



Protecting Your Data in AWS

Danielle Greshock
Manager, Solutions Architecture

September 28, 2016



What to expect from this session

- Understand your options for protecting your data with encryption in AWS
- Securing access to data on Amazon S3 using policies
- Database platform security
- Automatically validate and audit your data protection policies

Transport security

Authenticating AWS to you and protecting confidentiality using TLS

- TLS can be used with every AWS API to protect data upload/download and configuration change
- You can provide your own certificates to be presented to your customers when using:
 - Amazon Elastic Load Balancing
 - Amazon CloudFront (content distribution network)

AWS Certificate Manager (ACM)

- Provision trusted SSL/TLS certificates from AWS for use with AWS resources:
 - Elastic Load Balancing
 - Amazon CloudFront distributions
- AWS handles the muck
 - Key pair and CSR generation
 - Managed renewal and deployment
- Domain validation (DV) through email
- 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
- Can be used with AWS services, such as Elastic Load Balancing and Amazon CloudFront

Algorithms

- RSA 2048 and SHA-256

A white rectangular box containing the word "Free" in a large, bold, black sans-serif font.

Making TLS work better in your apps

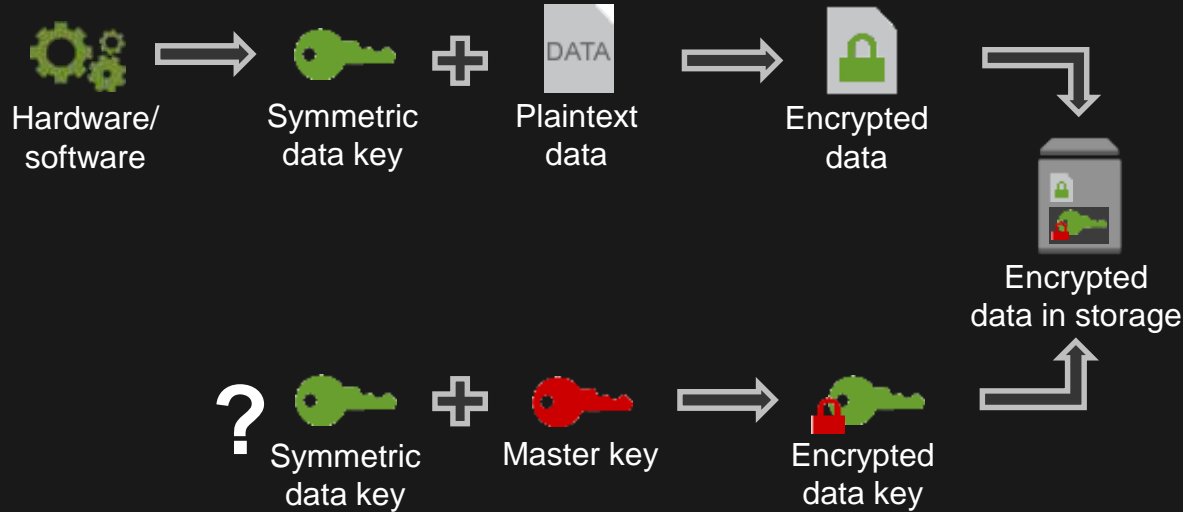


- “signal to noise”
- A TLS library designed by AWS to help your developers implement transport security
- Avoids implementing rarely-used TLS options and extensions; ~6,000 lines of code

<https://github.com/awslabs/s2n>

Data at rest security

Data at rest encryption primer



“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

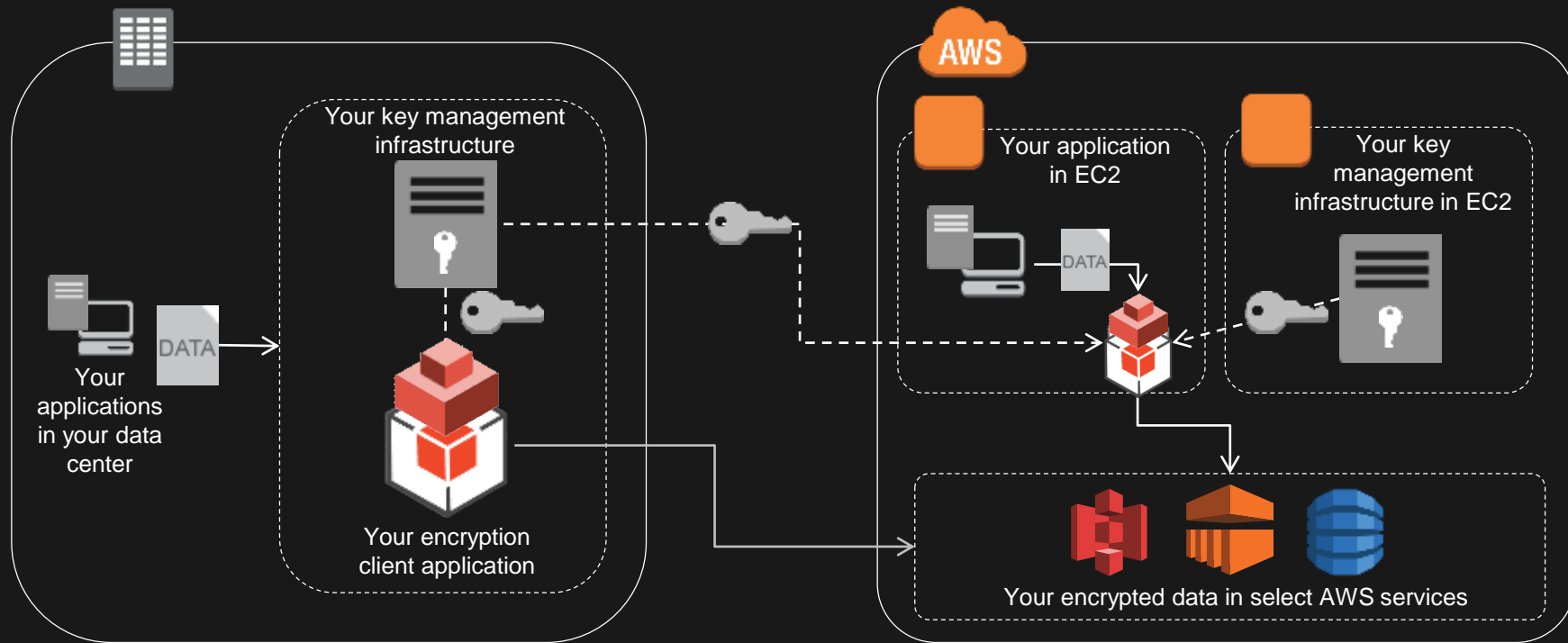
- You encrypt your data **before** data submitted to service
- You supply encryption keys OR use keys in your AWS account
- Available clients:
 - Amazon S3, Amazon EMR File System (EMRFS), Amazon DynamoDB

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

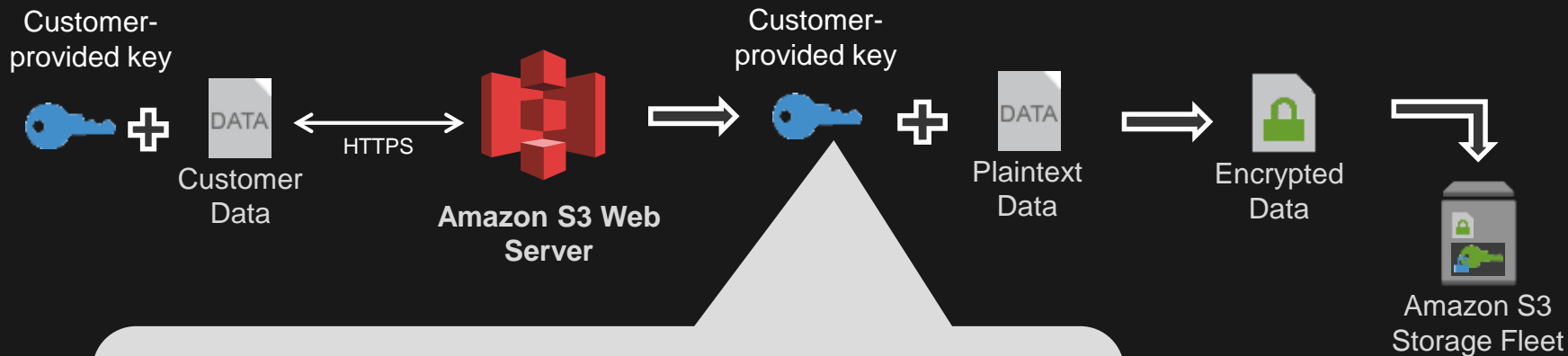
Client-side encryption in AWS

S3/EMRFS and DynamoDB encryption clients in AWS SDKs



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.

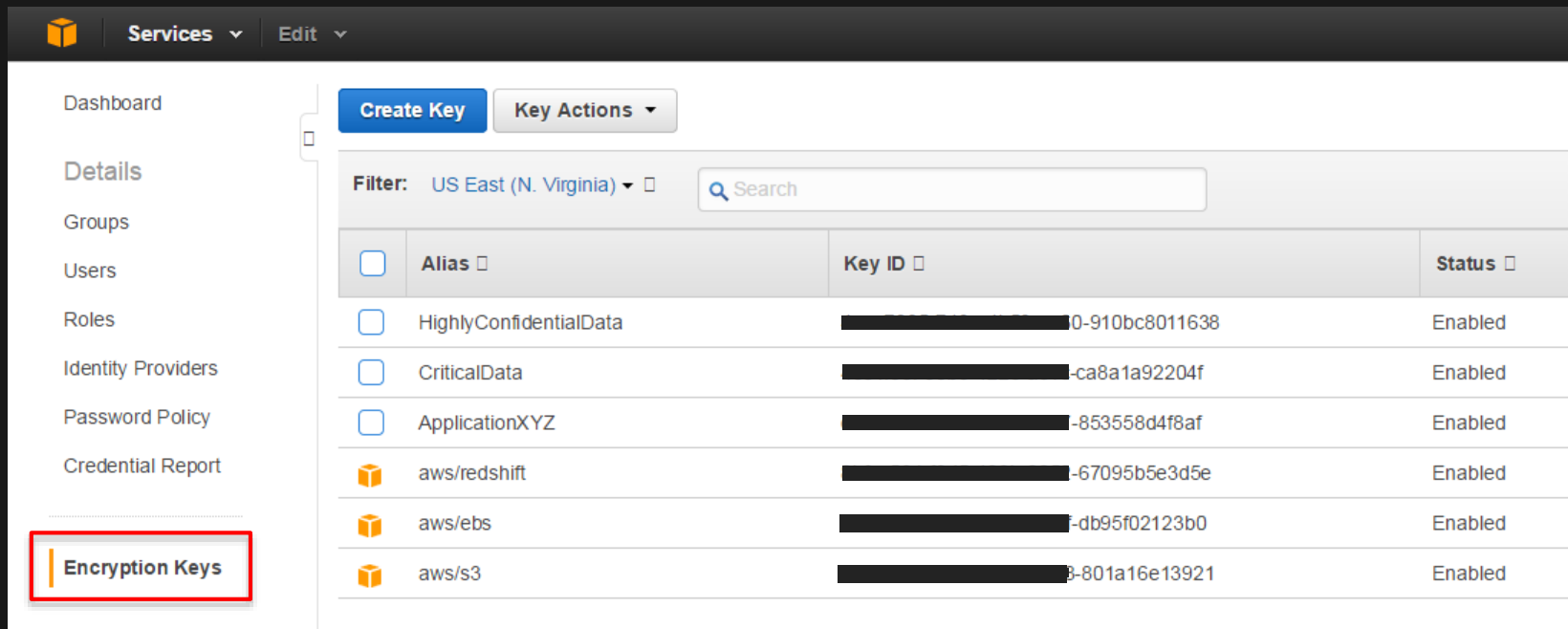
Customer must provide same key when downloading to allow S3 to decrypt data.

AWS Key Management Service (AWS KMS)




- Managed service that simplifies creation, control, rotation, deletion, and use of 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

AWS KMS

Integrated with AWS Identity and Access Management (IAM) console



The screenshot displays the AWS KMS console interface. On the left is a navigation sidebar with links to Dashboard, Details, Groups, Users, Roles, Identity Providers, Password Policy, and Credential Report. The 'Encryption Keys' link is highlighted with a red box. The main content area features a 'Create Key' button and a 'Key Actions' dropdown. Below these is a filter section showing 'US East (N. Virginia)' and a search bar. A table lists several keys, each with a checkbox, an alias, a key ID, and a status. The keys are: HighlyConfidentialData, CriticalData, ApplicationXYZ, aws/redshift, aws/ebs, and aws/s3. All keys are in an 'Enabled' state.

<input type="checkbox"/>	Alias <input type="checkbox"/>	Key ID <input type="checkbox"/>	Status <input type="checkbox"/>
<input type="checkbox"/>	HighlyConfidentialData	████████████████████0-910bc8011638	Enabled
<input type="checkbox"/>	CriticalData	████████████████████-ca8a1a92204f	Enabled
<input type="checkbox"/>	ApplicationXYZ	████████████████████-853558d4f8af	Enabled
	aws/redshift	████████████████████-67095b5e3d5e	Enabled
	aws/ebs	████████████████████-db95f02123b0	Enabled
	aws/s3	████████████████████3-801a16e13921	Enabled

KMS integration with AWS services

- **Storage:** EBS, S3, Snowball
- **Database:** All RDS engines
- **Data Analytics:** Amazon Redshift, EMR, Amazon Kinesis Firehose
- **Enterprise Apps:** WorkMail, WorkSpaces
- **Developer Tools:** AWS CodeCommit
- **Management:** CloudTrail
- **App Svcs:** Elastic Transcoder, Simple Email Service
- **AWS IoT**

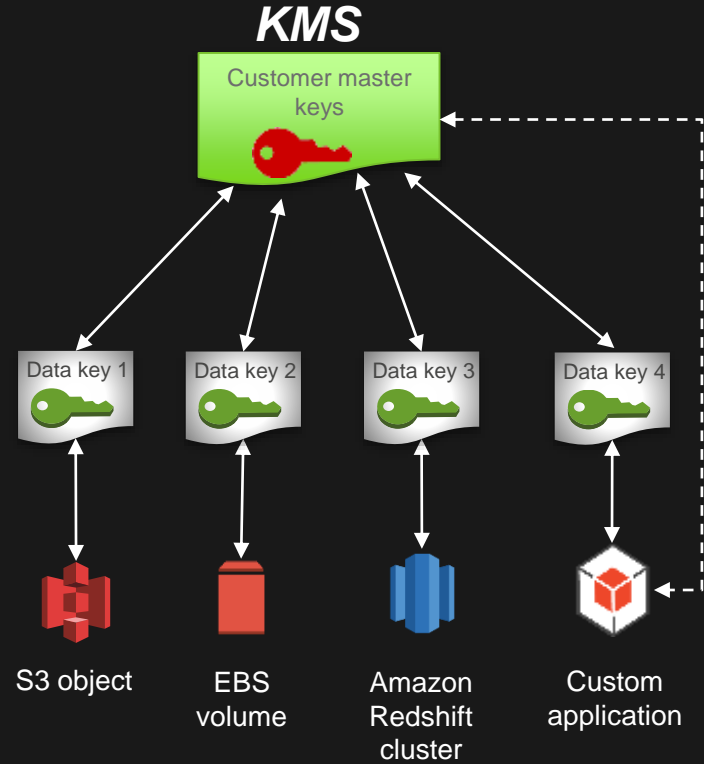
How clients and AWS services typically integrate with KMS

Two-tiered key hierarchy using envelope encryption

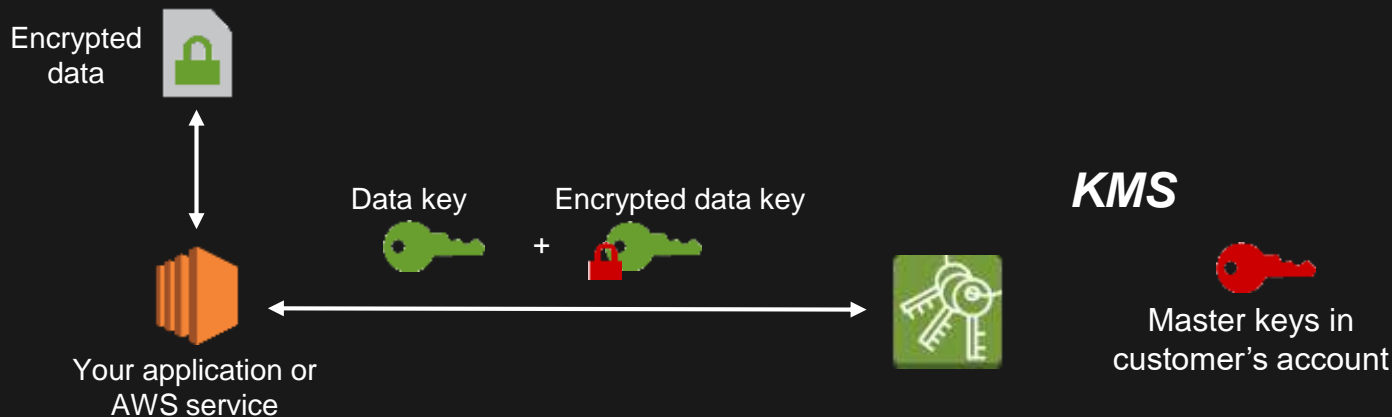
- Unique data key encrypts customer data
- KMS master keys encrypt data keys

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

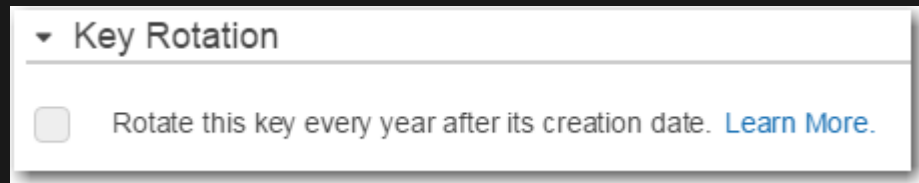
Sample permissions on a key:

- 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

Rotating master keys in KMS

Console (Key Summary Page)



AWS CLI

```
enable-key-rotation --key-id <value>
```

What key rotation means:

- A new version of a master key is created, but mapped to the same key ID or alias
- All new encryption requests use the new version
- All previous versions of keys are kept to perform decryption on older ciphertexts

There is nothing users or applications need to do after a rotation—the same key ID or alias just works

Auditability of KMS key usage through AWS CloudTrail

"EventName": "DecryptResult",

This KMS API action was called...

"EventTime": "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"}"

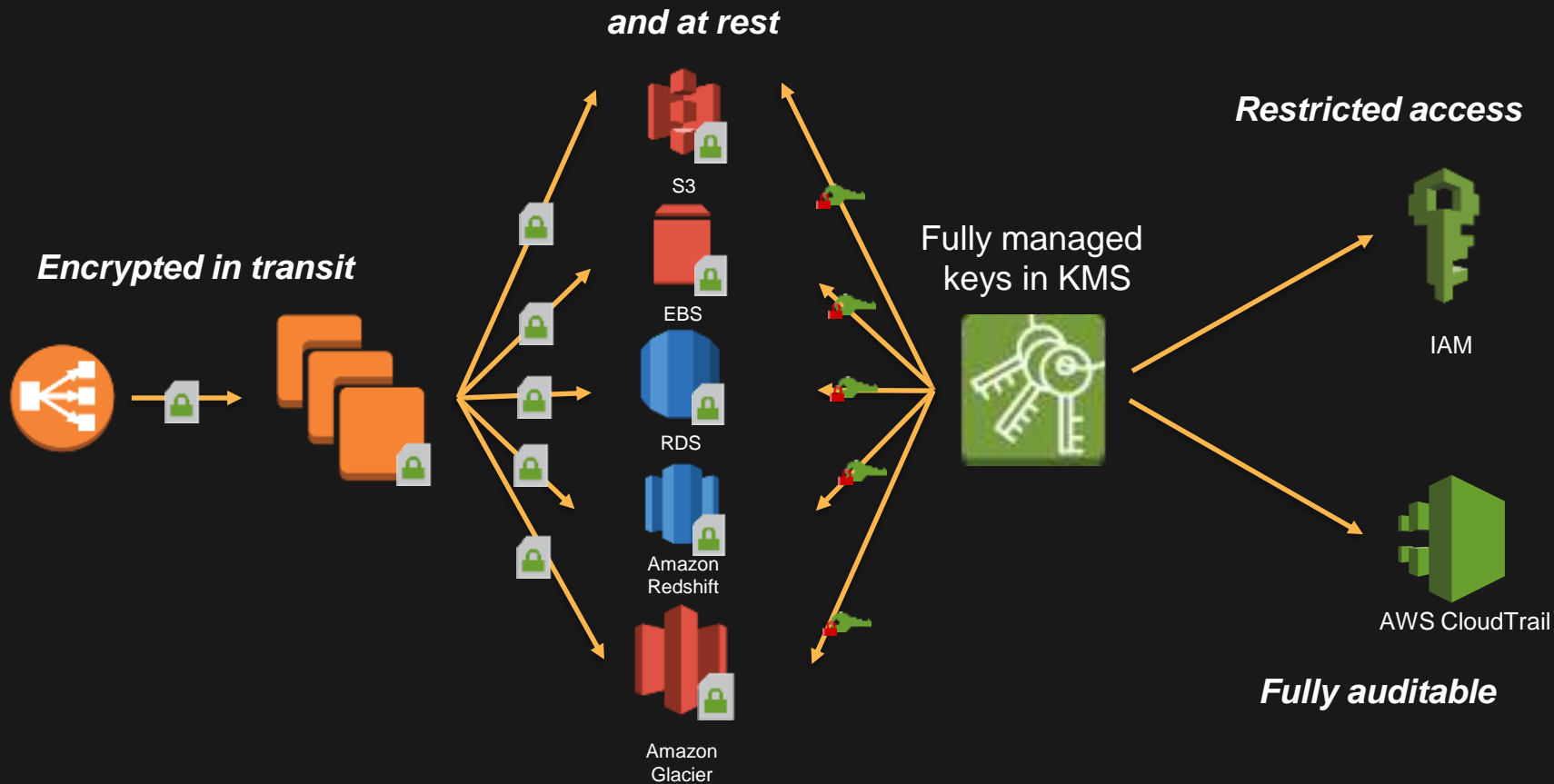
...by this AWS user in this account

KMS 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
 - See AWS Compliance packages for details

Ubiquitous encryption



Pricing for KMS

\$1/key version/month

\$0.03 per 10,000 API requests (\$0.04 per 10,000 API requests in AWS GovCloud)

- 20,000 free requests per month

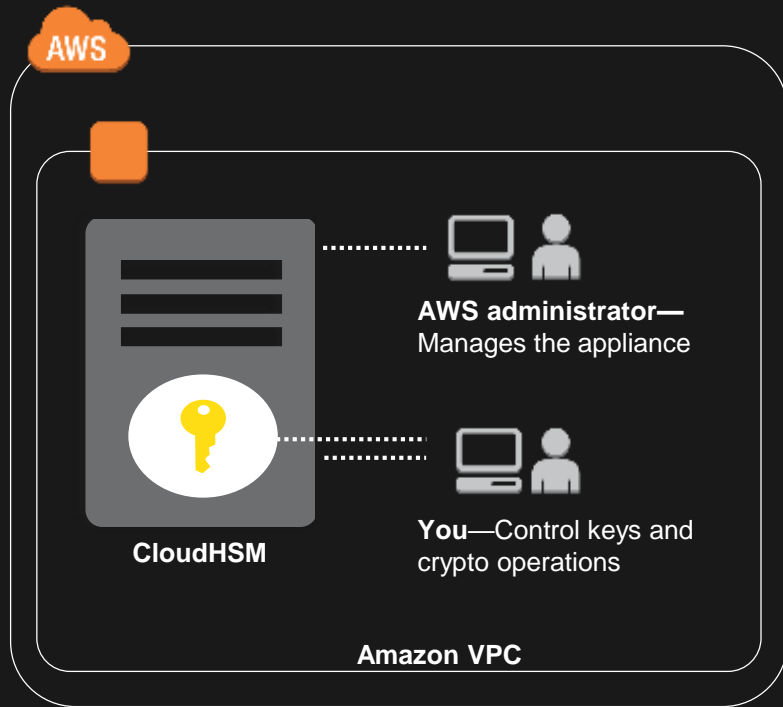
Alternatives to KMS

In order to have different controls over the security of your keys

1. AWS CloudHSM
2. AWS Partner solutions
3. Do it yourself

AWS CloudHSM

- You receive **dedicated access** to HSM appliances
- HSMs located in AWS data centers
- Managed and monitored by AWS
- **Only you have access to your keys and operations on the keys**
- HSMs are inside your Amazon VPC—
isolated from the rest of the network
- Uses SafeNet Luna SA HSM appliances



AWS CloudHSM

Available in eight regions worldwide

- US East (N. Virginia), US West (Oregon), AWS GovCloud (US), EU (Ireland), EU (Frankfurt), Asia Pacific (Sydney), Asia Pacific (Singapore) and Asia Pacific (Tokyo)

Compliance

- Included in AWS PCI DSS and SOC-1 compliance packages
- FIPS 140-2 level 2 (maintained by Gemalto/SafeNet)

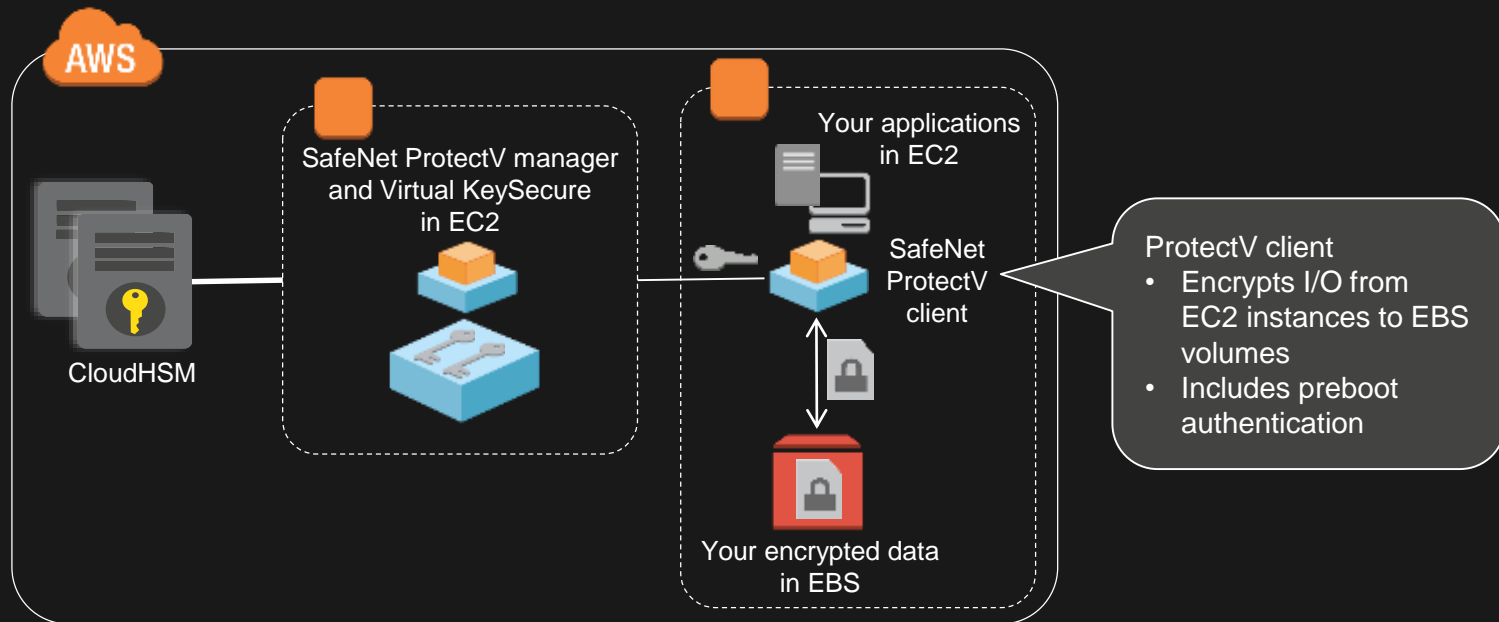
Typical use cases

- Use with Amazon Redshift and RDS for Oracle
- Integrate with third-party software (Oracle, Microsoft SQL Server, Apache, SafeNet)
- Build your own custom applications

EBS volume encryption with CloudHSM and SafeNet Software

SafeNet ProtectV with Virtual KeySecure

CloudHSM stores the master key



Pricing for CloudHSM

- HSM provisioned in any region has a \$5,000 one-time charge
- Starting at \$1.88/hour metered charge after setup
 - Hourly rate varies by region
- As low as \$21,500 in year one; \$16,500 in subsequent years
- Requests not billed; limited only by the device capacity
 - Varies depending on algorithm and key size

Comparing CloudHSM with KMS

CloudHSM

- Dedicated access to one or more HSM devices that comply with government standards (for example, FIPS 140-2, Common Criteria)
- You control all access to your keys and the application software that uses them
- Supported applications:
 - Your custom software
 - Third-party software
 - AWS services: Amazon Redshift, RDS for Oracle

KMS

- Highly available and durable key storage, management, and auditable service
- Easily encrypt your data across AWS services and within your own applications based on policies you define
- Supported applications:
 - Your custom software built with AWS SDKs/CLI
 - AWS services (S3, EBS, RDS, Amazon Aurora, Amazon Redshift, WorkMail, WorkSpaces, CloudTrail, Elastic Transcoder)

Partner solutions in AWS Marketplace

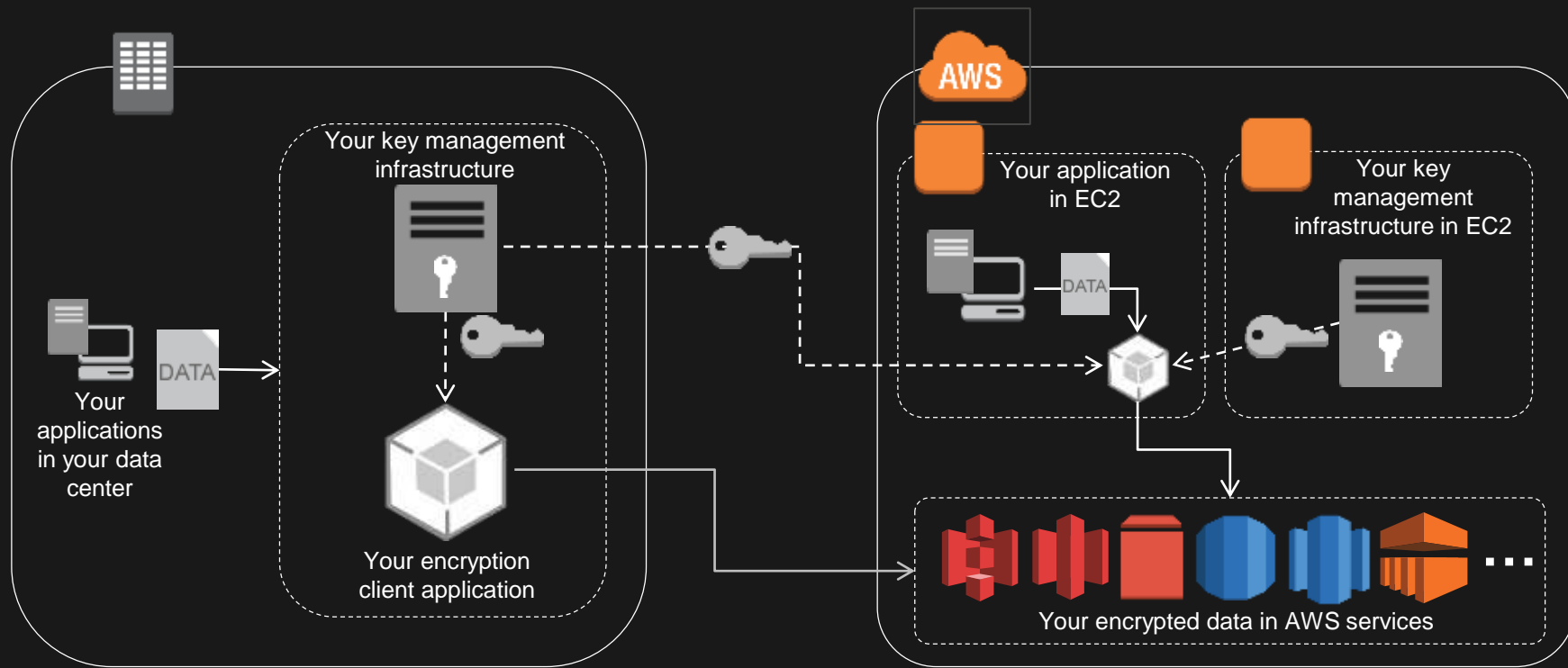
- Browse, test, and buy encryption and key management solutions
- Pay by the hour, monthly, or annually
- Software fees added to AWS bill
- Bring Your Own License

A screenshot of the AWS Marketplace interface for a partner solution. The interface is divided into several sections:
1. **Manual Launch**: A blue header with the text 'With EC2 Console, APIs or CLI'.
2. **Click "Accept Terms" to gain access to this software**: A section explaining that accepting terms grants access to the software in supported regions.
3. **Software Pricing**: A section with a table showing subscription terms and applicable instance types.
4. **Price for your selections:**: A section with a yellow 'Accept Terms' button and a note about subscription terms.
5. **Pricing Details**: A section with a dropdown for 'For region' set to 'US East (N. Virginia)' and a 'Free Trial' section.
6. **Usage Instructions**: A blue button labeled 'Usage Instructions'.
7. **Select a Version**: A section for selecting a version of the software.

Subscription Term	Applicable Instance Type
Hourly	Software fee
Annual	Varies: Depends on instance type, reference pricing chart.

DIY key management in AWS

Encrypt data client-side and send ciphertext to AWS storage services



Comparison of key management options

	KMS	CloudHSM	AWS Marketplace Partner Solutions	DIY
Where keys are generated and stored	AWS	In AWS, on an HSM that you control	Your network or in AWS	Your network or in AWS
Where keys are used	AWS services or your applications	AWS or your applications	Your network or your EC2 instance	Your network or your EC2 instance
How to control key use	Policy you define; enforced by AWS	Customer code + SafeNet APIs	Vendor-specific management	Config files, vendor-specific management
Responsibility for performance/scale	AWS	You	You	You
Integration with AWS services?	Yes	Limited	Limited	Limited
Pricing model	Per key/usage	Per hour	Per hour/per year	Variable

Data services security

Amazon S3 and Amazon RDS

S3 access control and data resiliency

S3 access control and auditing

IAM policies

Control API calls to S3

- Programmatic access by applications by using roles
- User-, group-, or role-based access policy

ACLs

Resource-based policy

- Object-level ACL for very specific object-level grants and access policy management
- Bucket-level ACL for log delivery

Bucket policies

Resource-based policy

- Ideal for cross-account permissions, supports all S3 actions

Logging

S3 access logging

CloudTrail Integration

S3 edge protection policies

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [ "arn:aws:s3:::examplebucket",
                    "arn:aws:s3:::examplebucket/*" ],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      },
      "Principal": "*"
    }
  ]
}
```

S3 edge protection policies

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [ "arn:aws:s3:::examplebucket",
                    "arn:aws:s3:::examplebucket/*" ],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      },
      "Principal": "*"
    }
  ]
}
```

S3 edge protection policies

```
{
  "Version":"2012-10-17",
  "Id":"PolicyForCloudFrontPrivateContent",
  "Statement":[
    {
      "Sid":" Grant a CloudFront Origin Identity access to support private content",
      "Effect":"Allow",
      "Principal":{"CanonicalUser":"79a59df90d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be"},
      "Action":"s3:GetObject",
      "Resource":"arn:aws:s3:::example-bucket/*"
    }
  ]
}
```

S3 edge protection policies

```
{  
  "Version": "2012-10-17",  
  "Id": "PolicyForCloudFrontPrivateContent",  
  "Statement": [  
    {  
      "Sid": "Grant a CloudFront Origin Identity access to support private content",  
      "Effect": "Allow",  
      "Principal": {"CanonicalUser": "79a59df90d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be"},  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::example-bucket/*"  
    }  
  ]  
}
```


Amazon S3 cross-region replication

Automated, fast, and reliable asynchronous replication of data across AWS regions



Lower latency

Distribute data to regional customers



Compliance

Store hundreds of miles apart



Secure

Remote replicas managed by separate AWS accounts

Cross-region replication: Details



Replication status

HEAD operation on a source object to determine replication status

- Replicated objects will not be re-replicated
- Use Amazon S3 COPY to replicate existing objects



Access control

Object ACL updates are replicated

- Objects with Amazon managed encryption key replicated
- KMS encryption not currently replicated



Cost

- Usual charges for storage, requests, and inter-region data transfer for the replicated copy of data
- Replicate into Standard-IA or Amazon Glacier



Delete operation

DELETE without object version ID

- Marker replicated

DELETE specific object version ID

- Marker NOT replicated

AWS database security

Database security

Commercial solutions through Amazon RDS:



Amazon database solutions:



**Amazon
DynamoDB**



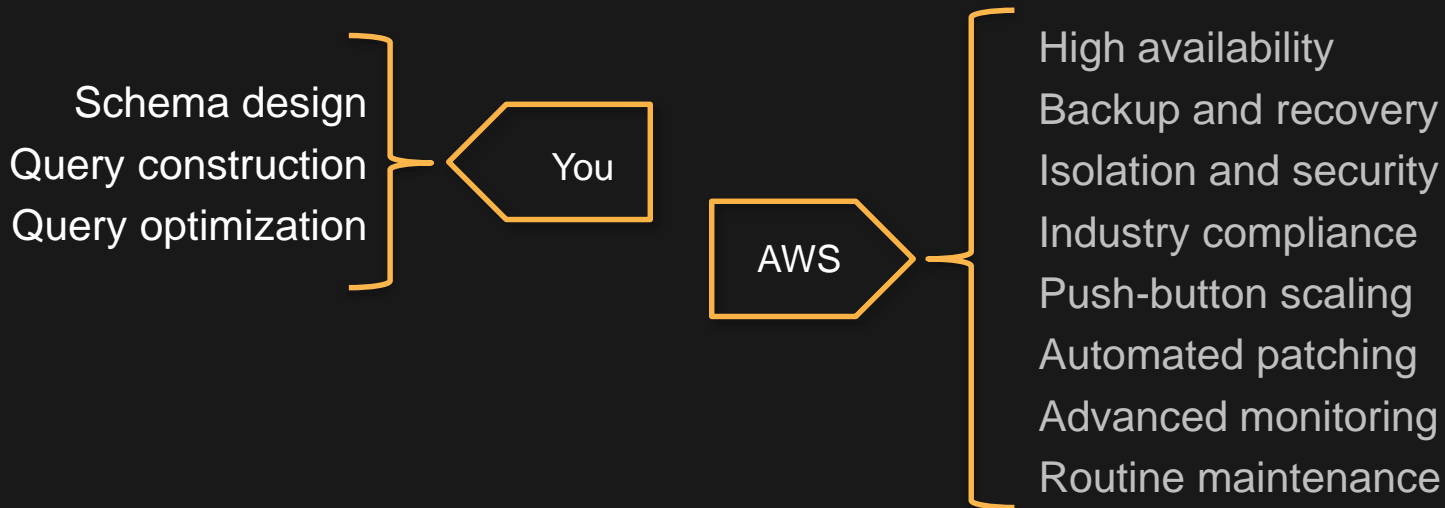
**Amazon
Redshift**



**Amazon
Aurora**

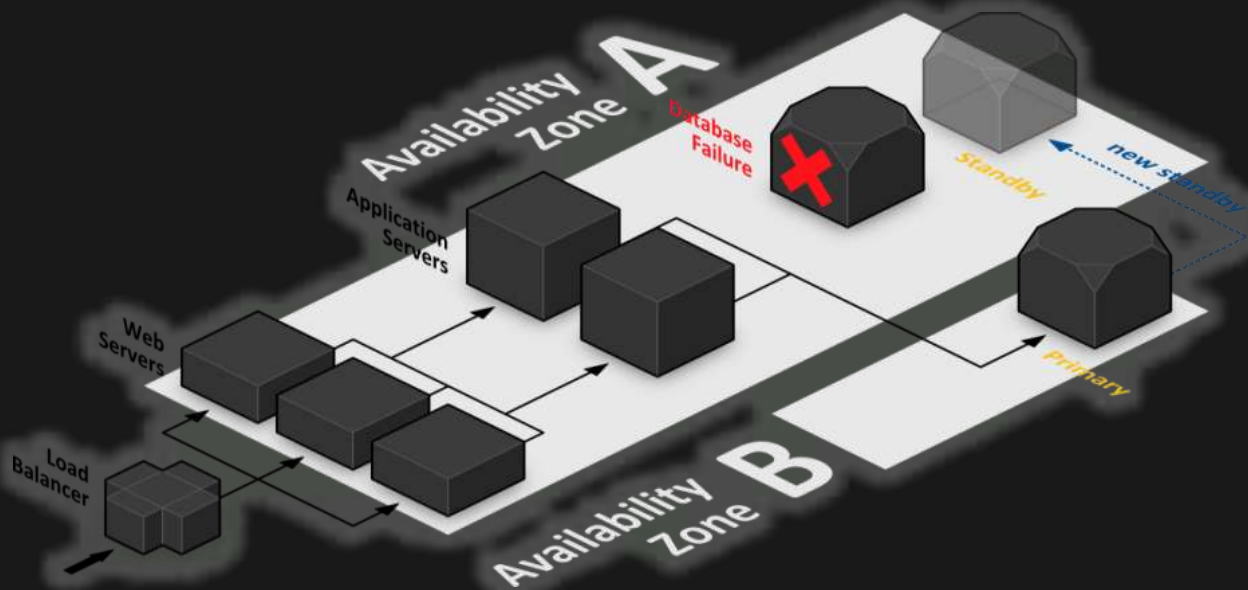
Why choose Amazon database solutions?

Amazon takes care of your time-consuming database security management tasks, freeing you to focus on your applications and business



High availability with Multi-AZ deployments

Enterprise-grade fault tolerance solution for production databases



- An Availability Zone is a physically distinct, independent infrastructure
- Your database is synchronously replicated to another AZ in the same AWS Region
- Failover occurs automatically in response to the most important failure scenarios

Choose cross-region snapshot copy for even greater durability, ease of migration



Copy a database snapshot or replicate data to a different AWS Region

Warm standby for disaster recovery

Or use it as a base for migration to a different region

AWS database services and encryption at rest

Server-side encryption with KMS

RDS MySQL

RDS PostgreSQL

RDS SQL Server

RDS Oracle

RDS MariaDB

Amazon Aurora

Amazon Redshift

Client-side encryption

DynamoDB encryption client

Server-side encryption with CloudHSM

Amazon Redshift

RDS Oracle—TDE

Microsoft SQL TDE

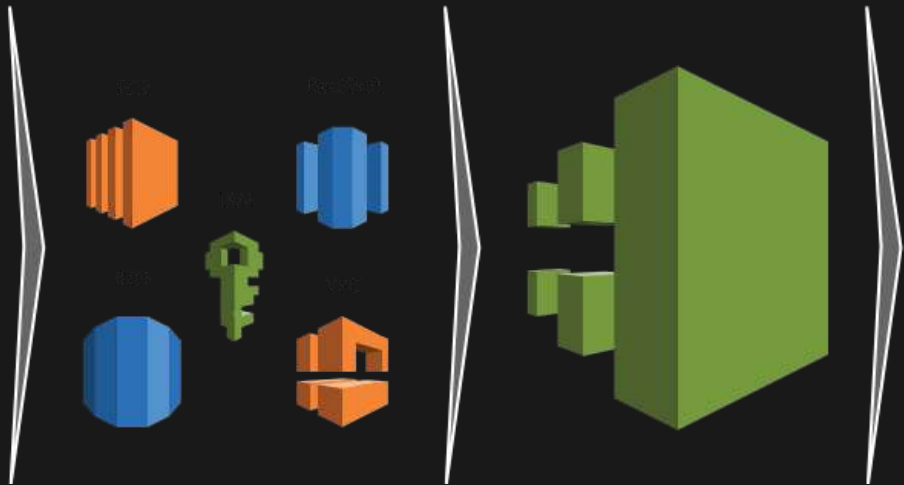
AWS data platforms—IAM and CloudTrail

- API permissions
 - Enforce separation of duties
- Resource-based permissions
 - Use tags by environment
- Integrated with CloudTrail
 - Alert on key management activities

A record of your API calls via AWS CloudTrail



You are making API calls...



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

CloudTrail is continuously recording API calls...

And delivering log files to you in S3

User	Action	Time
Tim	Created	1:30pm
Sue	Deleted	2:40pm
Kat	Created	3:30pm

Track, detect and take action

Tracking

- AWS Config rules
- Amazon CloudWatch Events
- AWS CloudTrail
- Amazon Inspector

Coordination

- Amazon SWF

Execution

- AWS Lambda

Securing

- MFA
- IAM policies

Track/Log

- Amazon CloudWatch Logs
- Amazon DynamoDB

Alert

- Amazon SNS

...

Partner Solutions for More Insights



Alerting

- Unauthorized Access Attempts
- Security Group Configuration Changes

Monitoring

- Parsing CloudTrail, CloudTrail Logs, VPC Flow Logs

Secure Configuration

- Validating permissions, ACLs

Summary

You have options to implement data controls that meet your business needs.

Take advantage of managed services, and let us do the heavy lifting.

Protect your data but also track, detect, and take action on changes and events.



Thank you!