
AWS
re:Invent

MGT304

Configuration, compliance, and audit at scale

Archana Sridhar
Sr. Product Manager
AWS

Matt Gravlin
Principal Software Engineer
Intuit

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Challenges around configuration, compliance and audit at scale

AWS services and capabilities that support use cases

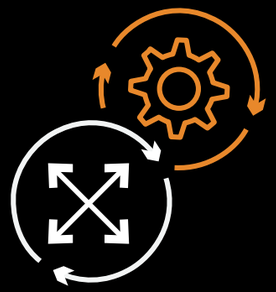
How Intuit did it

More features for at-scale usage



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

More innovation, greater agility, with control



Agility

Experiment

Be productive

Empower distributed team

Don’t choose between agility **or** control

Customers want both



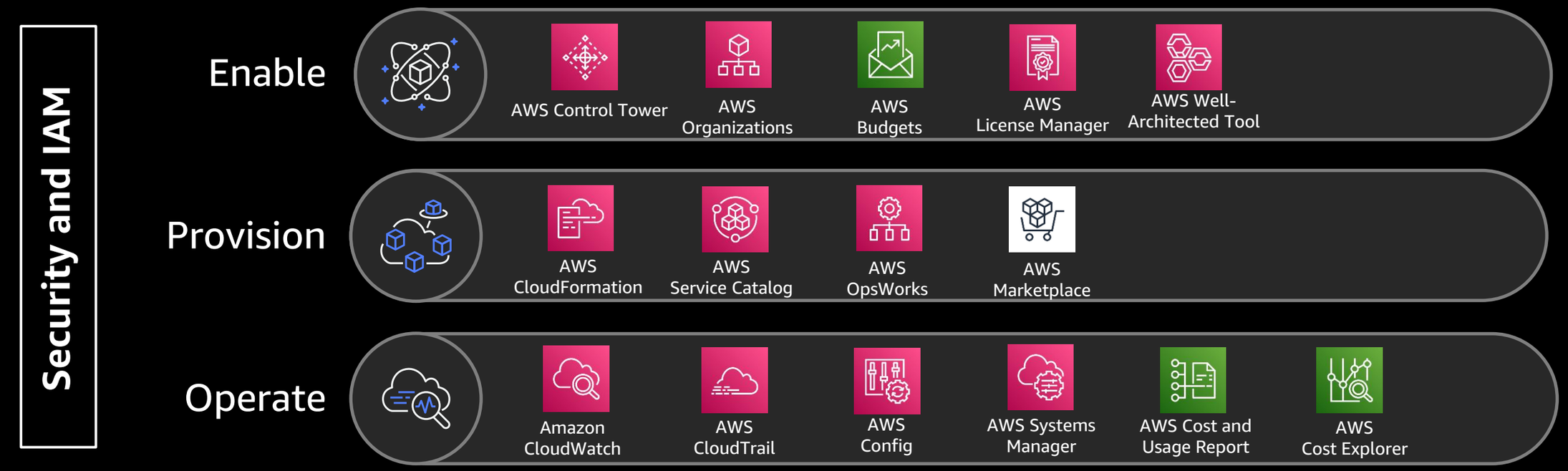
Governance

Enable

Provision

Operate

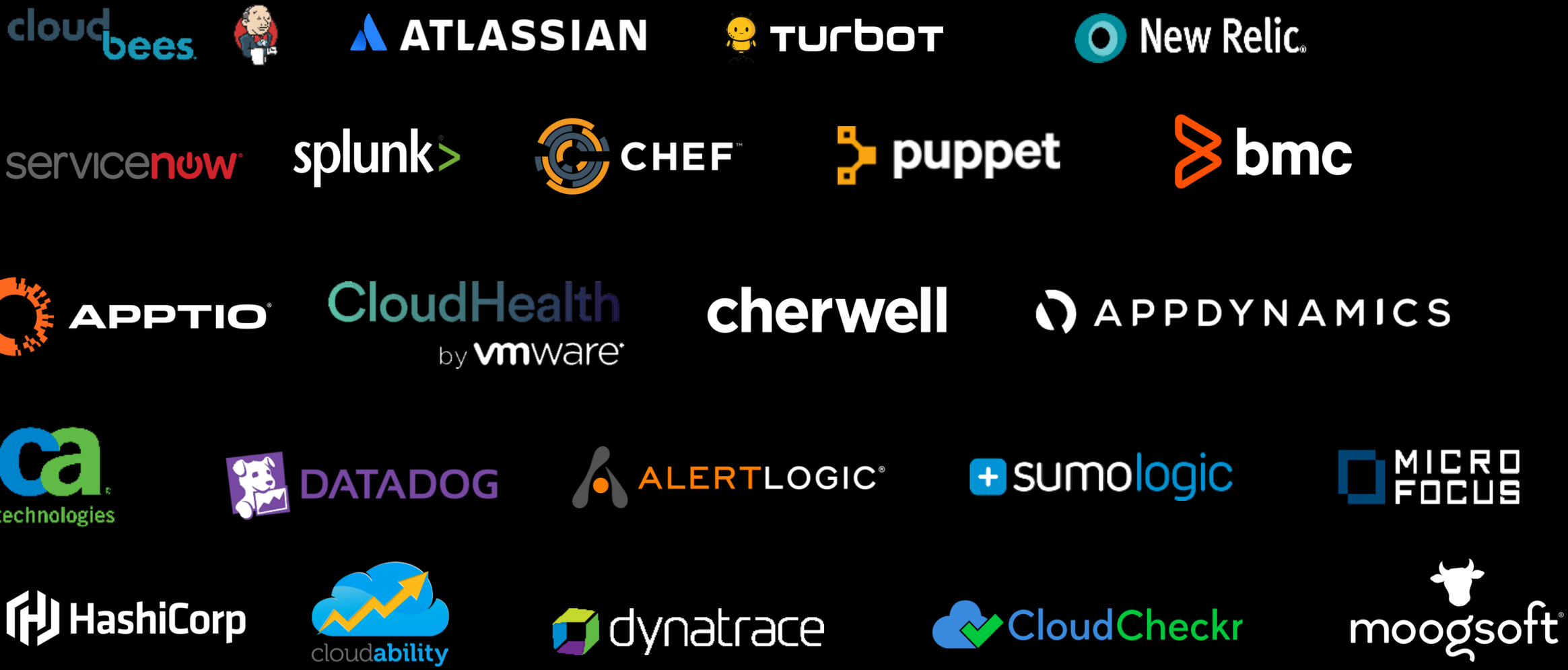
AWS management and governance services



Agility and Control

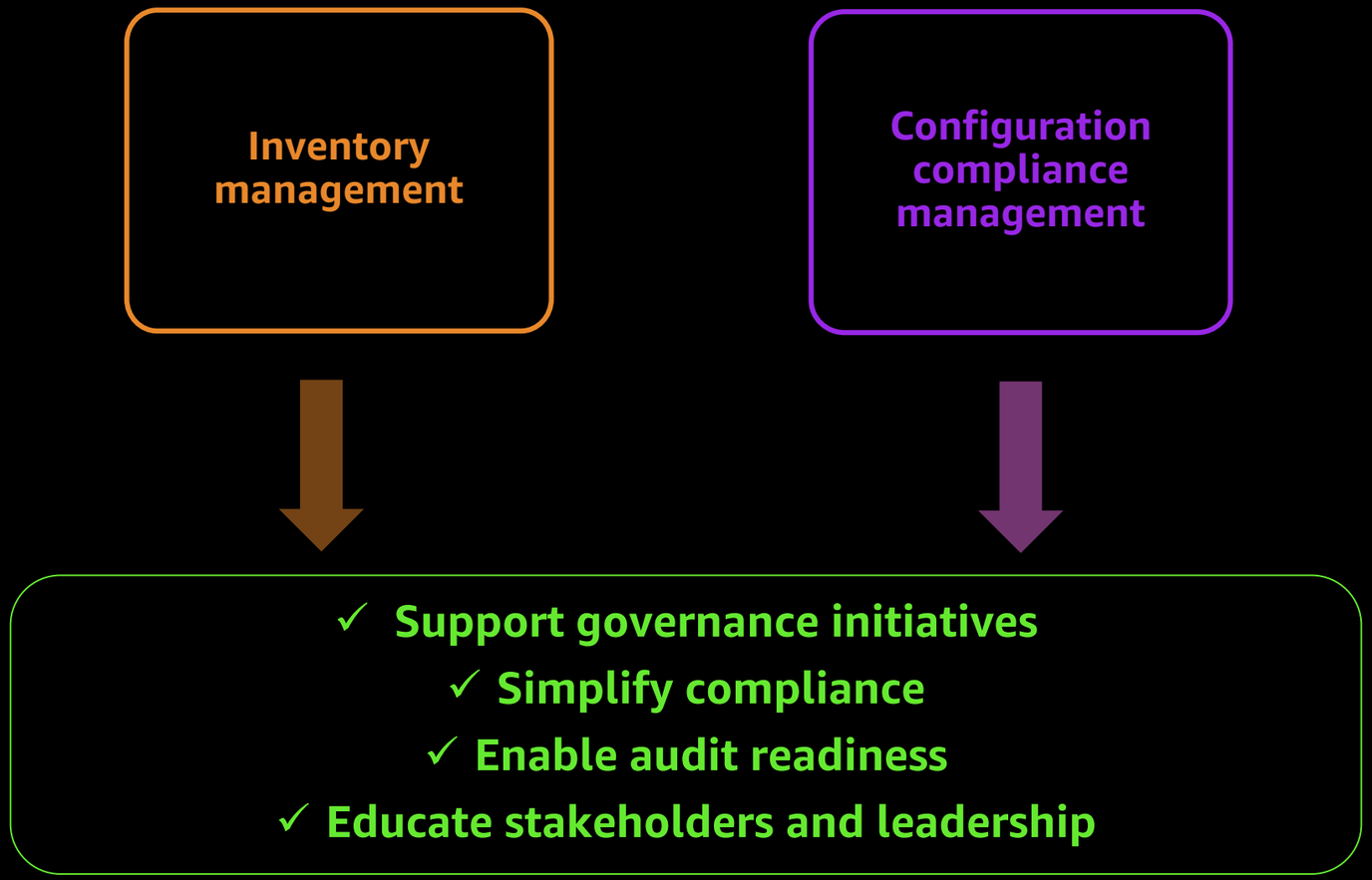
Automation

Extensive technology partner ecosystem



The logos on this slide are not meant to be comprehensive, this is just a sampling of AWS Partners that offer management and governance solutions.

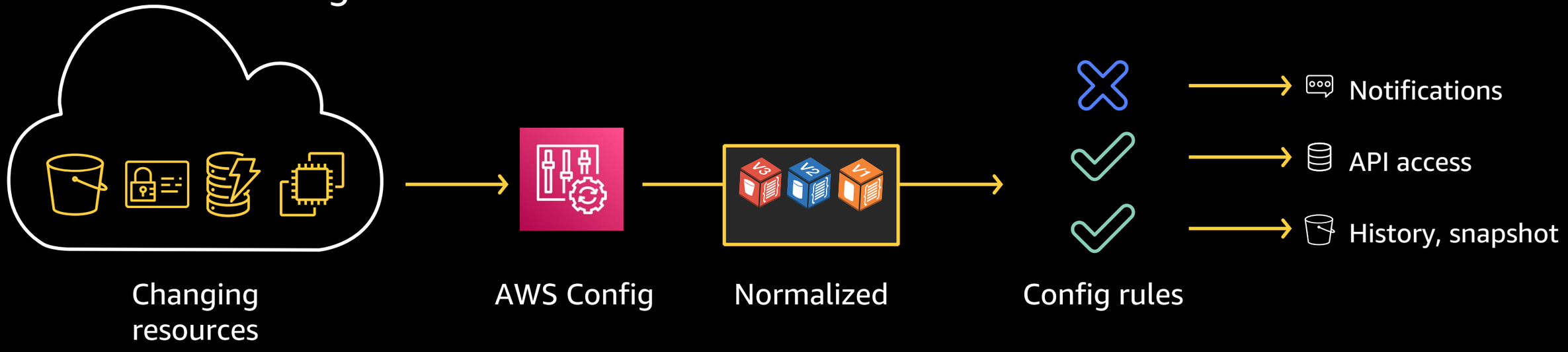
Configuration and compliance at scale



AWS Config

CONTINUOUS CONFIGURATION AUDITOR

- Continuous recording and continuous assessment service
- Tracks configuration changes to AWS resources
- Alerts you if the configuration is non-compliant with your policies
- Automated remediation of non-compliant resources
- Control and manage custom resources





INTUIT powering prosperity

turbotax quickbooks proconnect mint

Who we serve:

Consumers
Small businesses
Self-employed

Intuit’s transition to AWS changed how we look at compliance and audits



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From / To

From Datacenters	To Cloud
Smaller scale	Larger scale
Scripted, ad-hoc checks	Continuous compliance
Centralized team who owned all infrastructure	Decentralized teams who own their own infrastructure

Problem statement

What



- >10 frameworks (PCI, NIST, etc.)
- Millions of resources
- AWS and non-AWS resources

How



- Normalized controls
- Automation
- Common format

Process

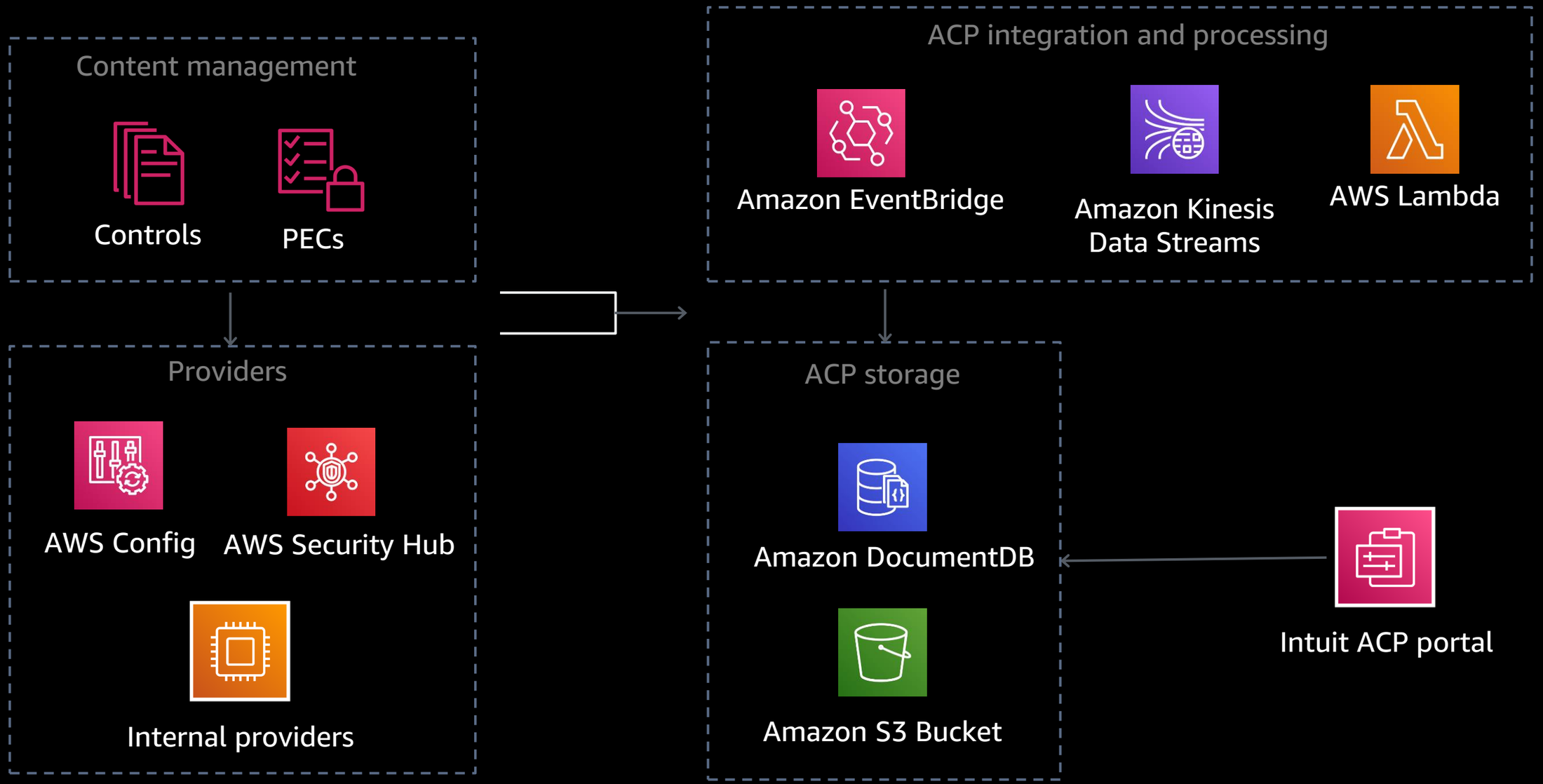


- Security awareness
- Team effort
- Build trust

Business outcomes

1. Demonstrate continuous compliance and be audit ready at all times
2. Effectively manage remediation
3. Auditors brought along the journey and implicitly trust the evidence

Automated Compliance Platform (ACP)



intuit

ACP’s use of AWS Config

- Half of our checks are from AWS Config rules
  - AWS Security Hub
  - Custom and managed Config rules
    - Custom integration using AWS Config aggregators
- Maintain state via AWS Config change events and CloudTrail

Result

- Transparent security posture
- Reduced audit fatigue by being prepared
- Reduced security vulnerabilities and risks
- Evidence used in audits
- Hundreds of checks sending >20 million results per day

Lessons learned / Call to action

- Audit fatigue has more to do with audit preparation than evidence collection
- There is no universal definition of acceptable evidence
- Traditional, interview-based / random sample audits need to be modernized
- To scale audits in the cloud, standards and automation is key

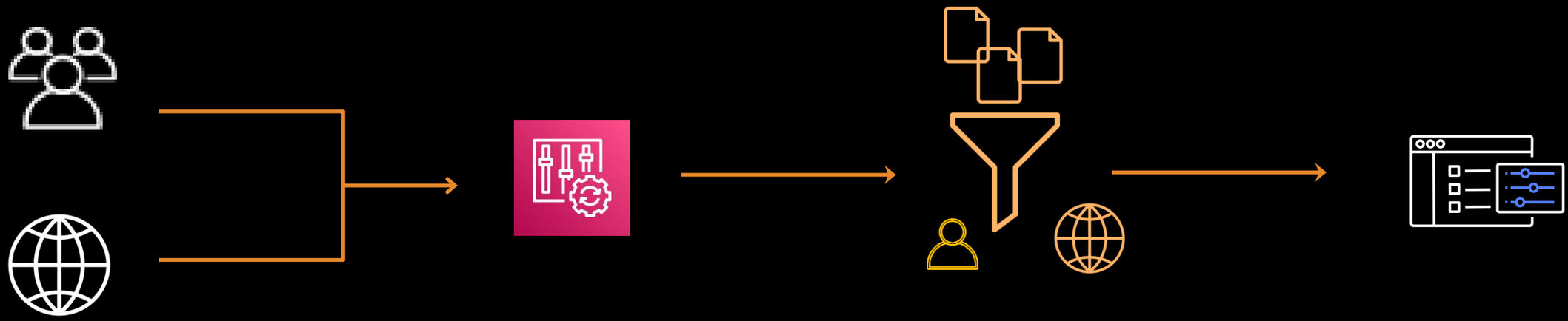
Features supporting configuration, compliance, and auditing at scale



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-account, multi-Region data aggregation



Accounts and Regions
Select the source accounts and Regions from where you want to to collect AWS Config data

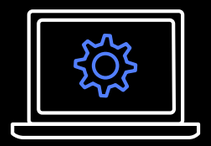
AWS Config data
Collection of AWS Config data from multiple source accounts and Regions

Aggregator
Contains the resource configuration information and the compliance data recorded in AWS Config

Aggregated view
View all compliant and non-compliant rules and resources for each aggregator

AWS Config features for configuration and compliance management at scale

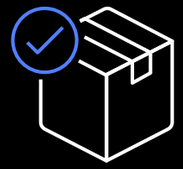
Advanced queries



Configuration attribute based queries against current state metadata

>50 sample queries available

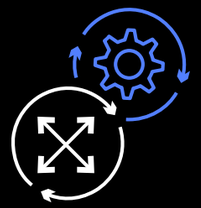
Conformance packs



Simplifies organization-wide deployment and reporting of compliance

>50 sample templates available to get started

Automatic remediation with Config rules



Enables you to automatically remediate noncompliant resources

>170 managed rules (and growing) + create custom rules

Demo: AWS Config features for configuration and compliance at scale



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.