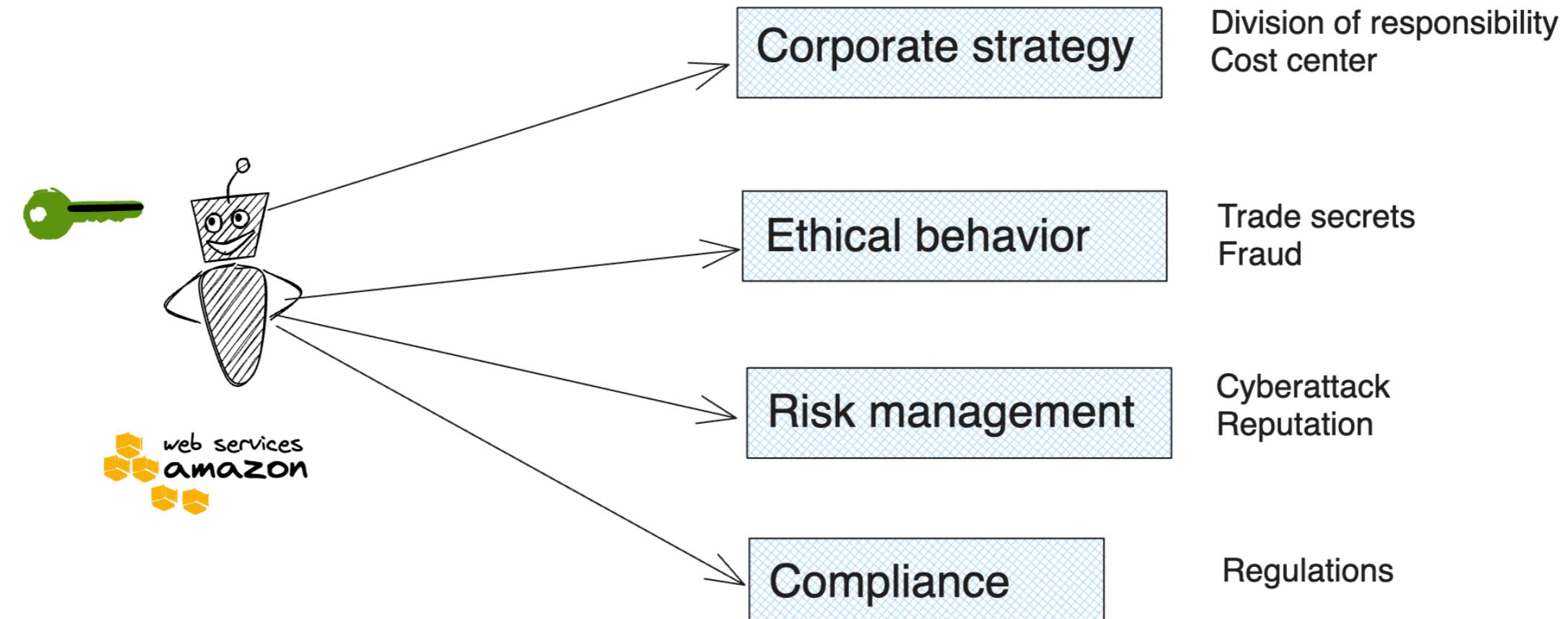


Dev Bhosale

Principal Data & Cloud Architect

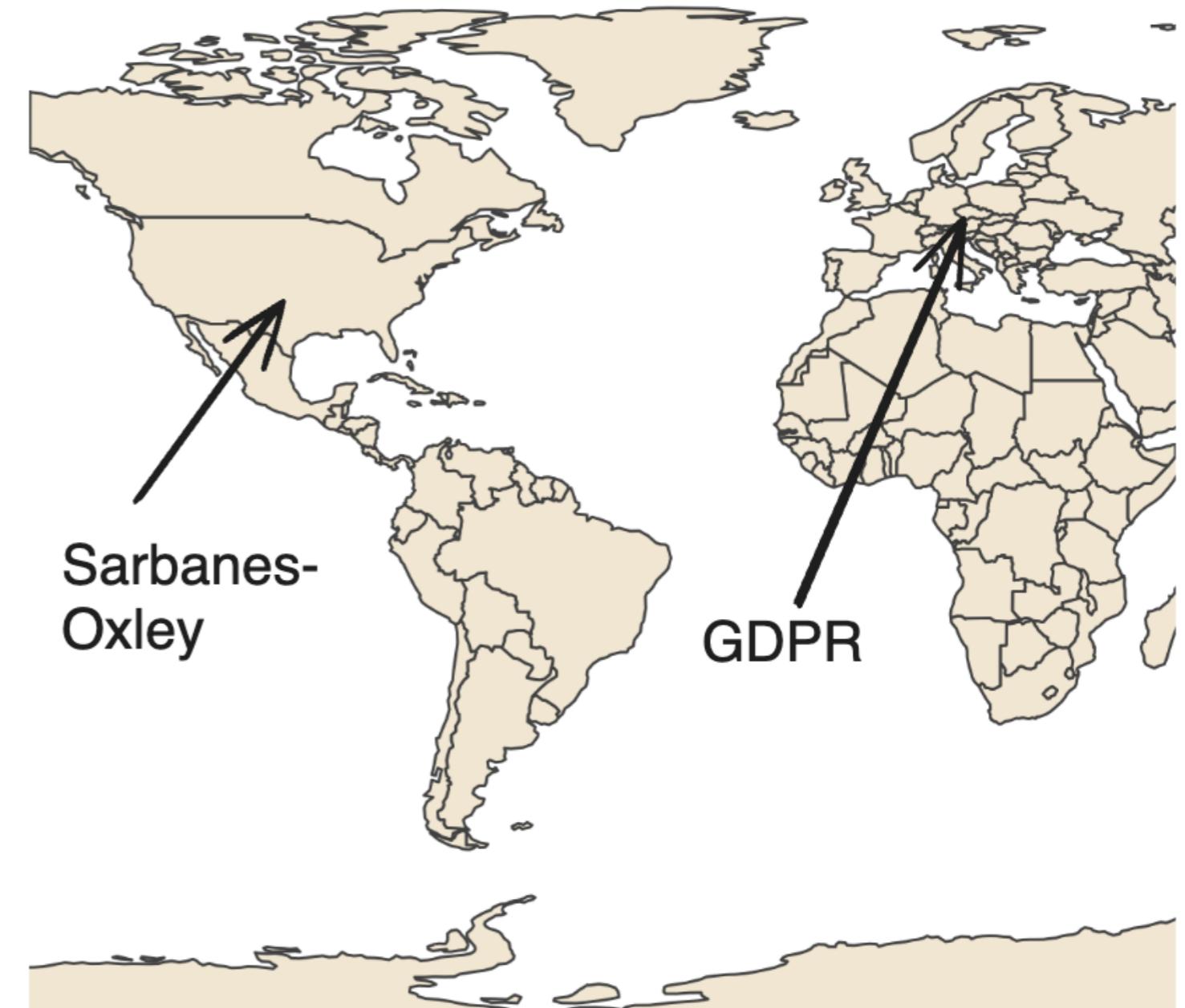
# Cloud governance

What is cloud governance?



# Regulations around the world

- Large companies are required to comply with regulations around the world
- Sarbanes-Oxley for accounting applies to all public companies in the US
- GDPR for consumer data protection applies to large companies in Europe



# Governance functions

- Identify critical resources and governance model
- Detect anomalies & malicious activities
- Protect data and assets
- Respond through incident response planning
- Recover to the prior condition (for data loss/attack)



Identify



Protect



Detect



Recover



Respond

# AWS tools for governance

Identify



 Organizations

 Security Hub

 Config

 Trusted Advisor

 Systems Manager

 Control Tower

Protect



 Shield

 Certificate Manager

 KMS

 Firewall

 WAF

 CloudHSM

Detect



 GuardDuty

 Macie

 Inspector

 Security Hub

 CloudWatch

 Lambda

 Detective

 CloudTrail

 Systems Manager

 Step Functions

Respond



 CloudWatch

 Lambda

 Detective

 CloudTrail

 Systems Manager

 Step Functions

Recover



 OpsWorks

 CloudFormation

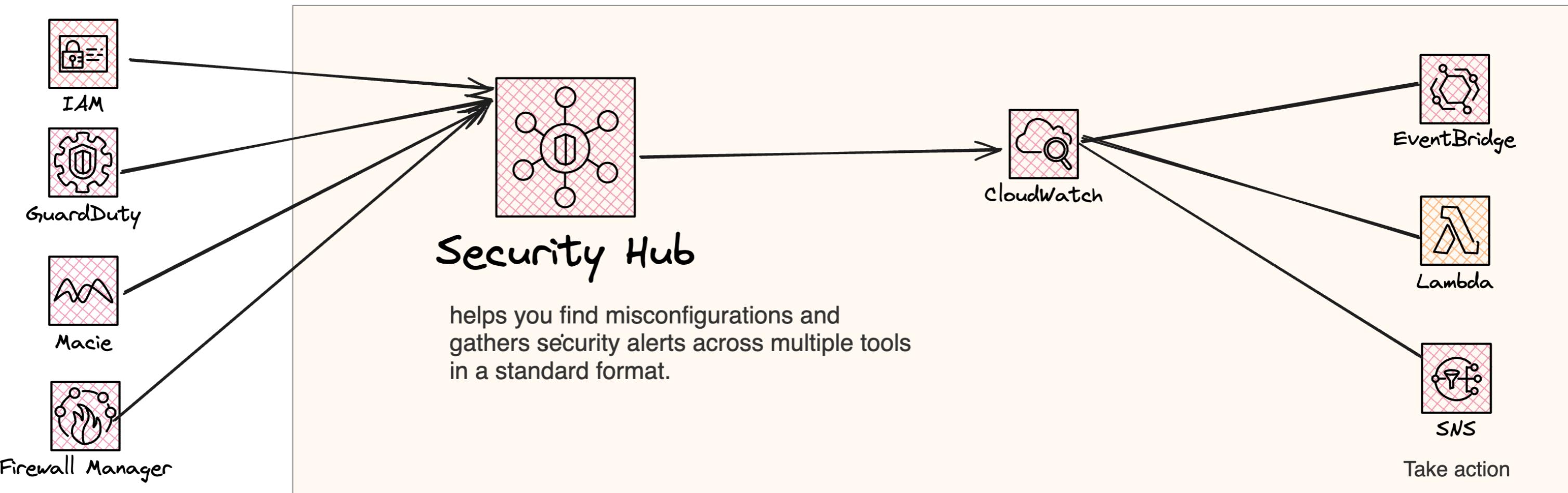
 Glacier

 Snapshot

 Archive

 CloudEndure

# Threat identification



- Continuously checks your AWS resources for security best practices
- Find misconfigurations and gathers security alerts

# Tools for protection



## Shield

aws Services Search [Option+S] Global DataCamp

**WAF & Shield** X

Getting started > Global threat dashboard

### Global threat dashboard across all AWS customers

The following is a sampling of the most significant attacks that AWS is monitoring and mitigating for customers on Amazon EC2, Amazon CloudFront, Elastic Load Balancing, and Amazon Route 53.

Select global threat period

Last Two Weeks

#### Attack frequency map

AWS WAF

- Getting started
- Web ACLs
- Bot control dashboard
- Application integration New
- IP sets
- Regex pattern sets
- Rule groups
- AWS Marketplace managed rules

Switch to AWS WAF Classic

**AWS Shield**

- Getting started
- Overview
- Protected resources
- Events
- Global threat dashboard



## IAM

aws Services Search [Option+S] Global DataCamp

**Identity and Access Management (IAM)** X

Identity and Access Management (IAM) Dashboard

Search IAM

#### Dashboard

**Access management**

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

**Access reports**

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report
- Organization activity
- Service control policies (SCPs)

**Security recommendations** 1

- Add MFA for root user
- Root user has no active access keys

**IAM resources**

Resources in this AWS Account

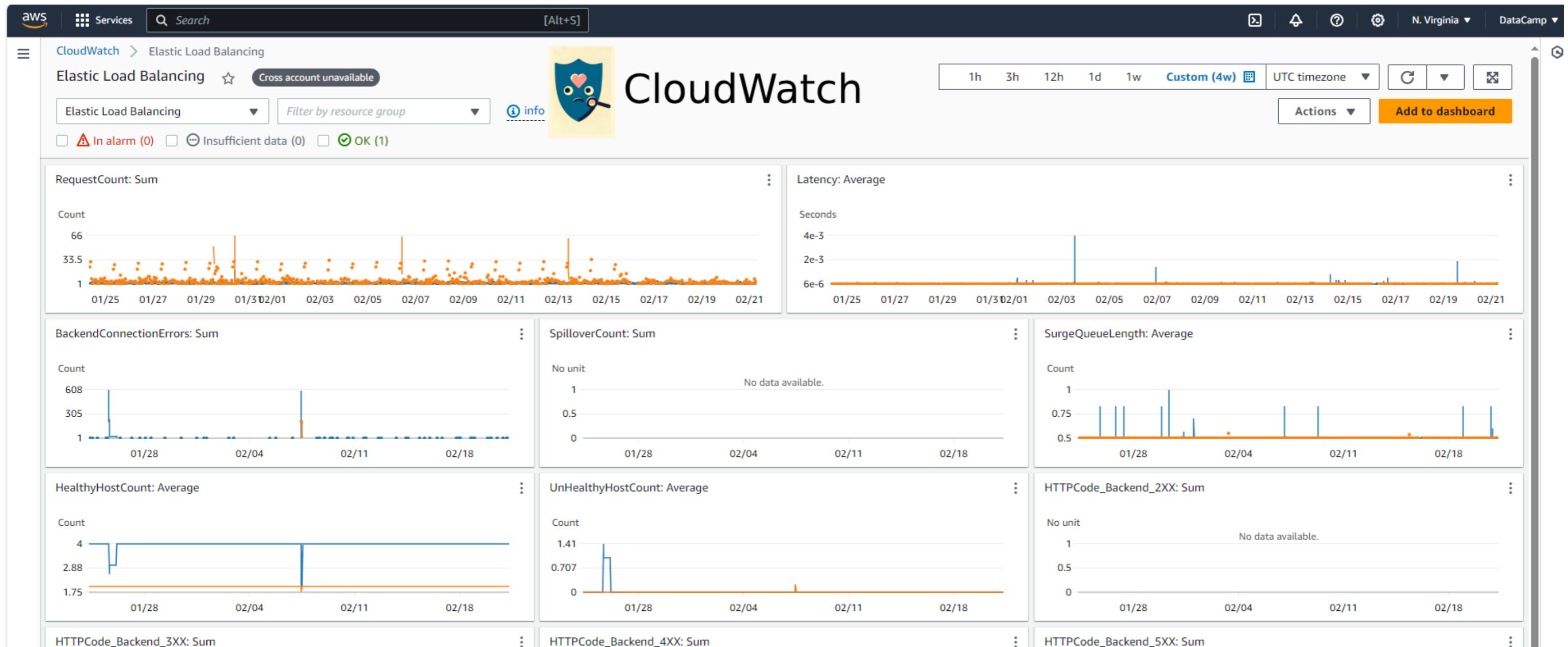
User groups	Users	Roles	Policies	Identity providers
7	16	35	11	0

**What's new** View all

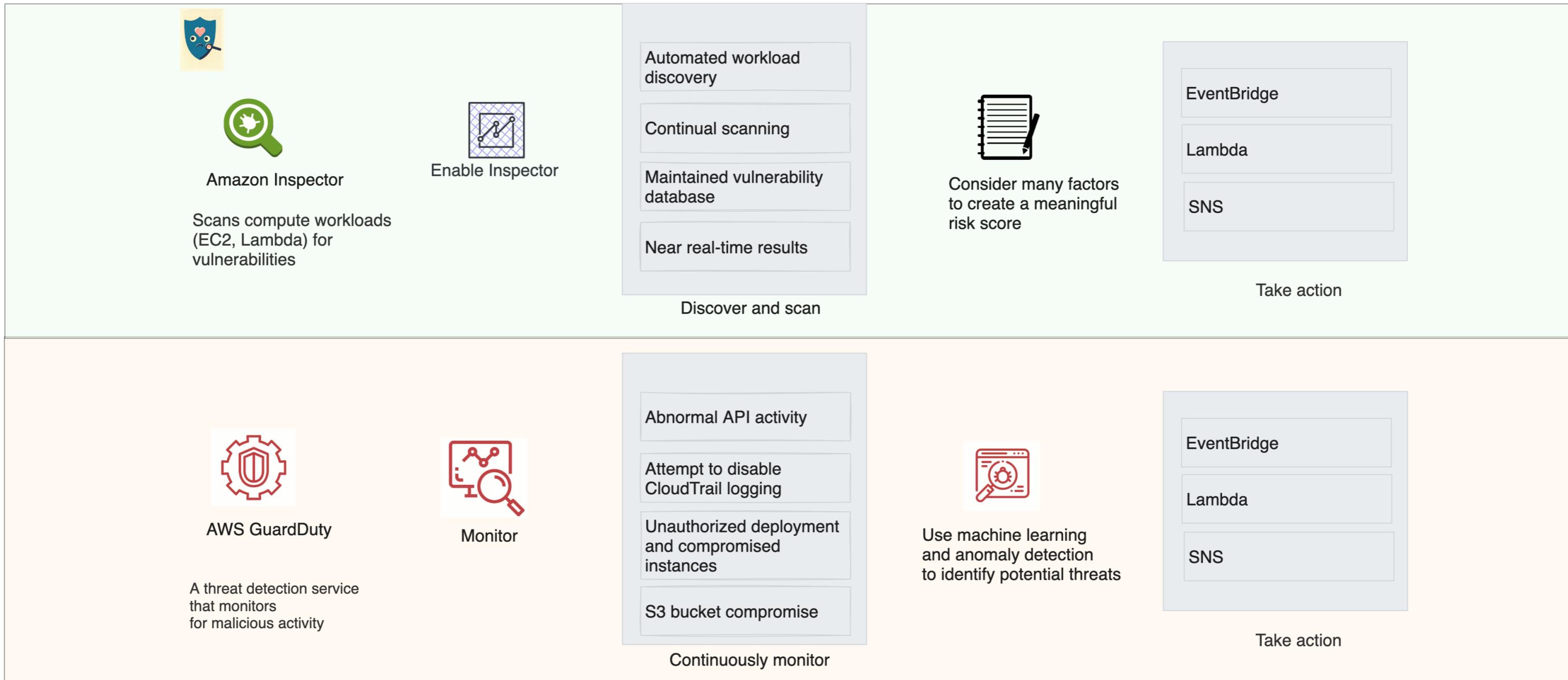
Updates for features in IAM

# Detect malicious activities

- Detect anomalies and malicious activities with continuous monitoring from CloudWatch



# Detect malicious activities



# Respond and recover



CloudWatch

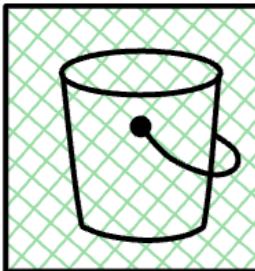
- Tracks user activity and API usage
- Records major events that modify or delete resources
- Helps with operational troubleshooting by keeping detailed logs.

# Respond and recover



CloudWatch

- Tracks user activity and API usage
- Records major events that modify or delete resources
- Helps with operational troubleshooting by keeping detailed logs.



S3 Glacier

- Archival storage solution built on S3 for long-term data storage.
- Optimized for large volumes with infrequent and slower retrieval times.
- Offers multiple retrieval options based on specific use cases.

# **Let's practice!**

**AWS SECURITY AND COST MANAGEMENT CONCEPTS**

# Security and compliance automation

AWS SECURITY AND COST MANAGEMENT CONCEPTS

Dev Bhosale

Principal Data & Cloud Architect



# AWS Security and compliance tools

Identify



Organizations



Organizations

Security Hub



Security Hub

Config



Config

Trusted Advisor



Trusted Advisor

Systems Manager



Systems Manager

Control Tower



Control Tower

Protect



Shield



Certificate Manager



KMS



Firewall



WAF



CloudHSM



Detect



GuardDuty



Macie



Inspector



Security Hub



CloudTrail



Systems Manager



Step Functions



Respond



CloudWatch



Lambda



Detective



CloudTrail



Systems Manager



Step Functions



Recover



OpsWorks



CloudFormation



Glacier



Snapshot



Archive



CloudEndure

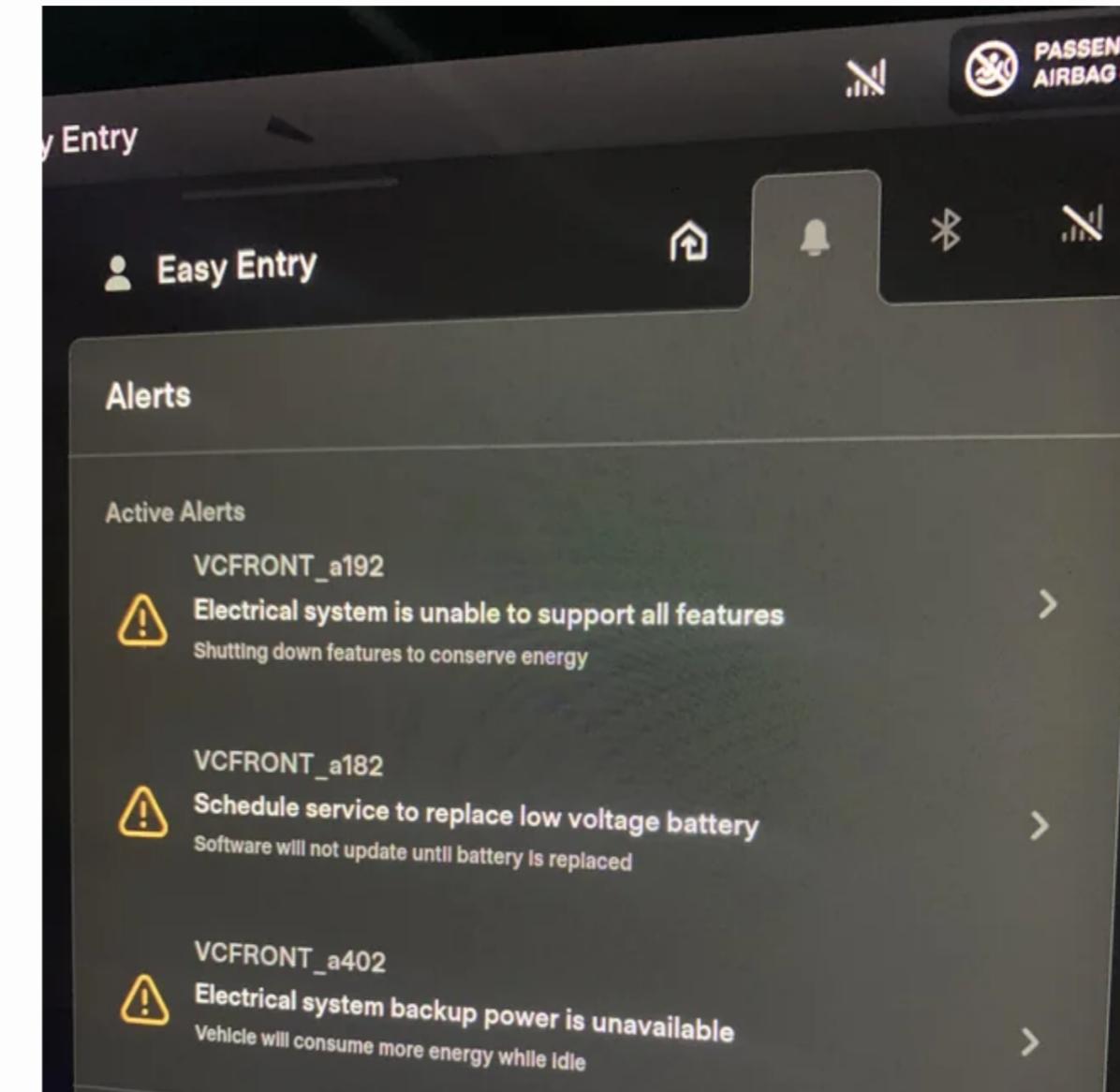


# Long checklist vs a dashboard

# The old way

UNDER VEHICLE			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Shock Absorbers / Suspension / Struts
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Steering Box, Linkage, Ball Joints, Dust Covers
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Muffler, Exhaust Pipes/Mounts, Catalytic Converter
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Engine Oil and Fluid Leaks
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Brakes Lines, Hoses, Parking Brake Cable
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Drive Shaft Boots, Constant Velocity Boots, U-Joint Transmission Linkage (if equipped)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Transmission, Differential, Transfer Case, (Check Fluid Level, Fluid Condition, and Fluid Leaks)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Fluid Lines and Connections, Fluid Tank Band, Fuel Tank Vapor Vent Systems Hoses
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Inspect Nuts and Bolts on Body and Chassis

# The new way



# AWS Security Hub Overview

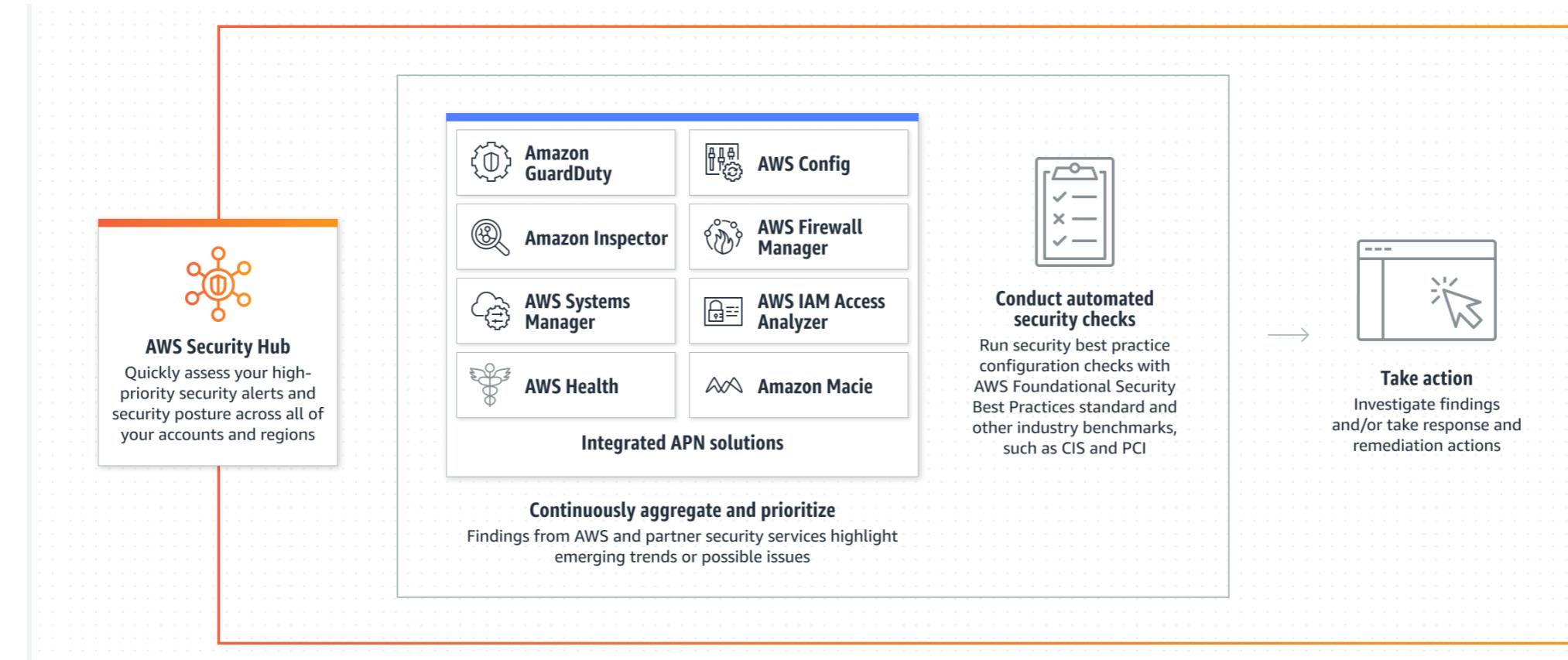
The screenshot shows the AWS Security Hub interface. The left sidebar includes sections for Summary, Controls, Security standards, Insights, Findings, Integrations, Management (Automations, Custom actions), and Settings (General, Regions, Configuration, Usage). The main content area is titled "Summary" and shows two main sections: "Security standards" and "Assets with the most findings".

**Security standards:** Displays a summary score and lists two benchmarks: "AWS Foundational Security Best Practices v1.0.0" and "CIS AWS Foundations Benchmark v1.2.0", both showing 0 Passed, 0 Failed, and 0% Score.

**Assets with the most findings:** Shows a table with columns for Resources, Accounts, and Applications. A single entry is visible: "AWS::::Account:4018850 55551". The "Resources" column has a progress bar indicating 100% completion, while "Accounts" and "Applications" show lower completion rates.

Filtering options include "Choose a filter set" dropdown, "Filter data" search bar, and three active filters: "Workflow status = NEW", "Workflow status = NOTIFIED", and "Record state = ACTIVE". Buttons for "Reset to default layout" and "+ Add widget" are also present.

# AWS Security Hub Overview



- Security best practice checks
- Aggregates alerts across 60+ services and integrations
- Supports automated remediation

# AWS Trusted Advisor

Dashboard

Cost Optimizing

Performance

Security

Fault Tolerance

Preferences

## Trusted Advisor Dashboard

Download  

Cost Optimizing	Performance	Security	Fault Tolerance
 1 ✓ 6 ▲ 0 ! <b>\$2,528.46</b> Potential monthly savings	 6 ✓ 2 ▲ 0 !	 2 ✓ 3 ▲ 4 !	 5 ✓ 6 ▲ 2 !

### Recent Changes

 Amazon EC2 Availability Zone Balance 7/28/14

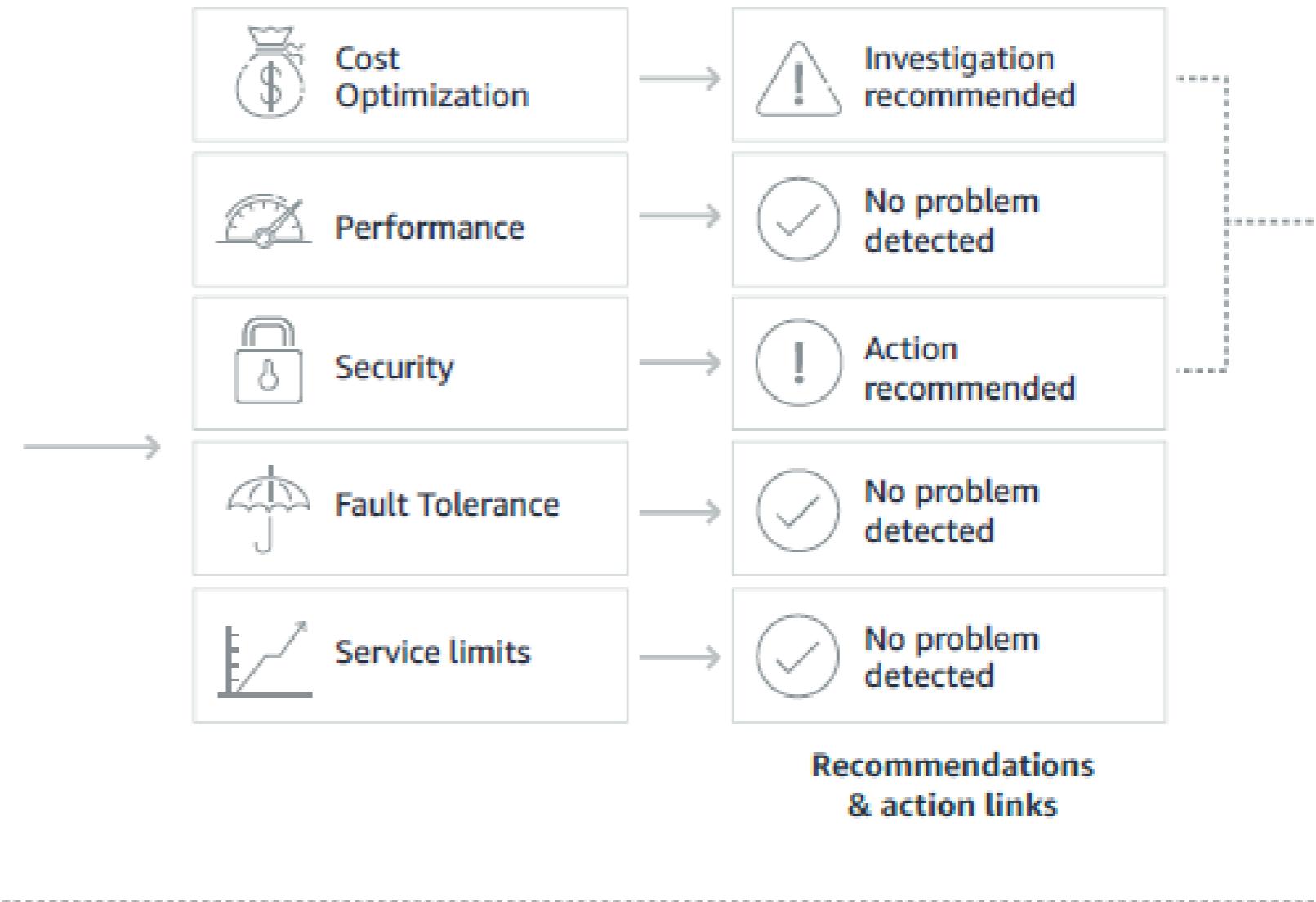
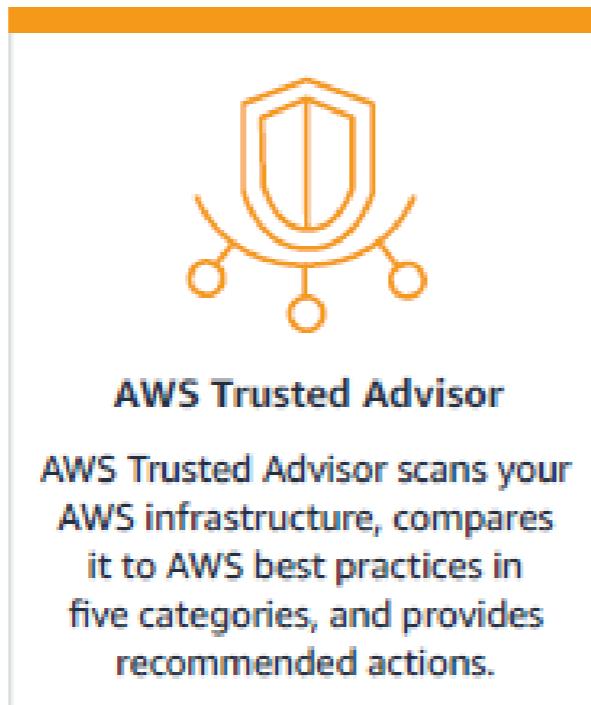
### What's New

Check: Service Limits check improvements  
Check: AWS CloudTrail and 4 Amazon Route 53 checks  
Check: CloudFront Content Delivery Optimization

# AWS Trusted Advisor



As an AWS customer, you want the most value from your investment. Trusted Advisor can help.



# Cost optimization

The screenshot shows the AWS Trusted Advisor Cost optimization interface. The left sidebar lists categories like Recommendations, Cost optimization (which is selected), Performance, Security, Fault tolerance, Service limits, and Operational excellence. Below that is a Preferences section with Manage Trusted Advisor and Notifications. The main content area has a header "Trusted Advisor > Cost optimization". A welcome message box contains text about the AWS Trusted Advisor console, mentioning IAM policies and restricted actions. Below this is a "Cost optimization" section with a "Refresh all checks" and "Download all checks" button. A note says to choose a check name for recommendations. The "Overview" section displays potential monthly savings of \$1,868.27, with four status indicators: 0 Action recommended (red), 5 Investigation recommended (orange), 12 No problems detected (green), and 0 Checks with excluded items (grey). The "Cost optimization checks" section includes a filter for tag keys and values, and buttons for "Reset" and "Apply filter".

Welcome to the AWS Trusted Advisor console!

For more information, see [Meet AWS Trusted Advisor](#). The Trusted Advisor console uses Identity and Access Management (IAM) policies for better security and flexibility. Some of your actions are currently restricted by these policies. Contact the account owner or administrator if you need help. [Learn more](#)

## Cost optimization

Choose a check name to see recommendations for ways to help save money for your AWS account. Trusted Advisor might recommend that you delete unused and idle resources, or use reserved capacity.

### Overview

Potential monthly savings **\$1,868.27**

Action recommended	Investigation recommended	No problems detected	Checks with excluded items
0	5	12	0

Cost optimization checks

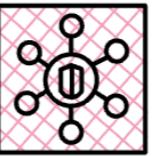
Filter by tag key [Learn more about using tags](#)

Tag Key Tag Value Reset Apply filter

- Trusted Advisor can detect over-provisioned servers and idle resources

# Limitations and differences

- Governance and compliance is a team sport
- Trusted Advisor checks on security, cost management, fault tolerance, and performance
- AWS tools make the job easier - similar to a cruise control
- Trusted Advisor checks are not customizable



Security Hub



Trusted Advisor

security findings only

customized checks available with custom actions

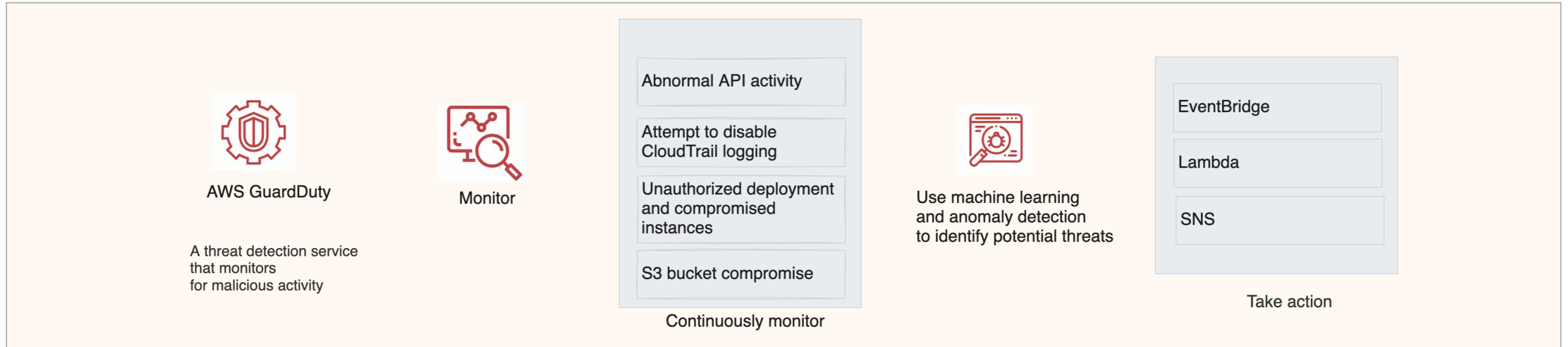
can check with a standard

recommendations on security, cost management, fault tolerance, and performance

checks are not customizable

cannot check compliance with a specific security standard

# GuardDuty



- Detects threats in AWS environments
- Generates detailed, actionable findings
- Operates independently, no performance impact

# **Let's practice!**

**AWS SECURITY AND COST MANAGEMENT CONCEPTS**