Accelerating FedRAMP Authorizations (ATOs) in AWS GovCloud (US)

Tim Sandage
Senior Security Partner Strategist
Amazon Web Services

Alexis Robinson
Technical Program Manager, Government Audits
Amazon Web Services

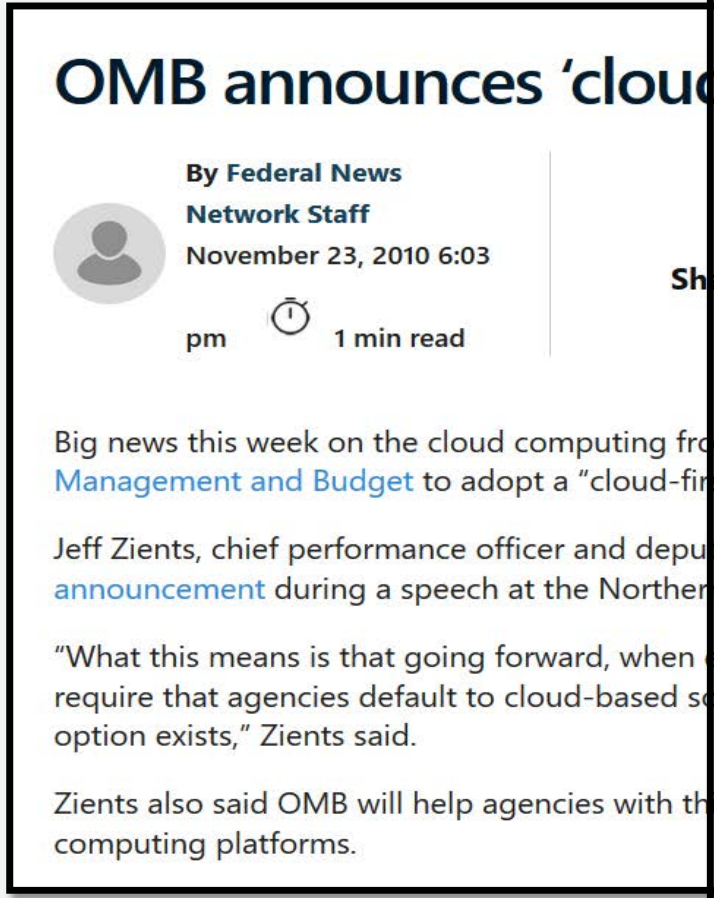
Agenda

- Understanding the history of cloud security in the federal government
- FedRAMP application to AWS
- AWS use cases for managing FedRAMP
- ATO on AWS

Know the history

Know the history

------ 2010 ---------------2011----------------2018----------



OMB announces ‘clou

By Federal News Network Staff

November 23, 2010 6:03 pm

1 min read

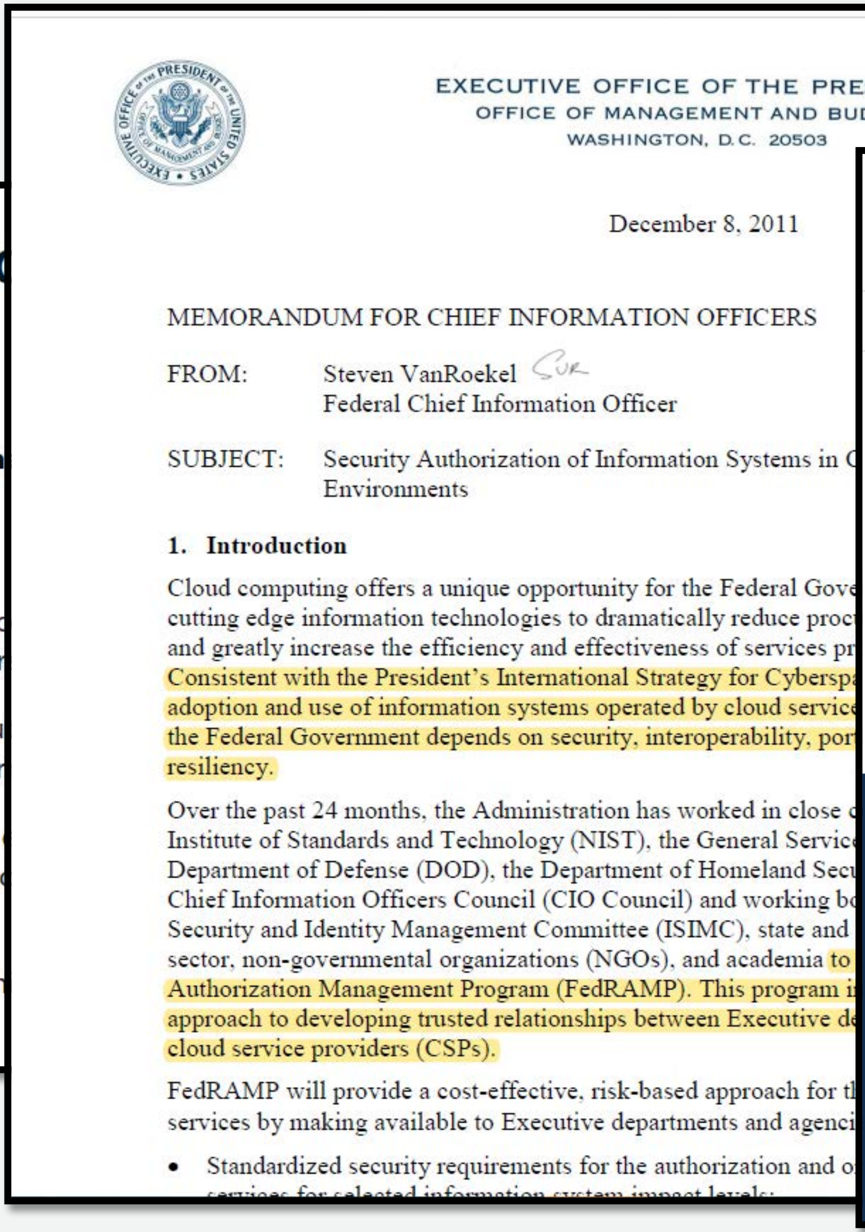
Sh

Big news this week on the cloud computing fr Management and Budget to adopt a “cloud-fir

Jeff Zients, chief performance officer and depu announcement during a speech at the Norther

“What this means is that going forward, when require that agencies default to cloud-based s option exists,” Zients said.

Zients also said OMB will help agencies with th computing platforms.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 8, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Steven VanRoekel SVR
Federal Chief Information Officer

SUBJECT: Security Authorization of Information Systems in C Environments

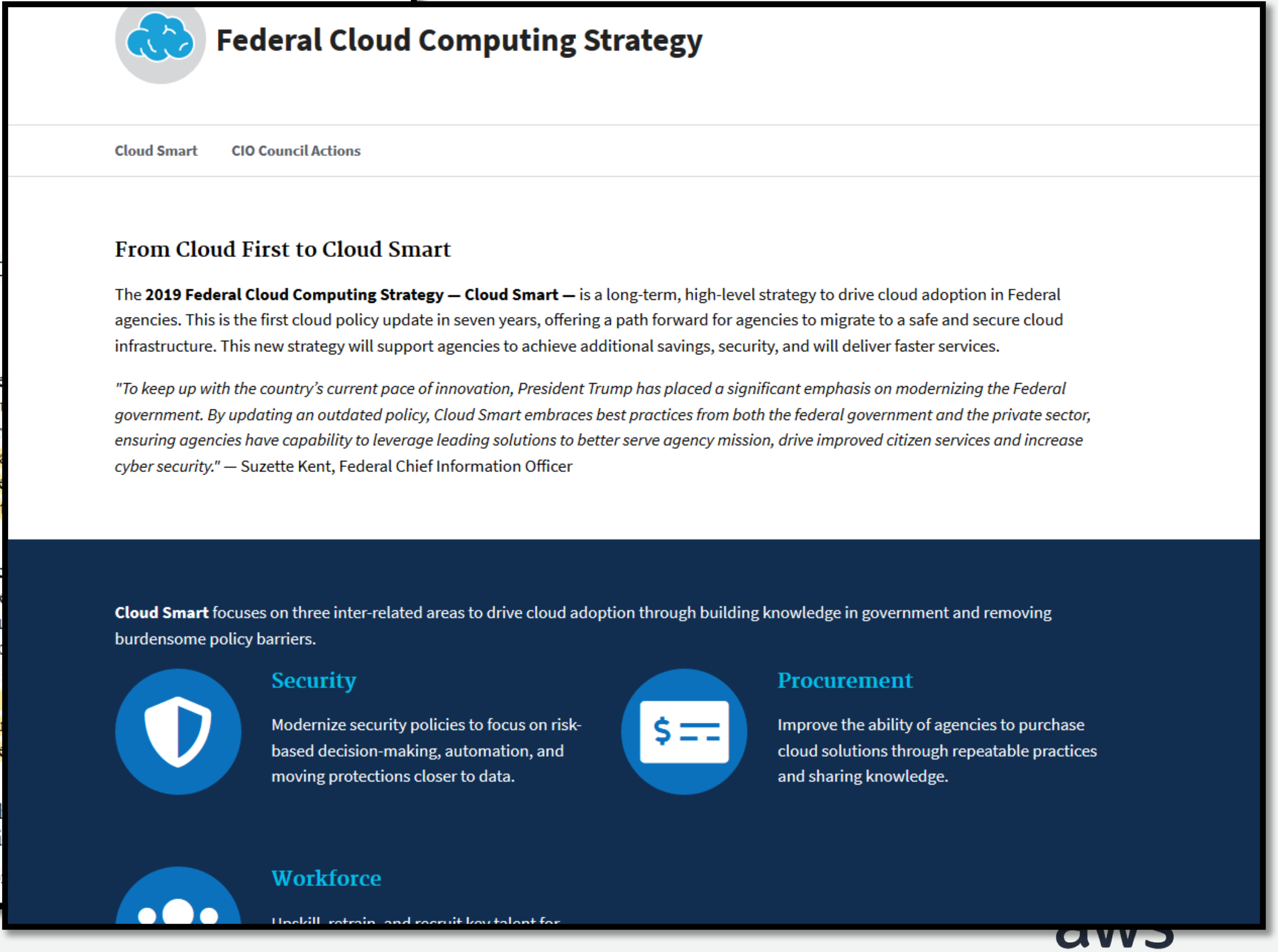
1. **Introduction**

Cloud computing offers a unique opportunity for the Federal Gove cutting edge information technologies to dramatically reduce proc and greatly increase the efficiency and effectiveness of services pr Consistent with the President’s International Strategy for Cybersp adoption and use of information systems operated by cloud service the Federal Government depends on security, interoperability, por resiliency.

Over the past 24 months, the Administration has worked in close Institute of Standards and Technology (NIST), the General Service Department of Defense (DOD), the Department of Homeland Secu Chief Information Officers Council (CIO Council) and working bo Security and Identity Management Committee (ISIMC), state and sector, non-governmental organizations (NGOs), and academia to Authorization Management Program (FedRAMP). This program i approach to developing trusted relationships between Executive de cloud service providers (CSPs).

FedRAMP will provide a cost-effective, risk-based approach for th services by making available to Executive departments and agenci

- Standardized security requirements for the authorization and o services for selected information system impact levels;



Federal Cloud Computing Strategy

Cloud Smart CIO Council Actions

From Cloud First to Cloud Smart

The **2019 Federal Cloud Computing Strategy — Cloud Smart —** is a long-term, high-level strategy to drive cloud adoption in Federal agencies. This is the first cloud policy update in seven years, offering a path forward for agencies to migrate to a safe and secure cloud infrastructure. This new strategy will support agencies to achieve additional savings, security, and will deliver faster services.

"To keep up with the country’s current pace of innovation, President Trump has placed a significant emphasis on modernizing the Federal government. By updating an outdated policy, Cloud Smart embraces best practices from both the federal government and the private sector, ensuring agencies have capability to leverage leading solutions to better serve agency mission, drive improved citizen services and increase cyber security." — Suzette Kent, Federal Chief Information Officer

Cloud Smart focuses on three inter-related areas to drive cloud adoption through building knowledge in government and removing burdensome policy barriers.

Security

Modernize security policies to focus on risk-based decision-making, automation, and moving protections closer to data.

Procurement

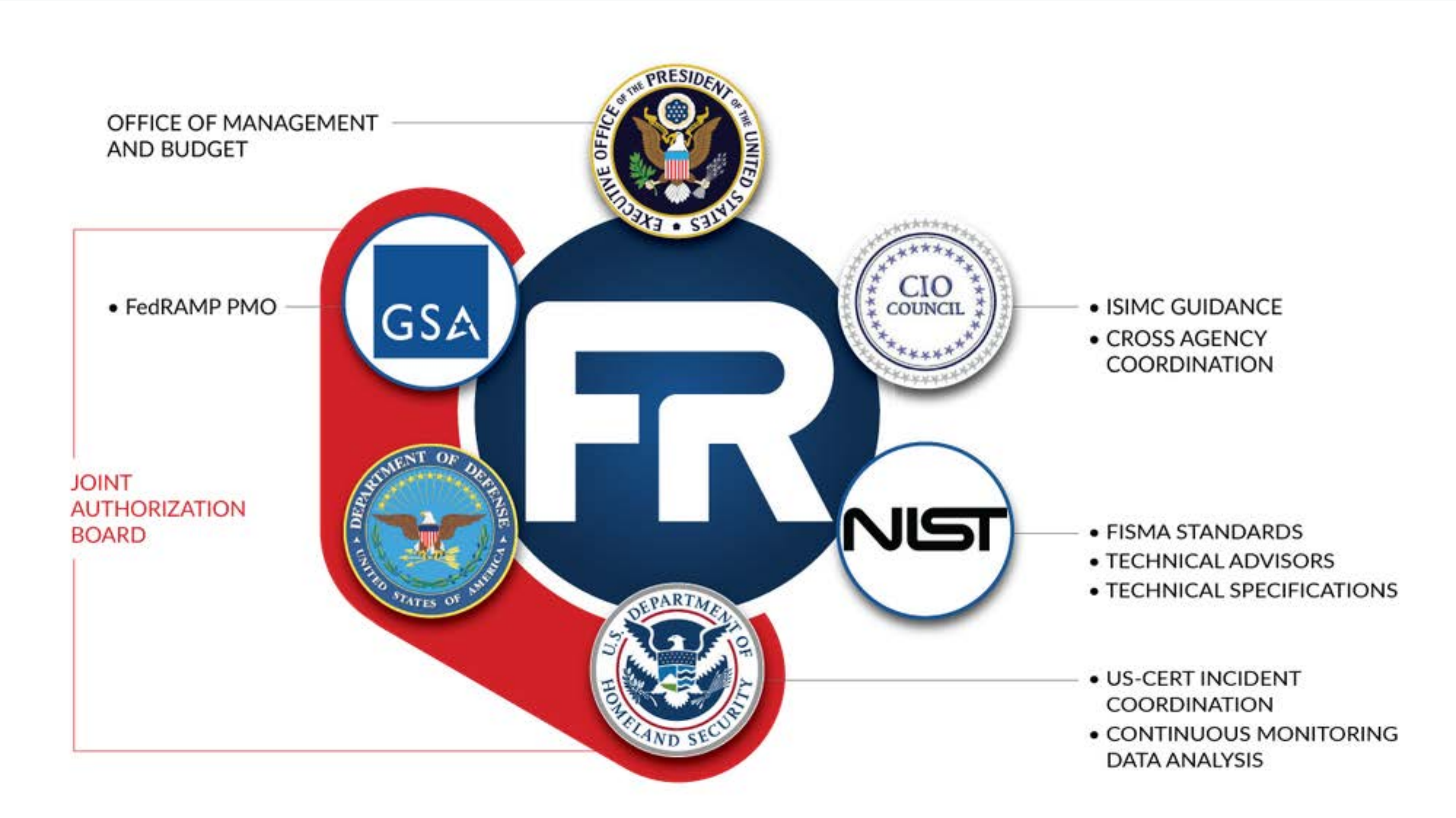
Improve the ability of agencies to purchase cloud solutions through repeatable practices and sharing knowledge.

Workforce

Upskill, retrain, and recruit key talent for

Know the history

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government-wide program that delivers a standard approach to the security assessment, authorization and continuous monitoring for cloud products and services.


OFFICE OF MANAGEMENT AND BUDGET
• FedRAMP PMO
JOINT AUTHORIZATION BOARD
GSA
FR
NIST
CIO COUNCIL
• ISIMC GUIDANCE
• CROSS AGENCY COORDINATION
• FISMA STANDARDS
• TECHNICAL ADVISORS
• TECHNICAL SPECIFICATIONS
• US-CERT INCIDENT COORDINATION
• CONTINUOUS MONITORING DATA ANALYSIS

The governing bodies of FedRAMP include the Office of Management and Budget (OMB), ***U.S. General Services Administration (GSA***), ***U.S. Department of Homeland Security (DHS)***, ***U.S. Department of Defense (DOD),*** National Institutes of Standards & Technology (NIST), and the Federal CIO Council.

Know the history

The FedRAMP memo introduced the following five (5) requirements which are fundamental to the FedRAMP program:

AWS must comply with NIST security requirements based on the security categorization.

AWS must have an assessment conducted by an independent third-party assessor (3PAO).

AWS must have authorization packages reviewed by a Joint Authorization Board (JAB) consisting of security experts from the three agencies.

AWS must leverage standardized contractual language and templates provided by the FedRAMP Project Management Office (PMO).

A repository of authorization packages must be available government-wide.

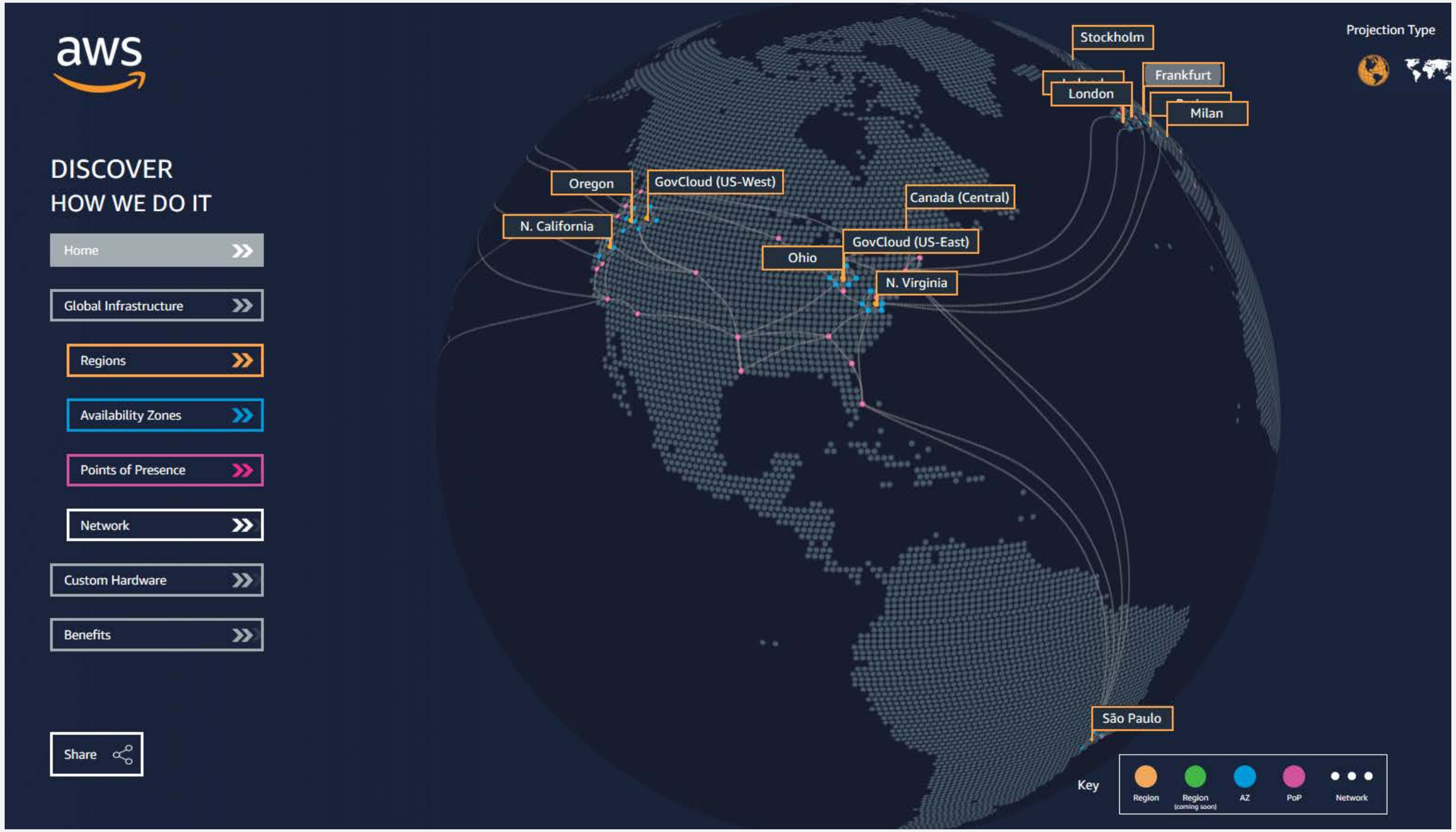
FedRAMP application to AWS

FedRAMP application to AWS

FedRAMP applicable Regions

In the United States, the commercial AWS East/West Regions (IAD, PDX, SFO, CMH) are authorized in the FedRAMP **Moderate** categorization.

The AWS GovCloud (US) Regions (PDT, OSU) are authorized in the FedRAMP **High** categorization.



FedRAMP application to AWS

AWS GovCloud (US)

# of AWS services FedRAMP High authorized in AWS GovCloud (US)	43
# of AWS services in FedRAMP High authorization queue	27
# of new AWS service FedRAMP High authorizations in 2019	15

AWS East/West (US)

# of AWS services FedRAMP Moderate authorized in AWS EastWest	48
# of AWS services in FedRAMP Moderate authorization queue	30
# of new AWS service FedRAMP Moderate authorizations in 2019	6

FedRAMP application to AWS

Most recent update: AWS has received authorizations from the following services in September 2019.

- Amazon API Gateway
- Amazon CloudWatch
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elasticsearch Service
- Amazon Inspector
- Amazon Polly
- AWS CodeDeploy
- AWS Config
- AWS Direct Connect
- AWS Elastic Beanstalk
- AWS Lambda
- AWS Step Functions

FedRAMP application to AWS

AWS service FedRAMP authorizations planned by Q1-2020

Amazon Aurora

Amazon Cloud Directory

Amazon Comprehend

Amazon GuardDuty

Amazon Kinesis Data Firehose

Amazon Rekognition

Amazon Route 53

Amazon SageMaker

Amazon Transcribe

Amazon Translate

Amazon WorkSpaces

AWS CodeBuild

AWS CodeCommit

AWS DataSync

AWS Directory Service

AWS Glue

AWS IoT Core

AWS IoT Device Management

AWS IoT Greengrass

AWS License Manager

AWS Organizations

AWS Service Catalog

AWS Server Migration Service (AWS SMS)

AWS Trusted Advisor

AWS WAF

Amazon Athena

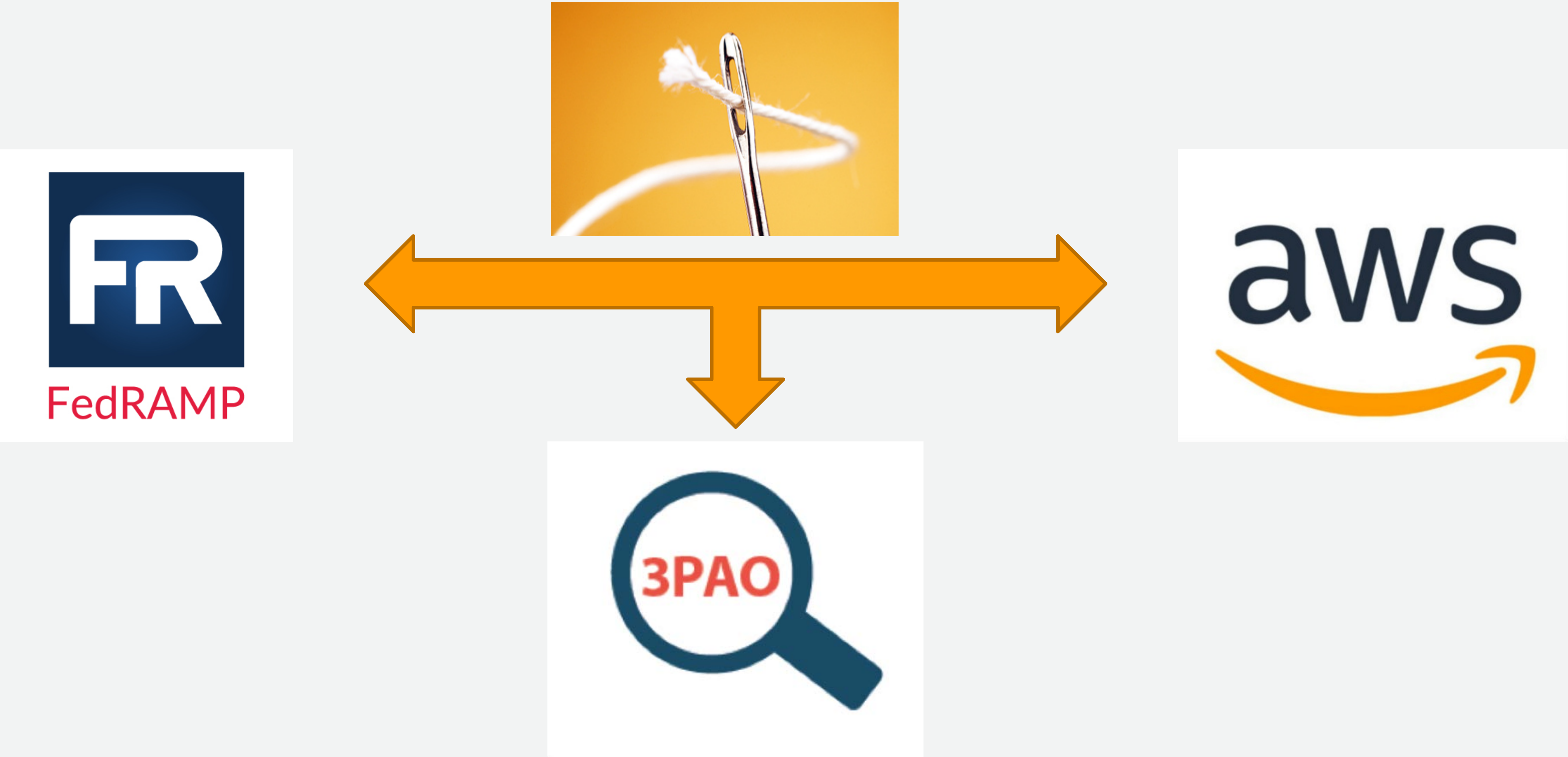
FedRAMP application to AWS

Amazon API Gateway
Amazon CloudWatch
Amazon CloudWatch Events
Amazon CloudWatch Logs
Amazon DynamoDB
Amazon Elastic Block Store
Amazon Elastic Compute Cloud
Amazon Elastic Container Registry
Amazon Elastic Container Service
Amazon Elastic File System
Amazon Elastic MapReduce
Amazon ElastiCache
Amazon Elasticsearch Service
Amazon S3 Glacier
Amazon Inspector
Amazon Kinesis Data Streams
Amazon Polly
Amazon RDS (MariaDB)
Amazon RDS (MySQL)
Amazon RDS (Oracle)
Amazon RDS (Postgres)
Amazon RDS (SQL Server)
Amazon Redshift
Amazon Simple Notification Service
Amazon Simple Queue Service
Amazon Simple Storage Service
Amazon Simple Workflow Service
Amazon Virtual Private Cloud
AWS Auto Scaling
AWS CloudFormation
AWS CloudTrail
AWS CodeDeploy
AWS Config
AWS Database Migration Service
AWS Direct Connect
AWS Elastic Beanstalk
AWS Identity & Access Management (IAM)
AWS Key Management Service (AWS KMS)
AWS Lambda
AWS Snowball
AWS Snowball Edge
AWS Step Functions
AWS Systems Manager
Elastic Load Balancing

Use cases for managing FedRAMP

AWS use cases for managing FedRAMP

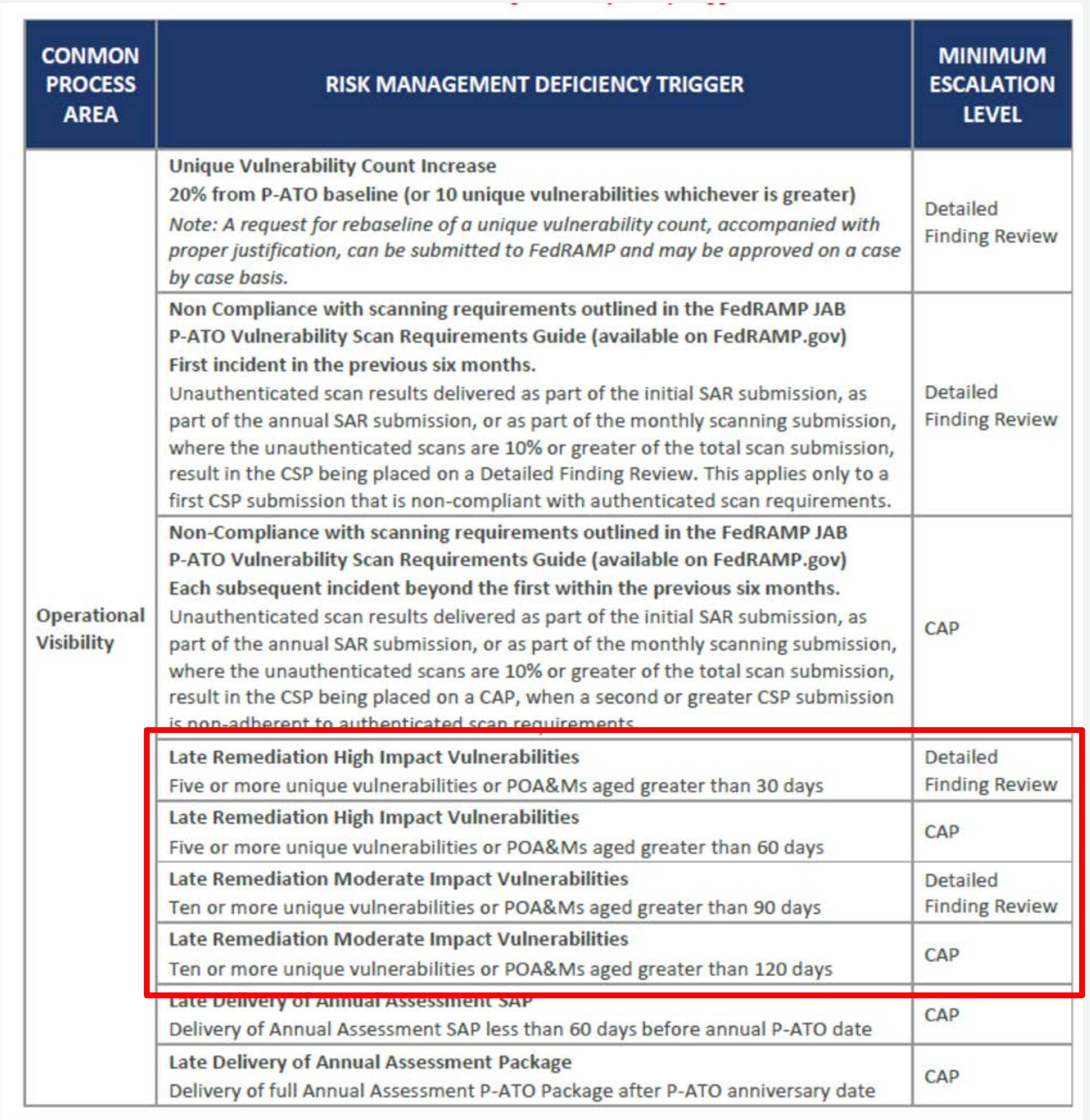
Threading the needle with the government, our 3PAO, and with AWS service teams



AWS use cases for managing FedRAMP

Challenges of meeting Continual Monitoring (ConMon) Performance Management Risk Management Triggers – a blanket threshold

- Patching for scan vulnerabilities across thousands of fleets and millions of hosts
- A continual onslaught of 3PAO pentest and manual control findings
- Won't hire/can't hire fast enough

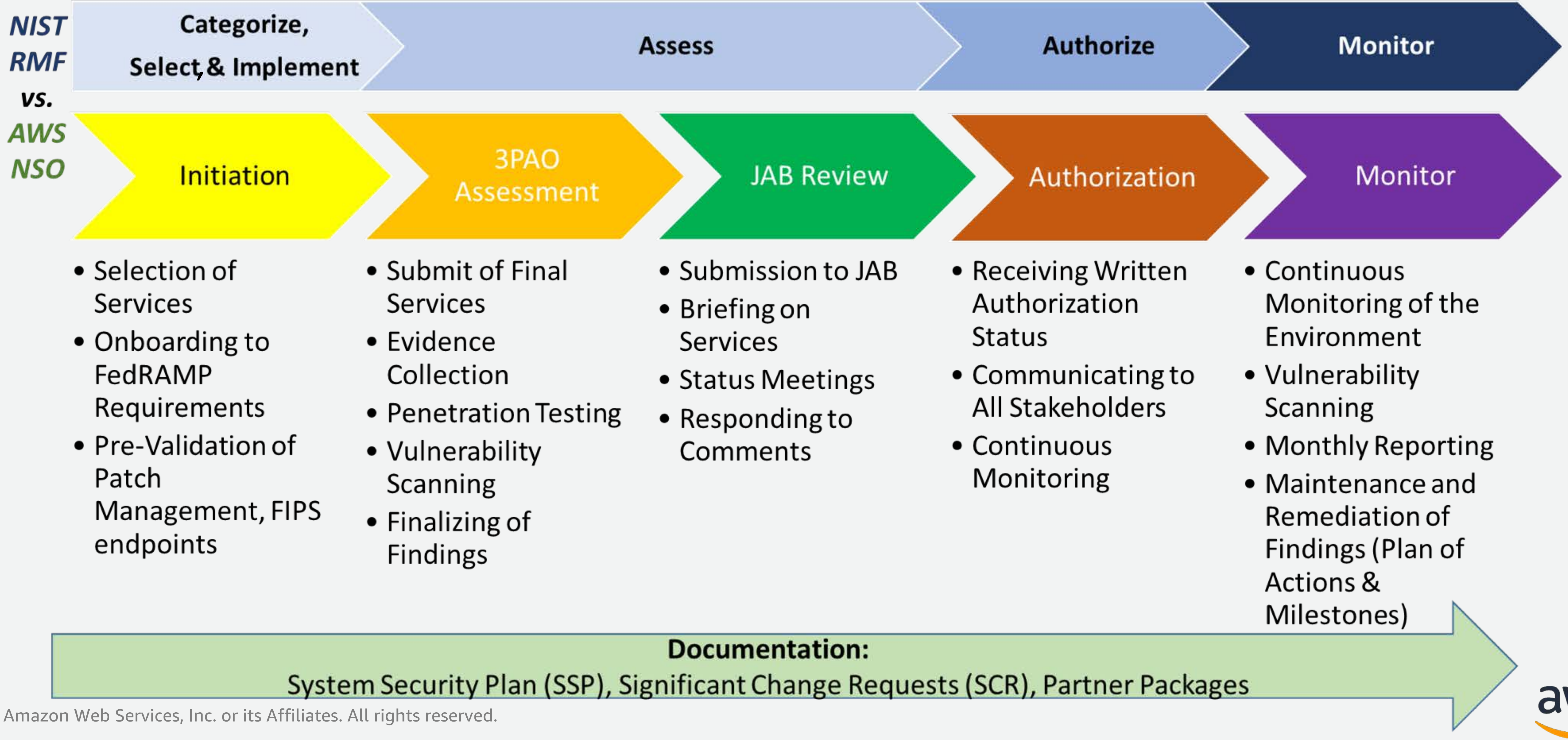


CONMON PROCESS AREA	RISK MANAGEMENT DEFICIENCY TRIGGER	MINIMUM ESCALATION LEVEL
Operational Visibility	**Unique Vulnerability Count Increase** **20% from P-ATO baseline (or 10 unique vulnerabilities whichever is greater)** *Note: A request for rebaseline of a unique vulnerability count, accompanied with proper justification, can be submitted to FedRAMP and may be approved on a case by case basis.*	Detailed Finding Review
	Non Compliance with scanning requirements outlined in the FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide (available on FedRAMP.gov) **First incident in the previous six months.** Unauthenticated scan results delivered as part of the initial SAR submission, as part of the annual SAR submission, or as part of the monthly scanning submission, where the unauthenticated scans are 10% or greater of the total scan submission, result in the CSP being placed on a Detailed Finding Review. This applies only to a first CSP submission that is non-compliant with authenticated scan requirements.	Detailed Finding Review
	Non-Compliance with scanning requirements outlined in the FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide (available on FedRAMP.gov) **Each subsequent incident beyond the first within the previous six months.** Unauthenticated scan results delivered as part of the initial SAR submission, as part of the annual SAR submission, or as part of the monthly scanning submission, where the unauthenticated scans are 10% or greater of the total scan submission, result in the CSP being placed on a CAP, when a second or greater CSP submission is non-adherent to authenticated scan requirements.	CAP
	Late Remediation High Impact Vulnerabilities Five or more unique vulnerabilities or POA&Ms aged greater than 30 days	Detailed Finding Review
	Late Remediation High Impact Vulnerabilities Five or more unique vulnerabilities or POA&Ms aged greater than 60 days	CAP
	Late Remediation Moderate Impact Vulnerabilities Ten or more unique vulnerabilities or POA&Ms aged greater than 90 days	Detailed Finding Review
	Late Remediation Moderate Impact Vulnerabilities Ten or more unique vulnerabilities or POA&Ms aged greater than 120 days	CAP
	Late Delivery of Annual Assessment SAP Delivery of Annual Assessment SAP less than 60 days before annual P-ATO date	CAP
	Late Delivery of Annual Assessment Package Delivery of full Annual Assessment P-ATO Package after P-ATO anniversary date	CAP

AWS use cases for managing FedRAMP

New Service Onboarding Process

6 AWS Security Teams – 4 Cycles in a Year – 9 Month Duration



NIST RMF **vs.** *AWS NSO*

Categorize, Select, & Implement → **Assess** → **Authorize** → **Monitor**

Initiation → 3PAO Assessment → JAB Review → Authorization → Monitor

Initiation

- Selection of Services
- Onboarding to FedRAMP Requirements
- Pre-Validation of Patch Management, FIPS endpoints

3PAO Assessment

- Submit of Final Services
- Evidence Collection
- Penetration Testing
- Vulnerability Scanning
- Finalizing of Findings

JAB Review

- Submission to JAB
- Briefing on Services
- Status Meetings
- Responding to Comments

Authorization

- Receiving Written Authorization Status
- Communicating to All Stakeholders
- Continuous Monitoring

Monitor

- Continuous Monitoring of the Environment
- Vulnerability Scanning
- Monthly Reporting
- Maintenance and Remediation of Findings (Plan of Actions & Milestones)

Documentation:
System Security Plan (SSP), Significant Change Requests (SCR), Partner Packages

AWS FedRAMP Compliance Program

Initiatives to help our partners accelerate and simplify the authorization process:

- Increasing accessibility of documentation for non-federal customers
- Providing timely updates to the Service in Scope webpage
- Additional granularity and direction in our documentation (i.e. Customer Responsibility Matrix) to apply the AWS Shared Responsibility Model
- Providing key documentation to assist agency authorizations

ATO on AWS

What is ATO on AWS?

Security & Compliance Acceleration Program

Helps customers, partners, and Independent Solution Vendors (ISVs)

Outcomes

Accelerates security & compliance authorization process

Reduces cost & time (average 18-24 months) – FedRAMP

Provides reusable artifacts including guidance, templates, tools, and pre-built templates from Amazon Partner Solutions

Builds and optimizes DevOps, SecOps, Continuous Integration/Continuous Delivery (CI/CD), Continuous Risk Treatment (CRT) strategies

Develops proven techniques using AWS Security Automation and Orchestration (SAO) methodology

Breaking It Down

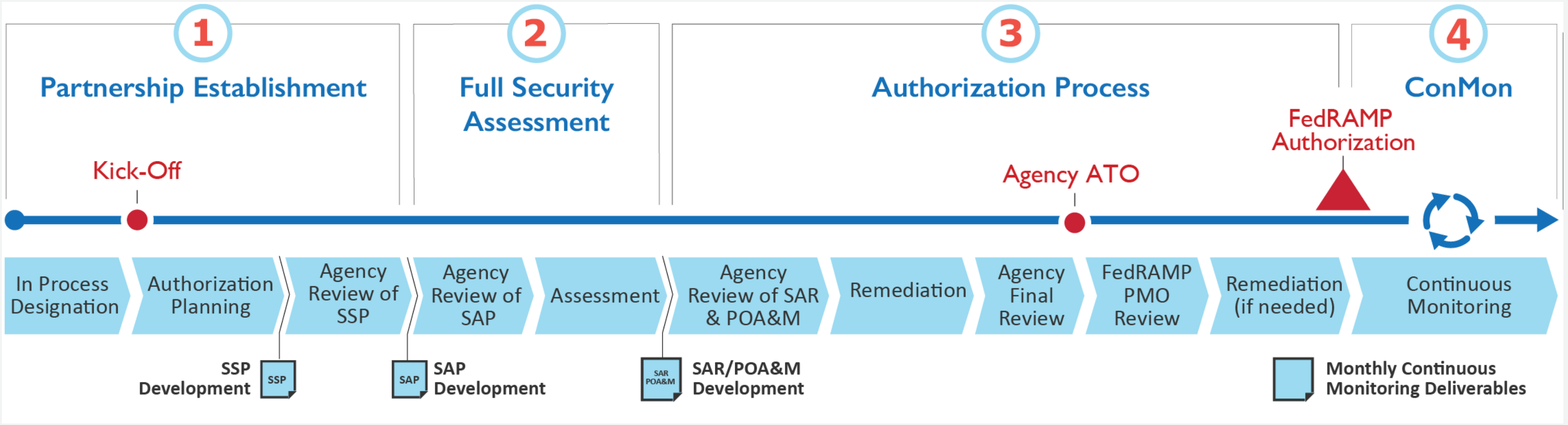
Amazon Partner Driven Process

Includes:

- ✓ Training
- ✓ Tools
- ✓ Pre-built automated deployment capabilities
- ✓ Control implementation details
- ✓ Pre-built artifacts
- ✓ Direct engagement
- ✓ Qualified System Integrators
- ✓ Visibility and marketing

The typical FedRAMP journey

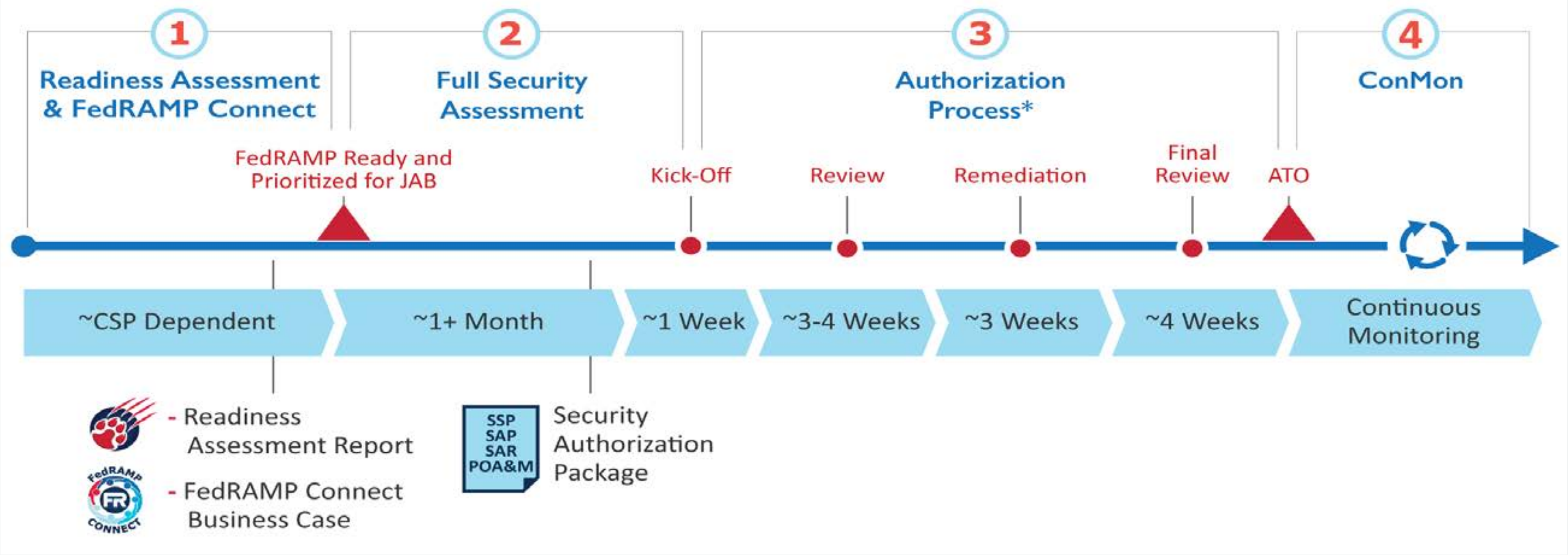
Agency Process



AVG Time to Moderate ATO: Agency

Months: 15

JAB Process



1 Readiness Assessment & FedRAMP Connect
2 Full Security Assessment
3 Authorization Process*
4 ConMon
FedRAMP Ready and Prioritized for JAB
Kick-Off
Review
Remediation
Final Review
ATO
~CSP Dependent
~1+ Month
~1 Week
~3-4 Weeks
~3 Weeks
~4 Weeks
Continuous Monitoring
- Readiness Assessment Report
- FedRAMP Connect Business Case
SSP SAP SAR POA&M
Security Authorization Package

AVG Time to Moderate ATO: JAB

Months: 18

ATO on AWS?

Benefits

Reduce effort to deploy security configurations and collect audit data to meet compliance requirements for solutions on AWS

Build an end-to-end automation capability to streamline regulated workload deployments

Collaborate with the Joint Partner Programs supported by AWS to develop and deliver unique capabilities and solutions

Works with Qualified System Integrators:

- ✓ To build and support environments that meet compliance standards and requirements
- ✓ To minimize and simplify ISV’s area of responsibility by offloading hosting and compliance management

ATO on AWS Designation

aws partner network | authority to operate

- ✓ FedRAMP on AWS
- ✓ DoD SRG on AWS
- ✓ CJIS on AWS
- ✓ PCI on AWS
- ✓ HITRUST on AWS
- ✓ IRS-1075 on AWS

Visibility and marketing for ISVs

ISV ATO's for solutions published and marketed on the ATO on AWS landing page with the option of a written or video case study

ATO on AWS APN designations for the solutions that can be used by the ISV in their marketing artifacts and materials

Real world examples:

Smartsheet

- Leveraged tools and partners available through the ATO on AWS program
- Accelerated from no presence in AWS GovCloud (US) to FedRAMP compliant **in less than 90 days**

Innovest and Coalfire

- Innovest Systems turned to ATO on AWS partner Coalfire for advisory services to build a FedRAMP-compliant platform
- Platform was built in **less than six months**, were able to attract a new government customer, and reduce costs

Guiding tenets for ATO on AWS

ATO on AWS Program

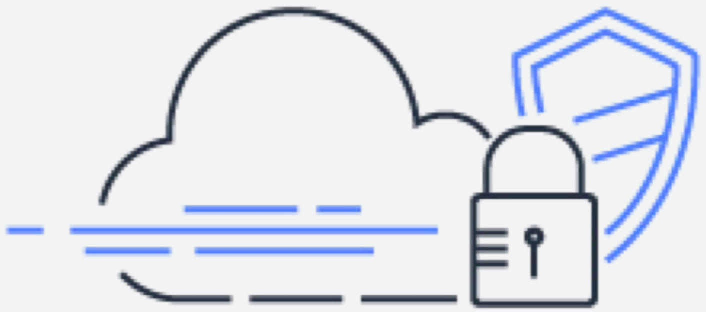
Automation leverages ***Infrastructure as Code*** concepts

Certification optimizes security processes

Validation enables continual tests and monitoring of security configurations

Empowerment emboldens informed decision-making and drives change

Implement security and compliant architectures



Goal

Verifiable compliance control solution for regulated workloads

Outcomes

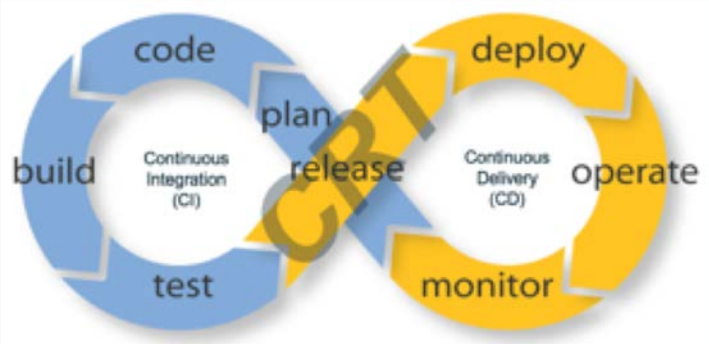
Accelerated path-to-production

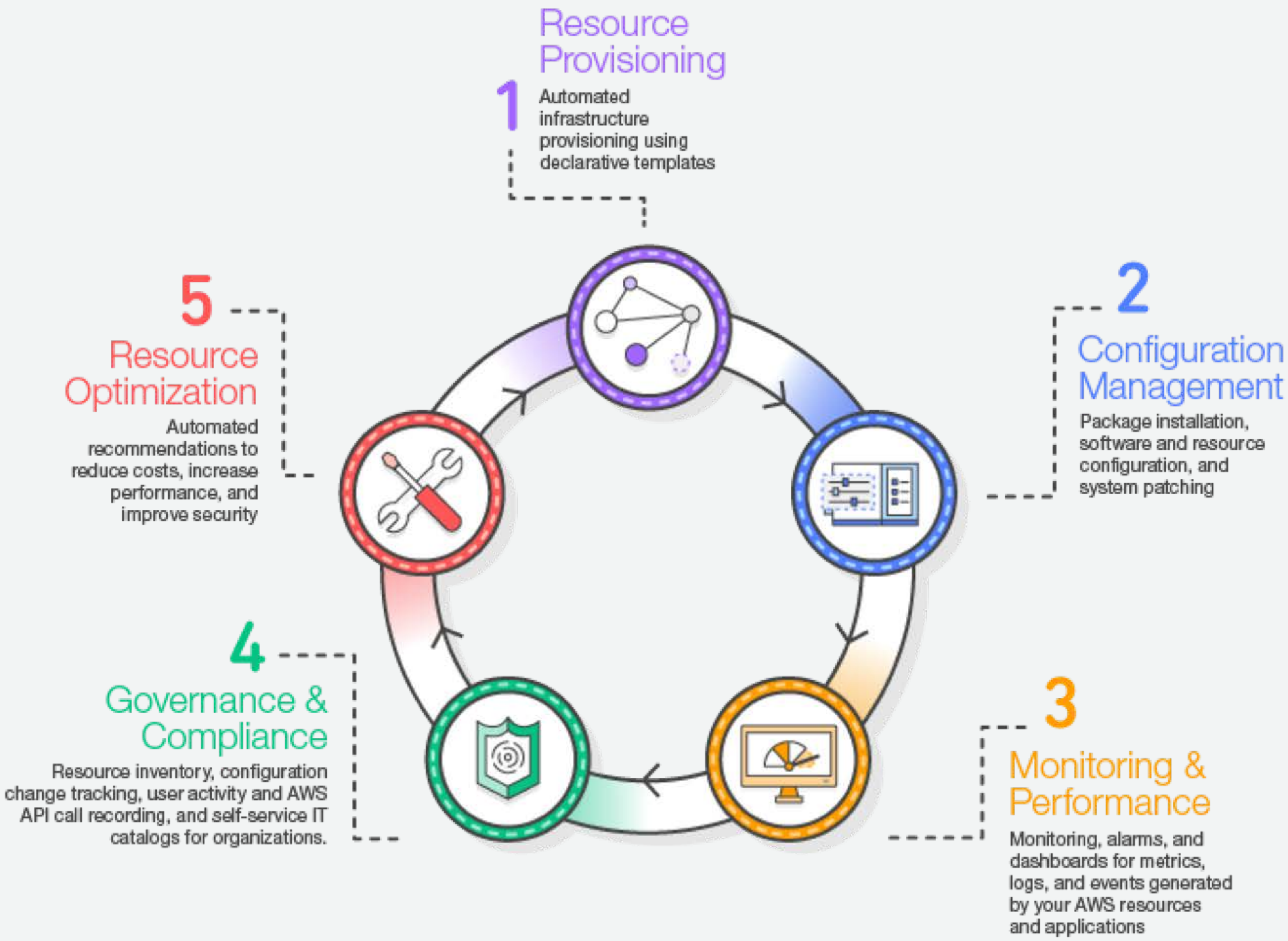
Improved compliance and security posture

Reduction in non-compliant findings and re-work

Demonstrable controls to support the assessment process

Optimized cloud risk management





1 Resource Provisioning

Automated infrastructure provisioning using declarative templates

2 Configuration Management

Package installation, software and resource configuration, and system patching

3 Monitoring & Performance

Monitoring, alarms, and dashboards for metrics, logs, and events generated by your AWS resources and applications

4 Governance & Compliance

Resource inventory, configuration change tracking, user activity and AWS API call recording, and self-service IT catalogs for organizations.

5 Resource Optimization

Automated recommendations to reduce costs, increase performance, and improve security

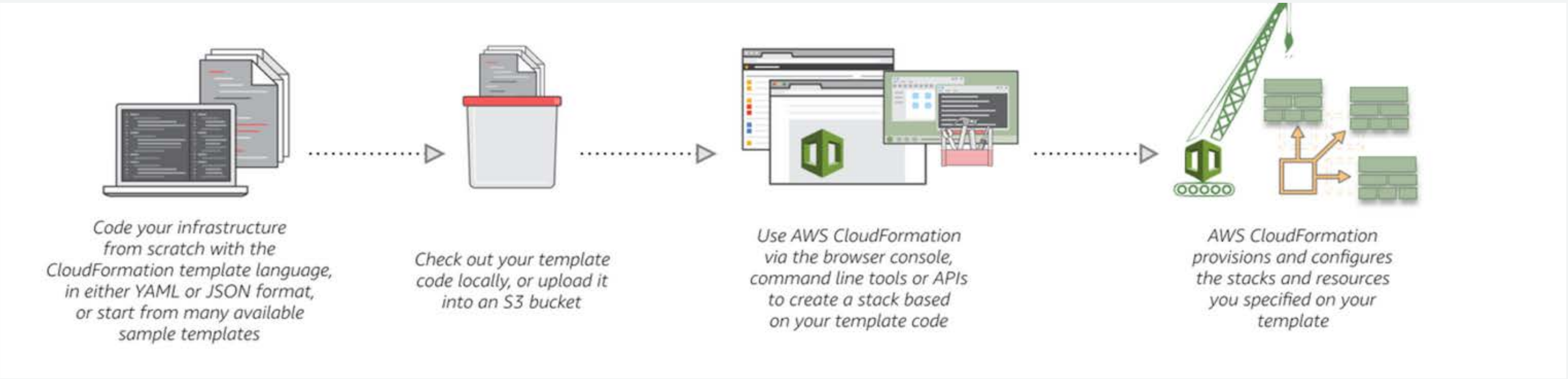
Resource provisioning

Resource Provisioning

1 Automated infrastructure provisioning using declarative templates

Automate and deploy

AWS CloudFormation provisions your resources in a safe, repeatable manner, allowing you to build and rebuild your infrastructure and applications without having to perform manual actions or write custom scripts.

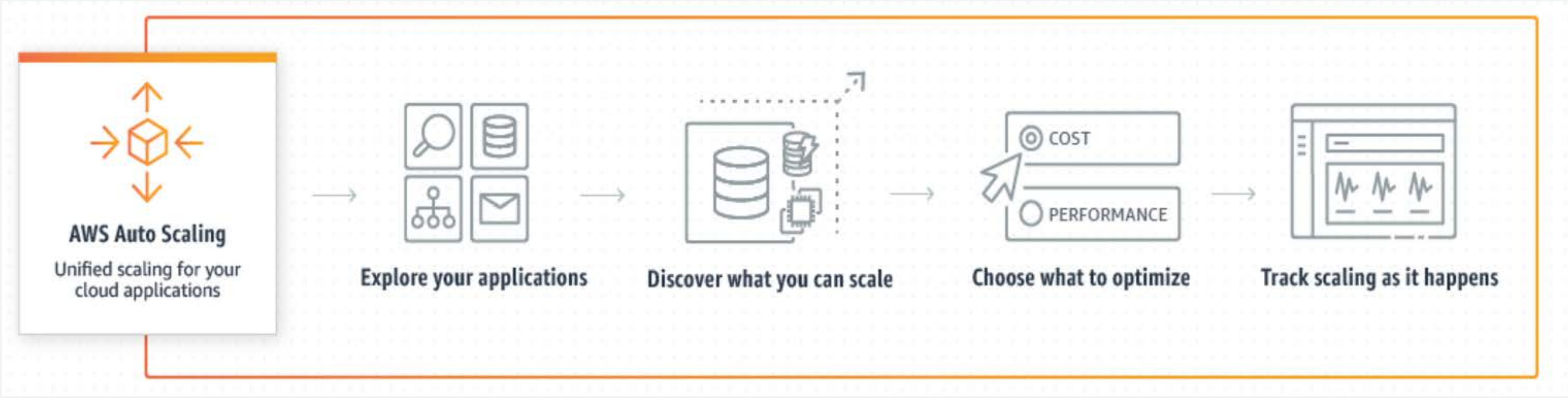


Code your infrastructure from scratch with the CloudFormation template language, in either YAML or JSON format, or start from many available sample templates

Check out your template code locally, or upload it into an S3 bucket

Use AWS CloudFormation via the browser console, command line tools or APIs to create a stack based on your template code

AWS CloudFormation provisions and configures the stacks and resources you specified on your template



AWS Auto Scaling

Unified scaling for your cloud applications

Explore your applications

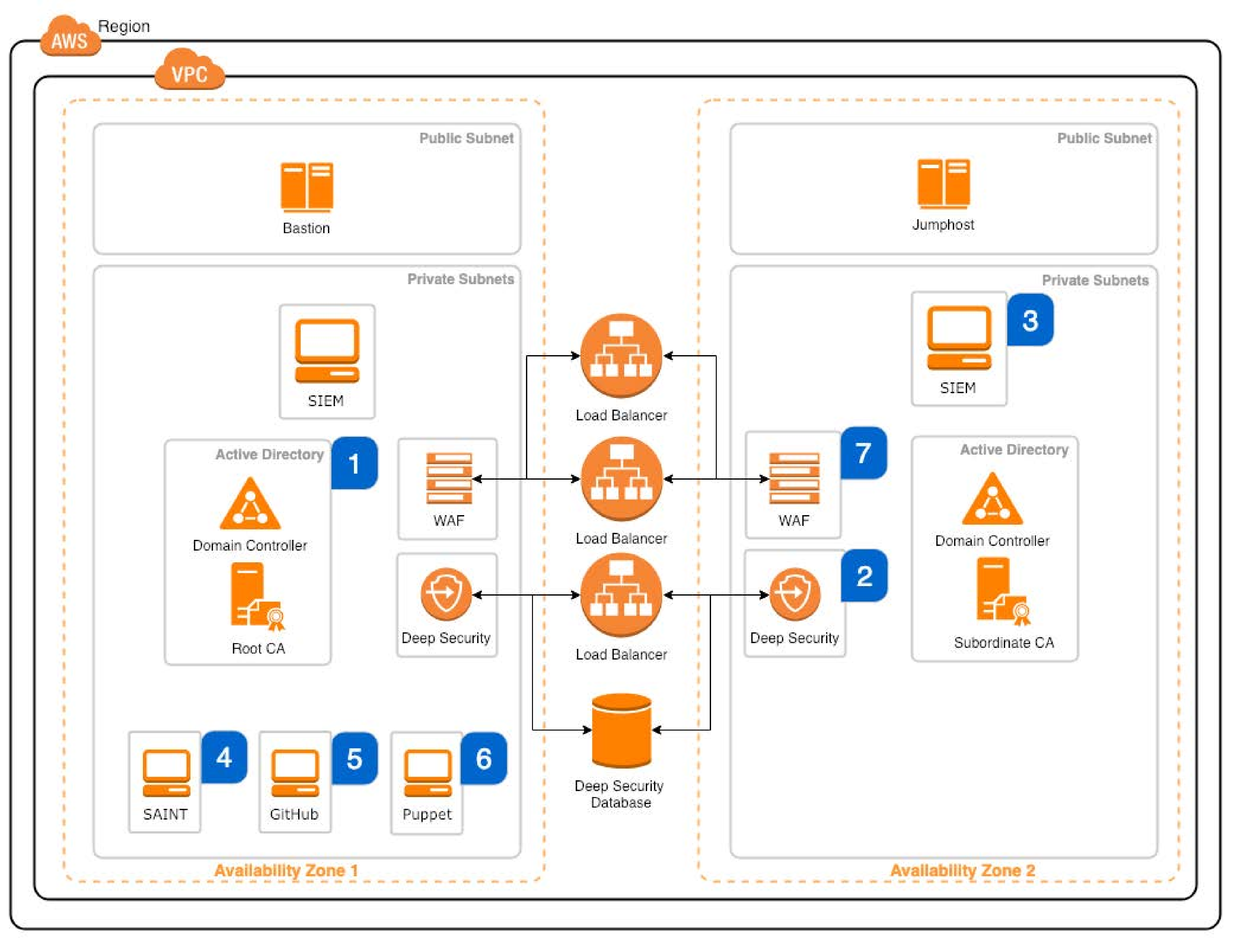
Discover what you can scale

Choose what to optimize

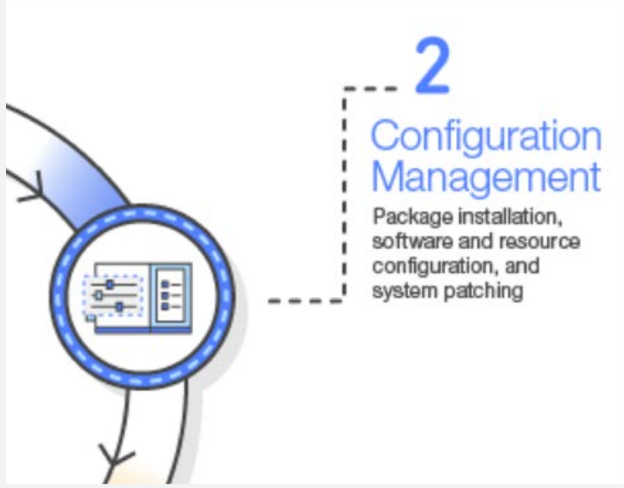
Track scaling as it happens

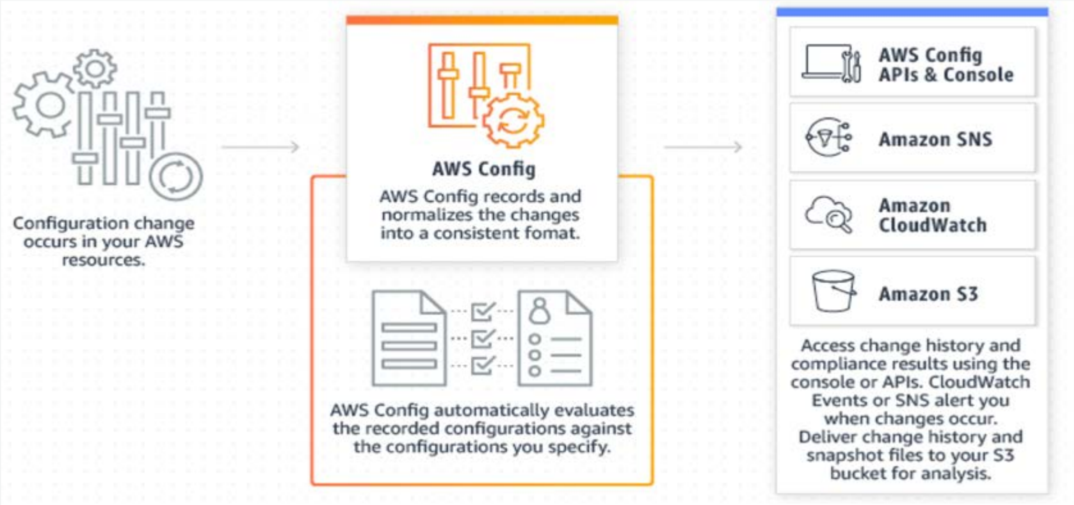
Automated architecture

Templated infrastructure provisioning



Configuration management

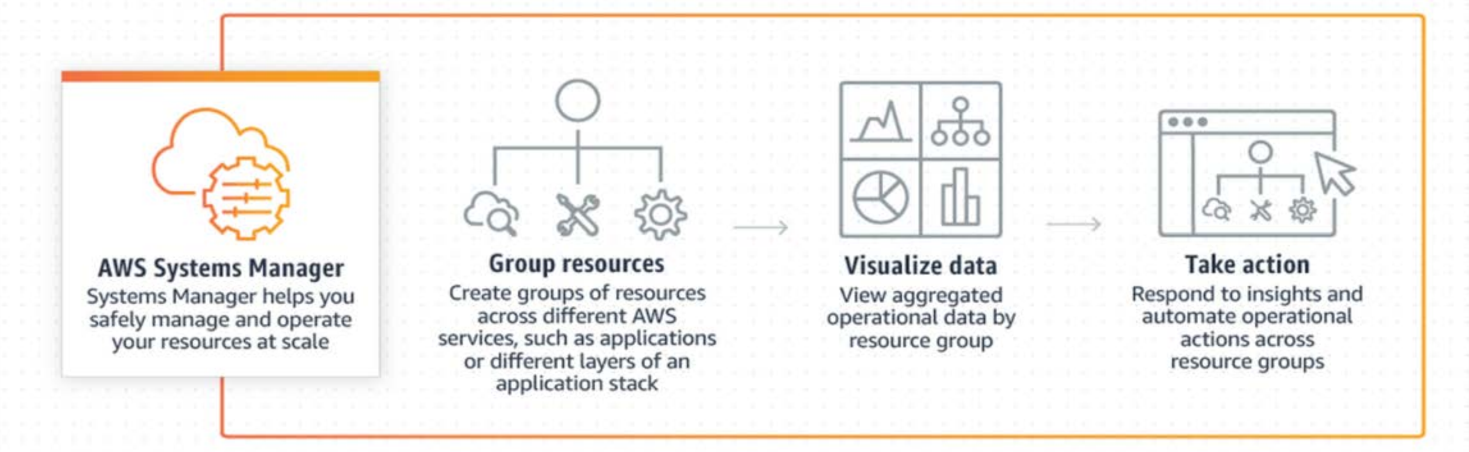

2
Configuration Management
Package installation, software and resource configuration, and system patching


Configuration change occurs in your AWS resources.

AWS Config
AWS Config records and normalizes the changes into a consistent fomat.

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

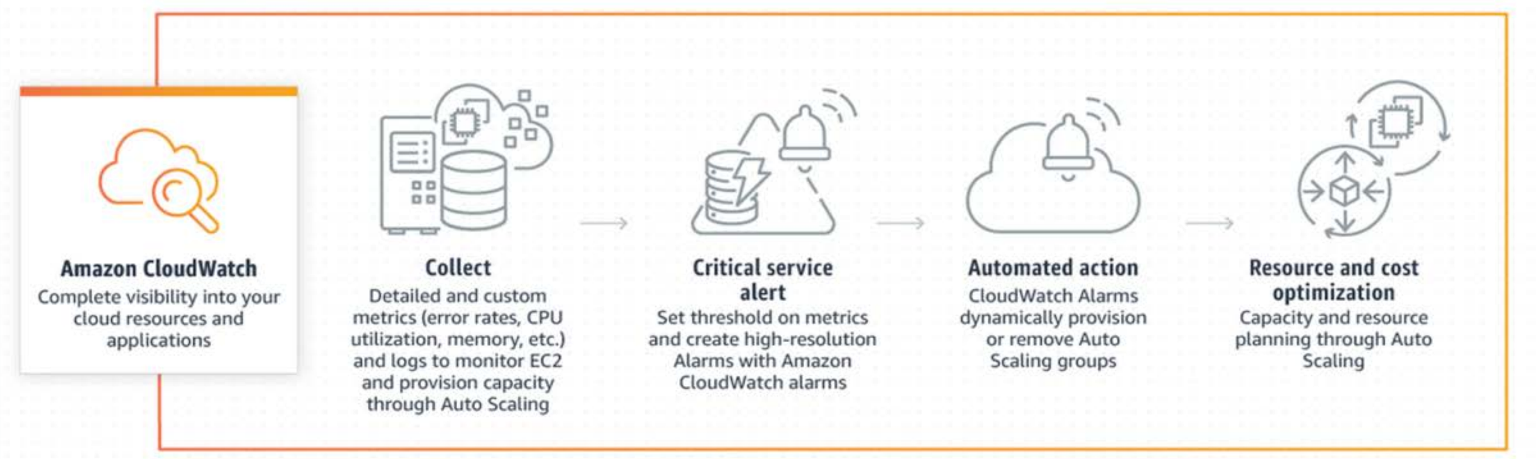
Access change history and compliance results using the console or APIs. CloudWatch Events or SNS alert you when changes occur. Deliver change history and snapshot files to your S3 bucket for analysis.


AWS Systems Manager
Systems Manager helps you safely manage and operate your resources at scale

Group resources
Create groups of resources across different AWS services, such as applications or different layers of an application stack

Visualize data
View aggregated operational data by resource group

Take action
Respond to insights and automate operational actions across resource groups


Amazon CloudWatch
Complete visibility into your cloud resources and applications

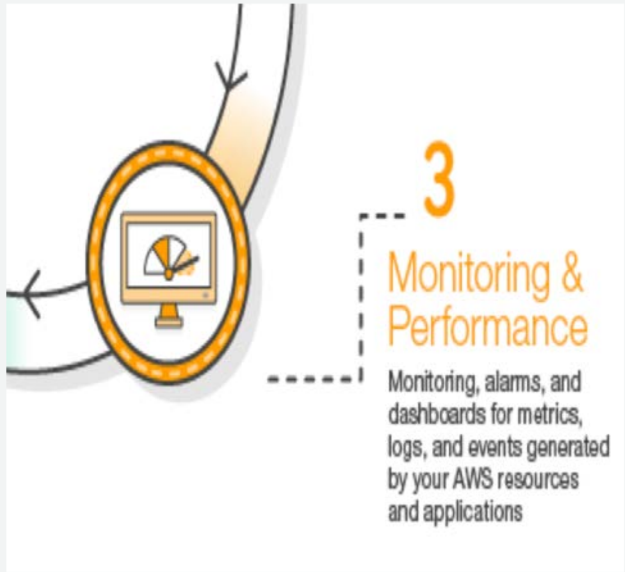
Collect
Detailed and custom metrics (error rates, CPU utilization, memory, etc.) and logs to monitor EC2 and provision capacity through Auto Scaling

Critical service alert
Set threshold on metrics and create high-resolution Alarms with Amazon CloudWatch alarms

Automated action
CloudWatch Alarms dynamically provision or remove Auto Scaling groups

Resource and cost optimization
Capacity and resource planning through Auto Scaling

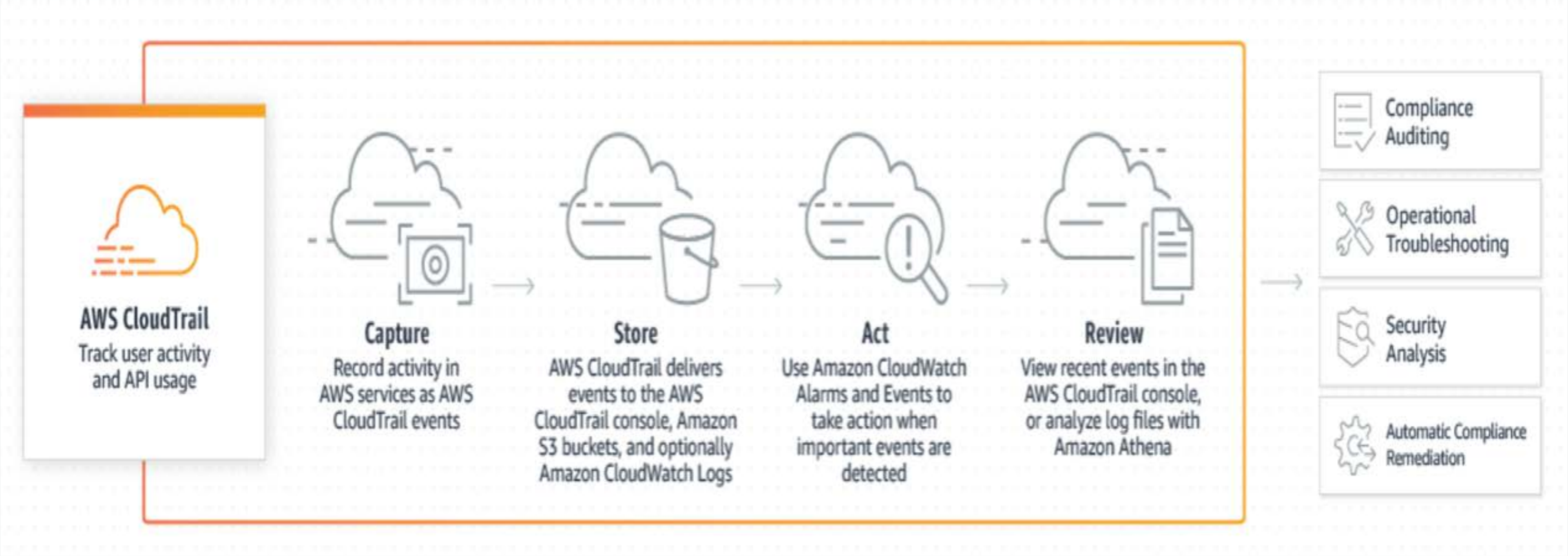
Monitoring & performance



3

Monitoring & Performance

Monitoring, alarms, and dashboards for metrics, logs, and events generated by your AWS resources and applications



AWS CloudTrail
Track user activity and API usage

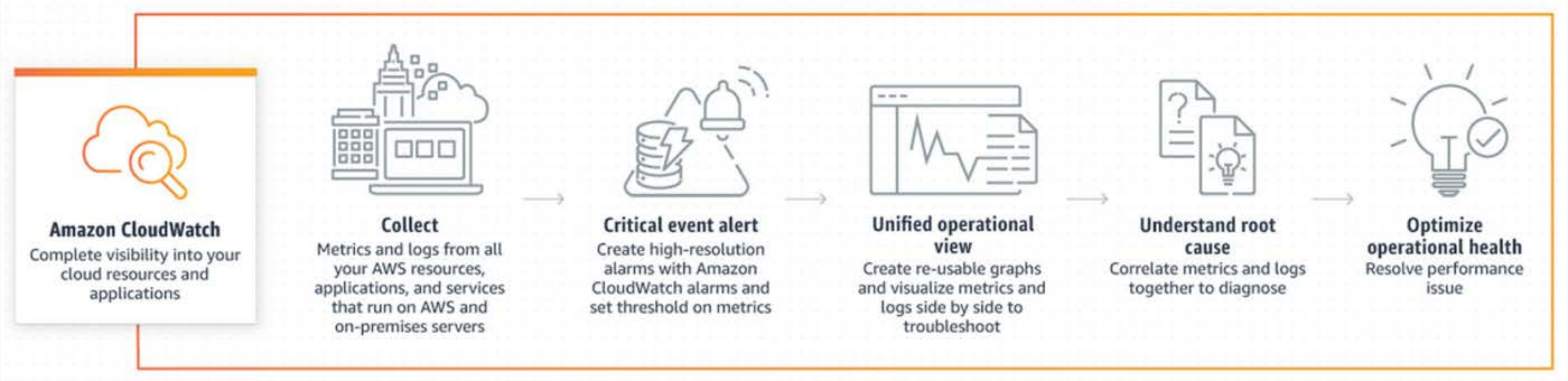
Capture
Record activity in AWS services as AWS CloudTrail events

Store
AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs

Act
Use Amazon CloudWatch Alarms and Events to take action when important events are detected

Review
View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena

- Compliance Auditing
- Operational Troubleshooting
- Security Analysis
- Automatic Compliance Remediation



Amazon CloudWatch
Complete visibility into your cloud resources and applications

Collect
Metrics and logs from all your AWS resources, applications, and services that run on AWS and on-premises servers

Critical event alert
Create high-resolution alarms with Amazon CloudWatch alarms and set threshold on metrics

Unified operational view
Create re-usable graphs and visualize metrics and logs side by side to troubleshoot

Understand root cause
Correlate metrics and logs together to diagnose

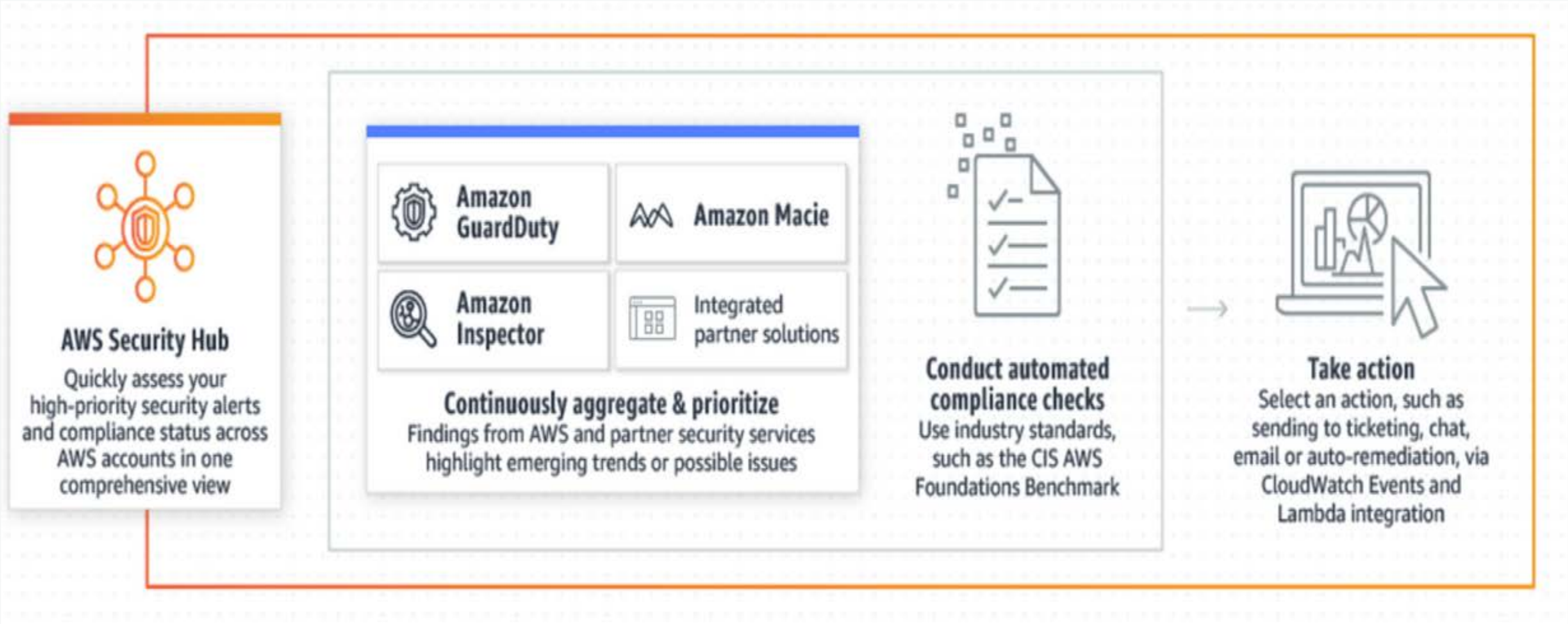
Optimize operational health
Resolve performance issue

Governance & compliance

4

Governance & Compliance

Resource inventory, configuration change tracking, user activity and AWS API call recording, and self-service IT catalogs for organizations.



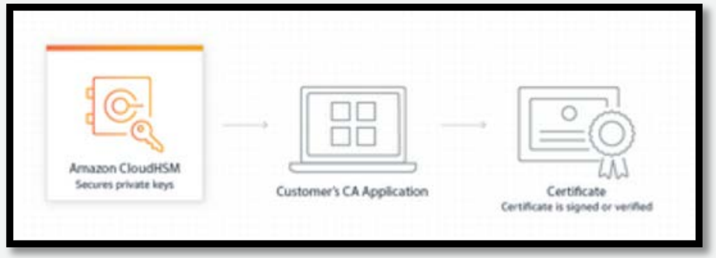
AWS Security Hub
Quickly assess your high-priority security alerts and compliance status across AWS accounts in one comprehensive view

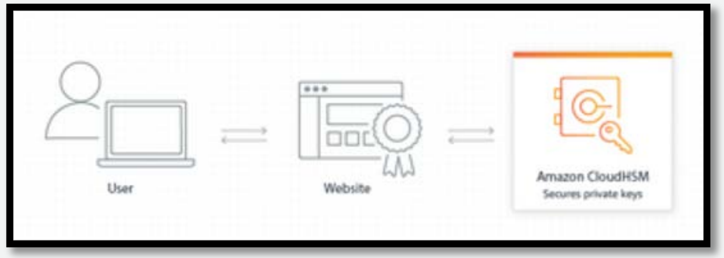
Continuously aggregate & prioritize
Findings from AWS and partner security services highlight emerging trends or possible issues

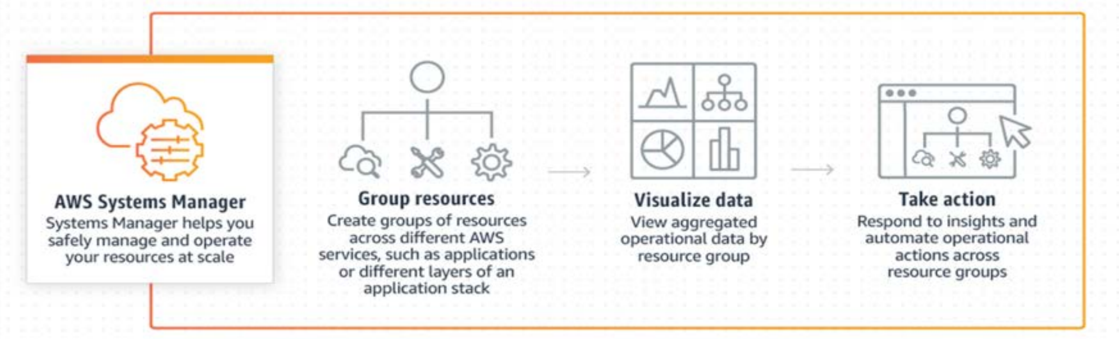
Conduct automated compliance checks
Use industry standards, such as the CIS AWS Foundations Benchmark

Take action
Select an action, such as sending to ticketing, chat, email or auto-remediation, via CloudWatch Events and Lambda integration

AWS CloudHSM is a cloud-based hardware security module (HSM)







AWS Systems Manager
Systems Manager helps you safely manage and operate your resources at scale

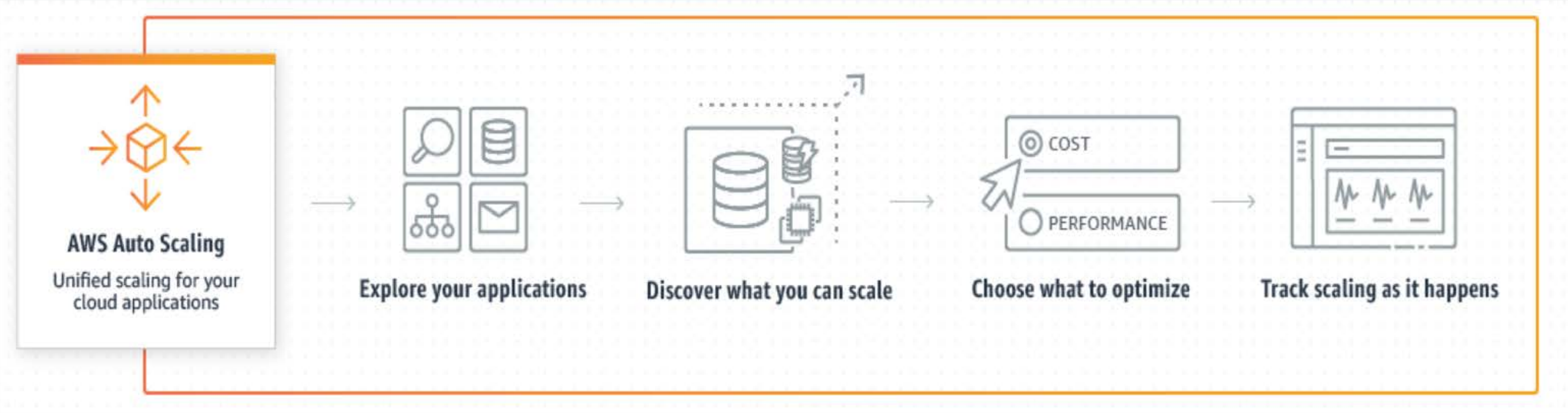
Group resources
Create groups of resources across different AWS services, such as applications or different layers of an application stack

Visualize data
View aggregated operational data by resource group

Take action
Respond to insights and automate operational actions across resource groups

Resource optimization

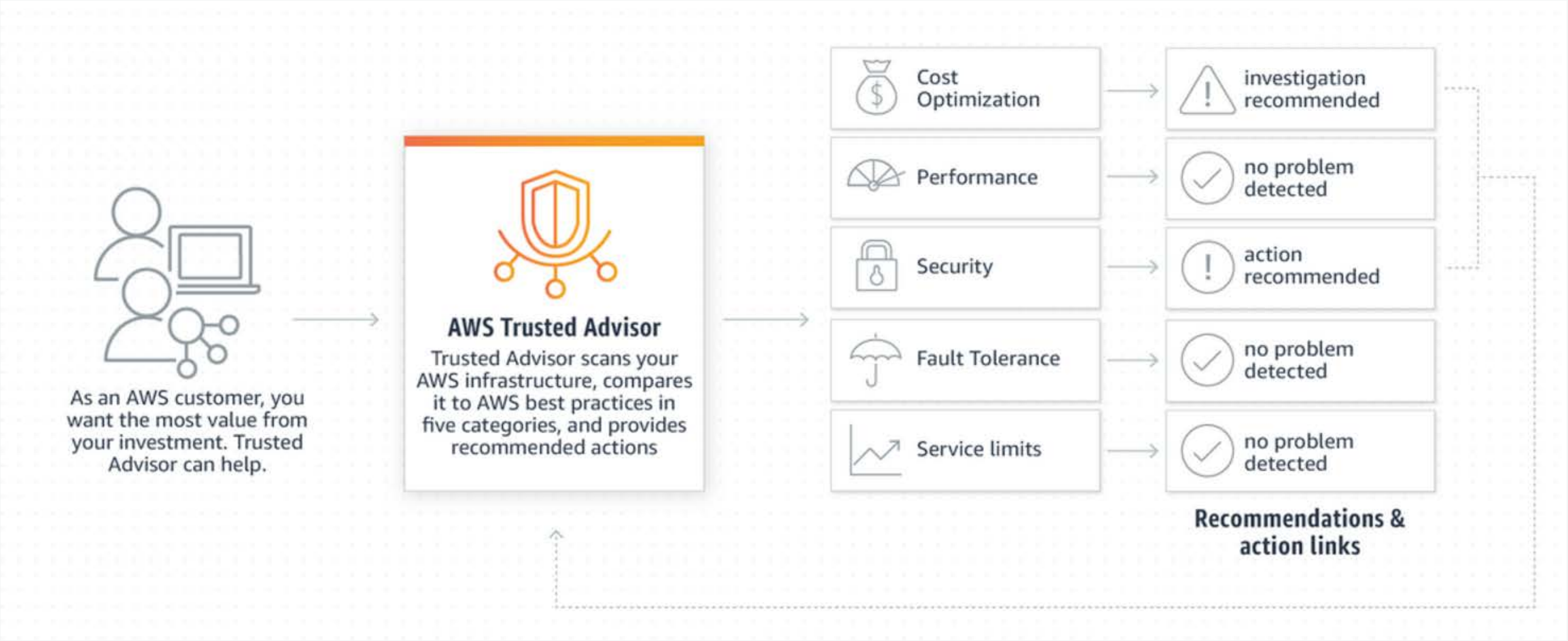
Automated recommendations to reduce costs, increase performance, and improve security



AWS Auto Scaling

Unified scaling for your cloud applications

→ Explore your applications → Discover what you can scale → Choose what to optimize → Track scaling as it happens



As an AWS customer, you want the most value from your investment. Trusted Advisor can help.

→ **AWS Trusted Advisor**

Trusted Advisor scans your AWS infrastructure, compares it to AWS best practices in five categories, and provides recommended actions

Cost Optimization	→ investigation recommended
Performance	→ no problem detected
Security	→ action recommended
Fault Tolerance	→ no problem detected
Service limits	→ no problem detected

Recommendations & action links

Thank you

Alexis Robinson

Technical Program Manager, Government Audits

Tim Sandage

Senior Security Partner Strategist