Building an AWS Onramp: Maintaining Guardrails for Self-Service AWS

Margaret Valtierra
@margaretvaltie
Blue Team Con 2021

 Photos

How Do You Secure

- 600+ AWS accounts
- 2,500 EC2 instances run
- 9,8000 S3 buckets in use
- 90,000 GB data transfers
- $40,000 cost

Per Day?

Margaret Valtierra

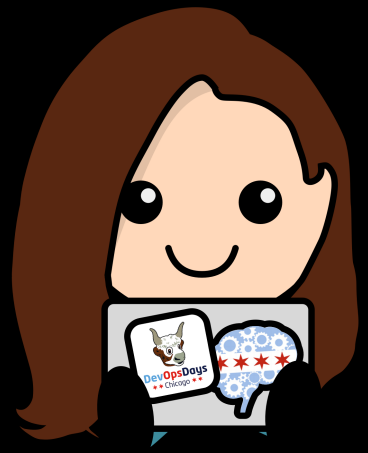


Image by @sosplush

Program Manager, Morningstar

AWS Community Hero

DevOpsDays Chicago Organizer

Chicago AWS user group leader

Building an AWS Onramp: Maintaining Guardrails for Self-Service AWS

- Build strong foundations: account set up
- Enable teams: security ownership at scale
- Enforce best practices: trust, but auto-terminate

A note on my co-presenters:

Matt

Nick

MORNINGSTAR®

A note on my co-presenters:

Matt

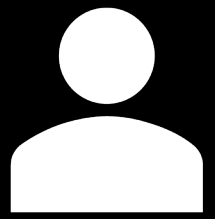
Nick

MORNINGSTAR®

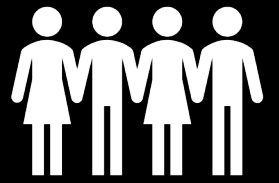
Foundations

AWS Account Structure:

Individual

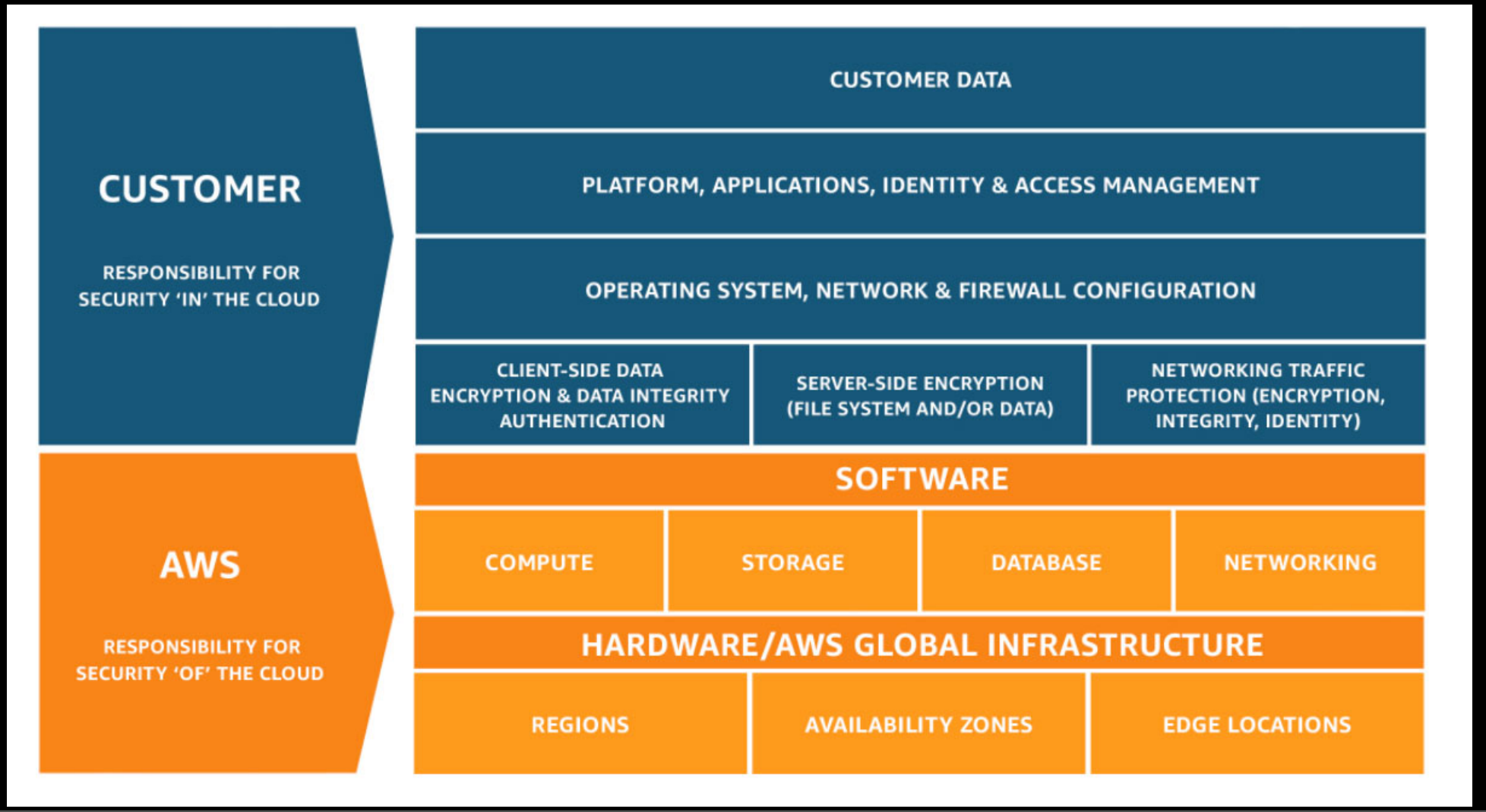


Team



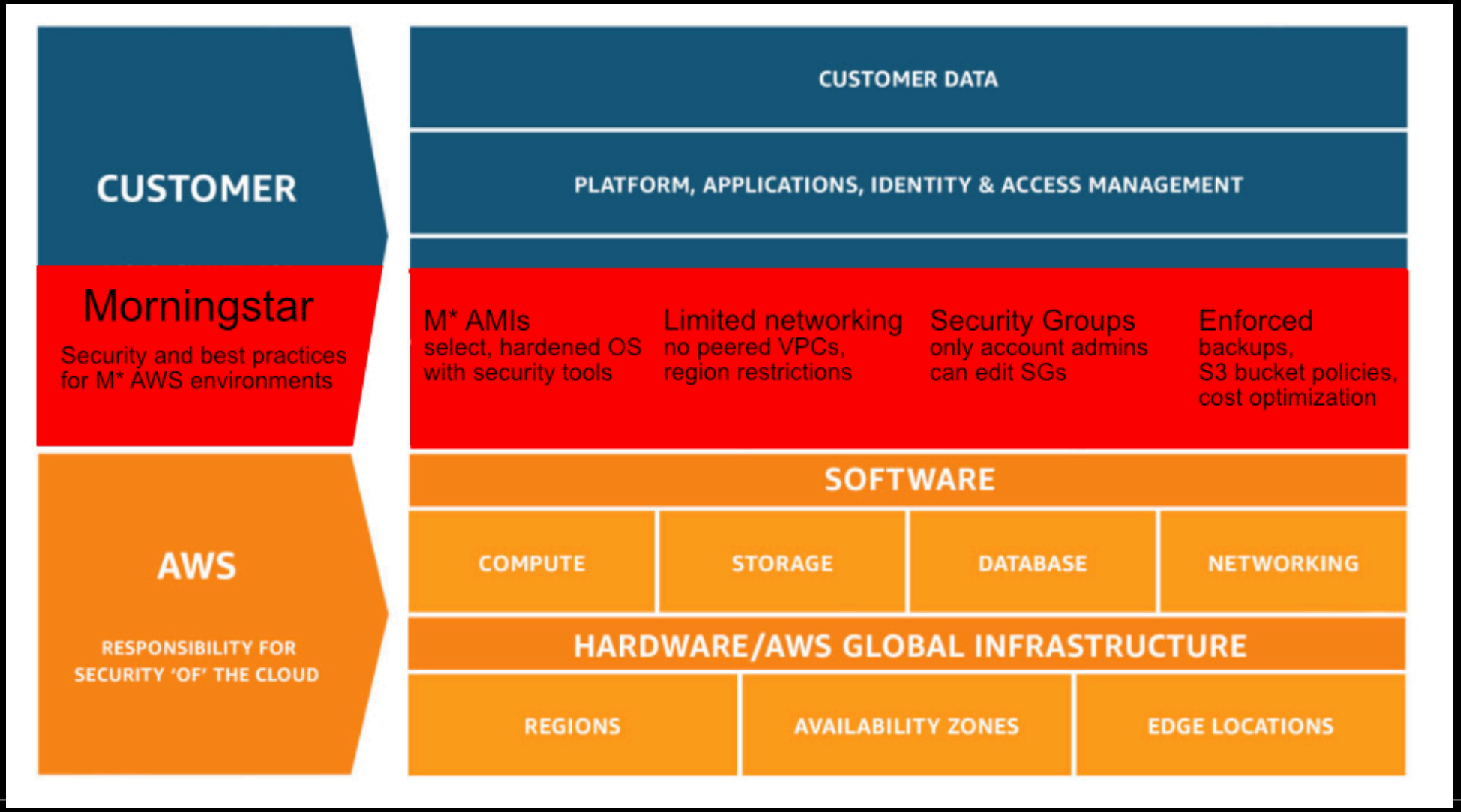
- Environment separation at account level
  - Production AWS account = UAT, PROD
  - Non-production AWS account = DEV, QA, STG
- Teams segmented into different accounts

AWS Shared Responsibility Model



MORNINGSTAR®

Our Shared Responsibility Model



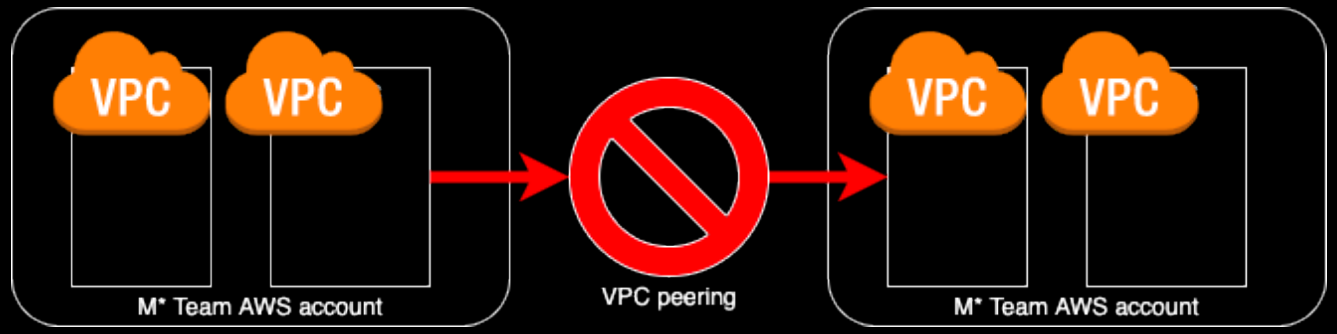
MORNINGSTAR®

Pre-built Amazon Machine Images (AMI)

- Patched, CIS hardened; monitoring and security built in
- Released monthly from central account to AWS team accounts
- SNS notifications trigger application pipelines & deployment

Standardized Network Controls

- Team accounts do not:
  - Allow traffic from AWS back to on-prem
  - VPC peer to other AWS accounts via VPC peering
- Network ACL vs Security Groups



MORNINGSTAR®

Monitoring and Alerting

- Team-level New Relic and Victor Ops via Amazon CloudWatch
- Centralized Splunk & Amazon GuardDuty alerts
  - IAM, keys, and root account changes
  - Network edit attempts

Centralized Security Processes

- 3 pre-defined IAM roles
- AWS Single Sign On with Okta MFA
- Certificates with Amazon Certificate Manager (ACM) and Private CA

MORNINGSTAR®

Enabling Teams to Own Security

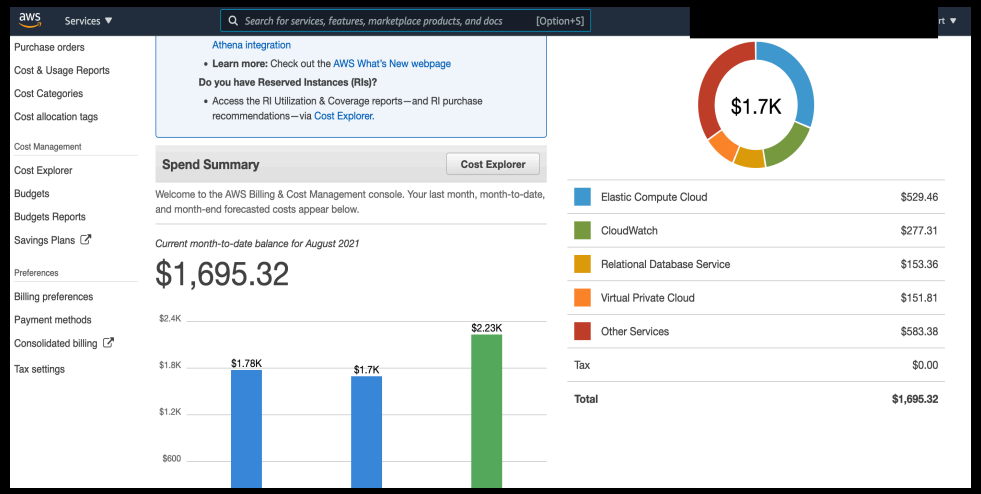
Well-Planned Foundations

- Stateful account configuration with GIT, Terraform
- AWS Enterprise Support 24x7
- Checks for budget approval at start

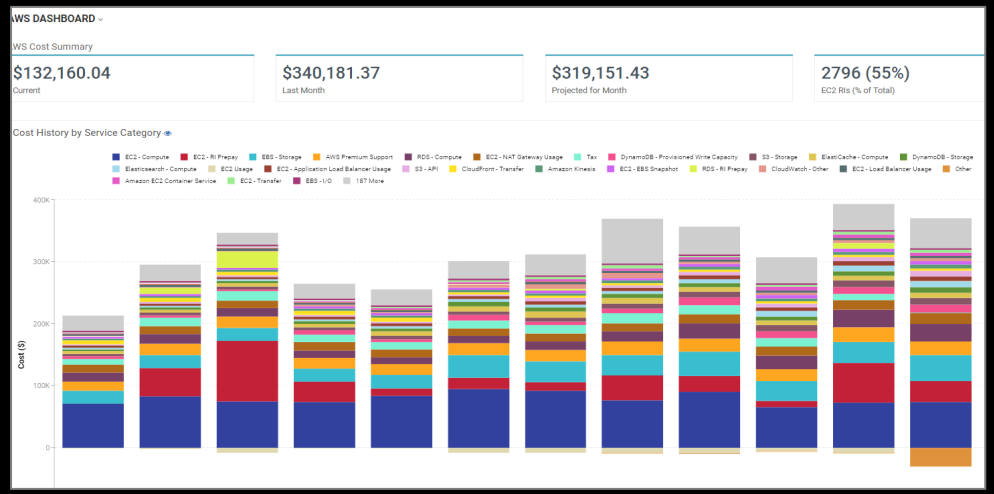
Step 1: Visibility

- Teams new to infra cost and cloud billing
- Cloud spend tracked by P&L, team, and account level

AWS Cost Explorer & Billing Console

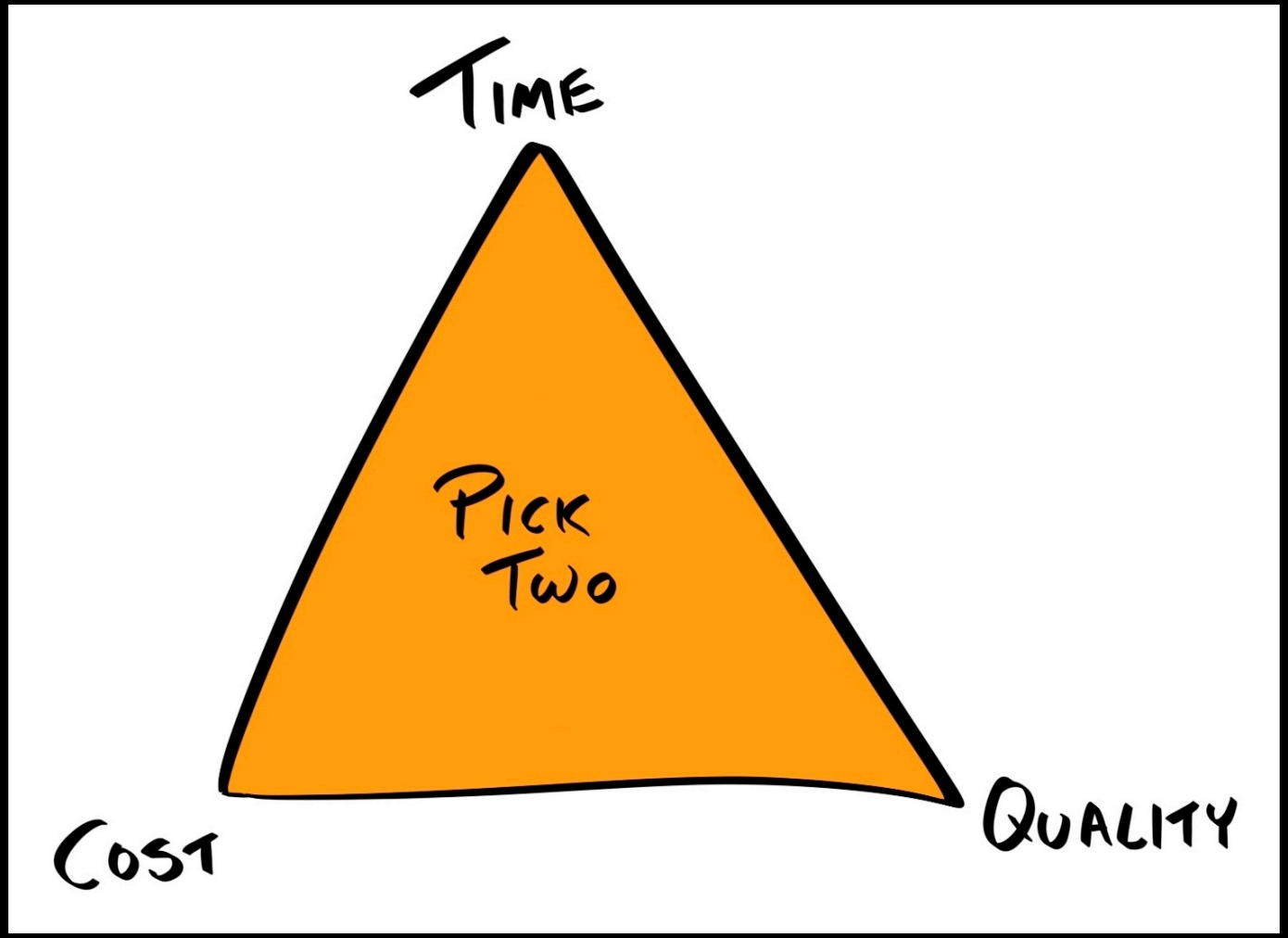


CloudHealth



MORNINGSTAR®

Step 2: Ownership



The triple constraint
O'Reily

MORNINGSTAR®

Ownership With Flexibility

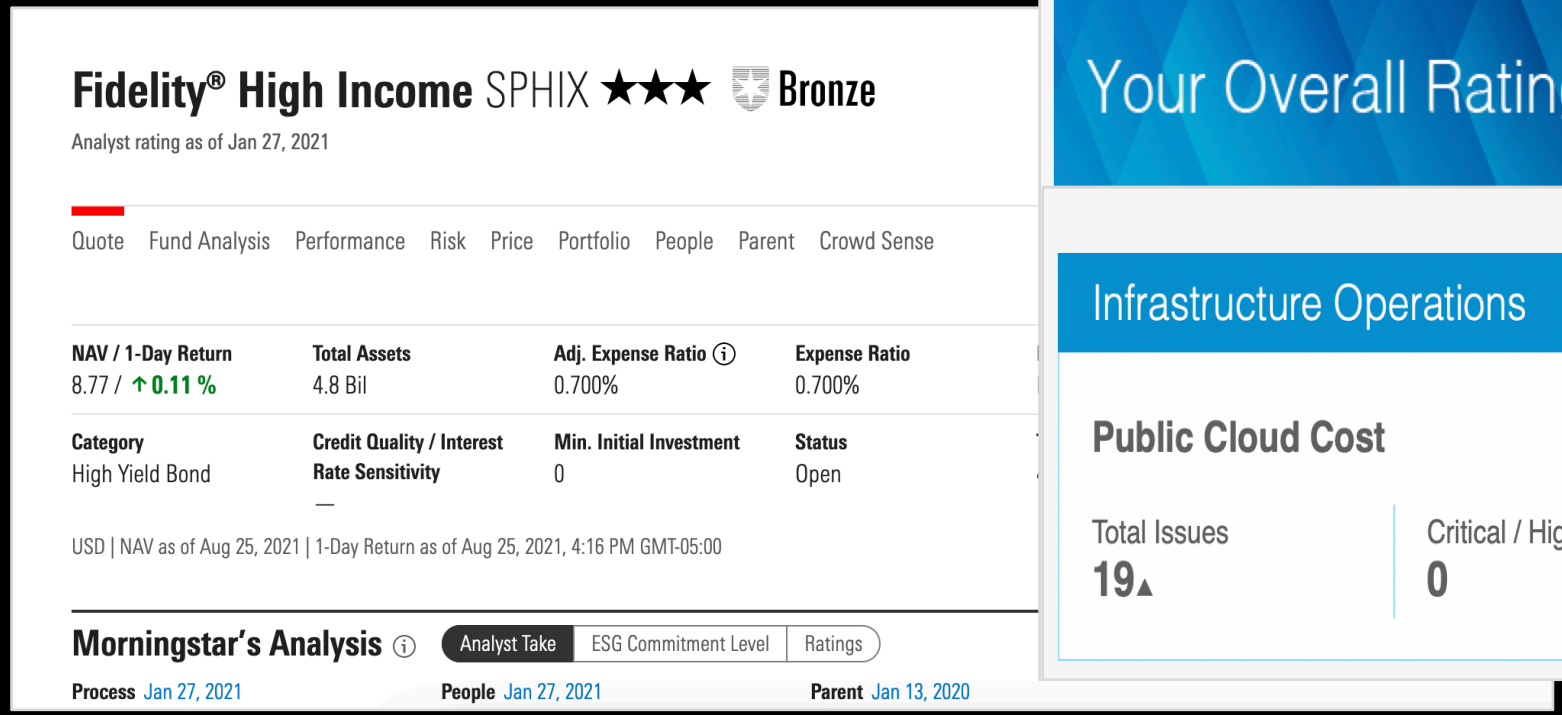
- Infrastructure-as-code
  - Custom IAM roles
  - New security group PR process
- Exception handling
- Training, education, and architecture

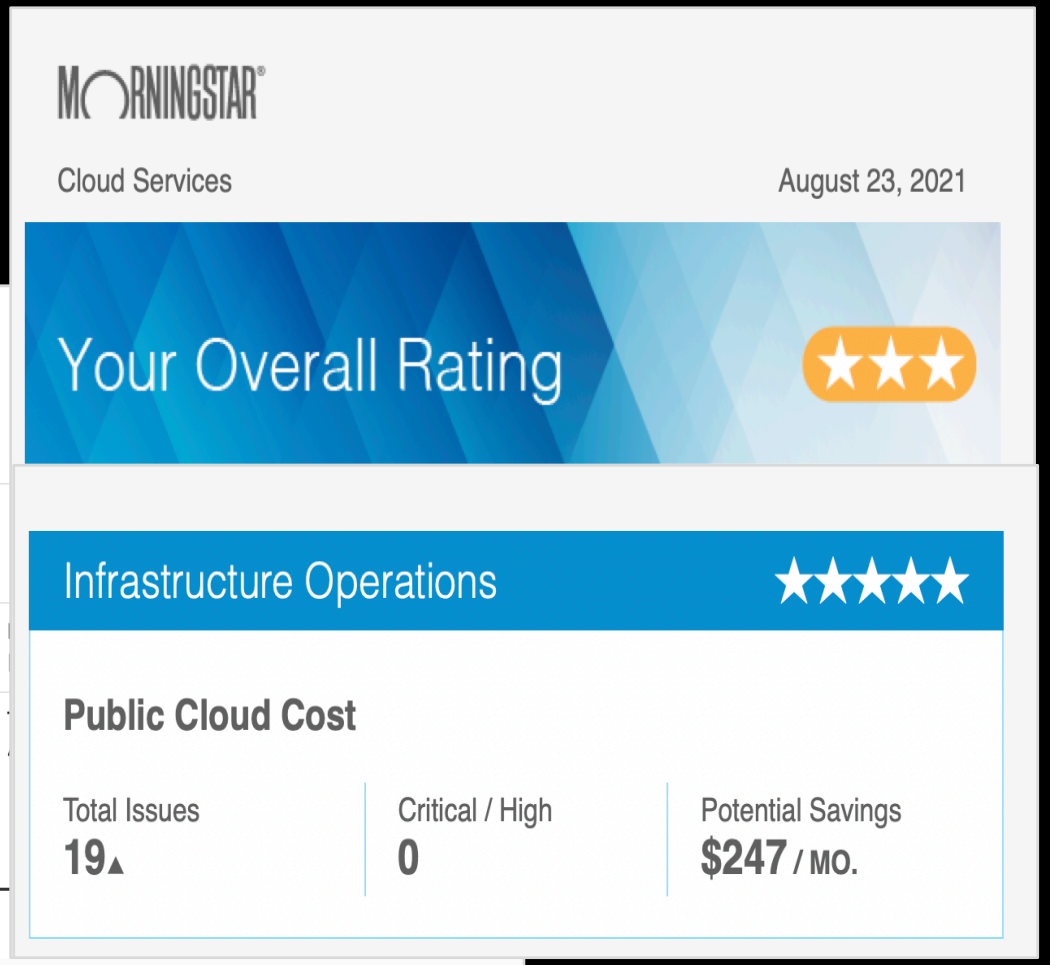
MORNINGSTAR®

Enforcing Best Practices

Scorecards Are Kinda Our Thing

MORNINGSTAR Premium

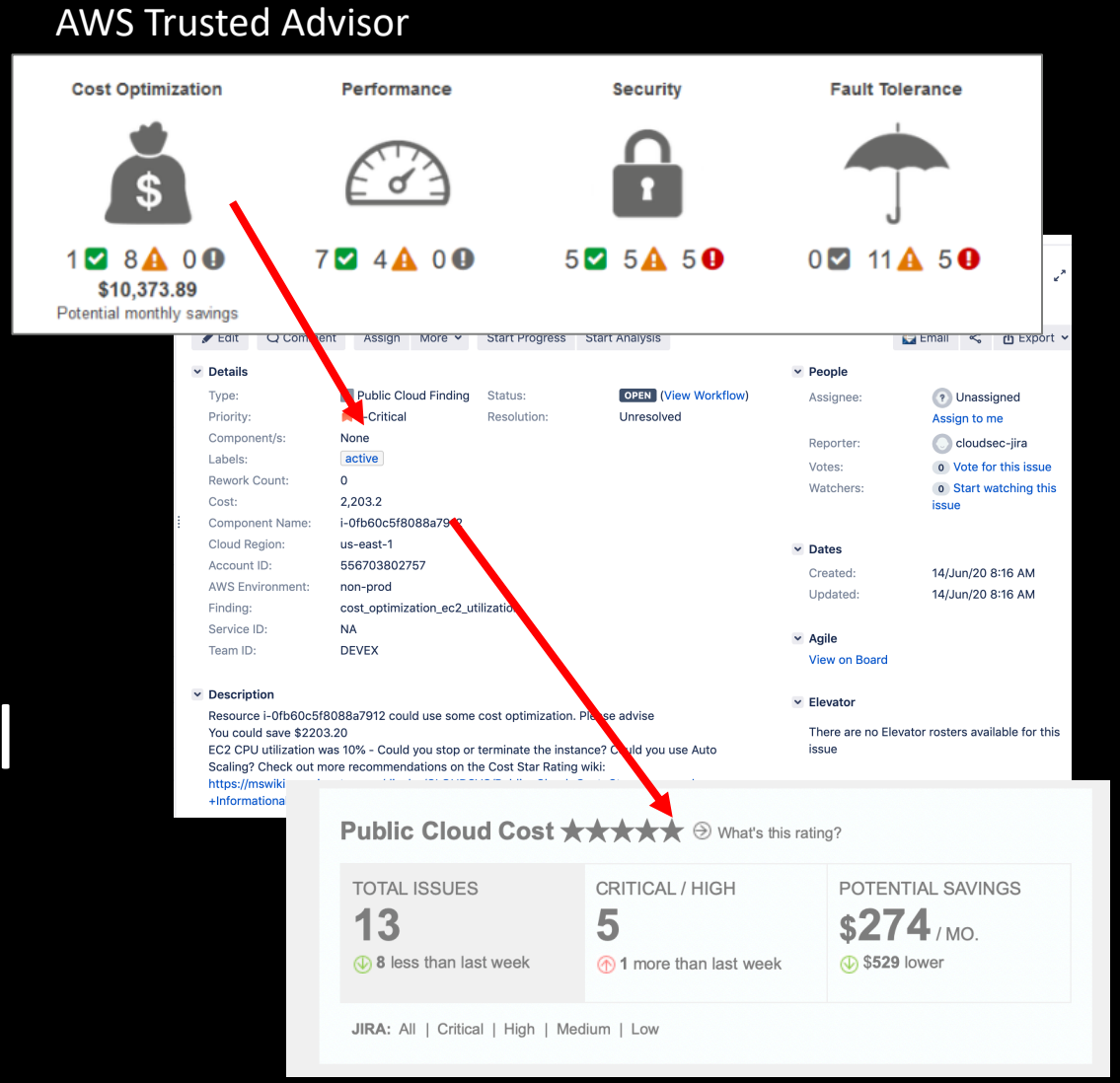




MORNINGSTAR

Accountability

- AWS Trusted Advisor recommendations in account
- Homemade API connectors
- Jira ticket per issue
- BRINQA scorecard rating email per team each week

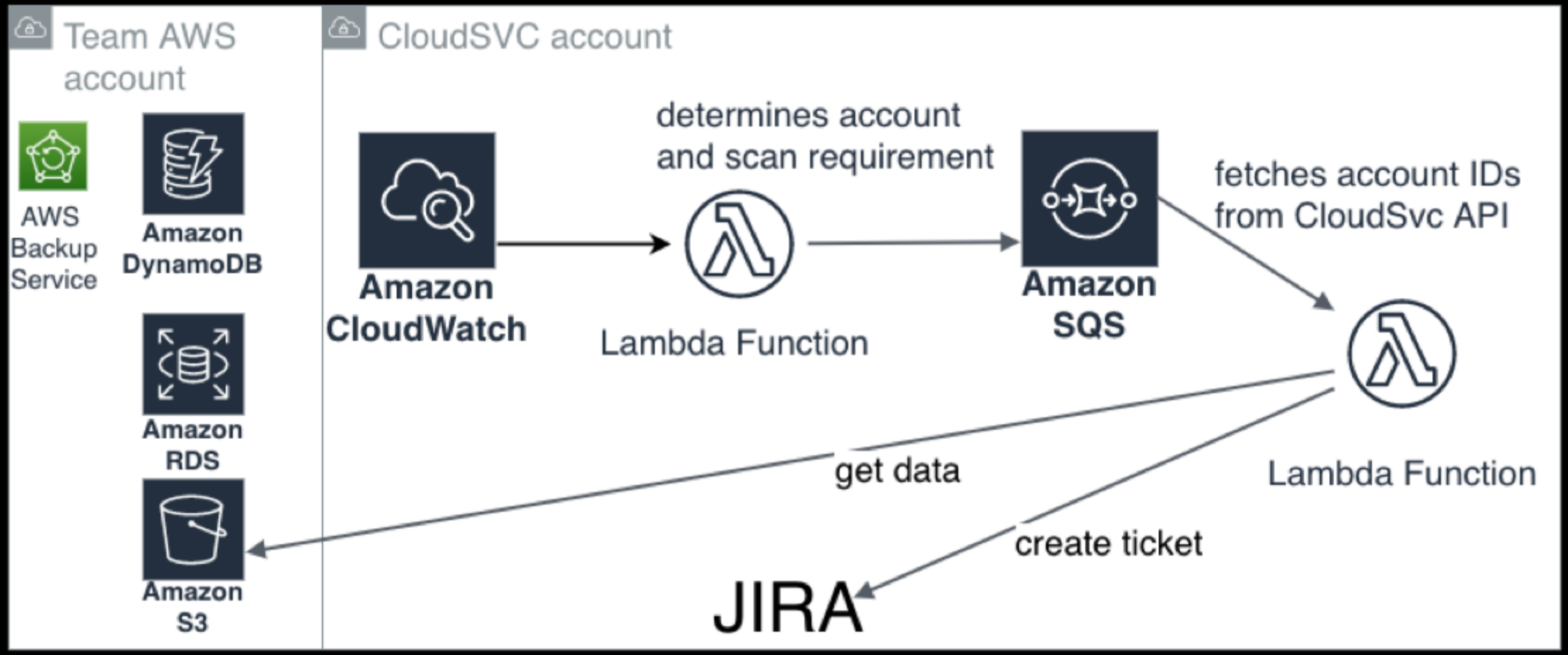


MORNINGSTAR®

Security Checks

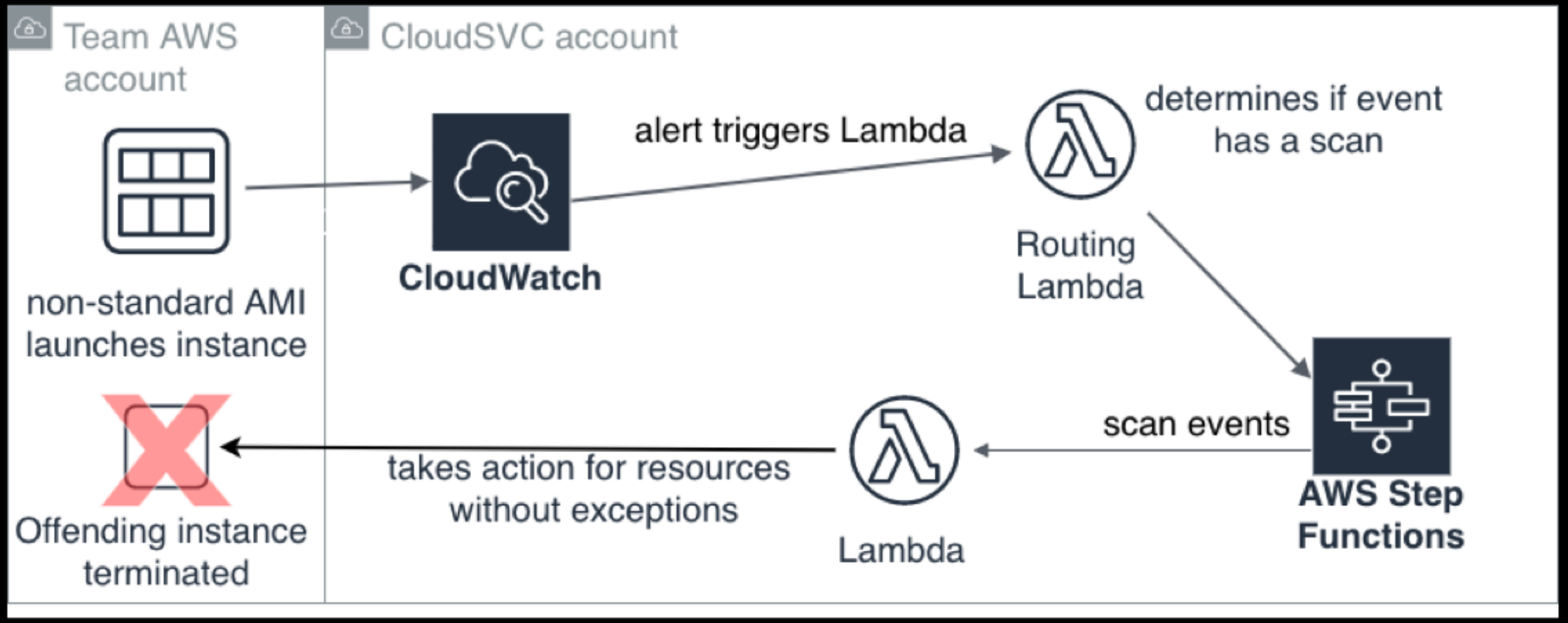
- Enforce backups for production
- Patch long-running EC2 instances
- Enforce IAM access key rotation
- Ensure encryption in transit on load balancers

Time-Based Back Up Scan Process



MORNINGSTAR®

Trust, but Auto-terminate



MORNINGSTAR®

What's Next?

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

Takeaways

- Plan
- Adapt
- Enforce

- Work with great people

MORNINGSTAR®

Join us!

- Security Engineer
- IT Project Manager - Disaster Recovery
- Senior Cloud Engineer – Network
- Application Security Lead
- Senior Manager - Information Systems and Operations

morningstar.com/careers

MORNINGSTAR®