# An Evolving Approach to Managing Multiple Amazon Web Services (AWS) Accounts

Matt Badanes

# Introduction.

## What we're going to be talking about

- As we began out AWS journey, we wanted to distribute responsibility for owning and operating (and managing costs!) assets in the public cloud while keeping AWS environments secure.
- We are working on a balance between giving developers freedom to build while keeping accounts secure, centrally managed, and observable.
- We have done this by creating multiple types of accounts and creating guardrails around these accounts to ensure the teams can develop and run their products in their own accounts, but minimize risk through a variety of scanning methods.
- This talk with discuss the overall structure as well as some of the scanning we've created along the way.

# Objectives

- Understand the need to distribute responsibility for owning and operating (and managing costs!) assets in the public cloud while keeping AWS environments secure
- Recognize the balance between giving developers freedom to build while keeping accounts secure, centrally managed, and observable
- Discuss the overall scanning structures

# Agenda

- Attendee Introduction
- Morningstar account overview and strategy
- Employee account experience
- Account Guardrails
- Questions

# Morningstar account overview and strategy

- Morningstar has three account types: Individual, Team Non-Prod, and Team Prod.
- We have a Cloud Services team, which acts like a central “center of excellence” in charge of account creation, networking basics, hardened AMIs, and global IAM roles.
- Centrally, we have 1 payer account, 1 shared account with logging and monitoring, and the ability to VPC peer to other team accounts.

## Employee account experience

- Individual Accounts or “sandbox accounts” are for individual employee to test and learn.
- Originally, we invited people to join using their Morningstar email address. The accounts were joined to the Morningstar payer account and rolled up to Morningstar but we had little control or insight.
- Since then, we’ve evolved and AWS introduced Organizations. We also learned the hard way how difficult it is to deactivate emailroot accounts for people who left the company. Don’t try it at home.

## Account Guardrails

- Team Accounts –groups of people and tech who share the same security, financial, and networking boundaries.
- We assume 2 accounts per team: nonprod and prod.
- These accounts do have more strict guardrails to lock down connectivity, data protections, and user access.
- We manage account and region creation via Terraform (learn more about that from Nick Bauch on our team, he's also submitting!).
- Since we started, AWS has released security and observably tools from Macie to GuardDuty. Some good, some ugly. Now with an updated Single Sign On (SSO) offering from AWS, we are revising how we manage AD groups, IAM roles, and account access.

## Lessons Learned

- After nearly 4 years of managing and security AWS accounts in real life, hear what we've learned.
- We continue to adapt AWS account strategy to fit the realities of internal developer teams requests and the firehose of AWS security services.

# Questions