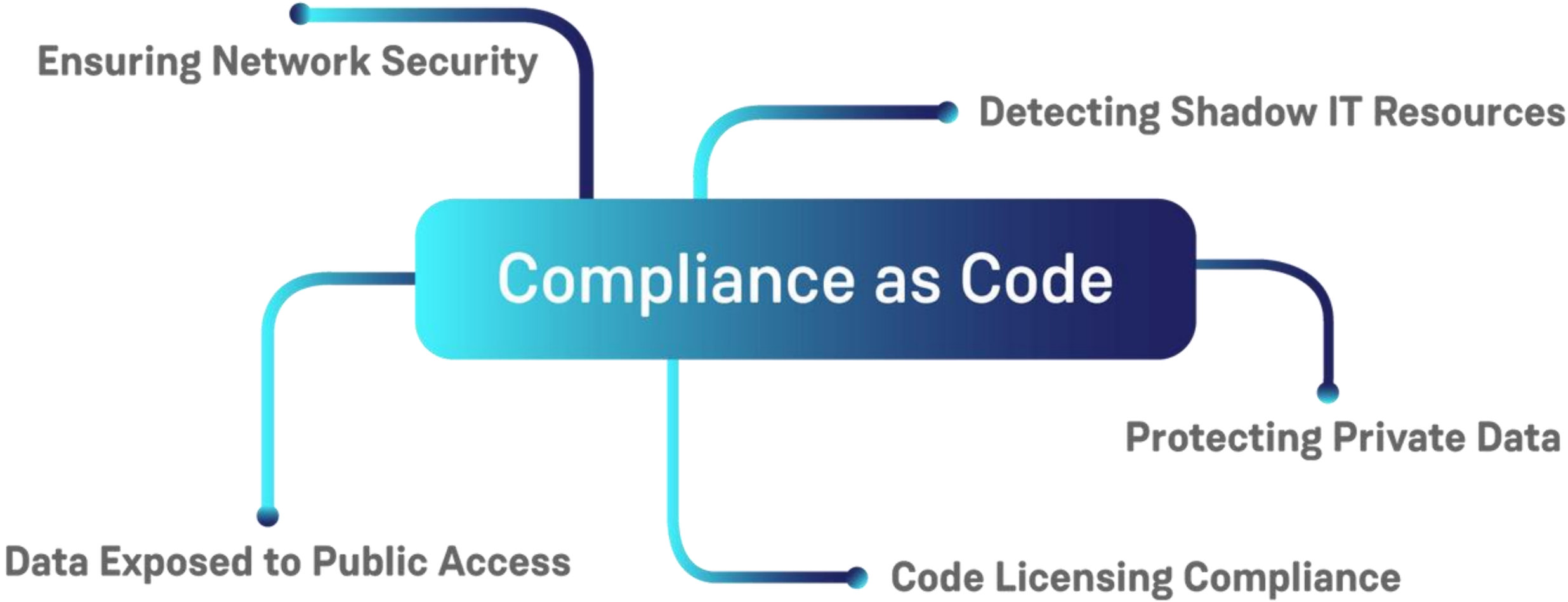
AWS Config & RDK

Assess, audit, and evaluate configurations of your resources

Rajesh Kumar

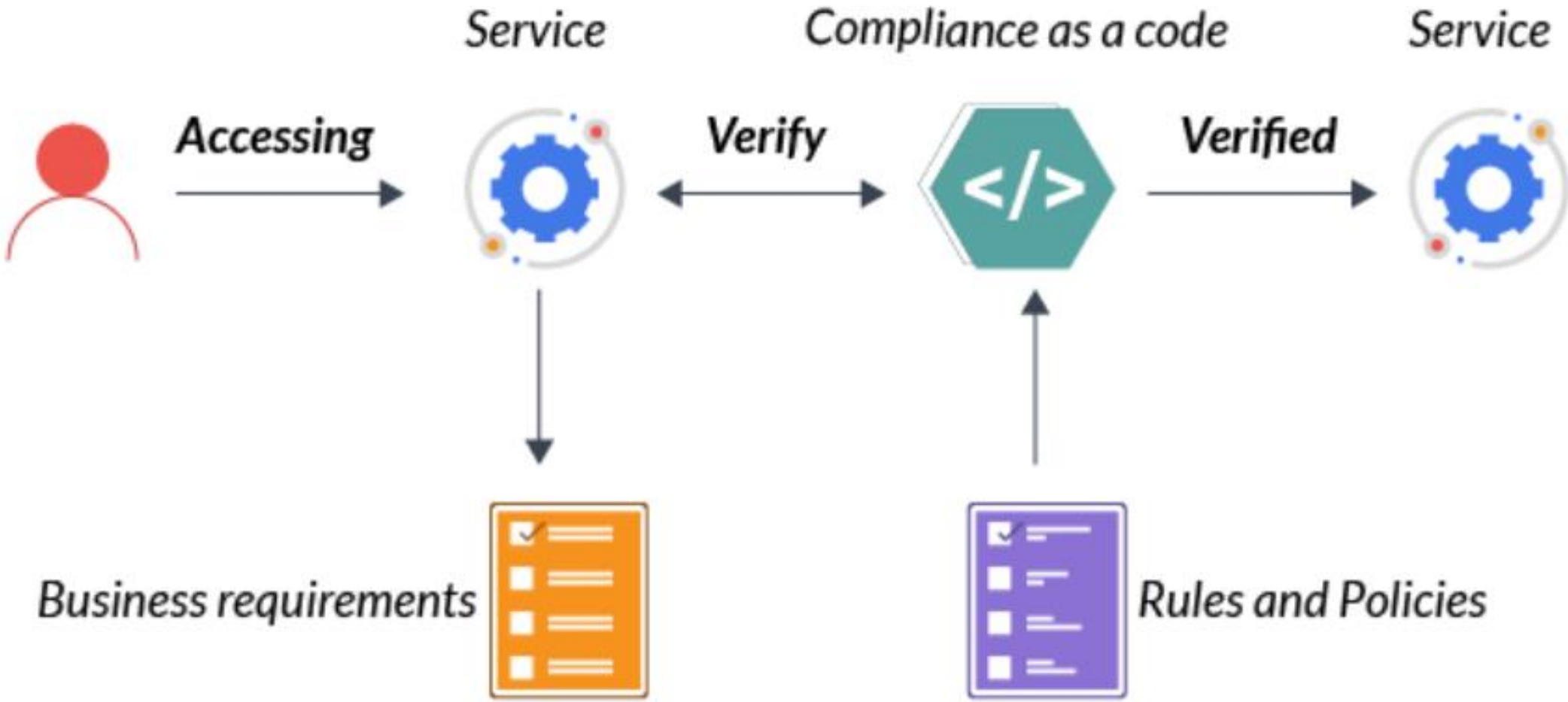
DevOps@RajeshKumar.xyz

www.RajeshKumar.xyz

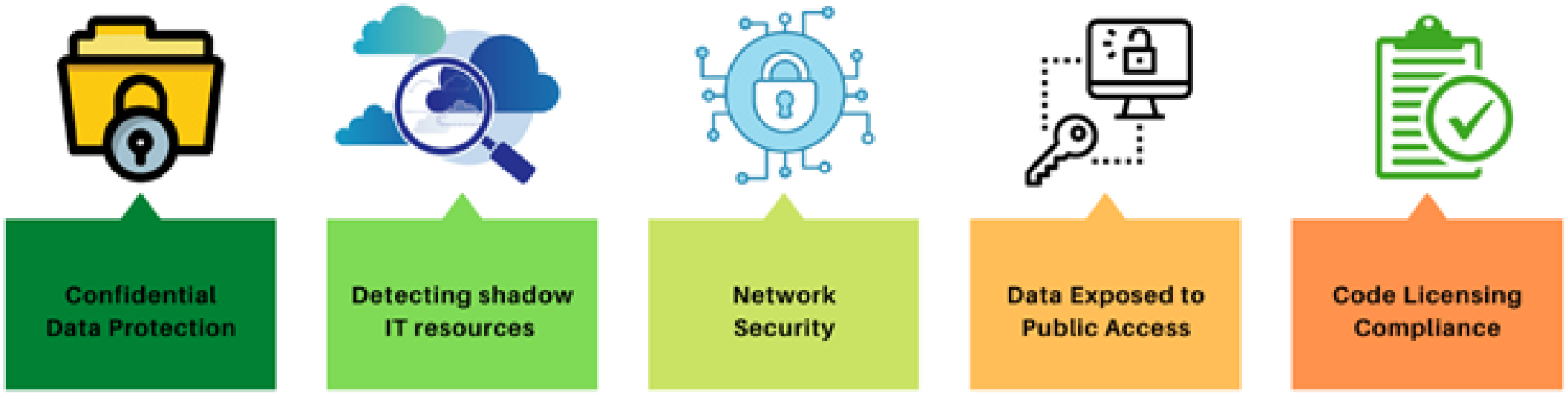

Ensuring Network Security
Detecting Shadow IT Resources
Compliance as Code
Protecting Private Data
Data Exposed to Public Access
Code Licensing Compliance

Working of Compliance as a code

XENONSTACK



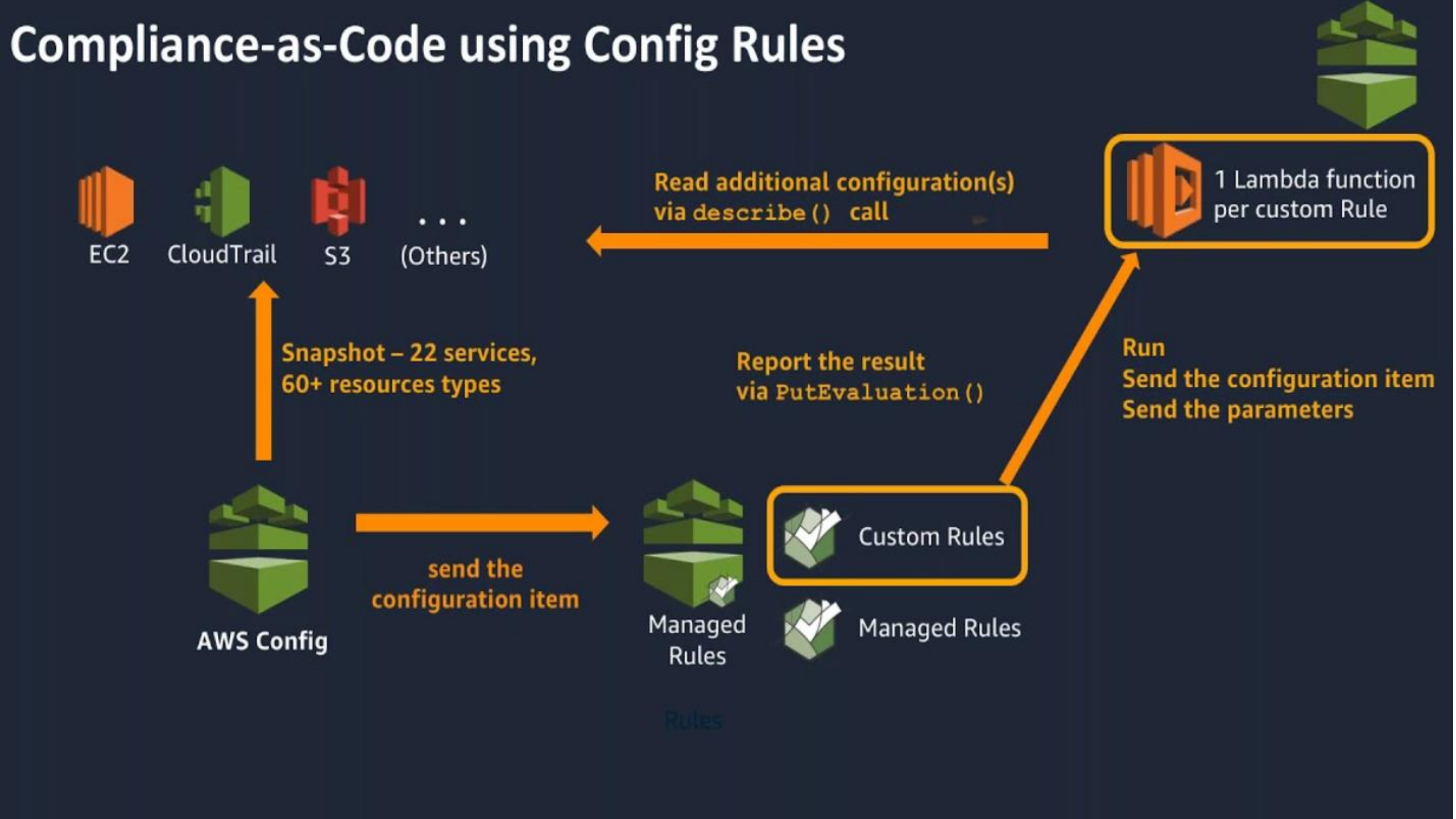
Use cases of Compliance as a code



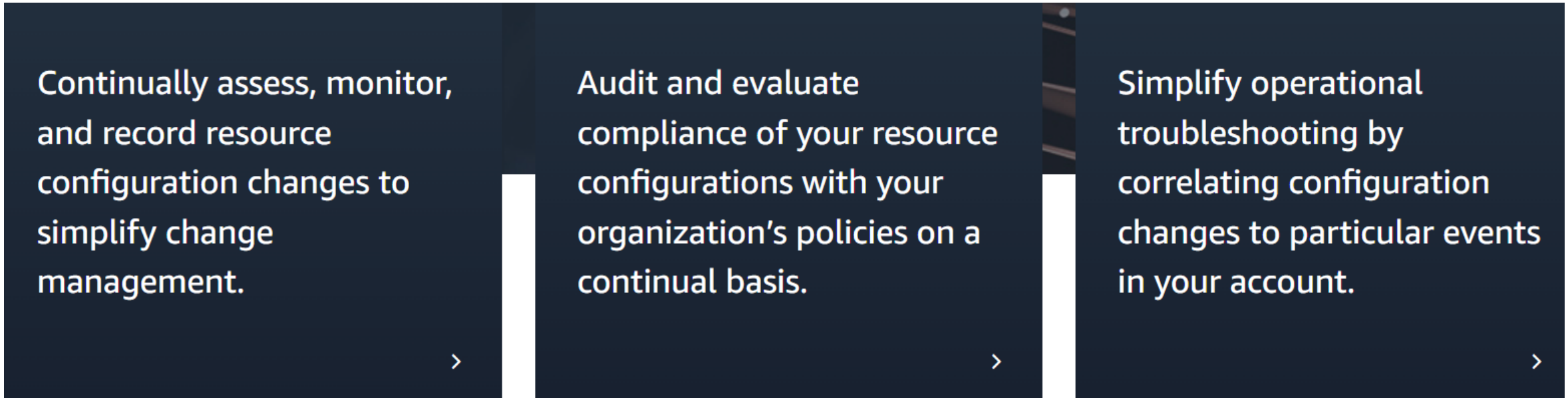
AWS Config
Compliance as a Code

Create rules in AWS Config
Evaluate AWS resources
Enforce compliance

Compliance-as-Code using Config Rules



Use of AWS Config



AWS Config: Benefits

Continuous monitoring

With AWS Config, you are able to continuously monitor and record configuration changes of your AWS resources.

Continuous assessment

AWS Config allows you to continuously audit and assess the overall compliance of your AWS resource configurations with your organization's policies and guidelines.

Change management

With AWS Config, you are able to track the relationships among resources and review resource dependencies prior to making changes.

Operational troubleshooting

With AWS Config, you can capture a comprehensive history of your AWS resource configuration changes to simplify troubleshooting of your operational issues.

AWS Config: Use Cases

Streamline operational troubleshooting and change management

Discover resources that exist in your account or publish the configuration data of third-party resources into AWS Config, record their configurations, and capture any changes to quickly troubleshoot operational issues.

AWS Config: Use Cases

Deploy a compliance-as-code framework

Codify your compliance requirements as AWS Config rules and author remediation actions, automating the assessment of your resource configurations across your organization.

AWS Config: Use Cases

Continually audit security monitoring and analysis

Evaluate resource configurations for potential vulnerabilities, and review your configuration history after potential incidents to examine your security posture.

AWS Config: Pricing

AWS Config

You pay $0.003 per configuration item recorded in your AWS account per AWS Region. A configuration item is recorded whenever a resource undergoes a configuration change or a relationship change. The resource could be an AWS, third-party, or custom resource. A relationship defines how a resource is related to other resources within an AWS account.

AWS Config rules

You are charged based on the number of AWS Config rule evaluations recorded. A rule evaluation is recorded every time a resource is evaluated for compliance against an AWS Config rule. Rule evaluations can be run in detective mode and/or in proactive mode, if available.

AWS Config: Pricing

AWS Config rules evaluations	Price
First 100,000 rule evaluations	$0.001 per rule evaluation per region
Next 400,000 rule evaluations (100,001-500,000)	$0.0008 per rule evaluation per region
500,001 and more rule evaluations	$0.0005 per rule evaluation per region

With consolidated billing, AWS will measure the total number of AWS Config rules evaluations from all of your accounts to determine which pricing tier applies, giving you a lower overall price at the higher tiers.

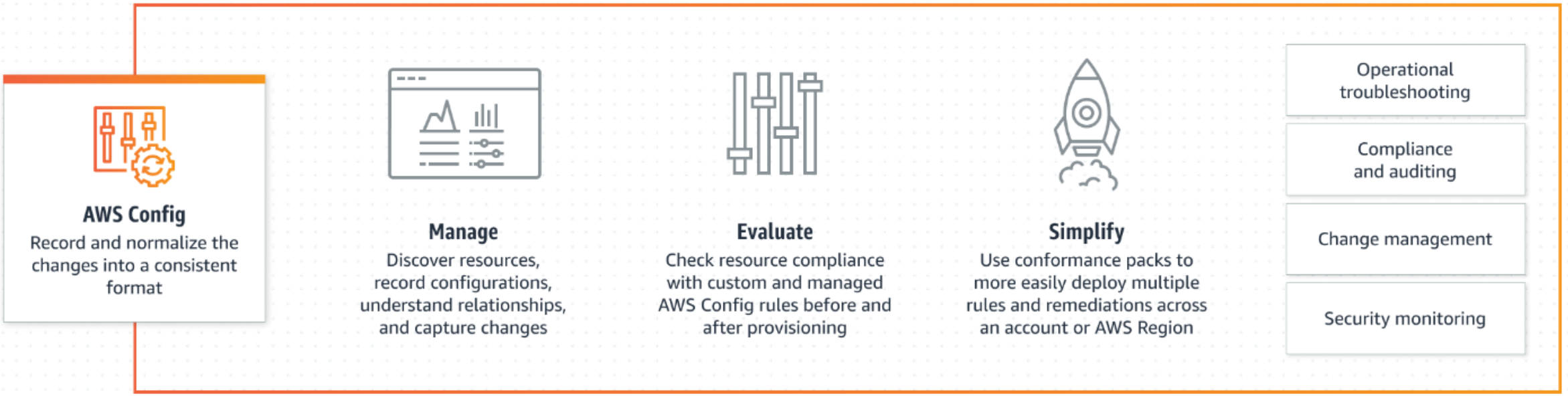
Conformance packs

You are charged per conformance pack evaluation in your AWS account per AWS Region based on the tier below. A conformance pack evaluation is defined as an evaluation of a resource by an AWS Config rule within the conformance pack. The following prices are effective as of September 14, 2022 and will be automatically reflected in your AWS bill.

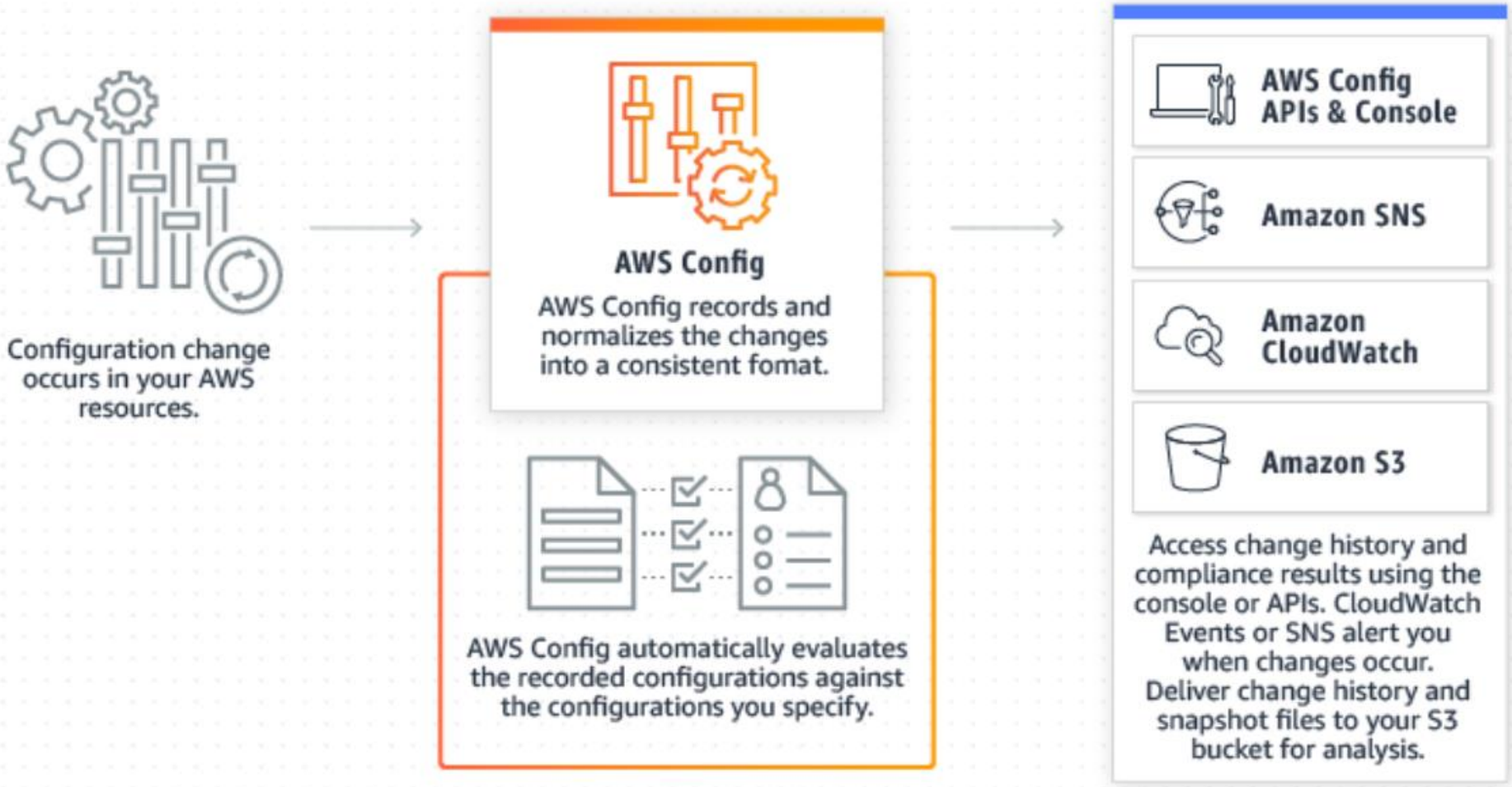
Conformance pack evaluations	Price
First 100,000 conformance pack evaluations	$0.001 per conformance pack evaluation per Region
Next 400,000 conformance pack evaluations (100,001-500,000)	$0.0008 per conformance pack evaluation per Region
500,001 and more conformance pack evaluations	$0.0005 per conformance pack evaluation per Region

AWS Config: How it works

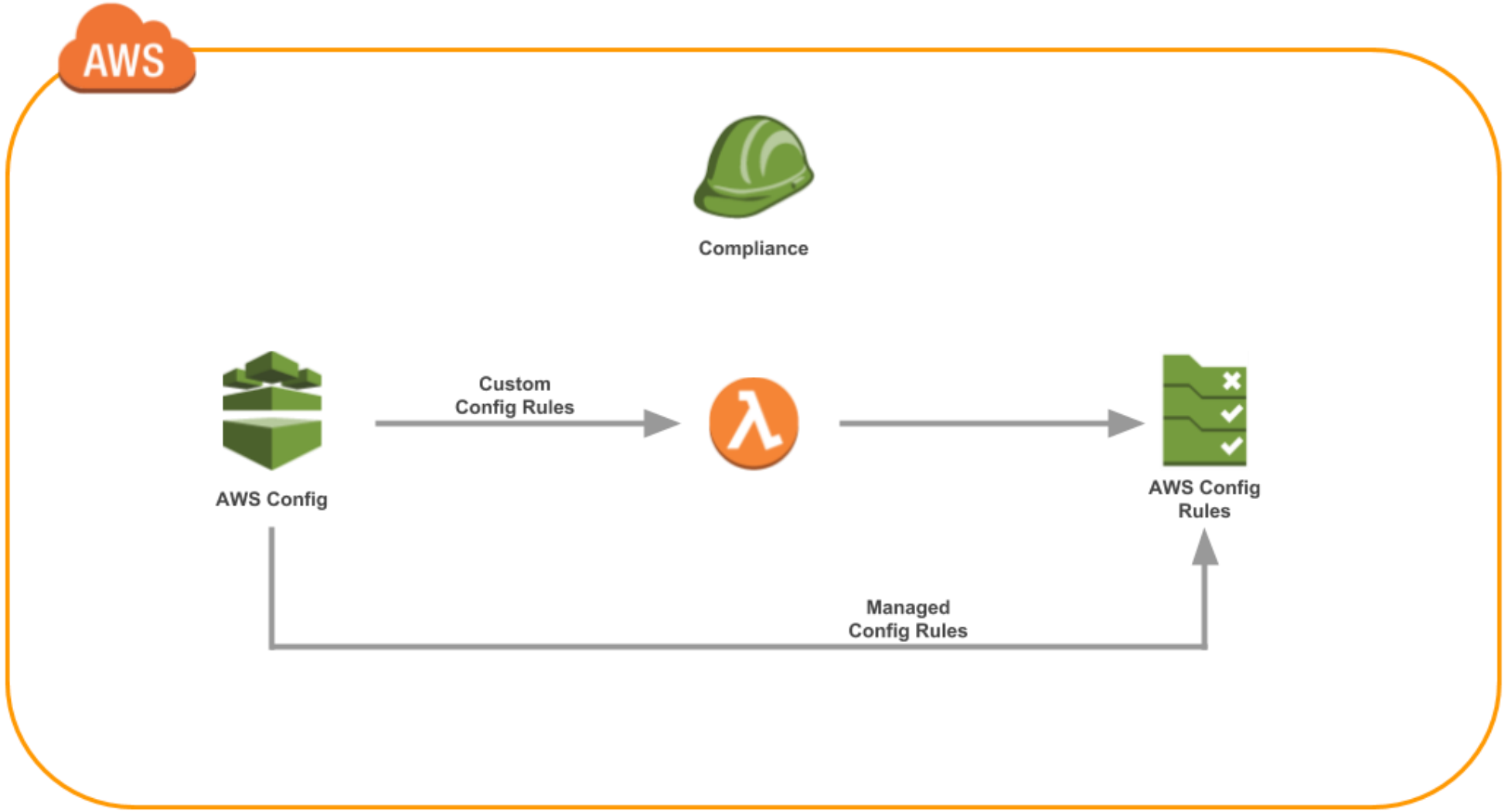
AWS Config continually assesses, audits, and evaluates the configurations and relationships of your resources on AWS, on premises, and on other clouds.



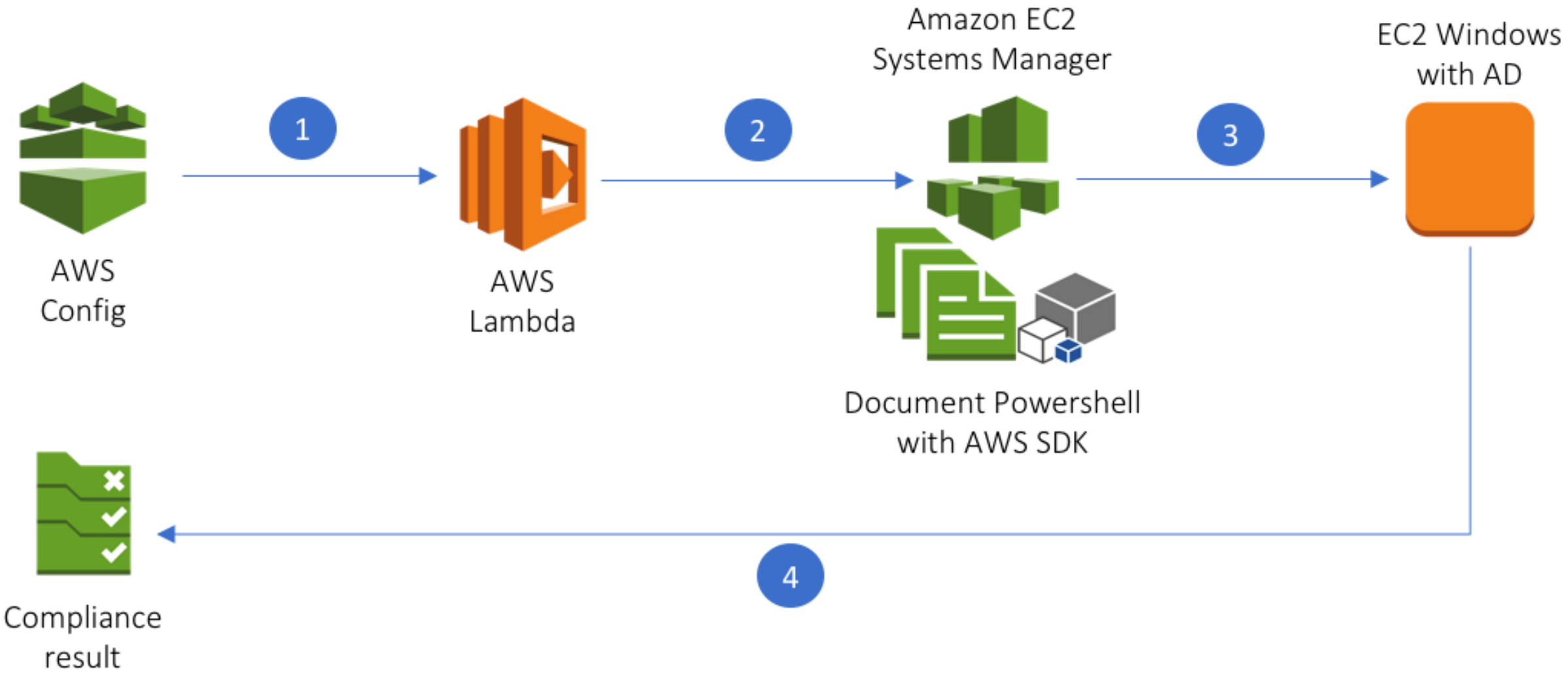
AWS Config: How it works



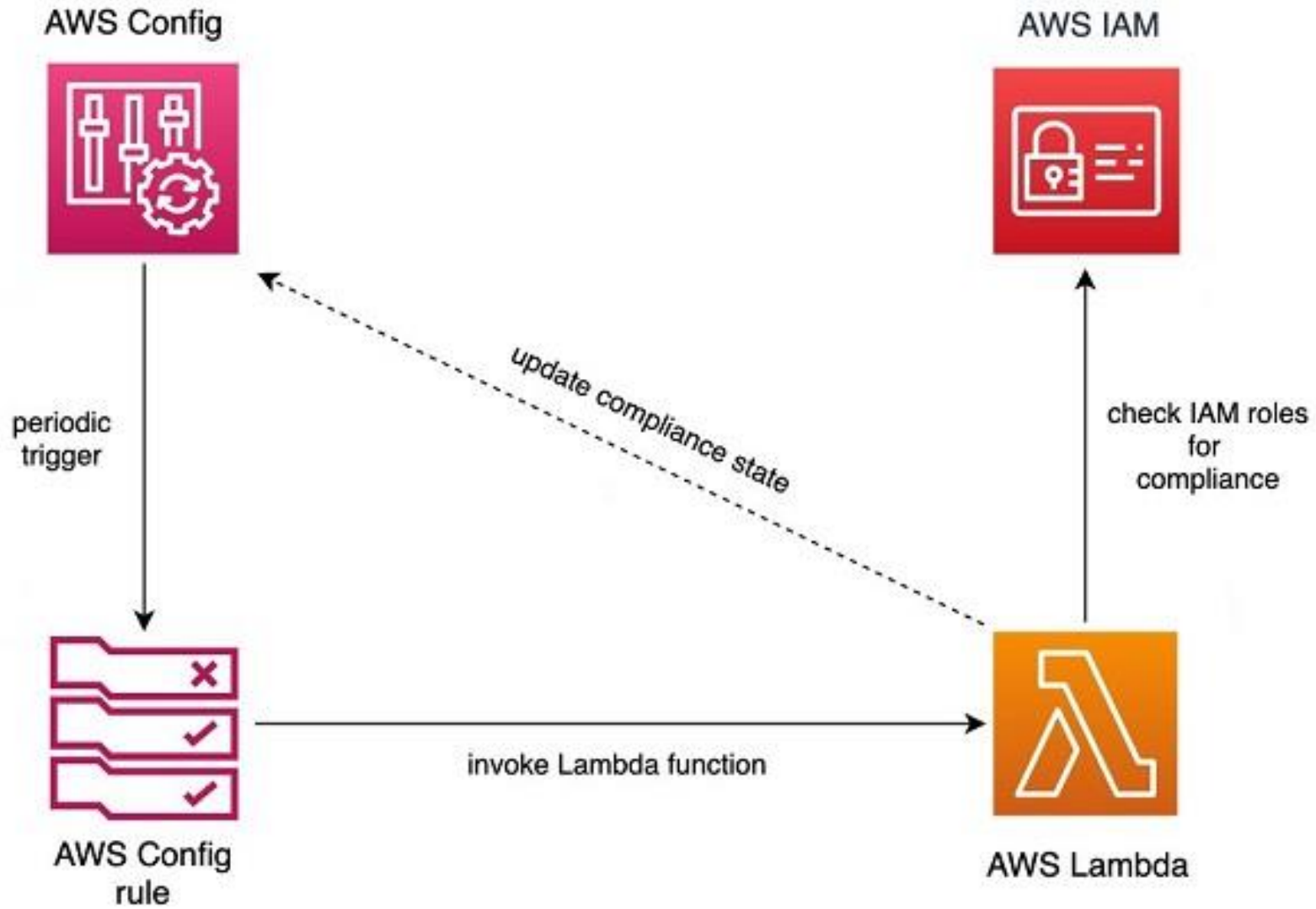
AWS Config: How it works



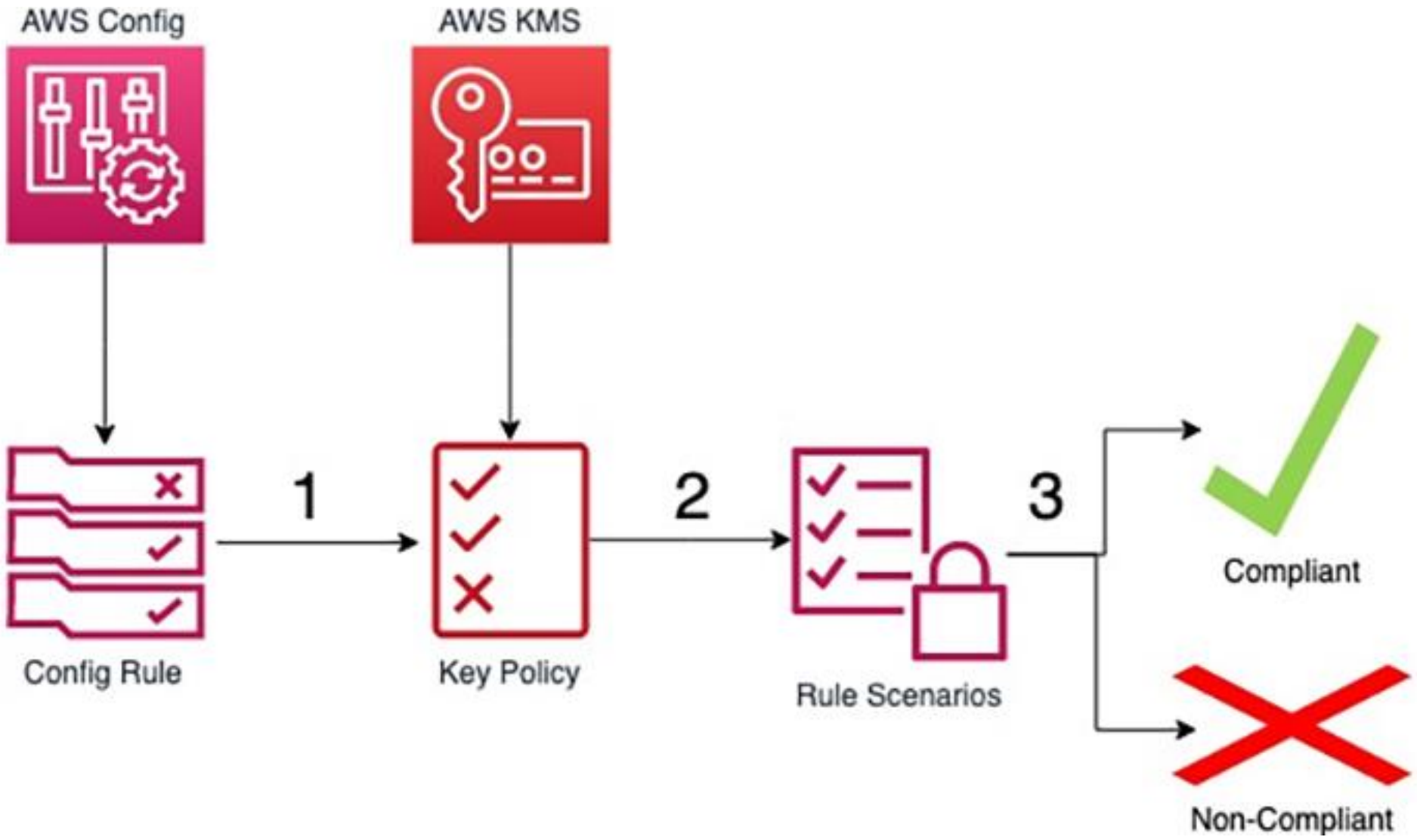
AWS Config: How it works



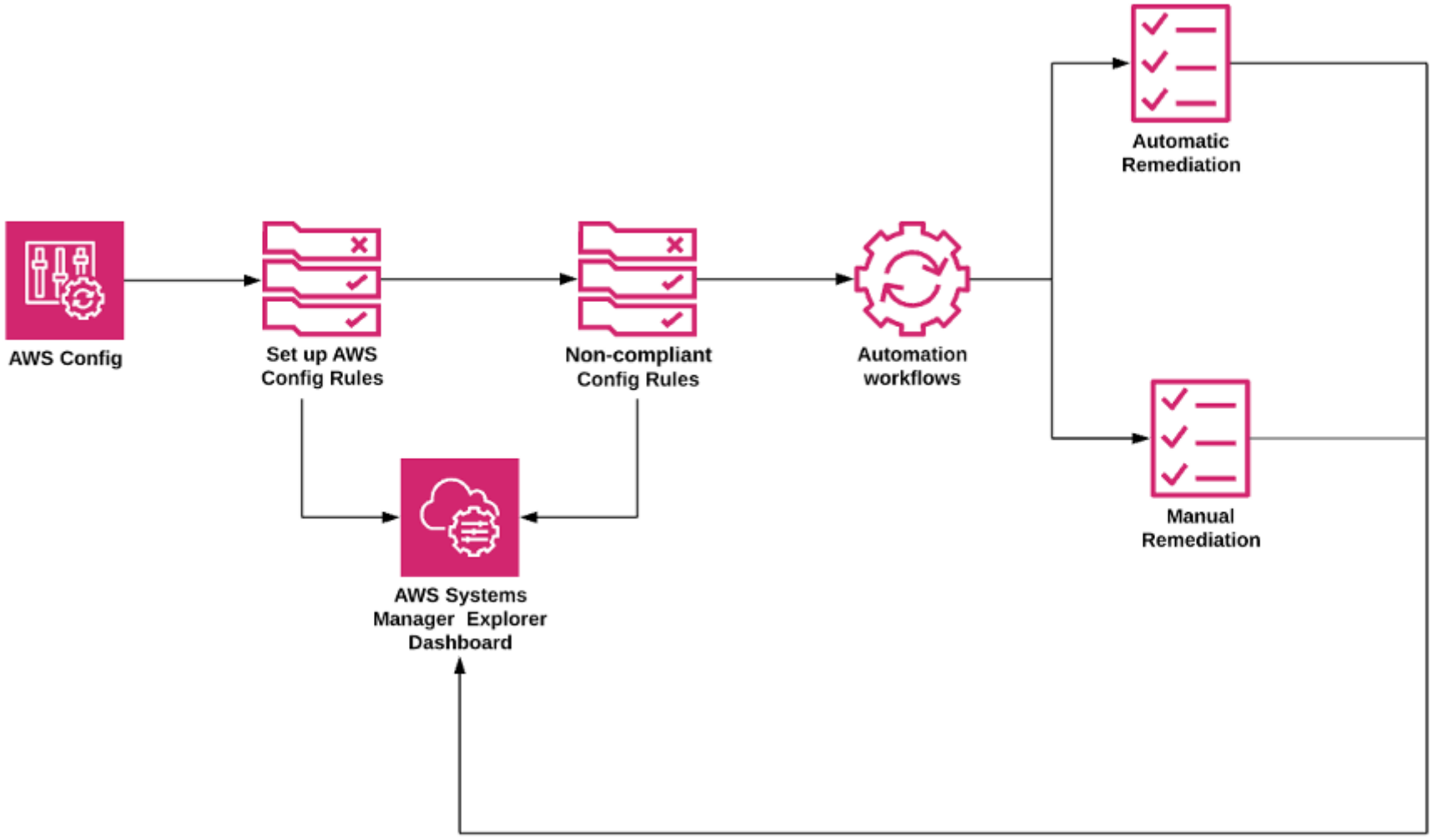
AWS Config: How it works

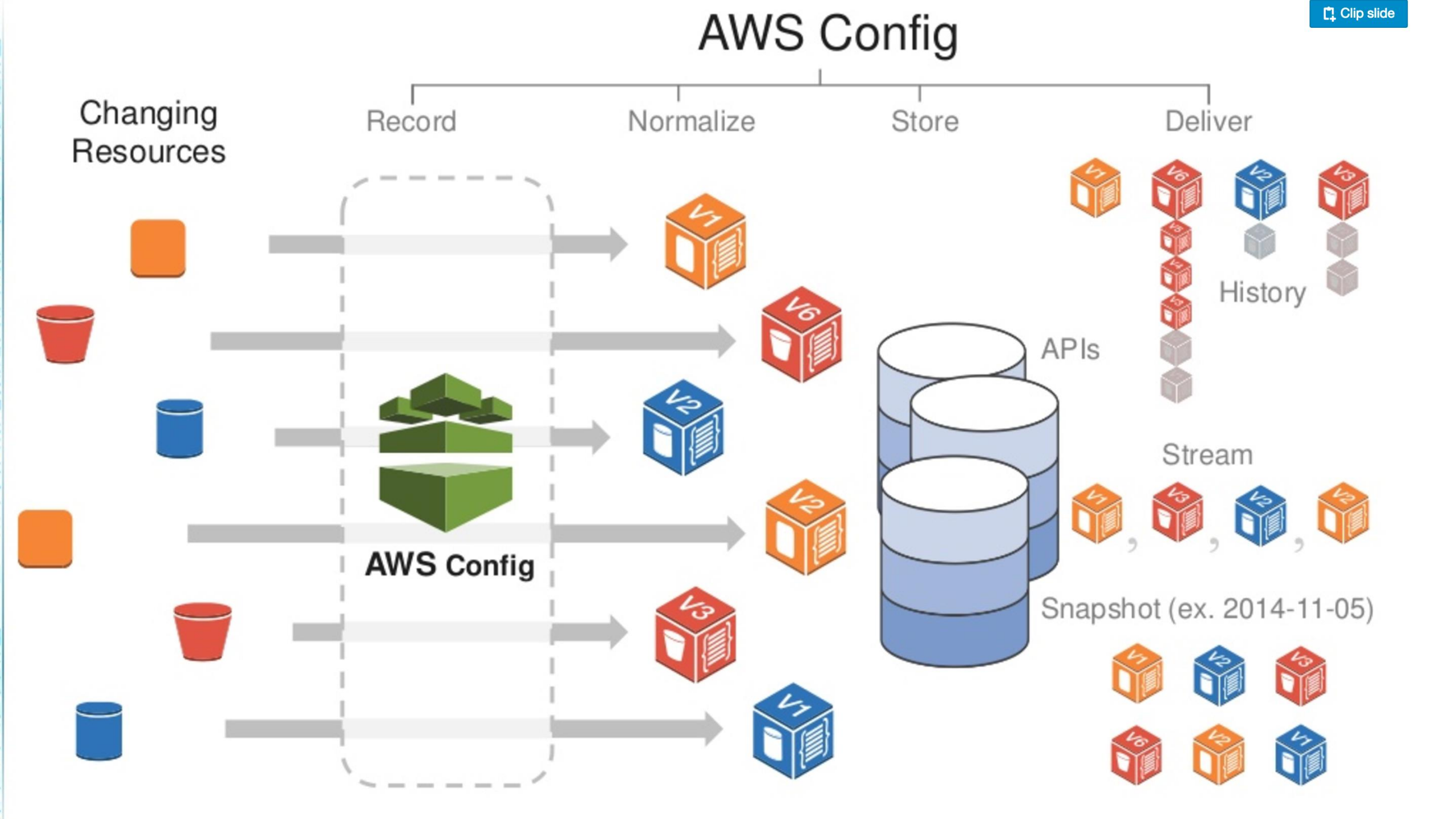


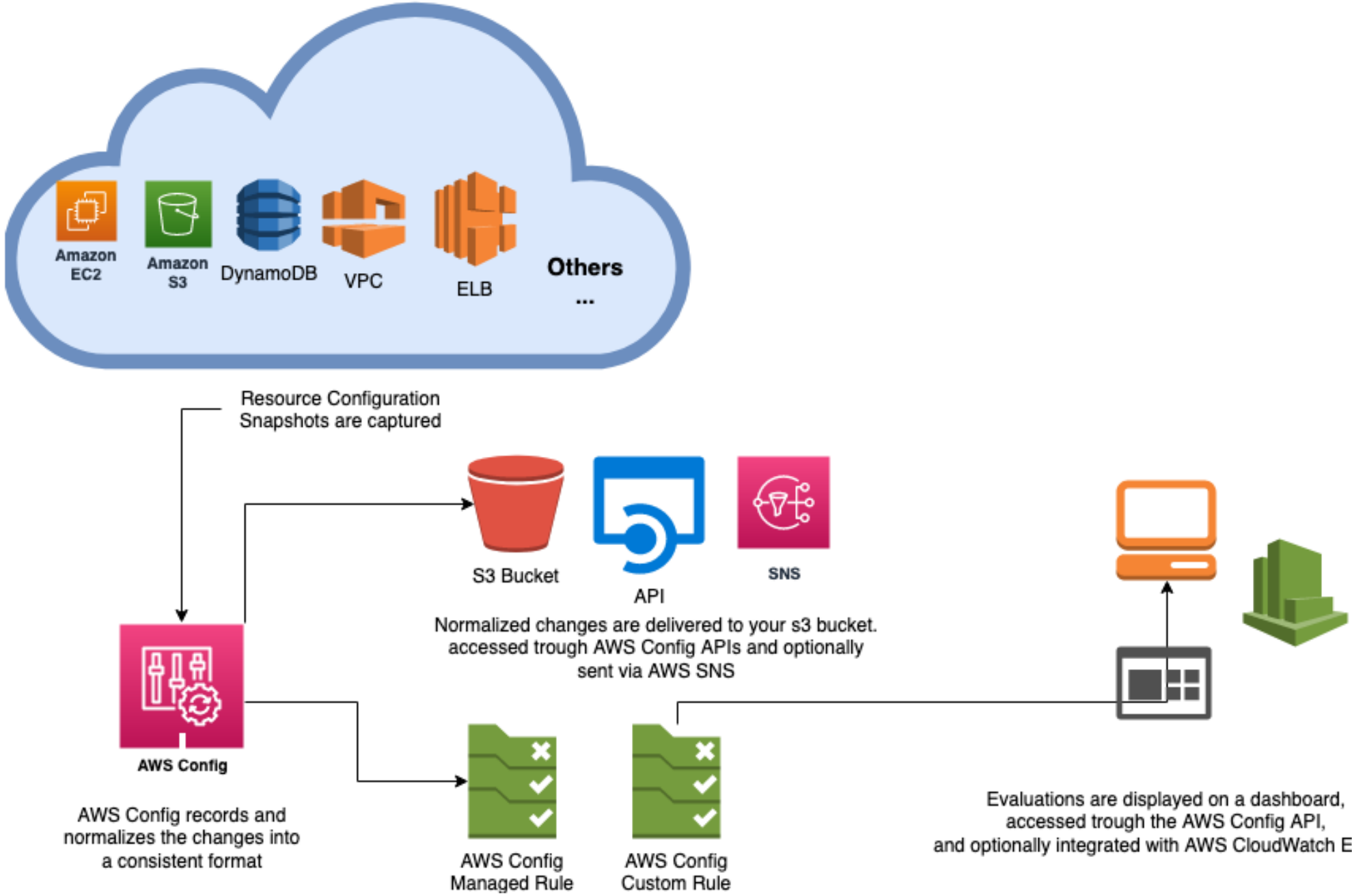
AWS Config: How it works



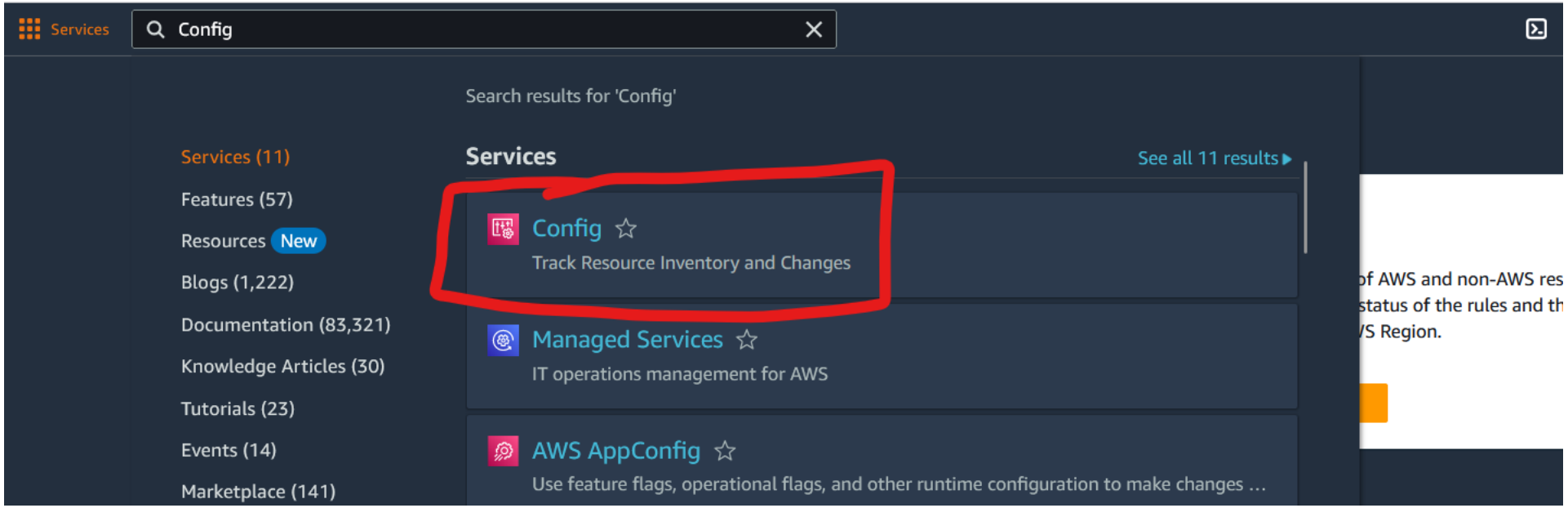
AWS Config: How it works



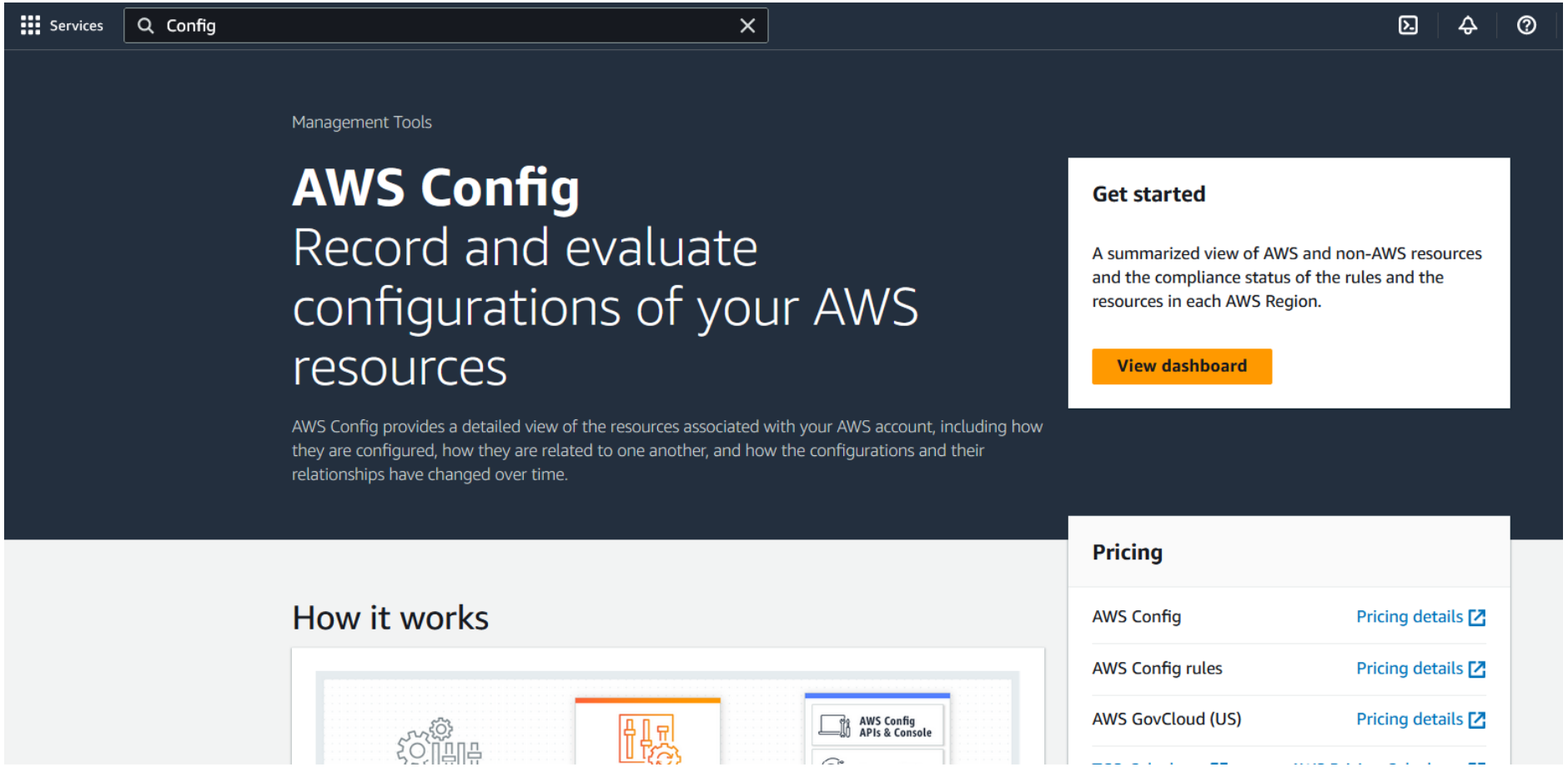

AWS Config
Record
Normalize
Store
Deliver
Changing Resources
AWS Config
APIs
History
Stream
Snapshot (ex. 2014-11-05)


Amazon EC2
Amazon S3
DynamoDB
VPC
ELB
Others ...
Resource Configuration Snapshots are captured
S3 Bucket
API
SNS
Normalized changes are delivered to your s3 bucket. accessed trough AWS Config APIs and optionally sent via AWS SNS
AWS Config
AWS Config records and normalizes the changes into a consistent format
AWS Config Managed Rule
AWS Config Custom Rule
Evaluations are displayed on a dashboard, accessed trough the AWS Config API, and optionally integrated with AWS CloudWatch Events

Getting started!



Getting started!



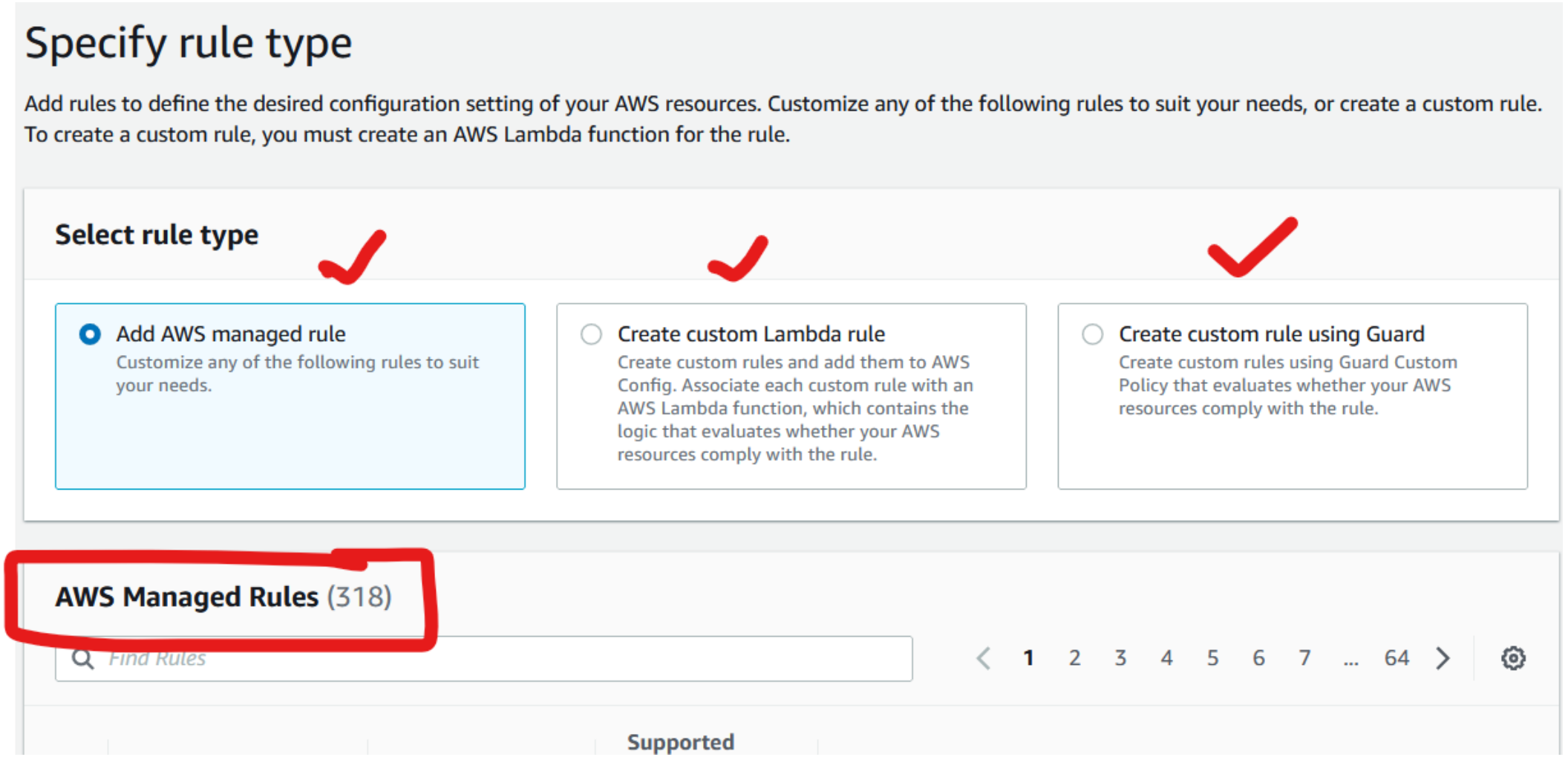
Getting started!

Getting started!

https://docs.aws.amazon.com/config/latest/developerguide/gs-console.html

How to develop Rules?

Rule Type


Specify rule type
Add rules to define the desired configuration setting of your AWS resources. Customize any of the following rules to suit your needs, or create a custom rule. To create a custom rule, you must create an AWS Lambda function for the rule.
Select rule type
Add AWS managed rule
Customize any of the following rules to suit your needs.
Create custom Lambda rule
Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.
Create custom rule using Guard
Create custom rules using Guard Custom Policy that evaluates whether your AWS resources comply with the rule.
AWS Managed Rules (318)
Find Rules
1 2 3 4 5 6 7 ... 64
Supported

AWS Config Rule Development Kit (RDK)

AWS Config released a Rule Development Kit (RDK) that greatly simplifies your **custom rule authoring experienc**e. **The RDK is an open-source tool that helps you set up AWS Config, author rules, and then test them using a variety of AWS resource types**. This allows you to focus on the development of the rule itself.

AWS Config Rules Repository

Managed by Community

- https://github.com/awslabs/aws-config-rules

Related Projects

- RDK (Rule Development Kit) - https://github.com/awslabs/aws-config-rdk
- RDKLib (Library to run rules at scale) - https://github.com/awslabs/aws-config-rdklib
- Config Rules Engine (Deploy and manage Rules at scale) - https://github.com/awslabs/aws-config-engine-for-compliance-as-code

Getting started with RDK

- https://aws.amazon.com/blogs/mt/introducing-the-aws-config-rule-development-kit-rdk/

Rajesh Kumar

DevOps@RajeshKumar.xyz

www.RajeshKumar.xyz