Alliance Key Manager for Amazon Web Services (AWS)

Solution Brief

Encryption Key Management in the Cloud

Alliance Key Manager is now available as an Amazon Machine Instance (AMI). The same FIPS 140-2 compliant key management solution available in Townsend Security's hardware security module (HSM) now runs as a virtual machine in Amazon Web Services (AWS). You can easily deploy the best encryption key management solution for your cloud applications directly in AWS and leverage all of the management options provided by Amazon. Alliance Key Manager for AWS helps protect your data in AWS or anywhere else it may reside. Your keys are instantly mirrored to backup key management servers ensuring that your keys are never lost and you never experience application interruptions.

About Townsend Security

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security's NIST and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, DIACAP, SOX, and other regulatory compliance requirements. Learn more at www.townsendsecurity.com.

Townsend SECURITY

NIST-Compliant Encryption
Protect your personally identifiable information (PII) with encryption that provably meets industry standards and best practices

The Platform You Need It On
Encryption and key management available in the cloud, as a virtual appliance, or physical hardware security module (HSM)

Meet Data Security Best Practices
Separarate encryption keys from the data that they protect with dual control and separation of duties

Affordable
Subscription and perpetual licensed options available for your budget

Certified
Certified to FIPS 140-2 Level 1 compliance (certificate #1449)

OASIS KMIP 1.0 Specification compliant

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360.357.9047

Alliance Key Manager for Amazon Web Services

Alliance Key Manager for Amazon Web Services (AWS) is a full Amazon Machine Image (AMI) that you can run on demand. Because Alliance Key Manager for AWS is deployed as an AMI, you only pay for what you use. You can start and stop your subscription at any time. Alliance Key Manager for AWS can protect data in any AWS environment (IaaS and PaaS) and can protect data in any non-AWS environment such as other cloud platforms, hosting providers, and traditional IT data centers.

Key Management Platforms

Alliance Key Manager is available in many form factors ranging from a traditional hardware security module (HSM) to a full cloud implementation in AWS. Alliance Key Manager can be deployed on any of the following platforms to protect data in AWS:

- Key management as an AMI
- Key management HSM in your data center
- Key management cloud HSM
- Key management for VMware

You can easily deploy Alliance Key Manager in any of these platforms and move to any other platform at any time. You can also mix and match key management platforms for high availability and key mirroring.

Availability Zones

For improved resiliency and redundancy you can deploy instances of Alliance Key Manager in different AWS availability zones. For example, your production key manager could be deployed in the us-west-1 zone and your high availability mirrored key server could be deployed in the us-west-2 zone. This provides for better resiliency for your applications.

AWS Virtual Private Cloud (VPC)

Encryption key management is a critical security function and many organizations will want to implement Alliance Key Manager in a virtual private cloud architecture to meet their security goals or to meet compliance regulations. Alliance Key Manager for AWS can be deployed in an AWS VPC environment without any changes.

Key Mirroring for High Availability (HA)

Because encryption and key management are mission critical functions, Alliance Key Manager fully implements real-time mirroring of encryption keys and key access policies and supports active-active mirroring. You can mirror keys in Alliance Key Manager for AWS to:

- Another instance of Alliance Key Manager for AWS
- Alliance Key Manager cloud HSM
- Alliance Key Manager HSM
- Alliance Key Manager for VMware

While most AWS users will mirror to a key management instance in a different availability zone, multiple mirroring targets are supported and you can chose the key management topology that makes the most sense.

Combining Cloud and Hardware Key Management Systems

Because the Alliance Key Manager software is exactly the same for hardware security modules (HSMs), cloud instances, and virtual platforms, you can deploy Alliance Key Manager across all of these platforms without restrictions on the functionality of the key manager. Backup and restore functionality also works across any supported platform.

Protecting Data in AWS

Alliance Key Manager includes a number of ready-to-use encryption applications and SDKs which can be deployed in AWS to protect databases and applications. These include:

- SQL Server EKM Provider for TDE and Cell Level Encryption
- SQL Server SDKs for SQL Server Standard and Web Editions
- Windows SDK for .NET applications
- Key Connection for Drupal
- Encryption solutions for Linux

Please contact Townsend Security for a complete list of applications, SDKs, and sample code to help you solve any encryption challenge.