

The logo for AWS Summit, featuring the lowercase text 'aws' with the Amazon arrow logo underneath it, followed by the word 'SUMMIT' in all caps. The background is a dark blue gradient with abstract, flowing shapes in shades of purple and blue.

aws SUMMIT

WASHINGTON DC |

SEC201

# Scaling automated governance with Landing Zone Accelerator on AWS

Mark Burr

Global Leader - Technology,  
Solutions and Delivery,  
AWS Professional Services  
Amazon Web Services

Randy Domingo

Principal Engineer, AWS  
Professional Services  
Amazon Web Services



**AWS gets customers at least 60% along their compliance journey in terms of security controls**

# Compliance requirements

- ✓ Personnel
- ✓ Incident response
- ✓ Boundary protection
- ✓ Identity and access control
- ✓ Disaster recovery
- ✓ Configuration management
- ✓ Highly available architecture
- ✓ System management & monitoring
- ✓ Log management & monitoring
- ✓ Compute and storage
- ✓ Networking
- ✓ Virtualization
- ✓ Data center

# Organizations need better visibility and security to optimize their next-gen cloud applications



Increase operational efficiency for your cloud-based workloads and applications



Improve visibility









Enhance security posture

# Use AWS services to achieve operational excellence in securing your cloud environment



- Centralize threat detection and monitoring
- Improve security posture assessment
- Optimize vulnerability management
- Streamline root cause analysis
- Improve sensitive data discovery
- Initiate and route workflows to existing systems
- Prioritize critical findings
- Automate remediation
- Scale deployments

# AWS security, identity, and compliance solutions

 <b>Identity &amp; access management</b>	 <b>Detection</b>	 <b>Infrastructure protection</b>	 <b>Data protection</b>	 <b>Incident response</b>	 <b>Compliance</b>
<ul style="list-style-type: none"> <li>AWS Identity &amp; Access Management (IAM)</li> <li>AWS Single Sign-On</li> <li>AWS Organizations</li> <li>AWS Directory Service</li> <li>Amazon Cognito</li> <li>AWS Resource Access Manager (AWS RAM)</li> </ul>	<ul style="list-style-type: none"> <li>AWS Security Hub</li> <li>Amazon GuardDuty</li> <li>Amazon Inspector</li> <li>Amazon CloudWatch</li> <li>AWS Config</li> <li>AWS CloudTrail</li> <li>VPC flow logs</li> <li>AWS IoT Device Defender</li> </ul>	<ul style="list-style-type: none"> <li>AWS Firewall Manager</li> <li>AWS Network Firewall</li> <li>AWS Shield</li> <li>AWS WAF – web application firewall</li> <li>Amazon Virtual Private Cloud (Amazon VPC)</li> <li>AWS PrivateLink</li> <li>AWS Systems Manager</li> </ul>	<ul style="list-style-type: none"> <li>Amazon Macie</li> <li>AWS Key Management Service (AWS KMS)</li> <li>AWS CloudHSM</li> <li>AWS Certificate Manager</li> <li>AWS Secrets Manager</li> <li>AWS VPN</li> <li>Server-side encryption</li> </ul>	<ul style="list-style-type: none"> <li>Amazon Detective</li> <li>CloudEndure Disaster Recovery</li> <li>AWS Config rules</li> <li>AWS Lambda</li> </ul>	<ul style="list-style-type: none"> <li>AWS Artifact</li> <li>AWS Audit Manager</li> </ul>

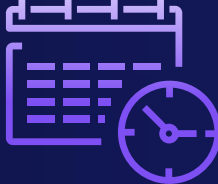
# Now, more than ever, organizations need strong foundational architectures



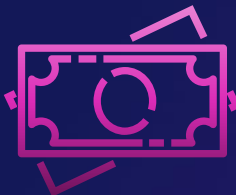
High performing



Secure



Reliable



Cost-efficient



Sustainable

# The architectural best practices portfolio

ACCELERATE CLOUD ADOPTION WITH CONFIDENCE

## EXPERTISE



### AWS Well-Architected

Improve operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability



### Sustainable architecture

Enhance sustainability in the cloud via energy reduction and workload efficiency



### AWS solutions

Deploy turnkey solutions or kick-start the building process with preconfigured architecture patterns



### Architecture center

Access a robust content library, including reference architecture diagrams, best practices, and more

## AWS SERVICES



# Build a secure foundation



# You need a landing zone

- A secure, scalable, multi-account AWS environment based on AWS best practices
- A starting point for net new development and experimentation
- A starting point for migrating applications
- An environment that allows for iteration and extension over time



# Landing zone elements

Secure and  
compliant

Meets the organization's  
security and auditing  
requirements

Scalable and  
resilient

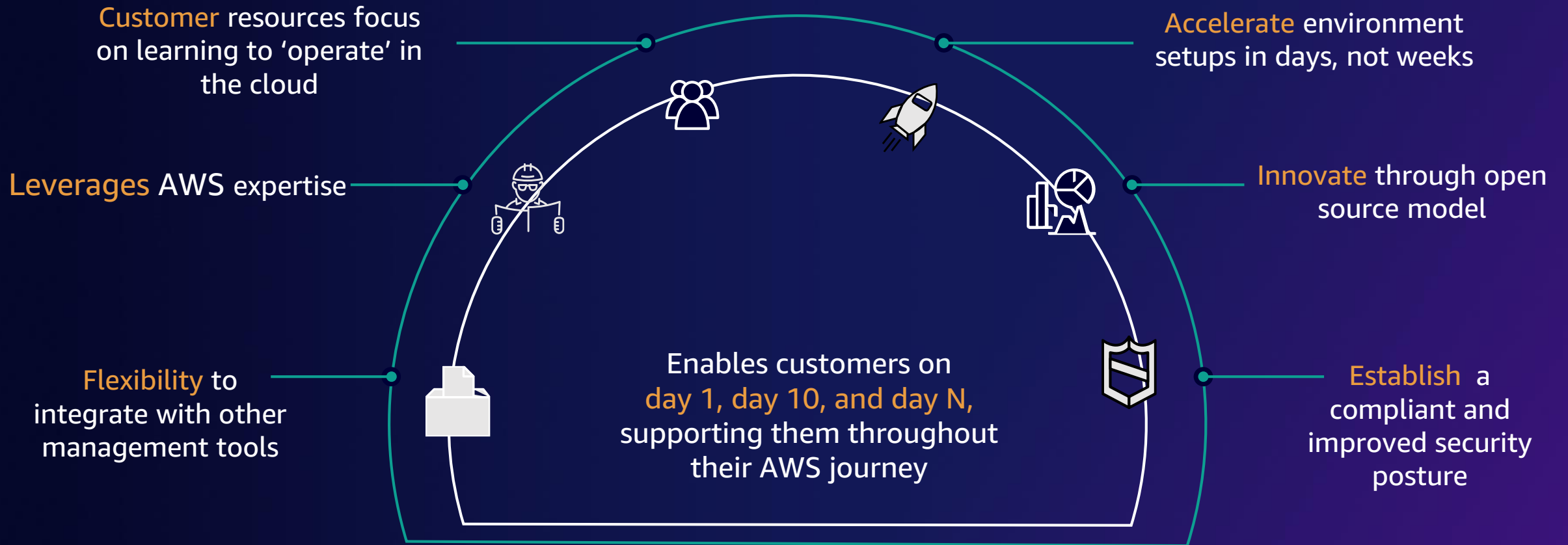
Ready to support  
highly available and  
scalable workloads

Adaptable and  
flexible

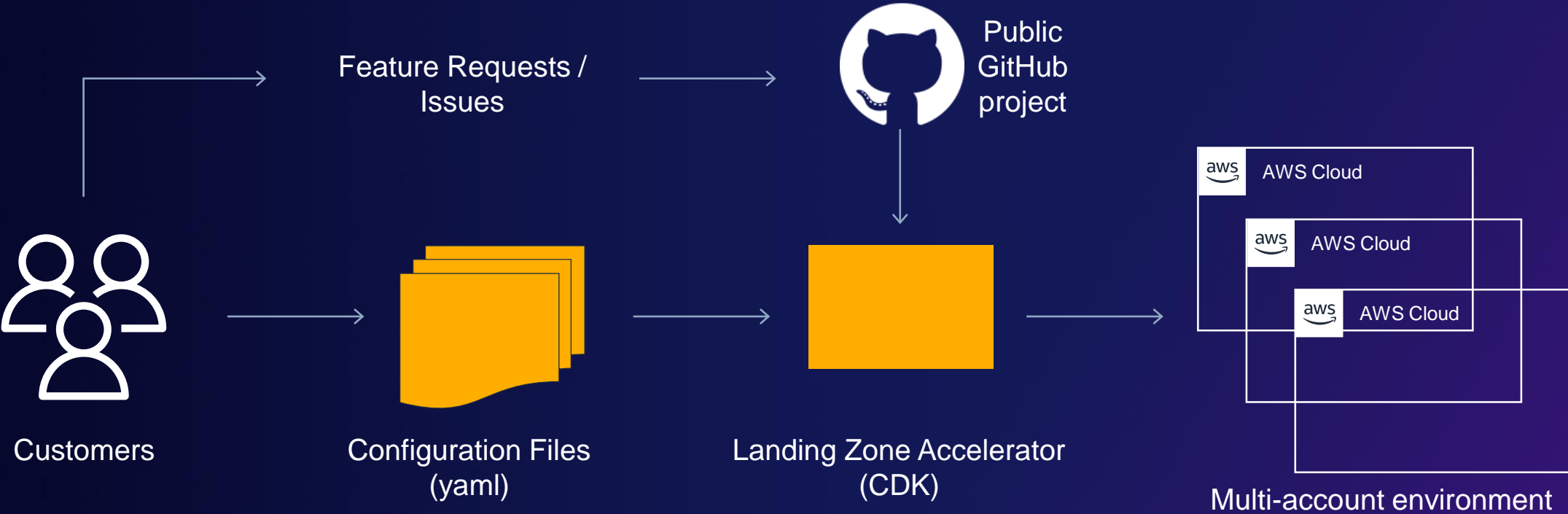
Configurable to  
support evolving  
mission requirements

**The **Landing Zone Accelerator on AWS** is an open source software solution that accelerates the implementation of a customer's technical security controls and infrastructure foundation on AWS**

# Landing Zone Accelerator Benefits



# Architecture



# Landing Zone Accelerator on AWS

1



Installation Template  
(AWS CloudFormation)

2



Configuration Files  
(yaml)

3



AWS CodePipeline

4



AWS Cloud  
Development Kit

Landing Zone  
Accelerator



# Landing Zone Accelerator on AWS

1



Installation Template  
(AWS CloudFormation)

2



Configuration Files  
(yaml)

3



AWS CodePipeline

4



AWS Cloud  
Development Kit

Landing Zone  
Accelerator

```
enable: true
organizationalUnits:
  - name: Security
  - name: Infrastructure
  - name: Dev
  - name: Test
  - name: Prod
serviceControlPolicies:
  - name: AcceleratorGuardrails1
    description: Accelerator GuardRails 1
    policy: service-control-policies/guardrails-1.json
    type: customerManaged
    deploymentTargets:
      organizationalUnits:
        - Infrastructure
        - name: AcceleratorGuardrails2
taggingPolicies:
  - name: TagPolicy
    description: Organization Tagging Policy
    policy: tagging-policies/org-tag-policy.json
    deploymentTargets:
      organizationalUnits:
        - Root
backupPolicies:
  - name: BackupPolicy
    description: Organization Backup Policy
    policy: backup-policies/org-backup-policies.json
    deploymentTargets:
      organizationalUnits:
        - Root
```

```
mandatoryAccounts:
  - name: Management
    email: example-management-root-account@amazon.com
    organizationalUnit: Root
  - name: LogArchive
    email: example-log-archive-account@amazon.com
    organizationalUnit: Security
  - name: Audit
    email: example-audit-account@amazon.com
    organizationalUnit: Security
workloadAccounts:
  - name: SharedServices
    email: example-shared-service-accounts@amazon.com
    organizationalUnit: Infrastructure
  - name: Network
    email: example-network-account@amazon.com
    organizationalUnit: Infrastructure
```

# Landing Zone Accelerator on AWS

1



Installation Template  
(AWS CloudFormation)

2



Configuration Files  
(yaml)

3



AWS CodePipeline

4



AWS Cloud  
Development Kit

Landing Zone  
Accelerator

Root OU



Management (Root) Account

Security OU



Log Archive Account

Infrastructure OU



Network Account



Audit / Security Tooling Account



Shared Services Account

Dev / Test / Prod OU (Workload Ous)



Workload Account 1 ... N

\*For illustration only to demonstrate where these  
additional capabilities and resources can be deployed



# Landing Zone Accelerator on AWS

1



Installation Template  
(AWS CloudFormation)

2



Configuration Files  
(yaml)

3



AWS CodePipeline

4



AWS Cloud  
Development Kit

Landing Zone  
Accelerator

```
homeRegion: &HOME_REGION us-east-1
centralSecurityServices:
  delegatedAdminAccount: Audit
  ebsDefaultVolumeEncryption:
    enable: true
    excludeRegions: []
  s3PublicAccessBlock:
    enable: true
    excludeAccounts: []
  macie:
    enable: true
  ...
  guardduty:
    enable: true
  ...
  securityHub:
    enable: true
    regionAggregation: true
    excludeRegions: []
    standards:
      - name: AWS Foundational Security Best Practices v1.0.0
        enable: true
        controlsToDisable:
          - IAM.1
          - EC2.10
          - Lambda.4
  ssmAutomation:
  ...
  accessAnalyzer:
    enable: true
  ...
```

```
iamPasswordPolicy:
  allowUsersToChangePassword: true
  hardExpiry: false
  requireSymbols: true
  requireNumbers: true
  minimumPasswordLength: 14
  passwordReusePrevention: 24
  maxPasswordAge: 90
awsConfig:
  enableConfigurationRecorder: true
  enableDeliveryChannel: true
  ruleSets:
    - deploymentTargets:
        organizationalUnits:
          - Root
      rules:
        - name: accelerator-iam-user-group-membership-check
          complianceResourceTypes:
            - AWS::IAM::User
          identifier: IAM_USER_GROUP_MEMBERSHIP_CHECK
        - name: accelerator-securityhub-enabled
          identifier: SECURITYHUB_ENABLEDcloudwatch:
metricSets:
  - regions:
      - *HOME_REGION
    deploymentTargets:
      - Root
    metrics:
      # CIS 1.1 - Avoid the use of the "root" account
      - filterName: RootAccountMetricFilter
        logGroupName: aws-controltower/CloudTrailLogs
        filterPattern: '${$.userIdentity.type="Root"}'
        metricNamespace: LogMetrics
        metricName: RootAccount
        metricValue: "1"
```

# Landing Zone Accelerator on AWS

1



Installation Template  
(AWS CloudFormation)

2



Configuration Files  
(yaml)

3



AWS CodePipeline

4



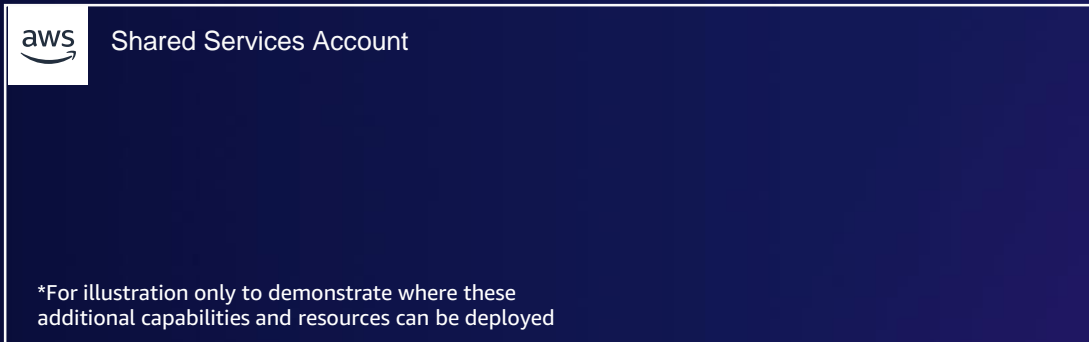
AWS Cloud  
Development Kit

Landing Zone  
Accelerator

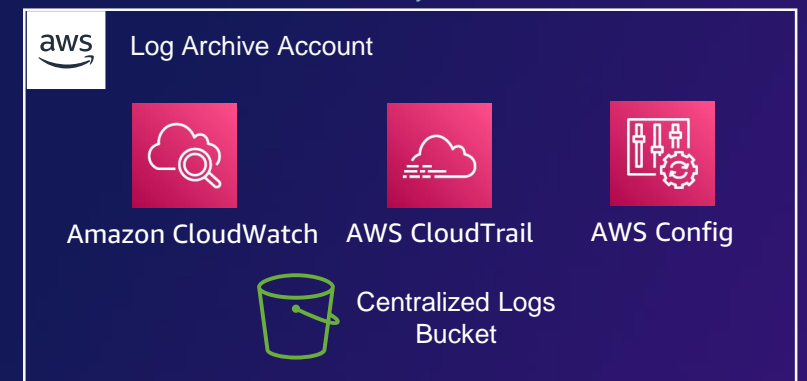
Root OU



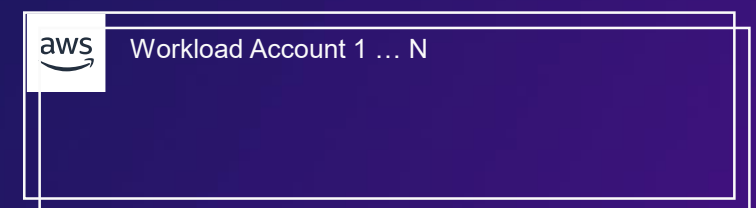
Infrastructure OU



Security OU



Dev / Test / Prod OU (Workload Ous)



# Landing Zone Accelerator on AWS

1



Installation Template  
(AWS CloudFormation)

2



Configuration Files  
(yaml)

3



AWS CodePipeline

4



AWS Cloud  
Development Kit

Landing Zone  
Accelerator

```
homeRegion: &HOME_REGION us-east-1
defaultVpc:
  delete: true
  excludeAccounts: []
transitGateways:
  - name: Network-Main
    account: Network
    region: *HOME_REGION
    shareTargets:
      organizationalUnits:
        - Infrastructure
    asn: 65521
    dnsSupport: enable
    vpnEcmpSupport: enable
    defaultRouteTableAssociation: disable
    defaultRouteTablePropagation: disable
    autoAcceptSharingAttachments: enable
    routeTables:
      - name: Network-Main-Core
        routes: []
      - name: Network-Main-Segregated
        routes: []
      - name: Network-Main-Shared
        routes: []
      - name: Network-Main-Standalone
        routes: []
```

vpcs:

```
- name: Network-Endpoints
  account: Network
  region: *HOME_REGION
  cidrs:
    - 10.1.0.0/22
  internetGateway: false
  enableDnsHostnames: true
  enableDnsSupport: true
  instanceTenancy: default
  routeTables:
    - name: Network-Endpoints-Tgw-A
      routes: []
    ...
  subnets:
    - name: Network-Endpoints-A
      availabilityZone: a
      routeTable: Network-Endpoints-A
      ipv4CidrBlock: 10.1.0.0/24
    ...
  transitGateway:
    name: Network-Main
    account: Network
  gatewayEndpoints:
    defaultPolicy: Default
    endpoints:
      - service: s3
      - service: dynamodb
  interfaceEndpoints:
    central: true
    defaultPolicy: Default
    endpoints:
      - service: ec2
      - service: ec2messages
```

# Landing Zone Accelerator on AWS

1



Installation Template  
(AWS CloudFormation)

2



Configuration Files  
(yaml)

3



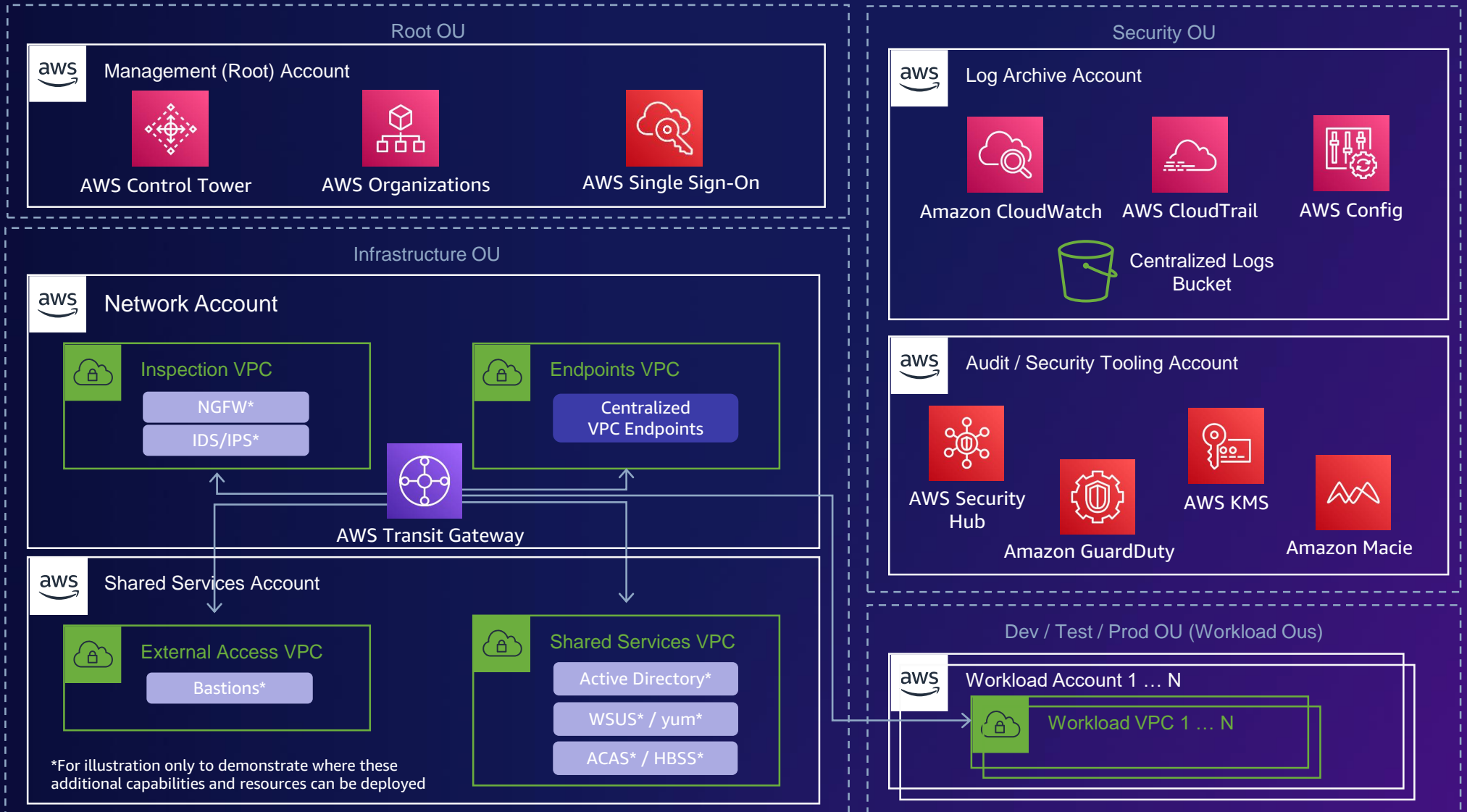
AWS CodePipeline

4



AWS Cloud  
Development Kit

## Landing Zone Accelerator



# Features - Security



AWS Control Tower



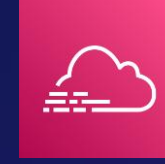
AWS Organizations



Amazon CloudWatch



AWS Config



AWS CloudTrail



AWS Service Catalog



AWS Systems Manager



AWS Security Hub



Amazon GuardDuty



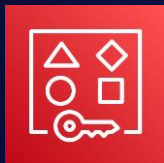
Amazon Inspector



Amazon Macie



AWS Firewall  
Manager



AWS Resource  
Access Manager



AWS Key Management  
Service (AWS KMS)

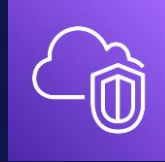


AWS Identity and Access  
Management (IAM)



AWS Network Firewall

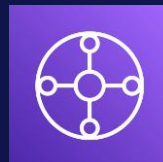
# Features - Networking



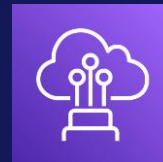
Amazon Virtual Private Cloud  
(Amazon VPC)



Amazon Route 53



AWS Transit Gateway



AWS Direct Connect

# Features - Operations



AWS Budgets



AWS Cost & Usage Report



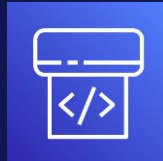
AWS Cost Explorer



AWS Tools and SDKs



AWS Cloud Development Kit (AWS CDK)



AWS CodePipeline



AWS CodeCommit



AWS CodeBuild



AWS Managed Services



AWS Professional Services



AWS Support

# Integrates with AWS Control Tower

Applications and Workloads

Built on top of resources deployed by the Landing Zone Accelerator on AWS and AWS Control Tower

Landing Zone Accelerator on AWS

Enables additional AWS security services, Foundational networking infrastructure, Configuration management

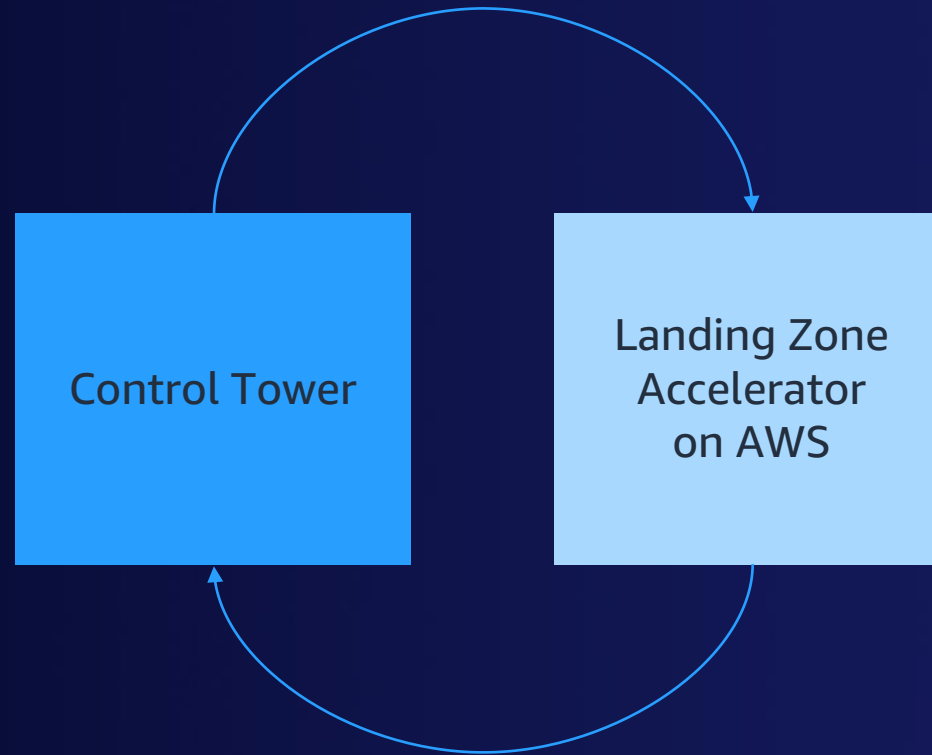
AWS Control Tower

Landing Zone, Account Factory, Preventative and Detective Guardrails



# A future with Control Tower

Accelerator environments use resources and guardrails from the Control Tower Landing Zone



Deprecate accelerator features in favor of a managed service

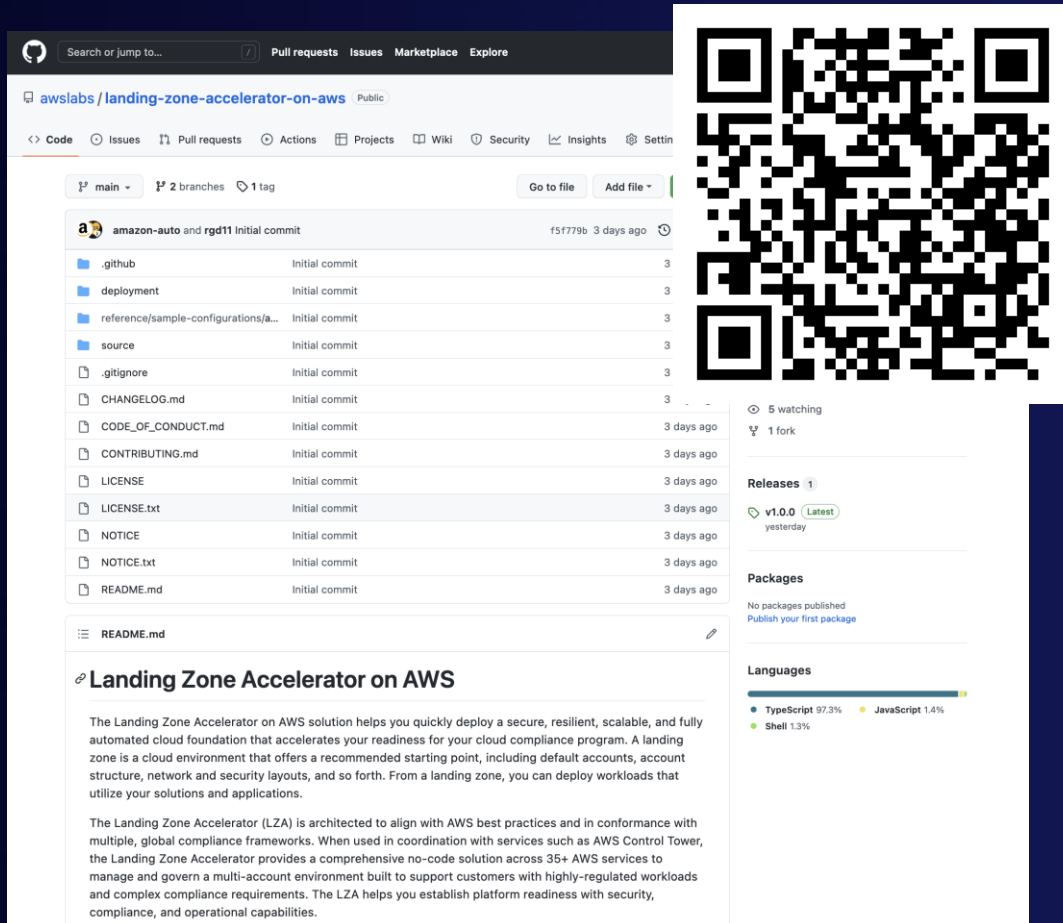
Landing Zone Accelerator environment can be enrolled into Control Tower, once present in desired home region

Feature requests are sent to Control Tower (and other AWS service teams)

# Solution Highlights

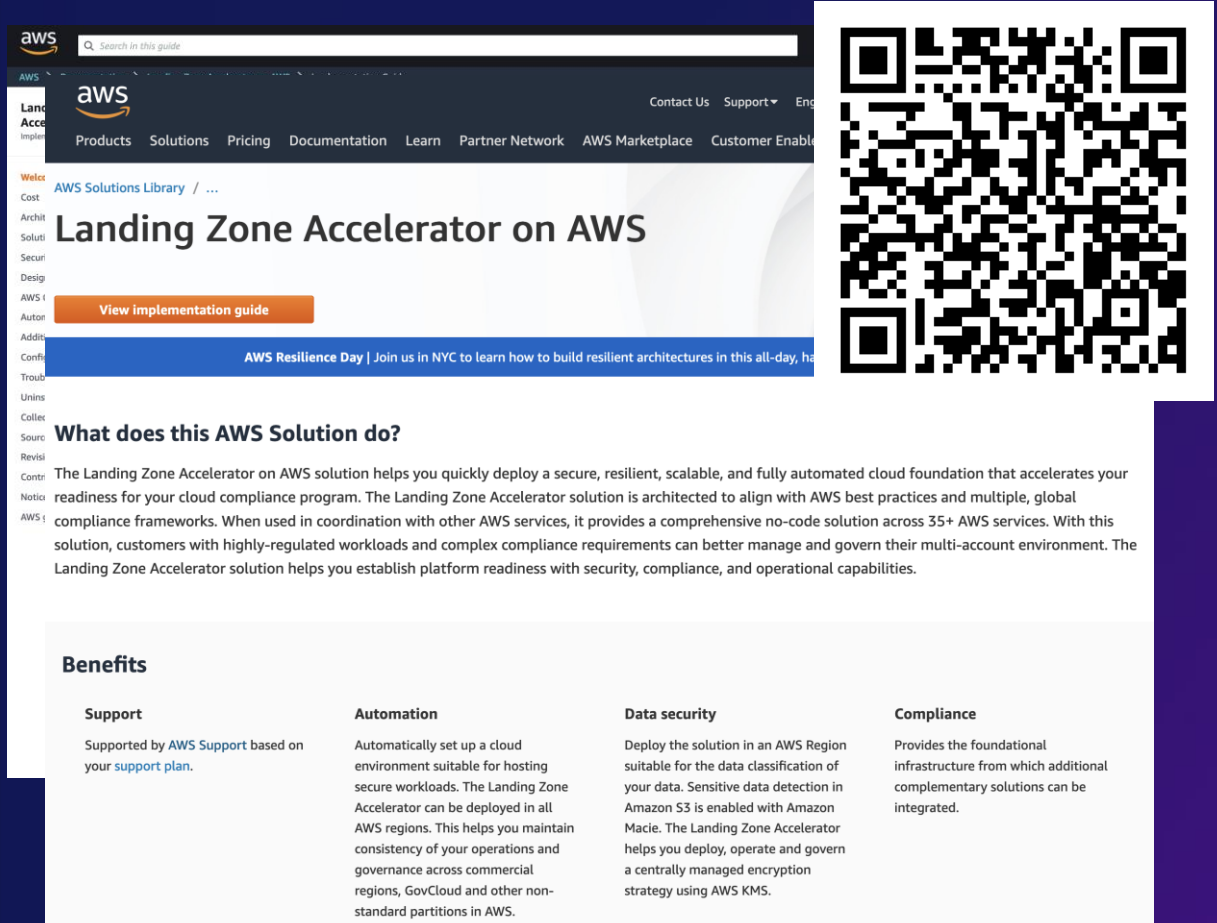
- Build secure and compliant AWS environments in days, instead of months or years.
- Focus time and critical budgets on migration, transformation, and innovation.
- Documentation helps demonstrate compliance requirements are met and shortens time to prepare for accreditation of their AWS environment.
- Customers can install the Solution directly from GitHub or have it delivered by AWS Professional Services or Partners.
- Customers can get technical assistance from AWS Support.

# Call to Action



The screenshot shows the GitHub repository page for 'aws-labs/landing-zone-accelerator-on-aws'. The repository is public and has 2 branches and 1 tag. The commit history shows an initial commit by 'amazon-auto and rgd11' 3 days ago. The file list includes .github, deployment, reference/sample-configurations/a..., source, .gitignore, CHANGELOG.md, CODE\_OF\_CONDUCT.md, CONTRIBUTING.md, LICENSE, LICENSE.txt, NOTICE, NOTICE.txt, and README.md. The repository description states: 'The Landing Zone Accelerator on AWS solution helps you quickly deploy a secure, resilient, scalable, and fully automated cloud foundation that accelerates your readiness for your cloud compliance program. A landing zone is a cloud environment that offers a recommended starting point, including default accounts, account structure, network and security layouts, and so forth. From a landing zone, you can deploy workloads that utilize your solutions and applications. The Landing Zone Accelerator (LZA) is architected to align with AWS best practices and in conformance with multiple, global compliance frameworks. When used in coordination with services such as AWS Control Tower, the Landing Zone Accelerator provides a comprehensive no-code solution across 35+ AWS services to manage and govern a multi-account environment built to support customers with highly-regulated workloads and complex compliance requirements. The LZA helps you establish platform readiness with security, compliance, and operational capabilities.'

<https://github.com/aws-labs/landing-zone-accelerator-on-aws>  
GitHub Repository



The screenshot shows the AWS Solutions Library page for 'Landing Zone Accelerator on AWS'. The page features a search bar, navigation links (Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, Customer Enable), and a 'View implementation guide' button. The main heading is 'Landing Zone Accelerator on AWS'. Below the heading, there is a section titled 'What does this AWS Solution do?' which states: 'The Landing Zone Accelerator on AWS solution helps you quickly deploy a secure, resilient, scalable, and fully automated cloud foundation that accelerates your readiness for your cloud compliance program. The Landing Zone Accelerator solution is architected to align with AWS best practices and multiple, global compliance frameworks. When used in coordination with other AWS services, it provides a comprehensive no-code solution across 35+ AWS services. With this solution, customers with highly-regulated workloads and complex compliance requirements can better manage and govern their multi-account environment. The Landing Zone Accelerator solution helps you establish platform readiness with security, compliance, and operational capabilities.' Below this, there is a 'Benefits' section with four columns: 'Support' (Supported by AWS Support based on your support plan), 'Automation' (Automatically set up a cloud environment suitable for hosting secure workloads. The Landing Zone Accelerator can be deployed in all AWS regions. This helps you maintain consistency of your operations and governance across commercial regions, GovCloud and other non-standard partitions in AWS.), 'Data security' (Deploy the solution in an AWS Region suitable for the data classification of your data. Sensitive data detection in Amazon S3 is enabled with Amazon Macie. The Landing Zone Accelerator helps you deploy, operate and govern a centrally managed encryption strategy using AWS KMS.), and 'Compliance' (Provides the foundational infrastructure from which additional complementary solutions can be integrated.).

<https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/>  
AWS Solutions  
Implementation and Deployment Guide



# Learn in-demand AWS Cloud skills



## AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand



Train now



## AWS Certifications

Earn an industry-recognized credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits



Access **new** exam guides

# Thank you!



Please complete  
the session survey  
in the mobile app

Android



iOS

