


The Global Advantage

aws training and certification

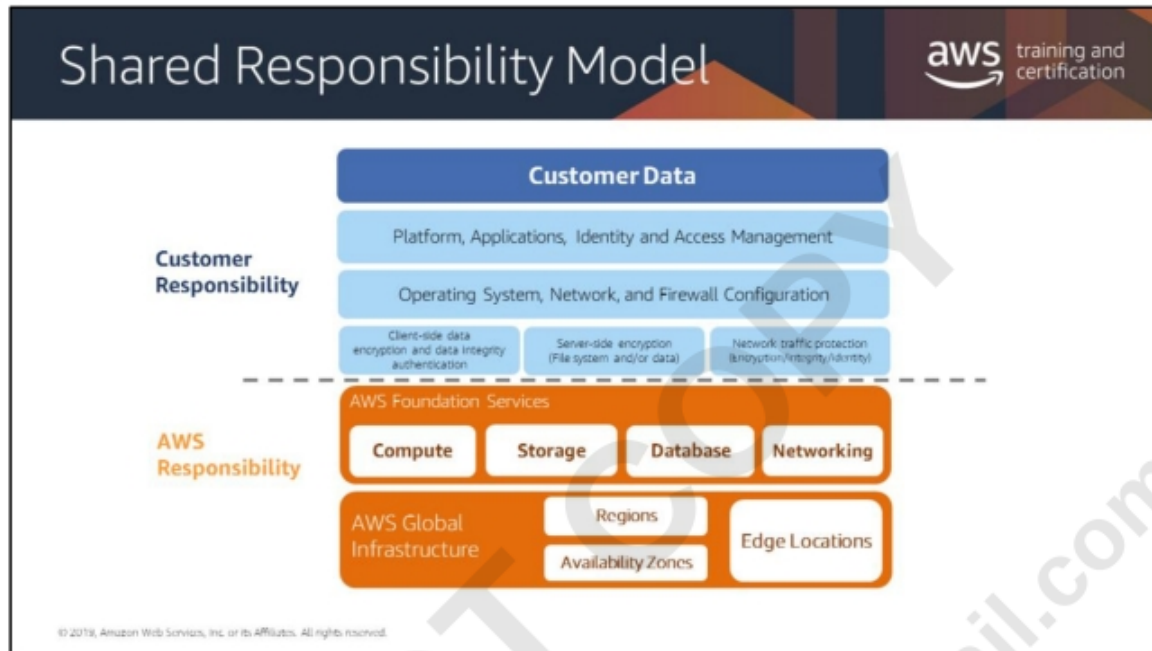
Go global in minutes.

- Multiple AWS Regions around the world
- Keep your application close to your users
- Facilitate high availability and disaster recovery



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

You can deploy your application in multiple regions around the world with just a few clicks—providing lower latency and better experience for your customers simply and at minimal cost.



Amazon Web Services provides the same familiar approaches to security that companies have been using for decades. Importantly, it does this while also allowing the flexibility and low cost of cloud computing. There is nothing inherently inconsistent about providing on-demand infrastructure while also providing the security isolation that companies expect in their existing, privately owned environments.

Understand Normal Behavior

AWS Shield helps you protect your website from all types of DDoS attacks including:

- Infrastructure layer attacks (like UDP floods).
- State exhaustion attacks (like TCP SYN floods).
- Application layer attacks (like HTTP GET or POST floods).

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

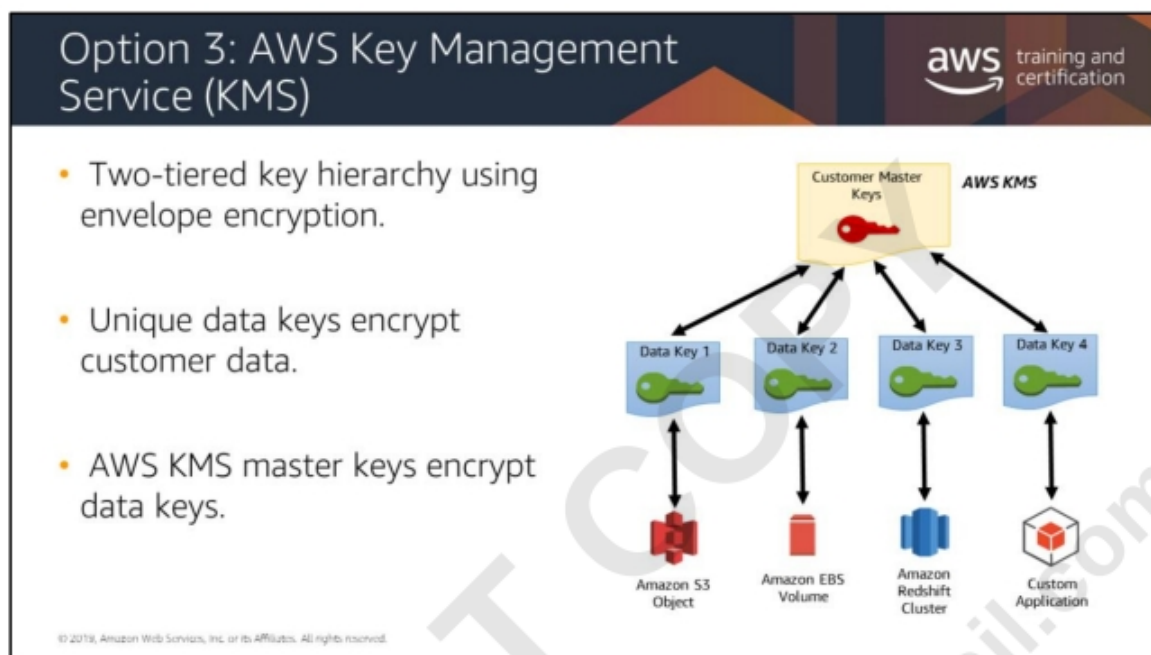
AWS provides AWS Shield Standard and AWS Shield Advanced for protection against DDoS attacks. AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services. For added protection against DDoS attacks, AWS offers AWS Shield Advanced. AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, and Amazon Route 53 hosted zones.

Typically, 99% of infrastructure layer attacks detected by AWS Shield are mitigated in less than 1 second for attacks on Amazon CloudFront and Amazon Route 53, and less than 5 minutes for attacks on Elastic Load Balancing. The remaining 1% of infrastructure attacks are typically mitigated in under 20 minutes. Application layer attacks are mitigated by writing rules on AWS WAF, which are inspected and mitigated inline with incoming traffic.

AWS Shield Standard automatically provides protection for web applications running on AWS against the most common, frequently occurring Infrastructure layer attacks like UDP floods, and State exhaustion attacks like TCP SYN floods. Customers can also use AWS WAF to protect against Application layer attacks like HTTP POST or GET floods.

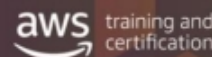
AWS Shield Advanced manages mitigation of layer 3 and layer 4 DDoS attacks. This means that your designated web applications are protected from attacks like UDP Floods, or TCP SYN floods. In addition, for application layer (layer 7) attacks, you can use AWS WAF to apply your own mitigations, or you can engage the 24X7 AWS DDoS Response Team (DRT), who can write rules on your behalf to mitigate Layer 7 DDoS attacks.

DO NOT COPY
krishnameenon@gmail.com



If you are a developer who needs to encrypt data in your applications, you should use the AWS SDKs with AWS KMS support to easily use and protect encryption keys. If you're an IT administrator looking for a scalable key management infrastructure to support your developers and their growing number of applications, you should use AWS KMS to reduce your licensing costs and operational burden. If you're responsible for providing data security for regulatory or compliance purposes, you should use AWS KMS to verify if that data is encrypted consistently across the applications where it is used and stored.

AWS KMS: Benefits

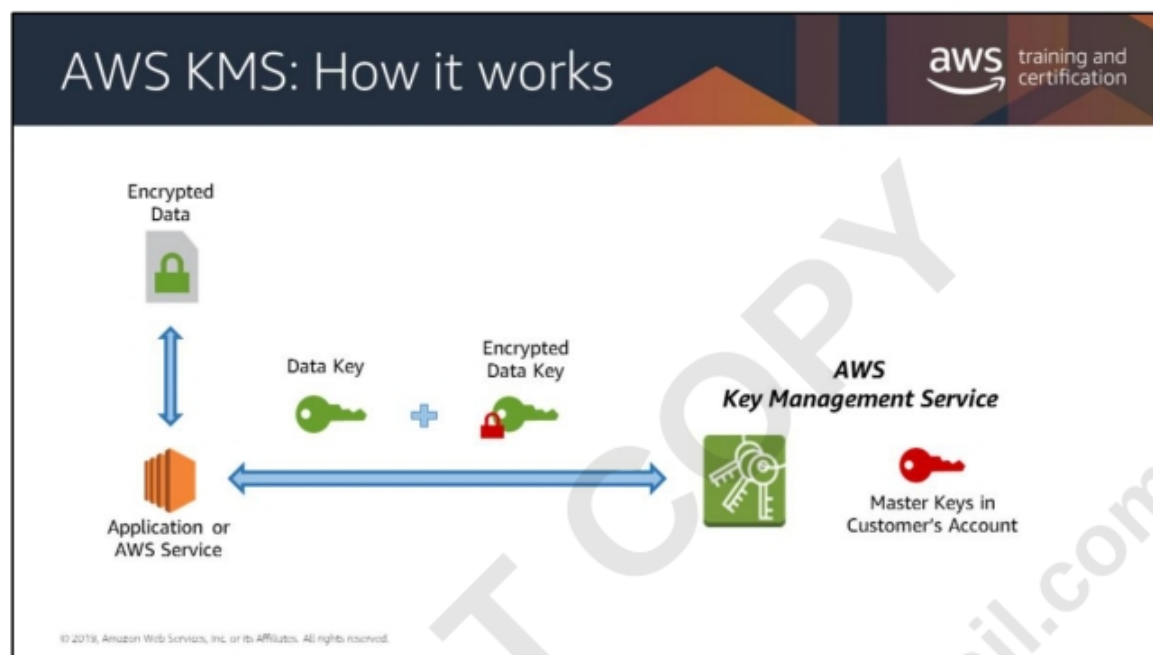


- The master key is never made available.
- Data keys are available directly to the customer and these should be unique to each item encrypted.
 - If one is compromised, it will not allow decryption of other objects.
- The risk of a compromised data key is limited.
- The performance for encrypting large data is improved.
- It is easier to manage a small number of master keys than millions of data keys.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

You can perform the following key management functions in AWS KMS:

- Create keys with a unique alias and description
- Define which IAM users and roles can manage keys
- Define which IAM users and roles can use keys to encrypt and decrypt data
- Choose to have AWS KMS automatically rotate your keys on an annual basis
- Disable keys temporarily so they cannot be used by anyone
- Re-enable disabled keys
- Audit use of keys by inspecting logs in AWS CloudTrail



1. An application or AWS service client requests an encryption key to encrypt data and passes a reference to a master key under the account.
2. The client requests are authenticated based on whether they have access to use the master key.
3. A new data encryption key is created and a copy of it is encrypted under the master key.
4. Both the data key and encrypted data key are returned to the client. The data key is used to encrypt customer data and then deleted as soon as it is practical.
5. The encrypted data key is stored for later use and sent back to AWS KMS when the source data needs to be decrypted.

Safeguard Layer 7 with a WAF

aws training and certification

A WAF inspects and applies filters to application layer traffic (HTTP and HTTPS).

- Important features:
 - OWASP Top 10
 - Rate limiting
 - Whitelist or blacklist (customizable rules)
 - Native automatic scaling with WAF Sandwich
 - Learning engine

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

A good example of how to rate-limit traffic is a web application firewall. WAFs are essentially firewalls that apply specific rules to HTTP and HTTPS traffic (i.e. port 80 and 443). In AWS, these are software firewalls that inspect your web traffic and verify that it conforms to the norms of expected behavior. The feature that enables WAF to do this is adherence to the Open Web Application Security Project (OWASP) top ten. The goal of the Top 10 project is to raise awareness about application security by identifying some of the most critical risks facing organizations. The Top 10 project is referenced by many standards, books, tools, and organizations, including MITRE, PCI DSS, DISA, and FTC.

As mentioned earlier, rate limiting is the ability to look at the amount or type of requests being sent to your service and define a threshold that caps how many can be requested per user, session, or IP address. Again, this is a great complement to ACLs because it provides coverage against unknown attackers.

Whitelist and blacklists allow you to explicitly allow or block users, similar to network ACLs but at the WAF layer; you should find more granularity regarding session and protocol settings.

