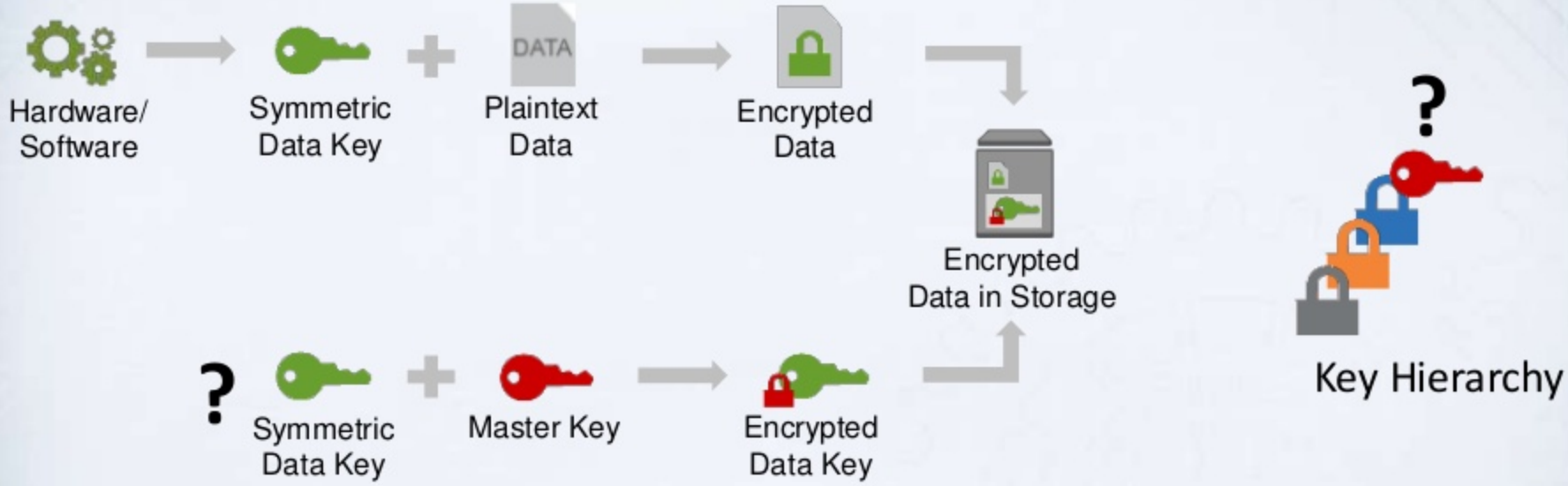
Protecting Your Data With AWS KMS and AWS CloudHSM

Camil Samaha

Agenda

- **Overview of encryption options in AWS**
  - **Client-Side Encryption:** You encrypt your data and manage your own keys; encryption is implemented in your code
  - **Server-Side Encryption:** AWS encrypts data and manages the keys for you; encryption is handled automatically
- **Key Management:**
  - On your own*
  - AWS Key Management Service (KMS)
  - AWS CloudHSM
  - Partner solutions

Encryption Primer



“Key” Questions to Consider

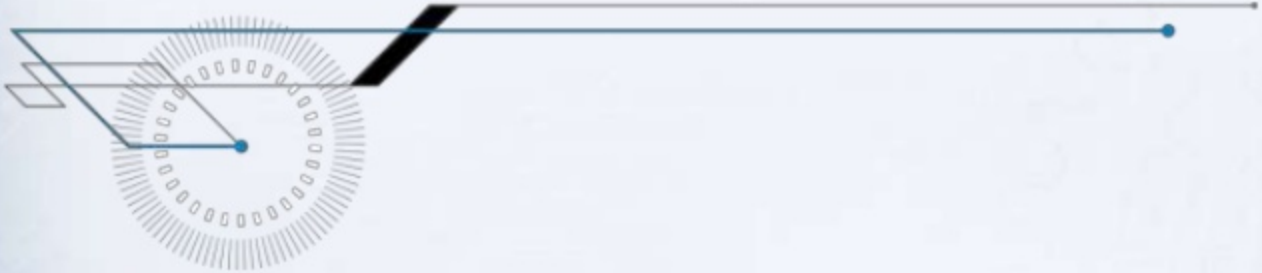
- Where are the keys stored?
- Where are the keys used?
- Who has access to the keys?

Encryption Models

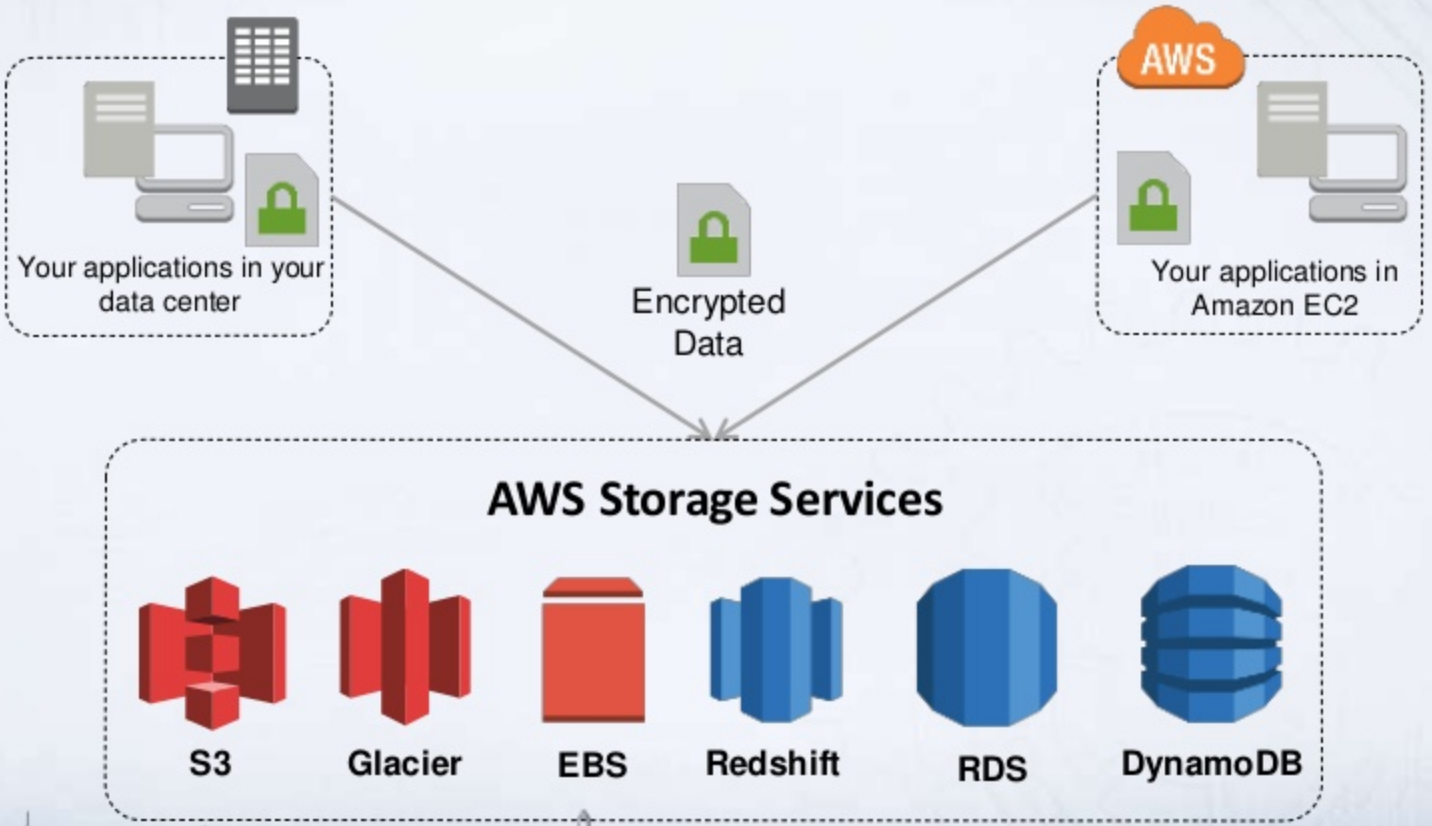
- **Client-Side Encryption #1:** You encrypt your data and manage your own keys
- **Client-Side Encryption #2**: You encrypt your data but utilize cloud services (AWS KMS or AWS CloudHSM) to help manage your keys
- **Server-Side Encryption:** AWS encrypts data automatically and manages the keys for you

Client-Side Encryption

You encrypt your data and send to AWS service

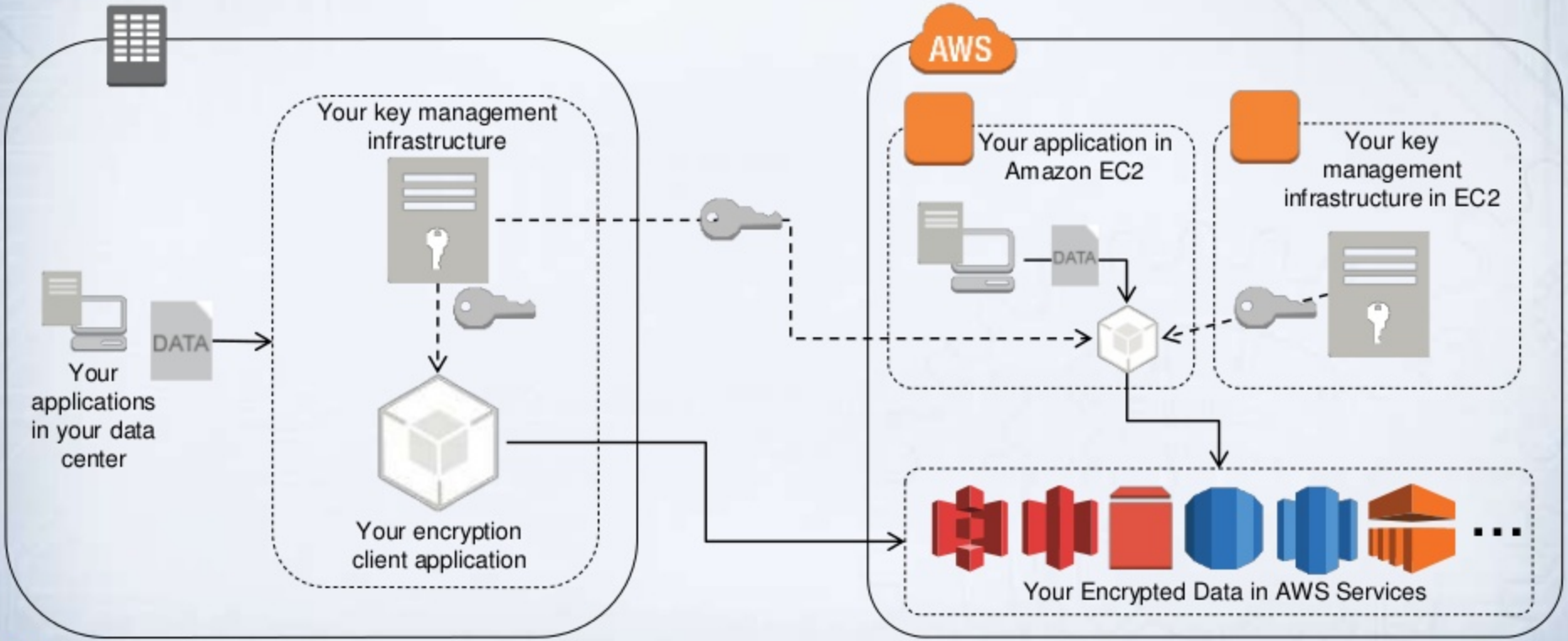


Client-Side Encryption



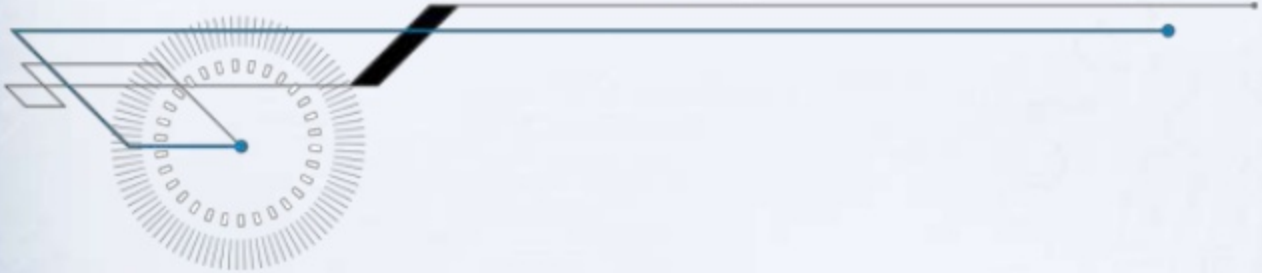
Client-Side Encryption

Overview

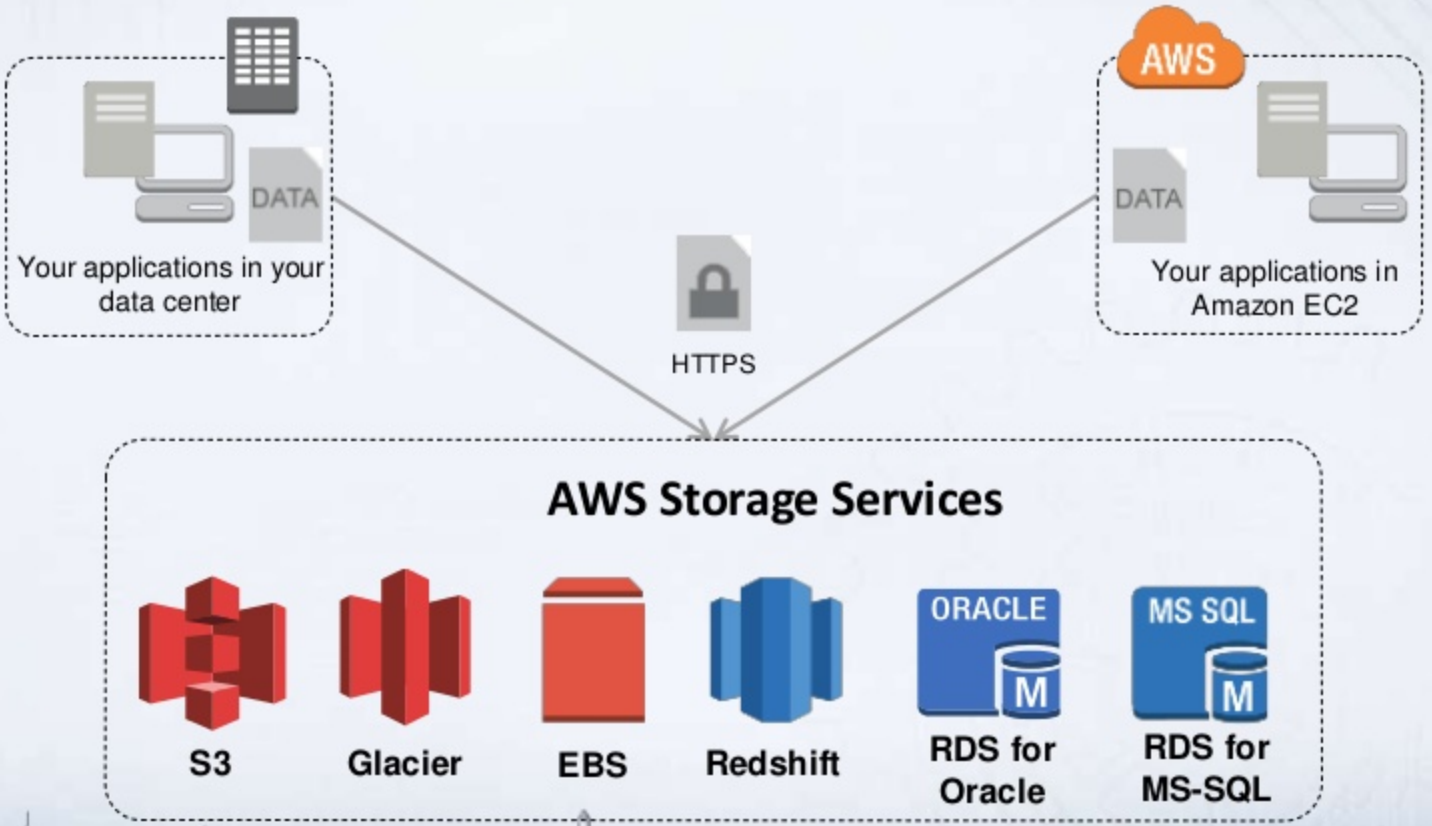


Server-Side Encryption

AWS services encrypt data for you

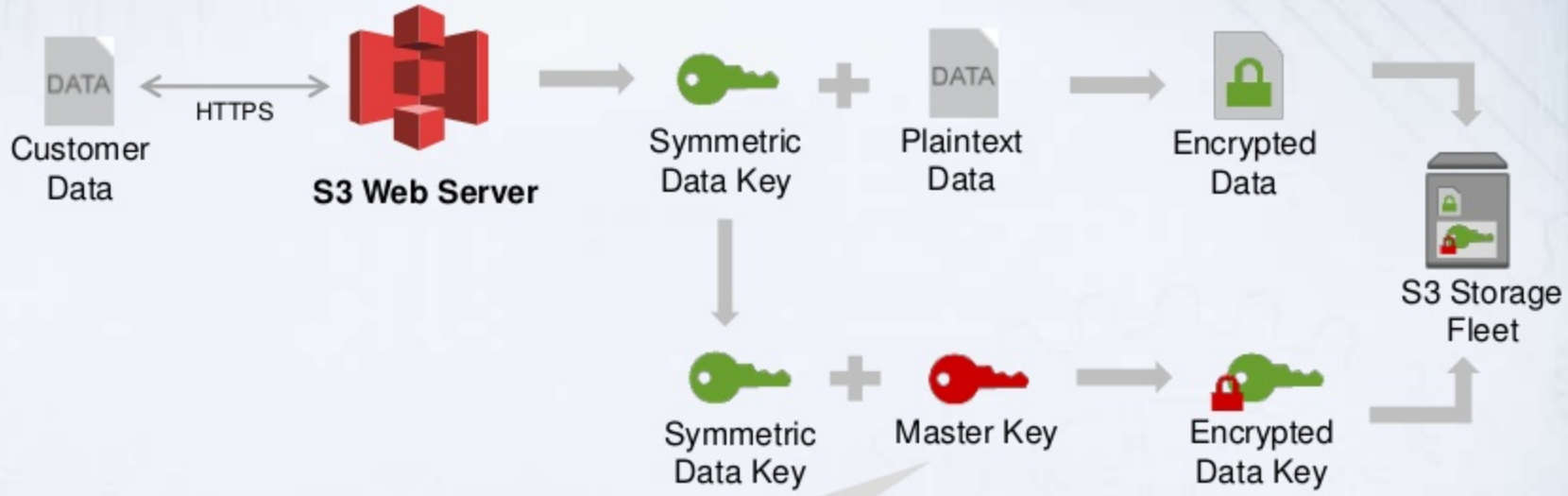


Server-Side Encryption

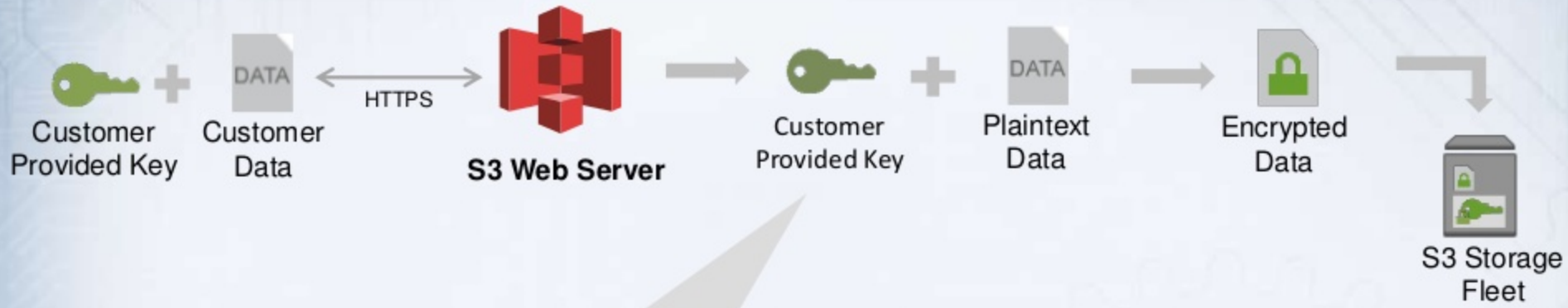


Amazon S3 Server Side Encryption

How SSE-S3 with AWS Managed Keys Works

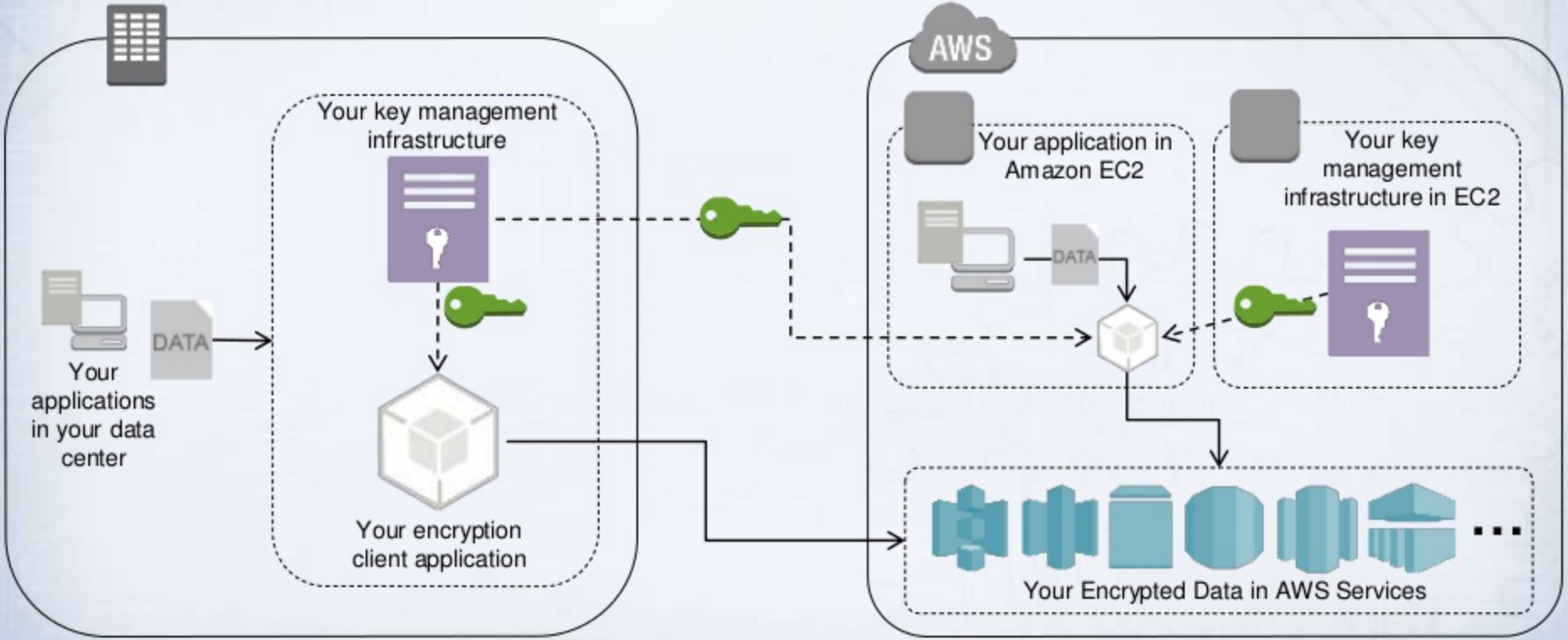


How SSE-C with Customer Provided Keys Works



- **Key is used at S3 Webserver, then deleted**
- **Customer must provide same key when downloading to allow S3 to decrypt data**

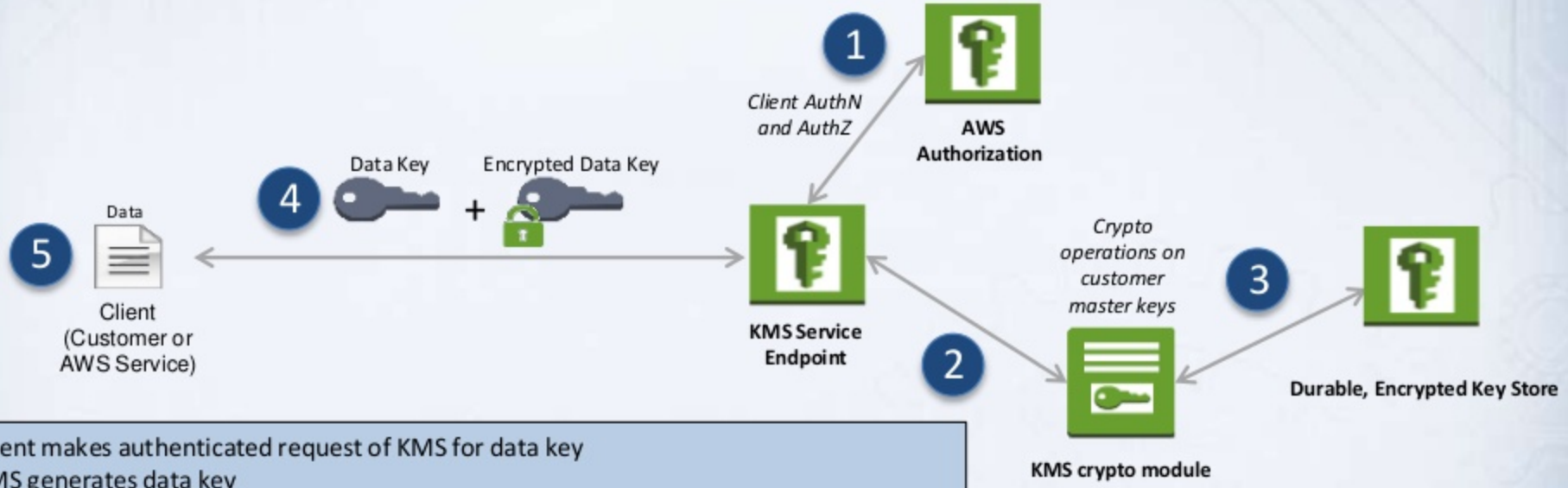
What About Key Management Infrastructure?



Introducing AWS Key Management Service

- A service that enables you to provision and use encryption keys to protect your data
- Allows you to create, use, and manage encryption keys from within…
  - Your own applications via AWS SDK
  - Supported AWS services (S3, EBS, RDS, Redshift)
- Available in all commercial regions

How AWS Key Management Service Works

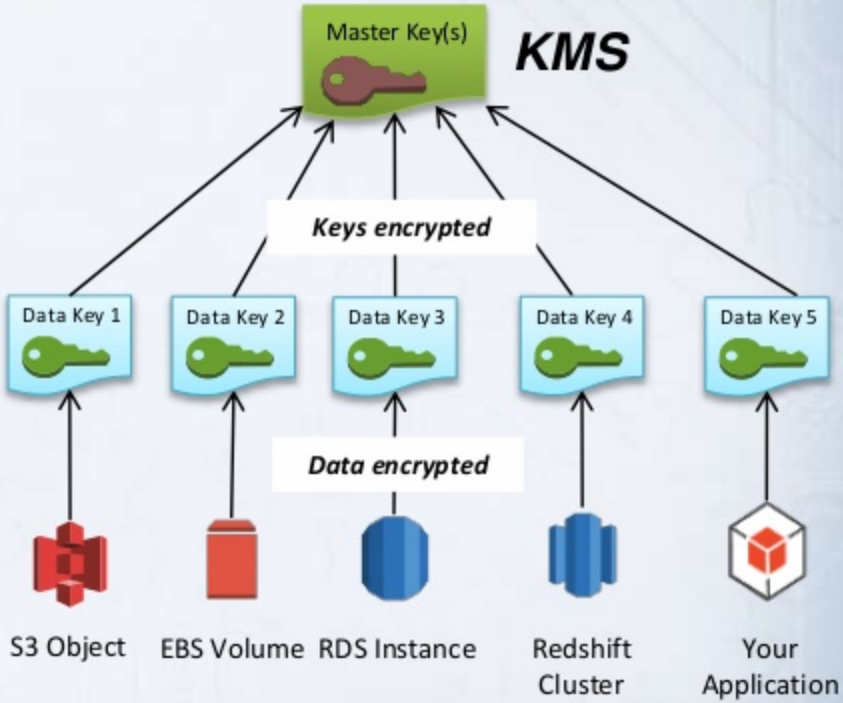


1. Client makes authenticated request of KMS for data key
2. KMS generates data key
3. KMS pulls encrypted customer master key from durable storage; decrypts in the KMS crypto module
4. KMS encrypts data key with named customer master key and returns plaintext data key and encrypted data key
5. Client uses data key to encrypt data, stores encrypted data key.

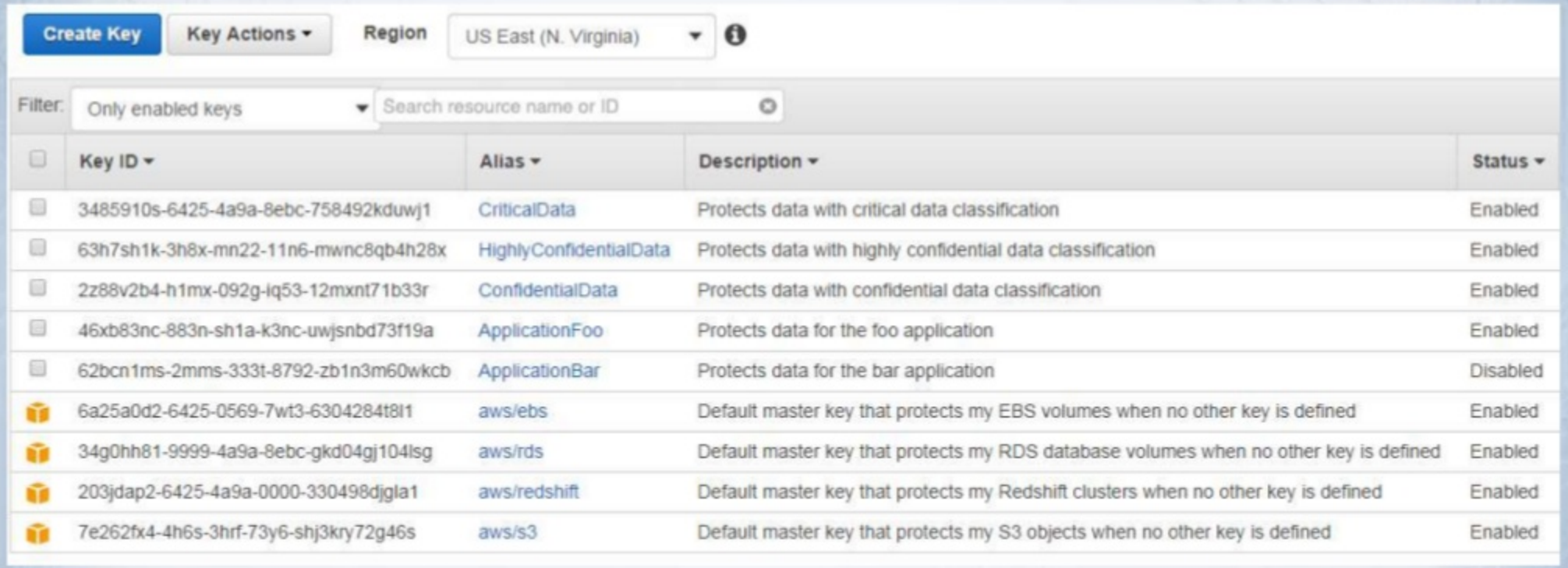
To decrypt: client submits encrypted data key to KMS for decryption; data key is needed to decrypt data

How AWS Services Integrate with KMS

- 2-tiered key hierarchy using envelope encryption
- Data keys encrypt customer data
- KMS master keys encrypt data keys
- Benefits:
  - Limits blast radius of compromised resources and their keys
  - Better performance
  - Easier to manage a small number of master keys than billions of resource keys



Creating and managing keys in AWS KMS



Amazon EBS encryption with AWS KMS

AWS KMS gives you control

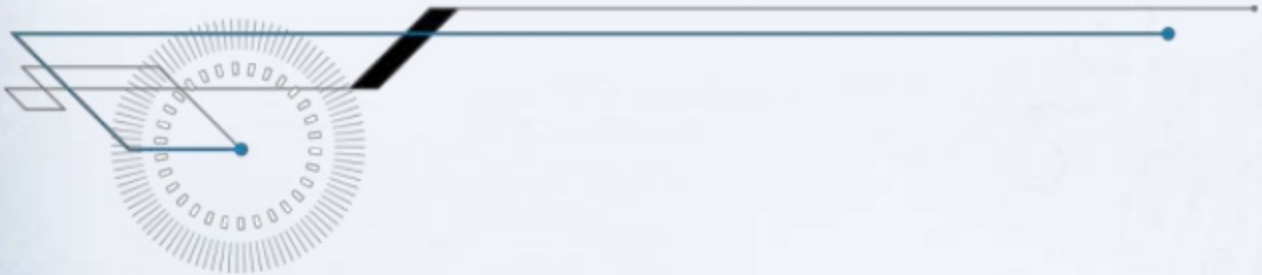
You define who can…

- Create a master key
- Use a master key
- Create and export a data key that is encrypted by a master key
- Enable/disable master keys
- Audit use of master keys in AWS CloudTrail

AWS KMS secures your keys

- Plaintext keys are never stored in persistent memory on runtime systems
- Separation of duties
  - AWS service team operators (S3, EBS, RDS) can't access KMS hosts that use master keys and KMS operators can't access service team hosts that use data keys
- Multi-party controls
  - Normal operations require signatures from two or more KMS operators on any API calls to an active host processing customer keys
- Verified claims in SOC1 and public white papers

Encryption and Key Management with AWS CloudHSM



amazon web services

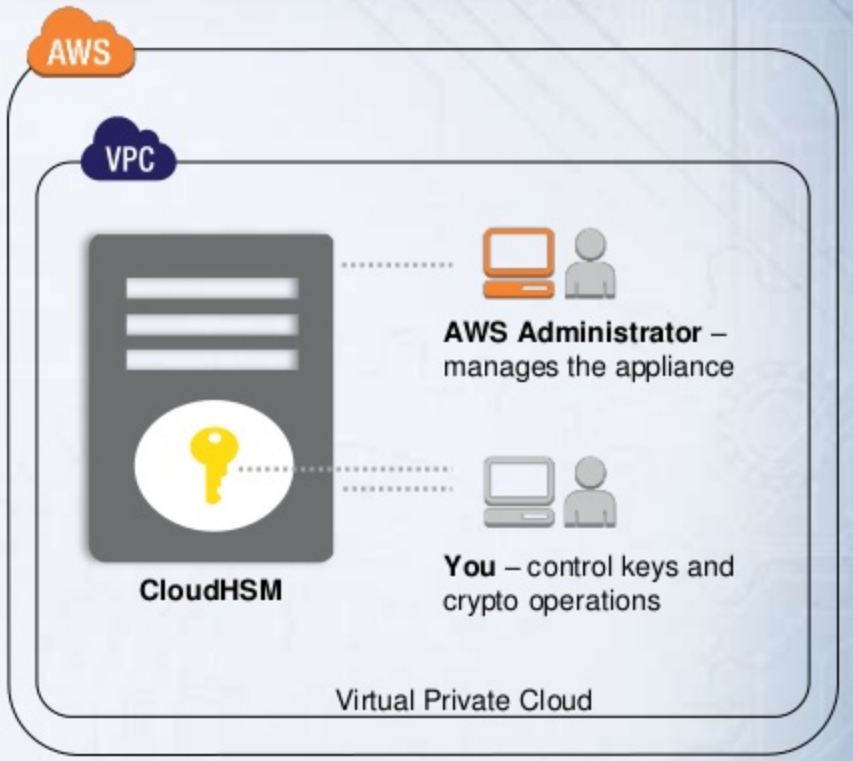
HSM – Hardware Security Module

- Hardware device for crypto ops and key storage
- Strong protection of private keys
  - Physical device control does not grant access to the keys
  - Security officer controls access to the keys
  - Appliance administrator has no access to the keys
- Certified by 3rd parties to comply with security standards

HSM

AWS CloudHSM

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



AWS CloudHSM

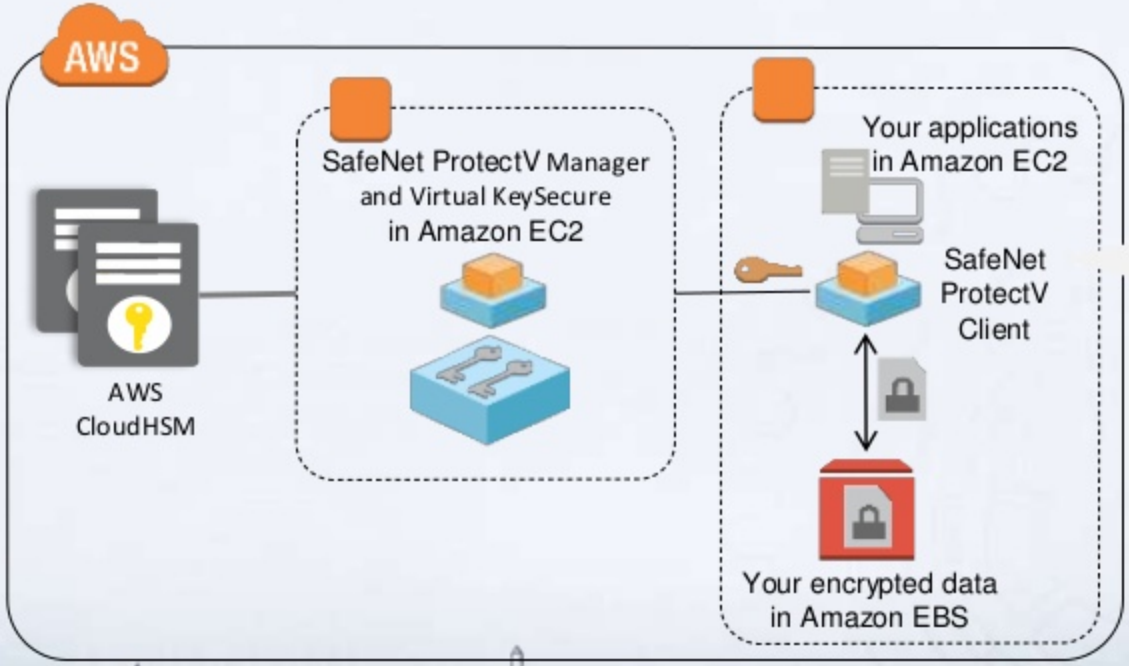
- Available in seven regions worldwide
  - N. Virginia, Oregon, Ireland, Frankfurt, Sydney, Singapore, and Tokyo
  - Easy to get started
  - AWS CloudFormation template
  - Application notes to help integrate with 3rd party software
- Compliance
  - Included in AWS PCI DSS and Service Organization Control (SOC) compliance packages

AWS CloudHSM

- Command Line Interface (CLI) Tools
  - Easier automation and administration
- Public API & SDK
  - Self-service provisioning and management
  - Appliance administrator operations
- Auditing
  - CloudTrail
  - Syslog

Amazon EBS volume encryption

- SafeNet ProtectV with Virtual KeySecure
- AWS CloudHSM stores the master key



ProtectV Client
- Encrypts I/O from Amazon EC2 instances to Amazon EBS volumes
- Includes pre-boot authentication

Comparing AWS CloudHSM with AWS KMS

AWS CloudHSM

- Dedicated access to HSM that complies with government standards (FIPS, CC)
- You control your keys and the application software that uses them

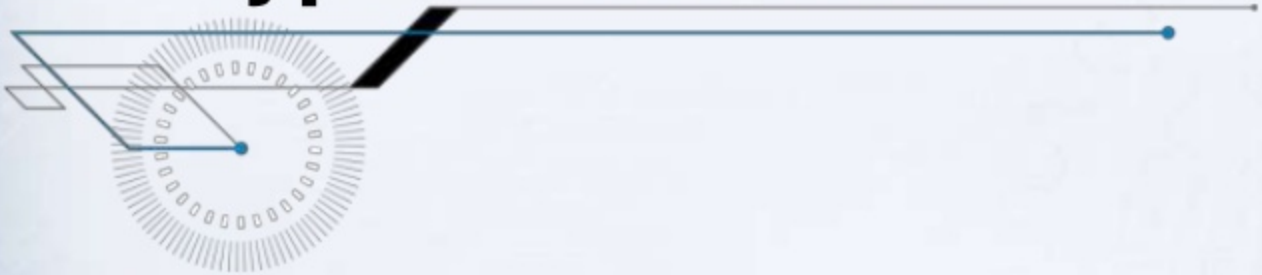
AWS KMS

- Builds on the strong protections of an HSM foundation
- Highly available and durable key storage, management, and auditing solution
- Easily encrypt your data across AWS services and within your own applications based on policies you define

Key Management Options Comparison

	On-Premises HSM	AWS CloudHSM	AWS Key Management Service
Where keys are generated and stored	Your network	AWS	AWS
Where keys are used	Your network or your EC2 instance	AWS + your network	AWS
How to use keys	Customer code	Customer code + Safenet APIs	Management Console, AWS SDKs
Performance/Scale/HA responsibility	You	You	AWS
AWS Services Integration?	No	Redshift	Yes
Price	$$$$	$$	$
Who controls key access	Only You	Only You	You + AWS

Alternate key management and encryption solutions



AWS Marketplace for security

- Browse, test and buy security software
- Pay-by-the-hour, monthly, or annual
- Software fees added to AWS bill
- Bring Your Own License

Key management and client-side encryption using an AWS partner solution

Solutions integrated with EC2, EBS, S3, and RDS

Resources

- AWS Key Management Service
  - https://aws.amazon.com/kms
- AWS CloudHSM
  - https://aws.amazon.com/cloudhsm/
- Whitepaper on data-at-rest encryption and key management in AWS
  - https://aws.amazon.com/whitepapers/
- S3 Encryption Client
  - http://aws.amazon.com/articles/2850096021478074
- AWS Partner Network
  - http://www.aws-partner-directory.com/
- AWS Security Blog
  - http://blogs.aws.amazon.com/security

Thank You.

This presentation will be loaded to SlideShare the week following the Symposium.
http://www.slideshare.net/AmazonWebServices