AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

GPS206

Security at scale with AWS Partners and AWS services

Sameer Kumar Vasanthapuram
Principal Solutions Architect
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why are we here?

Security is job zero

Customers want agility at scale

We want to help you move faster

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What should you walk away with?

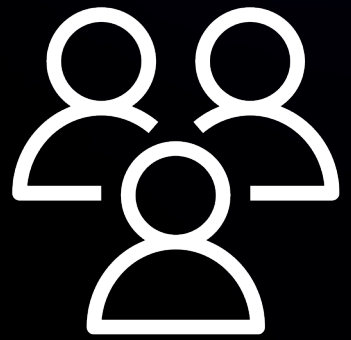
What customers expect

A perspective on how to scale with AWS services

Better understanding of security approaches on AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

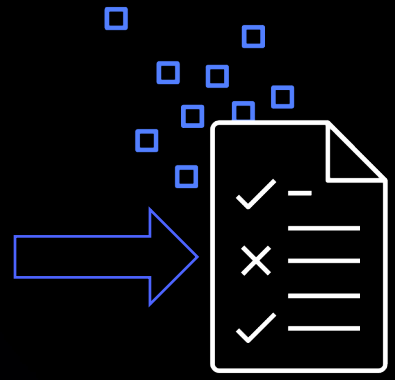
Customers want . . .



To enable many teams of **developers**



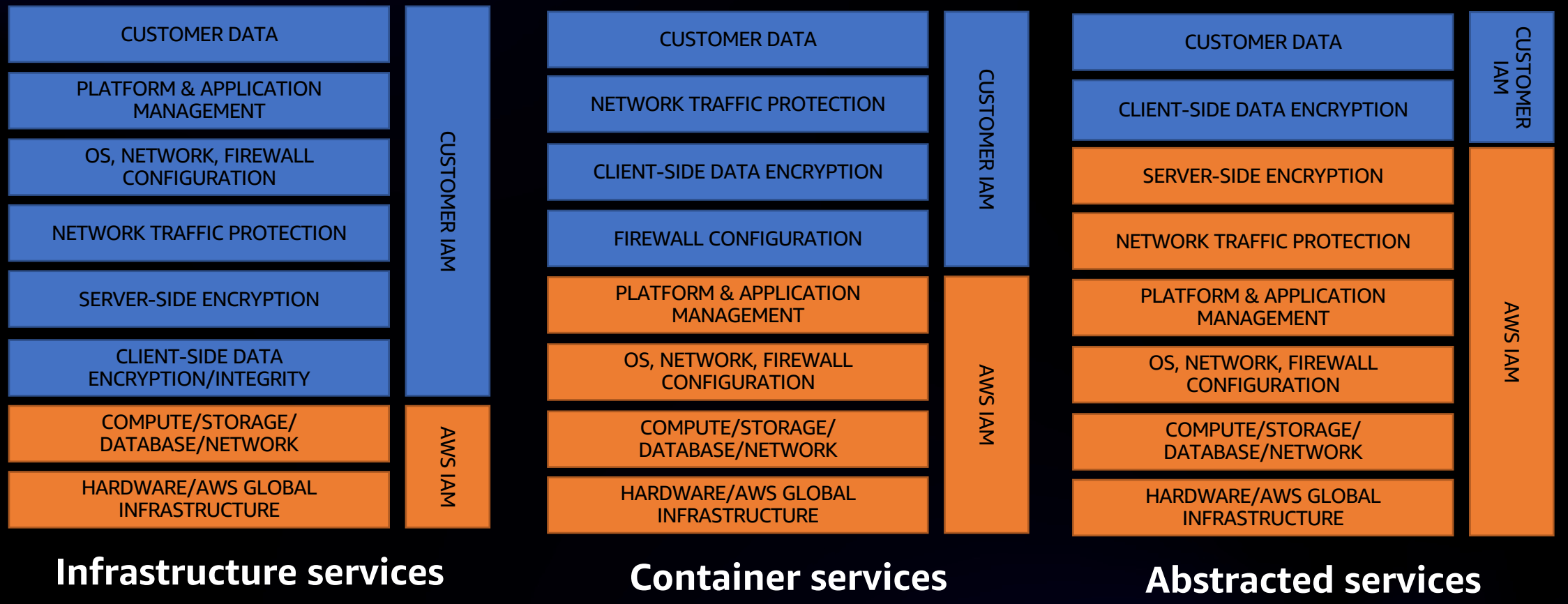
Security and compliance controls



To take action

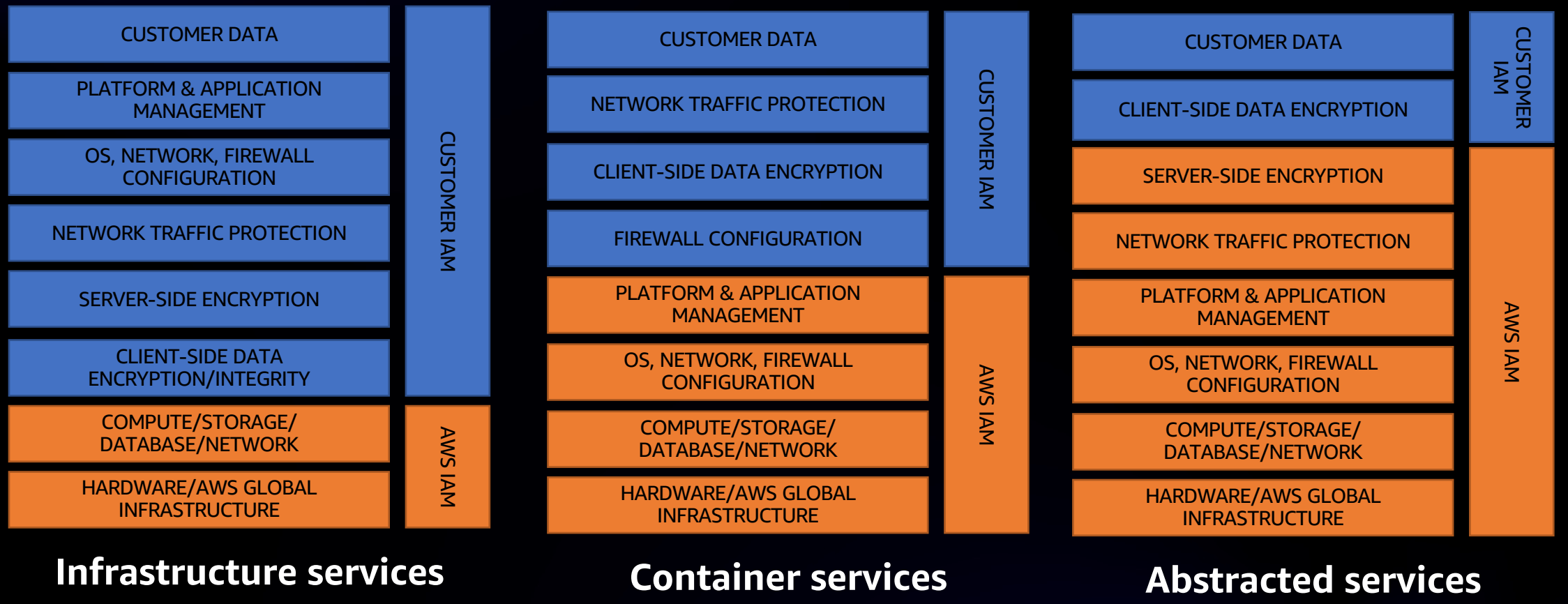
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Shared Responsibility Model



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Shared Responsibility Model



More best practices built in + less customer responsibility

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

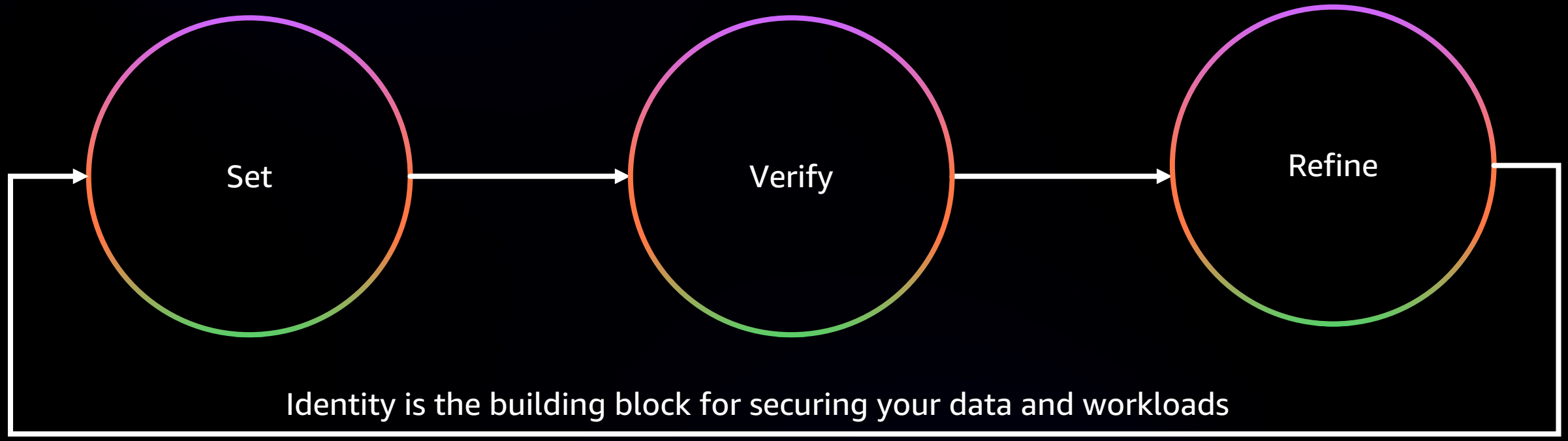


Identity

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identities and perimeters



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identity hygiene

Disable root access, enable MFA

Principle of least privilege

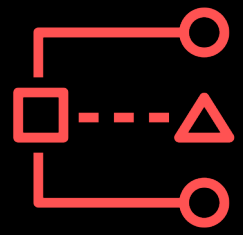
Roles over users wherever possible

Password policy and key rotation

Federation across accounts



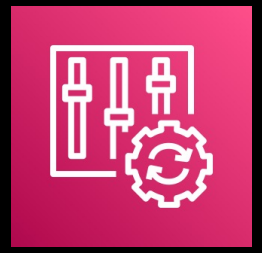
AWS CloudFormation



AWS IAM Access Analyzer



AWS CloudTrail



AWS Config



AWS Single Sign-On

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Verify intended permissions

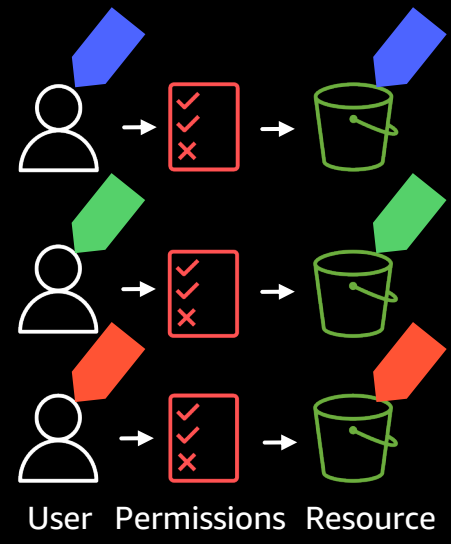
Public and cross-account access

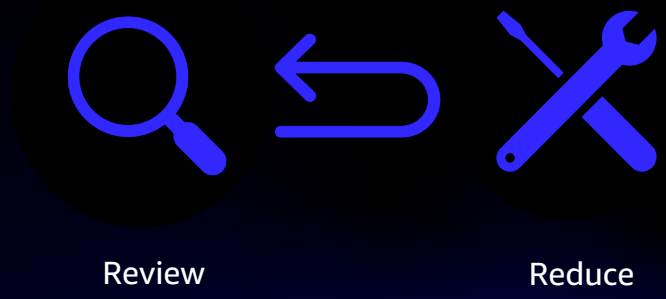
Tagging and attribute-based access controls to scale

Audit unused roles

Validate permissions periodically

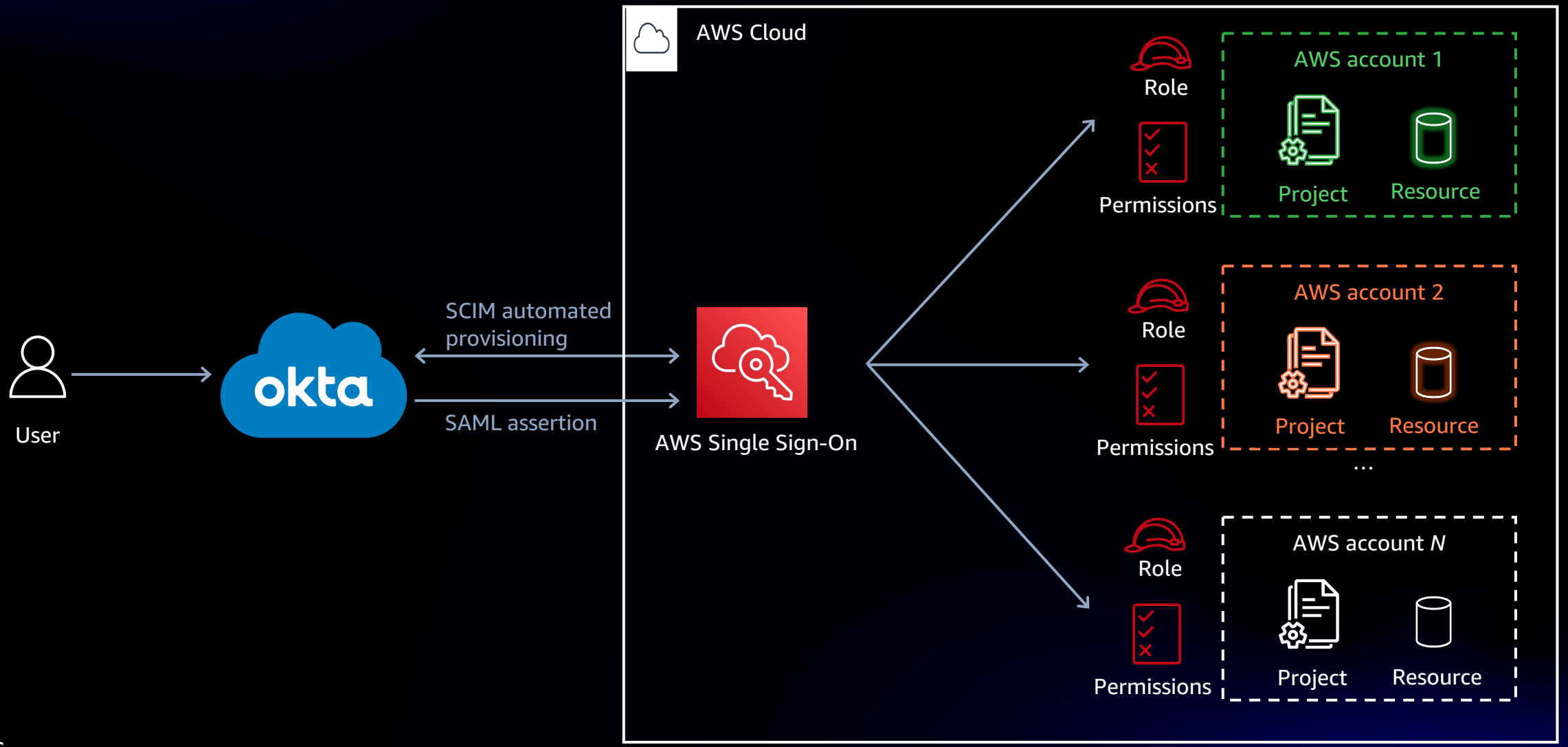
Iterate to tighten access





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Single sign-on with AWS SSO



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Foundations

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Foundations

Built first

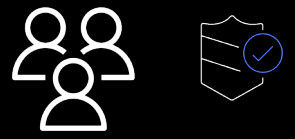
Allows you to build on top

Provides durability and resilience



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

APIs



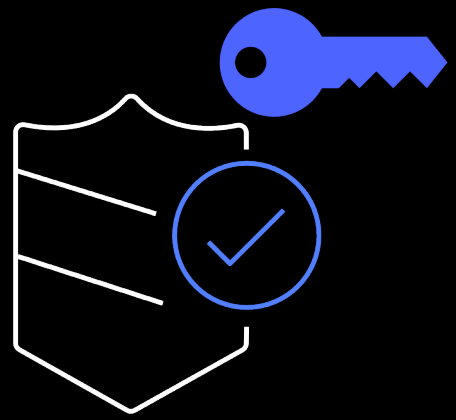
Every request is authenticated and authorized

Discover resources

Monitor every request

Orchestrate changes

Audit configuration



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

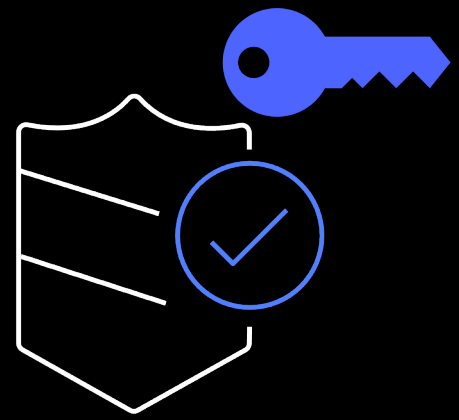
Using AWS APIs

Evaluate, implement, and enforce security baselines

Build controls for compliance and governance

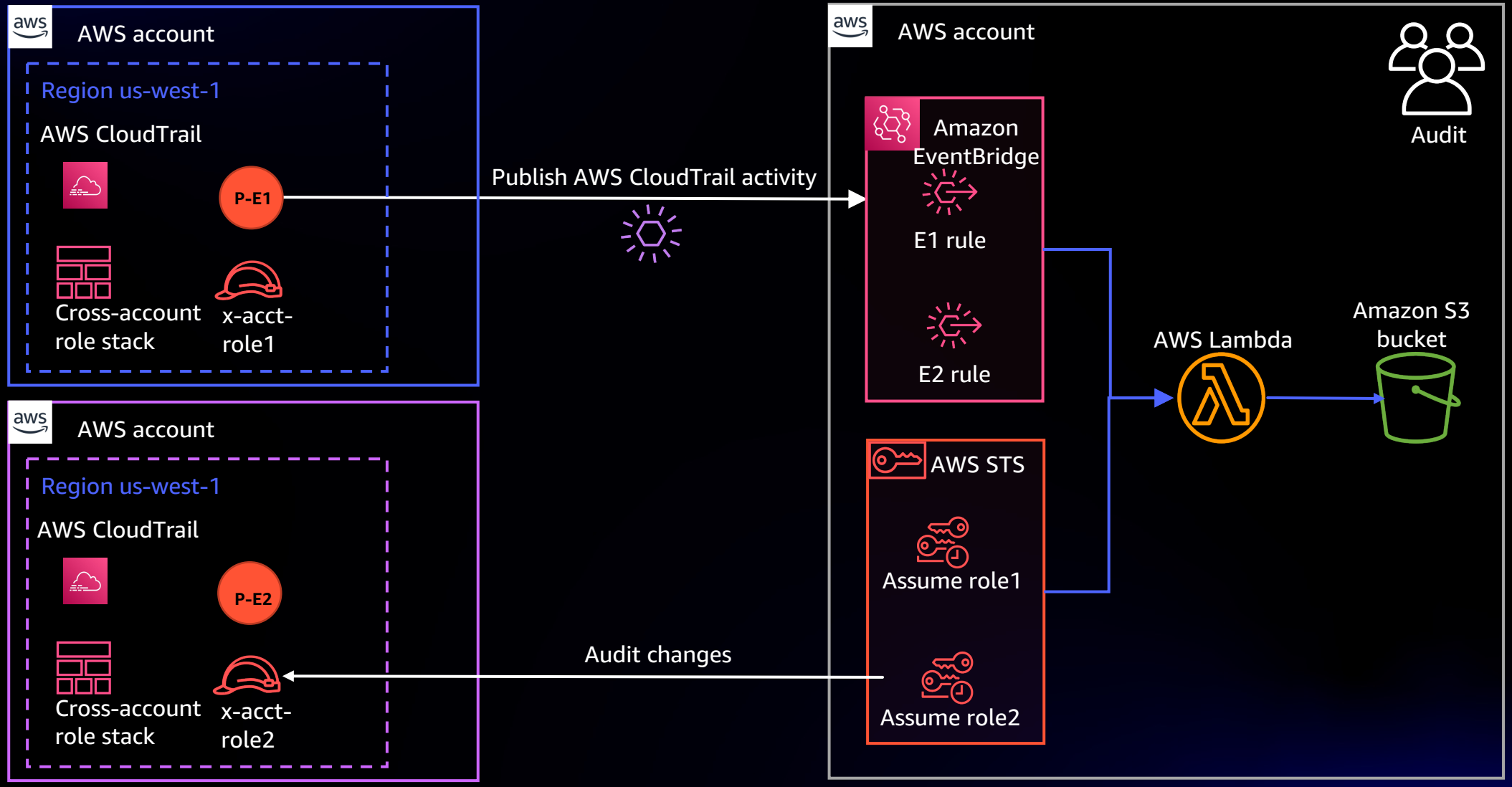
Correlate activity with users, roles, and AWS metadata

Prepare for audit, incident detection and response



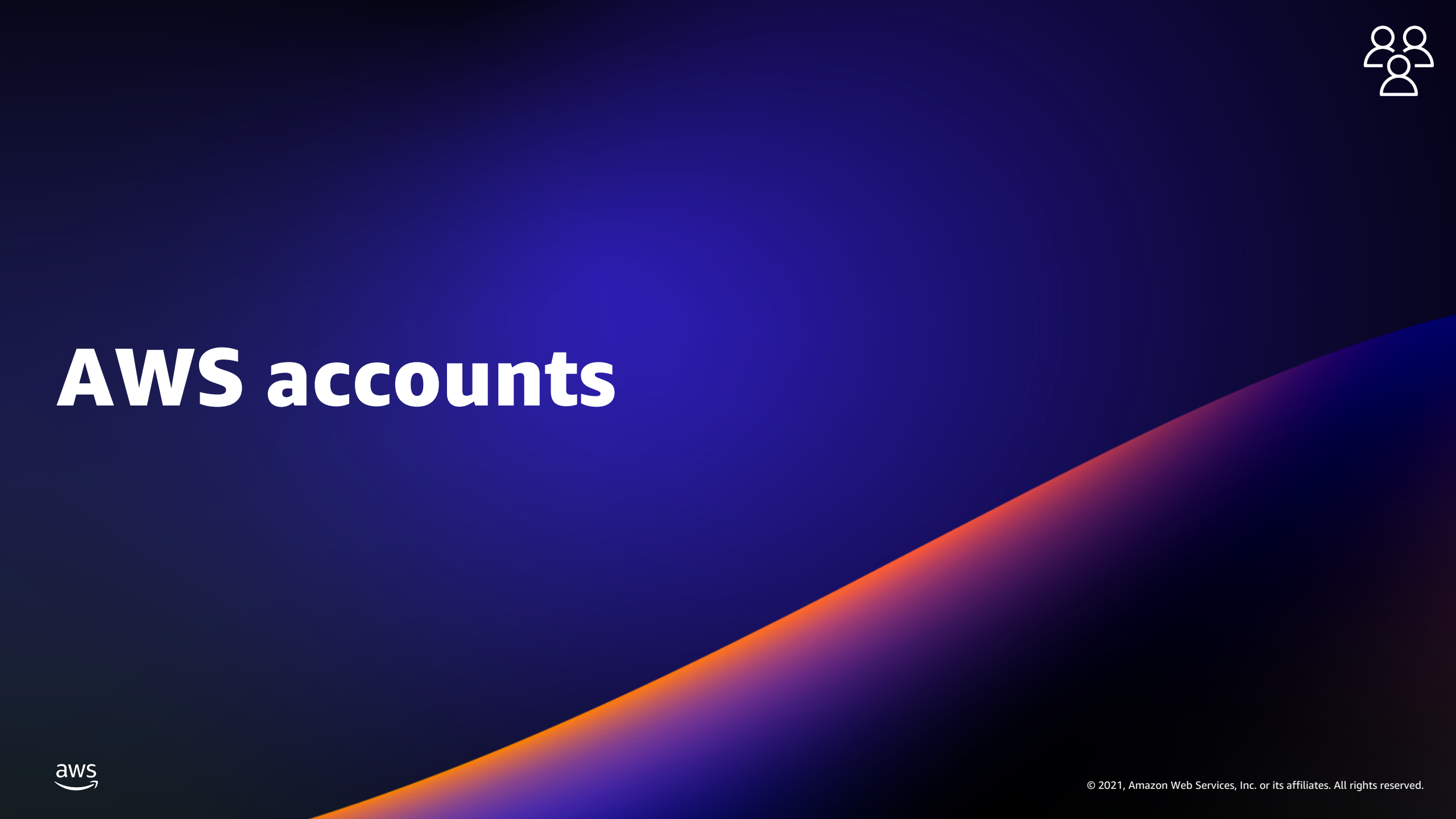
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Archive and audit APIs and metadata



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS accounts



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

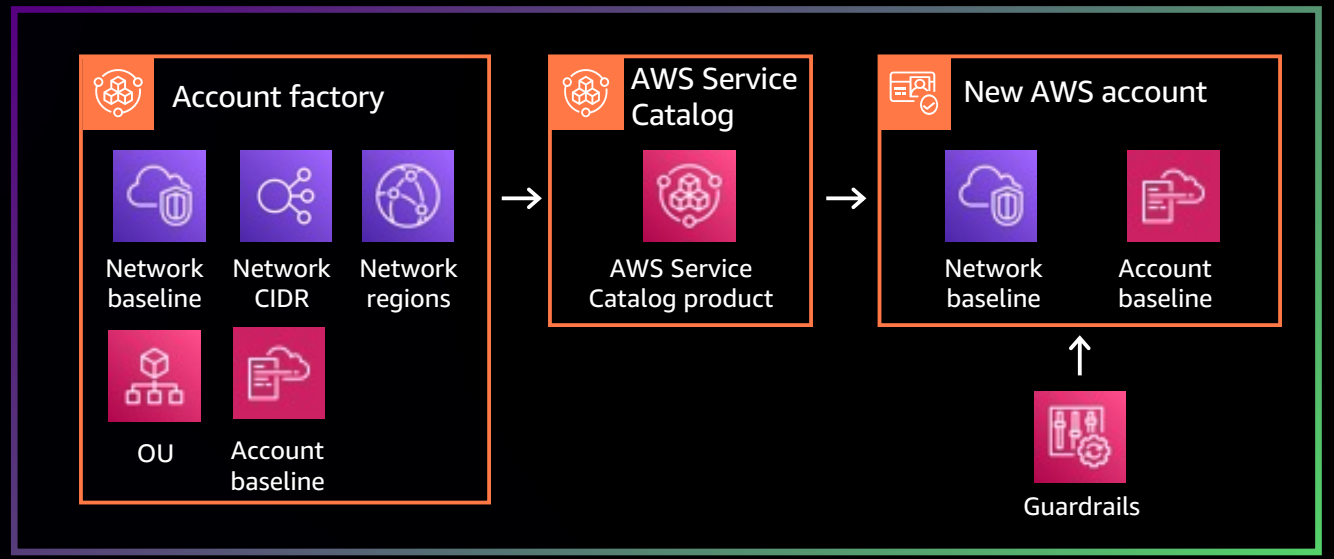
Account governance

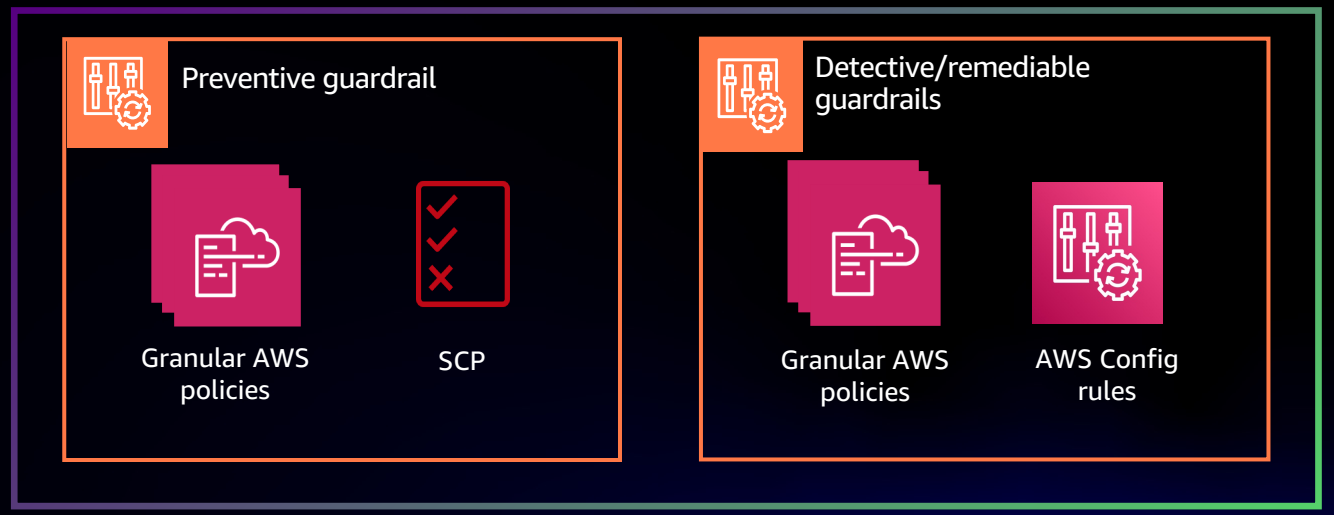
AWS CONTROL TOWER

Automated account provisioning with guardrails

Preventive and detective guardrails

Visibility into guardrail compliance across accounts





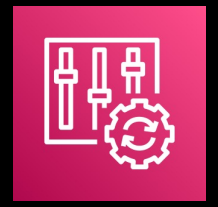
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Areas where you can scale

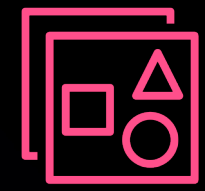
Log everything – API, OS, network, application



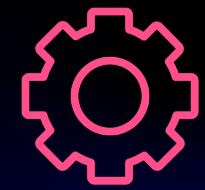
Audit and adjust controls



Multi-account strategy

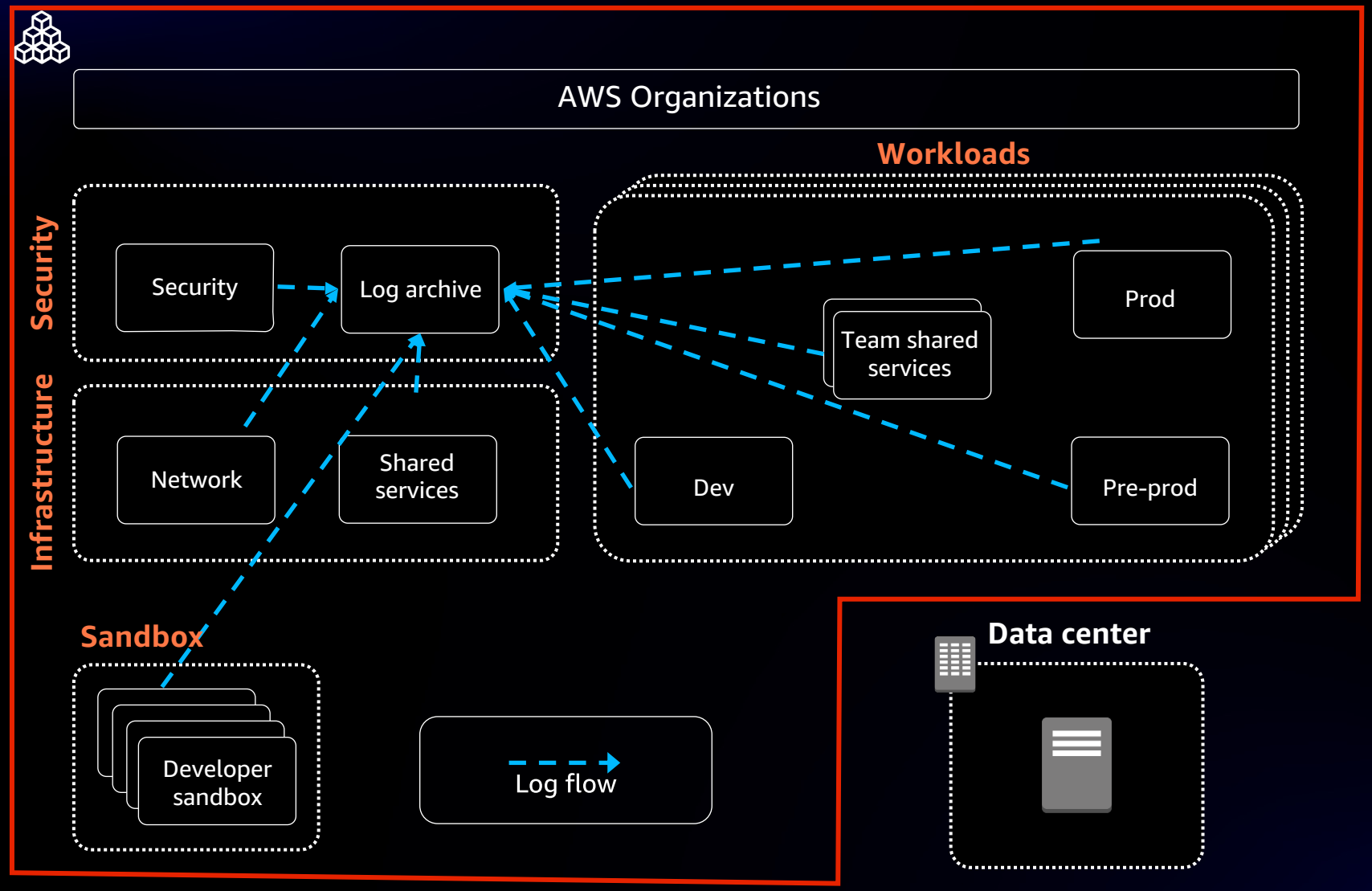


Workflow automation



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-account approach // security log flow



Orgs: Account management

Log archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev sandbox: Experiments, learning

Dev: Development

Pre-prod: Staging

Prod: Production

Team SS: Team shared services, data lake

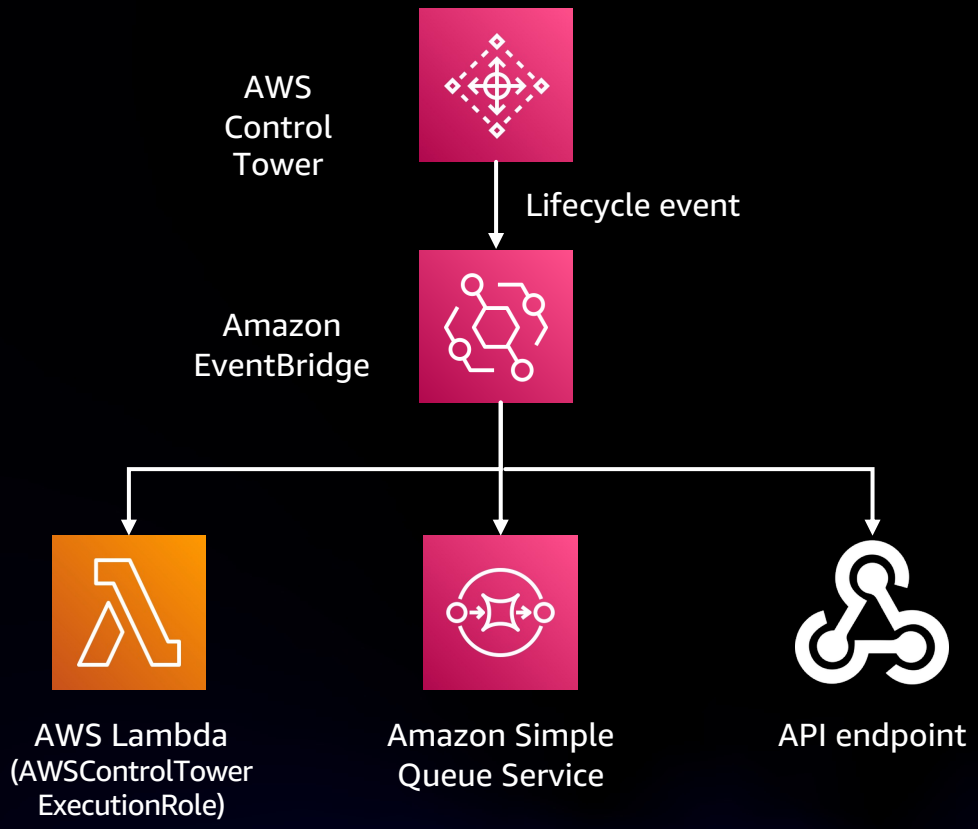
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workflow automation

Standardized cross-account access across the organization

Deploy once, scale across member accounts

Enables account governance and customizations



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security solutions extending AWS Control Tower





































© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Network activity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

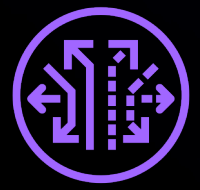
Network detection strategies



VPC Flow Logs



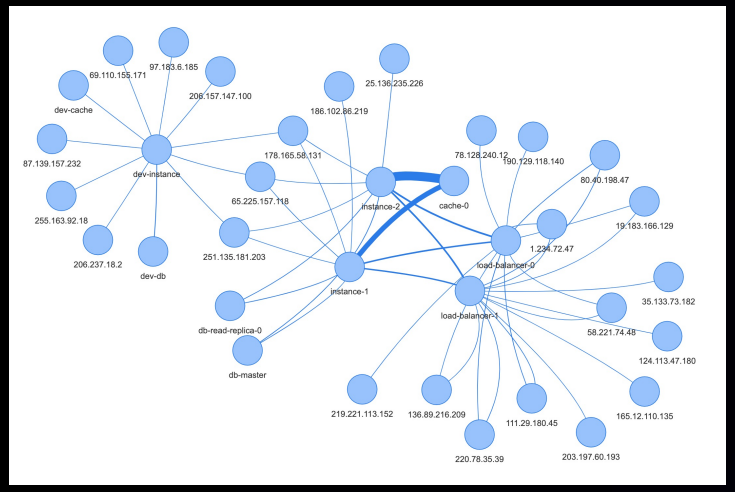
AWS Network Firewall



VPC Traffic Mirroring



AWS WAF



Point in time vs. anomaly detection

Evaluate passive vs. inline

Correlate with known bad domains, IP addresses, disallowed Regions

Application-dependent

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Taking action

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Taking action

API activity

Non-compliant resources

Anomaly detections

Detections from security services



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Remediations

Test your response workflow

Automate as much as possible

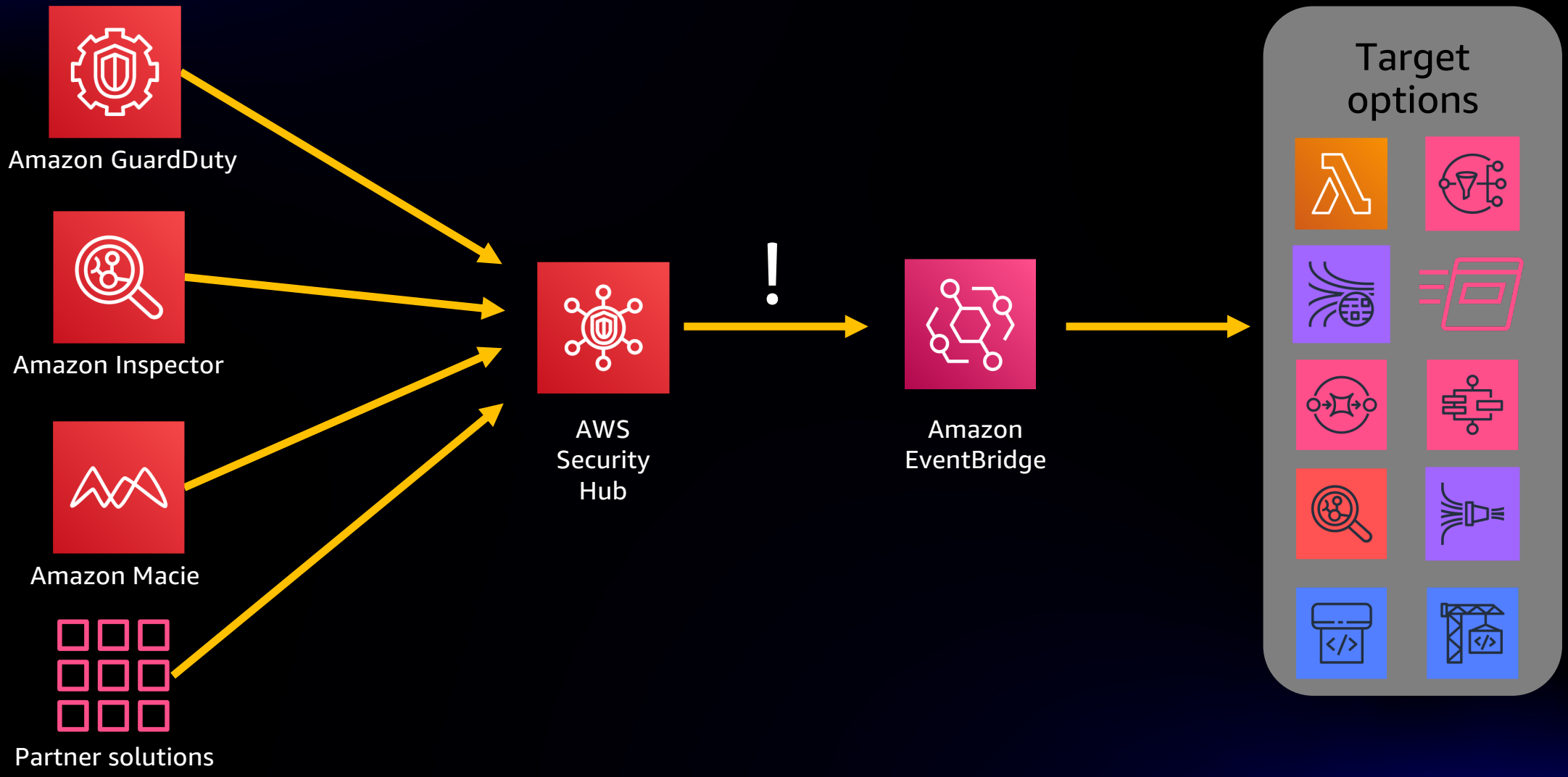
Classify risk, data, users

Context-rich data



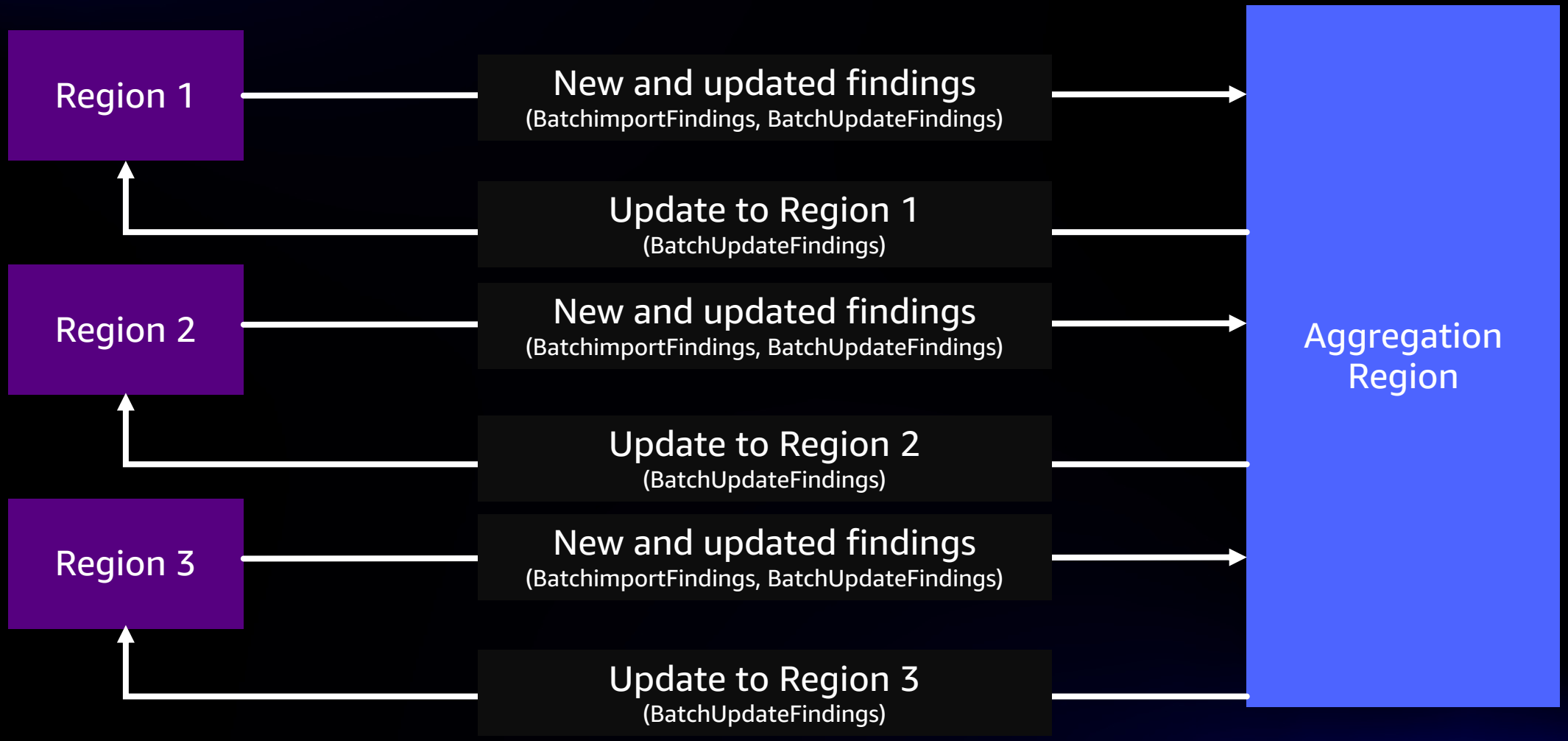
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Taking action with AWS Security Hub



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cross-Region aggregation



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where now?

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Summary

Identity

Security at scale

AWS services

Taking action



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS security partners

Network and infrastructure security



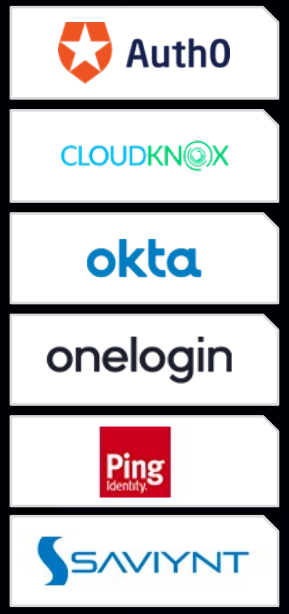
Host and endpoint security



Application security



Identity and access control



Vulnerability and configuration analysis



Data protection and encryption



Logging, monitoring, SIEM, threat detection, and analytics



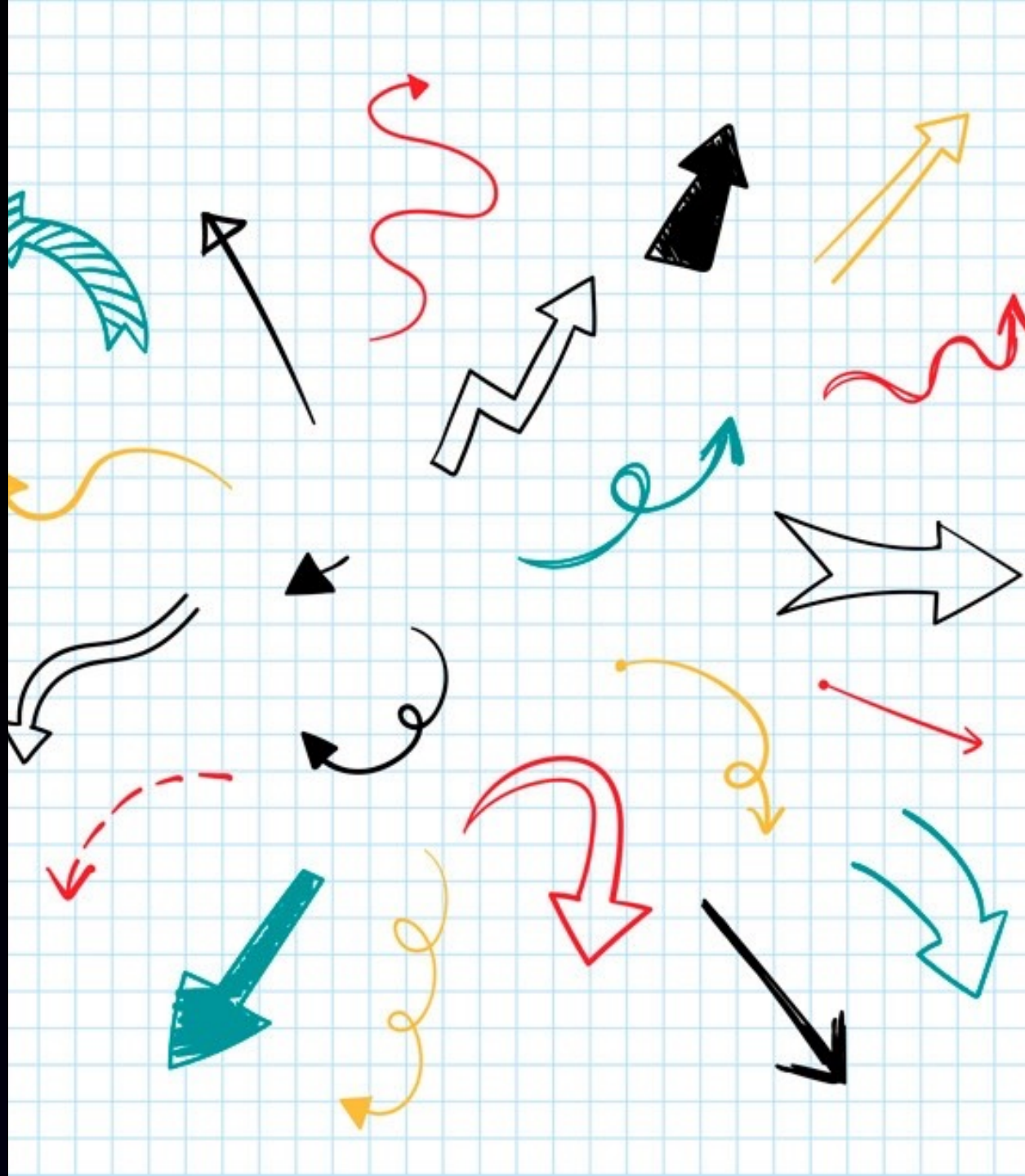
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where to find help

APN Portal

Partner solutions architects

AWS security services, AWS Partner and security partner booths



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Sameer Kumar Vasanthapuram

samvas@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.