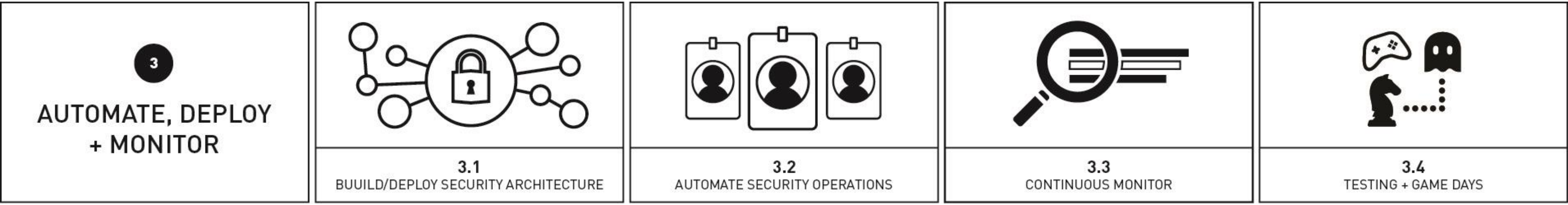
Security Automation & Orchestration (SAO)

MTG – Automate, Deploy and Monitor

Module – 3

2018

Build Security Automation



3

AUTOMATE, DEPLOY + MONITOR

3.1 BUUILD/DEPLOY SECURITY ARCHITECTURE

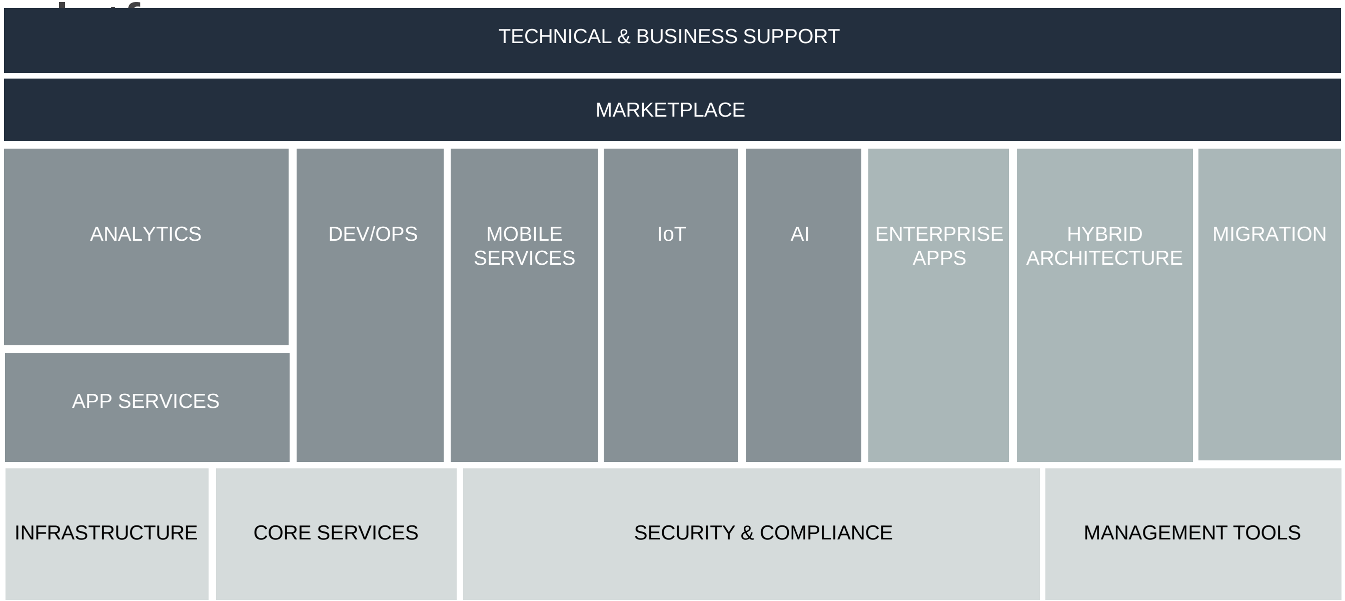
3.2 AUTOMATE SECURITY OPERATIONS

3.3 CONTINUOUS MONITOR

3.4 TESTING + GAME DAYS

Freedom to build, unfettered

Most robust, fully featured technology infrastructure



TECHNICAL & BUSINESS SUPPORT

MARKETPLACE

ANALYTICS

APP SERVICES

DEV/OPS

MOBILE SERVICES

IoT

AI

ENTERPRISE APPS

HYBRID ARCHITECTURE

MIGRATION

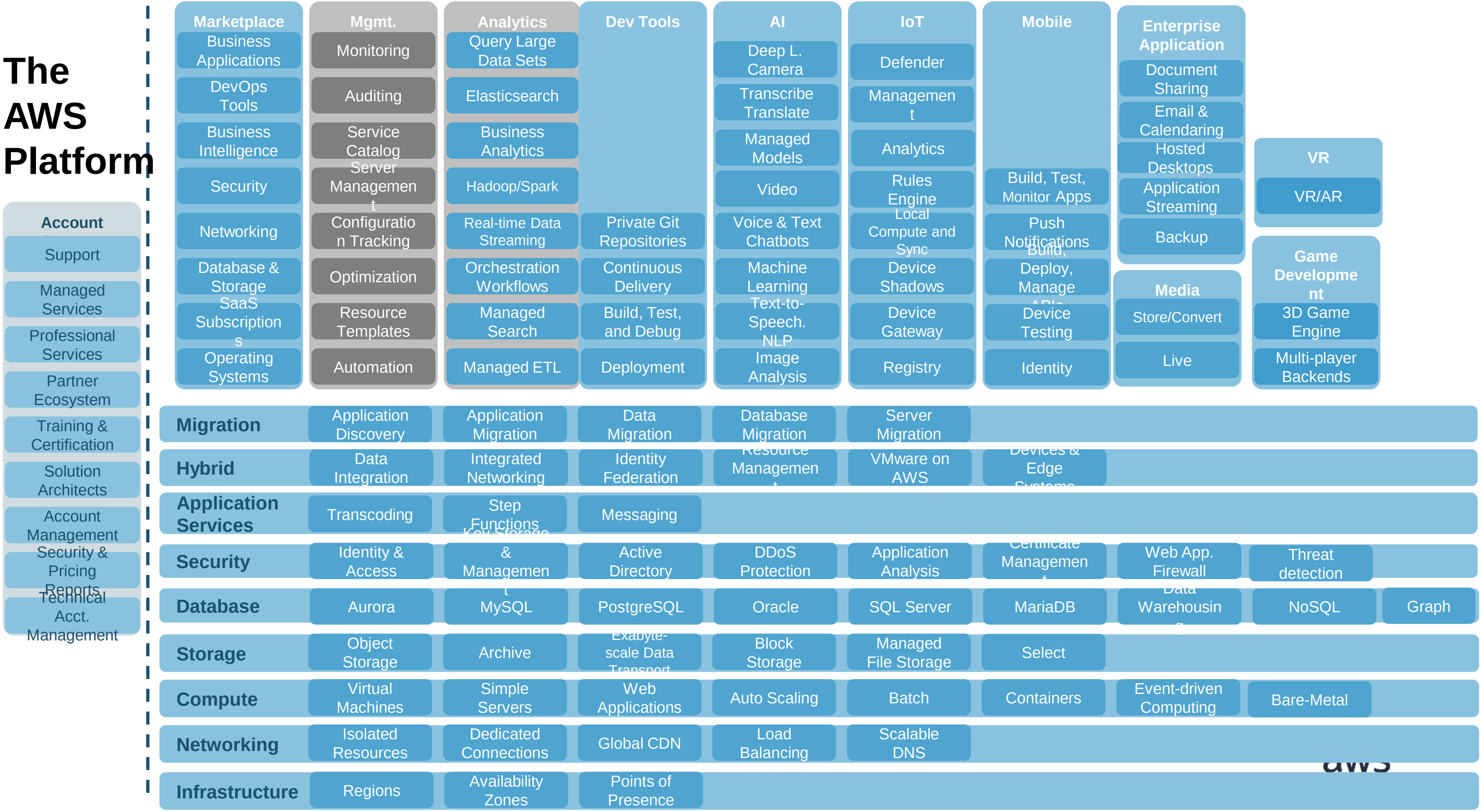
INFRASTRUCTURE

CORE SERVICES

SECURITY & COMPLIANCE

MANAGEMENT TOOLS

The AWS Platform



Account
- Support
- Managed Services
- Professional Services
- Partner Ecosystem
- Training & Certification
- Solution Architects
- Account Management
- Security & Pricing Reports
- Technical Acct. Management

Marketplace
- Business Applications
- DevOps Tools
- Business Intelligence
- Security
- Networking
- Database & Storage
- SaaS Subscription s
- Operating Systems

Mgmt.
- Monitoring
- Auditing
- Service Catalog
- Server Managemen t
- Configuratio n Tracking
- Optimization
- Resource Templates
- Automation

Analytics
- Query Large Data Sets
- Elasticsearch
- Business Analytics
- Hadoop/Spark
- Real-time Data Streaming
- Orchestration Workflows
- Managed Search
- Managed ETL

Dev Tools
- Private Git Repositories
- Continuous Delivery
- Build, Test, and Debug
- Deployment

AI
- Deep L. Camera
- Transcribe Translate
- Managed Models
- Video
- Voice & Text Chatbots
- Machine Learning
- Text-to-Speech. NLP
- Image Analysis

IoT
- Defender
- Managemen t
- Analytics
- Rules Engine
- Local Compute and Sync
- Device Shadows
- Device Gateway
- Registry

Mobile
- Build, Test, Monitor Apps
- Push Notifications
- Build, Deploy, Manage APIs
- Device Testing
- Identity

Enterprise Application
- Document Sharing
- Email & Calendaring
- Hosted Desktops
- Application Streaming
- Backup

Media
- Store/Convert
- Live

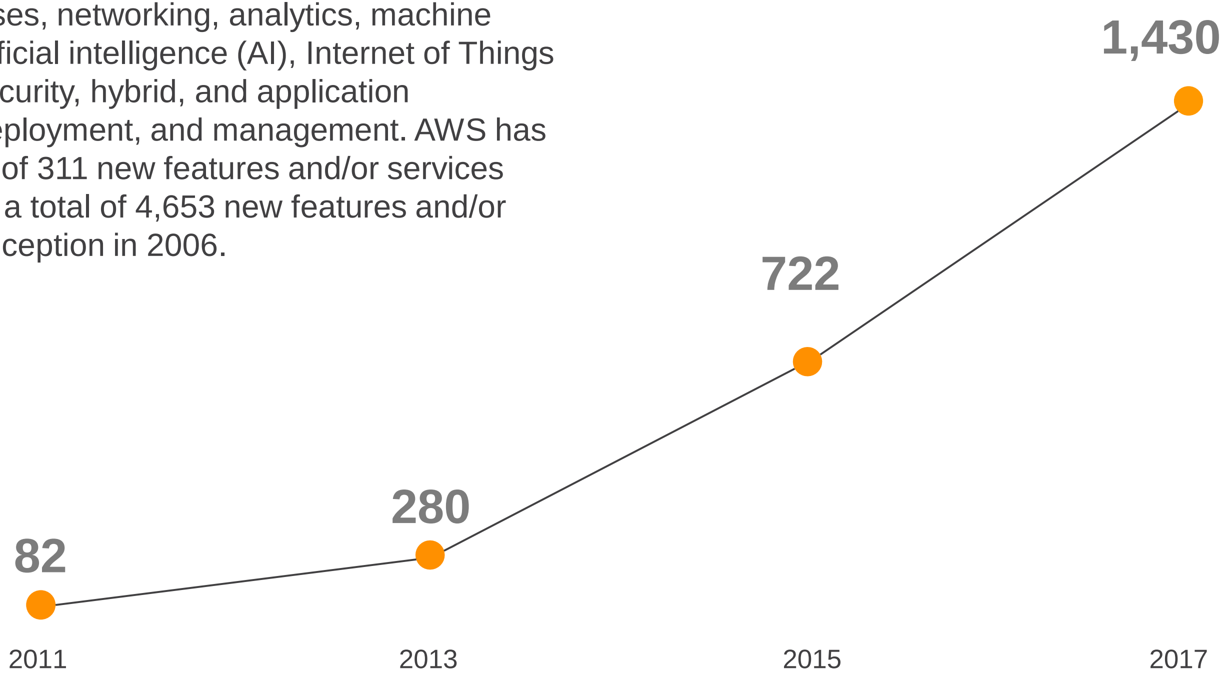
VR
- VR/AR

Game Developme nt
- 3D Game Engine
- Multi-player Backends

Migration	Application Discovery	Application Migration	Data Migration	Database Migration	Server Migration				
Hybrid	Data Integration	Integrated Networking	Identity Federation	Resource Managemen t	VMware on AWS	Devices & Edge Systems			
Application Services	Transcoding	Step Functions	Messaging						
Security	Identity & Access	Key Storage & Managemen t	Active Directory	DDoS Protection	Application Analysis	Certificate Managemen t	Web App. Firewall	Threat detection	
Database	Aurora	MySQL	PostgreSQL	Oracle	SQL Server	MariaDB	Data Warehousin g	NoSQL	Graph
Storage	Object Storage	Archive	Exabyte-scale Data Transport	Block Storage	Managed File Storage	Select			
Compute	Virtual Machines	Simple Servers	Web Applications	Auto Scaling	Batch	Containers	Event-driven Computing	Bare-Metal	
Networking	Isolated Resources	Dedicated Connections	Global CDN	Load Balancing	Scalable DNS				
Infrastructure	Regions	Availability Zones	Points of Presence						

AWS Pace of Innovation

AWS offers over 129 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, and application development, deployment, and management. AWS has launched a total of 311 new features and/or services year to date* for a total of 4,653 new features and/or services since inception in 2006.



* *As of 31 March 2018*

Schema Conversion Tool

AWS OpsWorks

CodeCommit

Amazon Inspector

Amazon Lightsail

AWS CodeDeploy

Amazon ElastiCache

AWS Storage Gateway

Amazon Config

Amazon Cognito

AWS Shield

EFS

Amazon Lumberyard

Amazon Appstream 2.0

AWS Elastic Beanstalk

AWS Batch

AWS Snowmobile

AWS Organizations

AWS Certificate Manager

AWS CodePipeline

Amazon Lex

AWS Managed Services

Redshift

Amazon Kinesis Firehose

4,653

Amazon Route 53

Lambda

AWS Glue

AWS X-Ray

Amazon Pinpoint

Dynamo DB

AWS Codebuild

AWS Snowball

Amazon Athena

Amazon Workmail

AWS WAF

AWS Snowball Edge

Amazon RDS for Aurora

AWS IoT

AWS OpsWorks for Chef Automate

Machine Learning

Amazon Rekognition

AWS Mobile Hub

Amazon Polly

WorkSpaces

AWS Greengrass

Device Farm

WorkDocs

Amazon QuickSight

CloudWatch Logs

Mobile Analytics

AWS Personal Health Dashboard

Amazon EC2 Systems Manager

AWS Direct Connect

Amazon Inspector

AWS Discovery Services

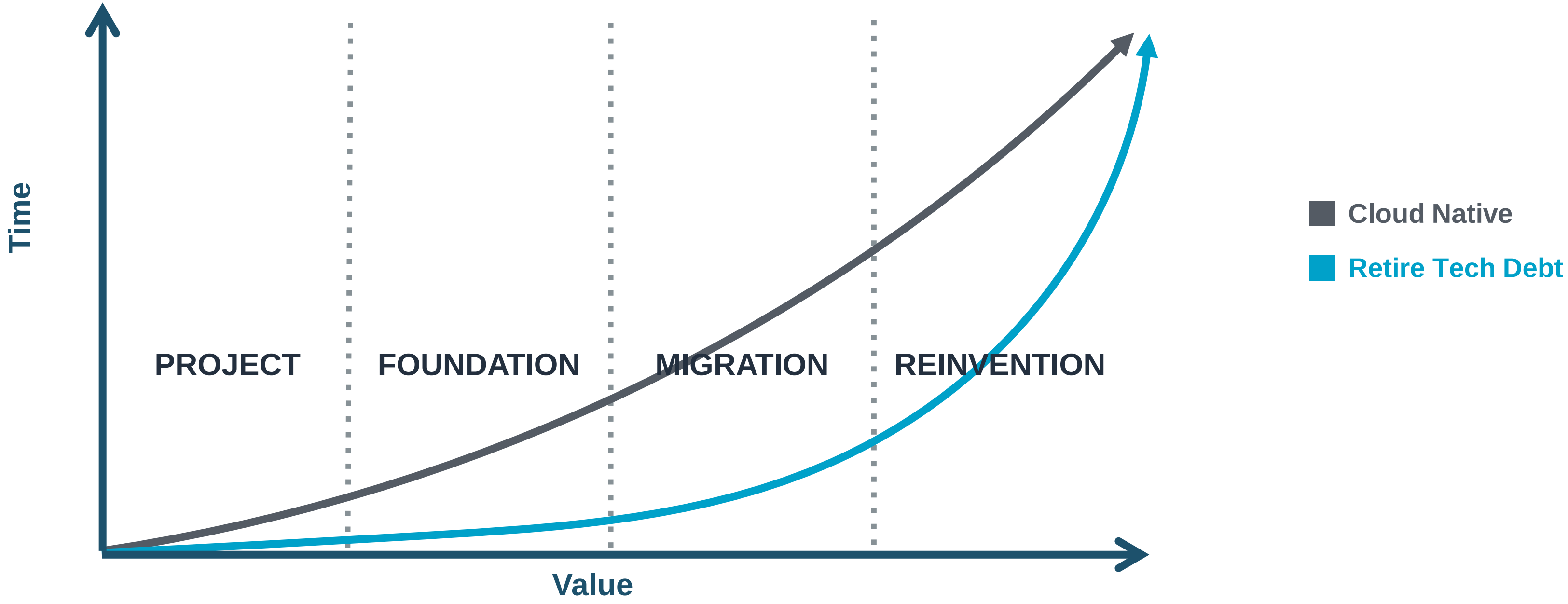
AWS Service Catalog

AWS Import/Export

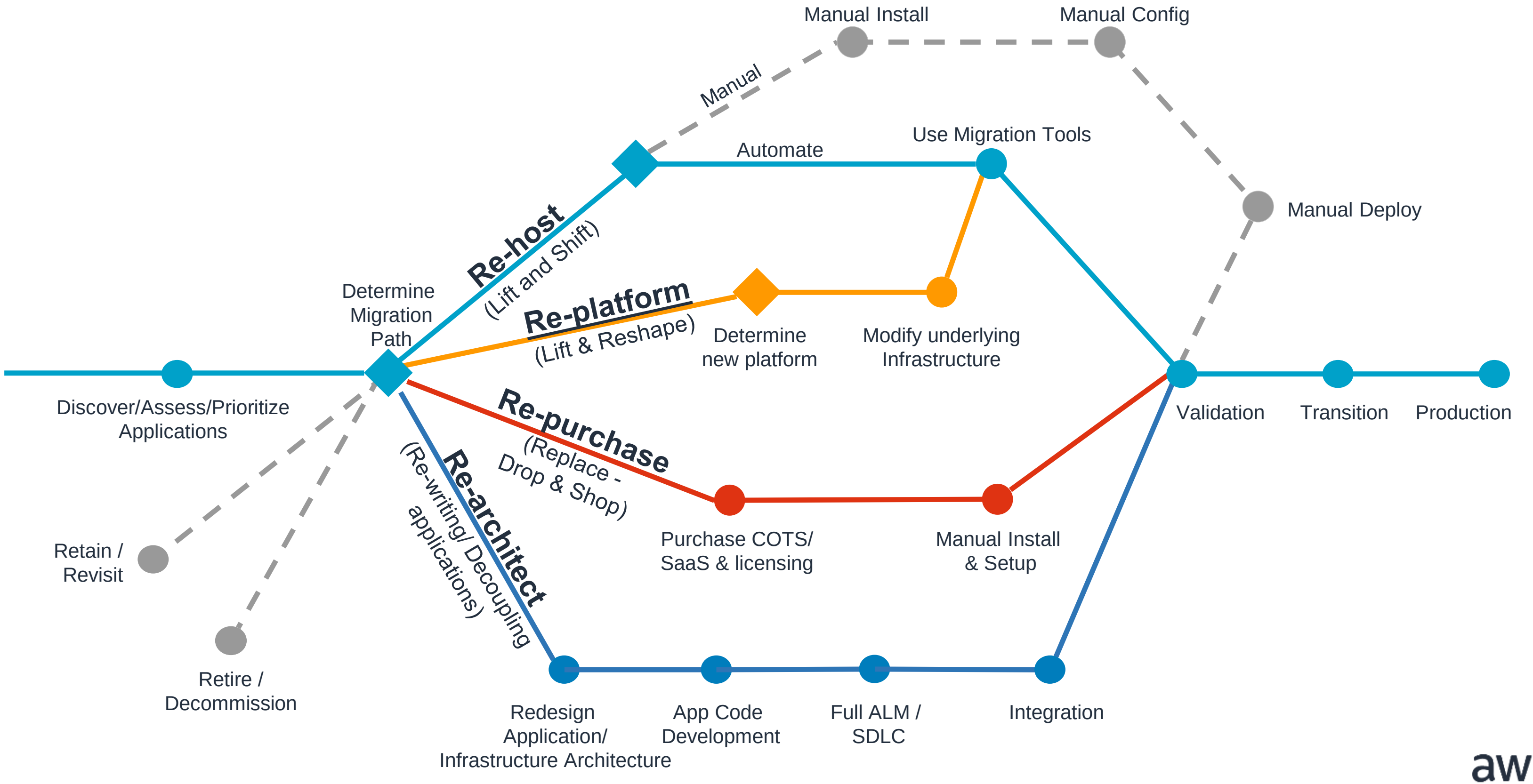
AWS Step Functions

** As of 31 March 2018*

Where are you on your journey?



Application migration patterns



Move fast. AND Stay secure.

allOfThis == $Code

https://secure.flickr.com/photos/wscullin/3770015991

Infrastructure as Code is a practice by where traditional infrastructure management techniques are supplemented and often replaced by using code based tools and software development techniques.

AWS CloudFormation

- Create templates that describe and model AWS infrastructure
- CloudFormation then provisions AWS resources based on dependency needs
- Version control/replicate/update the templates like app code
- Integrates with development, CI/CD, management tools
- No additional charge to use

Benefits

Templated resource provisioning

Infrastructure as code

Declarative and flexible

Easy to use

CloudFormation concepts and technology

Template

- JSON formatted file
- Parameter definition
- Resource creation
- Configuration actions

CloudFormation

- Framework
- Stack creation
- Stack updates
- Error detection and rollback

Stack

- Configured AWS resources
- Comprehensive service support
- Service event aware
- Customizable

Anatomy of a CloudFormation template: JSON

Plain Text

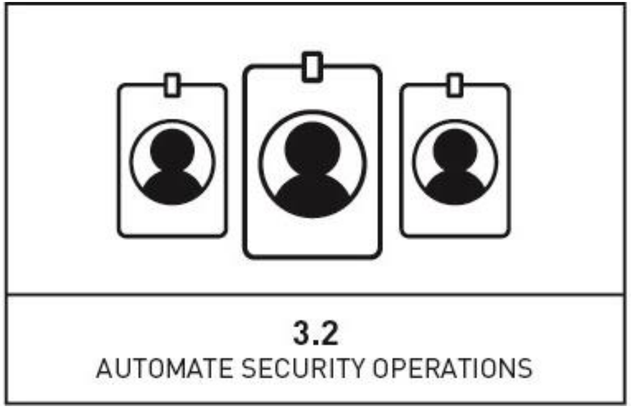
Perfect for version control

Can be validated

Template components

Headers	Description of what your stack does, contains, etc
Parameters	Provision time values that add structured flexibility and customization
Mappings	Pre-defined conditional case statements
Conditionals	Conditional values set via evaluations of passed references
Resources	AWS resource definitions
Outputs	Resulting attributes of stack resource creation

Automating Security Operations



How is Security in the Cloud Different?
Security as code!

1. Use the cloud to protect the cloud
2. Security infrastructure should be cloud aware
3. Expose security features as services via API
4. Automate everything so everything scales

Shared responsibility model

Customer

Responsible for security
IN the cloud

- Customer Data
- Platform, Applications, Identity & Access Management
- Operating System, Network & Firewall Configuration
- Client-side Data Encryption & Data Integrity Authentication
- Server-side Encryption (File System and/or Data)
- Network Traffic Protection (Encryption, Integrity, and/or Identity)

Compute

Responsible for security
OF the cloud

- Compute
- Storage
- Database
- Networking

- AWS Global Infrastructure
- Regions
- Availability Zones
- Edge Locations

Strengthen your security posture

- Over 60 global compliance certifications and accreditations
- Benefit from AWS industry leading security teams 24/7, 365 days a year
- Security infrastructure built to satisfy military, global banks, and other high-sensitivity organizations
- Leverage security enhancements from 1M+ customer experiences

> ” In the last four years as we transitioned to the cloud, I have come to realize that as a relatively small organization, we can be far more secure in the cloud and achieve a higher level of assurance at a much lower cost, in terms of effort and dollars invested. We determined that security in AWS is superior to our on-premises data center across several dimensions, including patching, encryption, auditing and logging, entitlements, and compliance.

John Brady
FINRA CISO

Access a deep set of cloud security tools

Networking

Virtual Private Cloud
Isolated cloud resources

Web Application Firewall
Filter Malicious Web Traffic

Shield
DDoS protection

Certificate Manager
Provision, manage, and deploy SSL/TSL certificates

Encryption

Key Management Service
Manage creation and control of encryption keys

CloudHSM
Hardware-based key storage

Server-Side Encryption
Flexible data encryption options

Identity & Management

IAM
Manage user access and encryption keys

SAML Federation
SAML 2.0 support to allow on-prem identity integration

Directory Service
Host and manage Microsoft Active Directory

Organizations
Manage settings for multiple accounts

Compliance

Service Catalog
Create and use standardized products

Config
Track resource inventory and changes

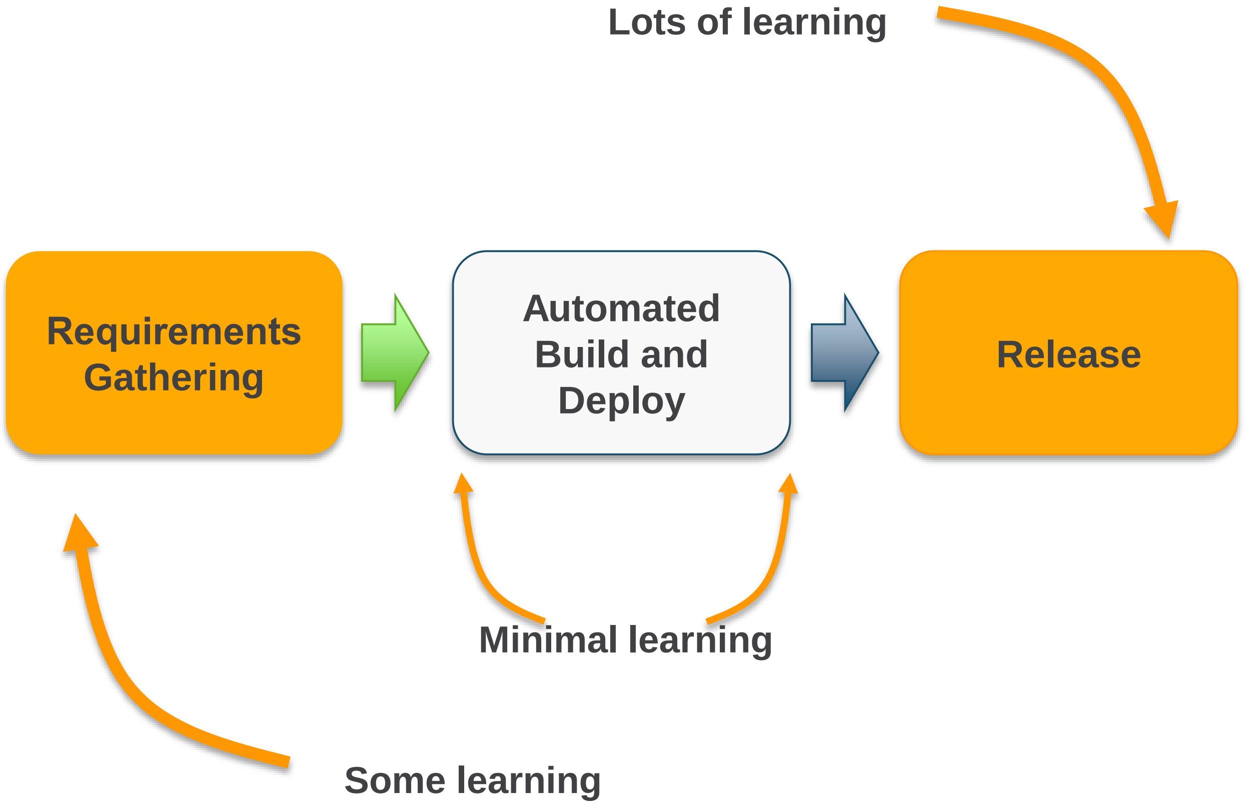
CloudTrail
Track user activity and API usage

CloudWatch
Monitor resources and applications

Inspector
Analyze application security

Macie
Discover, Classify & Protect data

Cloud Risk Management:



Lots of learning

Requirements Gathering

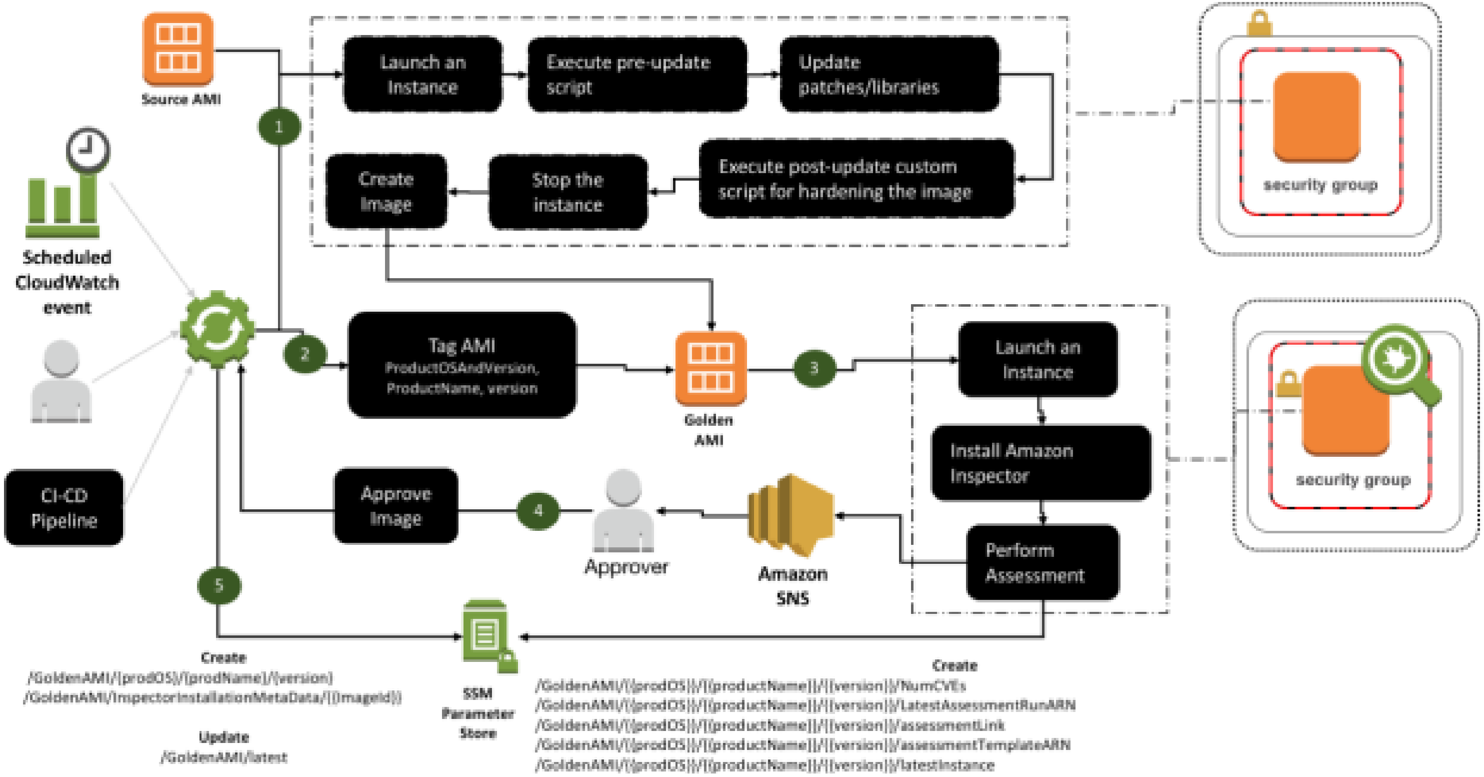
Automated Build and Deploy

Release

Minimal learning

Some learning

Here is the Architecture diagram for golden AMI creation process.



Source AMI

1

Launch an Instance

Execute pre-update script

Update patches/libraries

Execute post-update custom script for hardening the image

Stop the instance

Create Image

security group

Scheduled CloudWatch event

CI-CD Pipeline

2

Tag AMI
ProductOSAndVersion, ProductName, version

Golden AMI

3

Launch an Instance

Install Amazon Inspector

Perform Assessment

security group

Amazon SNS

Approver

4

Approve Image

5

SSM Parameter Store

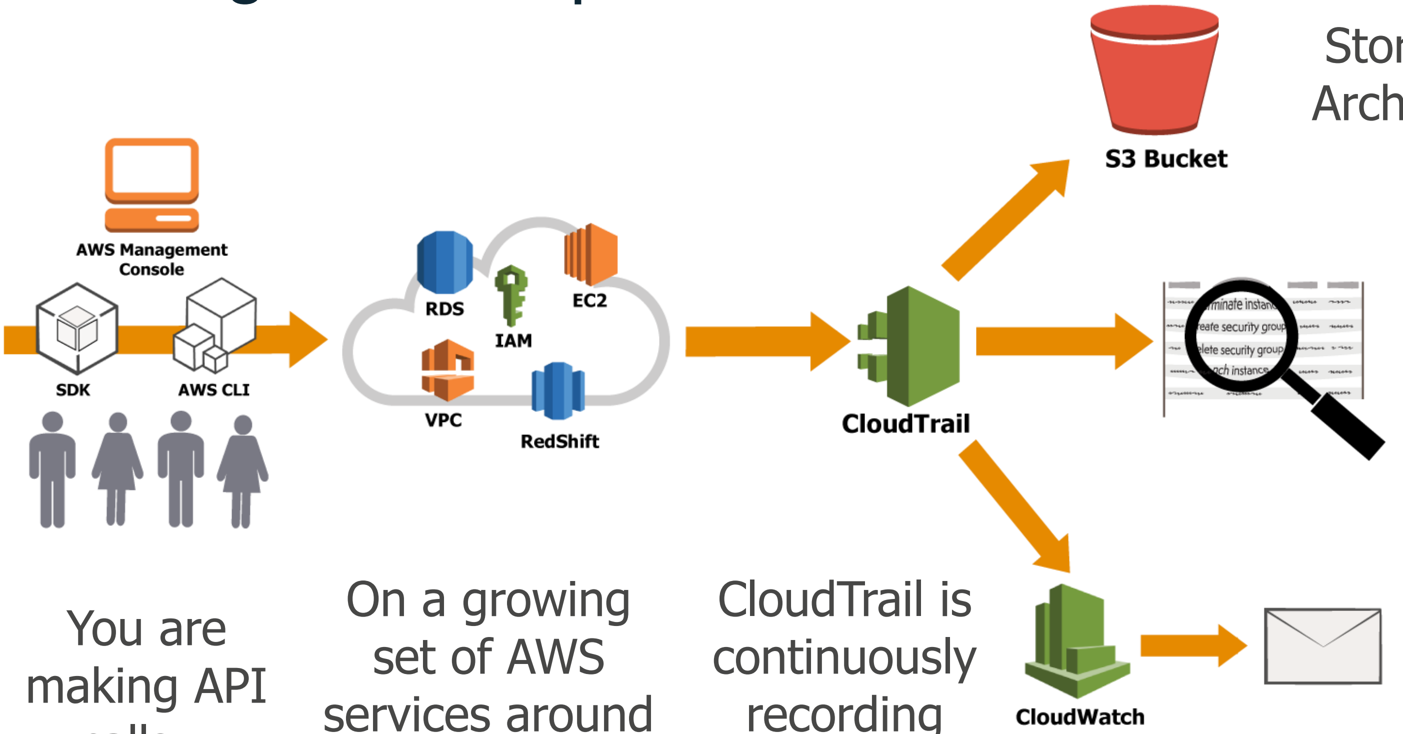
Create
/GoldenAMI/{{prodOS}}/{{prodName}}/{{version}}
/GoldenAMI/InspectorInstallationMetaData/{{imageId}}

Update
/GoldenAMI/latest

Create
/GoldenAMI/{{prodOS}}/{{productName}}/{{version}}/NumCVEs
/GoldenAMI/{{prodOS}}/{{productName}}/{{version}}/LatestAssessmentRunARN
/GoldenAMI/{{prodOS}}/{{productName}}/{{version}}/assessmentLink
/GoldenAMI/{{prodOS}}/{{productName}}/{{version}}/assessmentTemplateARN
/GoldenAMI/{{prodOS}}/{{productName}}/{{version}}/latestInstance

3.3
CONTINUOUS MONITOR

Audit logs for all operations



You are making API calls...

On a growing set of AWS services around the world..

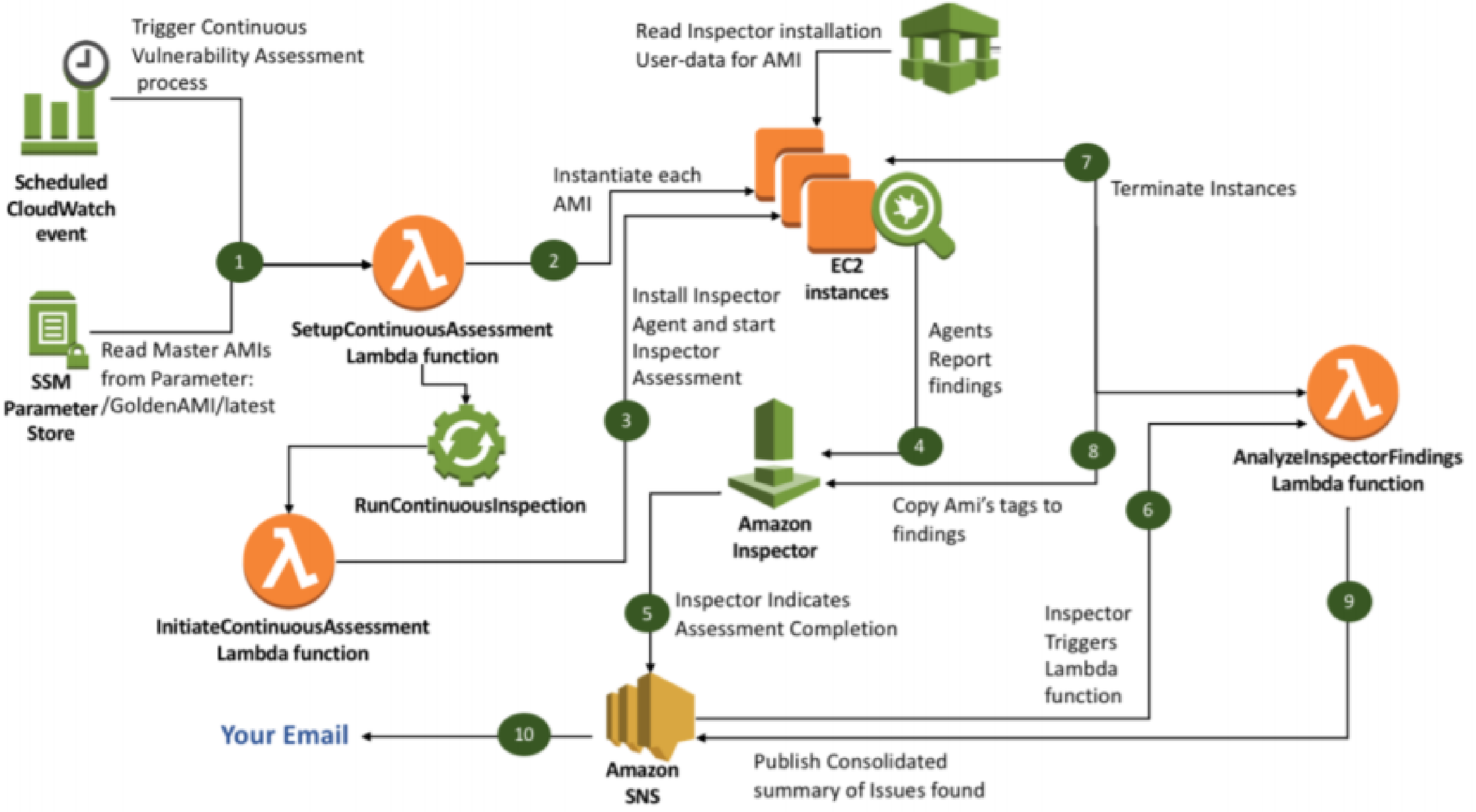
CloudTrail is continuously recording API calls

Store/ Archive

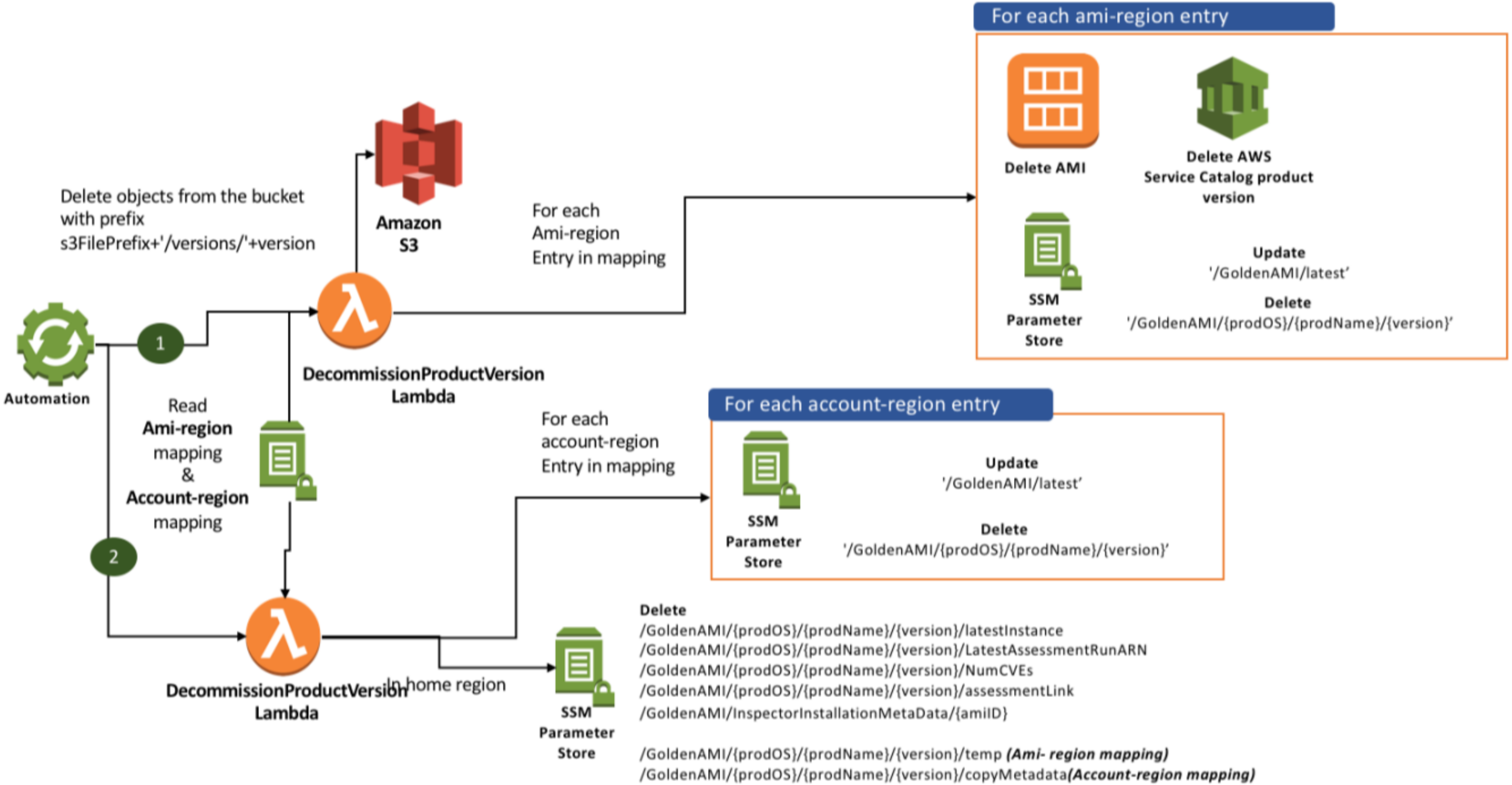
Troubleshoot

Monitor & Alarm

Continuous Inspection of a Golden AMI


Trigger Continuous Vulnerability Assessment process
Scheduled CloudWatch event
1
SSM Parameter Store
Read Master AMIs from Parameter: /GoldenAMI/latest
SetupContinuousAssessment Lambda function
2
Instantiate each AMI
Read Inspector installation User-data for AMI
EC2 instances
7
Terminate Instances
Install Inspector Agent and start Inspector Assessment
Agents Report findings
RunContinuousInspection
3
Amazon Inspector
4
8
Copy Ami's tags to findings
AnalyzeInspectorFindings Lambda function
6
InitiateContinuousAssessment Lambda function
5
Inspector Indicates Assessment Completion
Inspector Triggers Lambda function
9
Your Email
10
Amazon SNS
Publish Consolidated summary of Issues found

Decommissioning a Golden AMI



For each ami-region entry

Delete AMI

Delete AWS Service Catalog product version

SSM Parameter Store

Update '/GoldenAMI/latest'

Delete '/GoldenAMI/{prodOS}/{prodName}/{version}'

Delete objects from the bucket with prefix s3FilePrefix+'/versions/'+version

Amazon S3

For each Ami-region Entry in mapping

Automation

1

DecommissionProductVersion Lambda

Read **Ami-region** mapping & **Account-region** mapping

For each account-region Entry in mapping

For each account-region entry

SSM Parameter Store

Update '/GoldenAMI/latest'

Delete '/GoldenAMI/{prodOS}/{prodName}/{version}'

2

DecommissionProductVersion Lambda

In home region

SSM Parameter Store

Delete
/GoldenAMI/{prodOS}/{prodName}/{version}/latestInstance
/GoldenAMI/{prodOS}/{prodName}/{version}/LatestAssessmentRunARN
/GoldenAMI/{prodOS}/{prodName}/{version}/NumCVEs
/GoldenAMI/{prodOS}/{prodName}/{version}/assessmentLink
/GoldenAMI/InspectorInstallationMetaData/{amiID}

/GoldenAMI/{prodOS}/{prodName}/{version}/temp ***(Ami- region mapping)***
/GoldenAMI/{prodOS}/{prodName}/{version}/copyMetadata***(Account-region mapping)***

Questions?