
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SAS304-R

# Solving the SaaS compliance puzzle


Ranjith Raman

Sr. Partner Solutions Architect
AWS SaaS Factory

Bill Tarr

Sr. Partner Solutions Architect
AWS SaaS Factory


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# What is compliance?




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# SaaS and compliance



Compliant tenant onboarding



Meet data residency requirements



Stricter tenant identity requirements



Secure auditing, logging, and monitoring

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS shared responsibility model

aws

- Facilities
- Physical security
- Compute infrastructure
- Storage infrastructure
- Network infrastructure
- Virtualization layer (Amazon EC2)
- Hardened service endpoints
- Rich AWS Identity and Access Management (IAM) capabilities

+

**Customer**

- Network configuration
- Security groups
- OS firewalls
- Operating systems
- Applications
- Proper service configuration
- AuthN & acct management
- Authorization policies

=

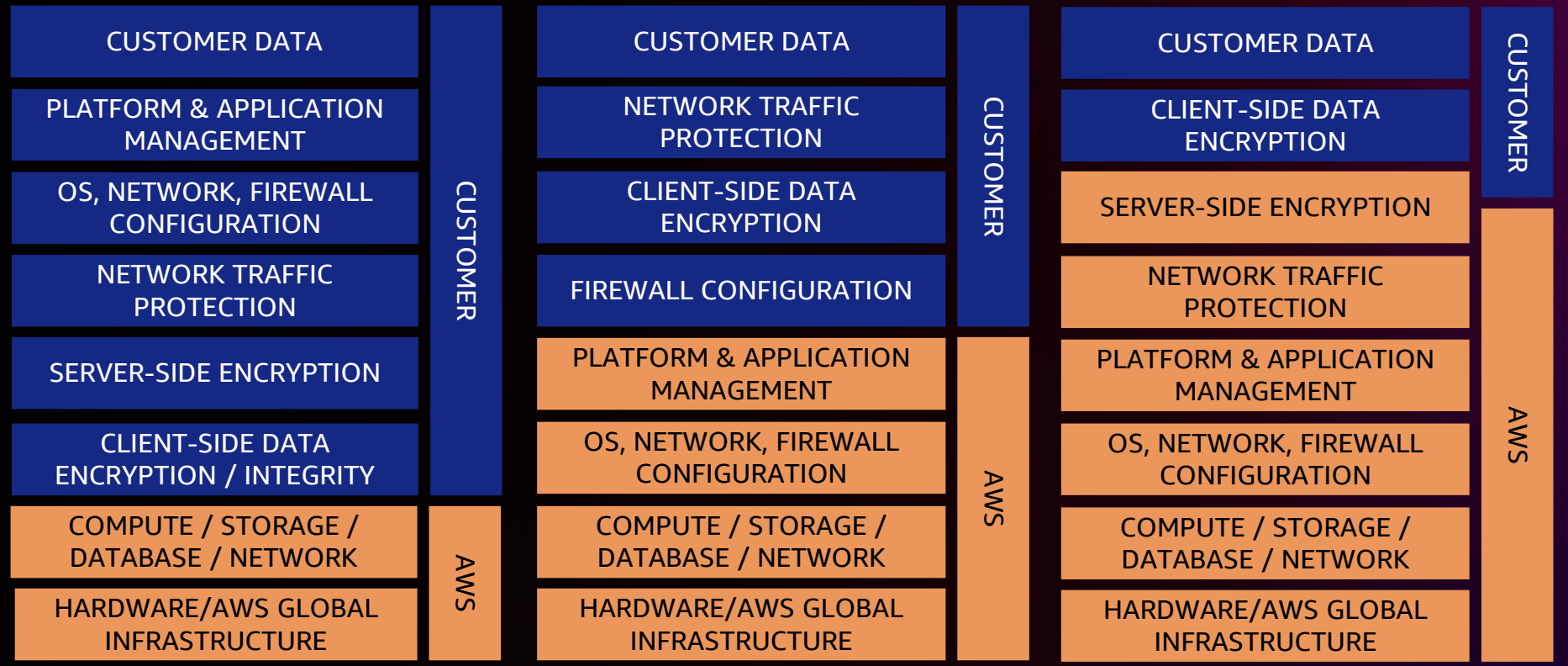



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Shared responsibility – The line varies . . .

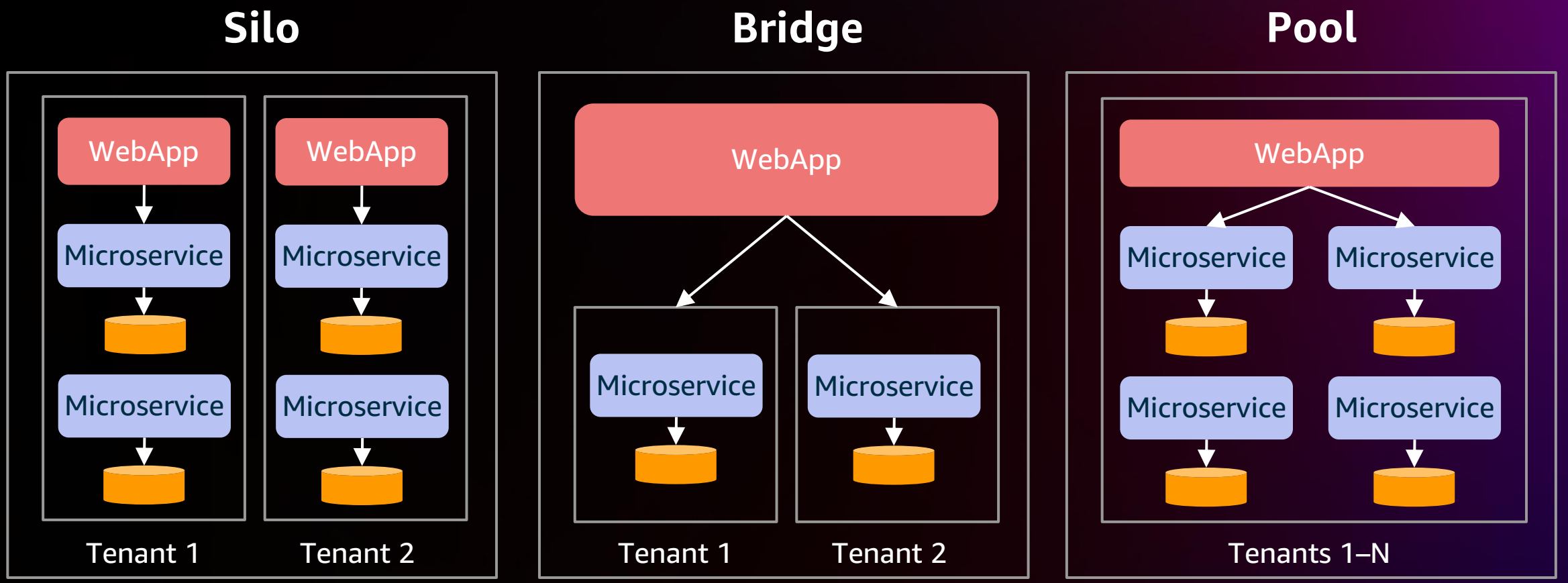
More customizable + More customer responsibility




Less customizable + Less customer responsibility + More best practices built-in

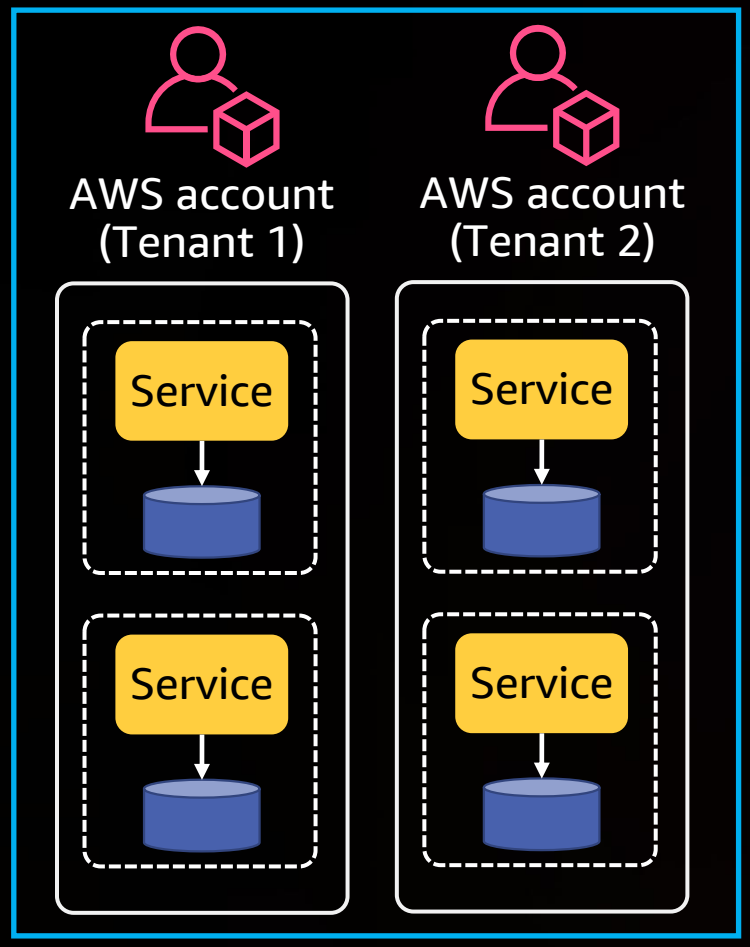
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# The three models of SaaS isolation

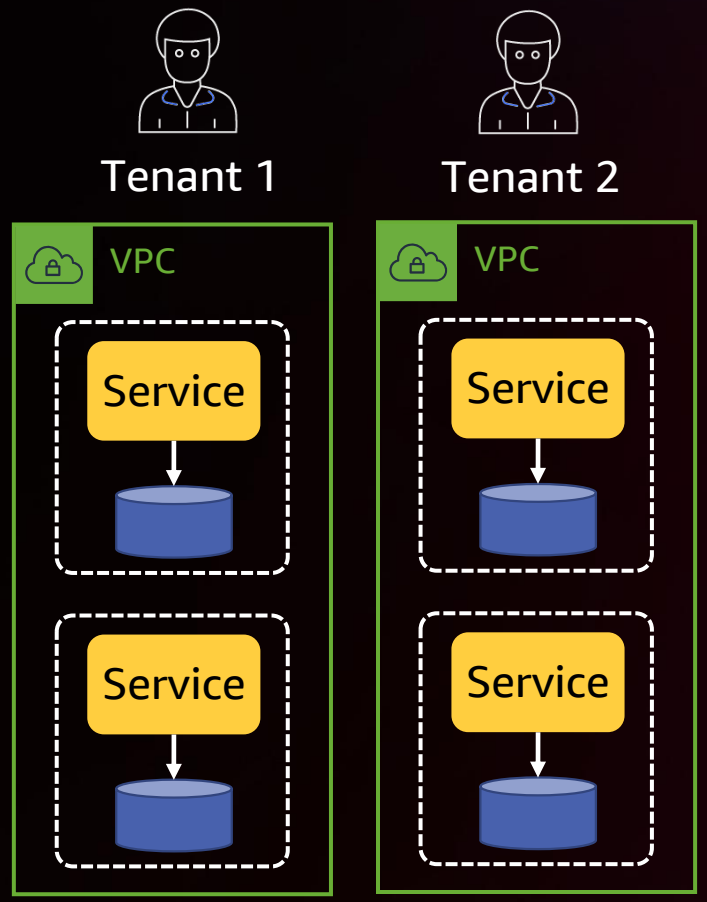



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

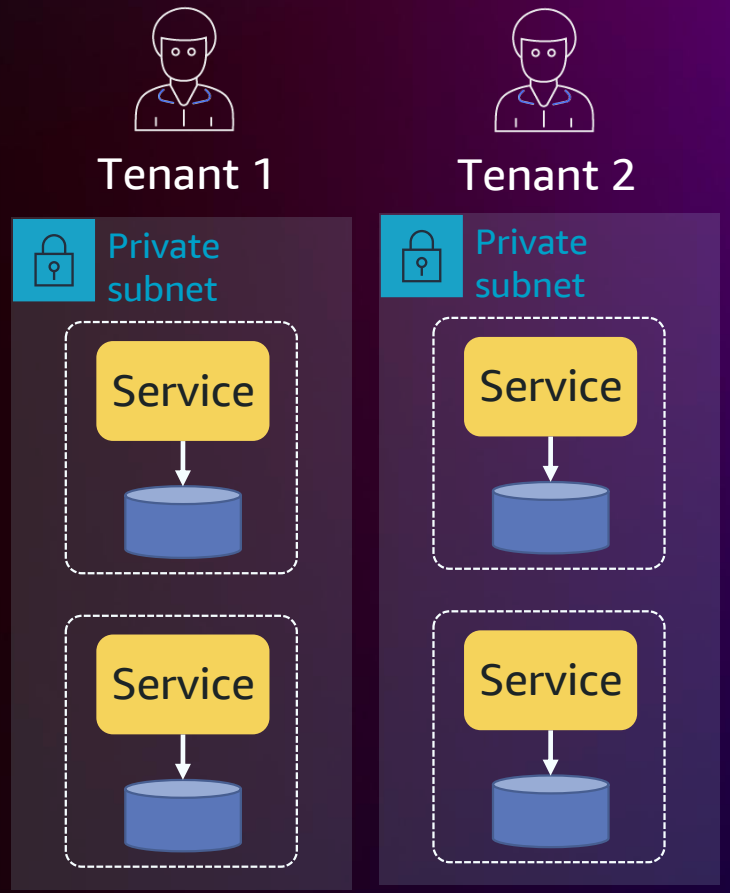
# Silo isolation strategies




Account per tenant




VPC per tenant




Subnet per tenant

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Silo tenant onboarding challenge



SaaS Admin
(Provider/ISV admin)

Tenant onboarding

AWS account
Tenant 1

Compliant

AWS account
Tenant 2

Noncompliant

AWS account
Tenant 3

Compliant

**Applying inconsistent policies and standards during tenant onboarding results in a noncompliant SaaS environment**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS services enabling compliance

## Manage risk



AWS Config



AWS CloudTrail



AWS Systems Manager



AWS Control Tower



AWS License Manager

## Oversee risk



AWS Security Hub



Amazon CloudWatch

## Assurance of risk management



AWS Audit Manager



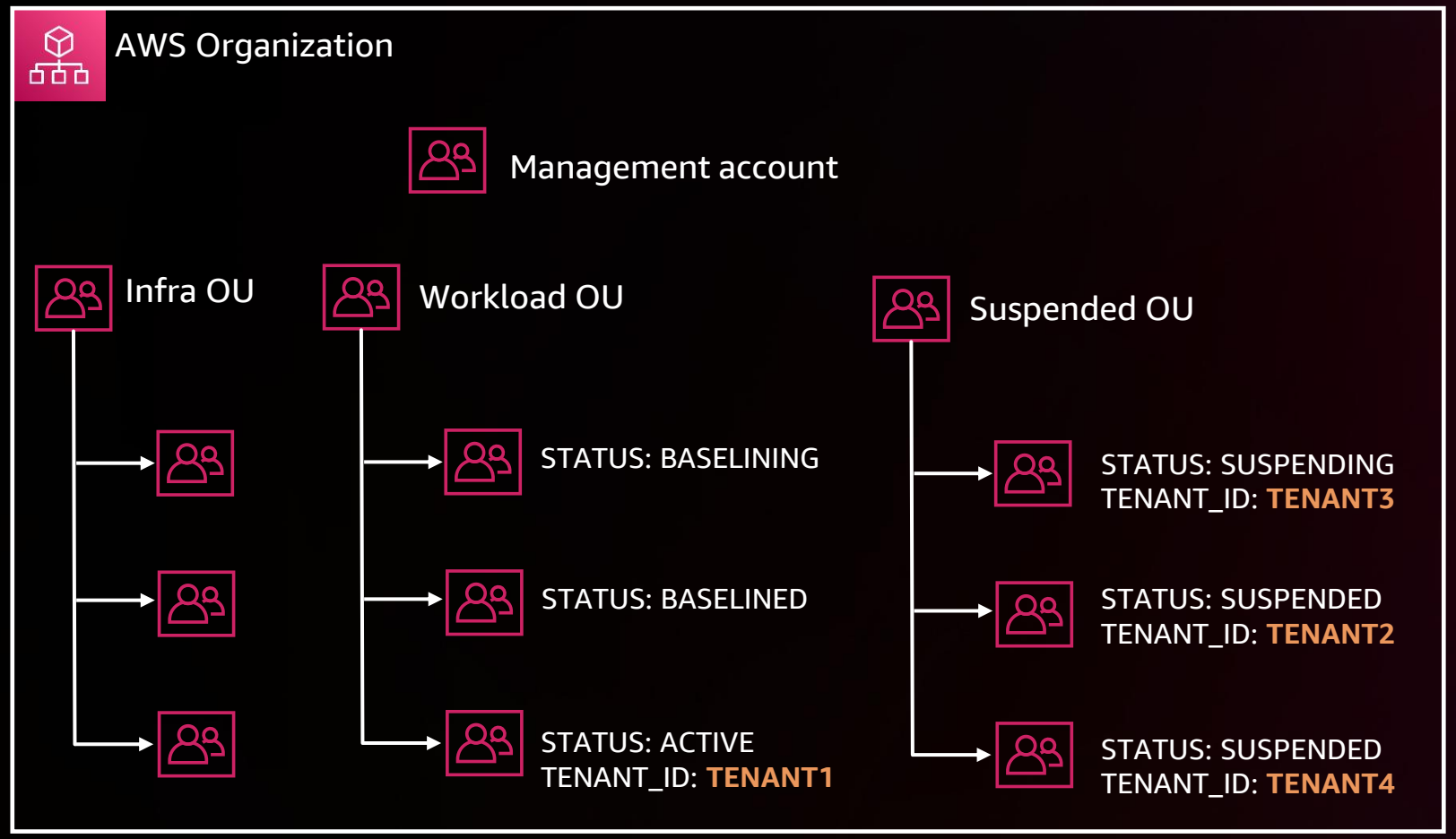
AWS Artifact



**AWS Well-Architected Framework**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

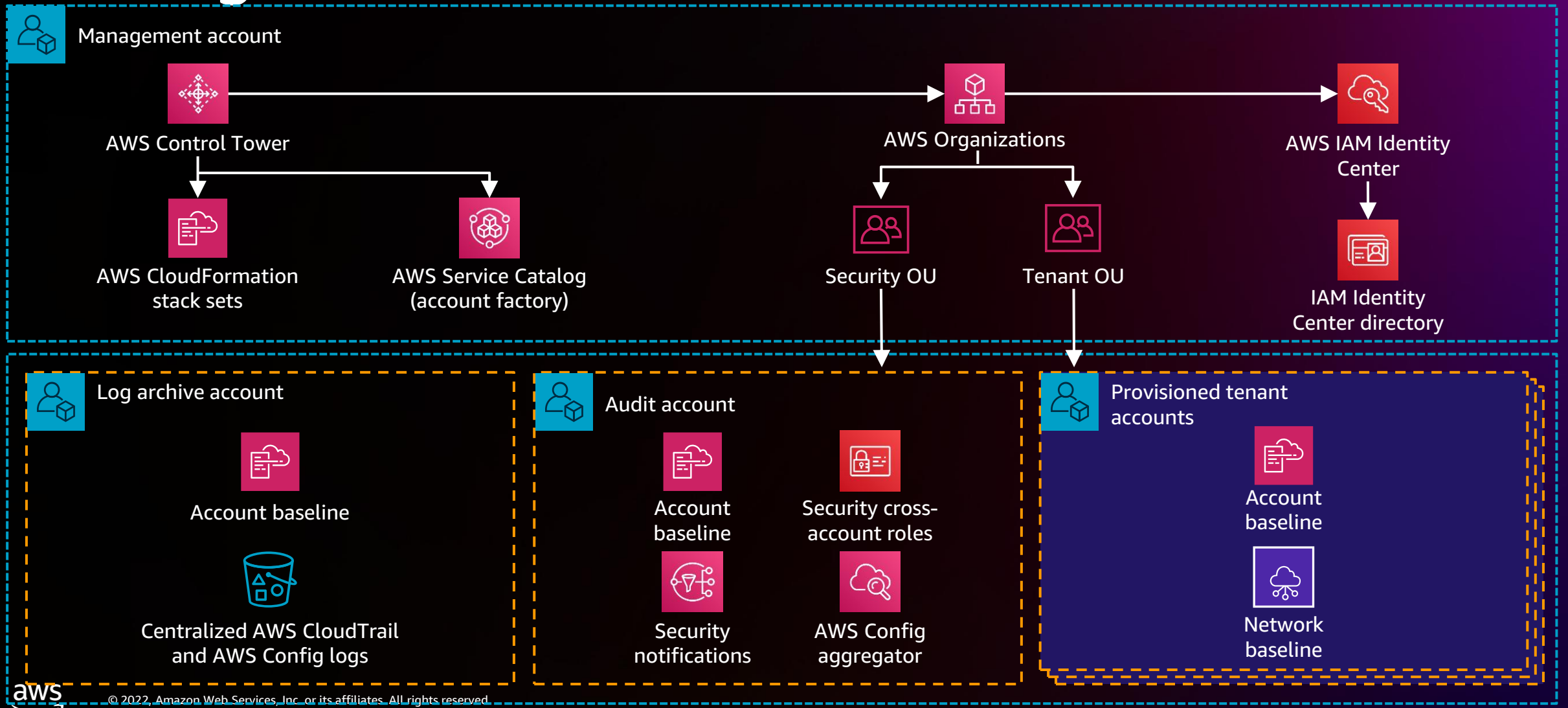
# AWS Organizations and AWS Control Tower to the rescue




- **Centrally provision** tenant accounts
- Secure and **audit** your environment for **compliance**
- **Share resources and control access** to accounts, AWS Regions, and services
- **Optimize costs** and identify cost-saving measures

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

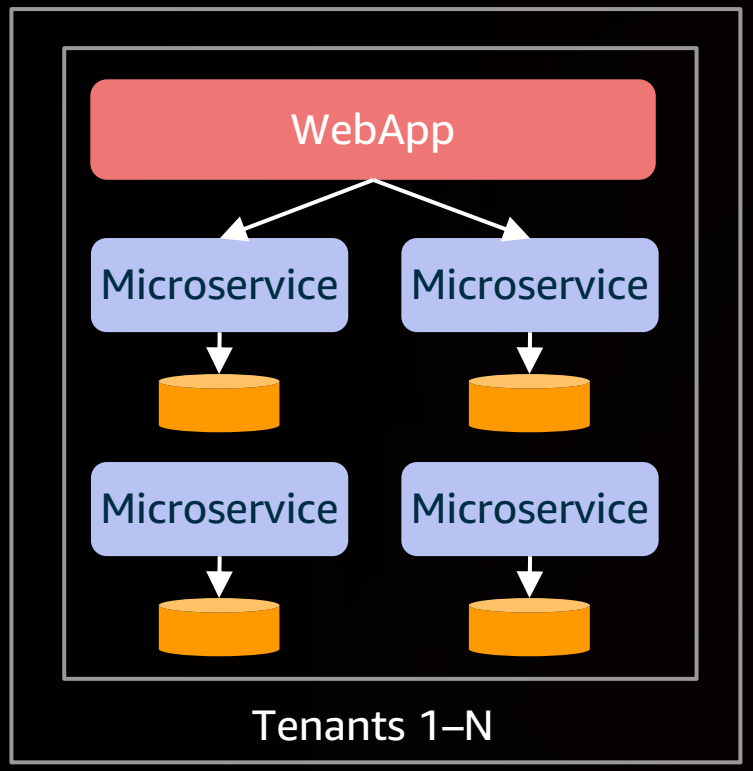
# Vend compliant tenant accounts using a landing zone




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Pooled model requires stronger security controls

## Pooled tenant isolation



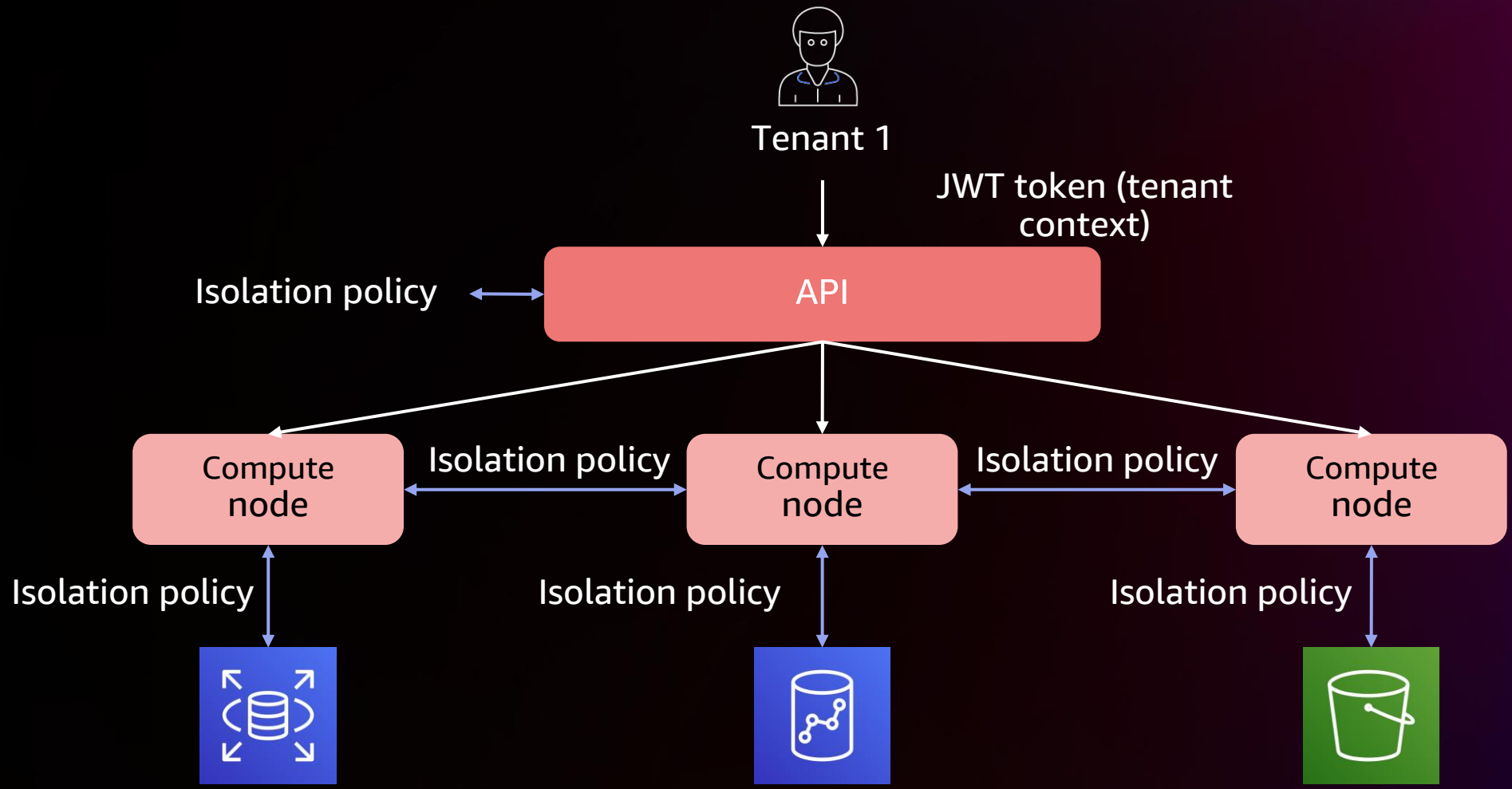

Requires

- Stronger identity, authentication, and authorization techniques
- Stronger encryption of data (at rest and in transit) and key management techniques
- Performance monitoring
- Audit logging, retention, and backup strategies
- Automated alerts

**Pooled isolation model sets a high bar for security, identity, performance, audit logging, and performance monitoring**

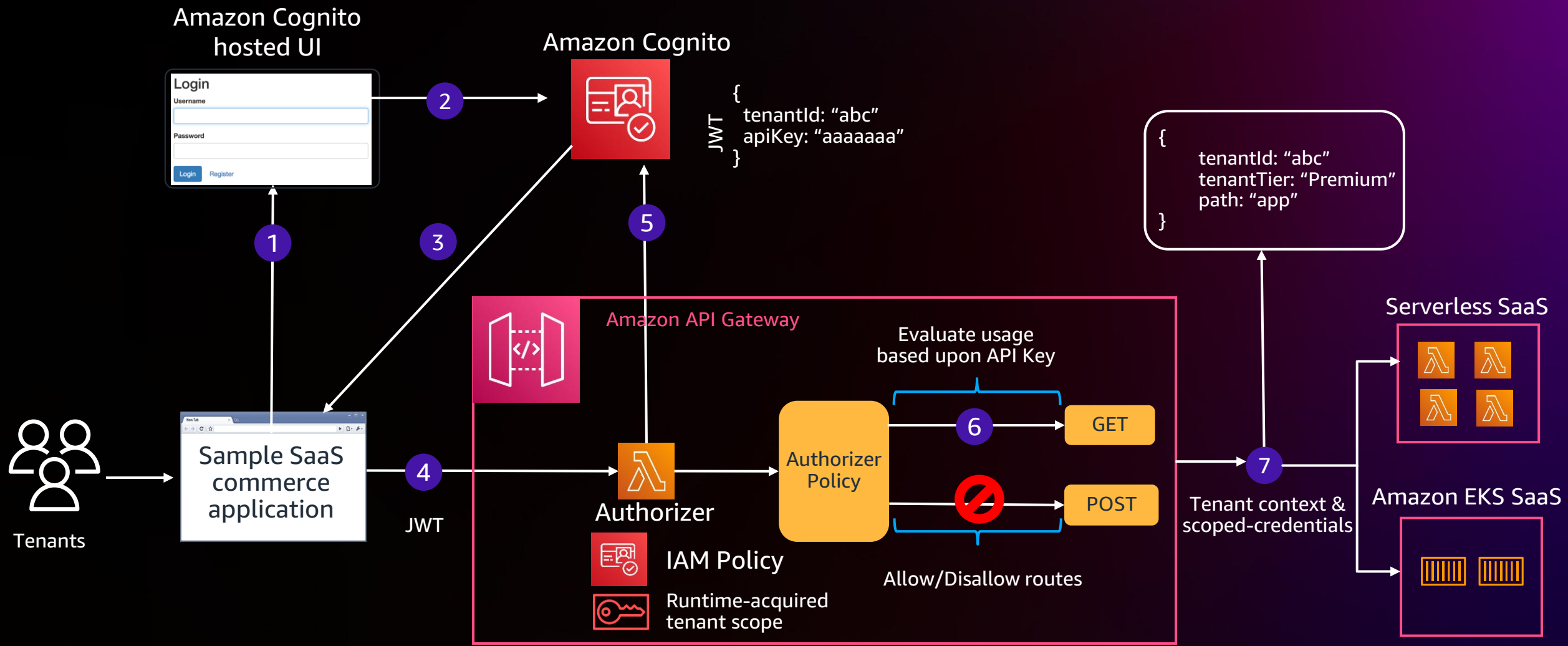
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Leverage runtime policies to control access




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Implement a robust identity and authentication flow




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Compliance guidance for Amazon Cognito and API Gateway

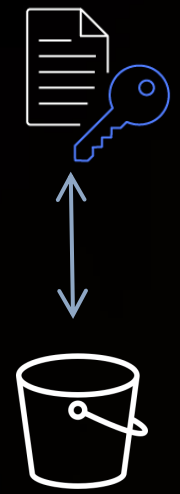
| Customer activity | Amazon API Gateway | Amazon Cognito |
|---|---|---|
| Identity and account management | Customers are responsible for protecting execution APIs through the use of IAM, interface endpoint policies, resource policies, **Amazon Cognito user pools, or Lambda Authorizers** for custom **bearer token** authentication strategies like OAuth and SAML | Amazon Cognito customers are responsible for using AWS IAM to **create an IAM user with an attached policy** to activate [service/EC2] permissions or create **custom policies** to attach to the role |
| Encryption at rest | If API Gateway customers choose to activate caching for a REST API, AWS recommends customers to **activate cache encryption** to ensure confidentiality | Customers are responsible for exporting user information and are responsible for **encrypting data at rest on the storage service** they choose in accordance with their organizational encryption requirements |
| Encryption in transit | API Gateway **doesn't support unencrypted** (HTTP) endpoints. For greater security, customers should choose a minimum Transport Layer Security (TLS) protocol version to be enforced for your API Gateway custom domain | All requests to Amazon Cognito must be made over the Transport Layer Security protocol (TLS). Clients must support Transport Layer Security (TLS) 1.0 or later. We **recommend TLS 1.2** or later |
| Audit logging | API Gateway integrates with **AWS CloudTrail**. CloudTrail captures MGMT API calls for API Gateway as events. These include calls from the API Gateway console and code calls to the API Gateway API operations | Amazon Cognito customers are responsible for audit log analysis, review, and reporting in accordance with their organizational requirements. Because Amazon Cognito exclusively generates logs from API calls, **CloudTrail** serves as the central repository for logs related to Amazon Cognito |

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Encrypt where? Encrypt everywhere!

**Data at rest**

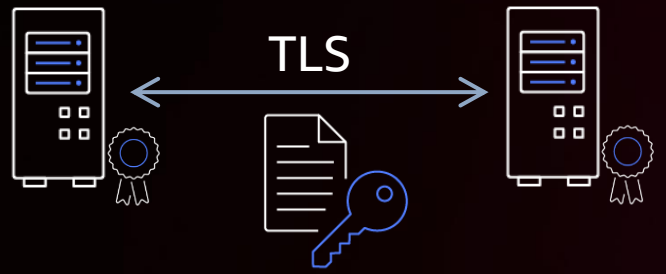
Storage encryption



Amazon S3 bucket

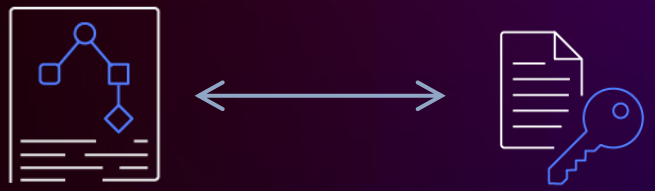
**Data in transit**

Network encryption




**Data in use**

Application-level encryption

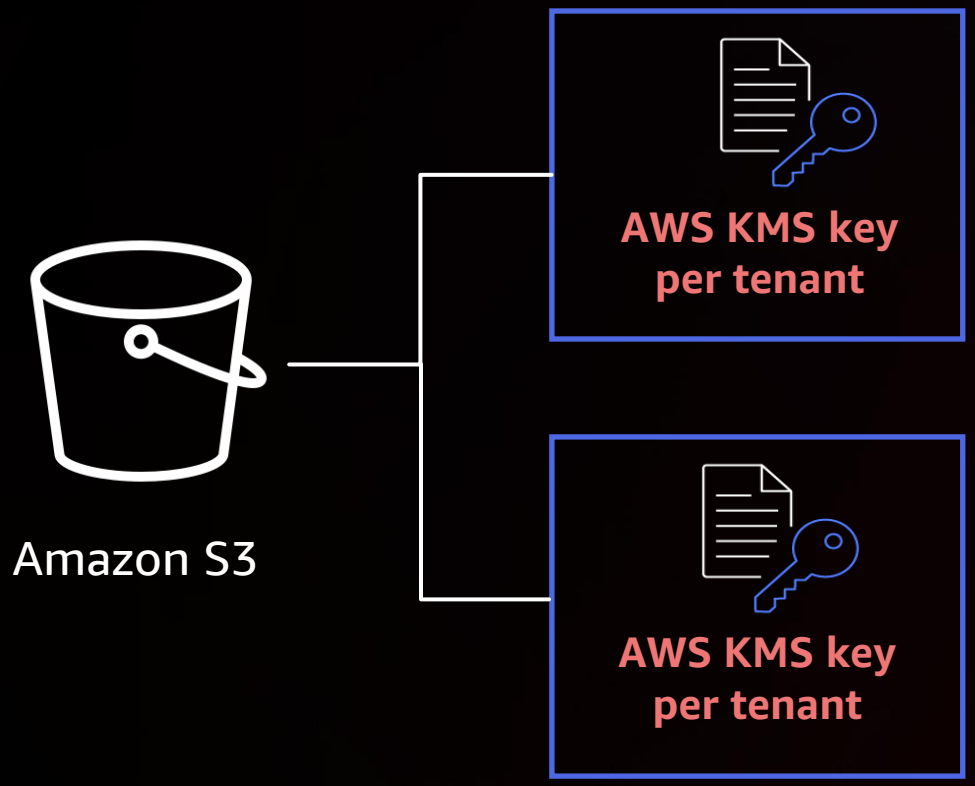


Application code

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Apply tenant-level encryption using keys at the storage layer




```
put-object
  --bucket <value>
    --key <value>
     [--ssekms-key-id <value>]
```

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

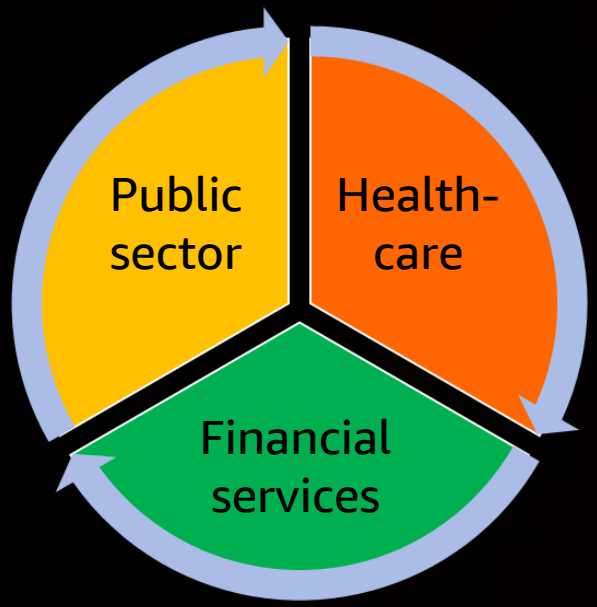
# Compliance guidance for AWS Key Management Service (AWS KMS)

| Customer activity | AWS Key Management Service |
| --- | --- |
| Encryption at rest | By default, the customer KMS keys that customers create in AWS KMS are generated in and protected by **hardware security modules (HSMs) that are FIPS 140-2** validated cryptographic modules. The KMS keys never leave the modules unencrypted |
| Encryption in transit | API endpoints receive client requests over an HTTPS connection. These **API endpoints authenticate and authorize the request** before passing the request for a cryptographic operation to the AWS KMS HSMs or your AWS CloudHSM cluster if you're using the KMS custom key store feature. Customers are responsible for choosing how to encrypt data in transit with KMS in accordance with their organizational requirements |
| Audit logging | AWS KMS integrates with **CloudTrail**. CloudTrail captures all API calls for AWS KMS as events, including calls from the AWS KMS console and from code calls to the AWS KMS APIs. AWS KMS customers are responsible for ensuring CloudTrail is activated for continuous delivery of events to a customer-specified Amazon S3 bucket |

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Global Security & Compliance Acceleration Program (GSCA)




## Program goals

**Support, enhance, and accelerate** customers' abilities to meet differing regulatory, security, and compliance requirements **globally**

**Partner with country and regional partners** to provide **localized** customer support and engagement

## Program outcomes

**Accelerated** security and compliance authorization processes

**Reduced** cost and time to achieve certifications/authorizations

**Improved** security, response, and continuous monitoring capabilities leveraging AWS services and AWS Partner solutions

**GSCA Partners:** https://aws.amazon.com/partners/programs/ato/

**Contact us:** scaglobal@amazon.com

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# First steps – AWS best practices

**AWS Startup Security Baseline (AWS SSB)** – A set of controls that create a minimum foundation for businesses to build securely on AWS. The controls in this guide are designed with early startups in mind, mitigating the most common security risks without requiring significant effort

- https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-startup-security-baseline/welcome.html

**AWS Well-Architected Tool and SaaS Lens** – AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads. The AWS Well-Architected Tool is designed to help you review the state of your applications and workloads, and it provides a central place for architectural best practices and guidance

- https://aws.amazon.com/well-architected-tool/
- https://docs.aws.amazon.com/wellarchitected/latest/saas-lens/saas-lens.html

**AWS Foundational Technical Review (FTR)** – Helps identify AWS Well-Architected best practices specific to your software or solution

- https://aws.amazon.com/partners/foundational-technical-review/

**CIS AWS Cloud Benchmarks** – Best practices integrated into AWS services (Amazon Inspector, AWS Audit Manager, AWS Config, AWS Security Hub)

- https://www.cisecurity.org/benchmark

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Summary

- SaaS sets a high bar for security, control, and compliance
- In a full-stack silo model, consider automating tenant account provisioning
- Apply guardrails to ensure a compliant SaaS environment
- Pooled models demand stricter isolation techniques to achieve compliance
- Apply isolation policies at every layer of your stack
- Use key encryption techniques to secure tenant data
- Leverage best practice on identity, authentication, and authorization techniques to satisfy compliance requirements
- Leverage AWS tools and services to help build a compliance solution

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# More SaaS sessions

## Breakout sessions

- SAS305 – SaaS architecture patterns: From concept to implementation
- SAS405 – SaaS microservices deep dive: Simplifying multi-tenant development
- SAS306 – SaaS migration: Inside a real-world multi-tenant transformation
- SAS302 – Supporting extensibility in SaaS environments
- PEX310 – Optimizing your multi-tenant SaaS architecture

## Workshops

- SAS403 - SaaS microservices deep dive: Multi-tenancy meets microservices
- SAS402 – Serverless meets SaaS: Inside a real-world serverless SaaS solution
- SAS401 – Amazon EKS SaaS: Building a working multi-tenant environment

## Business session

- PEX209 – Building your SaaS journey on AWS

# More SaaS session

## Chalk talks

- SAS307 – DevOps and SaaS: Applying automation in multi-tenant environments
- SAS303 – SaaS anywhere: Building SaaS that run in hybrid models
- SAS301 – Multi-tenant meets ML: Building ML-based SaaS environments
- PEX313 – The SaaS Control Plane: The heart of SaaS growth
- ARC403 – Amazon EKS SaaS deep dive: Inside a multi-tenant EKS solution
- ARC323 – Designing a multi-tenant SaaS tiering and throttling strategy
- SVS315 - Building multi-tenant applications with AWS Lambda and AWS Fargate

## Builder session

- ARC327 – How to optimize cost in your multi-tenant architecture

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Additional resources

1

## Subscribe to AWS SaaS Insights

Get monthly emails with bite-size advice and the latest updates

2

## Explore the SaaS on AWS hub

Check out the SaaS on AWS page for more resources and insights

3

## Discover resources for builders

Access our curated list of SaaS reference solutions, demos, tech events and more

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Thank you!

Ranjith Raman
ranraman@amazon.com

Bill Tarr
billtarr@amazon.com



Please complete the session survey in the **mobile app**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.