

Securing 250 accounts: Maintain guardrails for self-serve cloud adoption

Margaret Valtierra (she/her/hers)

Program Manager

Morningstar



Challenges

250 teams on AWS using 600+ accounts

Decentralized, product-driven teams

Self-service model

Focus on cost-optimization

Emphasize best practices

Industry regulation and compliance requirements



Photos

Margaret Valtierra

AWS Community Hero
Chicago AWS user group leader

MORNINGSTAR®

Join me at DevOpsDays Chicago!
devopsdays.com/chicago



Image by
@sosplush

Guardrails at scale

Strong foundations: Self-service with guardrails

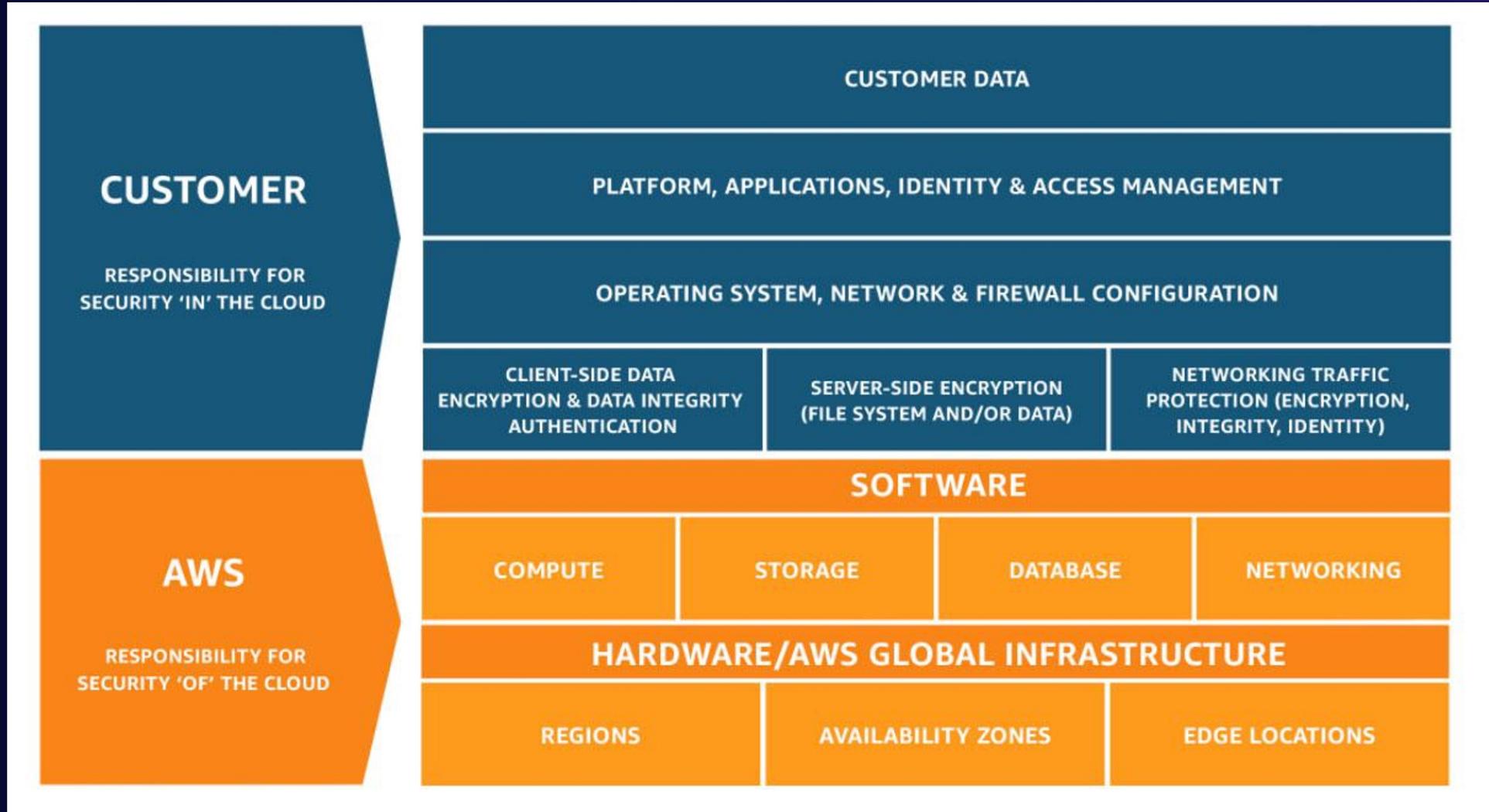
Trust, but auto-terminate

Scorecards for best practices

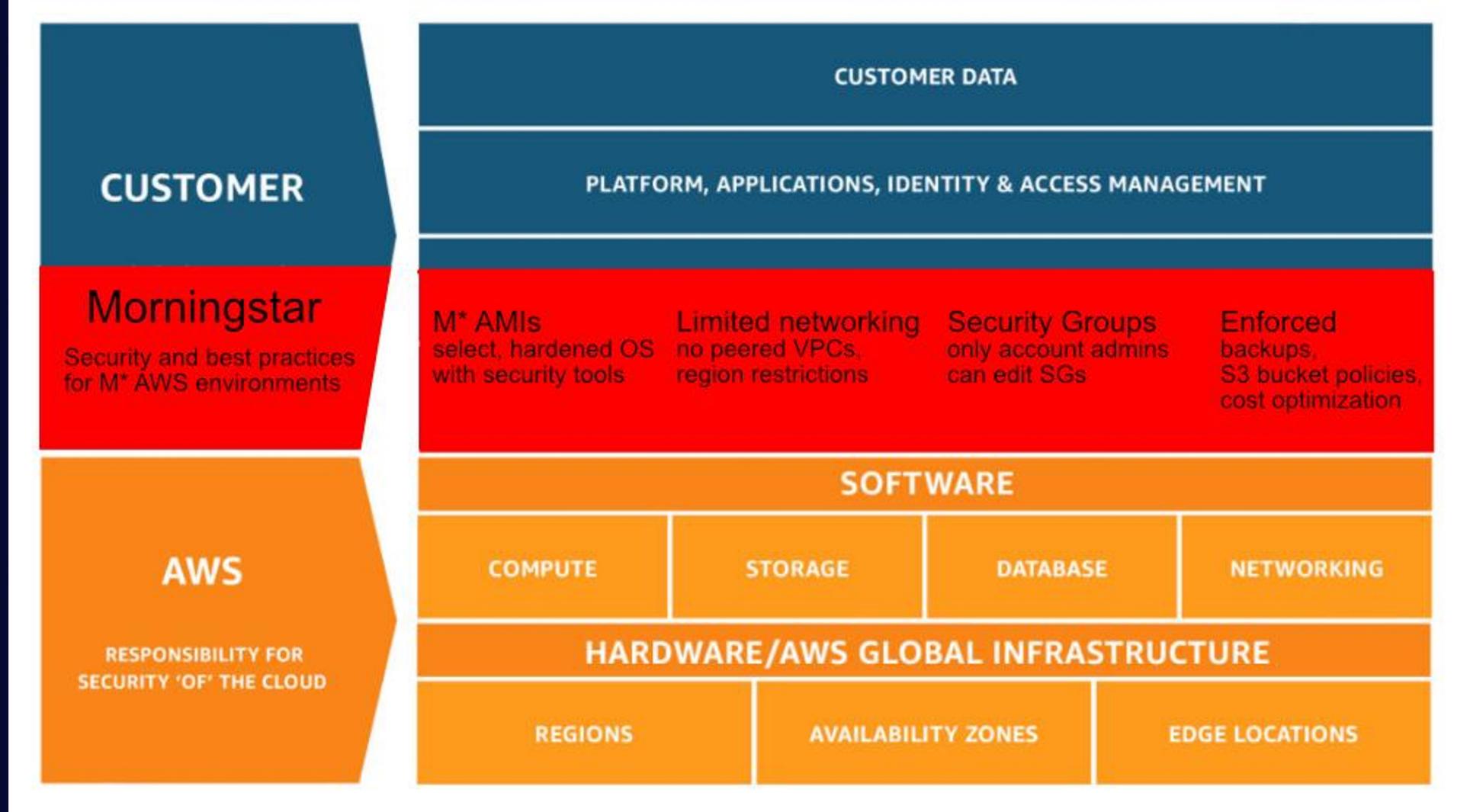
Adapting our guardrails

Up next: Moving cloud-native

AWS shared responsibility model

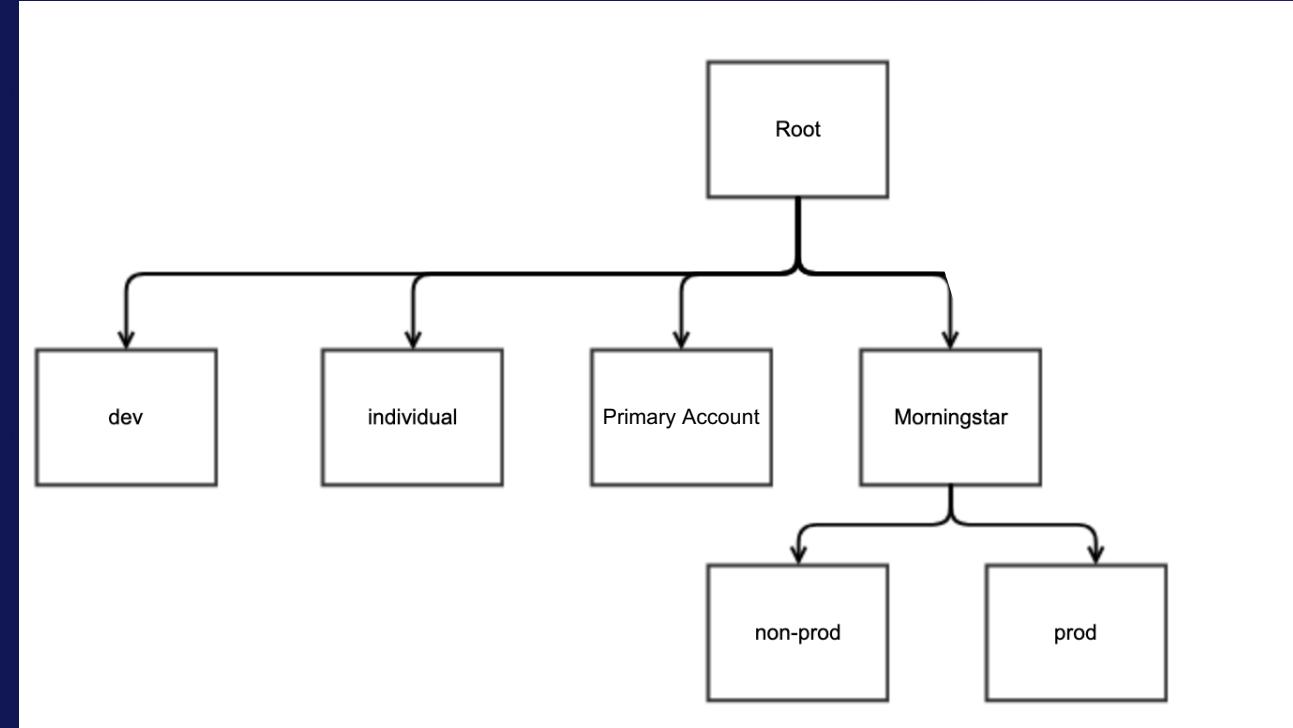


Our shared responsibility model



Strong foundations: Organization

- Team accounts for each product team
- Environment separation at account level
- Central billing, network and shared service accounts
- Limited VPC peering between accounts



Strong foundations: Accounts

Out of the box team accounts

- Configured core networking
- Uniform access with 3 standard IAM roles
- Standardized services
- Created via infrastructure as code (IaC)
- 24/7 AWS Enterprise Support



Read-only



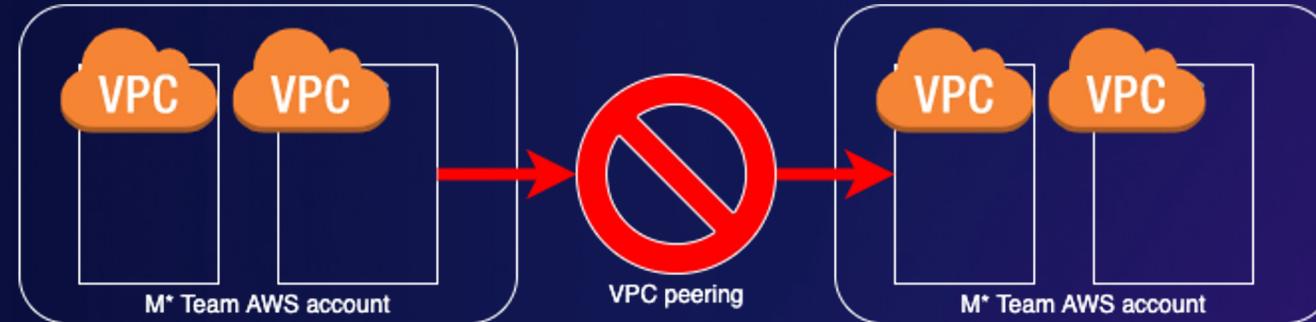
Operator



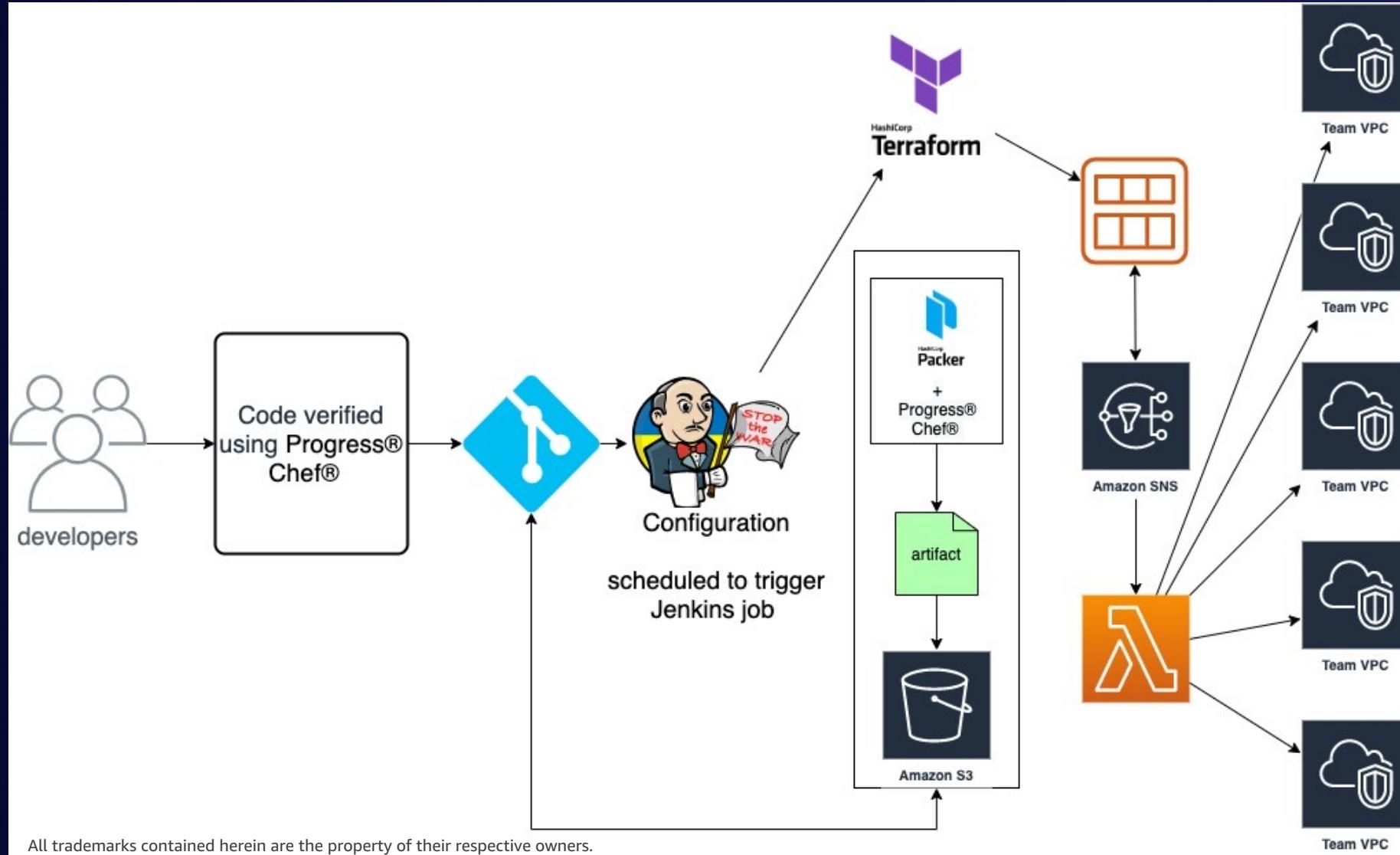
Admin

Strong foundations: Users

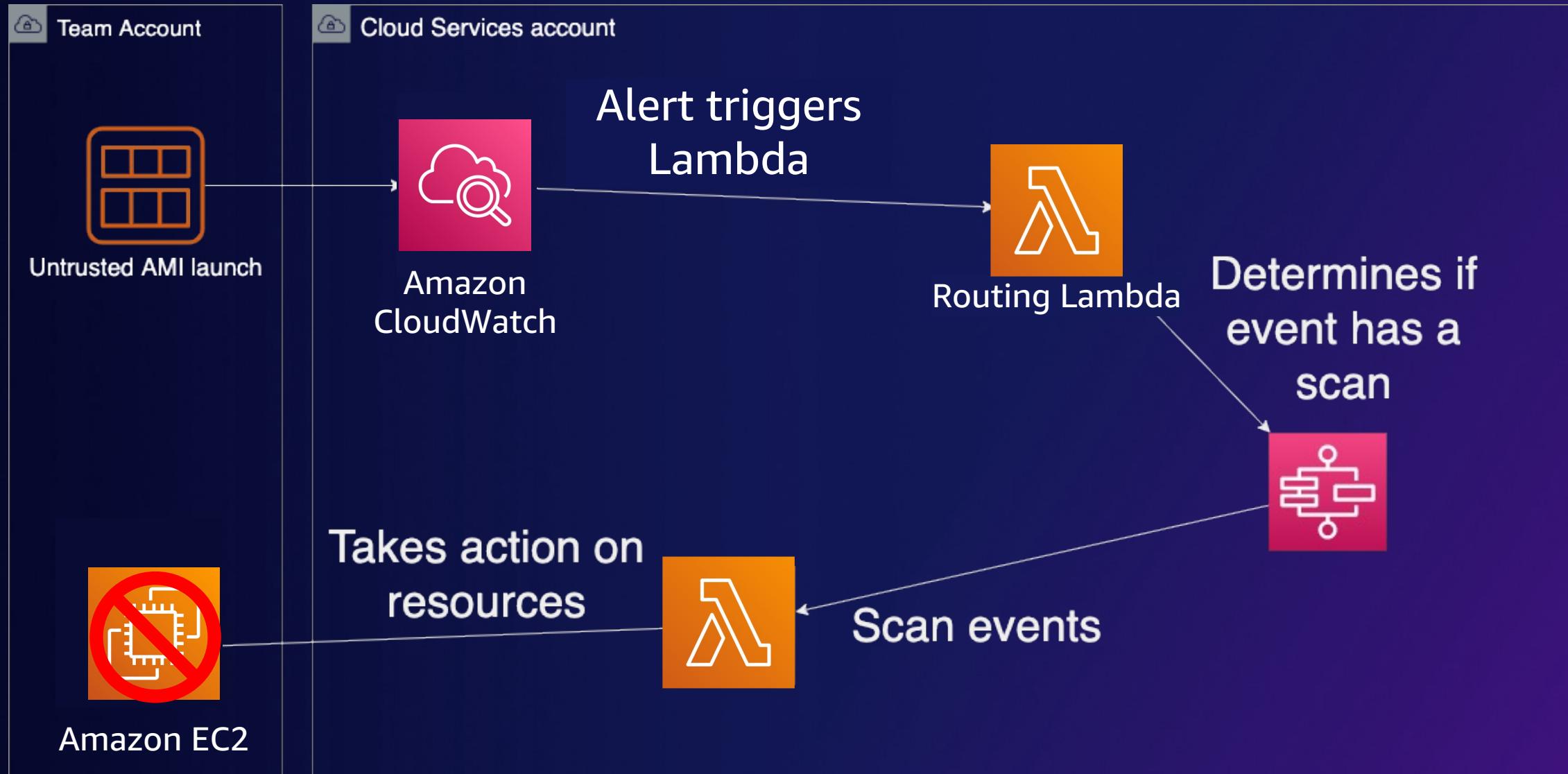
- Self-service capabilities
- Choice of tools and services
- Team-level ownership and customization
- Limited connectivity between accounts



Standard Amazon EC2 AMIs



Trust, but auto-terminate



Scorecards are kinda our thing

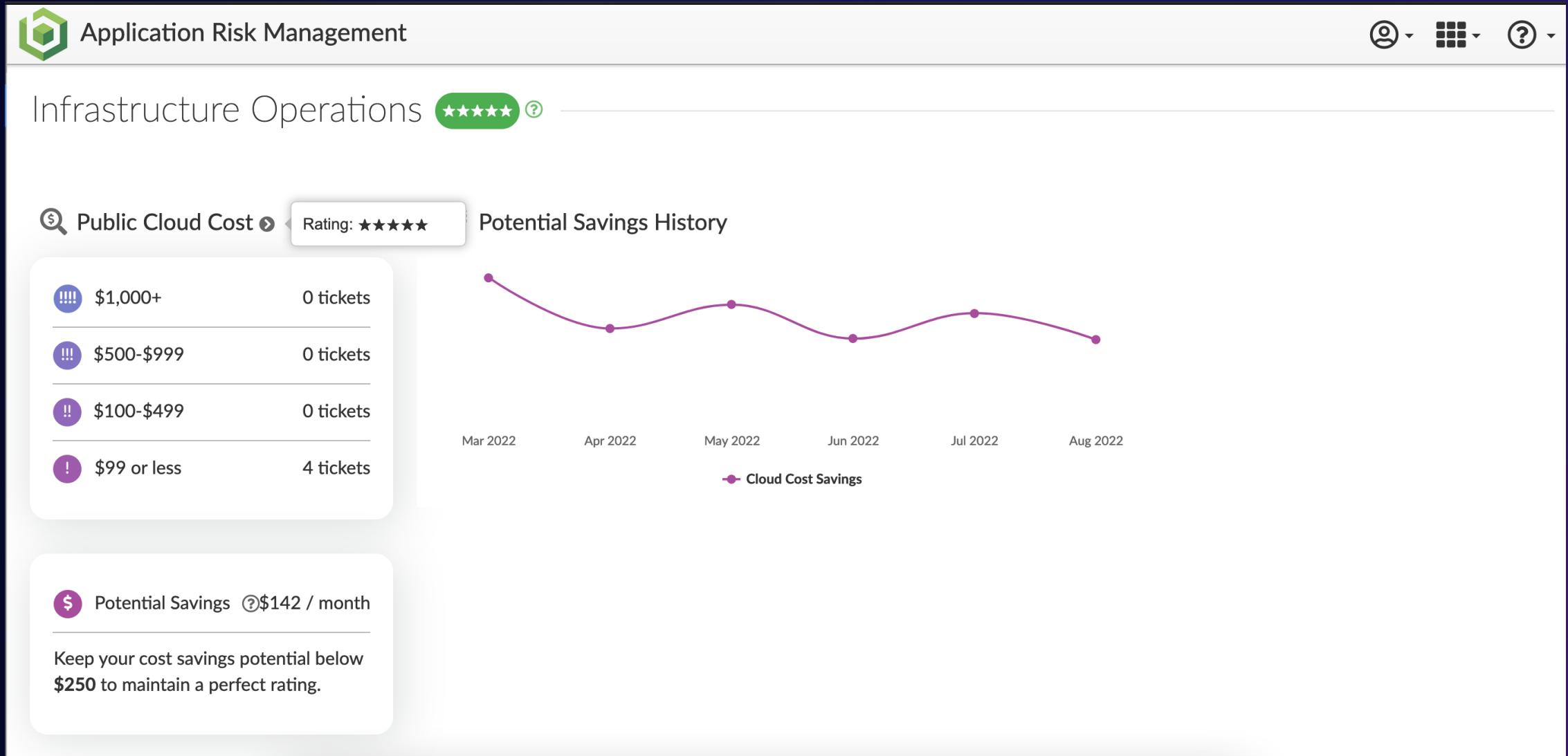
Overview of Morningstar's Fund Ratings

| Rating | Iconography | Type of Assessment | Benchmark | Eligibility Requirement |
|---|--|--|----------------------------|-------------------------|
| Star Rating (Incept: 2002) | ★★★★★ | <ul style="list-style-type: none">▶ Backward-looking, quantitative▶ Based on past risk-adjusted returns | Morningstar Category Peers | 36 months of returns |
| Analyst Rating (Incept: 2011) | Gold Silver Bronze Neutral Negative | <ul style="list-style-type: none">▶ Forward-looking, qualitative▶ Based on analysts' assessment of people, process, parent, and fees | Morningstar Category Index | None |
| Quantitative Rating (Incept: 2017) | Gold ^Q Silver ^Q Bronze ^Q Neutral ^Q Negative ^Q | <ul style="list-style-type: none">▶ Forward-looking, quantitative▶ Based on algorithmic assessment of people, process, parent, and fees | Morningstar Category Index | 1 month of returns |
| Sustainability Rating (Incept: 2019) | | <ul style="list-style-type: none">▶ Backward-looking, quantitative▶ Based on ESG risk assessment of funds' portfolio holdings | Morningstar Category Peers | Various |

MORNINGSTAR®



Cloud cost and risk scores



Product scorecards

Public Cloud Cost Report



Weekly Public Cloud Cost Report

The Public Cloud Cost Star Rating transparently measures cost optimization potentials and provides teams a self-service method to manage AWS. You can directly view cloud cost impact per resource in each Jira ticket. Rating methodology is determined by cost optimization targets and AWS Trusted Advisor. Ticket severity is determined by **total monthly savings potential**. For full methodology, steps to resolve, and FAQs [see the Public Cloud Cost Star Scorecard wiki](#).

 Subscribe users to this report by requesting access to the **Public Cloud Finance AD Group** in [Sailpoint](#).

| Product | TID | Cost Rating | Potential Savings (\$/month) | Change | Total Tickets | Critical | High |
|-------------------------|---------|-------------|------------------------------|-----------|---------------|----------|------|
| Data Services | DATASVC | ★ | \$10,475 | ▼ \$1,749 | 88 | 0 | 0 |
| DBRS | DBRS | ★ | \$9,483 | ▼ \$189 | 263 | 1 | 1 |
| Core Analytics Platform | CAP | ★ | \$7,086 | ▲ \$836 | 55 | 0 | 2 |
| International Sites | EURT | ★ | \$4,447 | ▼ \$1,353 | 51 | 0 | 0 |
| Mobile Solutions | MOB | ★ | \$3,873 | \$0 | 20 | 0 | 0 |
| Data Collection | DC | ★ | \$3,672 | ▼ \$177 | 174 | 0 | 0 |
| Quantitative Research | QUANT | ★ | \$3,538 | ▲ \$3,036 | 24 | 1 | 1 |
| Information Security | INFOSEC | ★ | \$2,995 | ▼ \$538 | 39 | 0 | 1 |



Scorecard sources: AWS

AWS Trusted Advisor

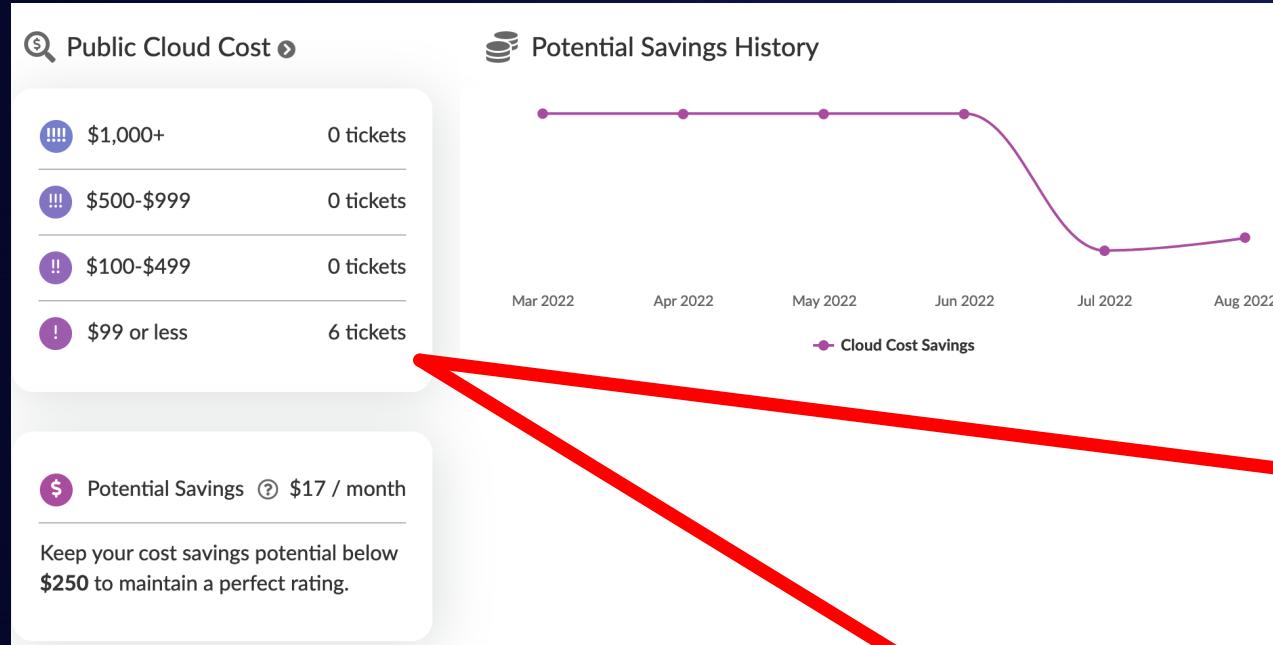
The screenshot shows the AWS Trusted Advisor Overview page. At the top, it displays "Potential monthly savings" of \$1,816.57. Below this, there are four status indicators: "Action recommended" (0), "Investigation recommended" (3), "No problems detected" (13), and "Checks with excluded items" (46). The "Cost optimization checks" section includes filters for "Tag Key" and "Tag Value", and buttons for "Reset" and "Apply filter". It also features search by keyword and source, with dropdowns for "Filter checks", "All sources", and "Investigation re...". A detailed section titled "Low Utilization Amazon EC2 Instances" is expanded, stating that it checks for instances running at 10% CPU utilization or less over 14 days. It found 6 of 32 instances to be underutilized, with monthly savings up to \$1,796.37. The page is last updated 5 hours ago.

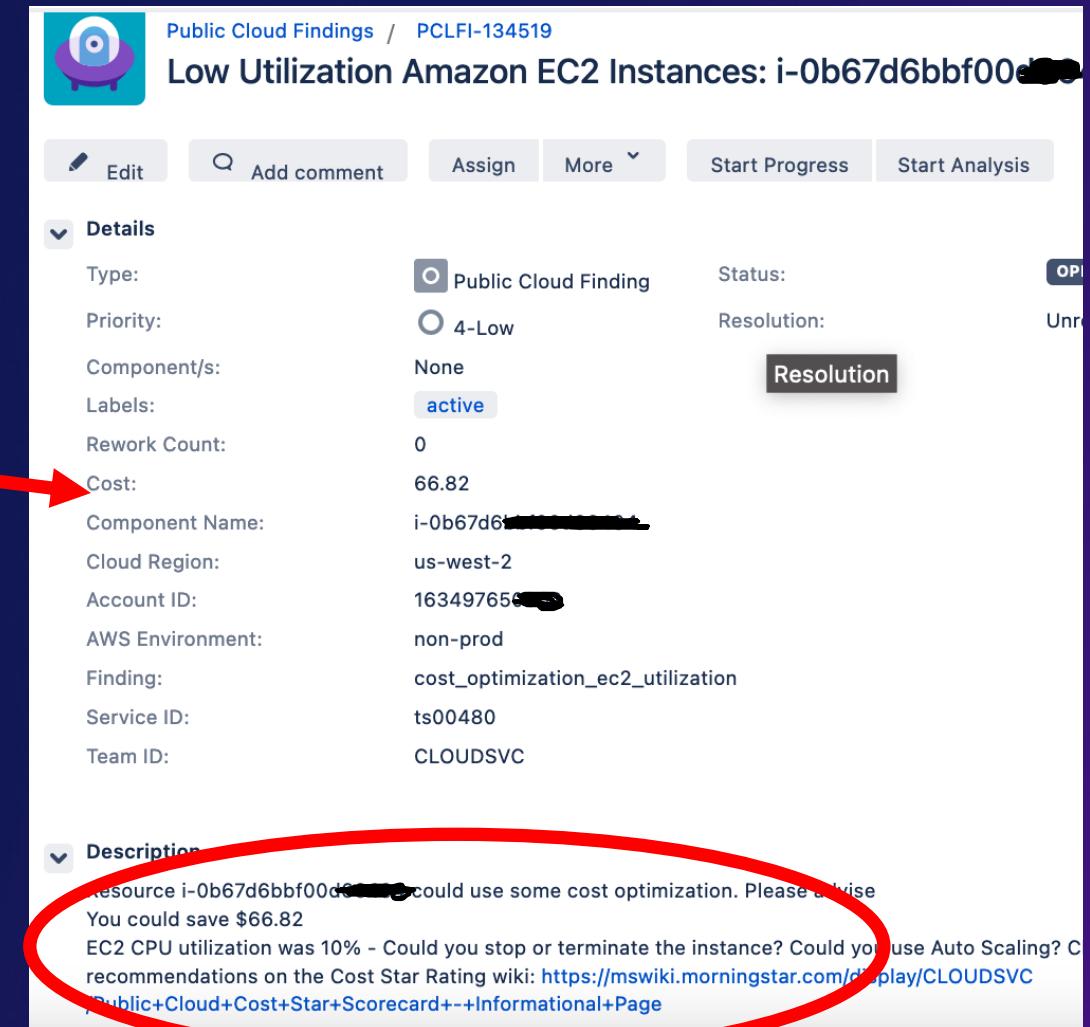
AWS Compute Optimizer

The screenshot shows the AWS Compute Optimizer Findings page for EC2 instances. It indicates 58 instances in total. A "View recommendations" button is available. The findings are categorized into three states: Under-provisioned (8.62%) with 5 instances, Optimized (18.97%) with 11 instances, and Over-provisioned (72.41%) with 42 instances. A horizontal bar chart visualizes the distribution of these states.

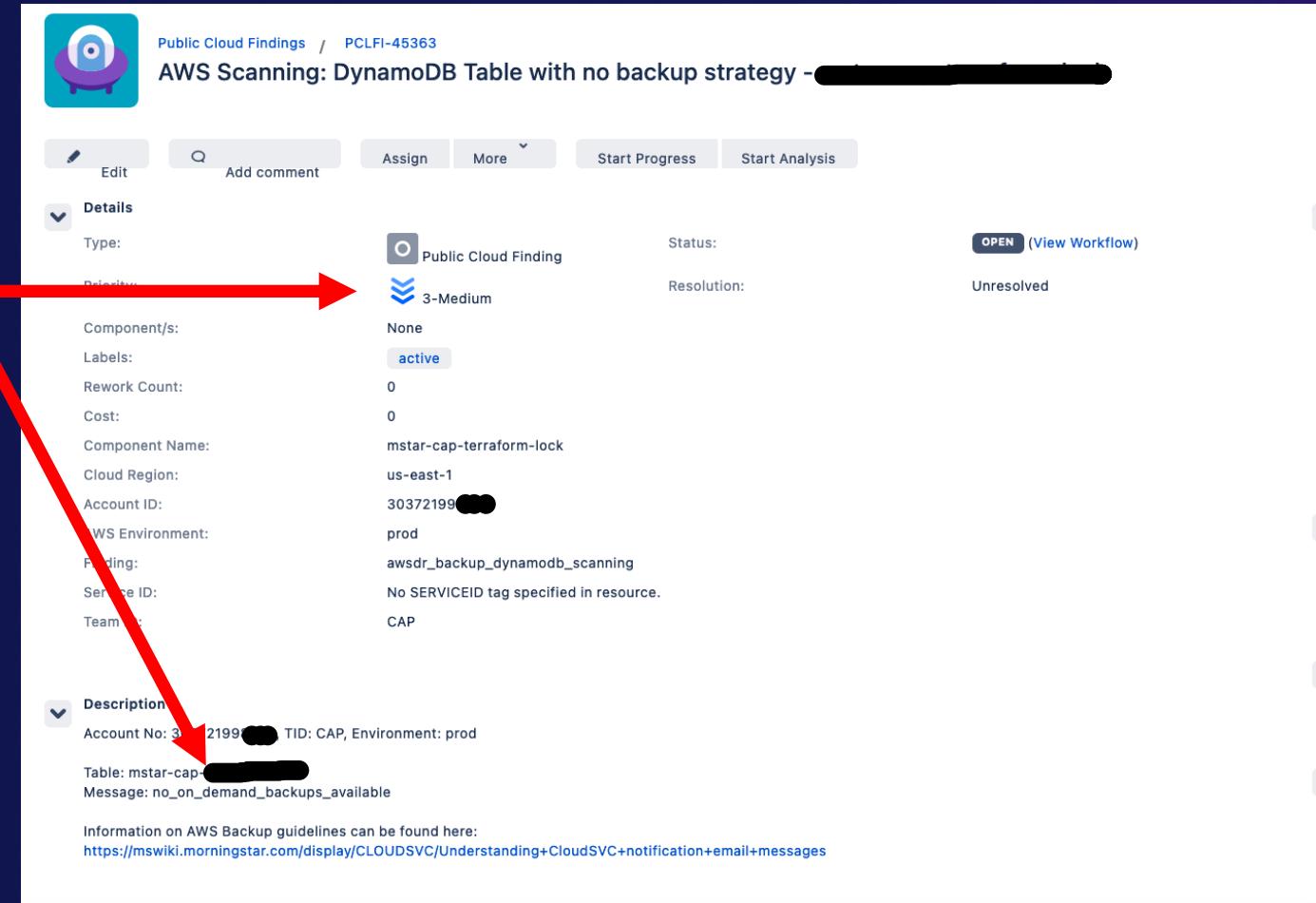
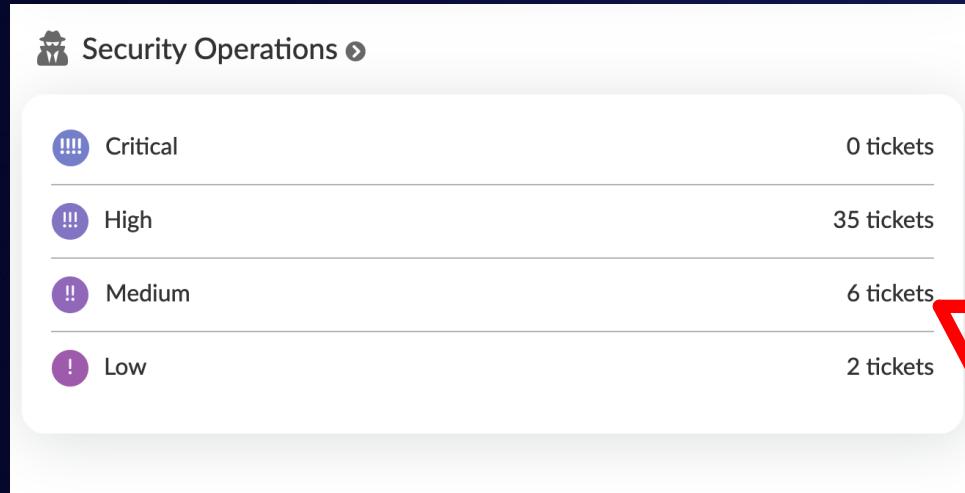


Scorecard outputs: Tickets for teams



A screenshot of a ticket detail view for a 'Public Cloud Finding'. The ticket ID is PCLFI-134519, titled 'Low Utilization Amazon EC2 Instances: i-0b67d6bbf00d...'. The ticket has a status of 'Open' and a priority of '4-Low'. It is labeled 'active' and has a cost of 66.82. The ticket is associated with component 'i-0b67d6bbf00d...', region 'us-west-2', account '16349765...', AWS environment 'non-prod', finding 'cost_optimization_ec2_utilization', service 'ts00480', and team 'CLOUDSVC'. A red arrow points from the 'Cost' field in the ticket details back to the 'Potential Savings' section of the scorecard. Another red arrow points from the 'Description' section of the ticket detail view, which contains a note about cost optimization and a link to the Cost Star Rating wiki.

Scorecard outputs: Tickets for teams

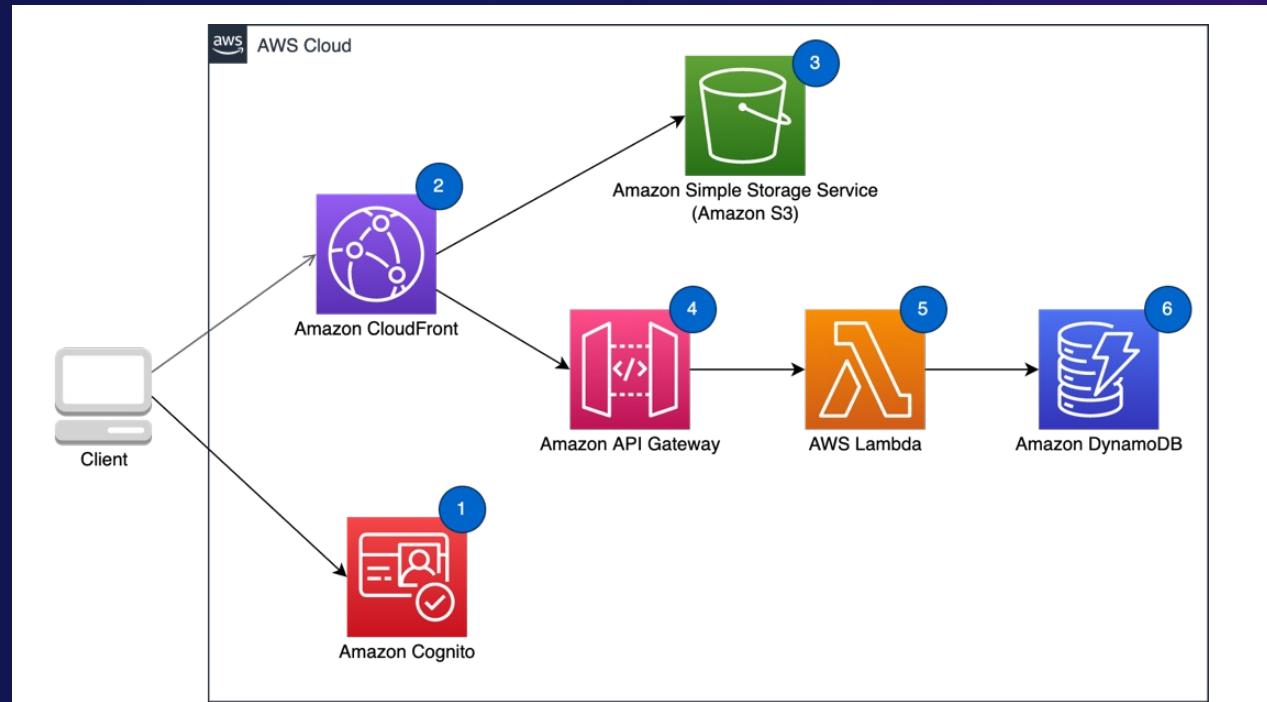


Time-based scan workflow

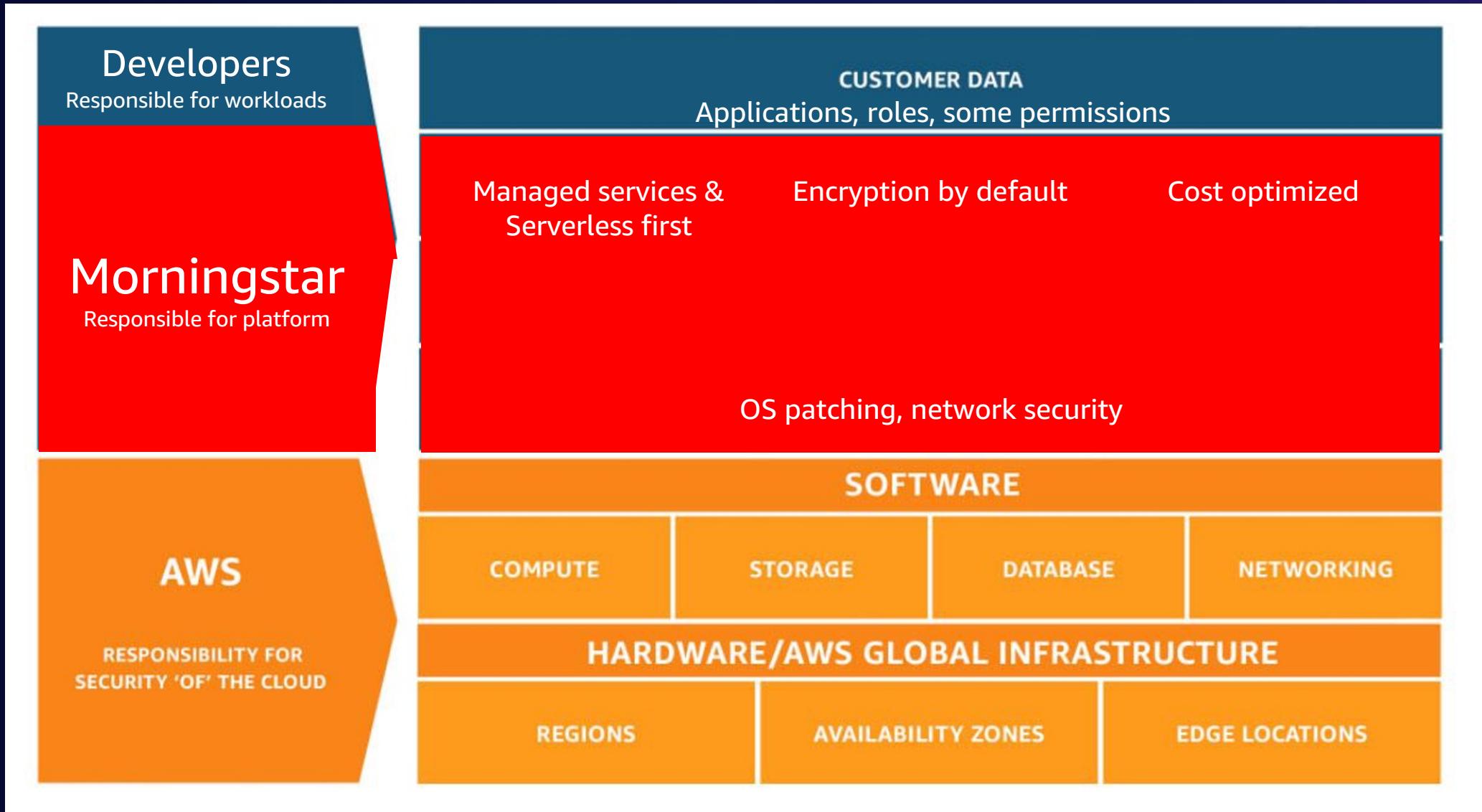


What's next

- Only pipelines deploy to prod
- Automations for security group change
- Encryption by default
- Well-Architected inputs and recommendations



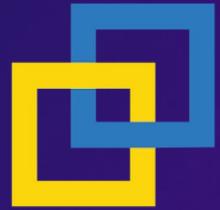
What's next



#SupportUkraine



CHARITY FOUNDATION 'KOLO'



RAZOM

Together We Are Ukraine



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Margaret Valtierra

 @margaretvaltie

Dev301



Please complete
the session survey