

AWS  
re:Invent



COM 304

# How robots can help make your AWS accounts more secure

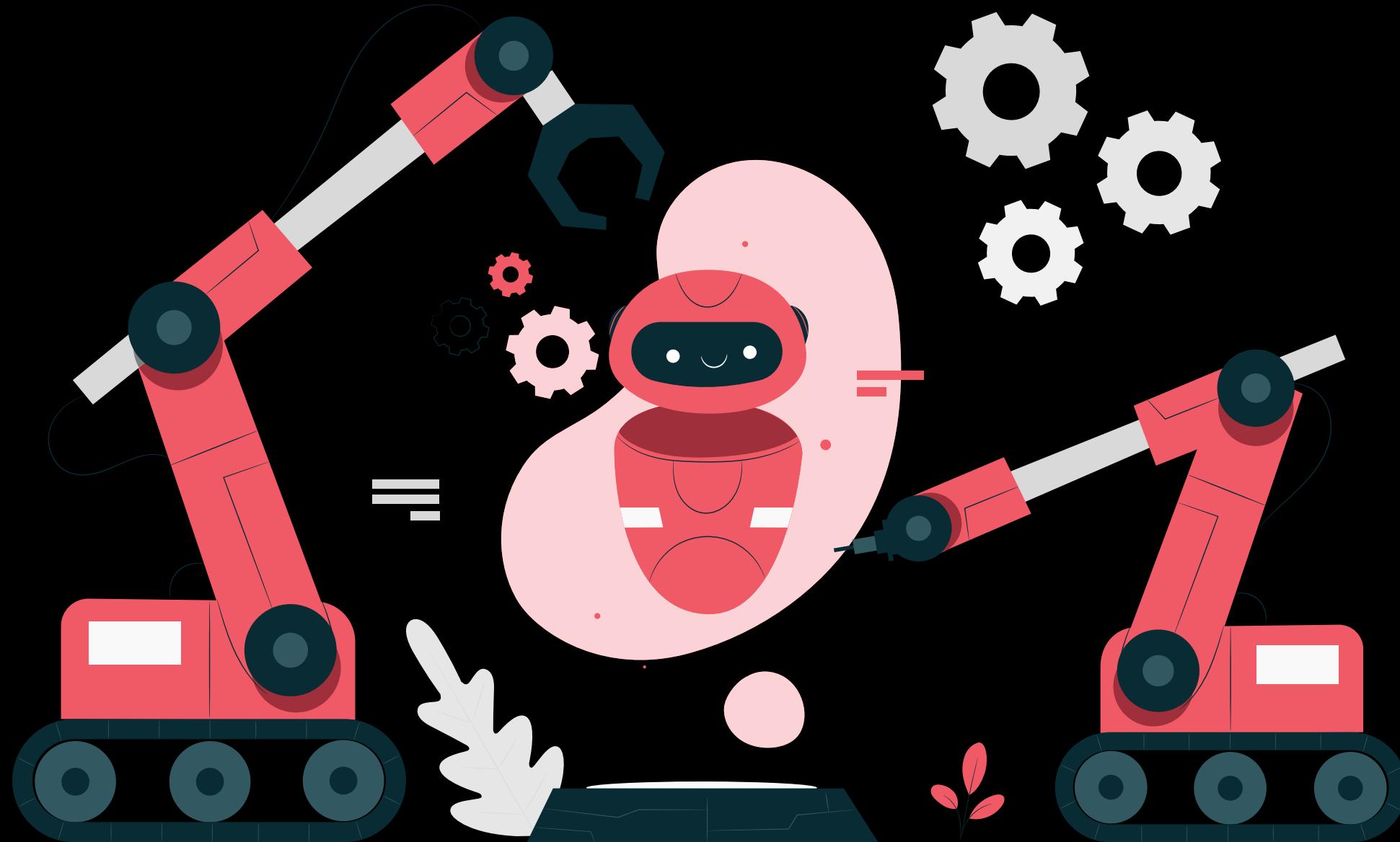
Margaret Valtierra  
Program Manager  
Morningstar



# Challenges

- Encourage developers to own AWS security best practices
- Offer self-service, decentralized account structure
- Comply with regulated industry standards

# Solution: Robots?



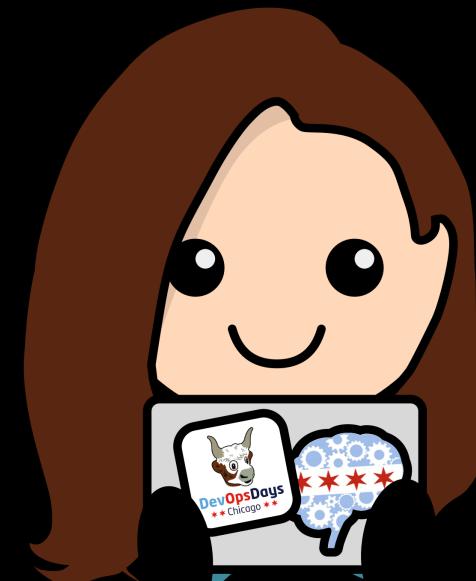
# About me

Program manager, Morningstar

AWS Community Hero

Chicago AWS user group leader

DevOpsDays Chicago organizer



Created by  
@sosplash

Get in touch!  
@margaretvaltie

# Tl;dr:

- Securing 200+ self-service accounts is hard
- Incentivize teams to own best practices
- Automate compliance and scanning
- Take advantage of AWS automations

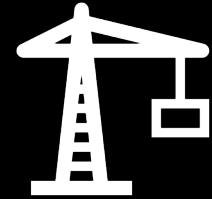
# Morningstar's public cloud setup



# Morningstar's public cloud strategy

- Stateful account configuration with GIT, Terraform
- Uniform access with IAM roles
- Standardized networking, services, infra control
- Requires budget approval process at P&L level

# Cloud services team



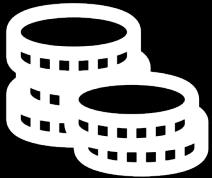
## Architecture

Architectural guidance  
POCs



## Infra

Account creation  
Connectivity  
Infrastructure as code



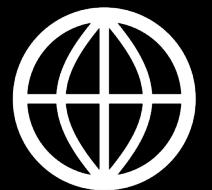
## Finance

Financial Governance  
Budgeting  
Cost optimization



## Security

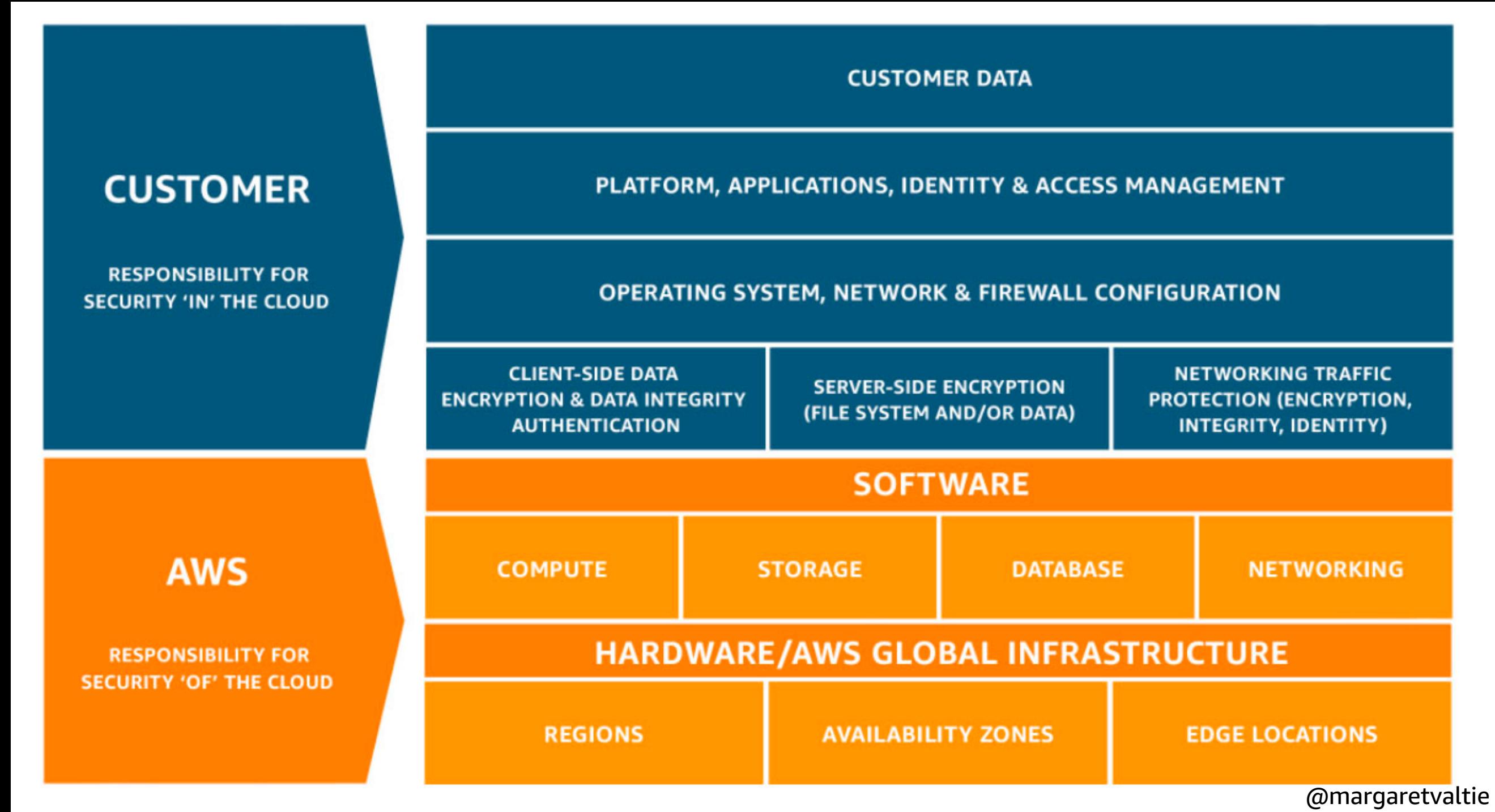
Governance  
Security  
Scanning



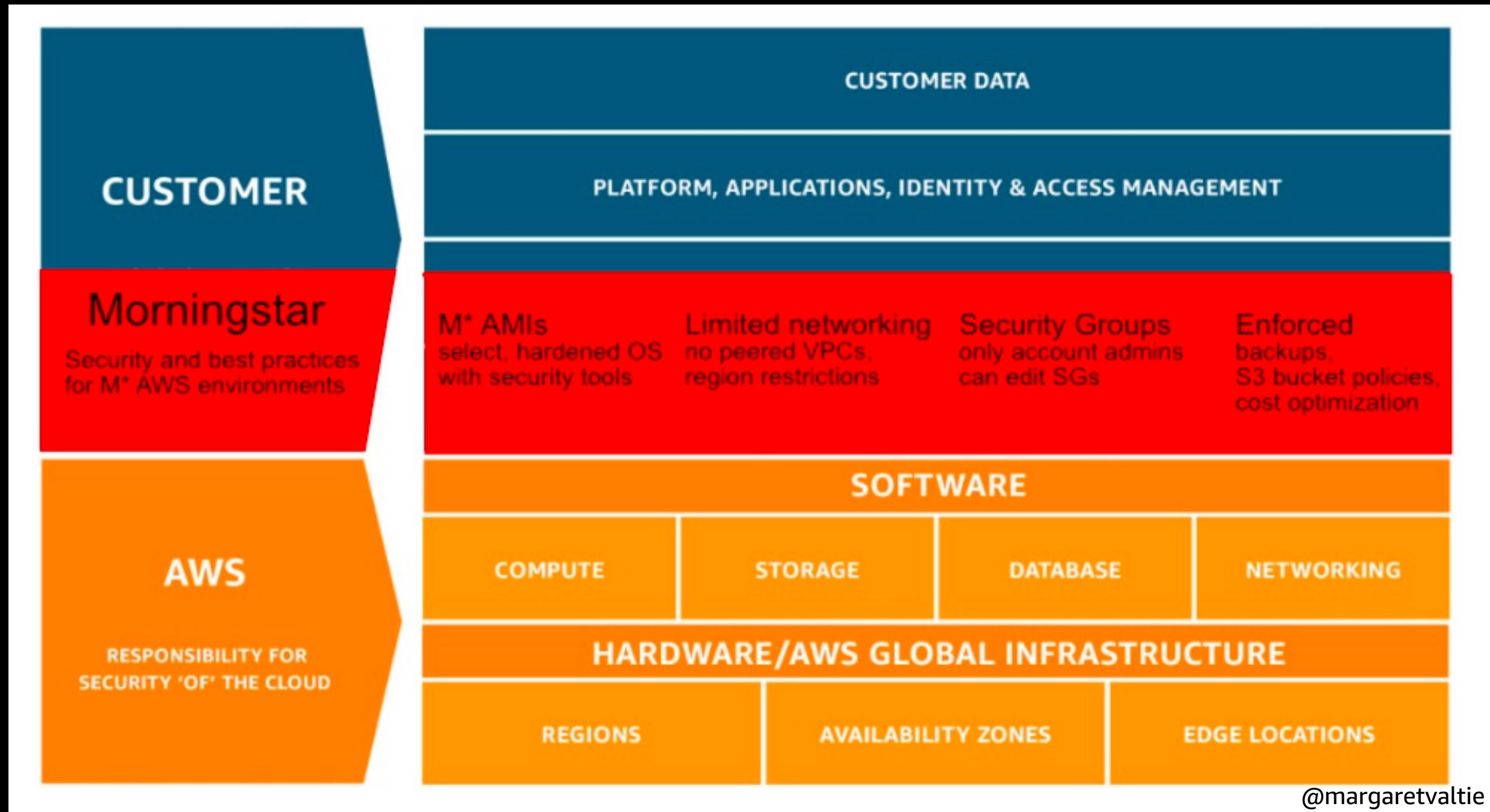
## Operations

Deployment pipelines  
Backups  
Operational support

# The AWS shared responsibility model



# Morningstar's responsibility model

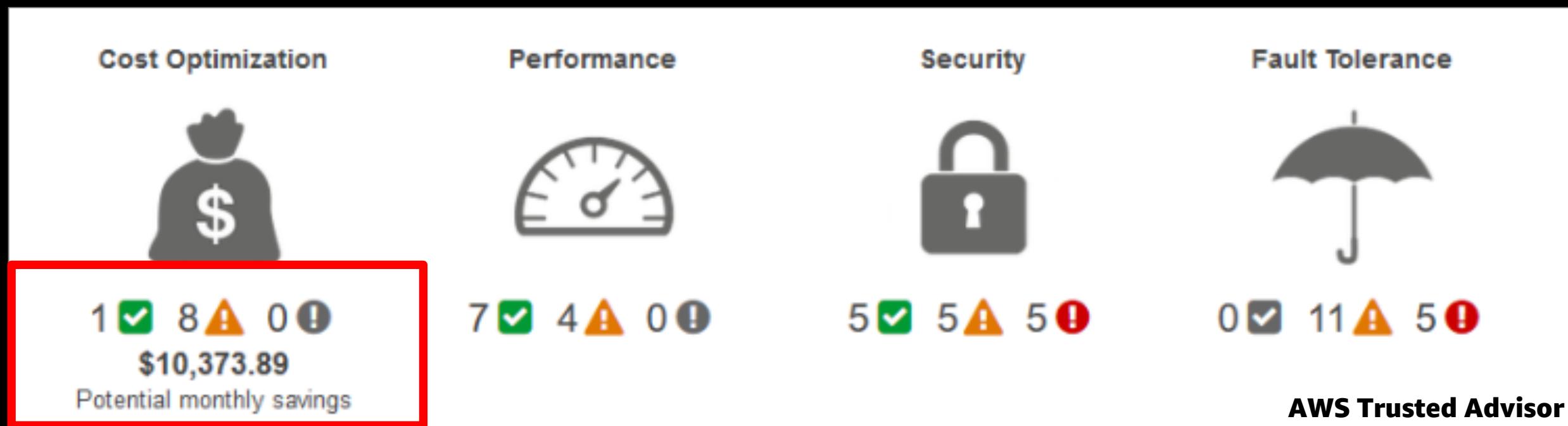


# Enforcement: Guardrails + behavior

- Cost management is account management
- Custom-built CloudSvc API
- Documentation, wikis, training

# Trusted source

- AWS Trusted Advisor and AWS Well-Architected Framework
- Actionable, account-based recommendations



Public Cloud Findings

+ Create board

Issues

Reports

Releases

Components

Calendar

Satisfaction

Scheduled Issues

PROJECT SHORTCUTS

Add a link to useful information for your whole team to see.

+ Add link

Public Cloud Findings / PCLFI-10756

Unattached EBS Volume: vol-0fa91b850a83a9bf9

Edit Comment Assign More Start Progress Start Analysis

**Severity**

**Resource name**

**Issue type**

**Savings impact and links to resources**

Type: Public Cloud Finding

Priority: 2-High

Component/s: None

Labels: active

Rework Count: 0

Cost: 17.2

Component Name: Youtrack Upgrade Test 9

Cloud Region: us-east-1

Account ID: 0000009100

AWS Environment: prod

Finding: cost\_optimization\_ebs\_utilization

Service ID: NA

Team ID: BOB

**Details**

Description

Volume vol- 0000009100000 with 0 snapshots is orphaned. Please terminate the volume or, if required, take a snapshot, the volume. Terminate Savings: \$17.2/month or \$206.4/year. Snapshot, then terminate savings: \$8.6/month or \$103.2/year.  
<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-storage-optimization/optimizing-amazon-ebs-storage.html>

# Rated cloud compliance

SCORECARDS ARE KINDA OUR THING



## Fidelity® Growth & Income FGRIX ★★ Silver

Analyst rating as of Jan 31, 2020

Quote Fund Analysis Performance Risk Price Portfolio People Parent

NAV / 1-Day Return 38.87 / <b>0.28 %</b>	Total Assets 6.4 Bil	Adj. Expense Ratio  0.610%	Expense Ratio 0.610%	Fee Level Below Average	Longest Manage 9.71 years
---	-------------------------	----------------------------	-------------------------	----------------------------	------------------------------

Category US Fund Large Blend	Investment Style Large Value	Min. Initial Investment 0	Status Open	TTM Yield 2.17%	Turnover 32%
---------------------------------	---------------------------------	------------------------------	----------------	--------------------	-----------------

USD | NAV as of Oct 16, 2020 | 1-Day Return as of Oct 16, 2020, 4:31 PM GMT-05:00

PREMIUM

### Morningstar's Analysis



Analyst rating as of Jan 31, 2020.

#### Process Pillar



Above Average

This fund's disciplined and consistent approach earns it an Above Average Process rating. Manager Matt Fruhan aims to beat the S&P 500 by building a yield-rich, large-cap-focused portfolio of businesses that he considers worthwhile long-term holdings. ...

#### People Pillar



Above Average

Manager Matt Fruhan's experience combined with Fidelity's resources earn the fund an Above Average People rating. Fruhan has led this fund since 2011. He's currently at the helm of other well-known Fidelity funds, including Fidelity Large Cap Stock FLCSX...

#### Parent Pillar



Above Average

Fidelity earns an Above Average Parent rating because of its ability to stay ahead of its competition. The firm's successful stock-picking mutual funds fueled its rise to prominence, and it has adapted well to investor preferences that have shifted...



[• View Live Scorecard](#)

Cloud Services, YOUR RATING

October 19, 2020

# hasn't changed

INFORMATION TYPE  
**Confidential**

YOUR OVERALL RATING

YOUR PEER'S RATING

Public Cloud Cost What's this rating?

TOTAL ISSUES

**64**

2 more than last week

CRITICAL / HIGH

**0**

no change

POTENTIAL SAVINGS

**\$646** / MO.

\$9 higher

To improve your cost star rating, start reviewing the Trusted Advisor recommendations under your AWS account. If you have questions, contact [CloudServices@morningstar.com](mailto:CloudServices@morningstar.com).

@margaretvaltie

# Event-based triggers



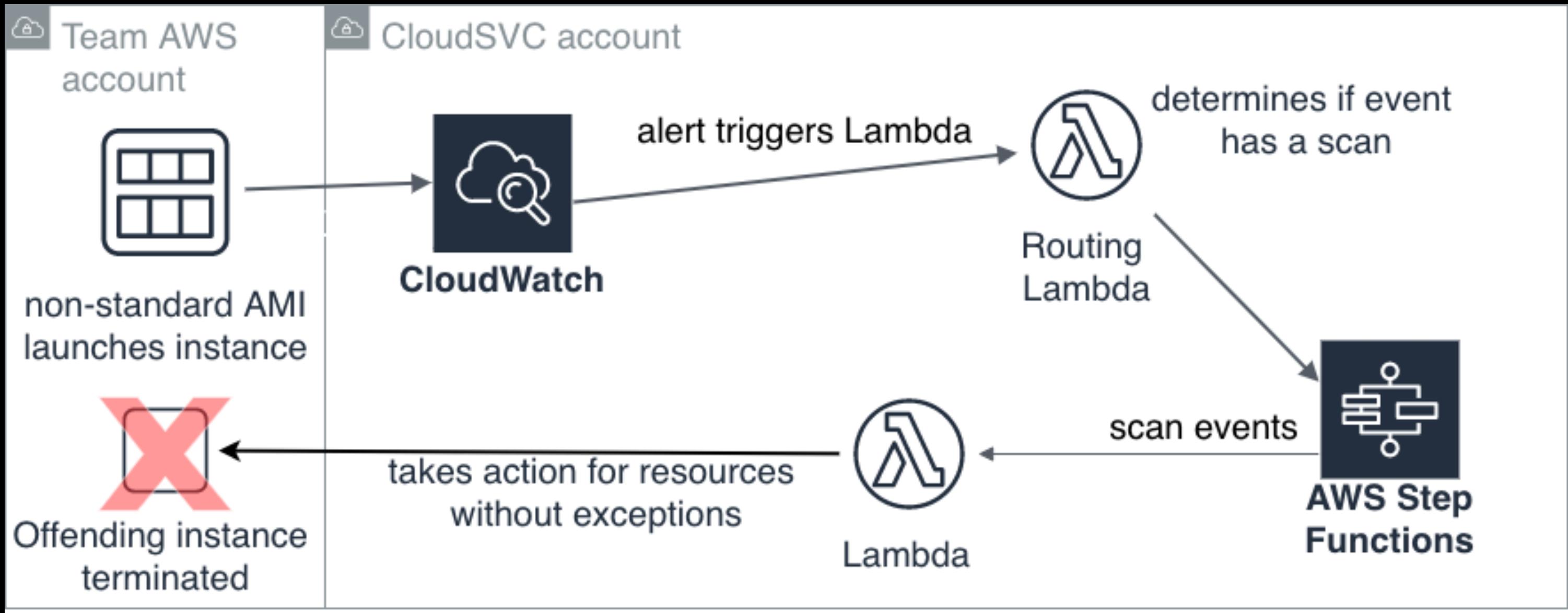
# Goal: Secure instances only

- Ensure only approved instances run in production
- Limit attack vector and licensing costs
- Add custom security, monitoring tools
- Account for exceptions
- Automate enforcement at the account level

# Morningstar AMI

- Built monthly with Chef, Packer, Terraform
- Patched, CIS hardened, with configuration management
- Not dependent on AWS-generated keys for authentication

# AMI auto-kill flow



# Time-based triggers



# Goal: Ongoing compliance

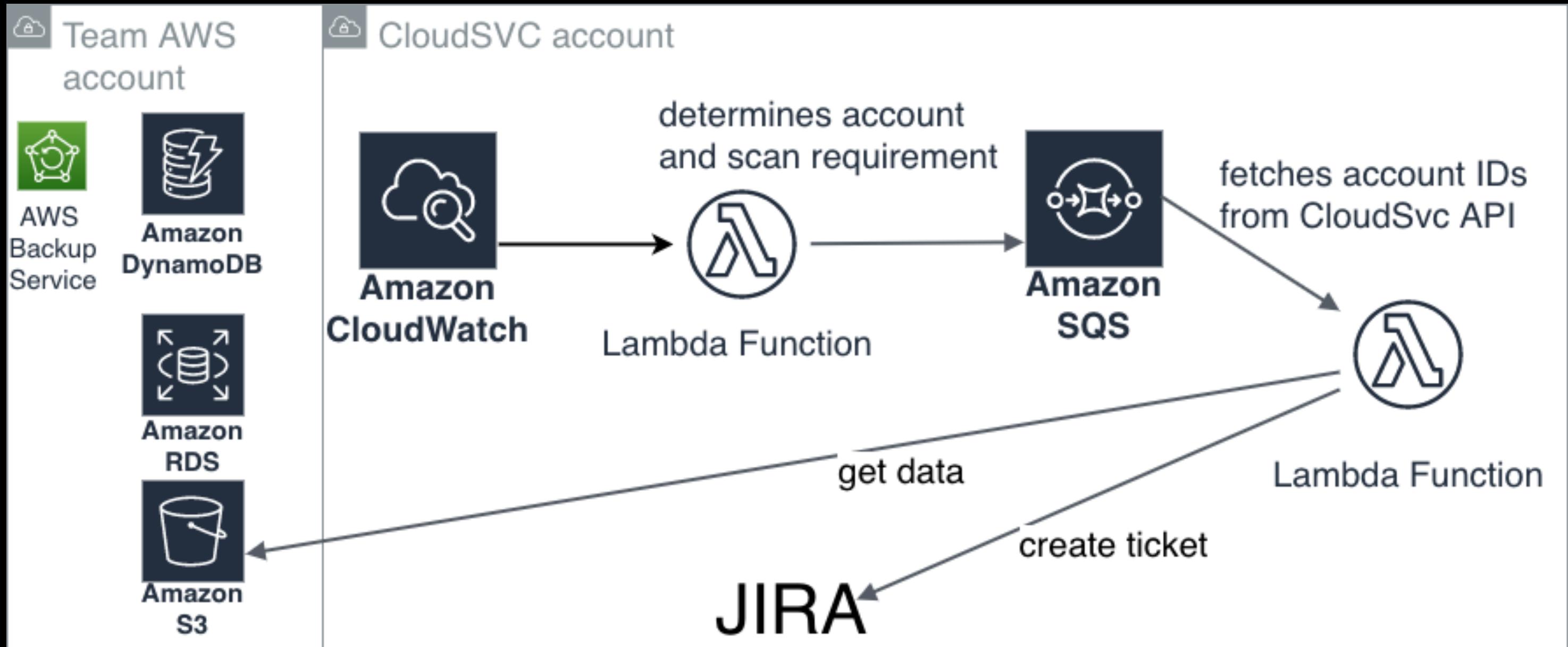
- Enforce backups
- Patch long-running Amazon Elastic Compute Cloud (Amazon EC2) instances
- Enforce AWS Identity and Access Management (IAM) access key rotation
- Ensure encryption in transit on ALBs and NLBs

# Backup scanners

- Standardize backup and recovery processes in cloud and on prem
- Focus on databases – Amazon Relational Database Service (Amazon RDS) and Amazon DynamoDB
- Verify backups weekly in production account
- Process for checking for manual backups



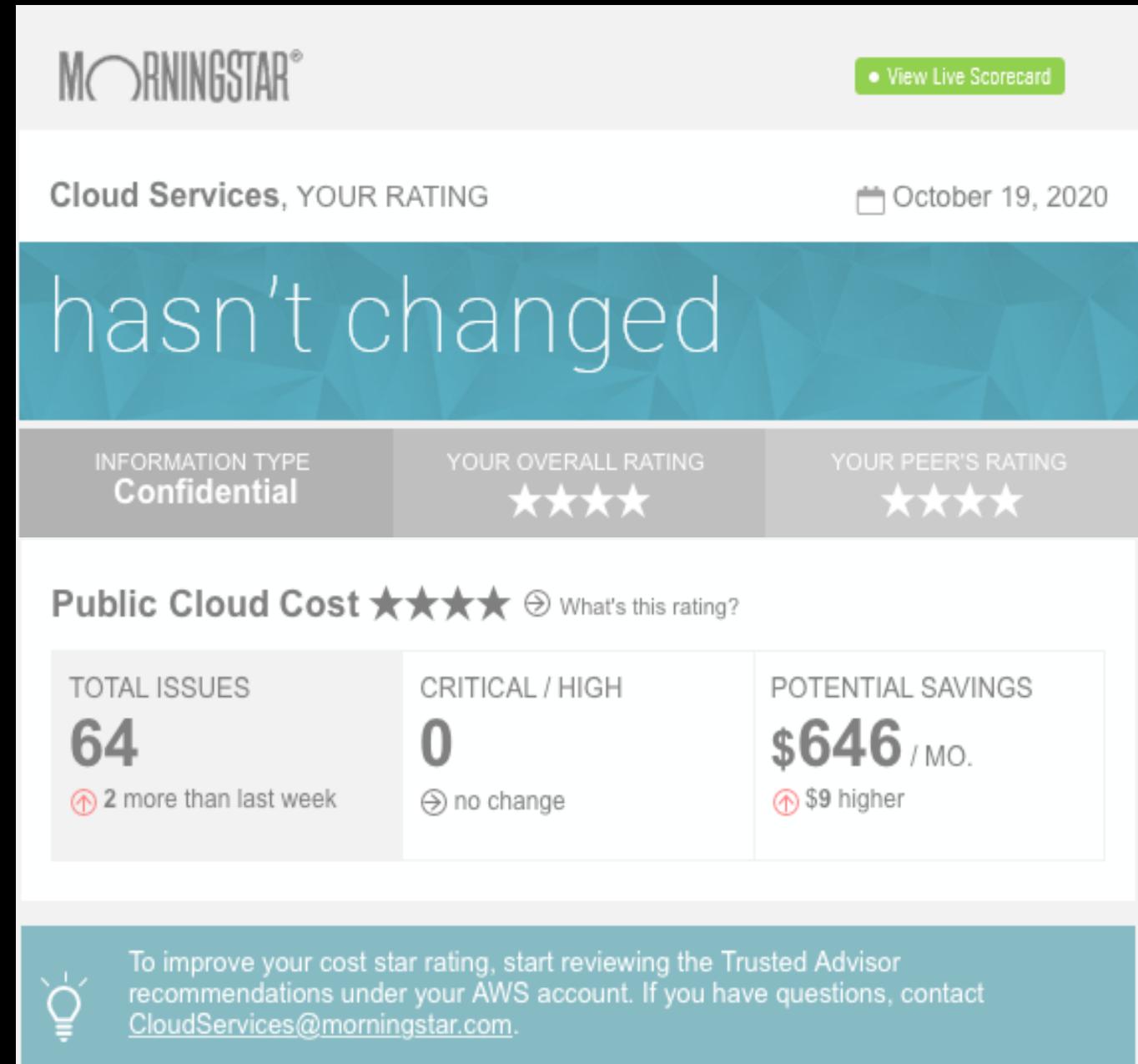
# Database backup checks



# What's next for Morningstar

- Scanning for more services
- Expanded scan criteria
- Automated actions for tagging
- Complex analyses and workflows

# Prove it



The screenshot shows a Morningstar scorecard for Cloud Services. At the top, the Morningstar logo is on the left and a green button labeled "View Live Scorecard" is on the right. Below that, the text "Cloud Services, YOUR RATING" is on the left and the date "October 19, 2020" is on the right. A large blue banner in the center says "hasn't changed". Below the banner, there are three grey boxes: "INFORMATION TYPE Confidential", "YOUR OVERALL RATING ★★★★", and "YOUR PEER'S RATING ★★★★". Underneath, a section titled "Public Cloud Cost" shows a rating of ★★★★ with a link "What's this rating?". It also displays "TOTAL ISSUES 64" (with a note "2 more than last week"), "CRITICAL / HIGH 0" (with a note "no change"), and "POTENTIAL SAVINGS \$646 / MO." (with a note "\$9 higher"). At the bottom, a lightbulb icon has the text "To improve your cost star rating, start reviewing the Trusted Advisor recommendations under your AWS account. If you have questions, contact [CloudServices@morningstar.com](mailto:CloudServices@morningstar.com)".

@margaretvaltie

# Thank you!

Margaret Valtierra

Program Manager  
Morningstar  
[@margaretvaltie](https://twitter.com/margaretvaltie)  
[#ChicagoAWS](https://twitter.com/ChicagoAWS)



Please complete  
the session survey

