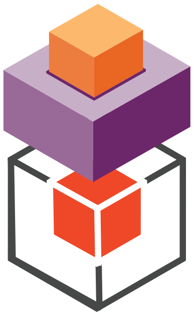
SafeNet

THE
DATA
PROTECTION
COMPANY



AWS S3, SafeNet ProtectApp and KeySecure

SOLUTION BRIEF

Key Advantages

AWS Simple Storage Service (S3) Advantages:

- Simple, scalable, affordable Internet storage
- Constant availability - Store and retrieve any amount of data from any browser at any time
- Allocate objects to be stored in geo-regional buckets, optimized for cost, latency, regulatory requirements, and jurisdictional preference

SafeNet ProtectApp and KeySecure Advantages:

- Add security to business applications, such as CRM, ERP, and HCM, with robust encryption
- Granularly encrypt data automatically according to preset security policy settings with no effect on user experience or performance
- Maintain control of and manage encryption keys

SafeNet and AWS S3 Combined Advantages:

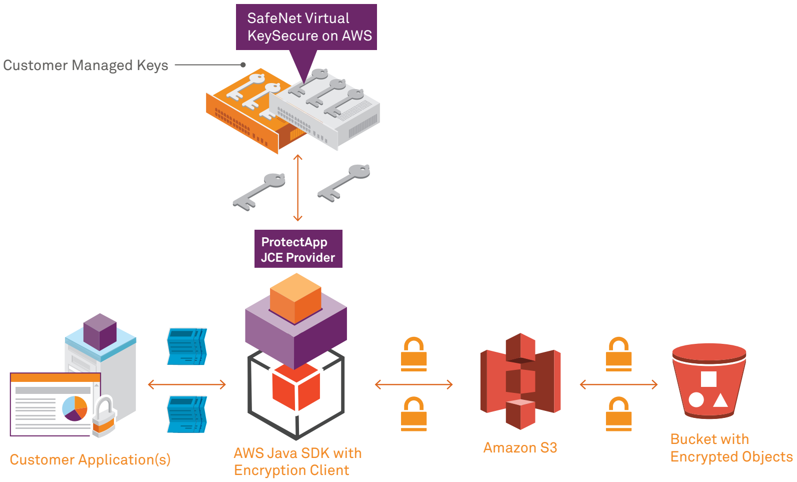
- Strengthen security to data at rest stored in Amazon S3 environments
- Achieve regulatory compliance and Safe Harbor integration with workflow
- Customers maintain complete control of encryption and key management with ProtectApp and KeySecure

Storing Data in the AWS S3 Cloud Is Easy and Efficient

Storing data in the cloud is affordable and efficient, and these key drivers are leading more and more companies to store their application data (as objects) in the cloud. Organizations making this move gain faster access to applications, better performance, broader reach, and higher efficiency. As reliance on cloud-based applications increases, the need to store data in growing volumes in the cloud goes hand in hand.

Amazon Web Services (AWS) and Amazon Simple Storage Service (S3) make it easy for application developers to use API/SDK interfaces to implement object storage solutions for sharing, backing up, and archiving data on the web. Developers can store objects with rich metadata in buckets based on geographic region using Amazon SimpleDB (database). This allows organizations to gain the rich query functionality of a database without the administrative overhead involved with in-house database maintenance.

For companies to adequately take advantage of this affordable and convenient cloud storage, they need security. Today's regulations impose strict requirements on keeping cloud information private. Using AWS SDKs, developers can integrate SafeNet ProtectApp to encrypt object data before it is stored in the cloud.


SafeNet Virtual KeySecure on AWS
Customer Managed Keys
ProtectApp JCE Provider
Customer Application(s)
AWS Java SDK with Encryption Client
Amazon S3
Bucket with Encrypted Objects

Encryption and Key Management Protects AWS Cloud Data

Companies know that encrypting data, along with secure key management, is recognized as a core method of protection that satisfies compliance regulations. SafeNet's ProtectApp provides robust encryption by aligning encryption algorithms with an organization's security policies, flexibly definable by users, roles, time of day, and data type. Once data is encrypted, the SafeNet KeySecure appliance enables administrators to keep and manage all their cryptographic keys from a central, on-premises (or cloud) location. Control of the encryption keys never leaves the organization, ensuring only authorized users and systems can access the sensitive data stored in the cloud. [optional: Due to the high security this provides, many regulations grant Safe Harbor protection if undecipherable, encrypted data is stolen.

ProtectApp and KeySecure: Two Scenarios for AWS Architecture

When companies elect to place volumes of data in the cloud, they ultimately have to control for the third-party administrators that maintain the cloud infrastructure. With SafeNet, organizations can separate duties, meaning that administrators in control of data encryption and the encryption keys remain separate from the cloud provider, in this case, AWS. This separation is what meets compliance and governance standards, and also allows for centralized monitoring and audit control.

Key Benefits

SafeNet KeySecure Benefits

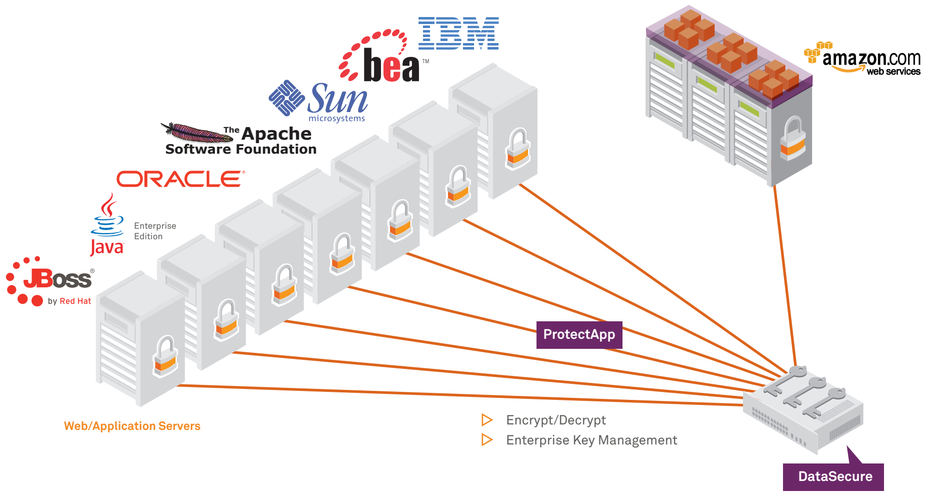
- SafeNet KeySecure delivers hardware appliances and hardened virtual appliances for enterprise key management
- Centralized key management lowers administration costs and TCO
- Simplified compliance and auditing saves staff time
- Tamper-proof hardware appliances and hardened virtual appliances mitigate risks

SafeNet KeySecure provides:

- Heterogeneous key management for multiple key types
- Centralized administration of granular access, authorization controls, and separation of duties
- Auditing and tracking of all key state changes
- FIPS 140-2 Level 2 certification
- Optional FIPS 140-2 Level 3 cryptographic module

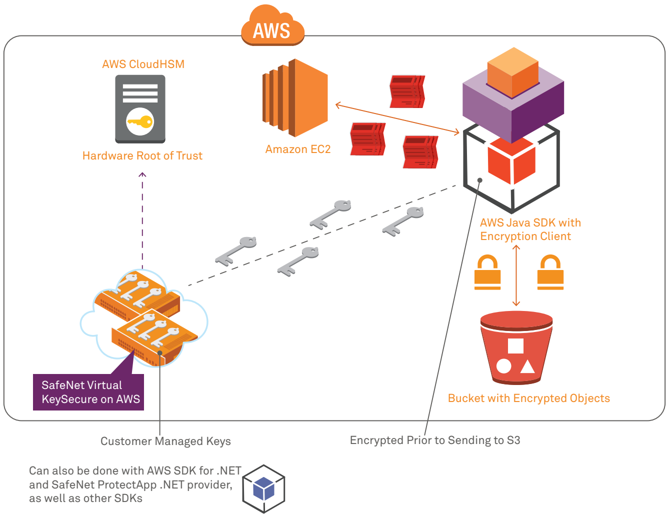
> *"Controlling and maintaining keys is the most important part of an enterprise encryption strategy."*
>
> *-John Kindervarg, Forrester Research*

> *"Companies are looking to protect data in the cloud through encryption keys and robust key management. This enables companies to secure data from breaches, as well as prevent the cloud provider from accessing the information if they decide to end their relationship with the cloud provider."*
>
> *Frost & Sullivan*



Model A: You control the encryption method and the entire KMI

In Model A, customers rely on SafeNet ProtectApp to control all encryption use KeySecure to manage the encryption keys. Your key management infrastructure's physical location can be on-premises outside of AWS, or alternatively, the keys can be held in an Amazon Elastic Compute Cloud (Amazon EC2) instance that the customer owns and manages.


AWS
AWS CloudHSM
Hardware Root of Trust
Amazon EC2
AWS Java SDK with Encryption Client
Bucket with Encrypted Objects
SafeNet Virtual KeySecure on AWS
Customer Managed Keys
Encrypted Prior to Sending to S3

Can also be done with AWS SDK for .NET and SafeNet ProtectApp .NET provider, as well as other SDKs

Model B: You control the encryption; everything else is in the cloud

Similar to Model A, Model B differs in that the keys are stored in an AWS CloudHSM appliance and managed by a virtual version of KeySecure deployed in an AWS EC2 environment. Virtual KeySecure – a hardened OS software version of the hardware appliance - is available in the AWS. While the keys are in the AWS environment, they remain inaccessible to any employee at AWS.

In both models, the important security component is that the customer's security administrators maintain full control over the encryption keys.

SafeNet KeySecure Provides Encryption Key Creation and Management

SafeNet KeySecure is the industry's leading platform for central management and security of encryption keys, protecting sensitive data in storage, virtual workloads, and applications across traditional and virtualized data centers and public cloud environments.

Conclusion

Through its simple web interface, Amazon S3 makes cloud storage for the Internet easy for developers. With SafeNet and Amazon S3, organizations can ensure that volumes of data stored in the cloud are safe and comply with the strictest security regulations.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/news-media