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

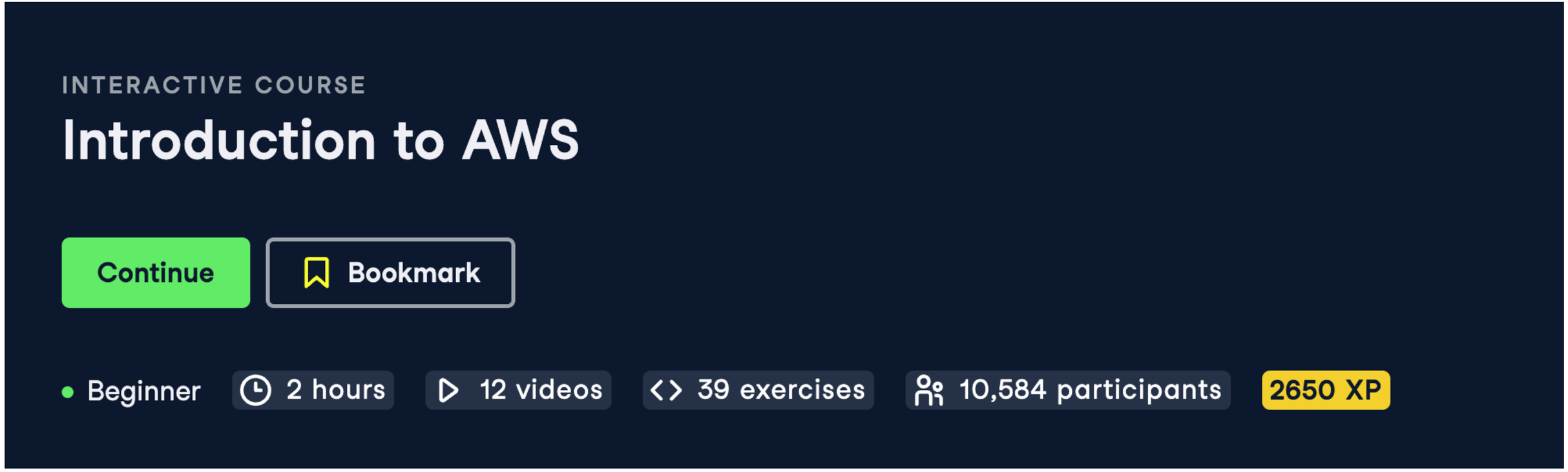
Chapter 1
Introduction to
AWS Security

Chapter 2
Security
Best Practices

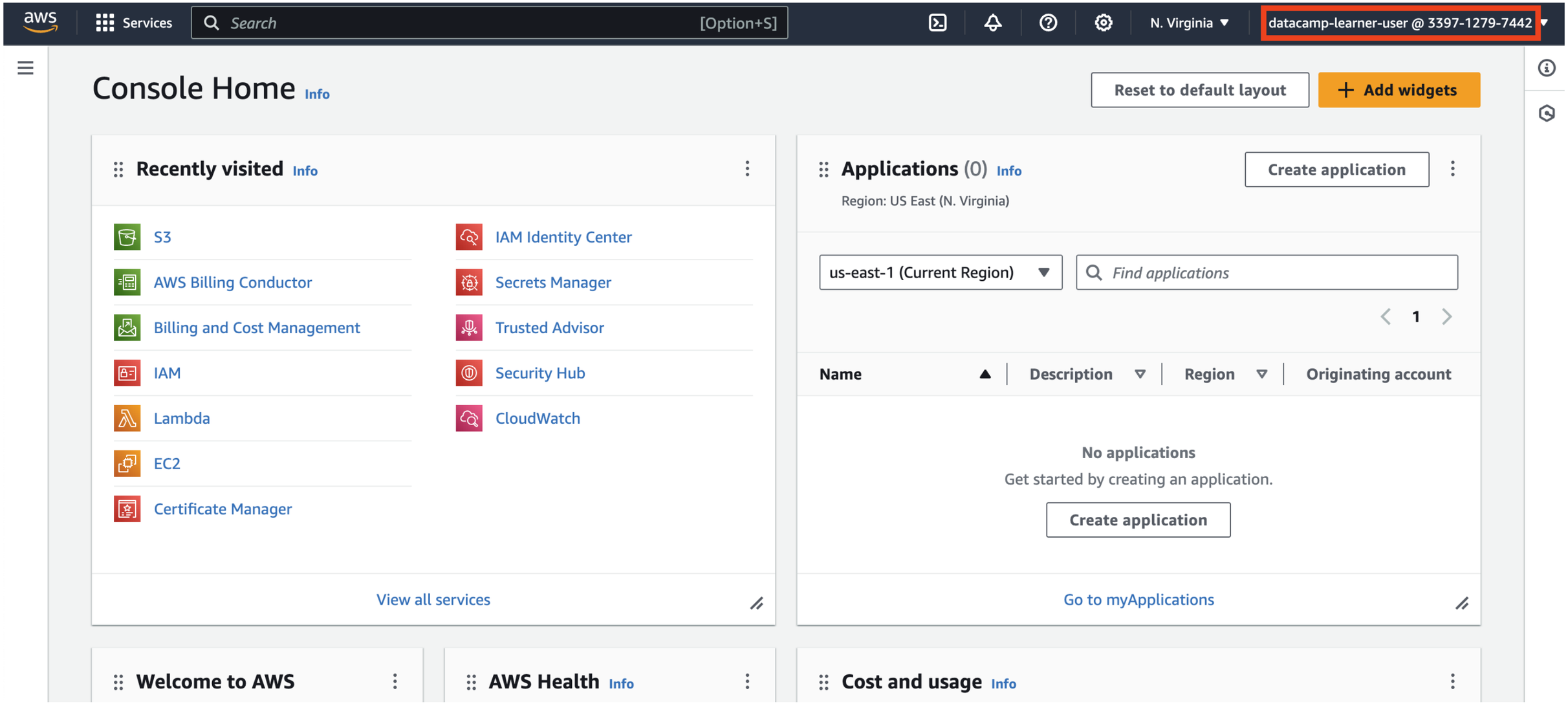
Chapter 3
Billing and
Cost Management

Prerequisites

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



Course Format



Let's practice!

AWS SECURITY AND COST MANAGEMENT CONCEPTS

AWS Shared Responsibility Model

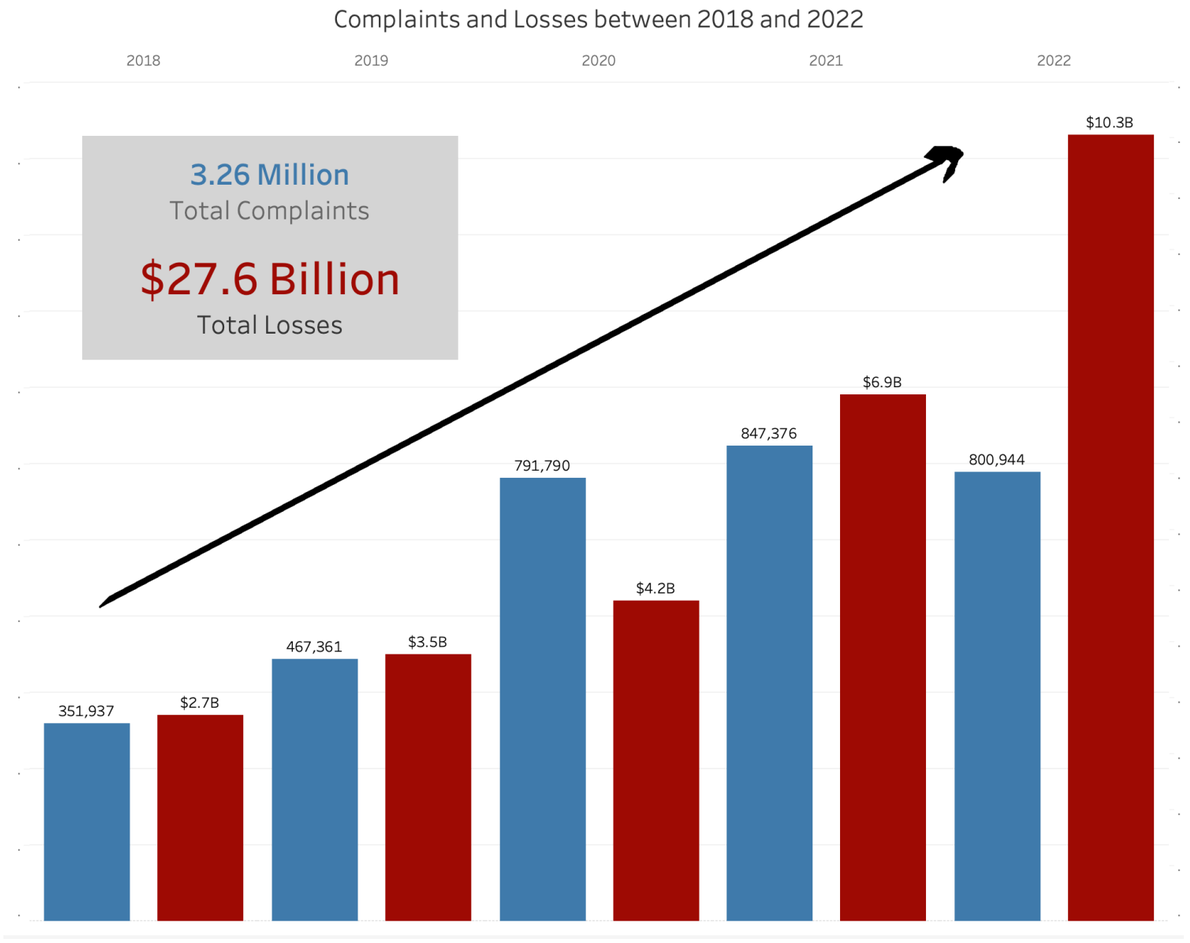
AWS SECURITY AND COST MANAGEMENT CONCEPTS

Dev Bhosale
Principal Data & Cloud Architect

datacamp

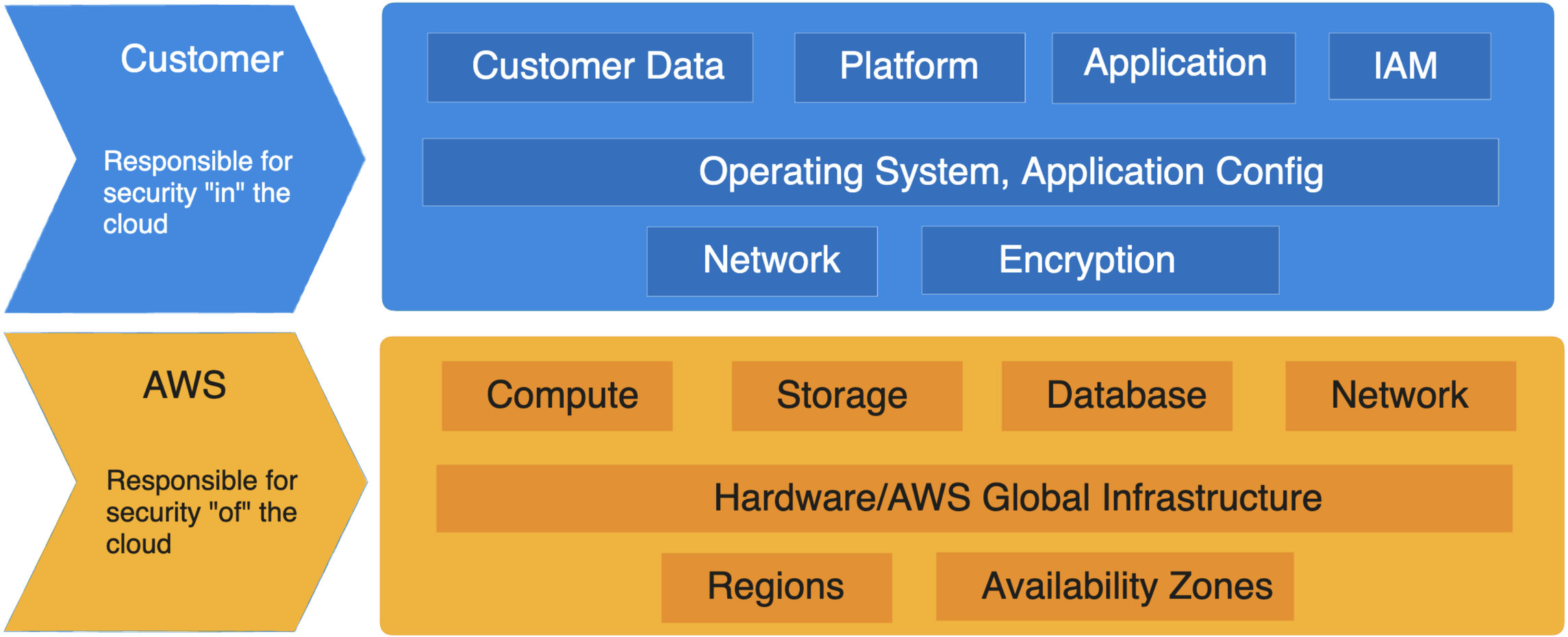
Why cloud security is important?

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



[1] https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/

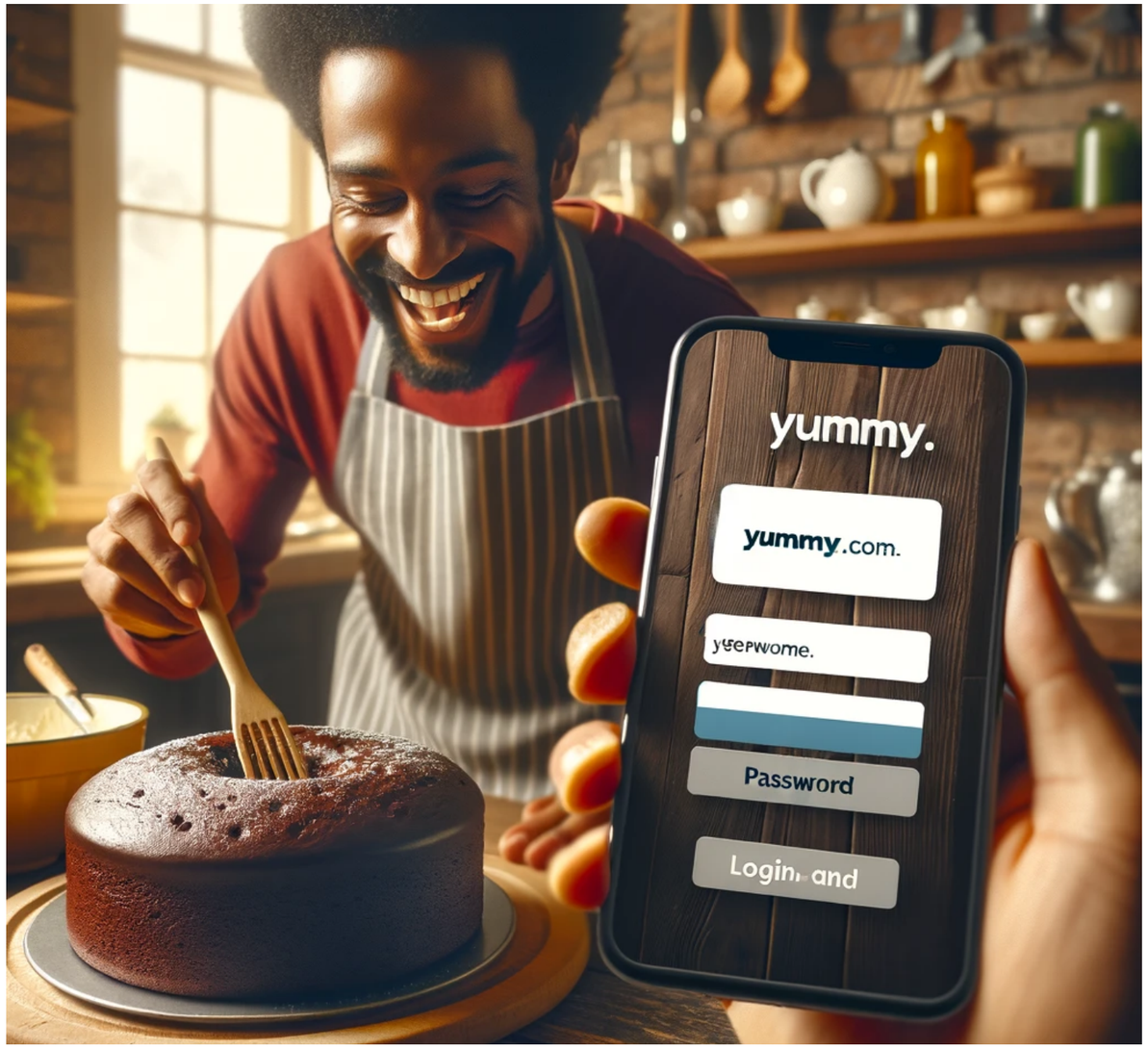
Shared responsibility model



Shared responsibility model

Security in the cloud - Customer responsibilities

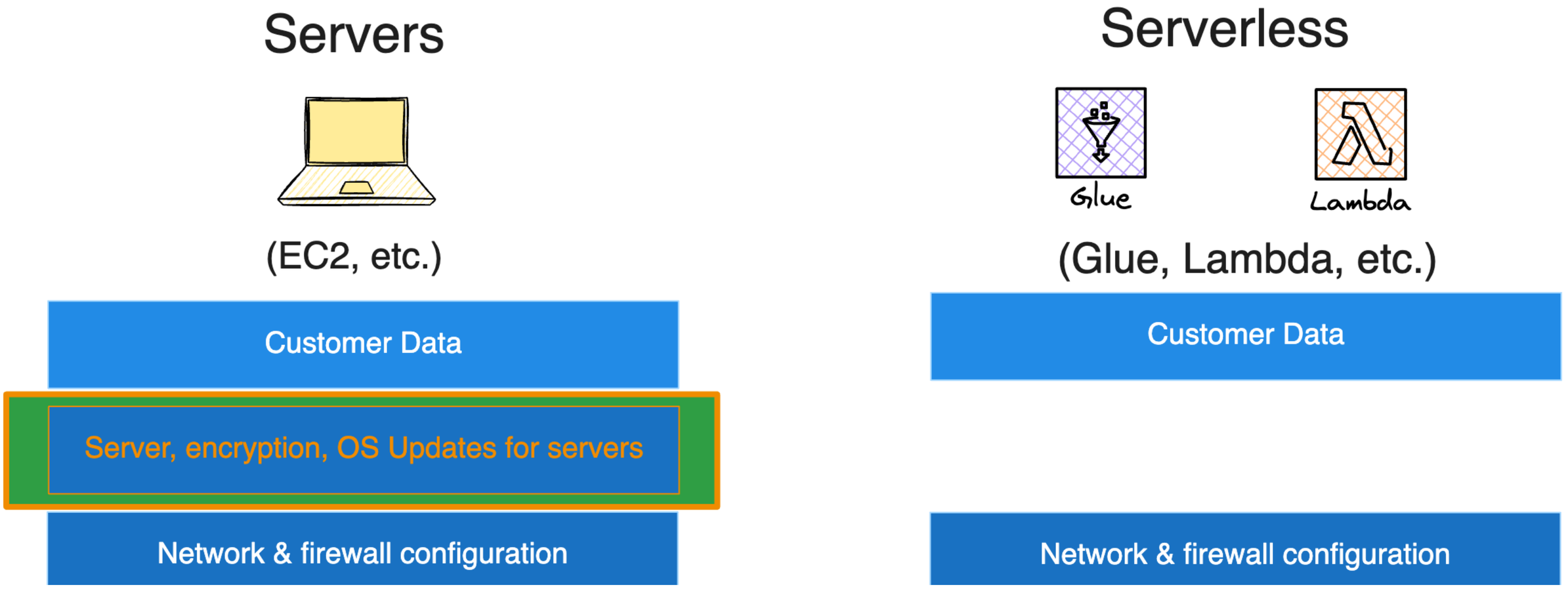
- Credentials to server
- Database access
- Application software installed on server
- Encryption keys



Security of the cloud - AWS responsibilities

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

How responsibilities change?



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

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

datacamp

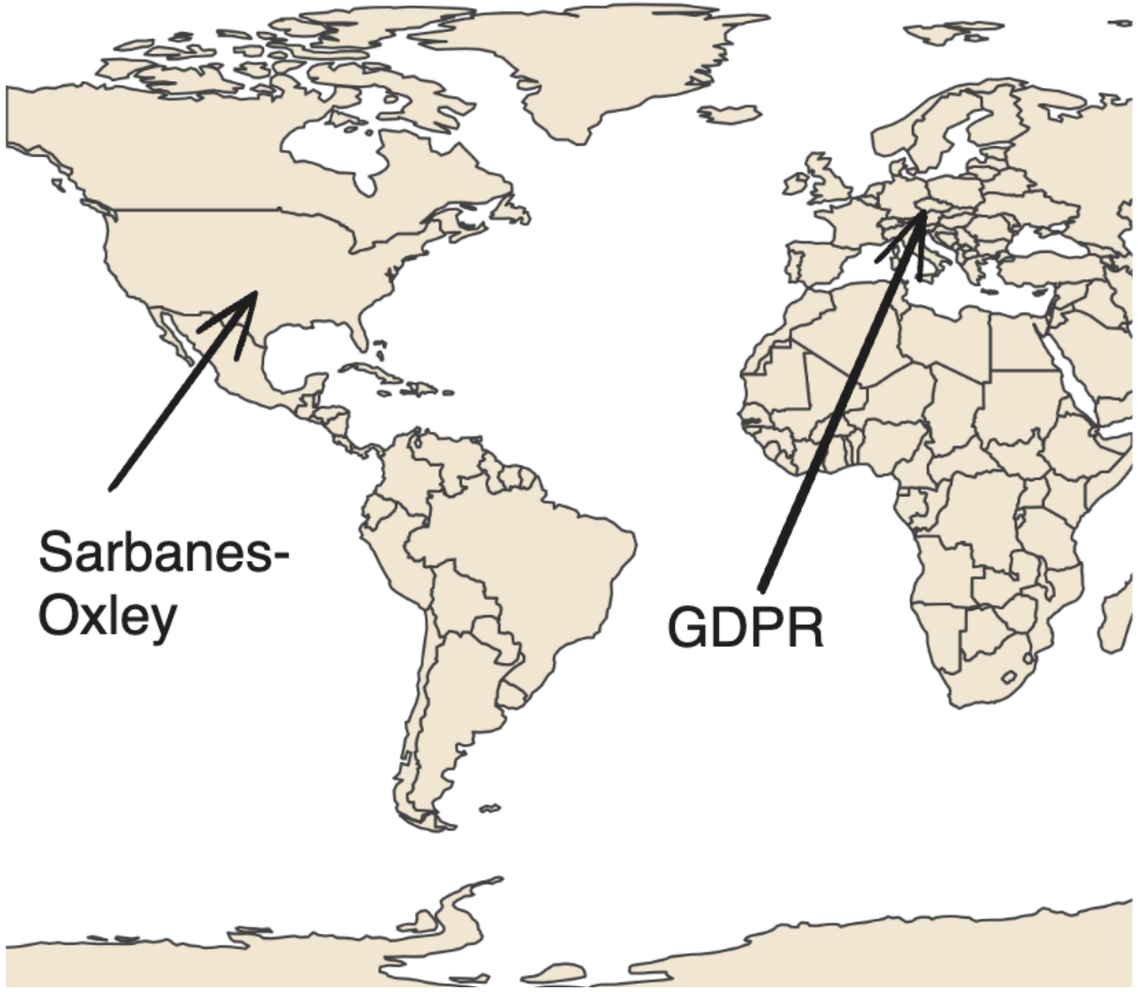
Cloud governance

What is cloud governance?

- Corporate strategy — Division of responsibility, Cost center
- Ethical behavior — Trade secrets, Fraud
- Risk management — Cyberattack, Reputation
- Compliance — Regulations

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

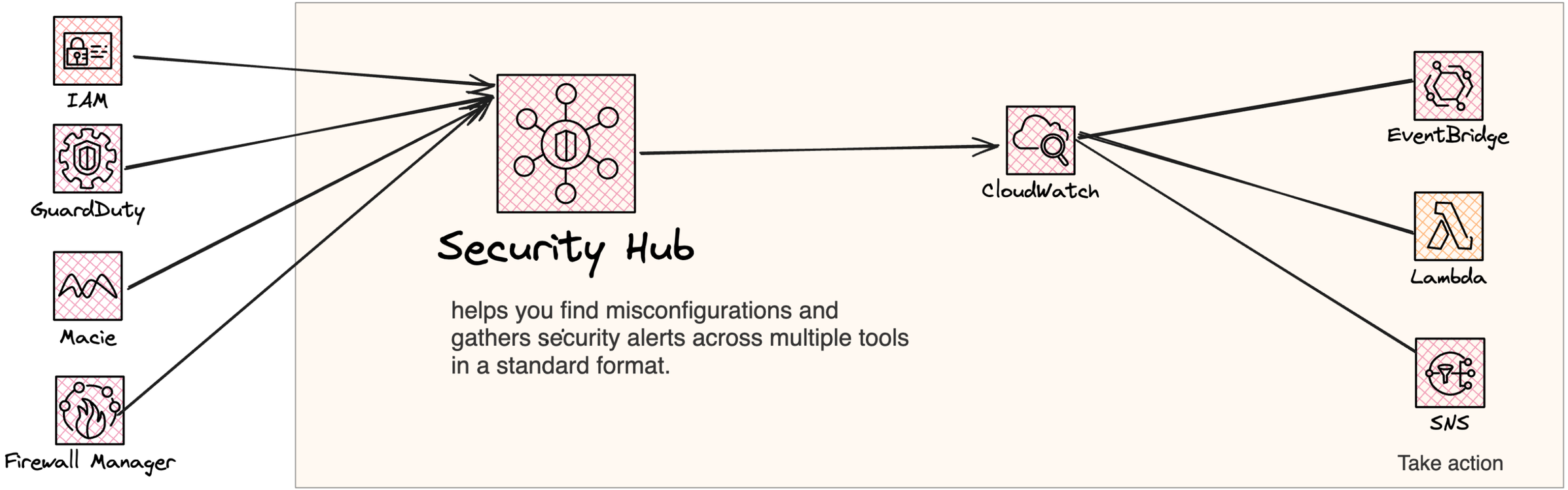
Recover

Respond

AWS tools for governance

Identify	Protect	Detect	Respond	Recover
				
Organizations	Shield	GuardDuty	CloudWatch	OpsWorks
Security Hub	Certificate Manager	Macie	Lambda	CloudFormation
Config	KMS	Inspector	Detective	Glacier
Trusted Advisor	Firewall	Security Hub	CloudTrail	Snapshot
Systems Manager	WAF		Systems Manager	Archive
Control Tower	CloudHSM		Step Functions	CloudEndure

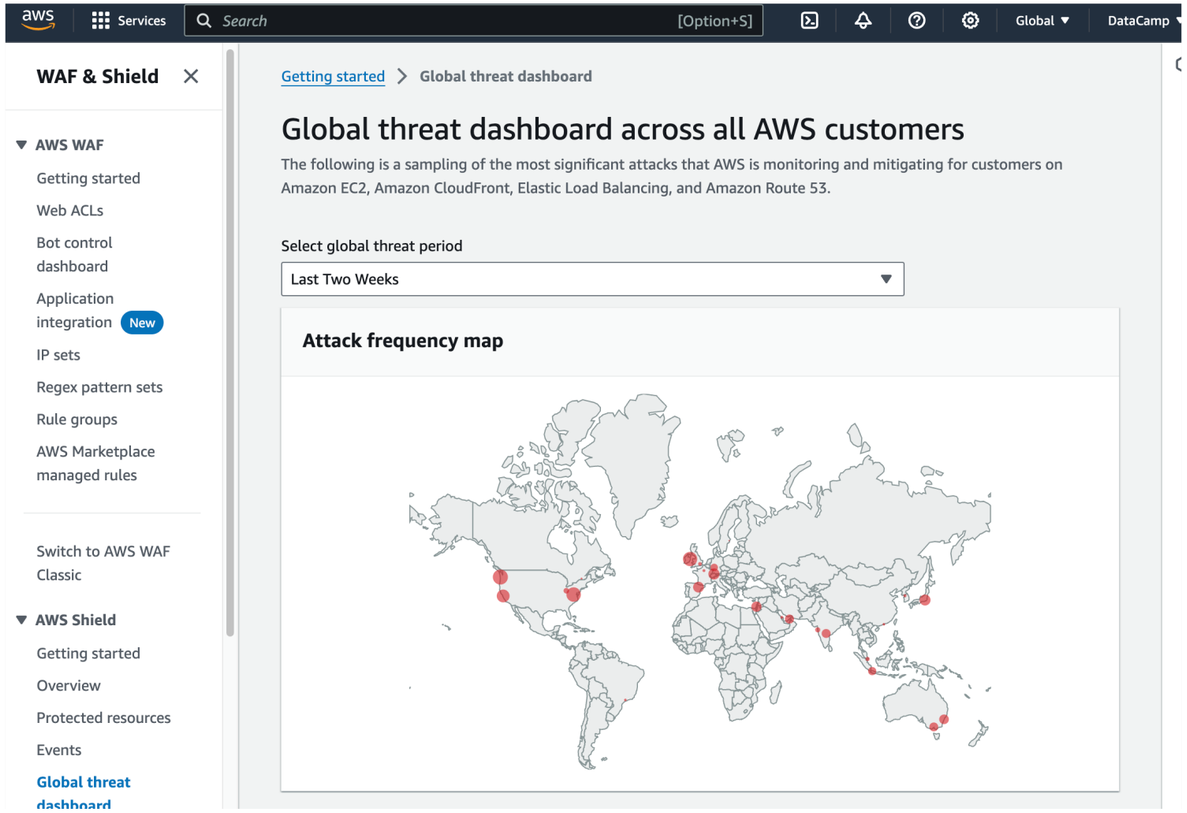
Threat identification



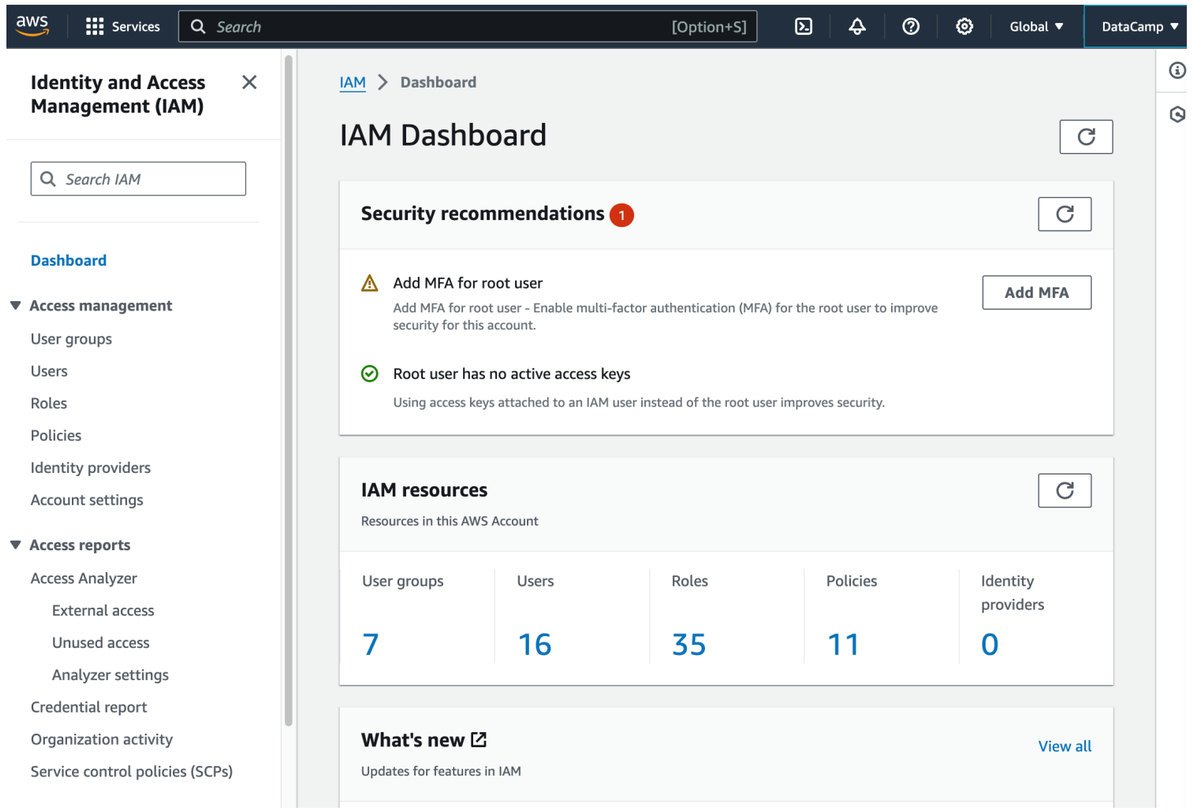
- Continuously checks your AWS resources for security best practices
- Find misconfigurations and gathers security alerts

Tools for protection

Shield

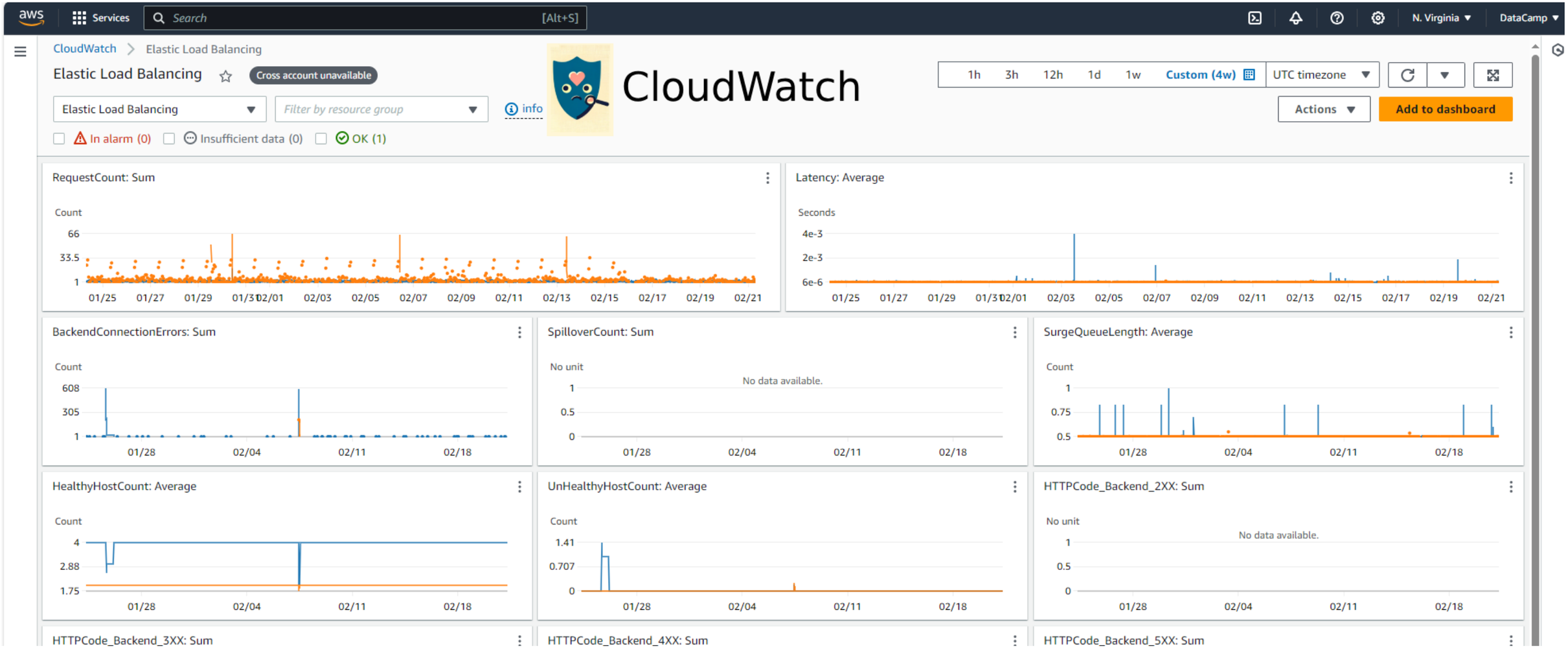


IAM



Detect malicious activities

- Detect anomalies and malicious activities with continuous monitoring from CloudWatch



Detect malicious activities

Amazon Inspector

Scans compute workloads (EC2, Lambda) for vulnerabilities

Enable Inspector

- Automated workload discovery
- Continual scanning
- Maintained vulnerability database
- Near real-time results

Discover and scan

Consider many factors to create a meaningful risk score

- EventBridge
- Lambda
- SNS

Take action

AWS GuardDuty

A threat detection service that monitors for malicious activity

Monitor

- Abnormal API activity
- Attempt to disable CloudTrail logging
- Unauthorized deployment and compromised instances
- S3 bucket compromise

Continuously monitor

Use machine learning and anomaly detection to identify potential threats

- EventBridge
- Lambda
- SNS

Take action

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

datacamp

AWS Security and compliance tools

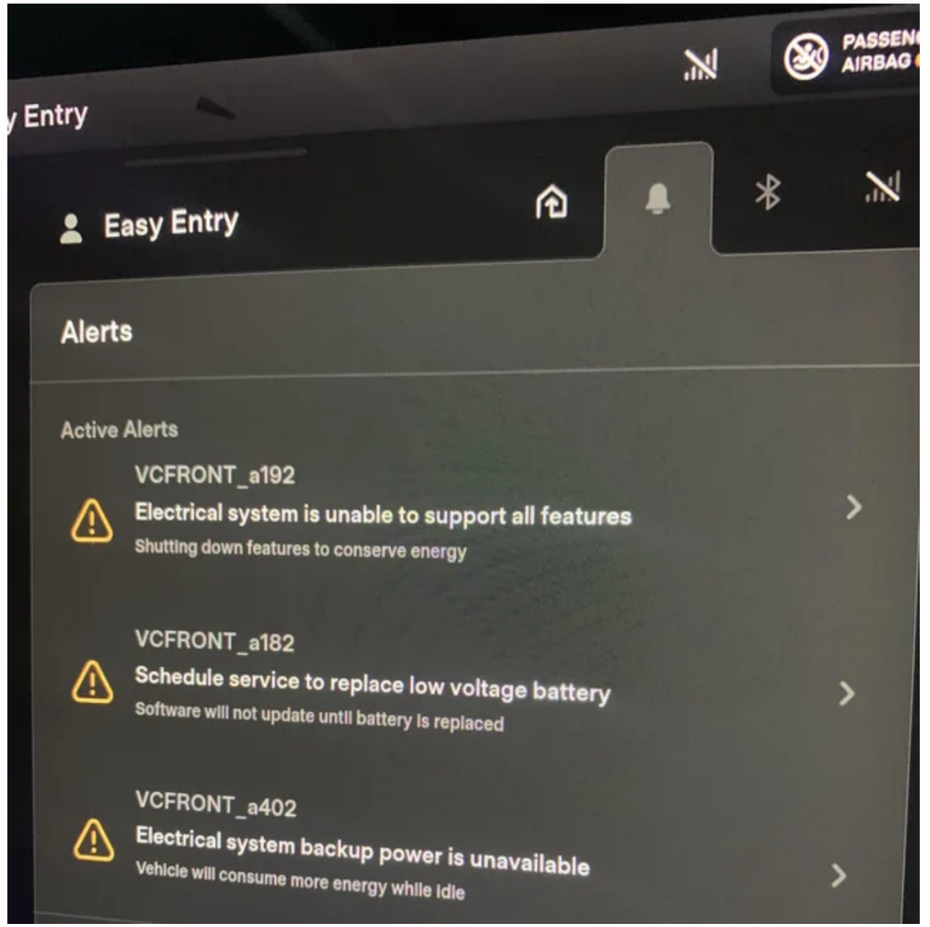
Identify	Protect	Detect	Respond	Recover
				
Organizations	Shield	GuardDuty	CloudWatch	OpsWorks
Security Hub	Certificate Manager	Macie	Lambda	CloudFormation
Config	KMS	Inspector	Detective	Glacier
Trusted Advisor	Firewall	Security Hub	CloudTrail	Snapshot
Systems Manager	WAF		Systems Manager	Archive
Control Tower	CloudHSM		Step Functions	CloudEndure

Long checklist vs a dashboard

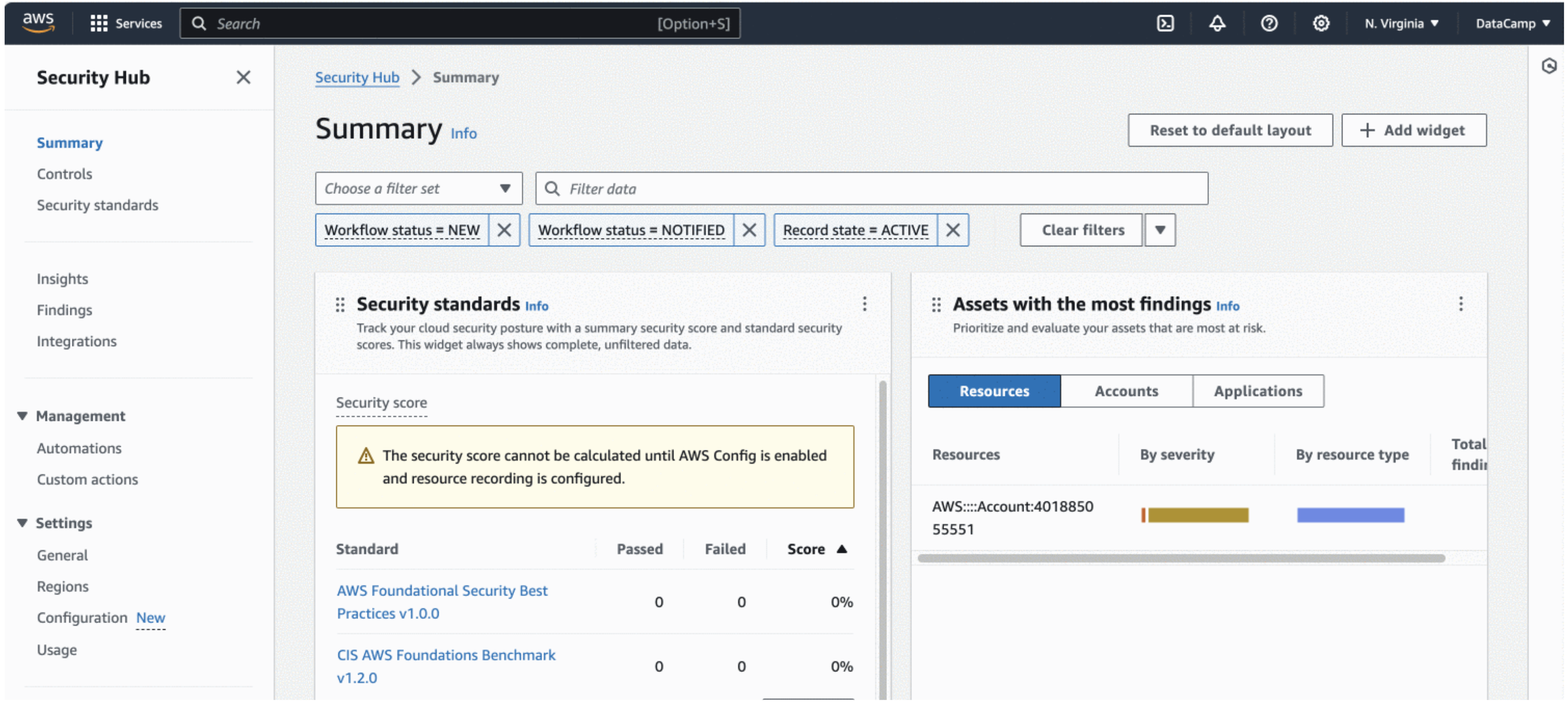
The old way

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

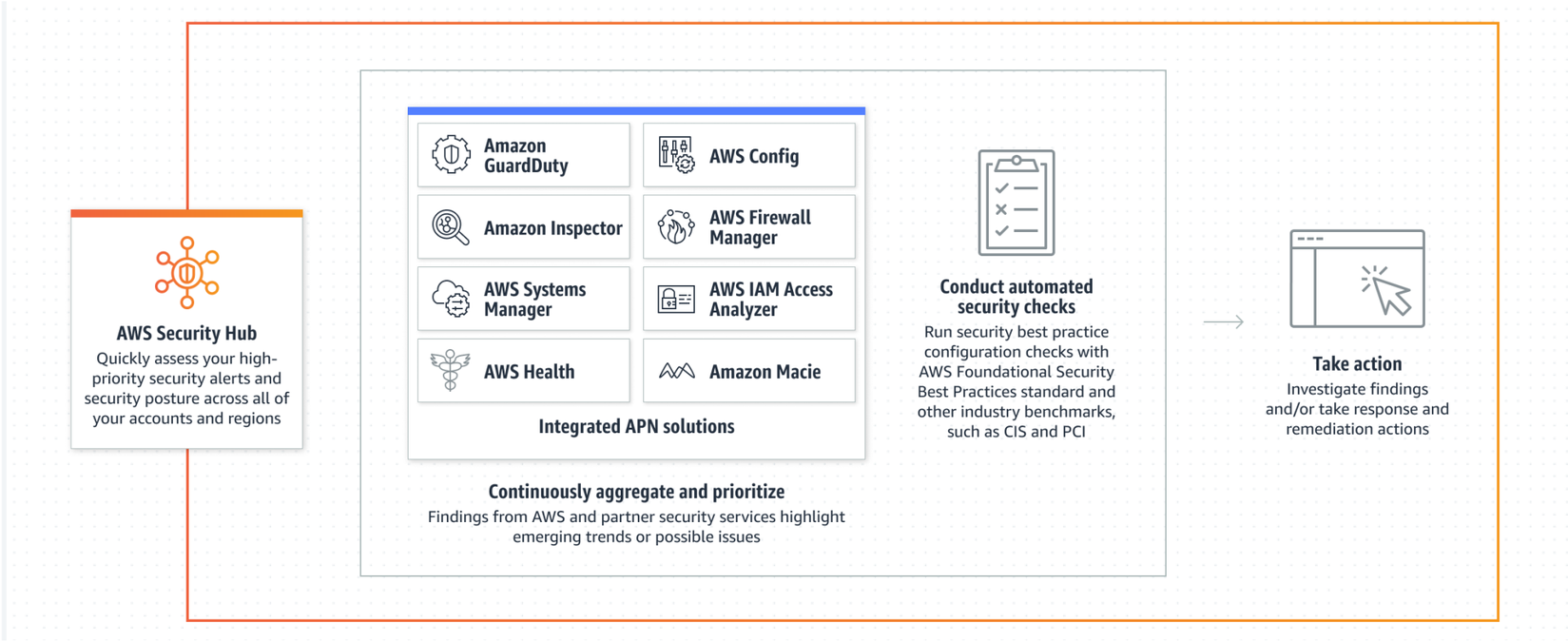
The new way



AWS Security Hub Overview

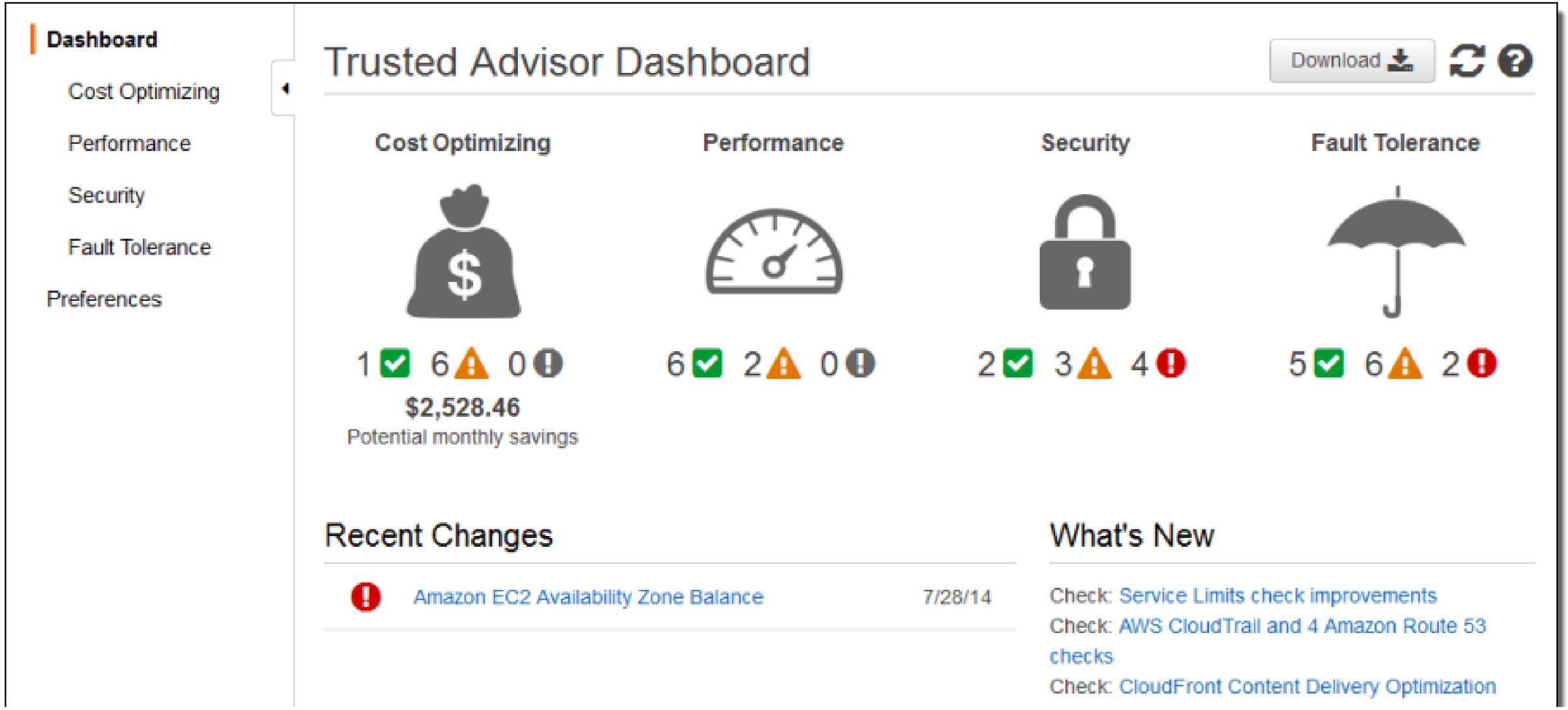


AWS Security Hub Overview



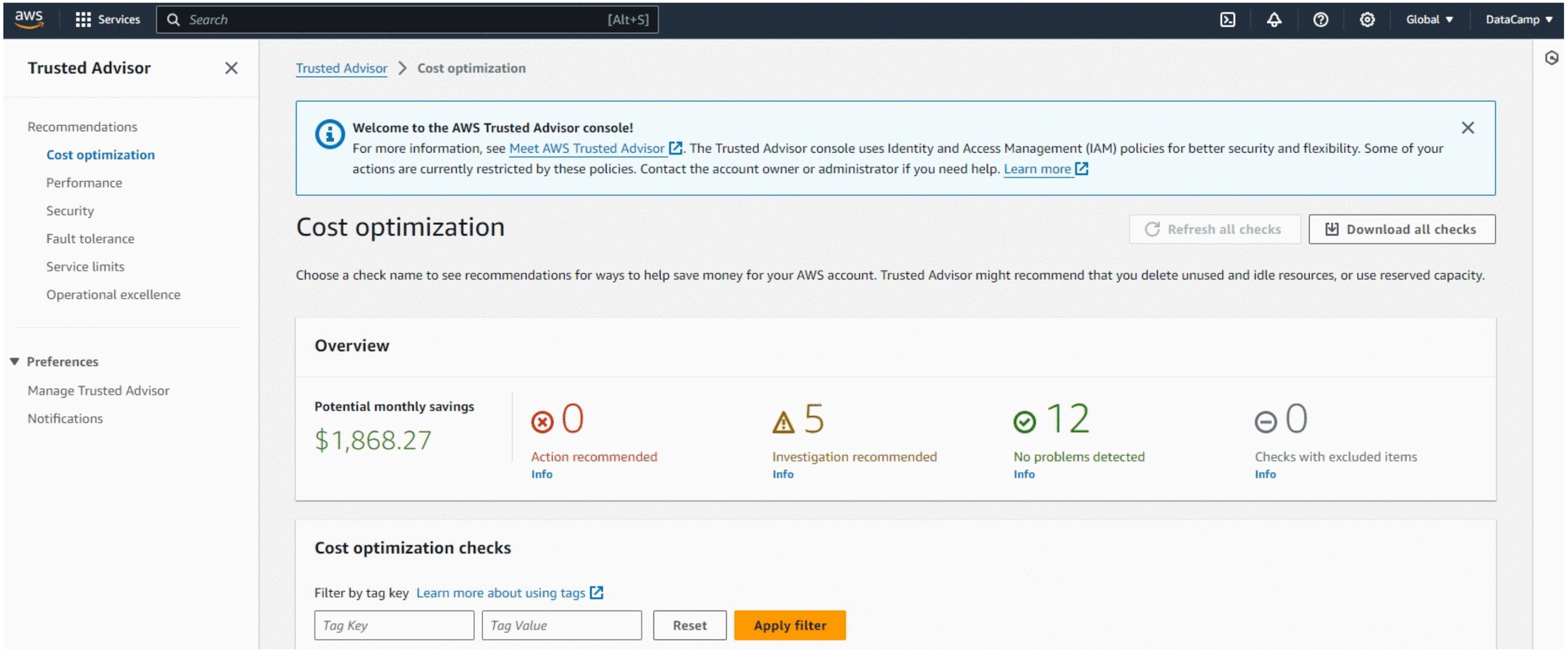
- Security best practice checks
- Aggregates alerts across 60+ services and integrations
- Supports automated remediation

AWS Trusted Advisor



AWS Trusted Advisor

Cost optimization



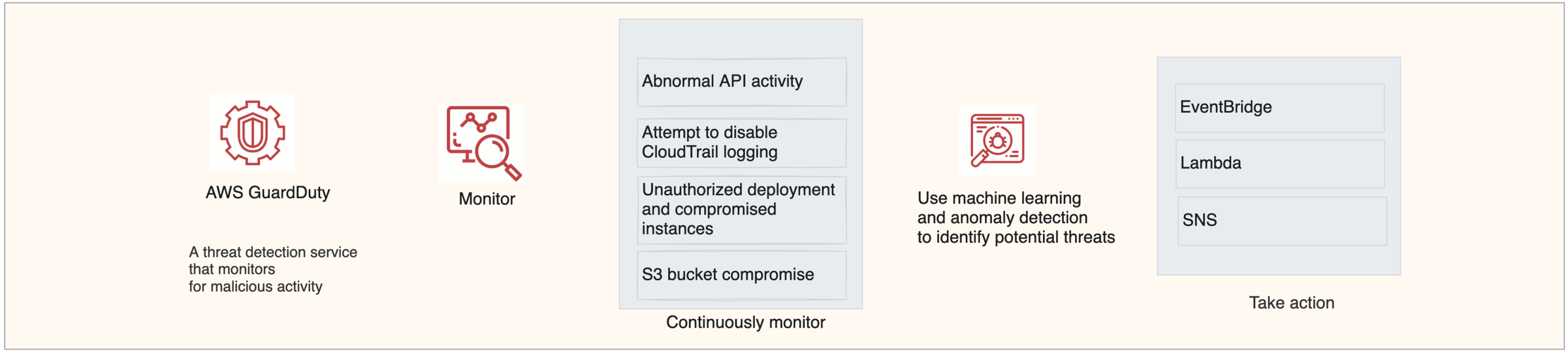
- Trusted Advisor can detect over-provisioned servers and idle resources

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	recommendations on security, cost management, fault tolerance, and performance
customized checks available with custom actions	checks are not customizable
can check with a standard	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