MOODY'S ANALYTICS

Bank RegTech Talks: Best Practices for SaaS Security

Yann Delacourt – Technology Strategy, Product Management

June, 2018

Agenda:

Moody's Analytics:

- Cloud adoption in financial services
- Regulators' perspectives on cloud services
- Key obstacles to cloud adoption in risk and finance functions
- SaaS applications security by Moody's Analytics & AWS

AWS:

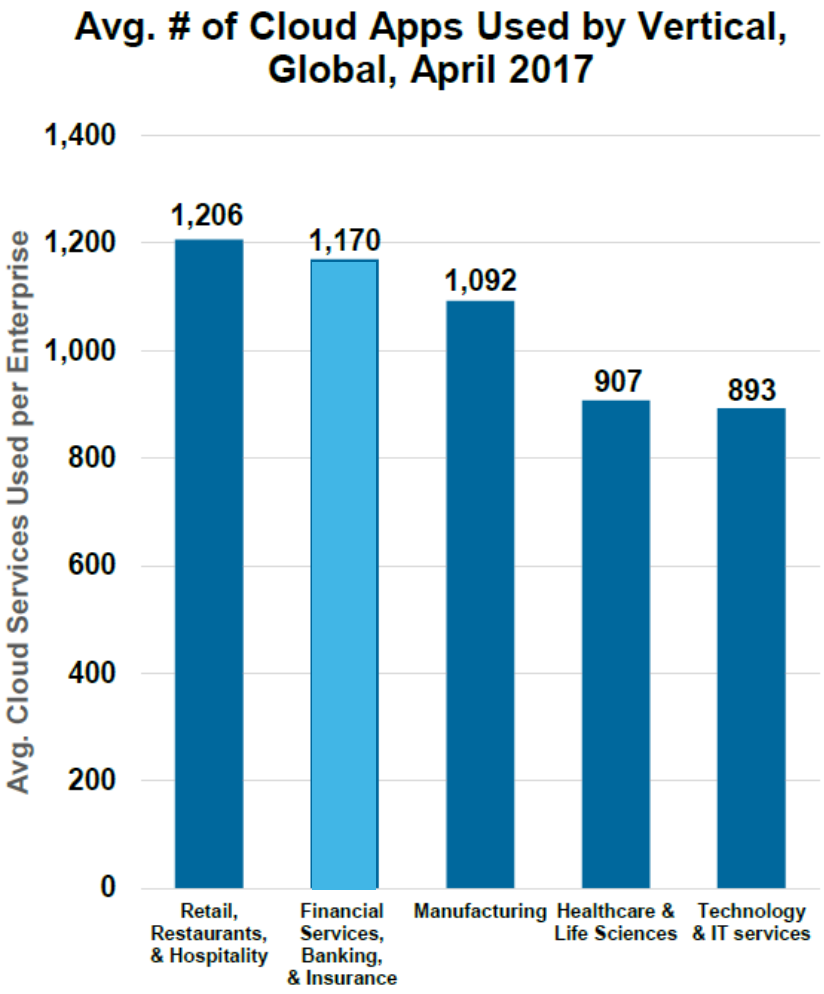
- Certifications
- Is "SaaS" really "SaaS"?
- Permissions and Policy Management
  - IAM, Bucket Policy
- Cryptography
  - Data at Rest (primarily KMS)
  - Data in Transit
  - A little bit on CloudHSM

The cloud adoption is rising to new heights in FIS

"Yet at the recent Sibos event, it was evident that financial institutions are now serious about embracing cloud – including the **public cloud – to reduce costs** and **improve resiliency and security**"

While industries such as gaming and retail have embraced public cloud, financial institutions have been much slower to do so. "This has been driven by a **misconception that the public cloud is not secure**."

Jonathan Charley, General Manager FSI EMEA at SAP



Source: Netskope & Kleiner Perkins May 2017

Many banks are paying for IT infrastructure capacity that they need for peak processing, which may occur for only a handful of days in a year. The large-scale public **cloud providers** not only **can invest far more in security than individual banks**, but also must because their reputations are dependent upon them being secure.

"**Reduced complexity**, greater flexibility and agility, **lower costs** and better business outcomes, that financial institutions must bear in mind when developing their migration strategy to the cloud"

Ambreesh Khanna, Group Vice President and General Manager of Oracle Financial Services

Cost reduction is a key driver… while regulatory barrier is perceived as a challenge

Key drivers to cloud adoption

Cost Reduction

- **All the banks** interviewed* migrate to the cloud for cost reasons. Their objective is to minimize IT costs (datacenters, hardware, staff, legacy systems, expensive legacy license)
- Yet, cost is **not the only reason** to migrate to cloud.

"Cost is the main reason to migrate to cloud, in particular to reduce Oracle license fees" **leading bank in APAC**

"The cost of processing one transaction in the legacy system is 10x higher than in the new cloud platform" **Large global Bank**

Flexibility / Scalability

- **Nearly half of the banks*** migrate to cloud to gain flexibility and scalability as a way to better respond to business needs (easily upscale or downscale IT requirements as and when required)

"Beyond cost, cloud will enhance the flexibility and efficiency of our IT" **Leading bank in APAC**

"Our legacy system wasn't agile enough, cloud offers greater scalability and flexibility" **Leading bank in EMEA**

Innovation and time to market

- **Over 1/3rd of banks*** think that cloud will allow them to develop products faster and meet customer demands more timely. Cloud is also seen as a lever for innovation by partnering with cloud vendors to co-develop products and services.

"Our larger cost savings will not come from shutting down data centers but from accelerated product development cycles" **Large global bank**

SaaS service model benefits

- **Over 1/3rd of banks*** mention the benefits of the SaaS service model: not having to maintain infrastructure, to manage software upgrades, and getting more frequent product releases, etc.

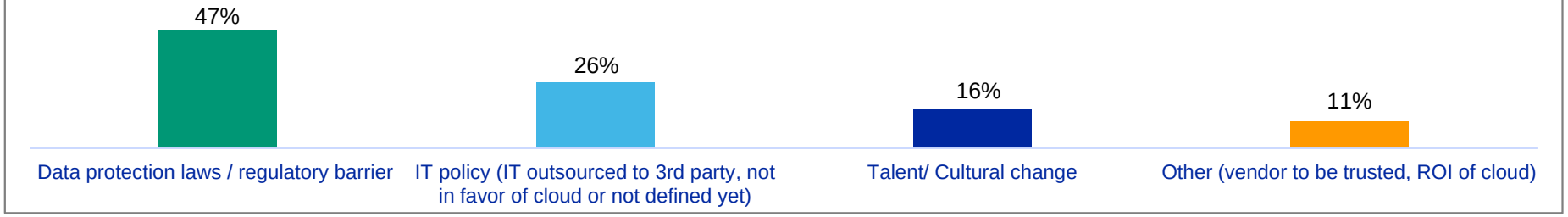
"We are interested in cloud because of the services it entails, in particular not having to manage IT infrastructure internally, or software upgrades or maintenance" **Bank in EMEA**

Other

- **Reduction of operational risk, business continuity and security** are other reasons mentioned by banks interviewed as key drivers for moving to cloud.

"SaaS offerings would be key to help us mitigate operational risks that we are facing linked to the current management of our software upgrades" **Large bank EMEA**

Main obstacles / challenges to cloud adoption



Source: Moody's Analytics market research - 21 leading banks across Europe and APAC

Source: Moody's Analytics market research discussions with 17 banks across Europe and APAC
* Among the 17 banks interviewed 11 of them have a plan to migrate to cloud computing

Iaas vs Paas vs Saas … where the value goes

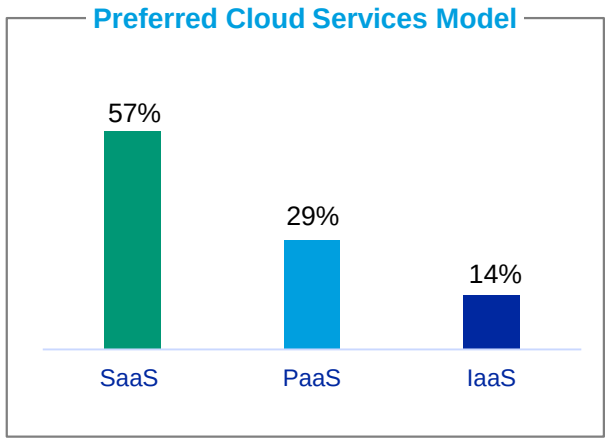
CIO Cloud Budget Allocation*

On Premise	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
30%	19%	45%	6% other as-a-service model such as Backup/Storage-as-a-Service, etc …
Customer managed: Application, Security, Database, Operating System, Virtualization, Servers, Storage, Networking, Data Centers	Customer managed: Application, Security, Database, Operating System Provider managed: Virtualization, Servers, Storage, Networking, Data Centers	Application, Security Provider managed: Database, Operating System, Virtualization, Servers, Storage, Networking, Data Centers	Provider managed: Application, Security, Database, Operating System, Virtualization, Servers, Storage, Networking, Data Centers

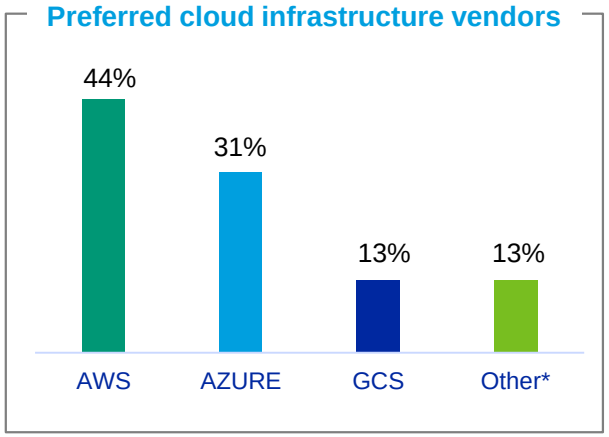
*Source IDG Cloud Research 2016

The SaaS model has by far the highest perceived ROI

SaaS is the first option banks are looking at



- **Over 40% of banks interviewed prefer native cloud solutions** to "lifting and shifting" their current solutions into the cloud.
- Yet, 18% of the banks interviewed will "lift and shift" or move to native cloud solutions **on a "case by case" basis.**
- **SaaS is the preferred service model**, followed by PaaS; most banks don't see benefit on an IaaS model.



- **AWS is the preferred infrastructure vendor** among banks in our sample, closely followed by **Azure.**
- **GCP** comes third behind.
- **Connection of applications** between different cloud providers requires some work but it is **not likely to entail major issues.**

Source: Moody's Analytics market research - 21 leading banks across Europe and APAC

Financial regulators' perspective

Learning & Adapting Guidance quickly

Clearing the way for financial institutions to adopt cloud solutions

Think that Public cloud providers are more secure than banks data centres if security patterns are properly implemented.

Obstacles aren't technical anymore but rather cultural. Regulators are using cloud technology themselves.

Since Cloud applications are being adopted quickly, regulators are planning **yearly audit on Security**.

Data Residency is a must have in all geographies.

Data Protection (such as GDPR, GLBA, PDPA, Privacy Act, etc …) is a must have in all geographies

Defining a Cloud due-diligence framework & delivering guidance to remove uncertainties

Access and audit rights

Location of data & data processing

Mitigating the risks of the outsourcing stack

Contingency plans and exit strategies

Regulators assessment & security audit of the cloud service providers

Key obstacles to adopting SaaS Applications

Security Transparency

Data Encryption end-to-end.
Encryption Key management.
Identity management and Access control.

Proven Cost Reduction

Proven and significant cost reduction. Not just limited to infrastructure but also to the operating cost.

Operating Model Change

Adoption of a SaaS operating model significantly impact internal IT processes.

Partner Reputation

Company wide and long standing Security Culture.

Legal framework aligned with the cloud operating model and regulators guidance.

Data Residency

Control and option to where the data are stored and processed.

Exit Plan

Ensure the solution is agnostic, it can be re-internalized or redeployed in a private cloud/different public cloud.

The check list for evaluating SaaS vendors

Banks have security requirements that SaaS vendors must match

Company wide Security Culture as if you were a leading Bank

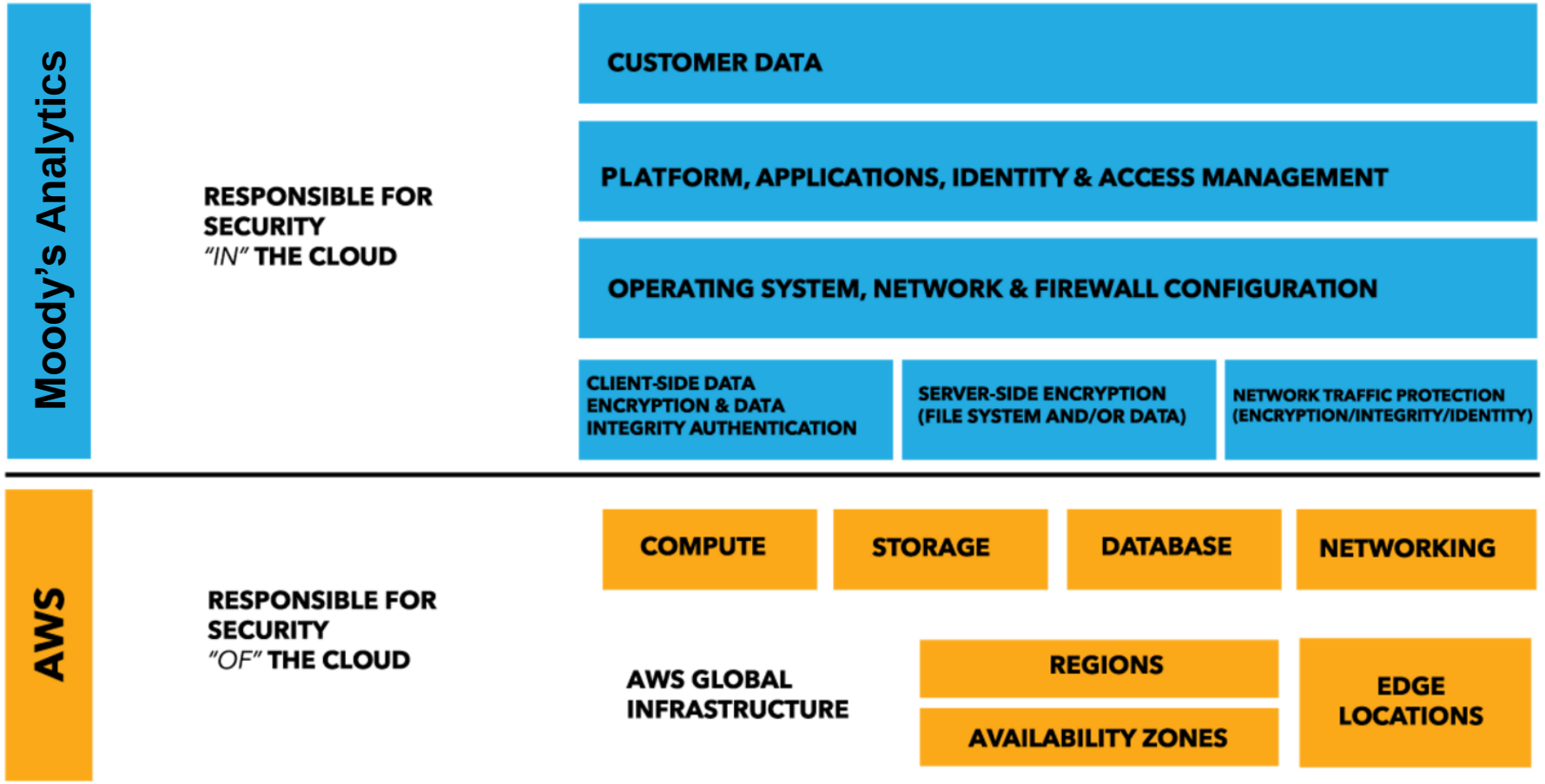
- Information security policies, awareness/training materials for employees and contractors
- Human Resources Security
- Technology Asset Management
- Physical Security
- Access Control Policy
- Business Continuity / Incident Response Policy
- Data Protection

Saas offering - Security & Reliability

- Perimeter & Network Security
- Data Isolation & Data Residency
- User Access Control Governance
- Business Continuity & Disaster Recovery

Rely on trusted partners end-to-end

Moody's Analytics has a proven track record protecting sensitive data partnering with AWS



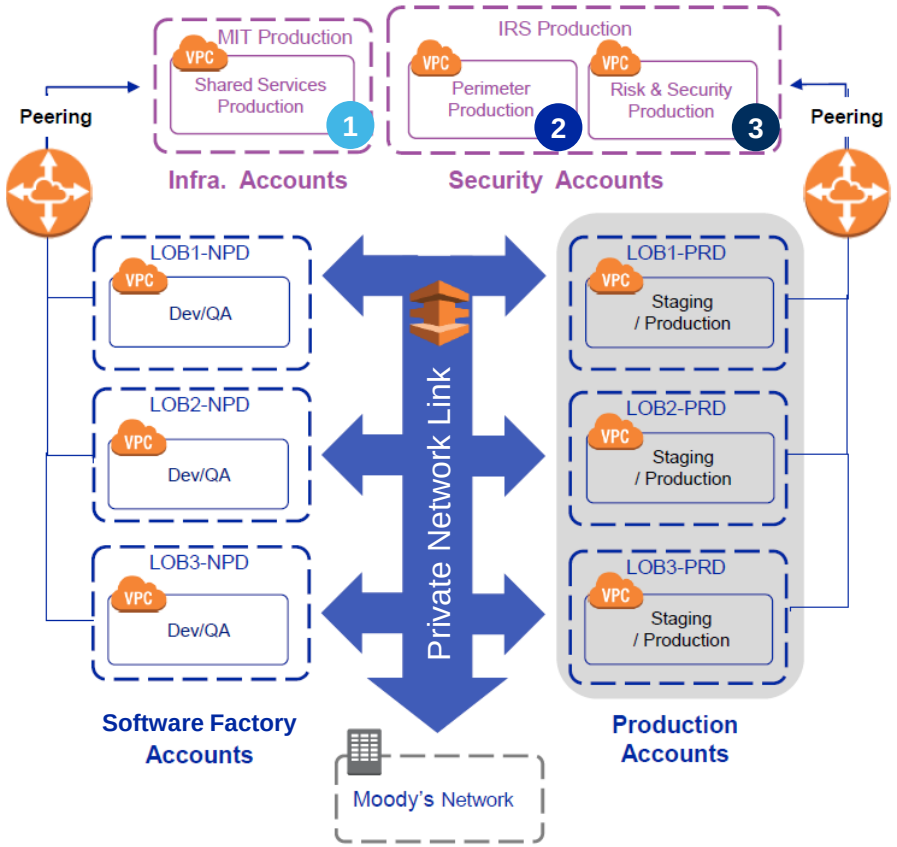
Saas Security framework

Access Management	Network Control	Perimeter Network Control	VM Management	Data Protection	Governance & Incident Management	Scalability Reliability
AD Integration	Security Group	Firewall	Patch Mngmt	Encryption	Cloud API	CDN
Role Based Access Control	JumpServers	IDS/IPS	Image Mngmt	Data Residency	Logging	Self-Healing
Dual Factor Authentication	NACLs	Detonation	Sys Hardening	PII(1) Evaluation	Monitoring	Redundancy
Granular permission		Proxy	Base SW Mngmt		ATP	DR Plan
		White/Black List	Tag/Asset Mngmt		Forensics	
		Denial of service protection				

(1) Personal Indentifiable Information (including GDPR)

Isolation & separation of duty by design

Strong network, infrastructure & accounts separation across cloud operation activities



Virtual Private Cloud (VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center.
Each « Saas service » is made available in its own VPC to maximizing isolation.

1 Separate accounts in charge of operating the infrastructure in production or non-production.
Responsability: reliability, availability, scalability & hardening.

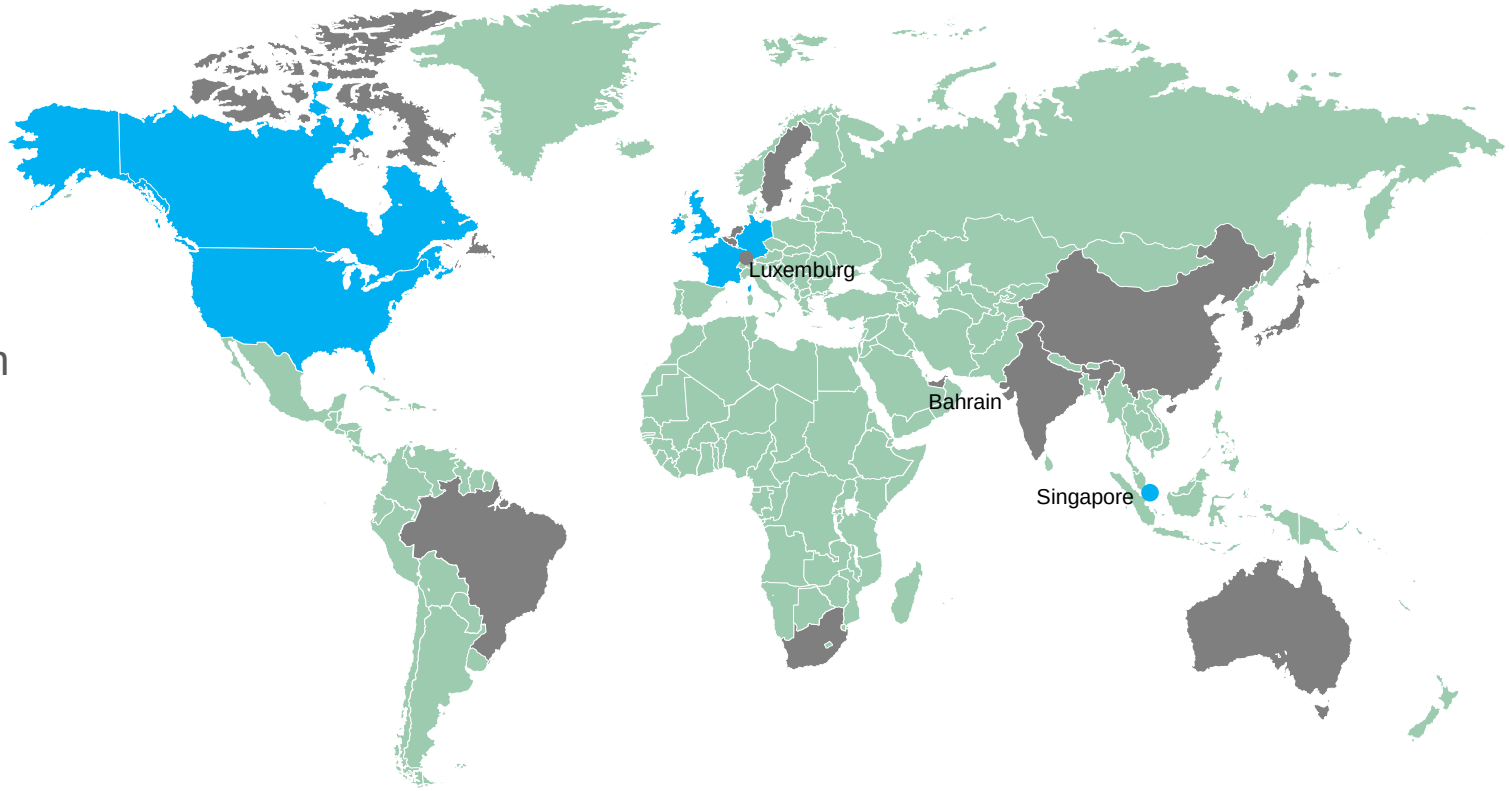
2 Separate accounts in charge of securing access to each perimeter in production.
Responsability: Secured Access, Network Isolation, Access Control

3 Separate accounts in charge of continuously evaluating the security of production independently of other accounts.
Responsability: identify security breaches if any, identify unexpected access, govern overall practices.

Data Residency

Storing & processing your data where it makes sense to you from a compliance perspective

- Encrypted secure storage (AWS S3) at any covered location of your choice.
- Mirroring of your data in the Disaster Recovery region of your choice to ensure the continuity of service should a disaster happen at a regional level.
- Regional network policies to prevent any access from a different region.



Already available or planned | Future | No plan

Customer Data Isolation

Strong Data & Processing Isolation per customer

Shared for reuse across all customer .

Serve a single customer at once.

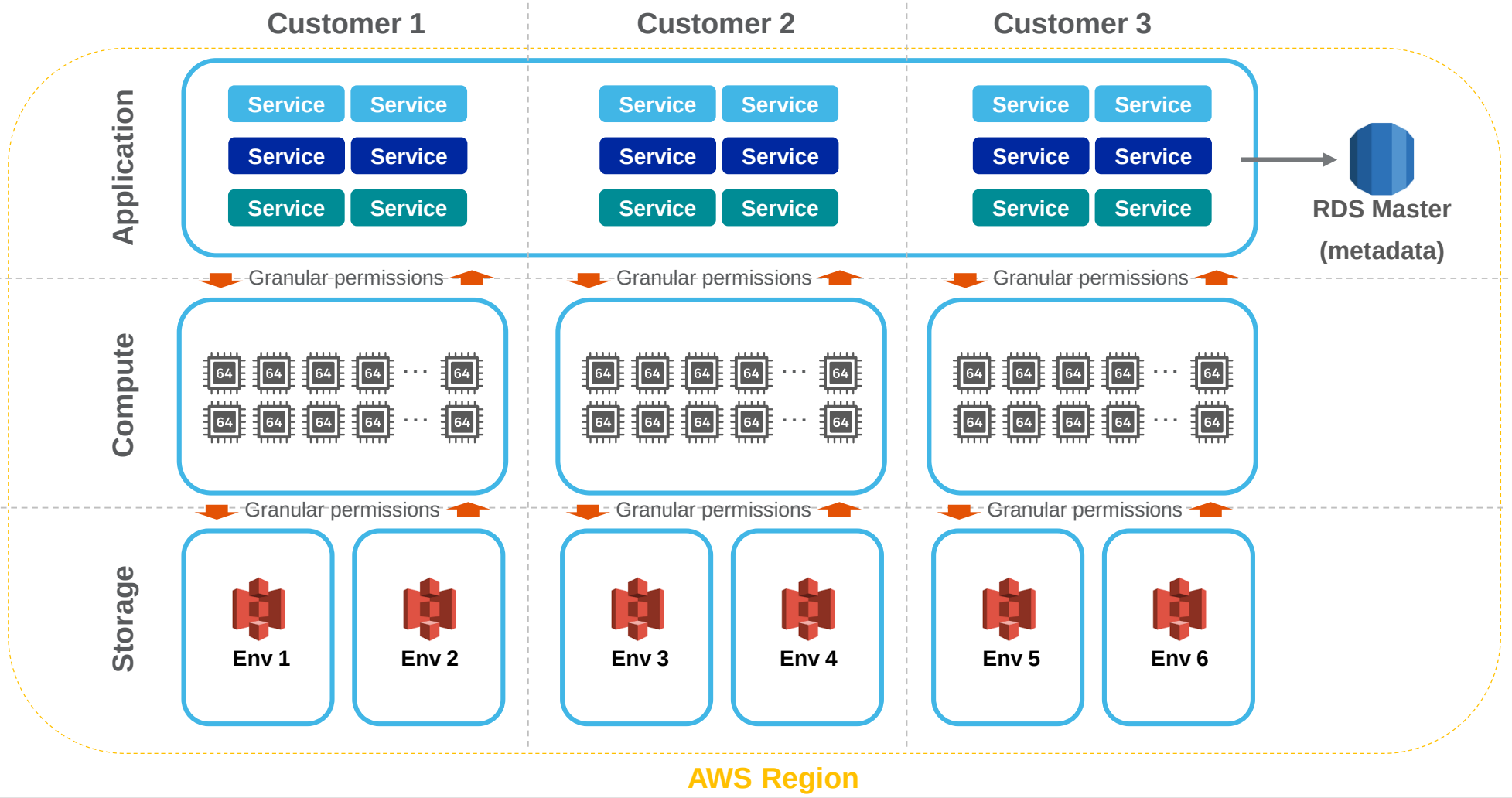
Processing cluster dedicated to a single customer.

Shared across all environments of same customer.

Storage is dedicated to a single environment.

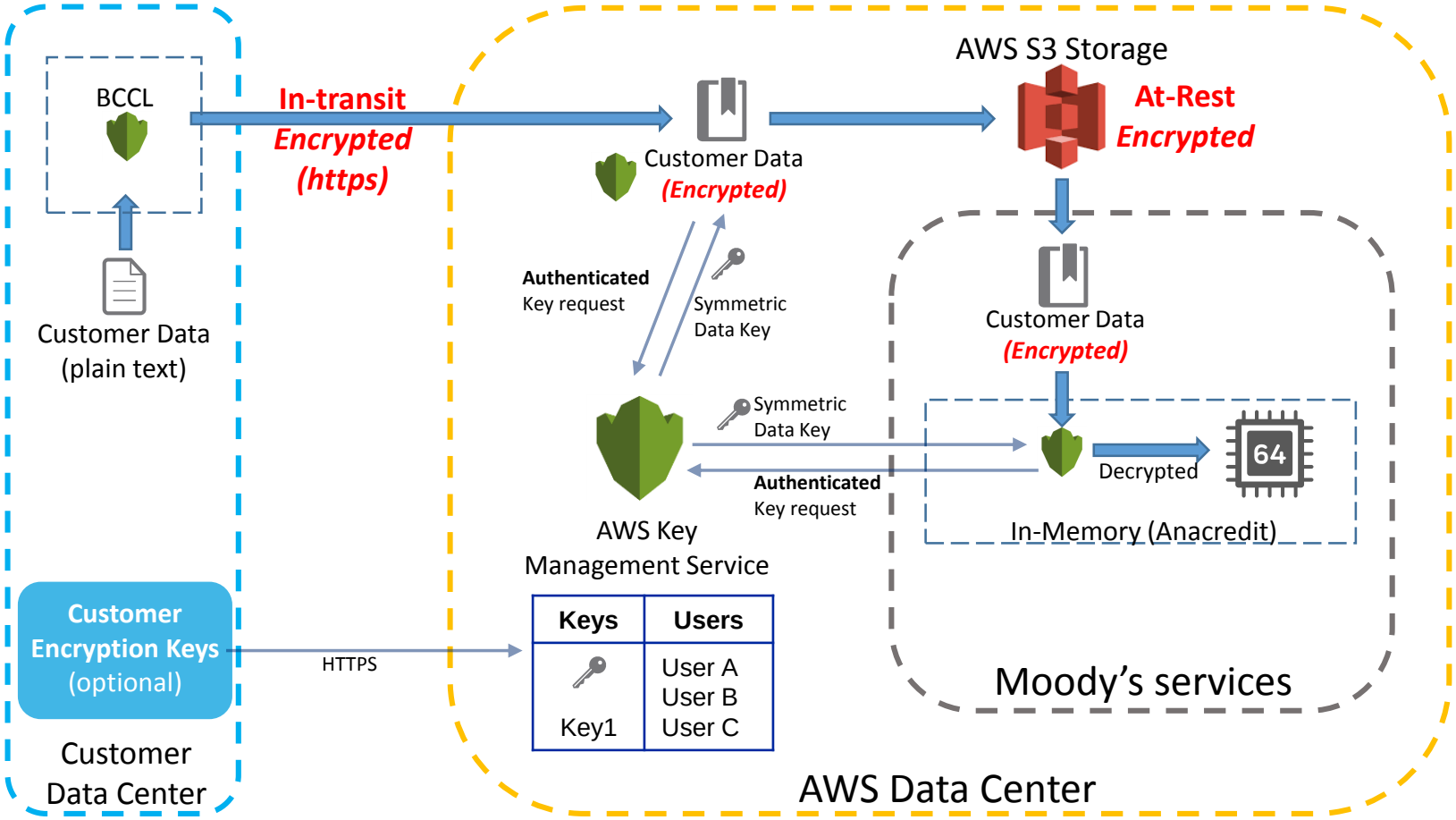
Strong encryption by design.

Only place where data remain.



Strong Encryption Policy End-to-End

- Rely on strong AWS encryption technology & practices.
- In-Transit or At-Rest, your data are encrypted end-to-end.
- Encryption Keys are only accessible to your users.
- Customer can manage Encryption Keys instead of Moody's Analytics.
- Our CloudOps cannot decrypt your data.



“Best Practices for SaaS Security”

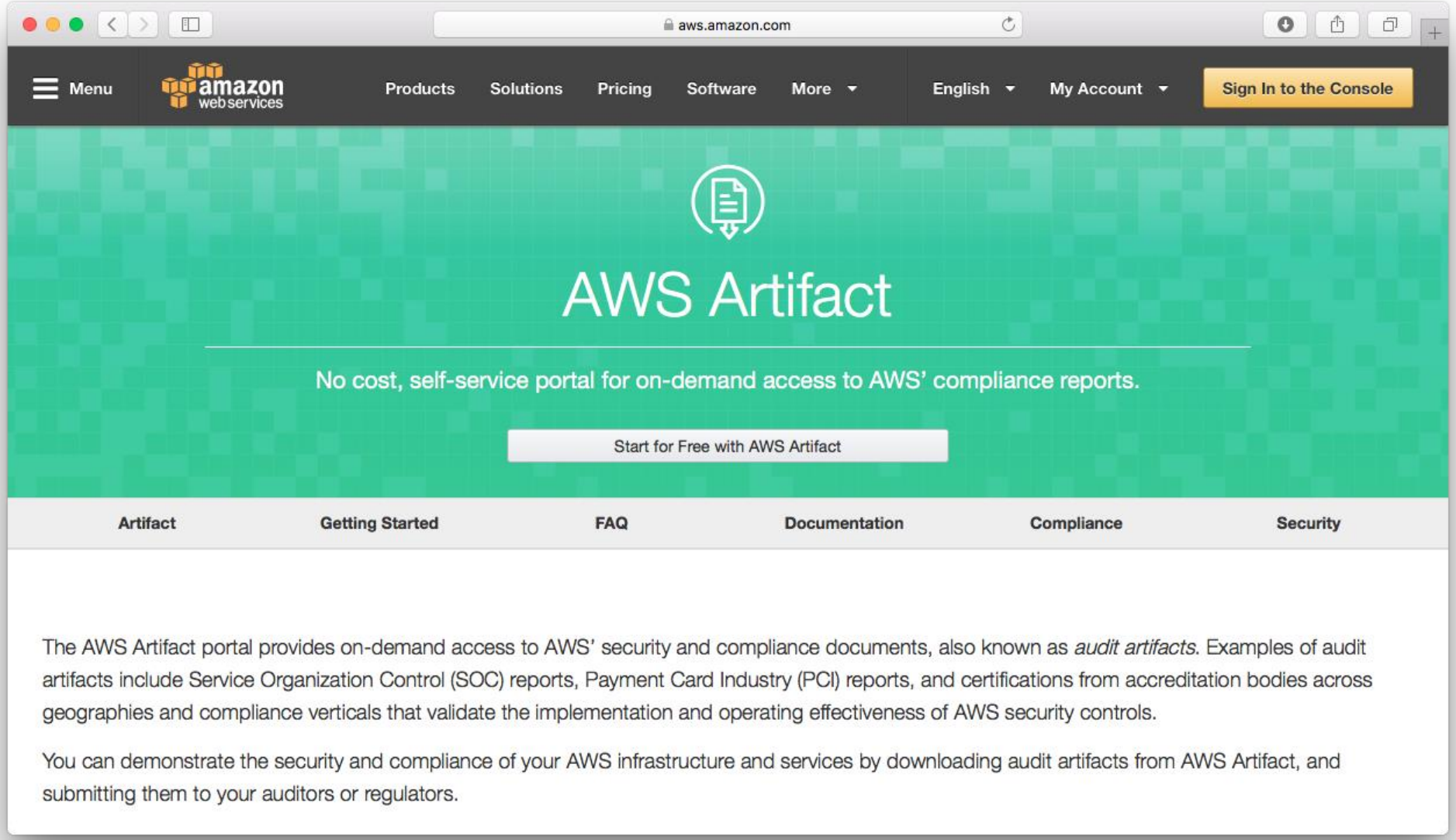
Dave Walker, Specialist Solutions Architect, Security and Compliance

Certifications

AWS and Compliance Standards

Certifications & Attestations		Laws, Regulations and Privacy		Alignments & Frameworks	
Cloud Computing Compliance Controls Catalogue (C5)	DE DE	CISPE	EU EU	CIS (Center for Internet Security)	
Cyber Essentials Plus	UK GB	EU Model Clauses	EU EU	CJIS (US FBI)	US US
DoD SRG	US US	FERPA	US US	CSA (Cloud Security Alliance)	
FedRAMP	US US	GLBA	US US	**Esquema Nacional de Seguridad**	ES ES
FIPS	US US	HIPAA	US US	EU-US Privacy Shield	EU EU
IRAP	AU U	HITECH		FISC	JP JP
ISO 9001		IRS 1075	US US	FISMA	US US
ISO 27001		ITAR	US US	G-Cloud	UK GB
ISO 27017		My Number Act	JP JP	GxP (US FDA CFR 21 Part 11)	US US
ISO 27018		Data Protection Act – 1988	UK GB	ICREA	
MLPS Level 3	CN CN	VPAT / Section 508	US US	IT Grundschutz	DE DE
MTCS	SG SG	Data Protection Directive	EU EU	MITA 3.0 (US Medicaid)	US US
PCI DSS Level 1		Privacy Act [Australia]	AU U	MPAA	US US
SEC Rule 17-a-4(f)	US US	Privacy Act [New Zealand]	NZ N	NIST	US US
SOC 1, SOC 2, SOC 3		PDPA - 2010 [Malaysia]	MY	Uptime Institute Tiers	
		PDPA - 2012 [Singapore]	SG SG	Cloud Security Principles	UK GB
		PIPEDA [Canada]	CA C		

The Artifact Service



Is “SaaS” Really “SaaS”?

AWS Shared Responsibility Model – Deep Dive

Will one model work for all services?

Infrastructure Services

Container Services

Abstract Services

AWS Shared Responsibility Model: for Abstract Services

Managed by

Customers

API Calls

Customer content

(optional)

Opaque Data: 1's and 0's

(in flight / at rest)

Client-Side Data Encryption
& Data Integrity Authentication

Data Protection by the Platform
Protection of Data at Rest

Network Traffic Protection by the Platform
Protection of Data at in Transit

AWS IAM

API Endpoints

Platform & Applications Management

Operating System, Network & Firewall Configuration

AWS Foundation Services

- **Compute**
- **Storage**
- **Database**
- **Networking**

AWS Global Infrastructure

- **Availability Zones**
- **Regions**
- **Edge Locations**

Managed by

amazon web services

aws

Infrastructure Service
Example – S3

AWS

- Foundational Services
- AWS Global Infrastructure
- AWS API Endpoints
- Operating System

- Platform / Application
- Data Protection (Rest - SSE, Transit)
- High Availability / Scaling

Customers

- Customer Data
- Data Protection (Rest – CSE)
- AWS IAM (Users, Groups, Roles, Policies)

Summary of Customer Responsibility in AWS

Infrastructure Services

- Data
- Customer IAM
- AWS IAM
- Applications
- Operating System
- Networking/Firewall

Container Services

- Data
- Customer IAM
- AWS IAM
- Firewall

Abstract Services

- Data
- AWS IAM

Permissions and Policy Management

Consider the 3 kinds of “human users”…

- Configurers of AWS services
  - …use the AWS APIs for the services involved
  - …via Console, CLI or SDK
- Maintainers and monitors of application configurations, data and activities within AWS services
  - …use some of the AWS APIs for the services involved, also via Console, CLI or SDK
  - …may also interact with service assets such as EC2 instances, at the CLI level
- Users of the applications running on the services
  - …may not even be aware that the applications are hosted on AWS

There are further “non-human users”…

- EC2 Instances
- ECS / EKS / Fargate Containers
- Lambda functions

IAM and Organizations are the Dual Arbiters of API Usage

- IAM: Users, Groups, Roles, Principals, Actions, Resources, Conditions
- Organizations: Accounts, Actions
- Centralised
- Federatable (IAM only)
- Mandatory
- Fine-grained
- Deny-by-default

Some Services have Further Access Control

- S3 Bucket Policies
- KMS Key Grants
- …

Anatomy of an IAM Policy

- JSON structure
  - Principals
  - Actions
  - Resources
  - Conditions
- Inline Policies
- Managed Policies
- See https://www.youtube.com/watch?v=aISWoPf_XNE

Roles are Special

- Recommendation:
  - Users have no permissions
  - Groups have permission to assume a Role
  - Roles have all the useful permissions
- Roles can also be assigned to EC2 Instances, Containers (ECS / EKS / Fargate) and Lambda functions
  - To execute AWS API calls on users' behalf
  - Necessary for automation!

Access Control with S3 Bucket Policies

- Other services also have their own access control mechanisms
- These work in concert with IAM and Organizations
- Recommendation: Implement the finest-granularity policy in the service's own mechanism, before "zooming out" to IAM and "out again" to Organizations SCPs for coarser-grained policy elements

Encryption

Encryption

- At Rest
- In Transit
- In Use(?)

Encryption: At Rest

- KMS
- CloudHSM Classic (in many Regions but not all; see https://docs.aws.amazon.com/general/latest/gr/rande.html)
- Work on integration for the new CloudHSM service is in progress

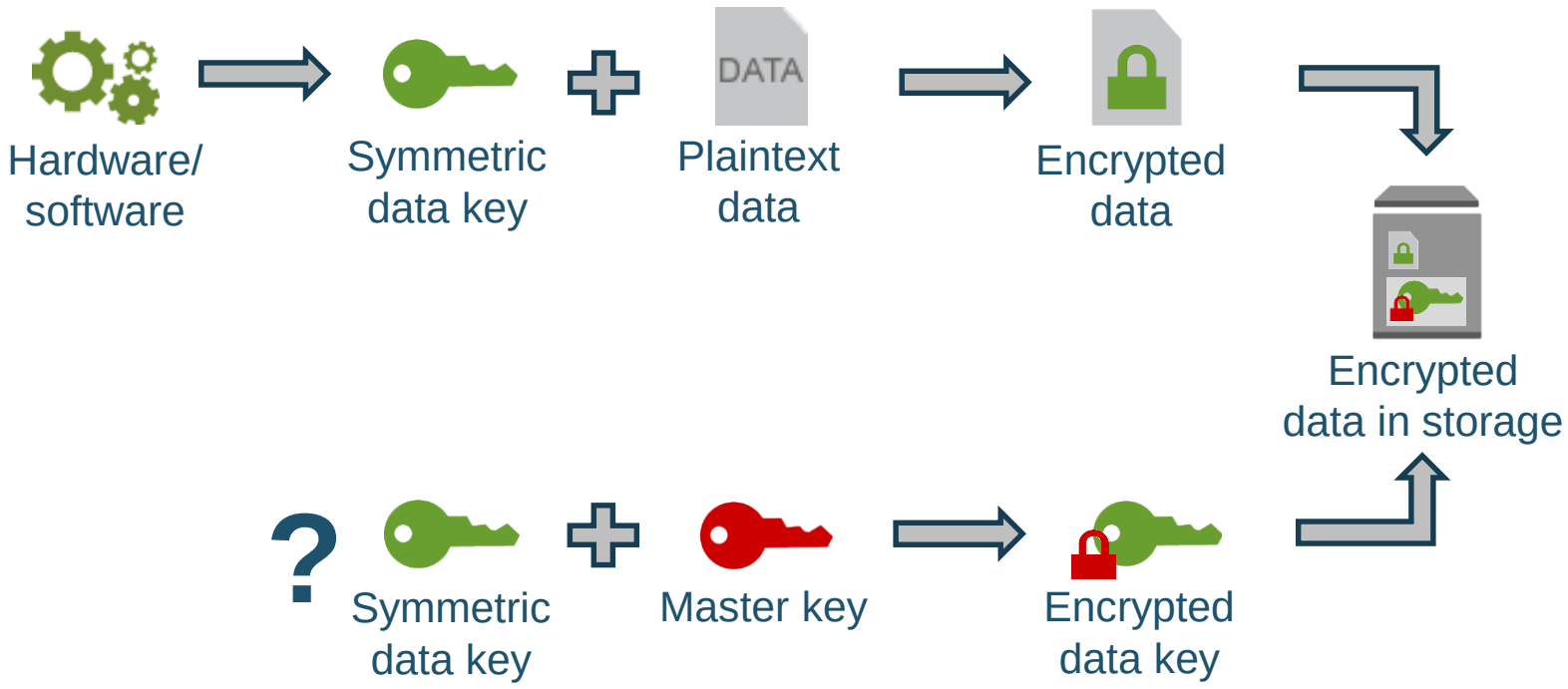
- CloudHSM Classic has FIPS 140-2 Level 2 certification (see
- CloudHSM has FIPS 140-2 Level 3 certification
- The update to KMS currently rolling-out has FIPS 140-2 Level 2 certification (see https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3009)

- Recommendation: “Unless you have a regulatory requirement which mandates the use of an HSM, use KMS”

More Detail:

- KMS: https://www.youtube.com/watch?v=X1eZjXQ55ec
- CloudHSM: https://www.youtube.com/watch?v=hEVks207ALM
- Whitepapers:
  - Encrypting Data at Rest: https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf
  - AWS Key Management Service Cryptographic Details: https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf

Data at rest encryption primer



Key hierarchy

“Key” questions to consider with any solution

Where are keys stored?

- Hardware you own?
- Hardware the cloud provider owns?

Where are keys used?

- Client software you control?
- Server software the cloud provider controls?

Who can use the keys?

- Users and applications that have permissions?
- Cloud provider applications you give permissions?

What assurances are there for proper security around keys?

Options for using encryption in AWS

Client-side encryption

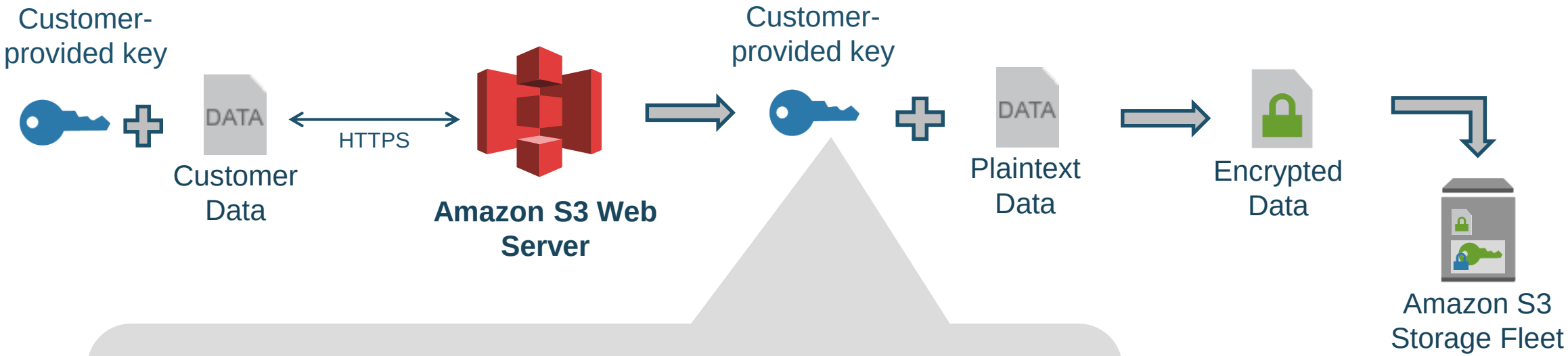
- You encrypt your data ***before*** data submitted to service
- You supply encryption keys OR use keys in your AWS account
- Available clients:
  - Amazon S3, Amazon EMR File System (EMRFS), Amazon DynamoDB

Server-side encryption

- AWS encrypts data on your behalf ***after*** data is received by service
- Integrated services:
  - S3, Amazon Elastic Block Store (Amazon EBS), Amazon RDS, Amazon Redshift, Amazon WorkMail, Amazon WorkSpaces, AWS CloudTrail, Amazon Simple Email Service (Amazon SES), Amazon Elastic Transcoder, AWS Import/Export Snowball, Amazon Kinesis Firehose

Server-side encryption in AWS

S3 server-side encryption with customer-provided encryption keys (SSE-C)

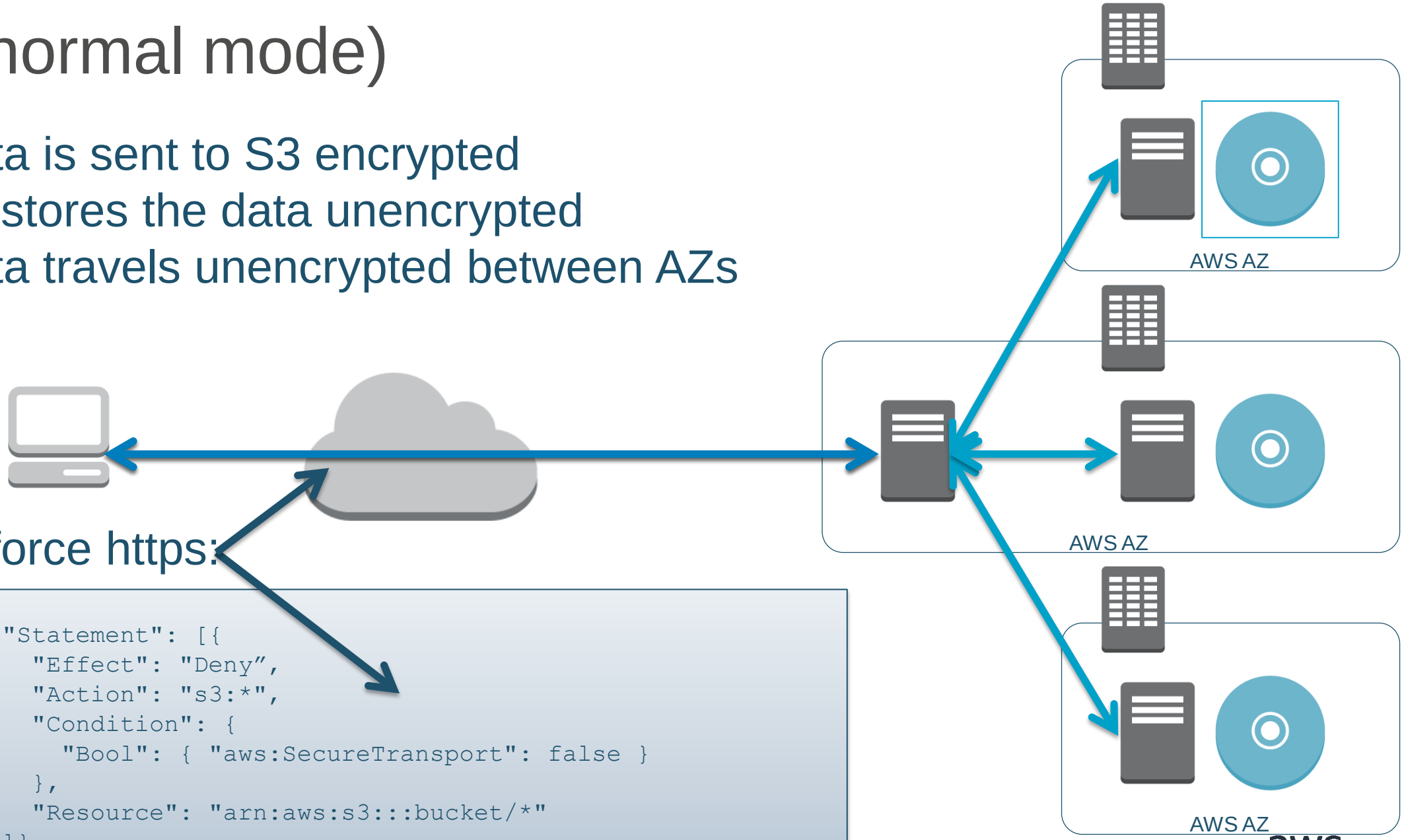


Key is used at S3 web server, and then deleted.

Customer must provide same key when downloading to allow S3 to decrypt data.

S3 (normal mode)

- Data is sent to S3 encrypted
- S3 stores the data unencrypted
- Data travels unencrypted between AZs

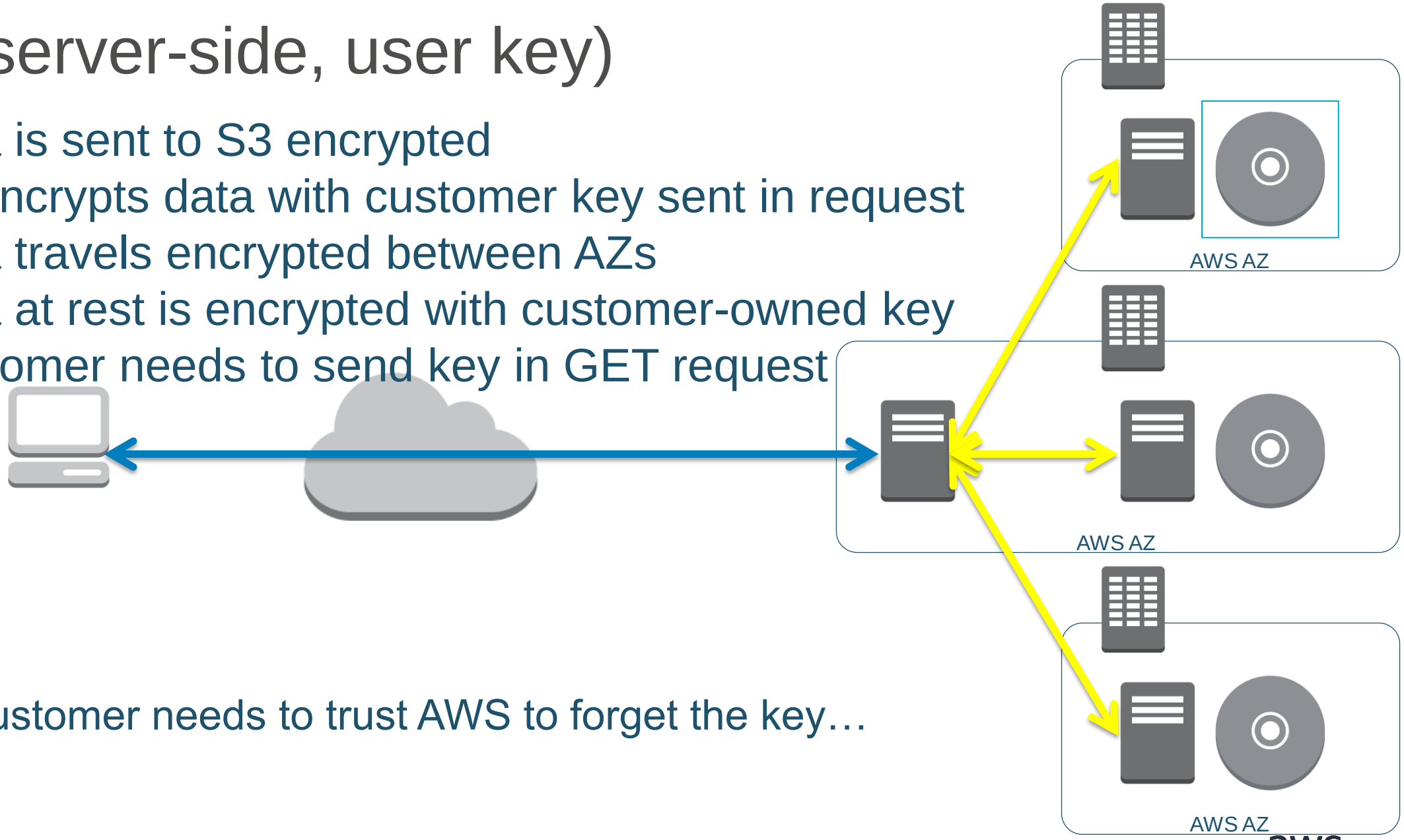


- Enforce https:

```
{
  "Statement": [{
    "Effect": "Deny”,
    "Action": "s3:*",
    "Condition": {
      "Bool": { "aws:SecureTransport": false }
    },
    "Resource": "arn:aws:s3:::bucket/*"
  ]}
}
```

S3 (server-side, user key)

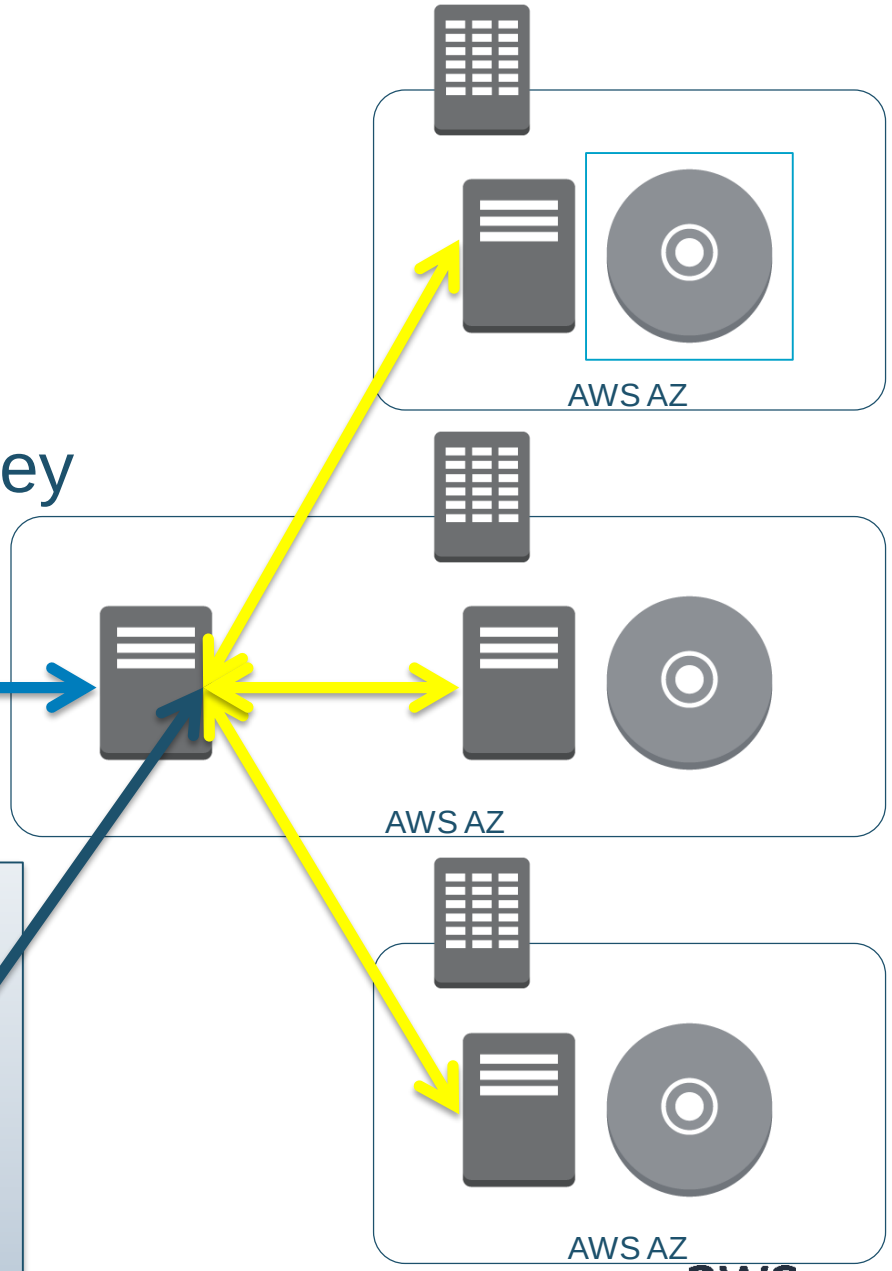
- Data is sent to S3 encrypted
- S3 encrypts data with customer key sent in request
- Data travels encrypted between AZs
- Data at rest is encrypted with customer-owned key
- Customer needs to send key in GET request



Customer needs to trust AWS to forget the key…

S3 (server-side encryption)

- Data is sent to S3 encrypted
- S3 encrypts data with AWS owned key
- Data travels encrypted between AZs
- Data at rest is encrypted with AWS-owned key

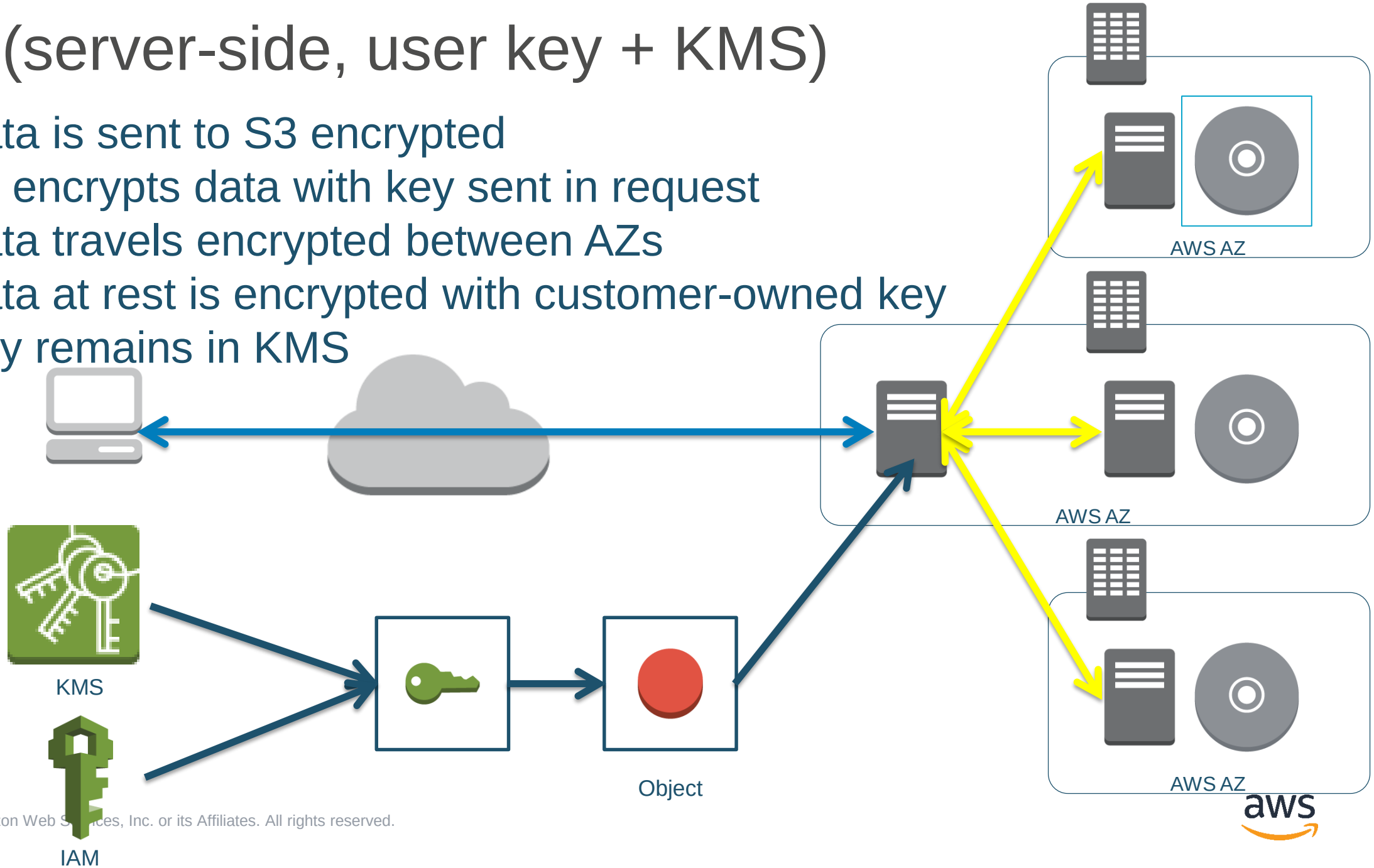


- Enforce at-rest encryption:

```
{
      "Statement":[{
         "Sid":"DenyUnEncryptedObjectUploads",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::YourBucket/*",
         "Condition":{
            "StringNotEquals":{
               "s3:x-amz-server-side-encryption":"AES256"
            } } } ] }
```

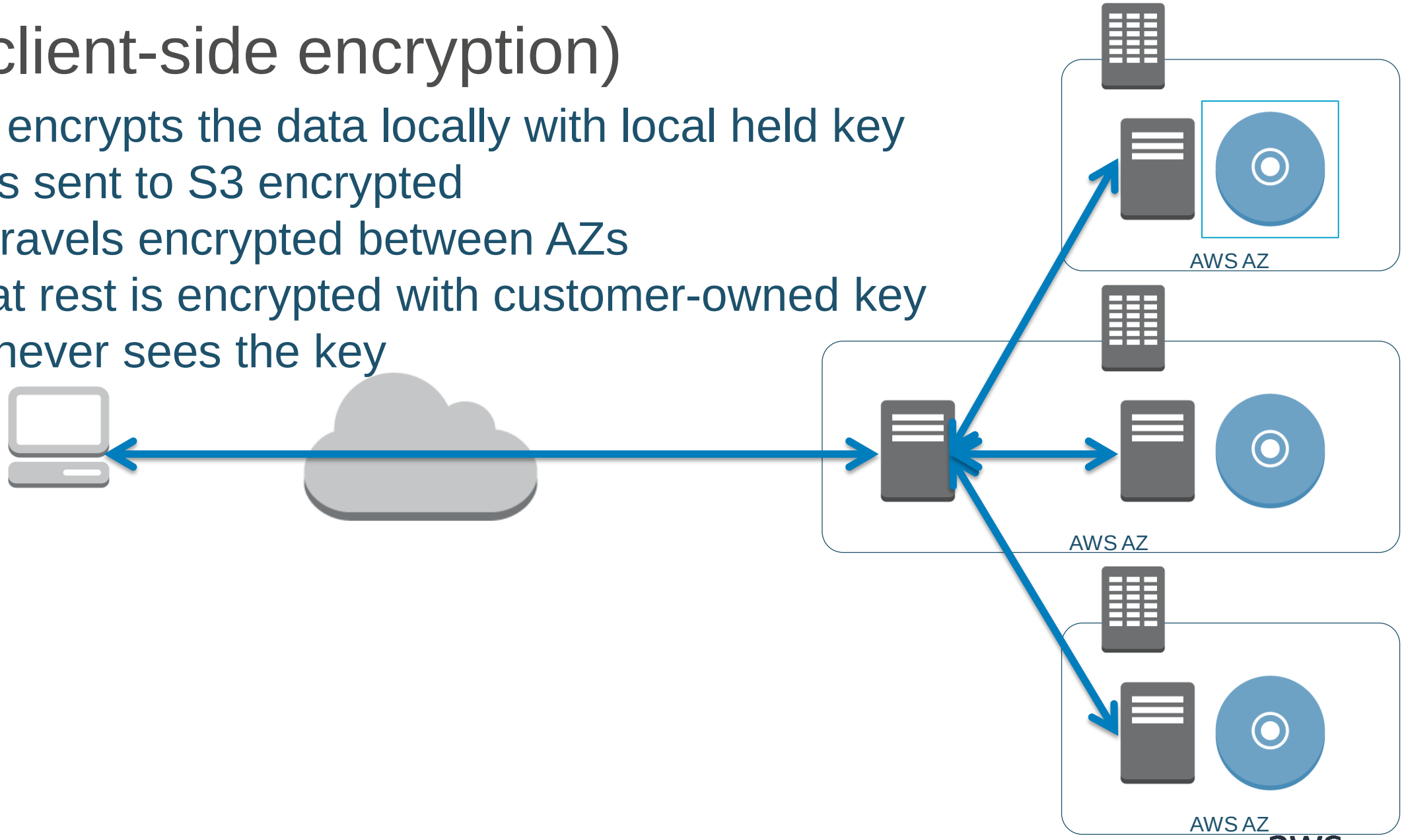
S3 (server-side, user key + KMS)

- Data is sent to S3 encrypted
- S3 encrypts data with key sent in request
- Data travels encrypted between AZs
- Data at rest is encrypted with customer-owned key
- Key remains in KMS



S3 (client-side encryption)

- Client encrypts the data locally with local held key
- Data is sent to S3 encrypted
- Data travels encrypted between AZs
- Data at rest is encrypted with customer-owned key
- AWS never sees the key



AWS Key Management Service (AWS KMS)

- Managed service that simplifies creation, control, rotation, deletion, and use of AES256 encryption keys in your applications
- Integrated with AWS server-side encryption
  - S3, EBS, RDS, Amazon Aurora, Amazon Redshift, Amazon WorkMail, Amazon WorkSpaces, AWS CloudTrail, and Amazon Elastic Transcoder
- Integrated with AWS client-side encryption
  - AWS SDKs, S3 encryption client, EMRFS client, and DynamoDB encryption client
- Integrated with CloudTrail to provide auditable logs of key usage for regulatory and compliance activities
- Available in all commercial regions except China

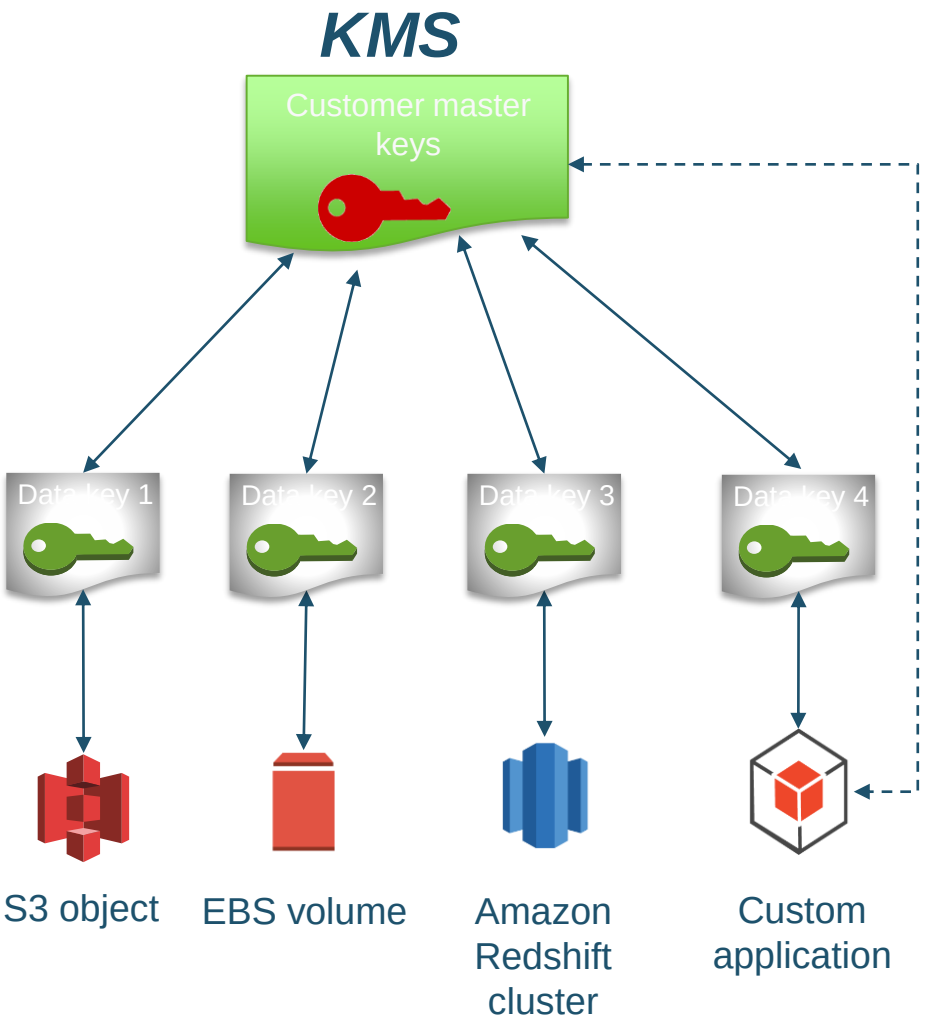
How clients and AWS services typically integrate with KMS

Two-tiered key hierarchy using envelope encryption

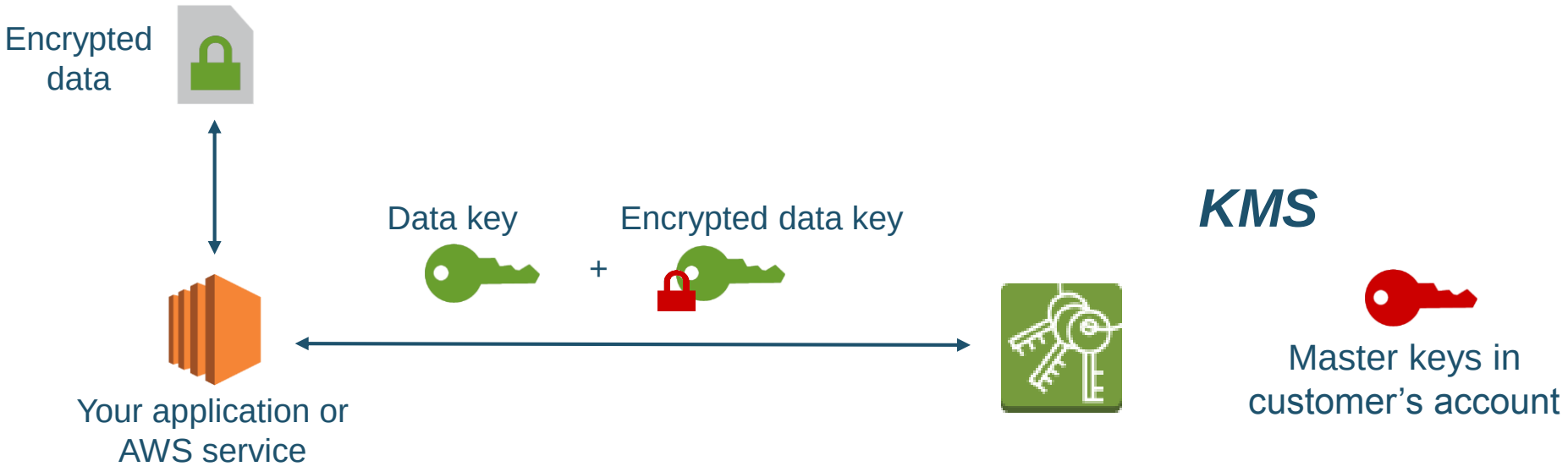
- Unique data key encrypts customer data
- KMS master keys encrypt data keys

Benefits

- Limits risk of compromised data key
- Better performance for encrypting large data
- Easier to manage small number of master keys than millions of data keys
- Centralized access and audit of key activity



How AWS services use your KMS keys



1. Client calls `kms:GenerateDataKey` by passing the ID of the KMS master key in your account.
2. Client request is authenticated based on permissions set on both the user and the key.
3. A unique data encryption key is created and encrypted under the KMS master key.
4. The plaintext and encrypted data key is returned to the client.
5. The plaintext data key is used to encrypt data and is then deleted when practical.
6. The encrypted data key is stored; it's sent back to KMS when needed for data decryption.

You control how and when your KMS keys can be used and by whom

Sample permissions on a key:

- Can only be used for encryption and decryption by <*these users and roles*> in <*this account*>
- Can only be used by application A to encrypt data, but only used by application B to decrypt data
- Can only be used to decrypt data if the service resource is active and additional parameters about the resource are passed in the call
- Can be managed only by this set of administrator users or roles

Fully integrated with AWS Identity and Access Management

Auditability of KMS key usage through AWS CloudTrail

"EventName":"DecryptResult",	**This KMS API action was called…**
"EventTiime":"2014-08-18T18:13:07Z",	**….at this time**
"RequestParameters": "{\"keyId\":\"2b42x363-1911-4e3a-8321-6b67329025ex”}”,	**…in reference to this key**
“EncryptionContext":"volumeid-12345",	**…to protect this AWS resource**
"SourceIPAddress":" 203.0.113.113",	**…from this IP address**
"UserIdentity": “{\"arn\":\"arn:aws:iam:: 111122223333:user/User123“}	**…by this AWS user in this account**

KMS APIs to build your own applications

Example management API actions

- CreateKey, CreateAlias
- DisableKey
- EnableKeyRotation
- PutKeyPolicy
- ListKeys, DescribeKey

Example data API actions

- Encrypt
- Decrypt
- ReEncrypt
- GenerateDataKey

26 API actions and growing

http://docs.aws.amazon.com/kms/latest/APIReference/Welcome.html

KMS assurances

Why should you trust AWS with your keys?

- Your plaintext keys are never stored in nonvolatile memory
- There are no tools in place to access your physical key material
- You control who has permissions to use your keys
- There is separation of duties between systems that use master keys and ones that use data keys with multiparty controls
- You can find evidence of every KMS API call in CloudTrail for you to monitor
- Also, there is third-party evidence of these controls:
    - Service Organization Control (SOC 1)
    - PCI-DSS
    - New update has completed FIPS 140-2
    - See AWS Compliance packages for details

Encryption

- At Rest
- In Transit
- In Use(?)

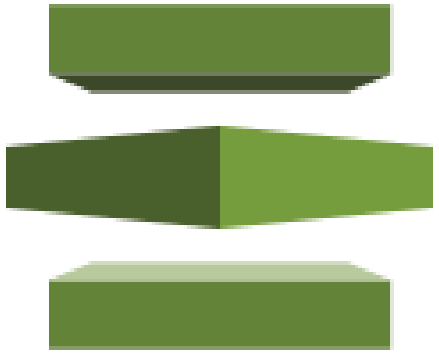
Authenticating AWS to You and Protecting Confidentiality using TLS

- TLS is used with every AWS API to protect data upload/download and configuration change, using unidirectional trust from the endpoint and ACM certificate / key pairs

- You can provide your own certificates to be presented to your customers when using:
  - Amazon Elastic Load Balancing
  - Amazon CloudFront (content distribution network)
  - Amazon API Gateway (new!)

AWS Certificate Manager (ACM)

- Provision trusted TLS certificates from AWS for use with AWS resources:
  - Elastic Load Balancing
  - Amazon CloudFront distributions
- AWS handles the drudgery
  - Key pair and CSR generation
  - Managed renewal and deployment
- Domain validation (DV) through email, DNS
- Available through AWS Management Console, AWS Command Line Interface (AWS CLI), or API



ACM-provided certificates

Domain names

- Single domain name: www.example.com
- Wildcard domain names: *.example.com
- Combination of wildcard and non-wildcard names
- Multiple domain names in the same certificate (up to 10)

ACM-provided certificates are **managed**

- Private keys are generated, protected, and managed
- ACM-provided certificates cannot be used on Amazon EC2 instances or on-premises servers
- For certificate issuance and handling policies, see https://www.amazontrust.com/repository/

Algorithms

- RSA-2048 and SHA-256

Free

Making TLS work better in your Apps

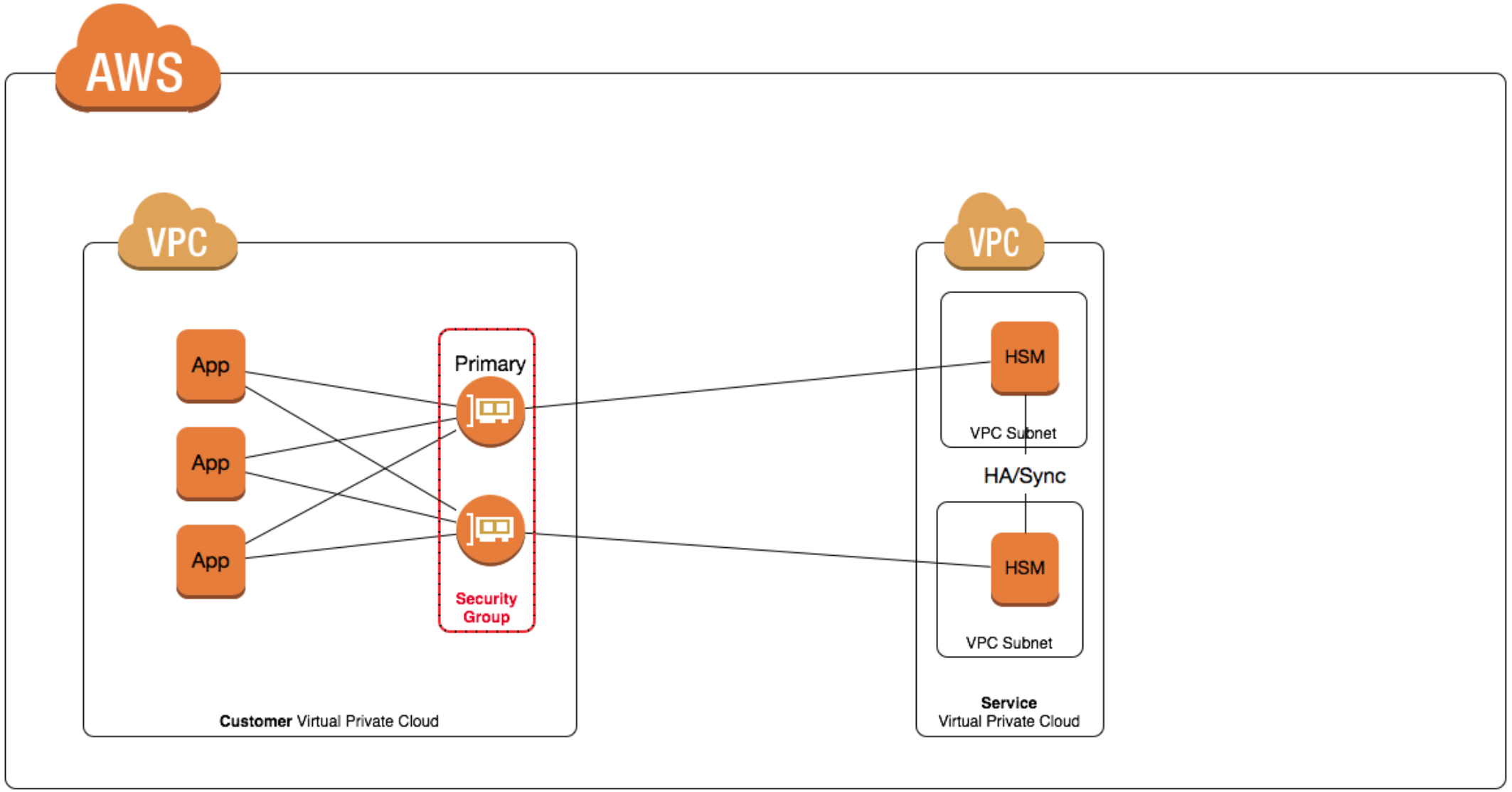
- “signal to noise”
- A TLS library designed by AWS to help your developers implement transport security
- Avoids implementing rarely-used TLS options and extensions; ~6,000 lines of code

https://github.com/awslabs/s2n

Encryption

- At Rest
- In Transit
- <u>In Use(?)</u>

New CloudHSM Architecture



Managed Backup

- AWS CloudHSM backs up encryption keys and entire HSM configuration, including users and policies.
- Your backups are encrypted by the HSM manufacturer and AWS.
  - Backups can only be decrypted inside your HSM
  - Manufacturer secret embedded in encrypted firmware
  - AWS secret loaded during initialization
  - Stored on Amazon S3 for high durability with extra layer of encryption with AWS Key Management Service (AWS KMS)
- You can clone your backups to create new clusters.

Total Control of Access Management

- AWS CloudHSM offers you secure HSM access to create users and policies.
- You can create granular access management policies for up to 1,024 users on your HSMs.
- Each user is in a private sandbox and can create keys that are not visible to other users.
- Keys can be shared with up to 8 other users who can use (but not manage) that specific key.
- AWS has no access to your encryption keys.

Separation of Duties

- Manufacturer
  - Produces, certifies and signs FIPS-validated firmware
- AWS
  - **No access** to crypto functions and **cannot** observe client<->HSM communications
  - Initialize (and zeroize) the adapter
  - Create and destroy/zeroize individual HSM's
  - Update firmware (FIPS validated only)
  - Backup and Restore HSMs (encrypted backups)
  - Manage Clustering (add/remove nodes, sync)
- Customer
  - All key management and cryptographic functions
  - Administrate authentication and access control to HSM (users, privileges, policies)
  - Perform file-based backup

Thank you!

Q&A