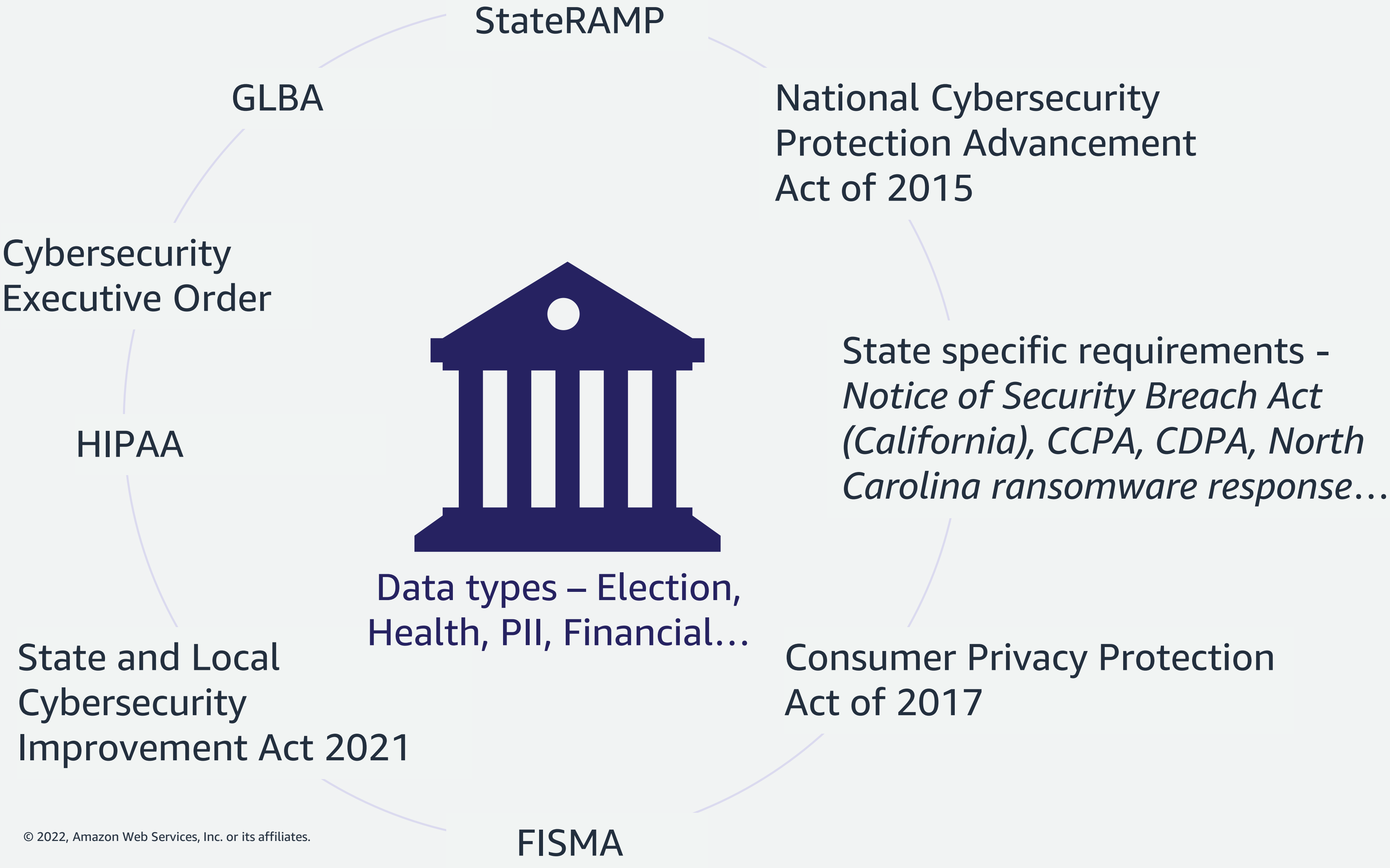
Securing your AWS Environment(s)

Leveraging native services

Brad Dispensa & **Brian** Stucker
WWPS Security & Compliance Specialists

SLG few key requirements…



StateRAMP

National Cybersecurity Protection Advancement Act of 2015

State specific requirements - *Notice of Security Breach Act (California), CCPA, CDPA, North Carolina ransomware response…*

Consumer Privacy Protection Act of 2017

FISMA

State and Local Cybersecurity Improvement Act 2021

HIPAA

Cybersecurity Executive Order

GLBA

Data types – Election, Health, PII, Financial…

- ❑ Cybersecurity plans
- ❑ Collaboration / sharing / Scalability
- ❑ Governance & Risk Management
- ❑ Data & information asset protection
- ❑ Access management
- ❑ Standardized approach / best practices

– –

Edu key requirements…

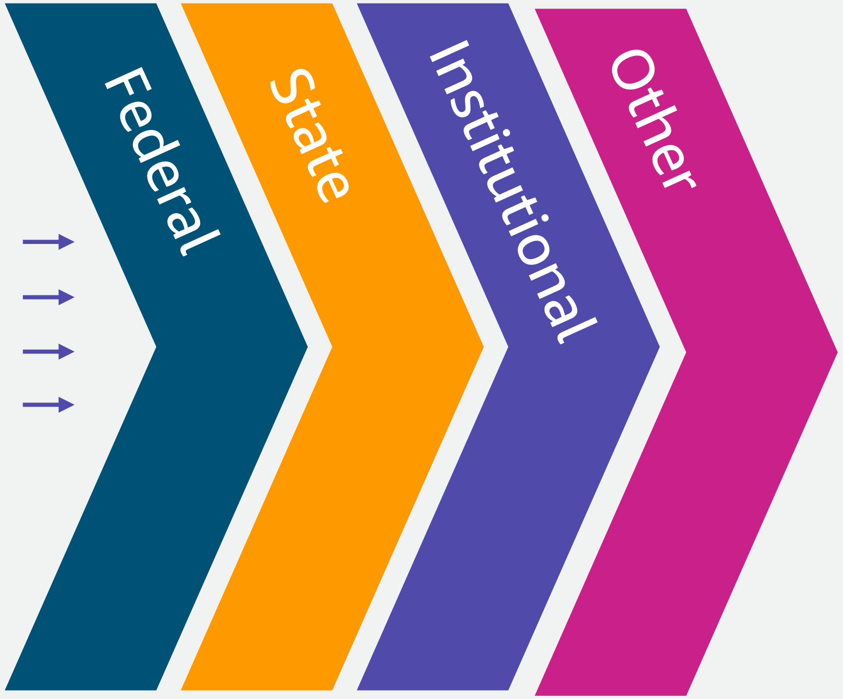
Student

Personnel

Research

Health

Financial



Federal

State

Institutional

Other

CCPA, Reasonable Security, Safe Harbor

Cyber + Ransomware threats, Resilience, Hybrid workplace

FERPA, FISMA,HEA HIPAA, CMMC, SAIG

NIST, CIS, ISO, Policies

Governance

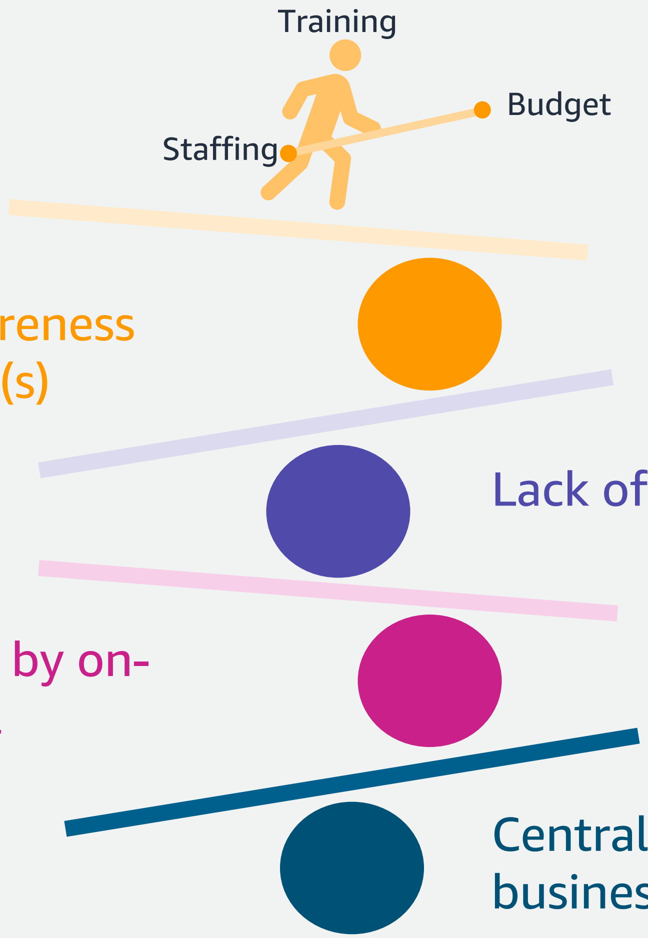
Scalability

Secure Design

Min overhead

Data Protection

Current key operational challenges…



Limited situational awareness across the environment(s)

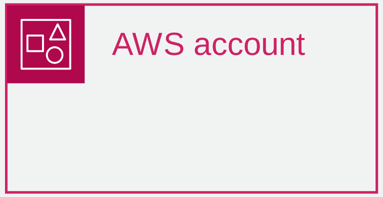
Lack of data type / sensitivity awareness

Cloud operations driven by on-premises security model

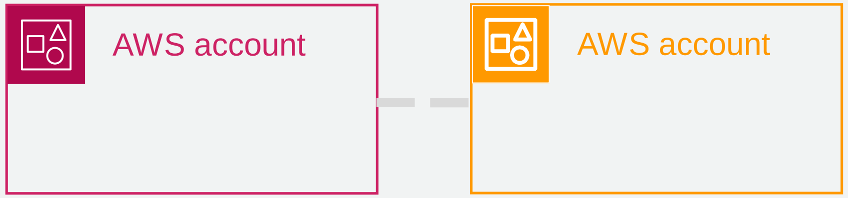
Centralized control vs. autonomy - Competing business requirements from different user groups

Current environment(s)...

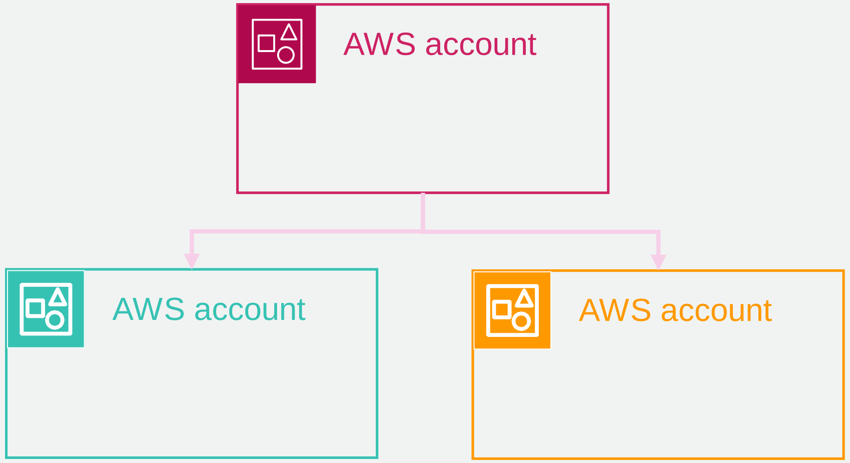
Workloads running in a single account



Workloads running in multiple accounts w/ no centralization



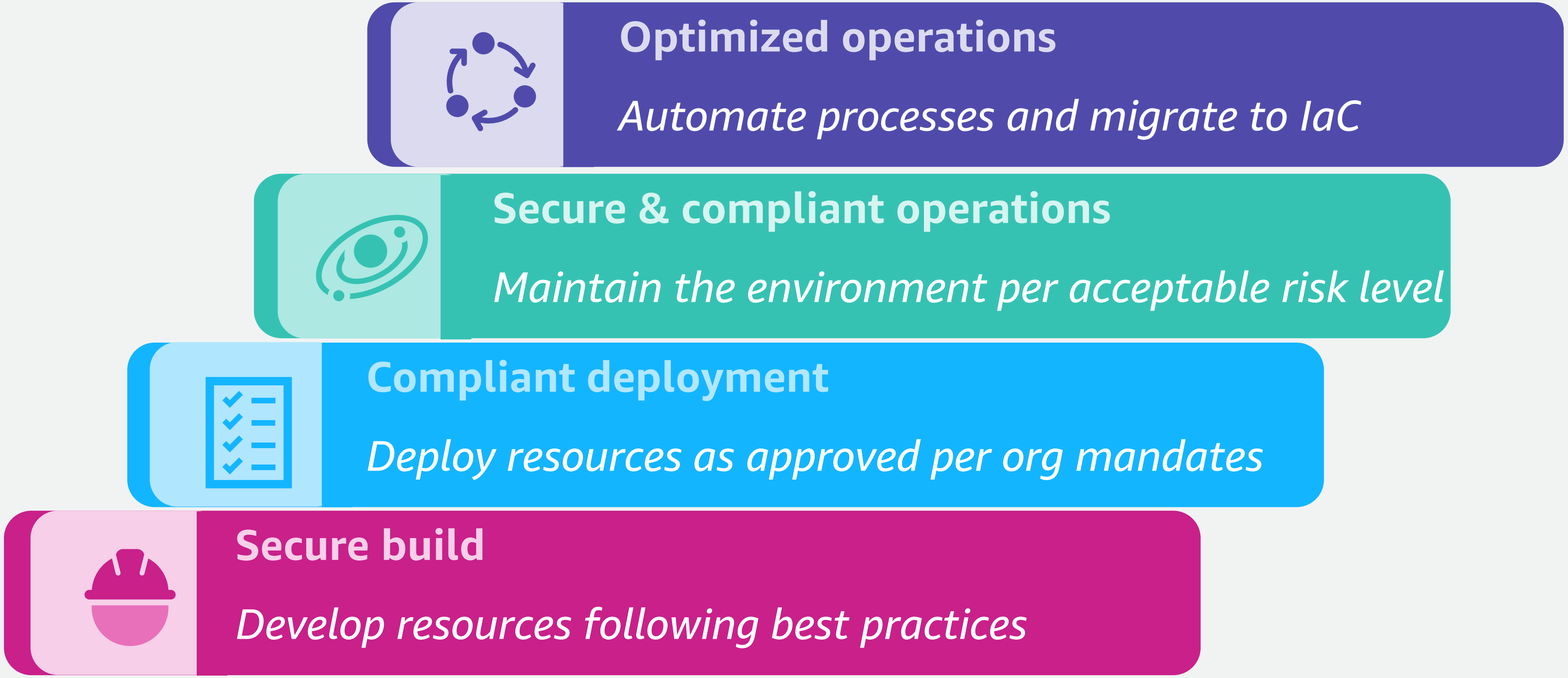
Workloads running in multiple accounts w/ some central oversight



In next 30 mins we will look at mechanisms to…

- ❑ Organize your security operations
- ❑ Create scalable design while providing autonomy
- ❑ Gain security visibility and responses with minimal overhead
- ❑ Operate in a compliant environment

Organizing your operations…



Optimized operations

Automate processes and migrate to IaC

Secure & compliant operations

Maintain the environment per acceptable risk level

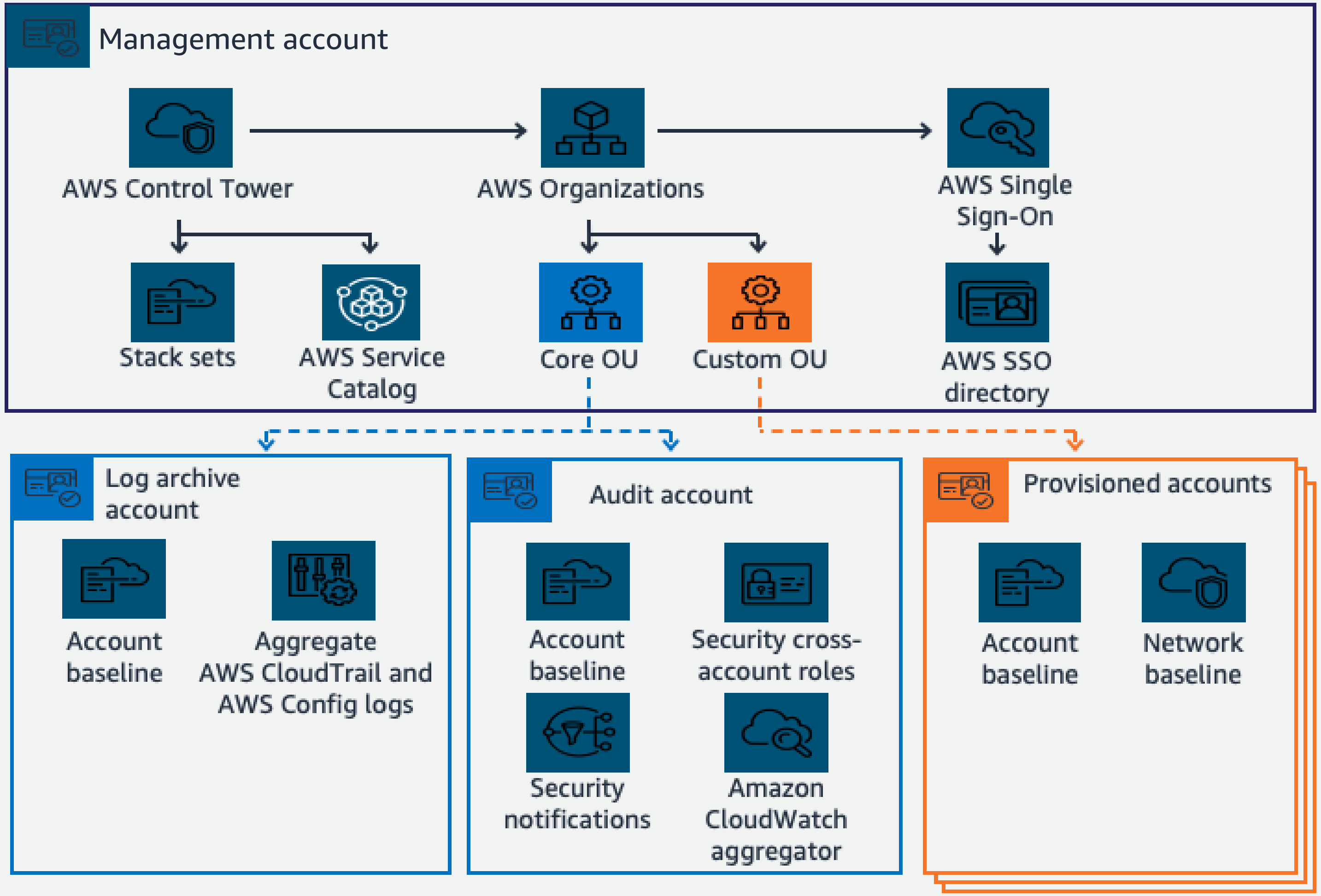
Compliant deployment

Deploy resources as approved per org mandates

Secure build

Develop resources following best practices

Multi-account framework using Control Tower



Control Tower baseline setup:

Core OU: AWS Control Tower baseline accounts (cannot change)

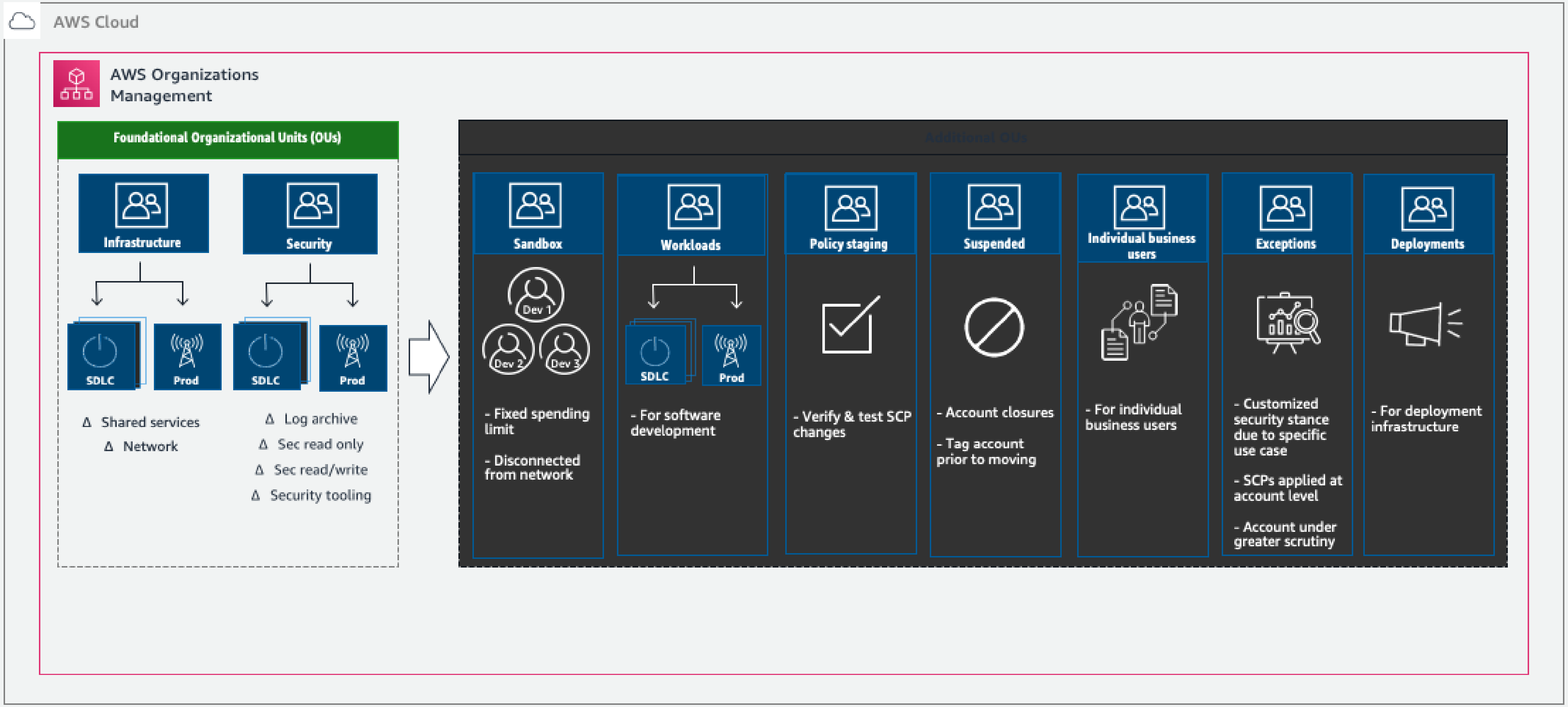
Custom OU: Your provisioned accounts

=> Mission Accounts

SRA Link here

Set up scalable organization foundation…

https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/



AWS Cloud

AWS Organizations Management

Foundational Organizational Units (OUs)

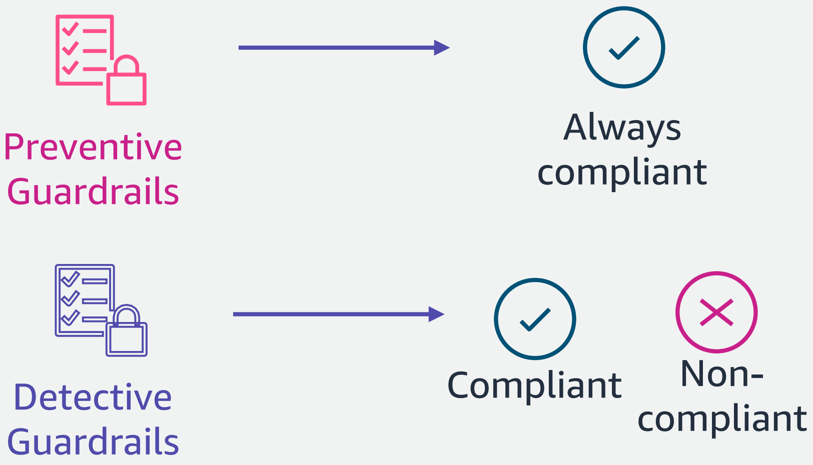
- Infrastructure: SDLC, Prod
  - ∆ Shared services
  - ∆ Network
- Security: SDLC, Prod
  - ∆ Log archive
  - ∆ Sec read only
  - ∆ Sec read/write
  - ∆ Security tooling

Additional OUs

- Sandbox (Dev 1, Dev 2, Dev 3)
  - Fixed spending limit
  - Disconnected from network
- Workloads (SDLC, Prod)
  - For software development
- Policy staging
  - Verify & test SCP changes
- Suspended
  - Account closures
  - Tag account prior to moving
- Individual business users
  - For individual business users
- Exceptions
  - Customized security stance due to specific use case
  - SCPs applied at account level
  - Account under greater scrutiny
- Deployments
  - For deployment infrastructure

Guardrails & SCPs - Rules for alignment with security and compliance

Applied at the OU/account level to restrict capabilities



Preventive Guardrails → Always compliant

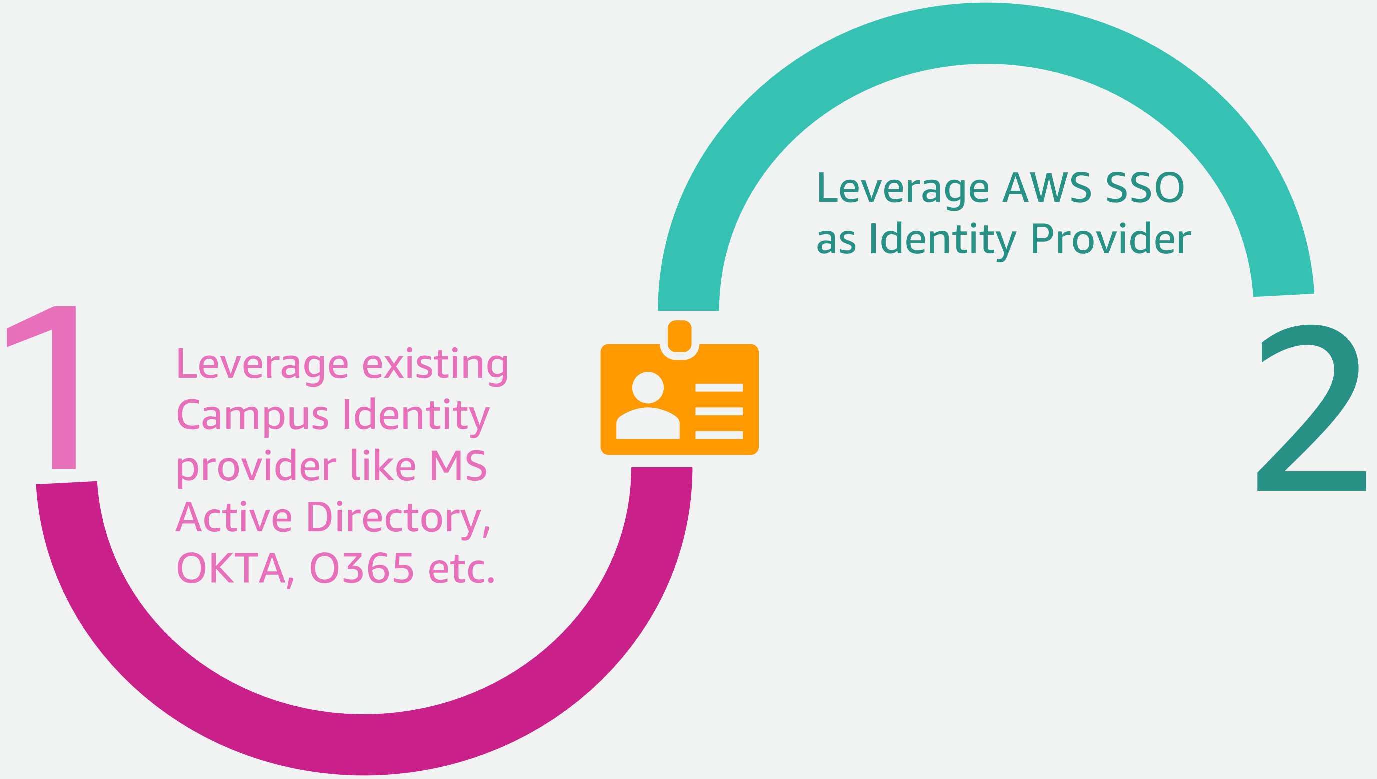
Detective Guardrails → Compliant / Non-compliant

#	Control	Enforcement mechanism	Control Type
1	Enforce S3 Encryption	SCP	Preventive
2	Deny Region Change for the account	SCP	Preventive
3	Disallow creating and attaching internet gateway (at account level)	SCP	Preventive
4	Only allow pre-defined EC2 instance types	SCP	Preventive
5	Disallow RDS database instances that are not storage encrypted	Guardrail	Detective
6	Disallow public read access to S3 buckets	Guardrail	Detective
7	Disallow internet connection through SSH	Guardrail	Detective

- Preventive guardrails: prevent policy violations through enforcement; implemented using AWS CloudFormation and SCPs
- Detective guardrails: detect policy violations and alert in the dashboard; implemented using AWS Config rules
- Mandatory and strongly recommended guardrails: provide prescriptive guidance

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_config.html

DO NOT create local IAM users… Federate instead



1

Leverage existing Campus Identity provider like MS Active Directory, OKTA, O365 etc.

Leverage AWS SSO as Identity Provider

2

IAM

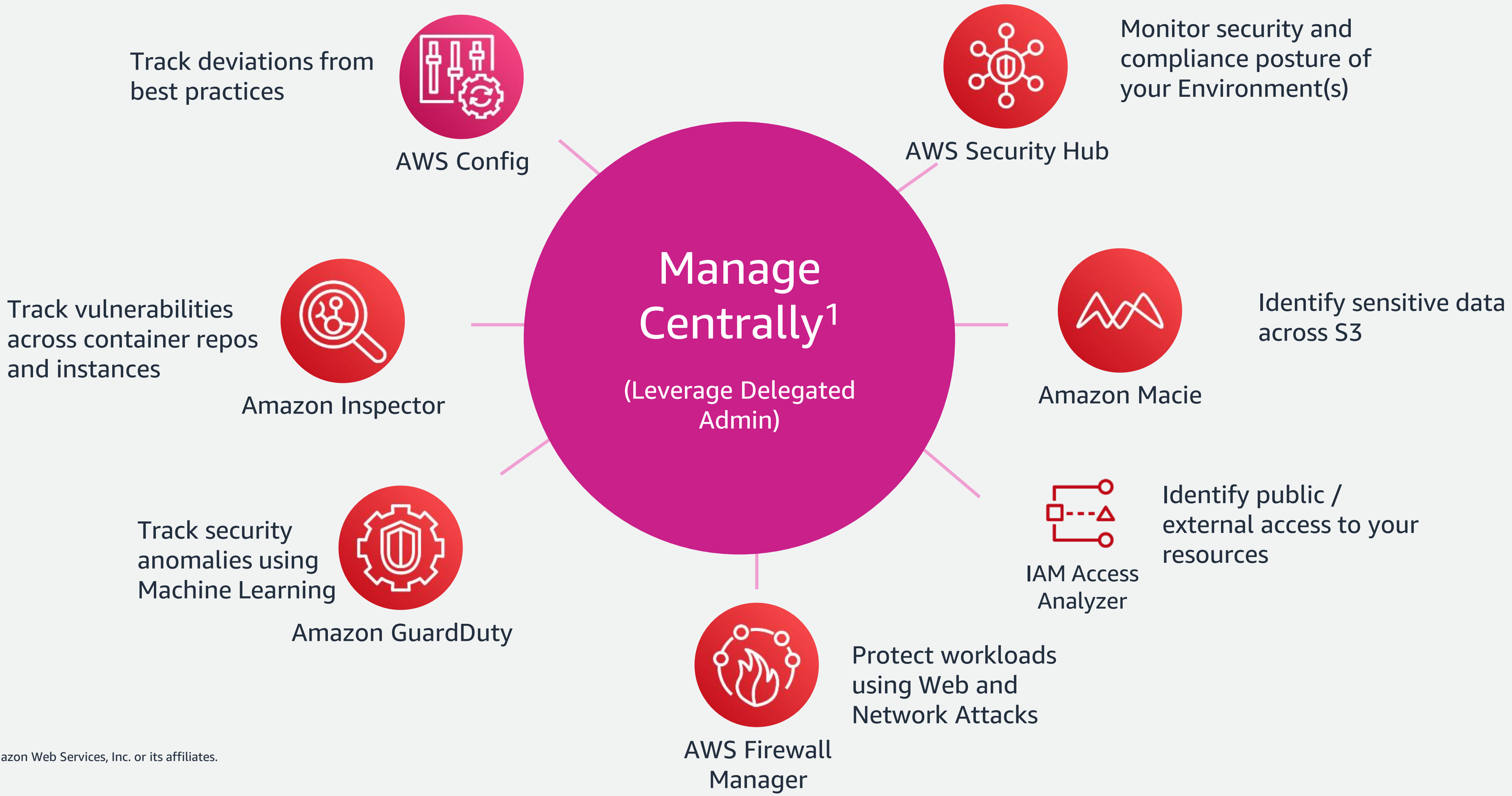
SSO

- Short term credentials (IAM Roles, Permission Sets)
- Multi-Factor enforcement
- Reduced attack surface
- Premade Job Function specific access policies
- Define maximum allowed permissions
- Reusable policies (ABAC)

SSO

- Single sign-on to 3rd Party applications
- Inherent federation across the Organization

Leverage managed services for security…



Manage Centrally[1]

(Leverage Delegated Admin)

AWS Config

Track deviations from best practices

AWS Security Hub

Monitor security and compliance posture of your Environment(s)

Amazon Inspector

Track vulnerabilities across container repos and instances

Amazon Macie

Identify sensitive data across S3

Amazon GuardDuty

Track security anomalies using Machine Learning

IAM Access Analyzer

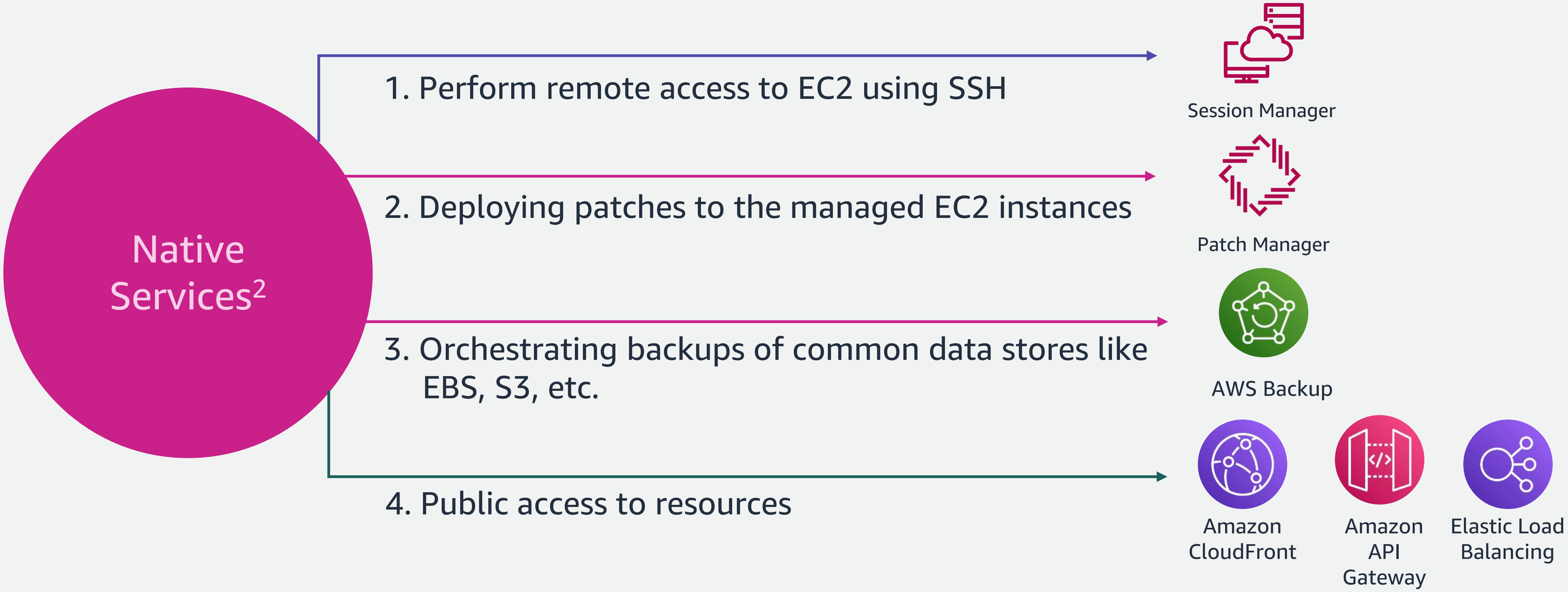
Identify public / external access to your resources

AWS Firewall Manager

Protect workloads using Web and Network Attacks

Leverage managed services for security…

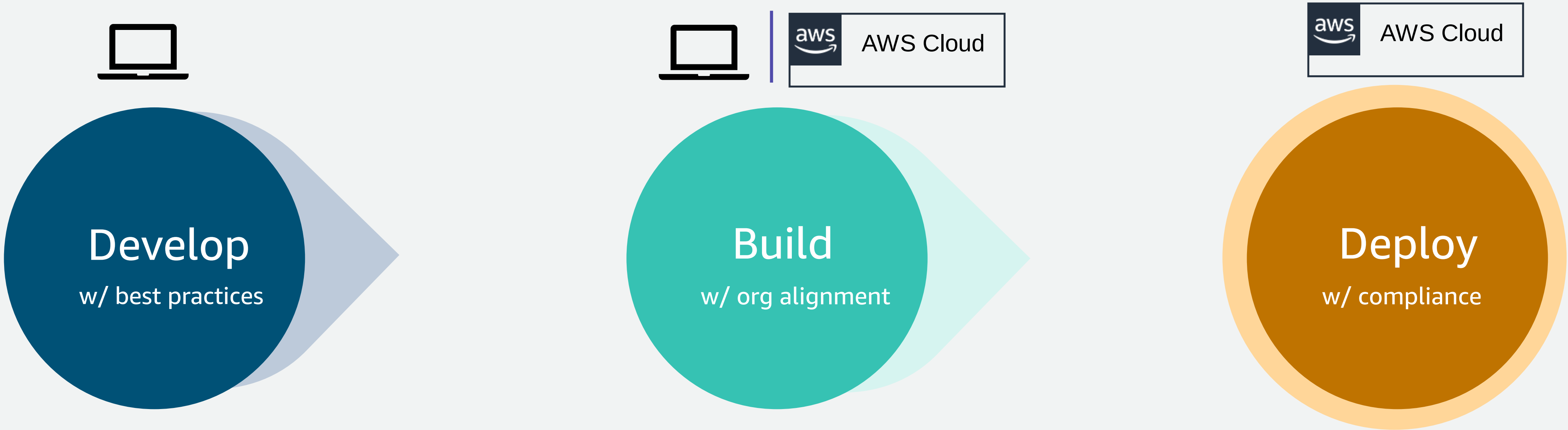
Reduce risk in common use cases using Native Services



Native Services[2]

1. Perform remote access to EC2 using SSH
2. Deploying patches to the managed EC2 instances
3. Orchestrating backups of common data stores like EBS, S3, etc.
4. Public access to resources

Enforcing continuous compliance – Infrastructure as Code



AWS Cloud

AWS Cloud

Develop
w/ best practices

Build
w/ org alignment

Deploy
w/ compliance

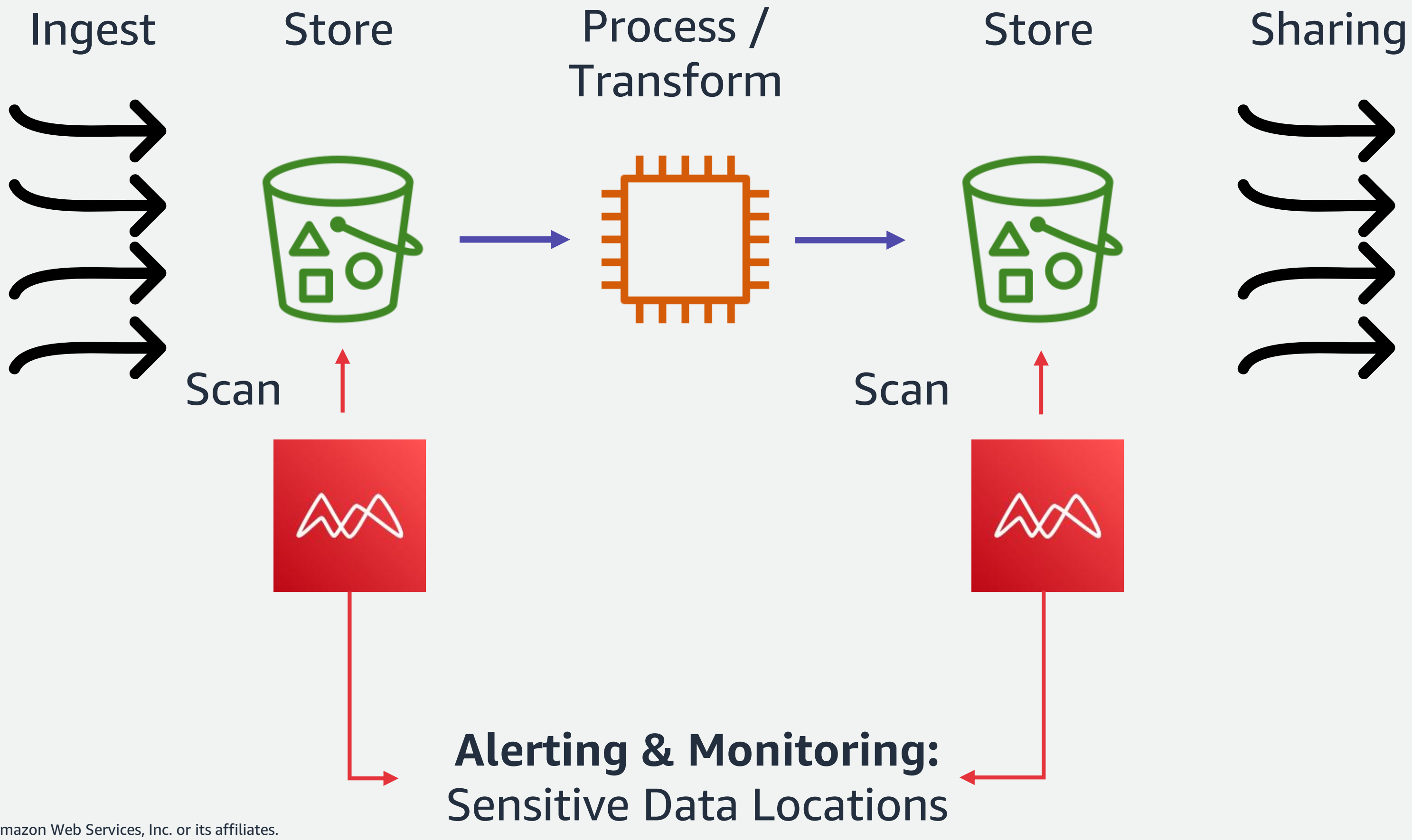
- ❑ Cfn-lint Check for common errors and best practices https://github.com/aws-cloudformation/cfn-lint
- ❑ Cfn-Guard* Checks against your security requirements https://github.com/aws-cloudformation/cloudformation-guard
- ❑ Cfn ensures immutable compliant environment https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/detect-drift-stack.html

» https://aws.amazon.com/blogs/devops/integrating-aws-cloudformation-guard/

*** Also covers Terraform**

Detect sensitive data as pipeline...

Macie can help identify sensitive data so you can enforce policies to prevent exposure



Set up detection and alerting…

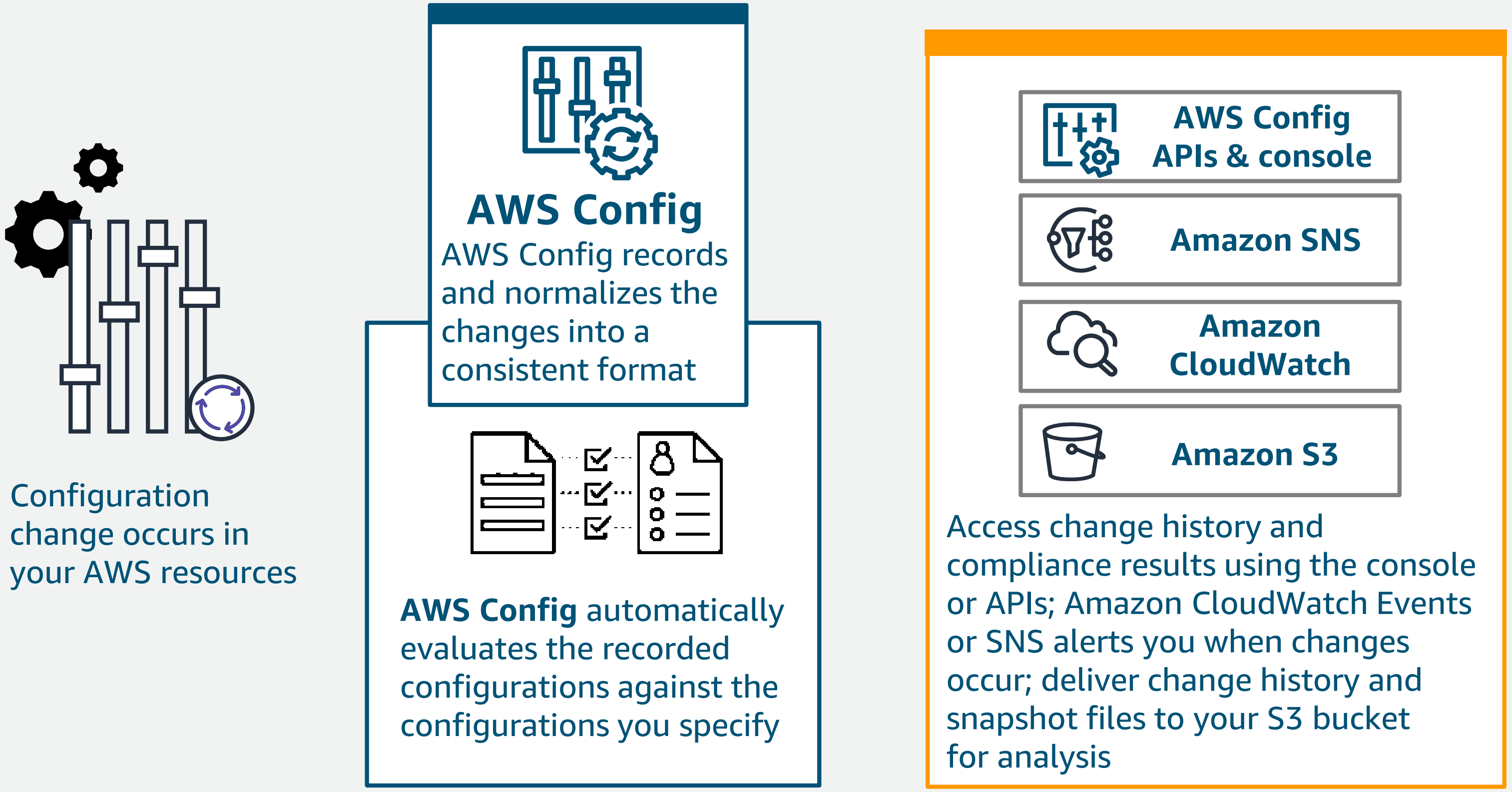
1. **Validate logging** is enabled across services (e.g. Flow logs, CloudTrail, Config, etc.)

2. **Enable Managed Services** for Detection (e.g. GuardDuty, Inspector, Config etc.)

3. **Set up alerting** for key items (e.g. GuardDuty findings, Root Account use etc.)

Alert customer use case example (One vs many team)

Managing continuous compliance – AWS Config



Configuration change occurs in your AWS resources

AWS Config

AWS Config records and normalizes the changes into a consistent format

AWS Config automatically evaluates the recorded configurations against the configurations you specify

Access change history and compliance results using the console or APIs; Amazon CloudWatch Events or SNS alerts you when changes occur; deliver change history and snapshot files to your S3 bucket for analysis

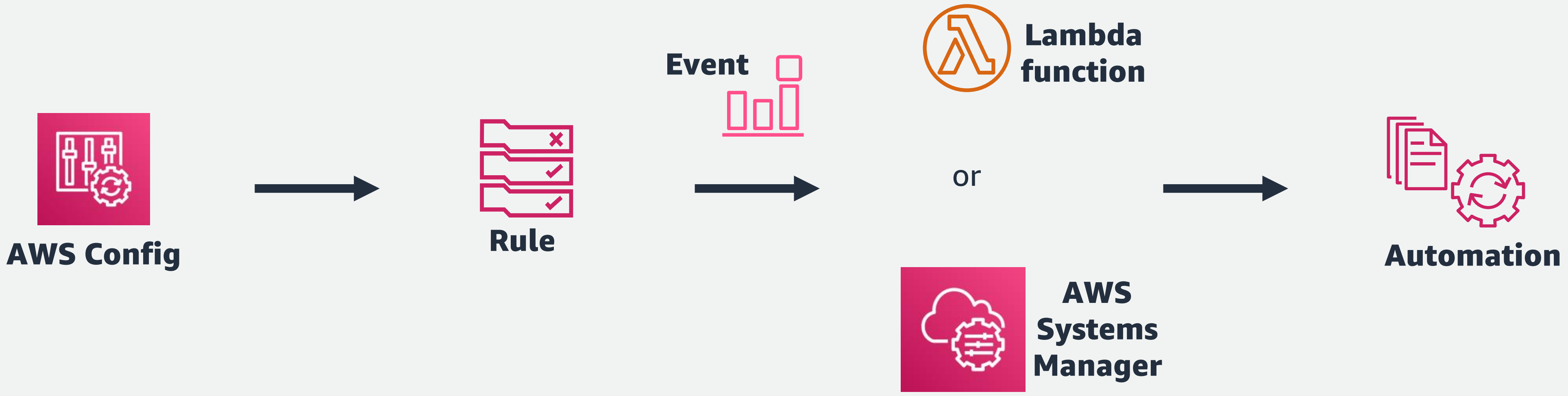
✓Requirements enforced using managed rules

✓Rules applied on a defined schedule or configuration changes

✓Rules can be scoped based on resource tags

https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html

Managing continuous compliance – AWS Config



1. AWS Config continuously records changes to AWS resources

2. A rule evaluation is triggered either periodically or when a resource configuration changes

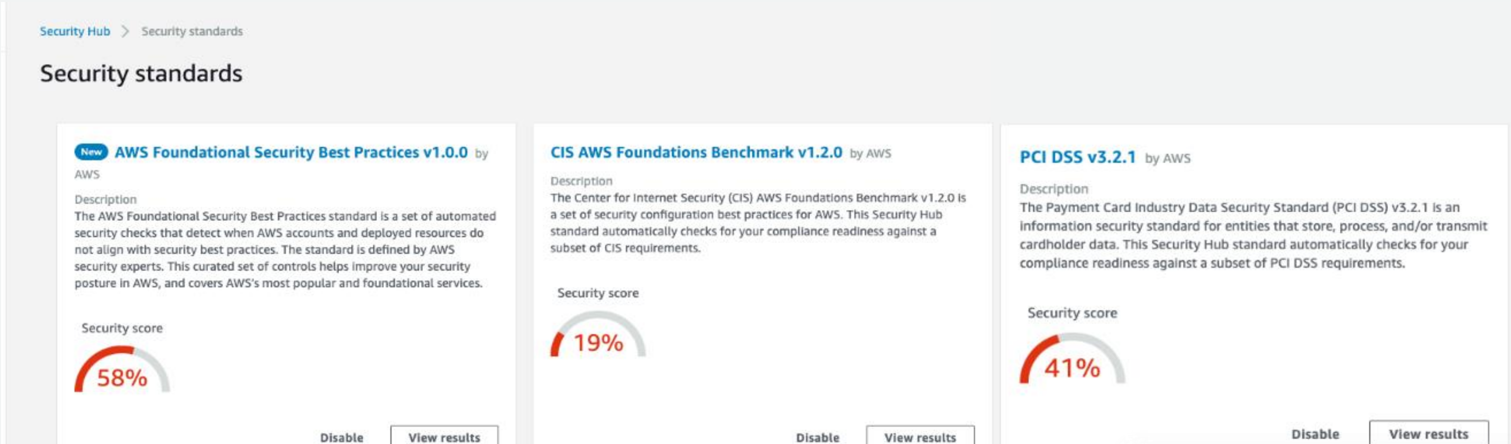
   The evaluation will return a state of "compliant" or "noncompliant" based off of a set of criteria

3. For "noncompliant" outcomes, an auto remediation via Lambda or SSM can be triggered

4. Lambda or SSM can perform the remediation

   After completion, the resource will return to a compliant state after the configuration change is made and the resource is re-evaluated

Managing continuous compliance – AWS Security Hub



Security Hub > Security standards

Security standards

New AWS Foundational Security Best Practices v1.0.0 by AWS

Description
The AWS Foundational Security Best Practices standard is a set of automated security checks that detect when AWS accounts and deployed resources do not align with security best practices. The standard is defined by AWS security experts. This curated set of controls helps improve your security posture in AWS, and covers AWS's most popular and foundational services.

Security score: 58%

CIS AWS Foundations Benchmark v1.2.0 by AWS

Description
The Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.

Security score: 19%

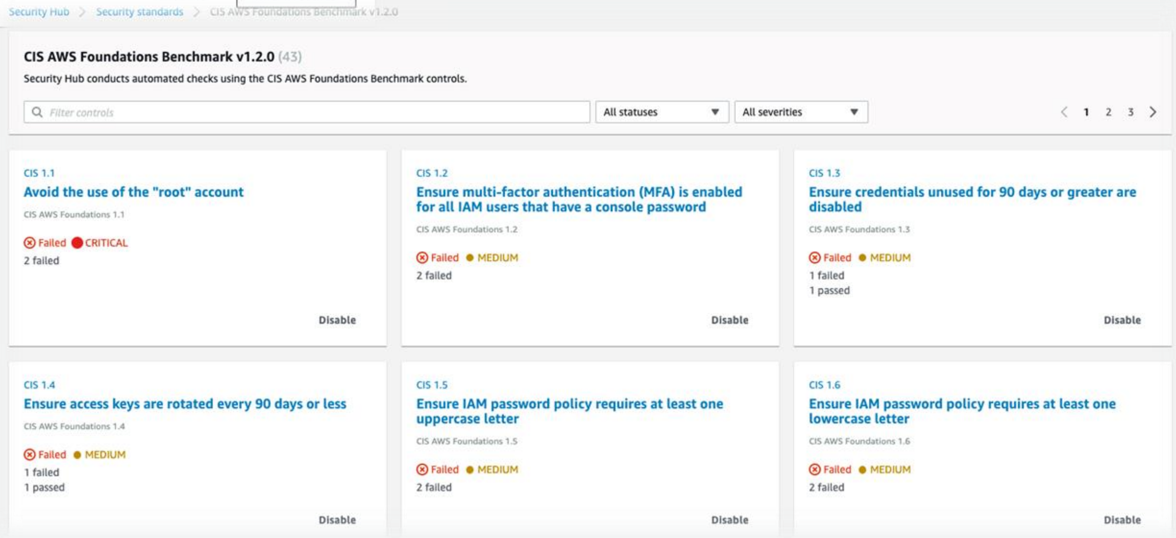
PCI DSS v3.2.1 by AWS

Description
The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data. This Security Hub standard automatically checks for your compliance readiness against a subset of PCI DSS requirements.

Security score: 41%

- ❑ Single click deployment
- ❑ Continuous monitoring

- ○ Detailed dashboard
- ○ Actionable information
- ○ Support for automated remediation



Security Hub > Security standards > CIS AWS Foundations Benchmark v1.2.0

CIS AWS Foundations Benchmark v1.2.0 (43)

Security Hub conducts automated checks using the CIS AWS Foundations Benchmark controls.

Filter controls | All statuses ▼ | All severities ▼ | < 1 2 3 >

CIS 1.1
Avoid the use of the "root" account
CIS AWS Foundations 1.1
⊗ Failed ● CRITICAL
2 failed

CIS 1.2
Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
CIS AWS Foundations 1.2
⊗ Failed ● MEDIUM
2 failed

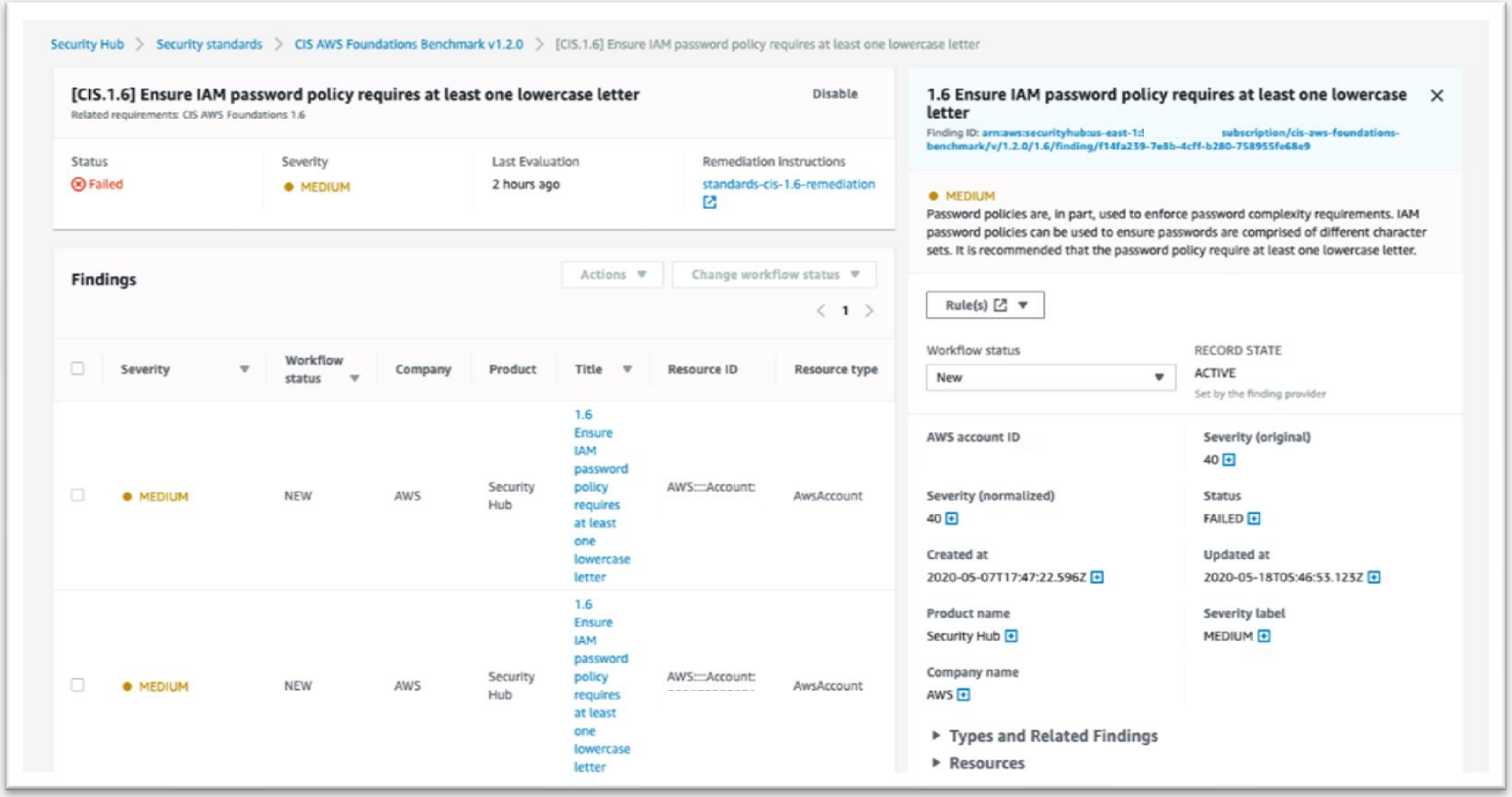
CIS 1.3
Ensure credentials unused for 90 days or greater are disabled
CIS AWS Foundations 1.3
⊗ Failed ● MEDIUM
1 failed
1 passed

CIS 1.4
Ensure access keys are rotated every 90 days or less
CIS AWS Foundations 1.4
⊗ Failed ● MEDIUM
1 failed
1 passed

CIS 1.5
Ensure IAM password policy requires at least one uppercase letter
CIS AWS Foundations 1.5
⊗ Failed ● MEDIUM
2 failed

CIS 1.6
Ensure IAM password policy requires at least one lowercase letter
CIS AWS Foundations 1.6
⊗ Failed ● MEDIUM
2 failed

Managing continuous compliance – AWS Security Hub



Security Hub > Security standards > CIS AWS Foundations Benchmark v1.2.0 > [CIS.1.6] Ensure IAM password policy requires at least one lowercase letter

[CIS.1.6] Ensure IAM password policy requires at least one lowercase letter

Related requirements: CIS AWS Foundations 1.6

Status	Severity	Last Evaluation	Remediation instructions
Failed	● MEDIUM	2 hours ago	standards-cis-1.6-remediation

Findings

□	Severity	Workflow status	Company	Product	Title	Resource ID	Resource type
□	● MEDIUM	NEW	AWS	Security Hub	1.6 Ensure IAM password policy requires at least one lowercase letter	AWS::::Account:	AwsAccount
□	● MEDIUM	NEW	AWS	Security Hub	1.6 Ensure IAM password policy requires at least one lowercase letter	AWS::::Account:	AwsAccount

1.6 Ensure IAM password policy requires at least one lowercase letter

Finding ID: arn:aws:securityhub:us-east-1: subscription/cis-aws-foundations-benchmark/v/1.2.0/1.6/finding/f14fa239-7e8b-4cff-b280-758955fe68e9

● MEDIUM

Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure passwords are comprised of different character sets. It is recommended that the password policy require at least one lowercase letter.

Workflow status: New

RECORD STATE: ACTIVE
Set by the finding provider

AWS account ID

Severity (original): 40

Severity (normalized): 40

Status: FAILED

Created at: 2020-05-07T17:47:22.596Z

Updated at: 2020-05-18T05:46:53.123Z

Product name: Security Hub

Severity label: MEDIUM

Company name: AWS

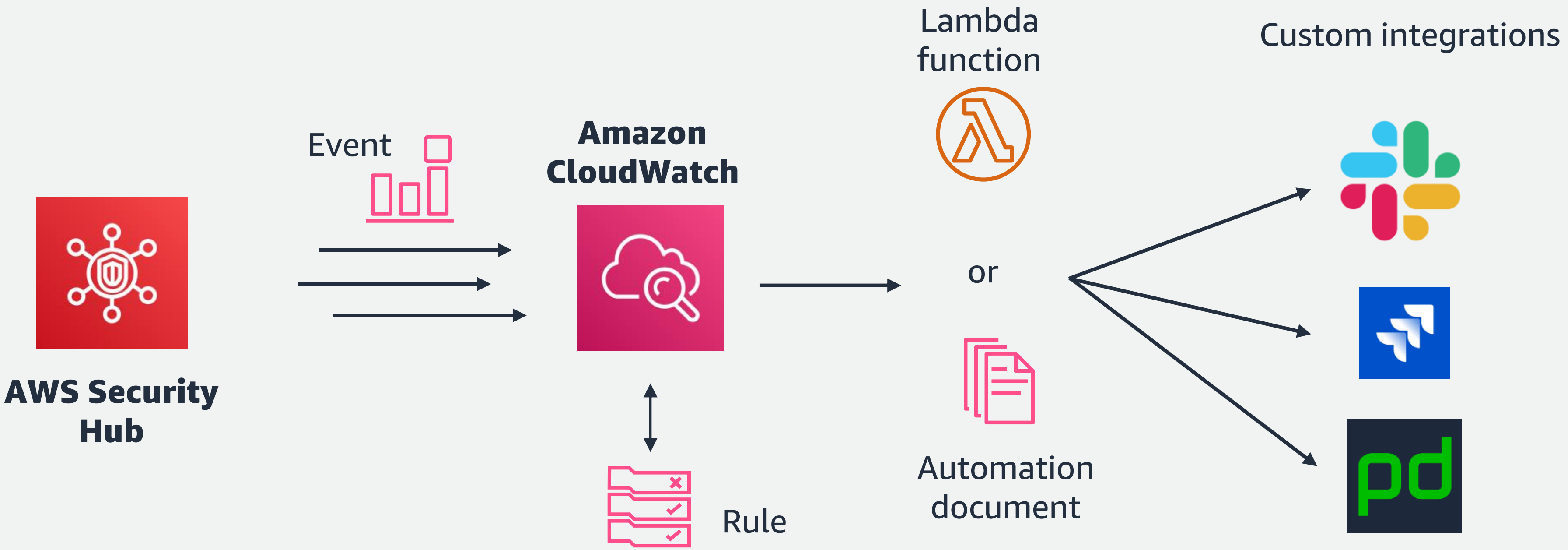
▸ Types and Related Findings

▸ Resources

- ❑ Detailed information about each control
- ❑ Supports risk acceptance and management workflows
- ❑ Integrates with multiple partner products

https://aws.amazon.com/solutions/implementations/aws-security-hub-automated-response-and-remediation/

Managing continuous compliance – AWS Security Hub



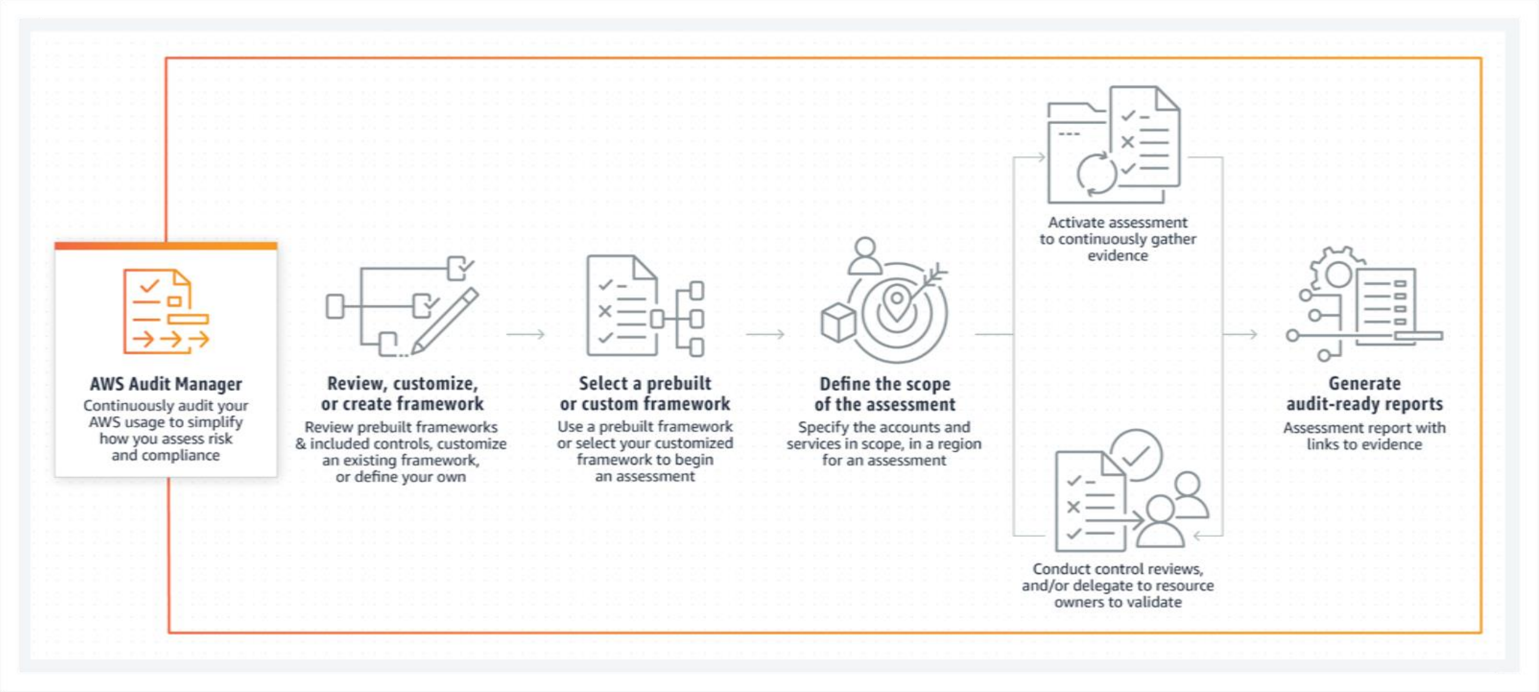
1. All findings automatically sent to Amazon CloudWatch Events
2. Security Hub user selects findings in the console and takes custom action; findings sent to CloudWatch, decorated with a custom action ID

3. User creates CloudWatch Events rules to look for certain findings associated with a custom action ID or specific characteristics

4. The rule defines a target, typically a Lambda function, Step Function, or automation document

5. The target could be things like a chat, ticketing, on-call management, SOAR platform, or custom remediation playbook

Reporting continuous compliance – AWS Audit Manager


AWS Audit Manager
Continuously audit your AWS usage to simplify how you assess risk and compliance
Review, customize, or create framework
Review prebuilt frameworks & included controls, customize an existing framework, or define your own
Select a prebuilt or custom framework
Use a prebuilt framework or select your customized framework to begin an assessment
Define the scope of the assessment
Specify the accounts and services in scope, in a region for an assessment
Activate assessment to continuously gather evidence
Conduct control reviews, and/or delegate to resource owners to validate
Generate audit-ready reports
Assessment report with links to evidence

- □ Single click deployment
- □ Continuous evidence collection
- □ Creates audit ready reports
- □ Reduces manual errors
- □ Tamper proof authoritative evidence repository

https://aws.amazon.com/blogs/security/streamlining-evidence-collection-with-aws-audit-manager/

Optimize security process using AWS Solutions… (1/2)

1. **Reduce the noise** by fine tuning the security findings (e.g. suppressing GuardDuty findings)
2. **View the security posture** across your organization **centrally** using Security Hub insights
3. **Set up automated response** to best practice violations

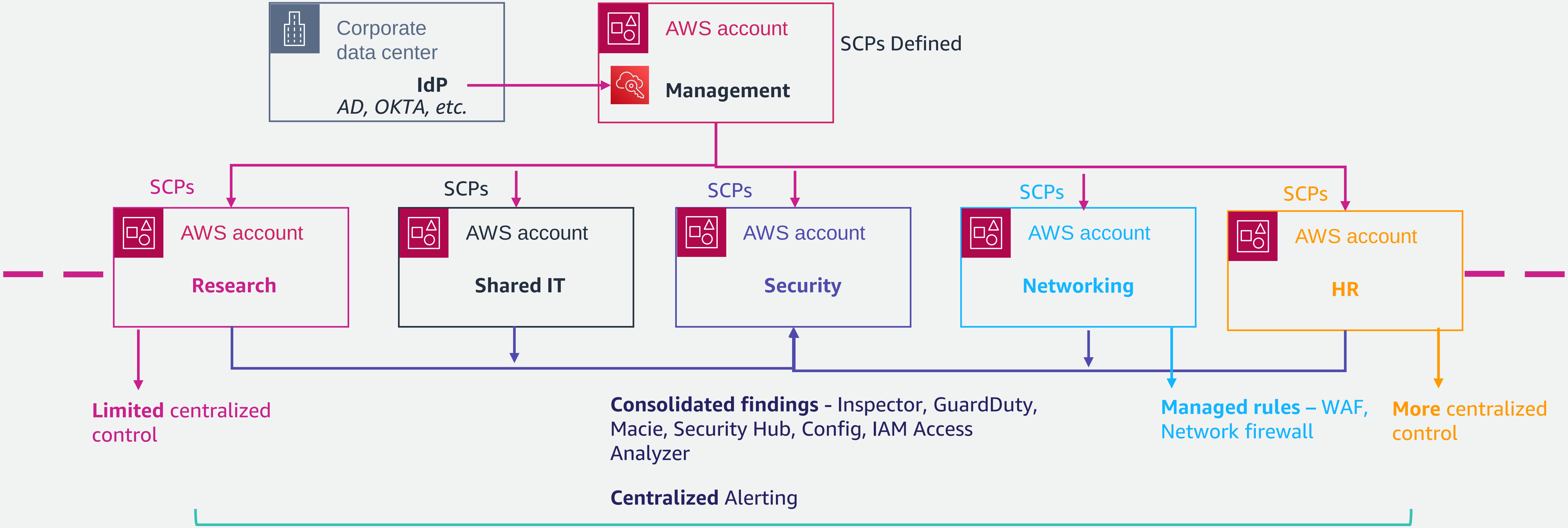
Optimize security process using AWS Solutions… (2/2)

IAM Access Analyzer can help reduce risk of accidental public exposure

Automatically fine grain the permissions periodically

Automate the detection of public access

Putting it all together...



Corporate data center

IdP

AD, OKTA, etc.

AWS account

Management

SCPs Defined

SCPs

AWS account

Research

SCPs

AWS account

Shared IT

SCPs

AWS account

Security

SCPs

AWS account

Networking

SCPs

AWS account

HR

Limited centralized control

Consolidated findings - Inspector, GuardDuty, Macie, Security Hub, Config, IAM Access Analyzer

Centralized Alerting

Managed rules – WAF, Network firewall

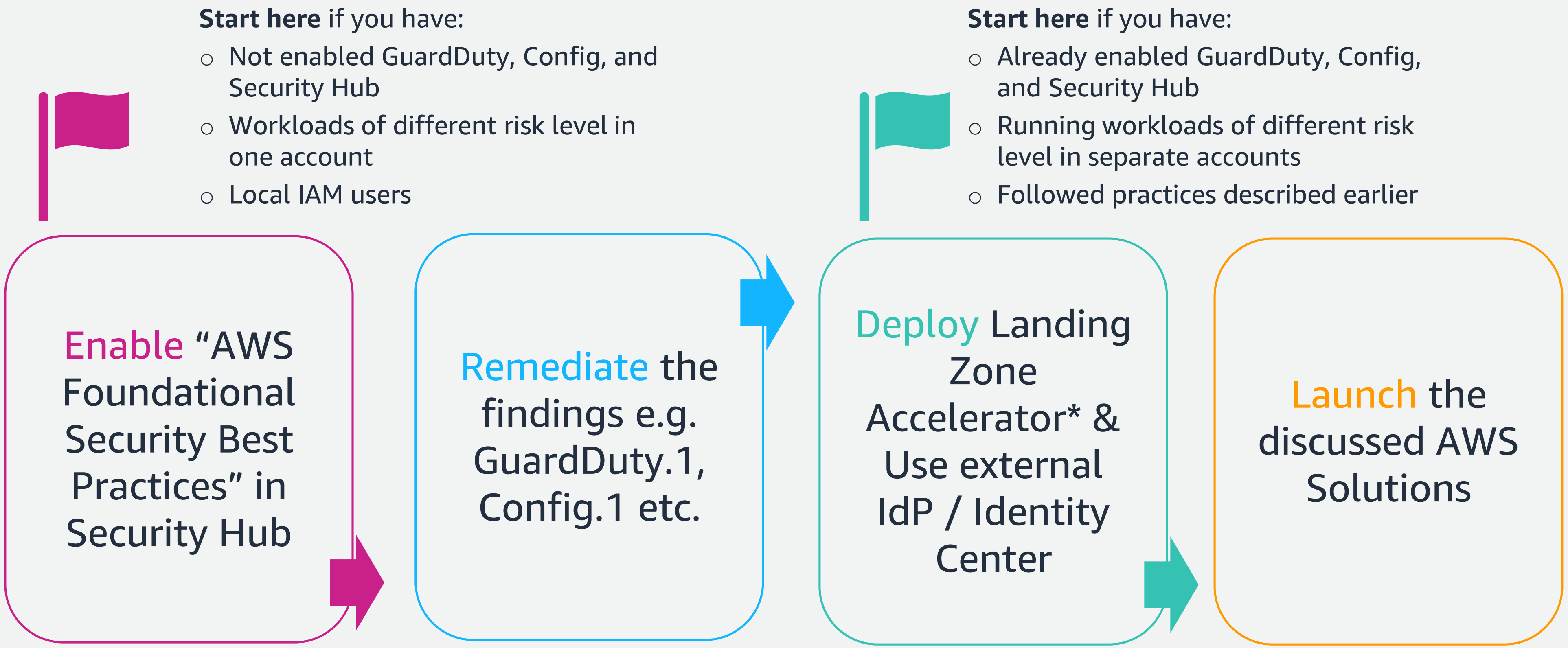
More centralized control

Centralized deployment:

- **Automated** remediation playbooks
- IAM **Permission Boundaries**
- Custom Policies (Identity Store)

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

Where do I start?



Start here if you have:

- Not enabled GuardDuty, Config, and Security Hub
- Workloads of different risk level in one account
- Local IAM users

Start here if you have:

- Already enabled GuardDuty, Config, and Security Hub
- Running workloads of different risk level in separate accounts
- Followed practices described earlier

Enable “AWS Foundational Security Best Practices” in Security Hub

Remediate the findings e.g. GuardDuty.1, Config.1 etc.

Deploy Landing Zone Accelerator* & Use external IdP / Identity Center

Launch the discussed AWS Solutions

* *https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/*

Thank you!

Resources

- Leverage managed services for security:

1. Manage centrally:
   - https://aws.amazon.com/blogs/mt/automating-amazon-guardduty-deployment-in-aws-control-tower/
   - https://controltower.aws-management.tools/security/securityhub/
   - https://aws.amazon.com/blogs/mt/using-delegated-admin-for-aws-config-operations-and-aggregation/
   - https://aws.amazon.com/blogs/mt/enabling-aws-identity-and-access-analyzer-on-aws-control-tower-accounts/
   - https://aws.amazon.com/solutions/implementations/aws-firewall-mgr-automations-for-aws-orgs/
2. Native services for common use cases:
   - https://aws.amazon.com/blogs/storage/create-and-share-encrypted-backups-across-accounts-and-regions-using-aws-backup/
   - https://aws.amazon.com/blogs/aws/new-port-forwarding-using-aws-system-manager-sessions-manager/

Resources

- Optimize using Security Solutions:

1. Reduce the noise by fine tuning the security findings https://aws.amazon.com/blogs/security/how-to-create-auto-suppression-rules-in-aws-security-hub/

2. View the security posture across your organization centrally using Security Hub insights https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-insights.html

3. Set up automated response to best practice violations https://aws.amazon.com/solutions/implementations/aws-security-hub-automated-response-and-remediation/

Resources

- Leverage IAM Access Analyzer:

1. Fine grain the permissions periodically
   https://aws.amazon.com/blogs/security/iam-access-analyzer-makes-it-easier-to-implement-least-privilege-permissions-by-generating-iam-policies-based-on-access-activity/
2. Automate the detection of public access
   https://aws.amazon.com/blogs/security/how-to-use-aws-iam-access-analyzer-api-to-automate-detection-of-public-access-to-aws-kms-keys/