
AWS
re:Invent

COM304

How robots can help make your AWS accounts more secure

Margaret Valtierra
Program Manager
Morningstar

AWS re:Invent

Challenges

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

Solution: Robots?

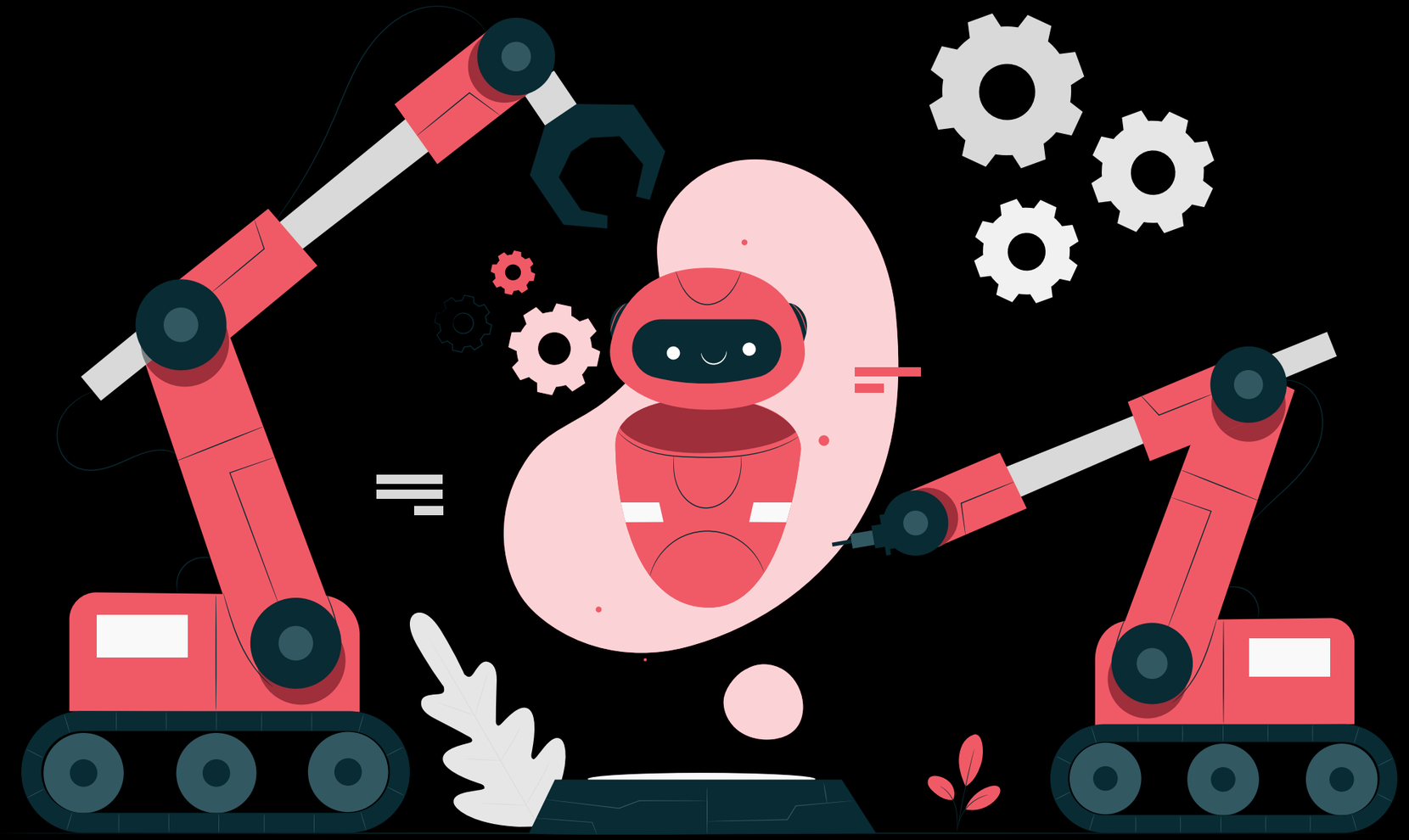
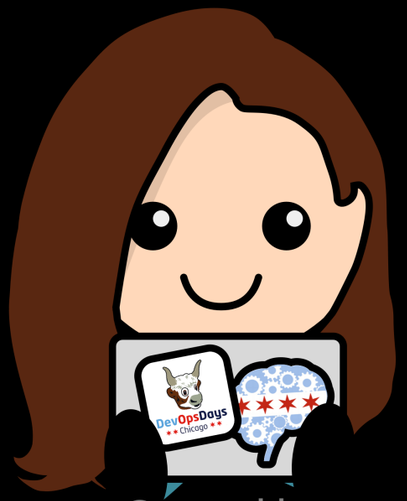


Image source: Freepik.com

About me

Program manager, Morningstar
AWS Community Hero
Chicago AWS user group leader
DevOpsDays Chicago organizer



Created by
@sosplush

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

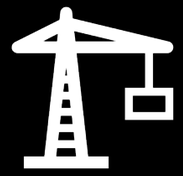
Morningstar's public cloud setup

AWS re:Invent

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

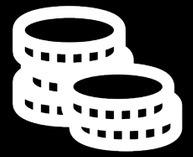


Architecture

Architectural guidance
POCs

Infra

Account creation
Connectivity
Infrastructure as code



Finance

Financial
Governance
Budgeting
Cost optimization

Security

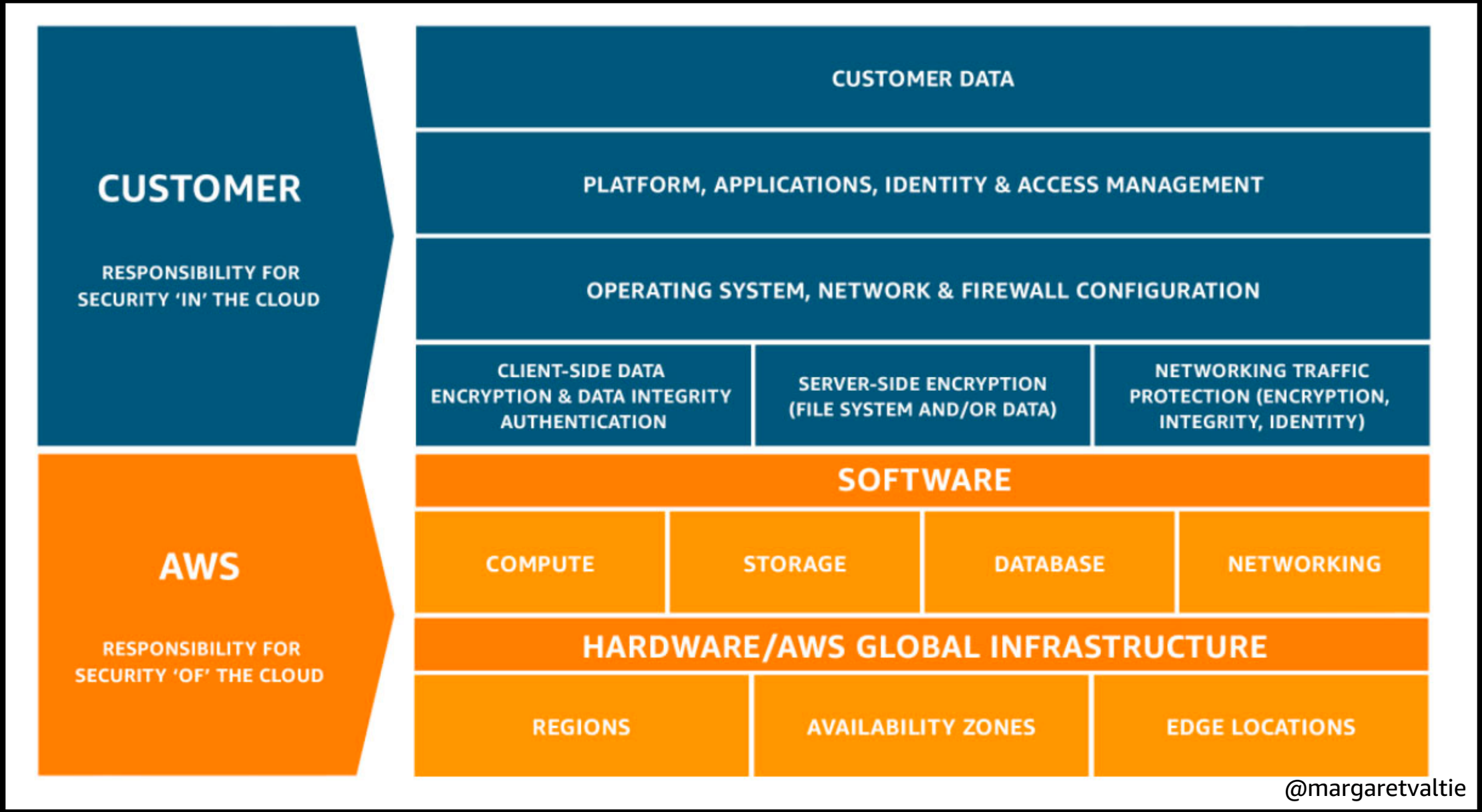
Governance
Security
Scanning

Operations

Deployment pipelines
Backups
Operational support

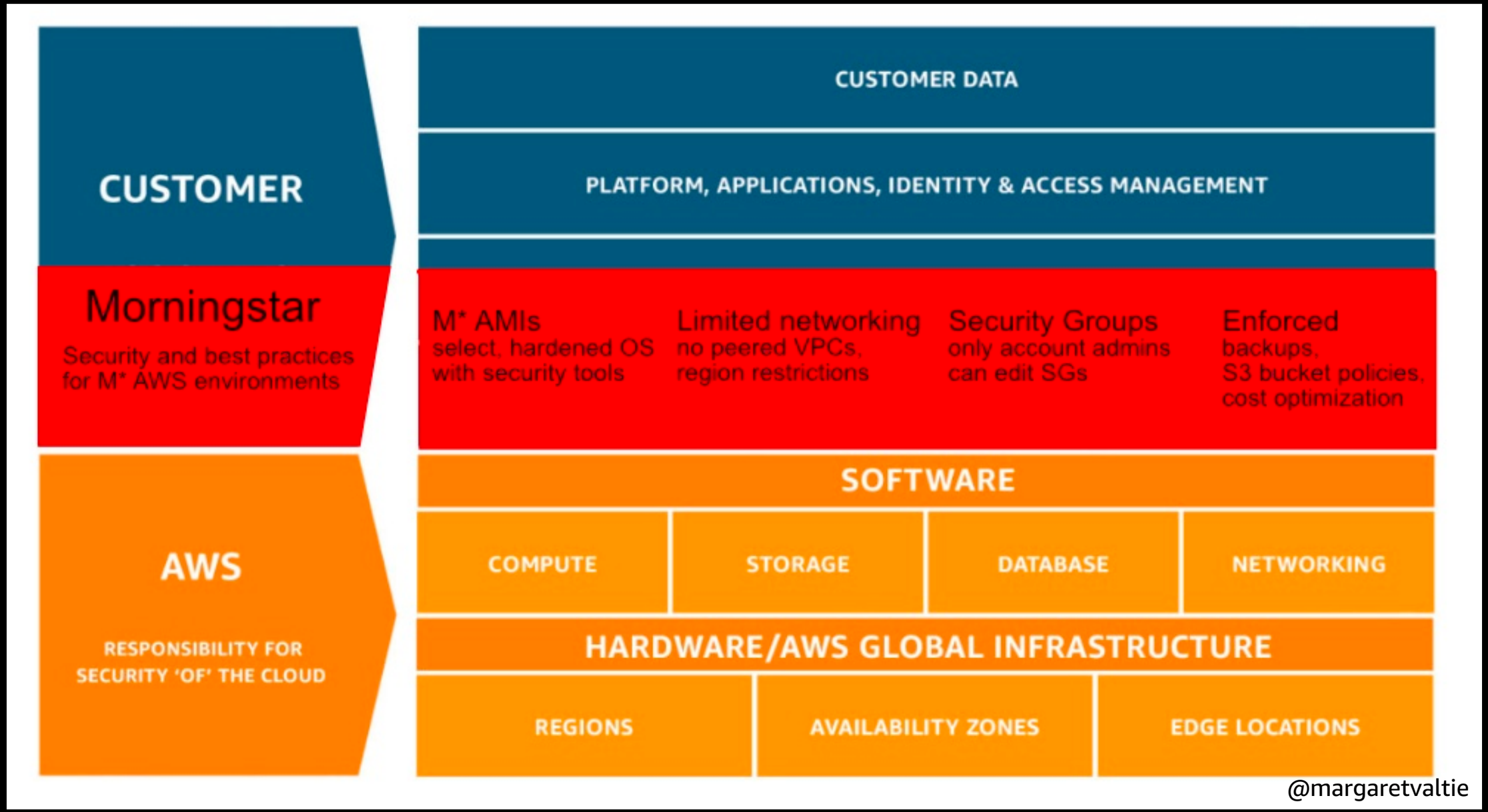
@margaretvaltie

The AWS shared responsibility model



@margaretvaltie

Morningstar's responsibility model



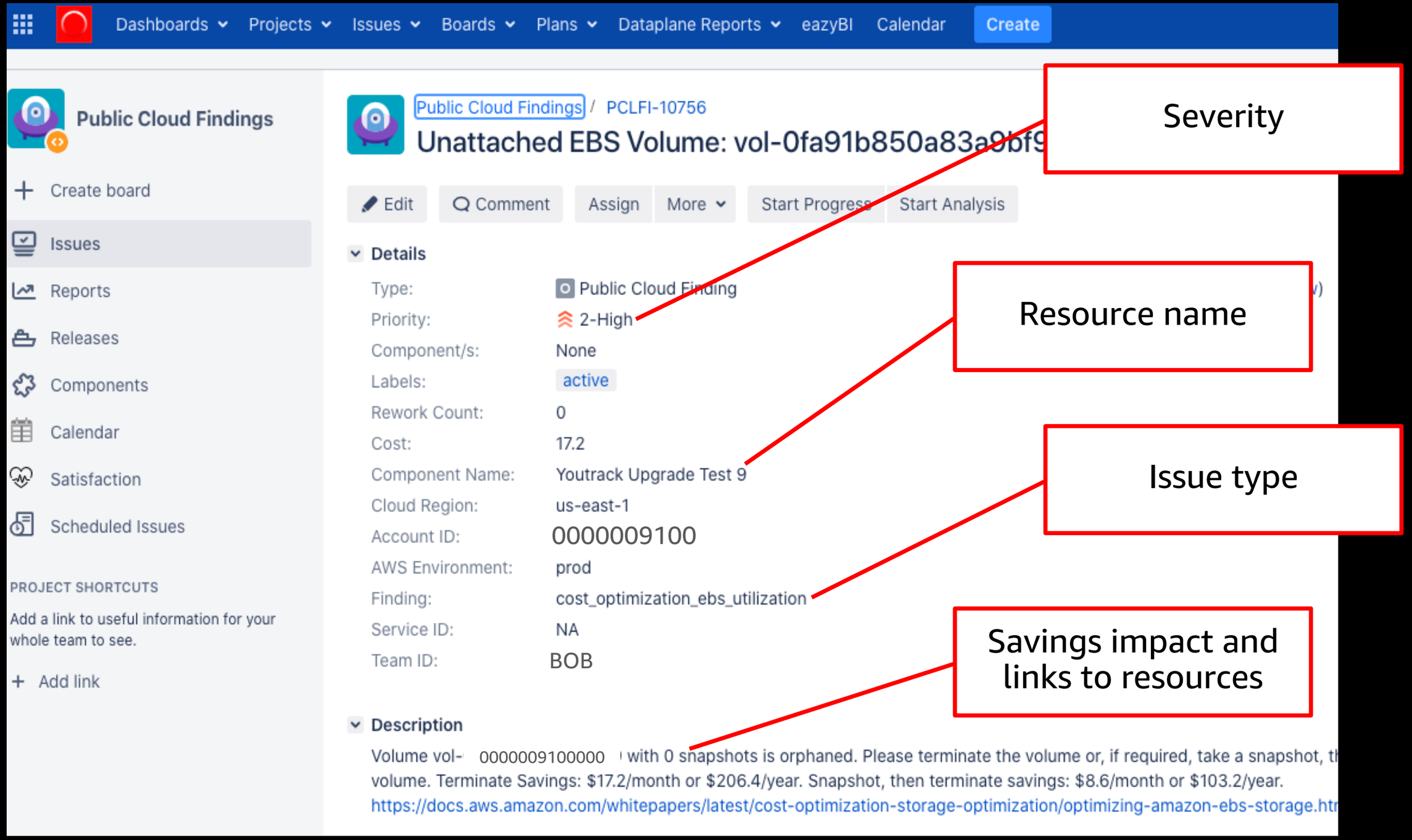
@margaretvaltie

Enforcement: Guardrails + behavior

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

Trusted source

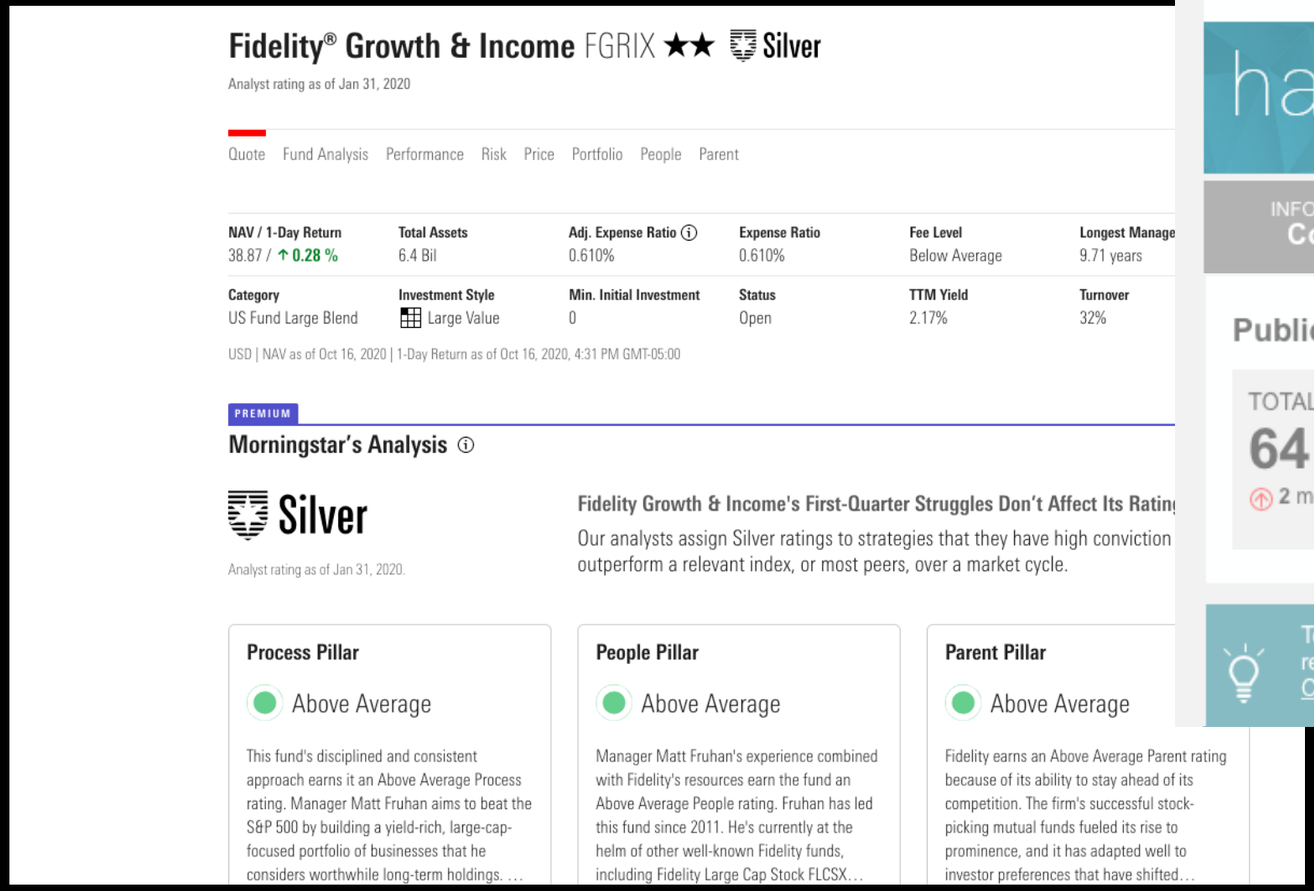
- AWS Trusted Advisor and AWS Well-Architected Framework
- Actionable, account-based recommendations

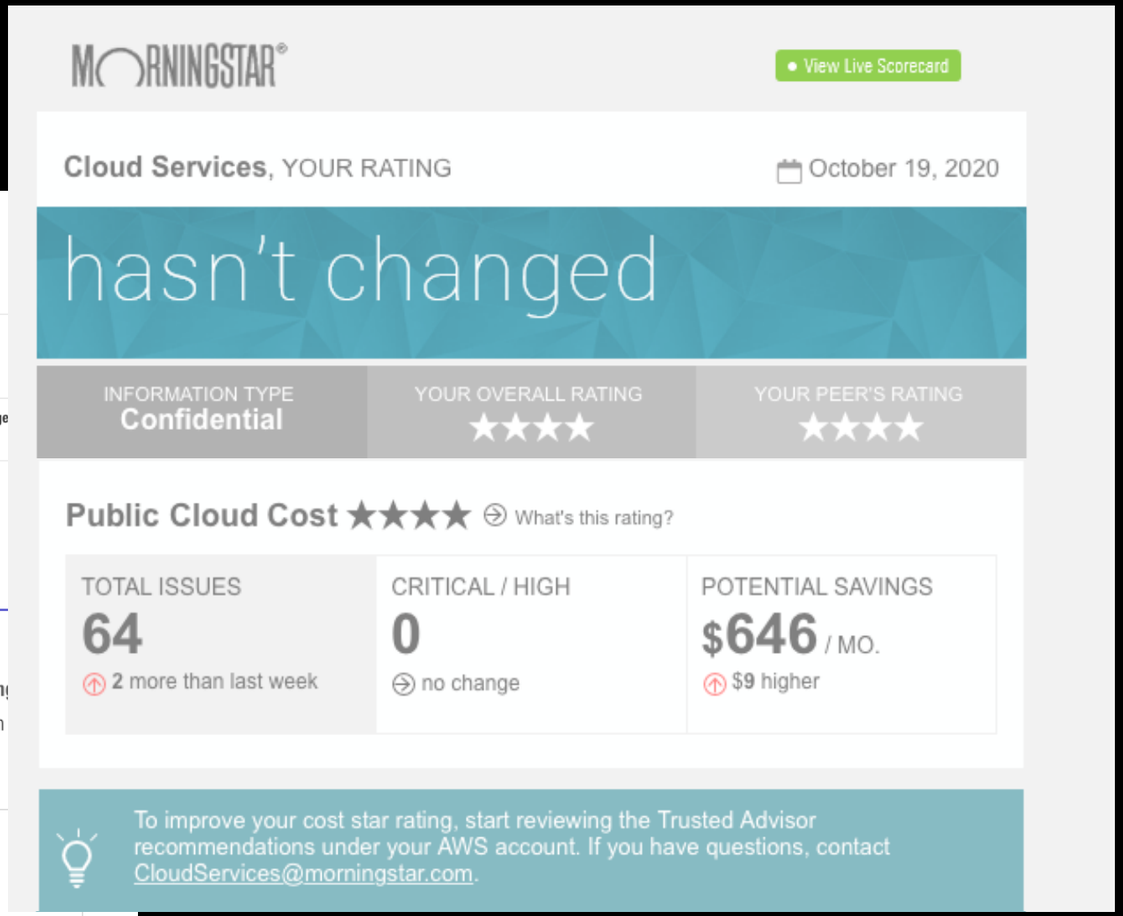

Dashboards
Projects
Issues
Boards
Plans
Dataplane Reports
eazyBI
Calendar
Create
Public Cloud Findings
Create board
Issues
Reports
Releases
Components
Calendar
Satisfaction
Scheduled Issues
PROJECT SHORTCUTS
Add a link to useful information for your whole team to see.
Add link
Public Cloud Findings / PCLFI-10756
Unattached EBS Volume: vol-0fa91b850a83a9bf9
Edit
Comment
Assign
More
Start Progress
Start Analysis
Details
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
Description
Volume vol- 0000009100000 with 0 snapshots is orphaned. Please terminate the volume or, if required, take a snapshot, th
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.htr
Severity
Resource name
Issue type
Savings impact and links to resources

Rated cloud compliance

SCORECARDS ARE KINDA OUR THING

MORNINGSTAR





@margaretvaltie

Event-based triggers

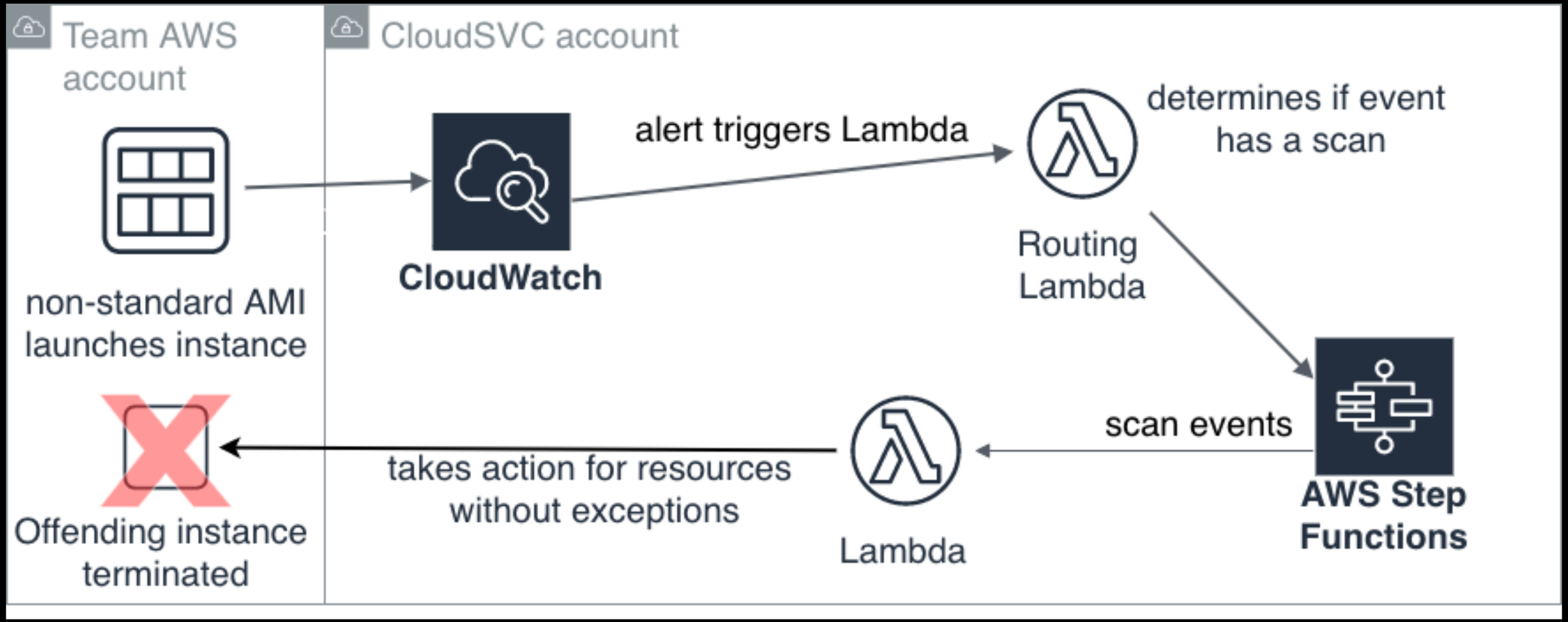
Goal: Secure instances only

- 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

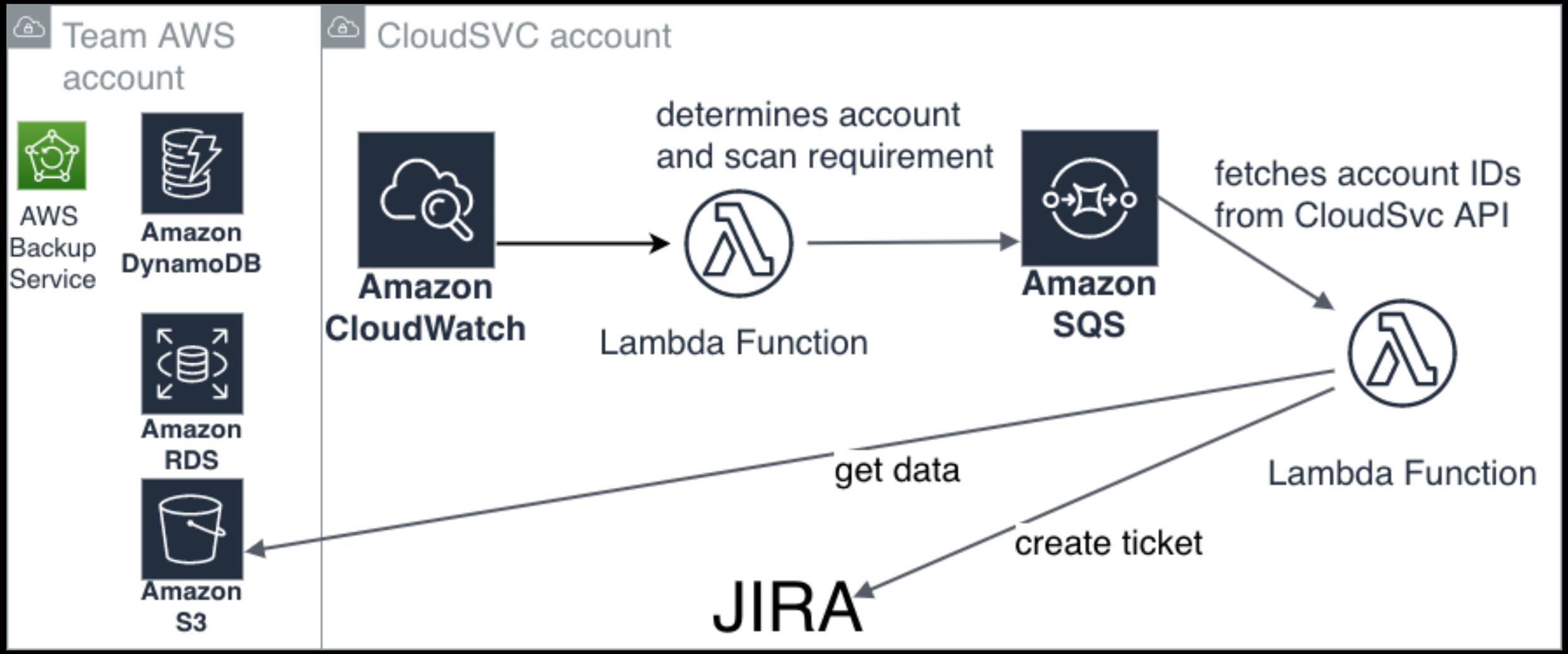
Goal: Ongoing compliance

- 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

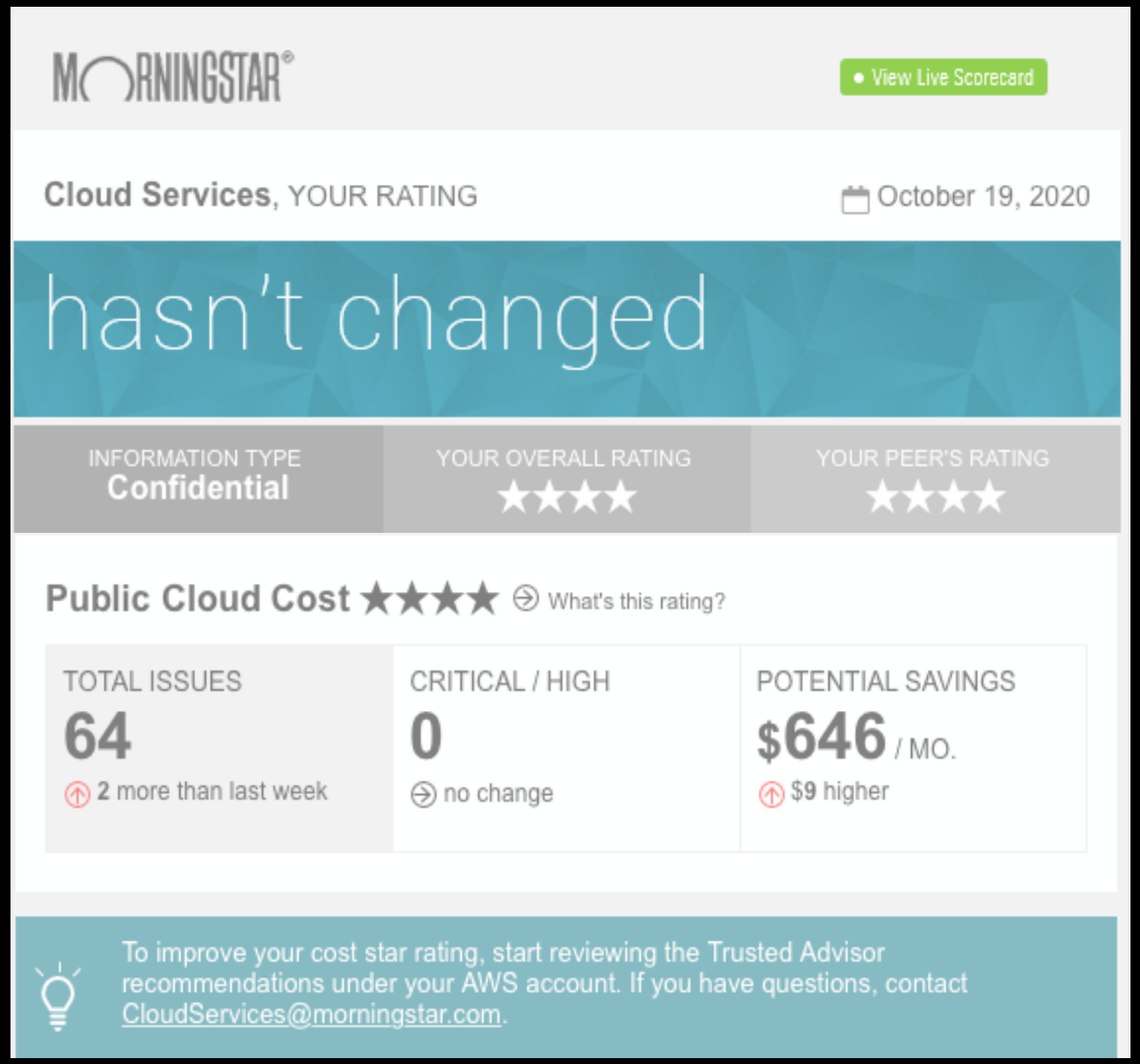
Database backup checks



What's next for Morningstar

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

Prove it


MORNINGSTAR®
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.

Thank you!

Margaret Valtierra

Program Manager
Morningstar
@margaretvaltie
#ChicagoAWS

AWS re:Invent

Please complete the session survey

AWS re:Invent