
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

COP305

Best practices for organizing and operating on AWS

Bianca Lankford

VP, Cloud Security
Warner Bros. Discovery

Andrew Blackham

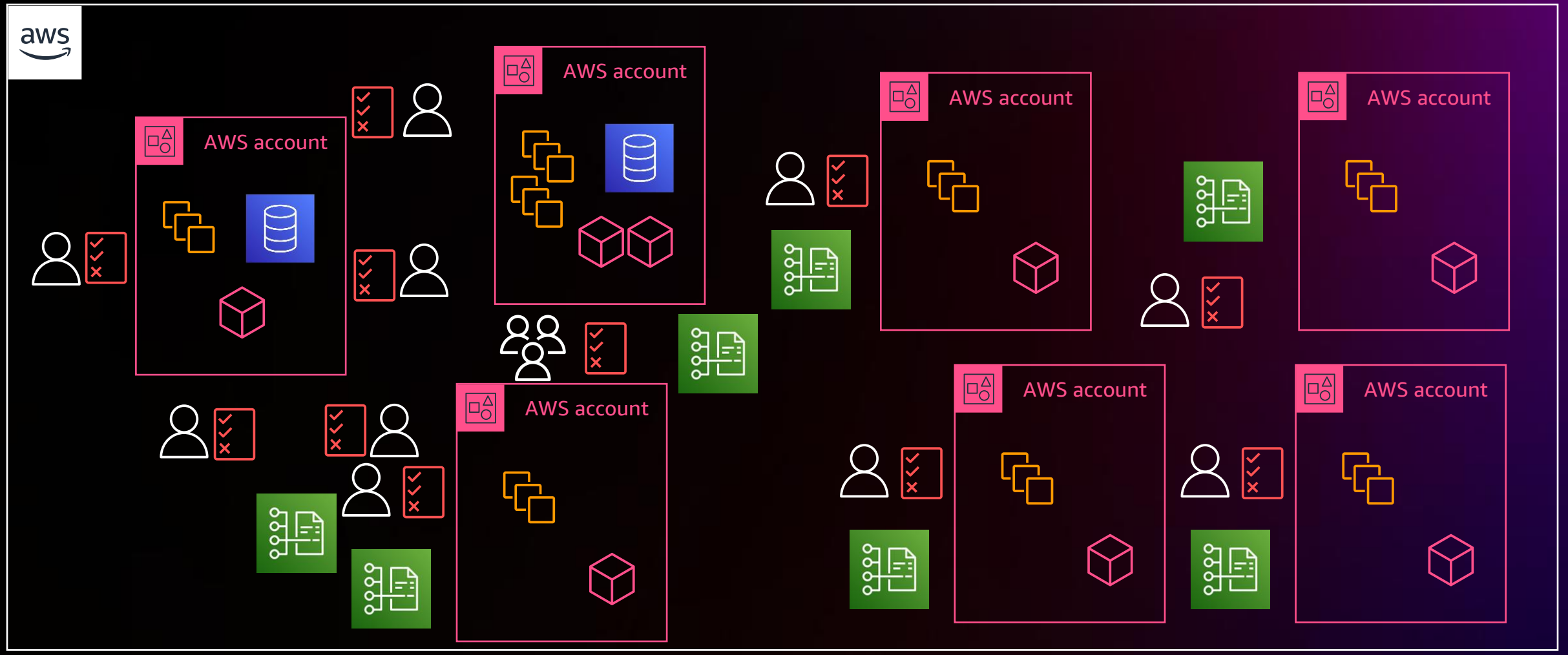
Senior Product Manager
AWS

Steve Rice

Principal Product Manager
AWS

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

A common customer scenario



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



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



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

Why AWS Cloud Operations?



Return on investment (ROI)

241% ROI over 3 years*



Staff productivity

62% more efficient IT infrastructure staff



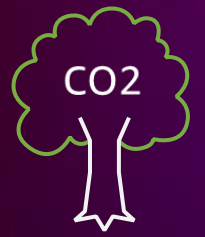
Operational resilience

57% decrease in downtime



Business agility

37% decrease in time to market



Carbon savings

88% reduction in carbon footprint of IT operations

Based on independent research of 1,500 AWS enterprise customers

*Source: “The Total Economic Impact of AWS Cloud Operations: Cost Savings and Business Benefits Enabled by Operation on AWS.” May 2022. A commissioned study conducted by Forrester Consulting on behalf of Amazon Web Services.

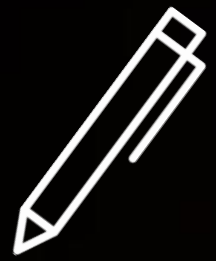
aws

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

Your journey to operating at cloud scale

Get started with AWS Cloud Operations

Set up



Establish a secure foundation for governance and compliance

Build and migrate



Migrate applications to the cloud, or build new applications

Operate



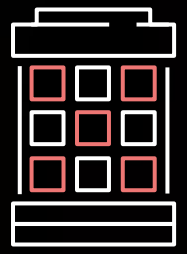
Simplify ops management with an integrated experience to manage and monitor resources and apps to detect and remediate risks quickly

aws

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

What we will talk about today

Elements of scaling



Structure

Accounts and organizations

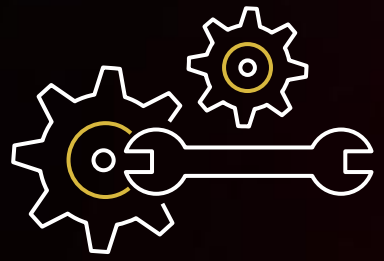
Management tools



Security

Central visibility

Incidents and change



Operations

Applications

WARNER BROS. DISCOVERY

How Warner Brothers Discovery incorporates these elements



Best practices and path forward

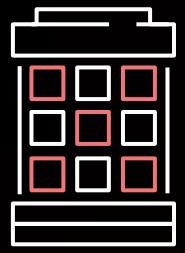
aws

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

The key to scaling:
Set up things correctly now to have success later

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

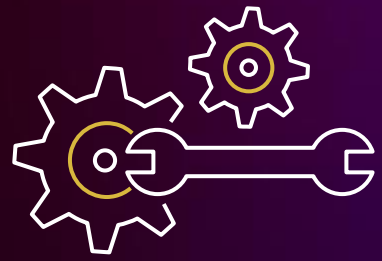
Key elements of scaling



Structure



Security



Operations

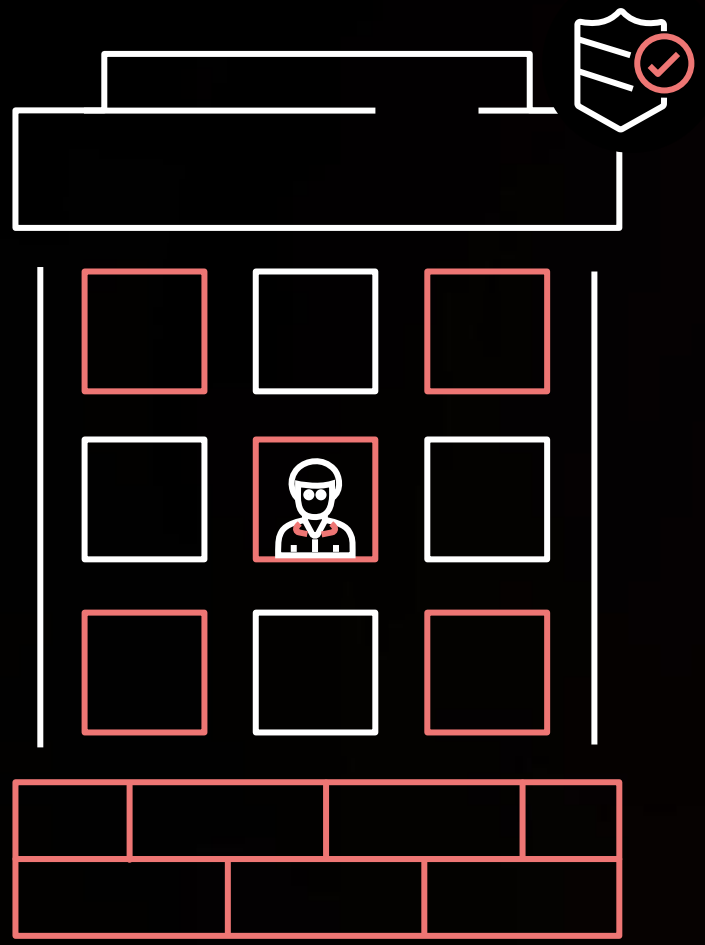
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Elements

Structure

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

Key elements of scaling – Structure



Brick/material

Framework or structure

Building manager

Security system

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

Accounts are the building blocks

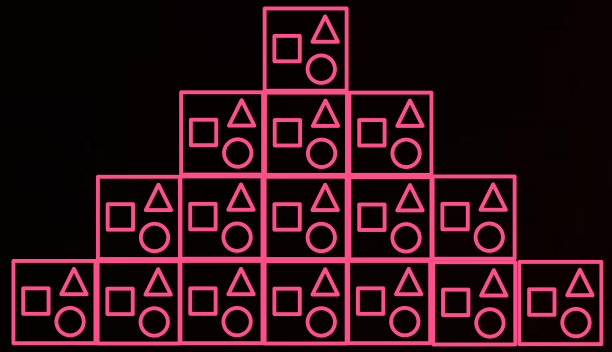
Think of AWS resources (instances, storage, etc.) as material and accounts as bricks

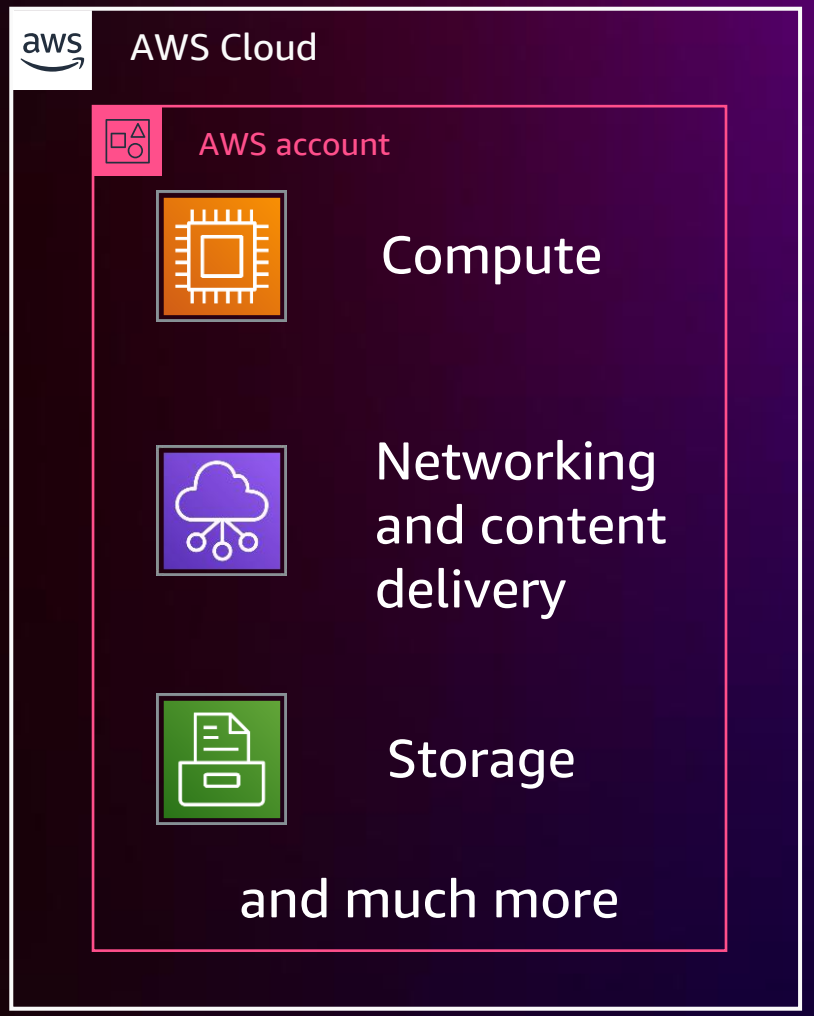
Scale across accounts

Account limits
Quotas

Security
Natural boundaries, isolation

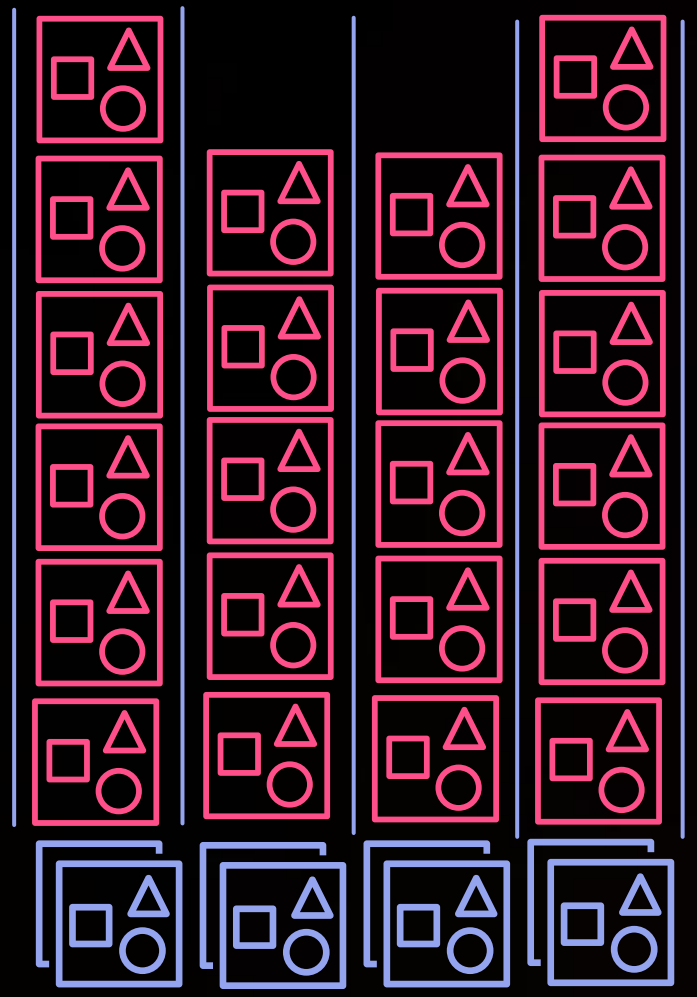
Compliance/ business processes
Billing, custom requirements





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

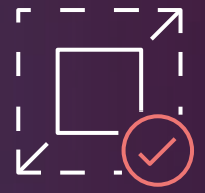
Framework for accounts: OUs



To build out structure, you need supports, trusses, or frames in place to define the pattern for bricks

Organizational units (OUs) are the frames

Design your OU structure around security and operational needs



Start small and broad, expand as needed



Guardrails/ policies are assigned to OUs

aws

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

Common anti-patterns

Building a structure that doesn't scale and requires a lot of overhead to maintain



Teams

Teams and users fluctuate



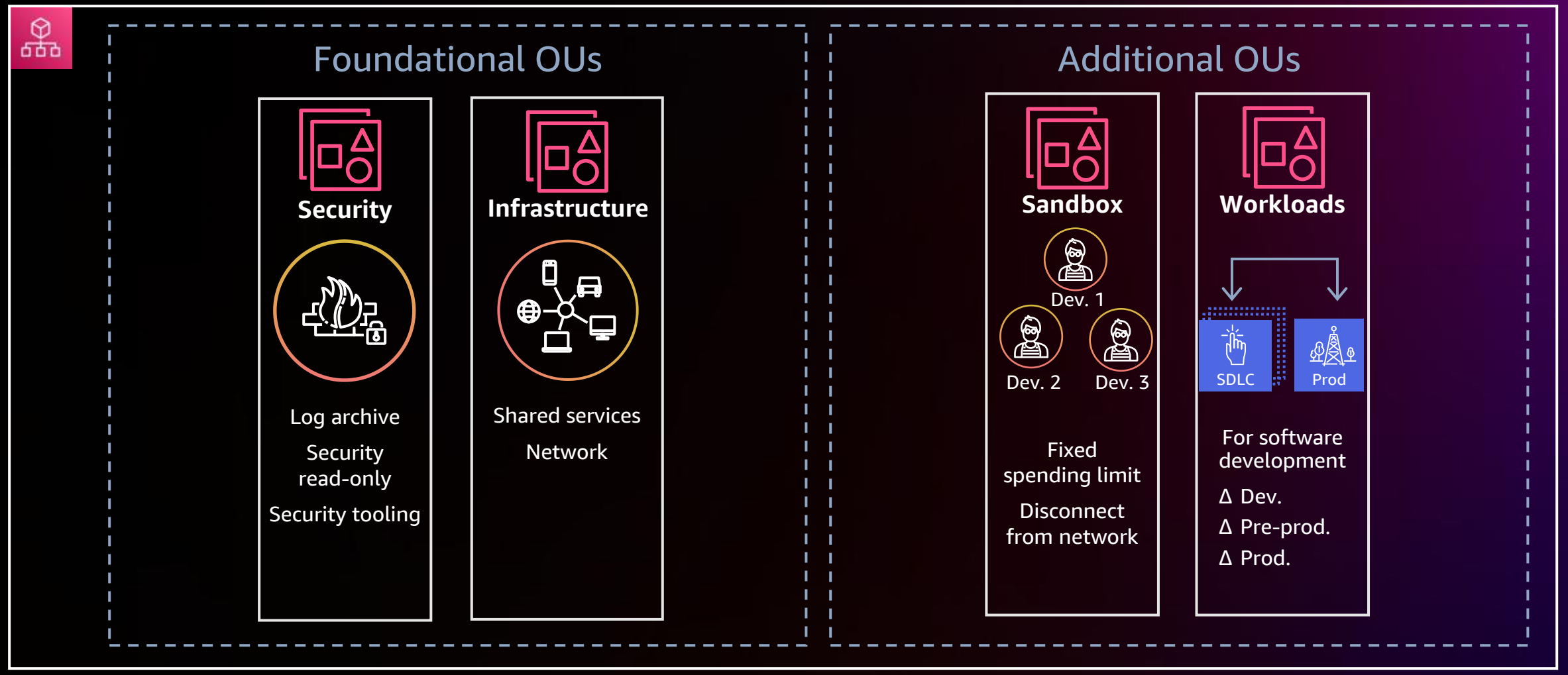
Customers

We recommend you start small, then build

aws

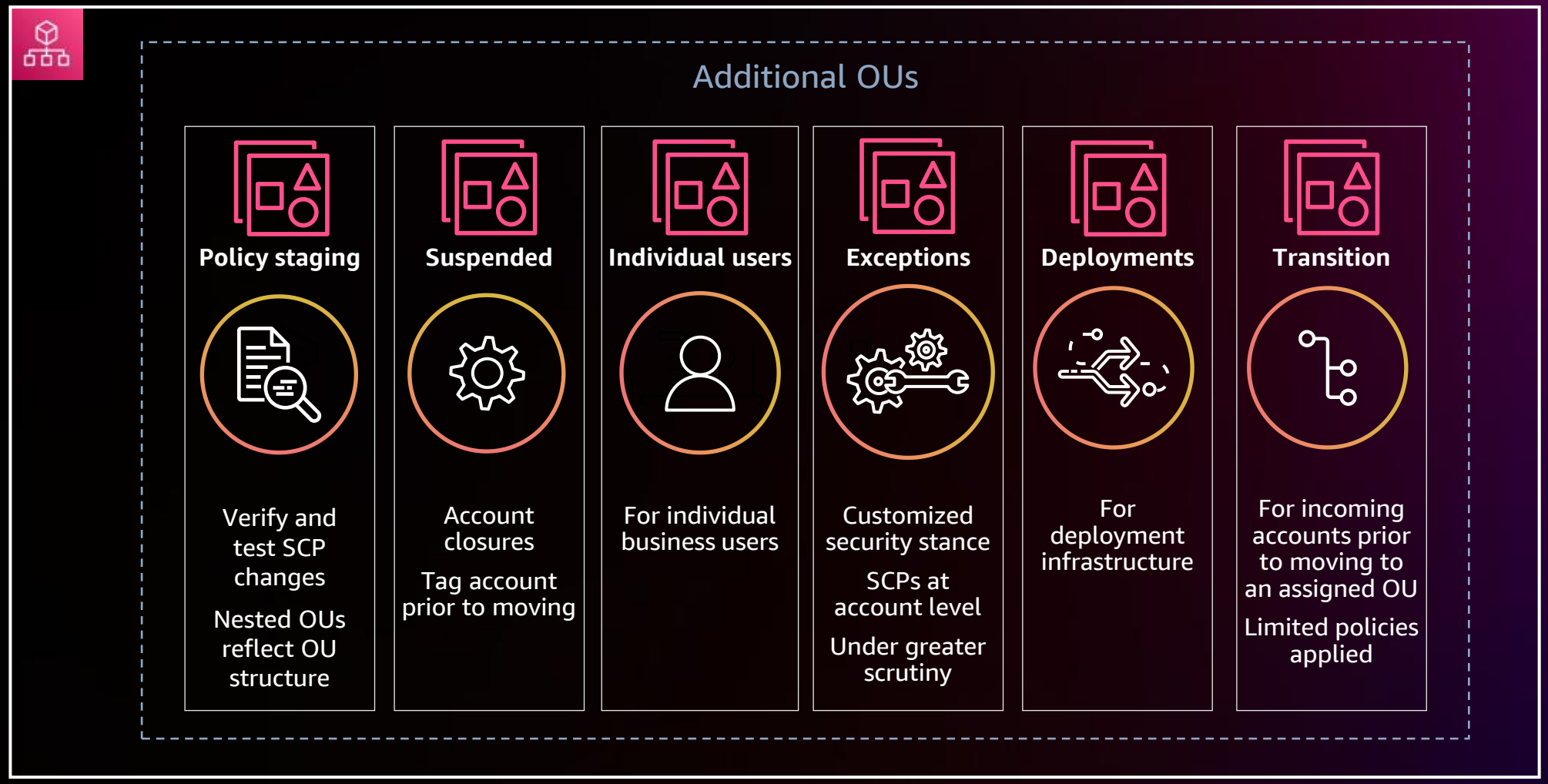
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS-recommended OU structure



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

Other recommended OUs



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

Tools for the building manager

Services for building – AWS Organizations

Build the structure (create accounts and OUs)

Management account for administration

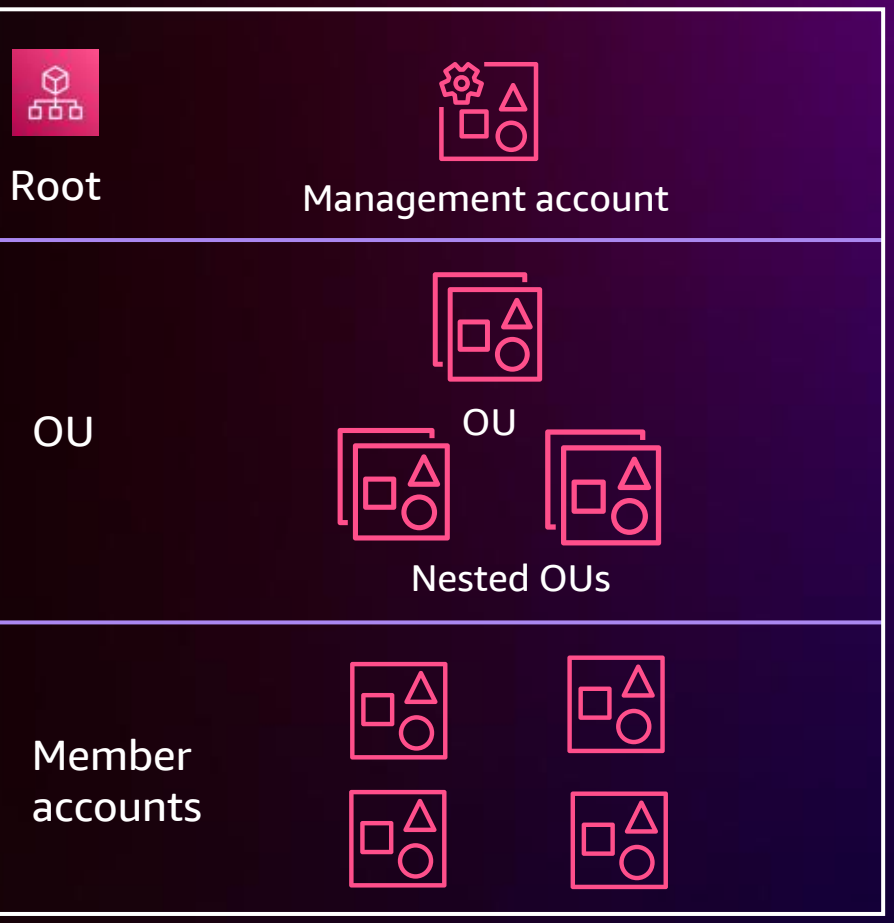
- Activate cross-account services and delegate administration to member accounts
- Limited access to management account

Tools for automating your building

- AWS Control Tower

New (as of 2022)

- CloseAccount API
- Account management APIs (contacts and alternate contacts info)
- Support for AWS CloudFormation

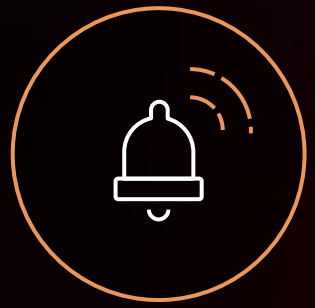


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Your security system



Best practices for security in your cloud environment



Employ proactive security mechanisms



Equip your security team with central visibility and controlled access

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

Security

Preventative controls

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

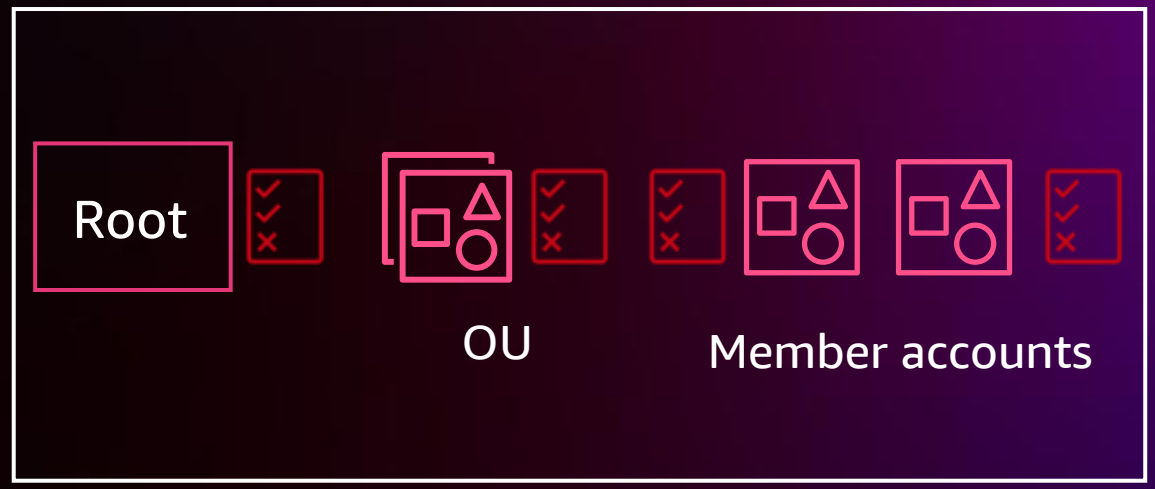
How SCPs work

Centrally create and apply custom guardrails for your organization

Granular policies can allow or limit API actions from users in member accounts

They can be applied to member accounts, OUs, or the organization root

- Simplifies permissions at scale; member accounts “inherit” policies or permissions applied at other levels
- Also known as preventative guardrails (AWS Control Tower)




```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

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

SCP use cases

1. Use of common services with each OU
2. Limit usage to certain AWS Regions
3. Require tags upon resource creation
4. Specify allowed instance sizes
5. Prevent actions from root users
6. Prevent deletion or modification of IAM roles
7. Prevent default encryption from being turned off



aws

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

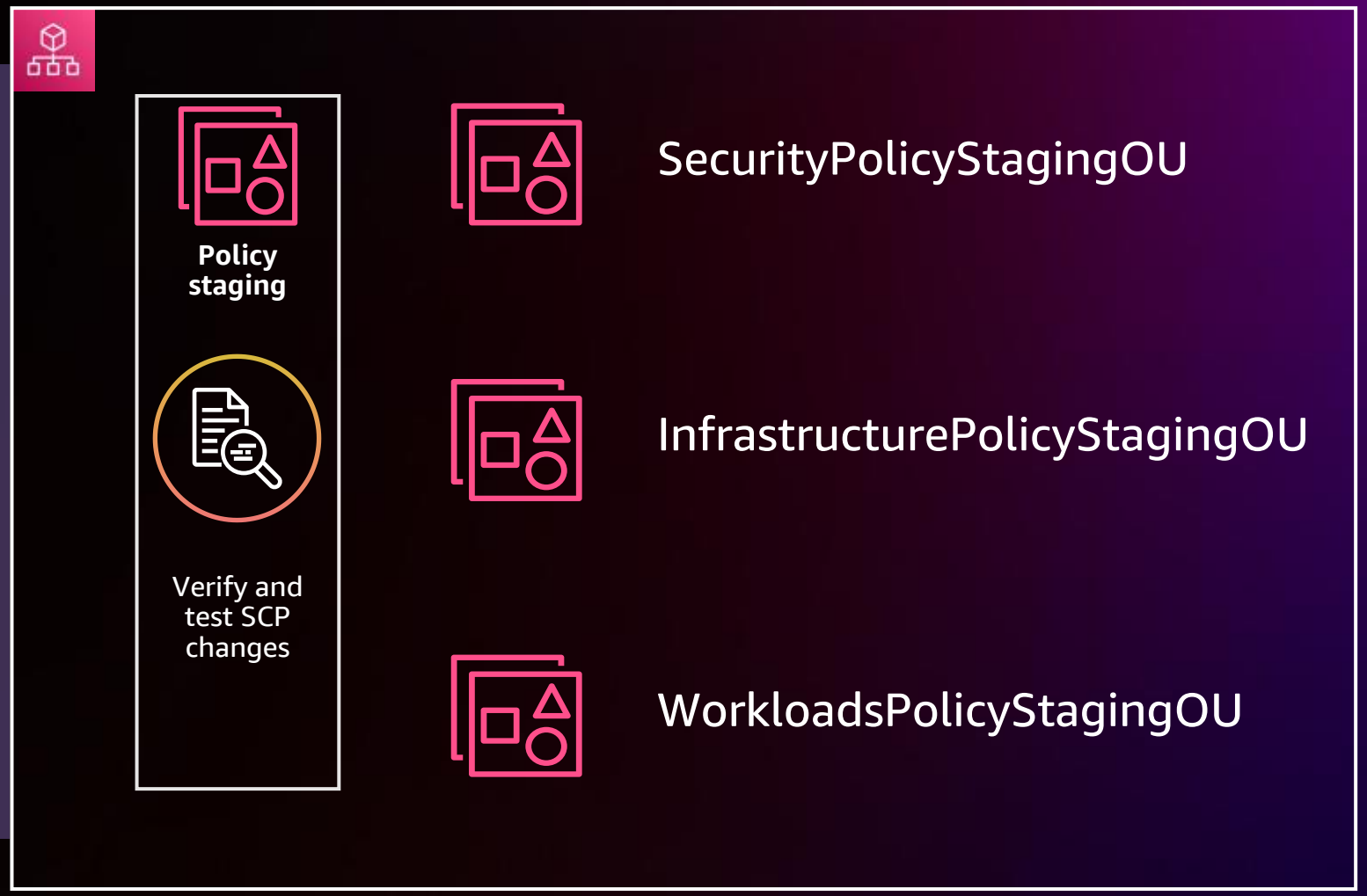
SCP design

Start with broad policies at the highest level, then more granular at lower levels

- E.g., Allow Amazon EC2 at root/ OU level, then specify allowed instance types at lower levels

Use SCPs to adhere to compliance standards (PCI, HIPAA, etc.)

Test SCPs prior to implementation



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

Security

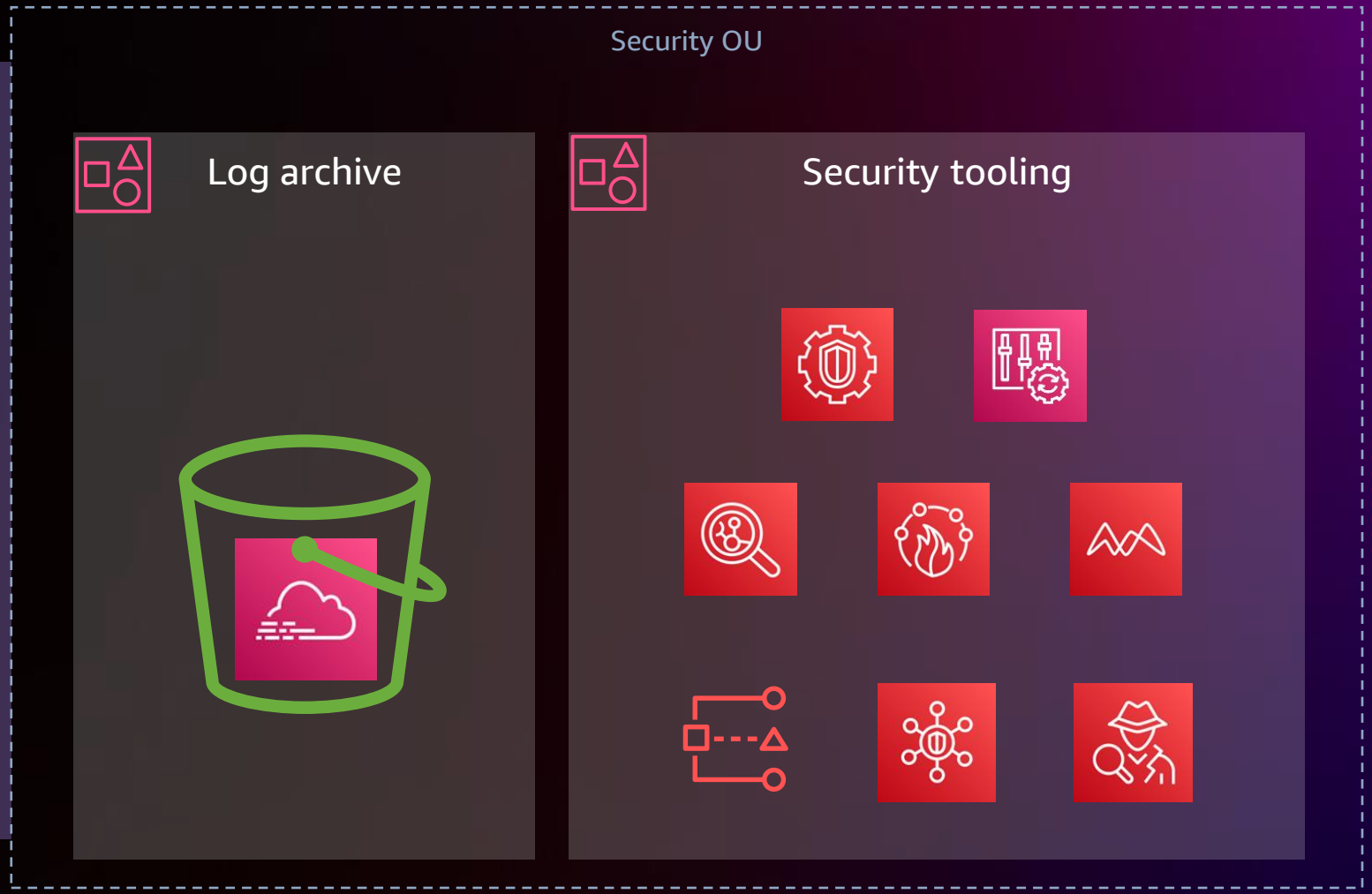
Central access and consolidated findings

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

Your security system – Central visibility

Employ AWS security services in your organization

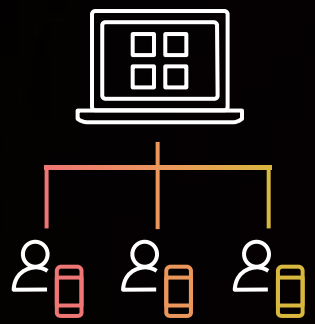
Delegate visibility to a dedicated security tooling account



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

Setting up security and other services

Typically involves two steps



Set up service for the organization



Register a delegated administrator account for management

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

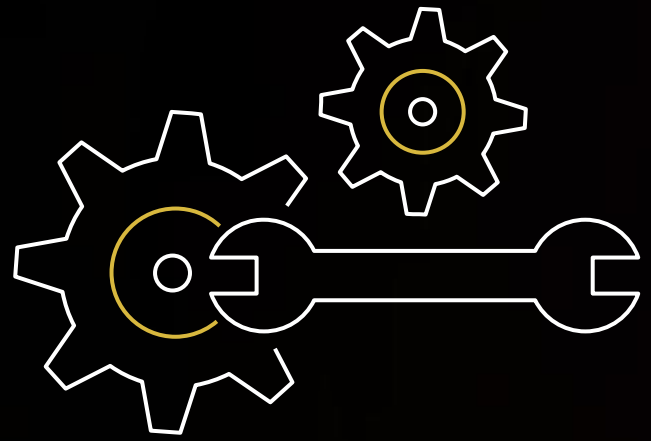
Elements for scaling

Operations

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

Key elements of scaling

OPERATIONS





Operations is where we see if our planning will survive the battlefield



Everything you set up is stress tested

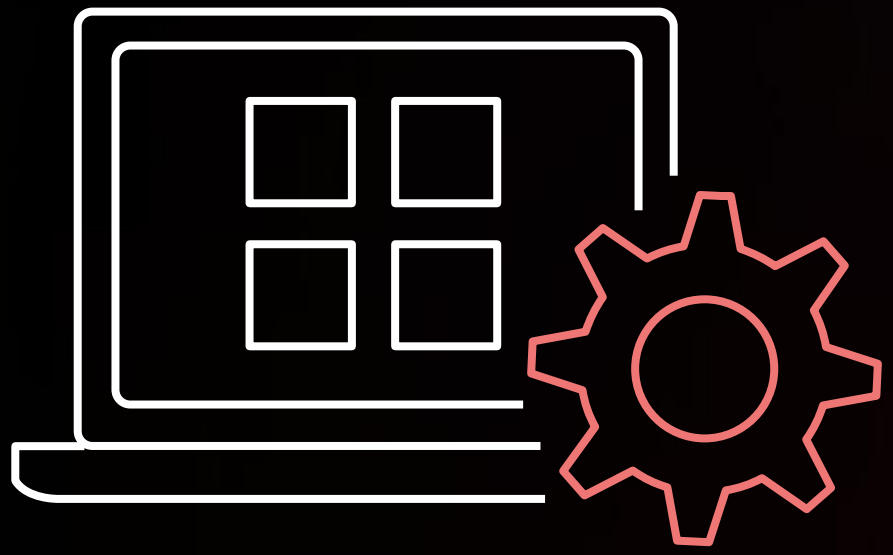


Must have data and tools to see what holds up and where cracks are

aws

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

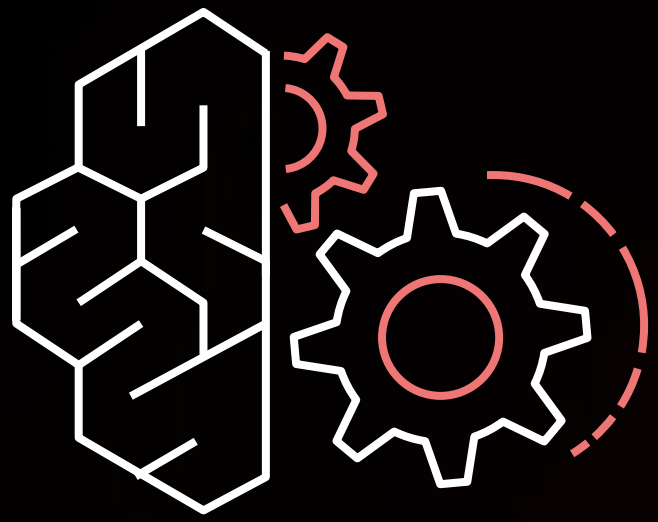
Operations best practices



Use a single pane of glass to monitor your system health

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

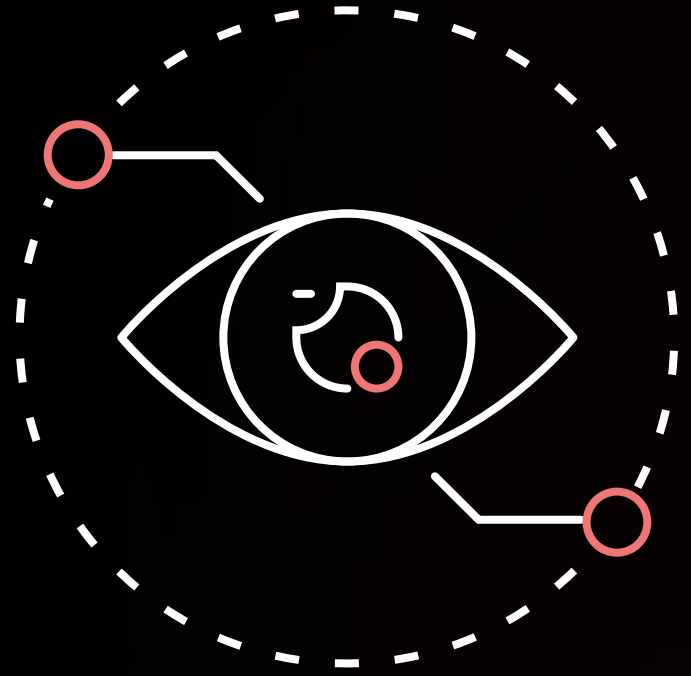
Operations best practices



Build runbooks and automation to address issues faster than a human can react

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

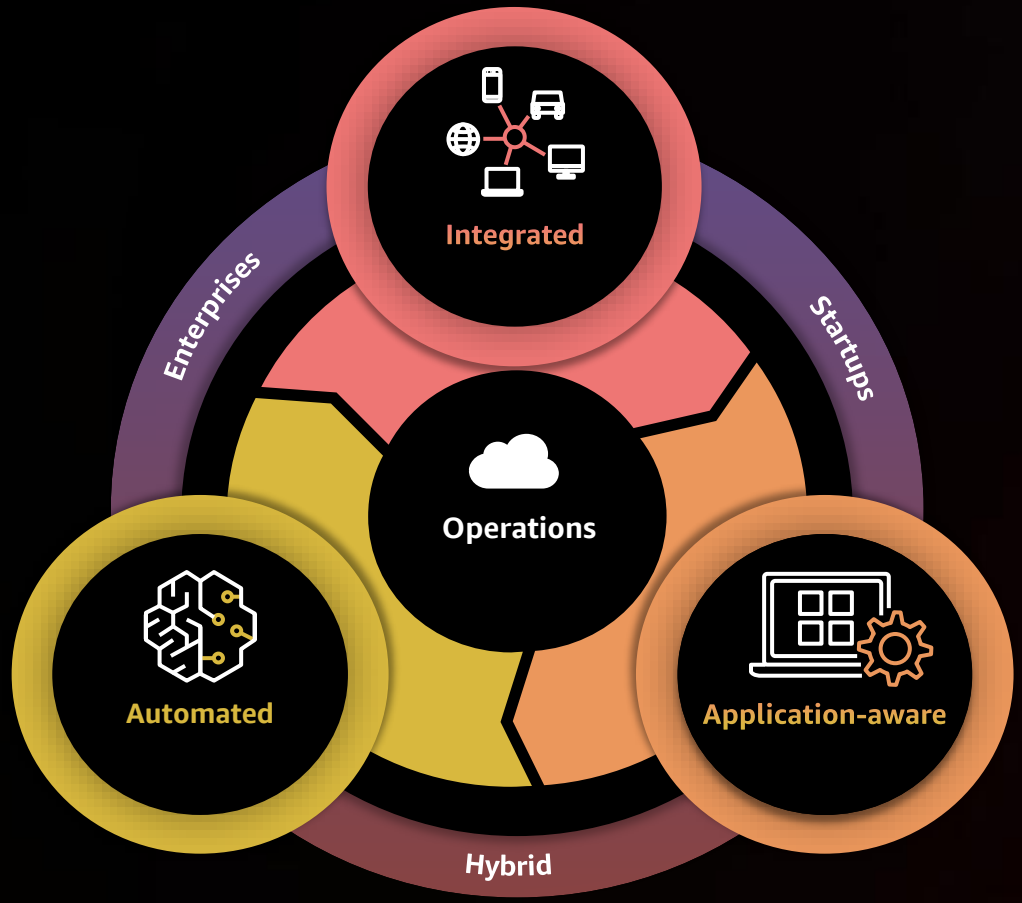
Operations best practices



Build a feedback loop to add preventative dials and switches into your system to allow for easy adjustments

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

Tools should enable your priorities



AWS Systems Manager

Agility, scale, and control across all environments

- Enable visibility
- Proactively automate
- Remediate centrally

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

Operations

AWS Systems Manager

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

AWS Systems Manager

https://us-east-1.console.aws.amazon.com/systems-manager/home?region=us-east-1#

aws | Services | Search [Option+S] | N. Virginia

Systems Manager | CloudFormation | EC2 | CloudWatch | Amazon EventBridge | IAM | S3 | Cloud9 | Step Functions | Console Home | CodePipeline | CodeBuild | Control Tower

AWS Systems Manager

- Quick Setup
- Operations Management
  - Explorer
  - OpsCenter
  - CloudWatch Dashboard
  - Incident Manager
- Application Management
  - Application Manager
  - AppConfig
  - Parameter Store
- Change Management
  - Change Manager
  - Automation
  - Change Calendar
  - Maintenance Windows
- Node Management
  - Fleet Manager
  - Compliance

MANAGEMENT TOOLS

AWS Systems Manager
Gain Operational Insight and Take Action on AWS Resources.

Get Started with Systems Manager

View operational data for groups of resources, so you can quickly identify and act on any issues that might impact applications that use those resources.

How it works

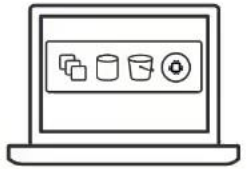


Group your resources



View insights

See relevant operational



Take action

Mitigate issues by

More resources

- Documentation
- API reference
- FAQs

Feedback | Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy | Terms | Cookie preferences

Deep dive

Warner Bros. Discovery

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

Warner Bros. Discovery Growth

2022 MERGER BETWEEN DISCOVERY AND WARNERMEDIA

The new company combines WarnerMedia's premium entertainment, sports, and news assets with Discovery's leading nonfiction and international entertainment and sports businesses, including Discovery Channel, discovery+, Warner Bros. Entertainment, CNN, DC, Eurosport, HBO, HBO Max, HGTV, Food Network, Investigation Discovery, TLC, TNT, TBS, truTV, Travel Channel, MotorTrend, Animal Planet, Science Channel, New Line Cinema, Cartoon Network, Adult Swim, Turner Classic Movies, and others



aws

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

Studios & Networks

Motion Pictures



Media Networks & Original Content

HBOmax · HBO · Discovery · TNT · HGTV · discovery+ · CNN · tbs · OWN · DC · EUROSPORT · TLC · [adult swim] · CN · food · MAGNOLIA NETWORK · ID

Direct-to-Consumer

HBOmax · discovery+ · kitchen · MOTORTREND

International

Real Time · HBO · TNT · Giallo · OhK · FRISBEE · familia · ChileVisión · CNN · CN · tvn · SPACE · MONDO TV · NOVE · CARTOONITO · TABI

News & Sports

CNN · HLN

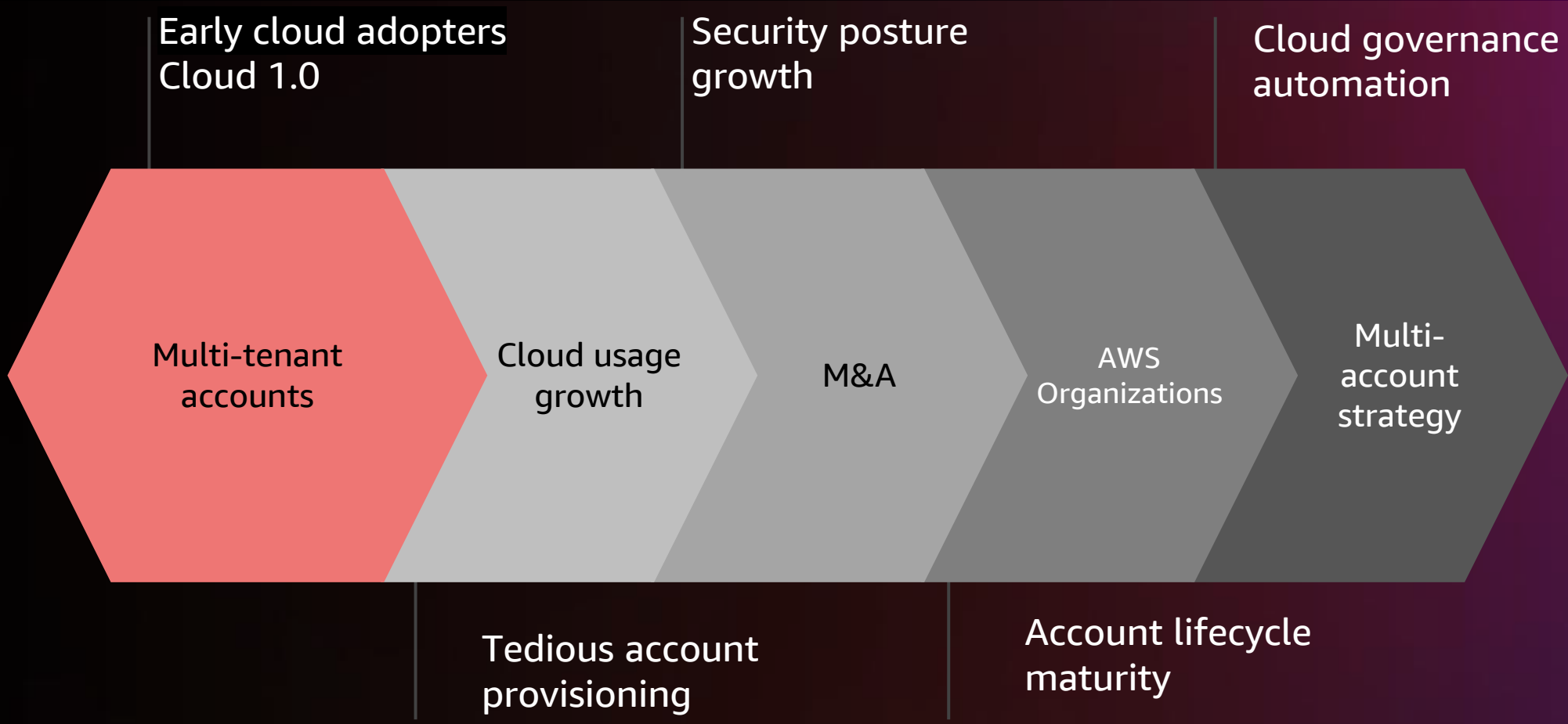
TURNER SPORTS · B/R BLEACHER REPORT · TNT SPORTS

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

WARNER BROS. DISCOVERY

Warner Bros. Discovery: Where we started

THE BEGINNING



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

Warner Bros. Discovery: Path to self-service

Fully use the power of AWS to continue creating cutting-edge products with high developer velocity in a governed and secured manner

Established a productized approach to cloud governance

- Model for accounts
- Automated account lifecycle
- Delivery transparency
- Accountability and ownership
- Base set of policies

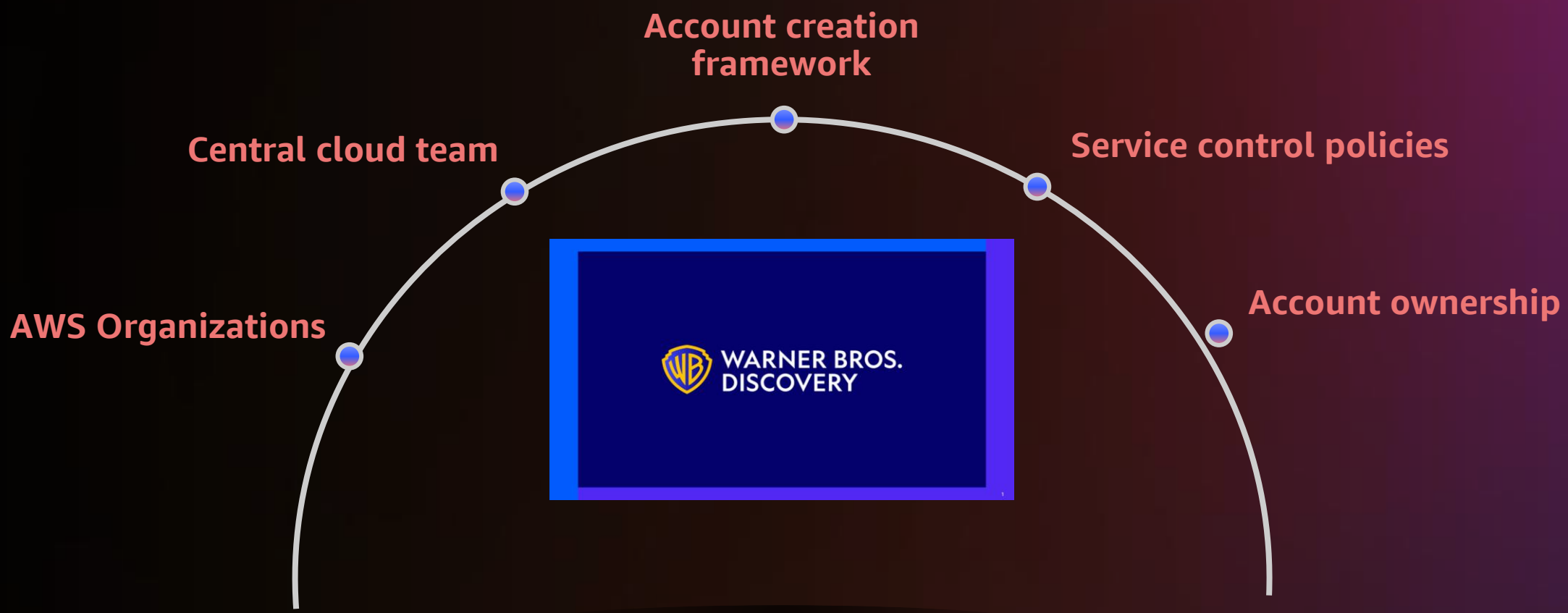


WARNER BROS. DISCOVERY

aws

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

Warner Bros. Discovery: Account lifecycle



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

Warner Bros. Discovery deep dive

THE RIGHT TEAM STRUCTURE

Warner Bros. Discovery has a centralized, globally distributed, dedicated team for managing centralized governance and AWS account posture; the team is named Global Cloud Services (GCS)

The team is comprised of highly skilled engineers, solution architects, and program manager responsible for curating AWS Organizations for Discovery

As owners of the cloud platform, GCS is responsible for the full cloud account lifecycle, including the creation, onboarding, recordkeeping, and closure of cloud accounts

Productized approach to cloud governance allows for organizations to customize controls tailored to their business needs



The right team structure

aws

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

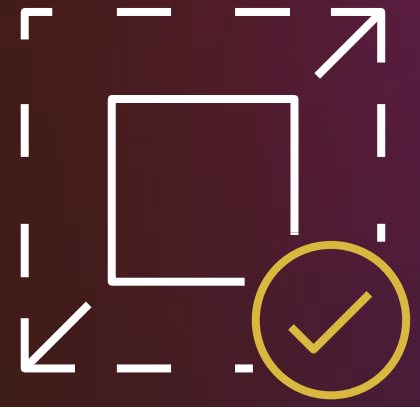
WARNER BROS. DISCOVERY

Warner Bros. Discovery deep dive

PRODUCTIZED GOVERNANCE AT SCALE

More than a set of policies, governance at scale at WBD is a product, delivered in an agile framework, treated like any other software product with the same rigor of automation, releases, and testing

The productized approach keeps governance prioritized in an organization, and it allows it to stay ahead of the growth of various business areas



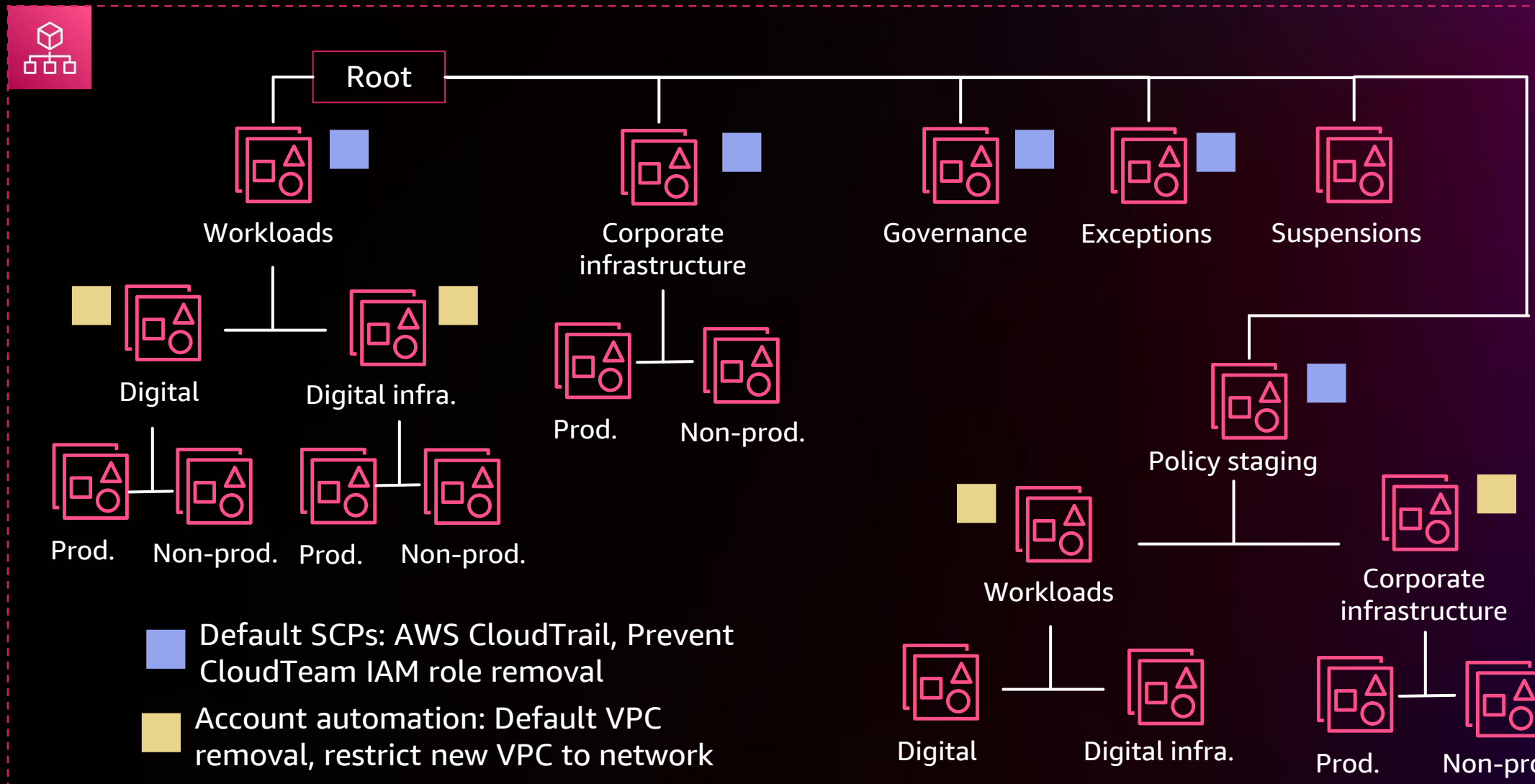
Productized governance at scale

aws

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

WARNER BROS. DISCOVERY

Warner Bros. Discovery deep dive: AWS Organizations



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

Warner Bros. Discovery deep dive

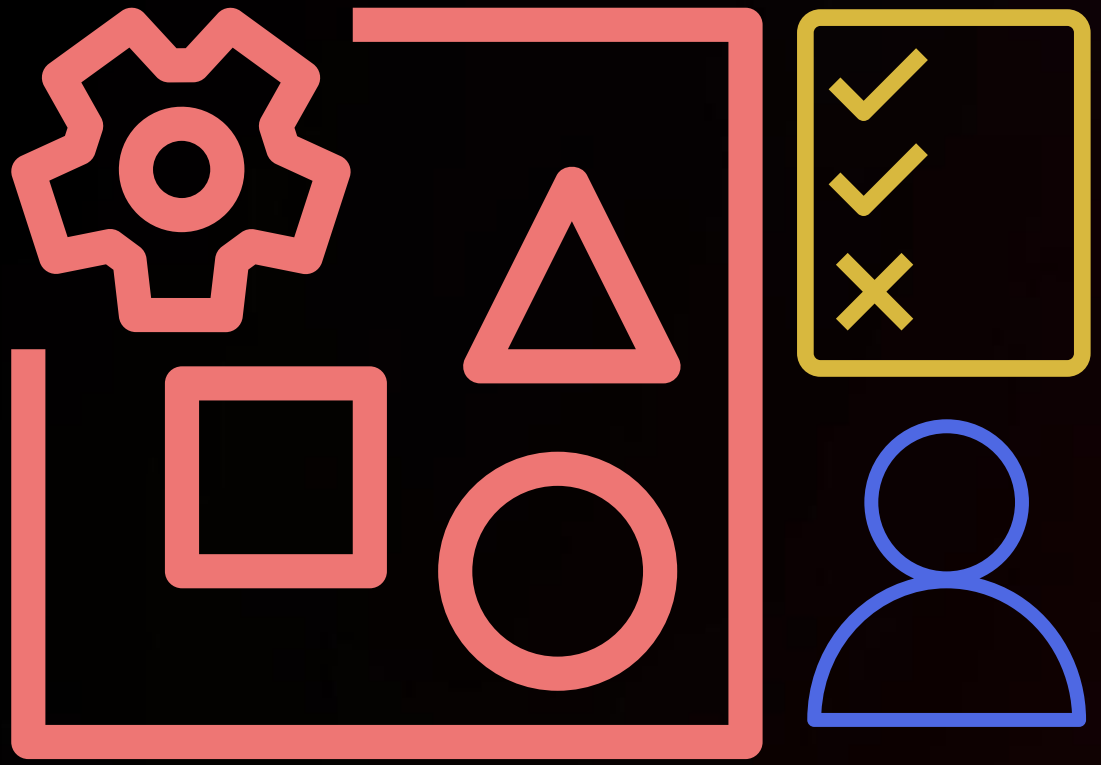
ACCOUNT LIFECYCLE



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

Warner Bros. Discovery deep dive

ACCOUNT LIFECYCLE



Automated delivery of accounts with a defined feature set

Defined set of standard features

Established accountability

Account owners

Application owners

Development teams

Security teams

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

Warner Bros. Discovery deep dive

EASE OF OPERATIONS FOR M&A

Automated frameworks for governance policies allow for ease of integrating newly acquired business units

Organizational unit specifically created as a landing spot for newly acquired business units

Account(s) placed in the M&A (organizational units); OUs get all the top-level controls and security tooling

As business decisions are made around the newly acquired company, accounts are moved to more appropriate business units



Ease of operations for M&A

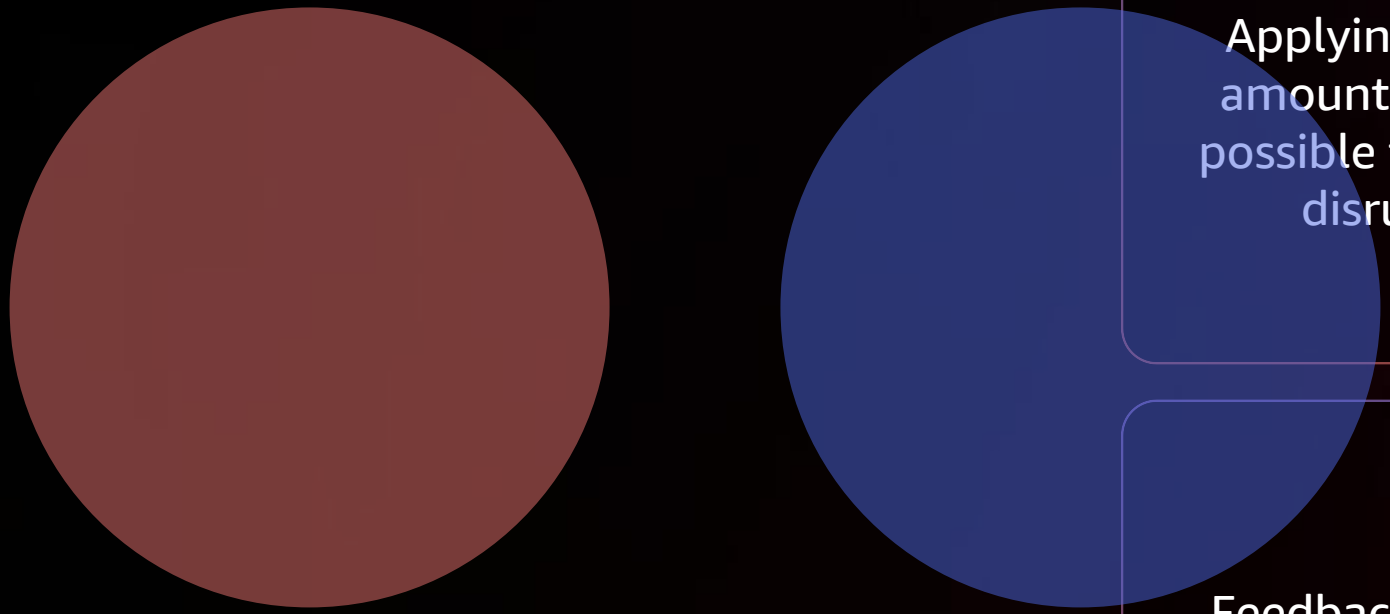
aws

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

WARNER BROS. DISCOVERY

Warner Bros. Discovery deep dive

M&A CONSIDERATIONS



Applying the least amount of policies possible to minimize disruptions

Difficult to test the unknown

Feedback loop with app. and dev. teams

Partnership with cloud security team(s)

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

Warner Bros. Discovery deep dive

AWS SYSTEMS MANAGER

Using Systems Manager to meet organizational need

Patch Manager, a capability of AWS Systems Manager, for compliance scanning

Session Manager, a capability of AWS Systems Manager

Parameter Store, a capability of AWS Systems Manager



AWS Systems Manager

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

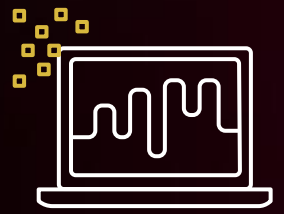
Warner Bros. Discovery deep dive

FINAL BUSINESS OUTCOME

WARNER BROS. DISCOVERY



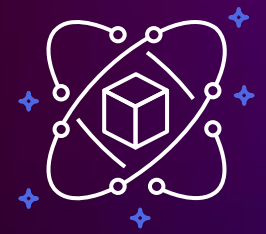
Governance is treated like a software product that grows and is iterated on over time



Even with major disruptions of M&A activities, the business environment continues to operate securely and seamlessly



Significant cost savings with centralized practices



Centralized view into the company cloud posture

aws

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

Warner Bros. Discovery deep dive

BEST PRACTICES



Use AWS Organizations

Dedicated team to manage automation for account lifecycle, organizational units, and service control policies

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

Warner Bros. Discovery deep dive

BEST PRACTICES



Use AWS Organizations

Dedicated team to manage automation for account lifecycle, organizational units, and service control policies

Use service controls policies to adhere to security baselines and overall business baselines

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

Warner Bros. Discovery deep dive

BEST PRACTICES



Dedicated team to manage automation for account lifecycle, organizational units, and service control policies

Use service controls policies to adhere to security baselines and overall business baselines

Determine a basic set of policies to start with based on risk and business impact

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

Warner Bros. Discovery deep dive

BEST PRACTICES



Use service controls policies to adhere to security baselines and overall business baselines

Determine a basic set of policies to start with based on risk and business impact

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



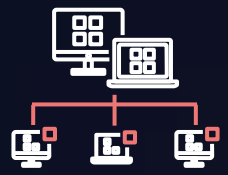
Where we started

Let’s review – where did we come from? Scattered accounts, no visibility, high risk, no governance or control

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

Where we started

LET'S REVIEW – WHERE DID WE COME FROM?



Scattered accounts



No visibility



High risk



No governance or control

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

Where we are now



Purposeful structure



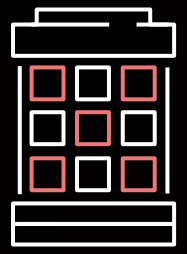
Built-in security and visibility



Centralized tools for administration, and operational efficiency

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

List of best practices/key takeaways



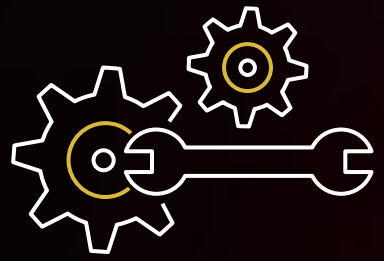
Plan an effective structure

Think of accounts as static; start small and expand



Limit access and use preventative controls

SCPs and delegated admin for services



Equip your teams with centralized tools

Use a single pane of glass to monitor your system health and security



Build runbooks and automation

Address issues faster than a human can react



Build a preventative feedback loop to

Add dials and switches to allow for easy adjustments

aws

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

Next steps (for you)

1

Take a photo of these **best practices**

2

Start **small** and grow from there

3

Enable standardized security controls and operations for your teams

4

Build the right structure and process now in **anticipation of your growth**

aws

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

Resources

Organizing your AWS Environment whitepaper

https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/organizing-your-aws-environment.html

Security reference architecture

https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/organizations.html

Operational excellence in the AWS Well-Architected Framework

https://docs.aws.amazon.com/wellarchitected/latest/framework/a-operational-excellence.html

Best practices for SCPs in a multi-account environment

https://aws.amazon.com/blogs/industries/best-practices-for-aws-organizations-service-control-policies-in-a-multi-account-environment/

aws

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

Want to see more AWS Cloud Operations?

Please complete the session survey in the mobile app



Ask us anything at our kiosks in the AWS Village (Expo Hall)



Find related sessions in our re:Invent blog post

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

Thank you!



Please complete the session survey in the **mobile app**

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