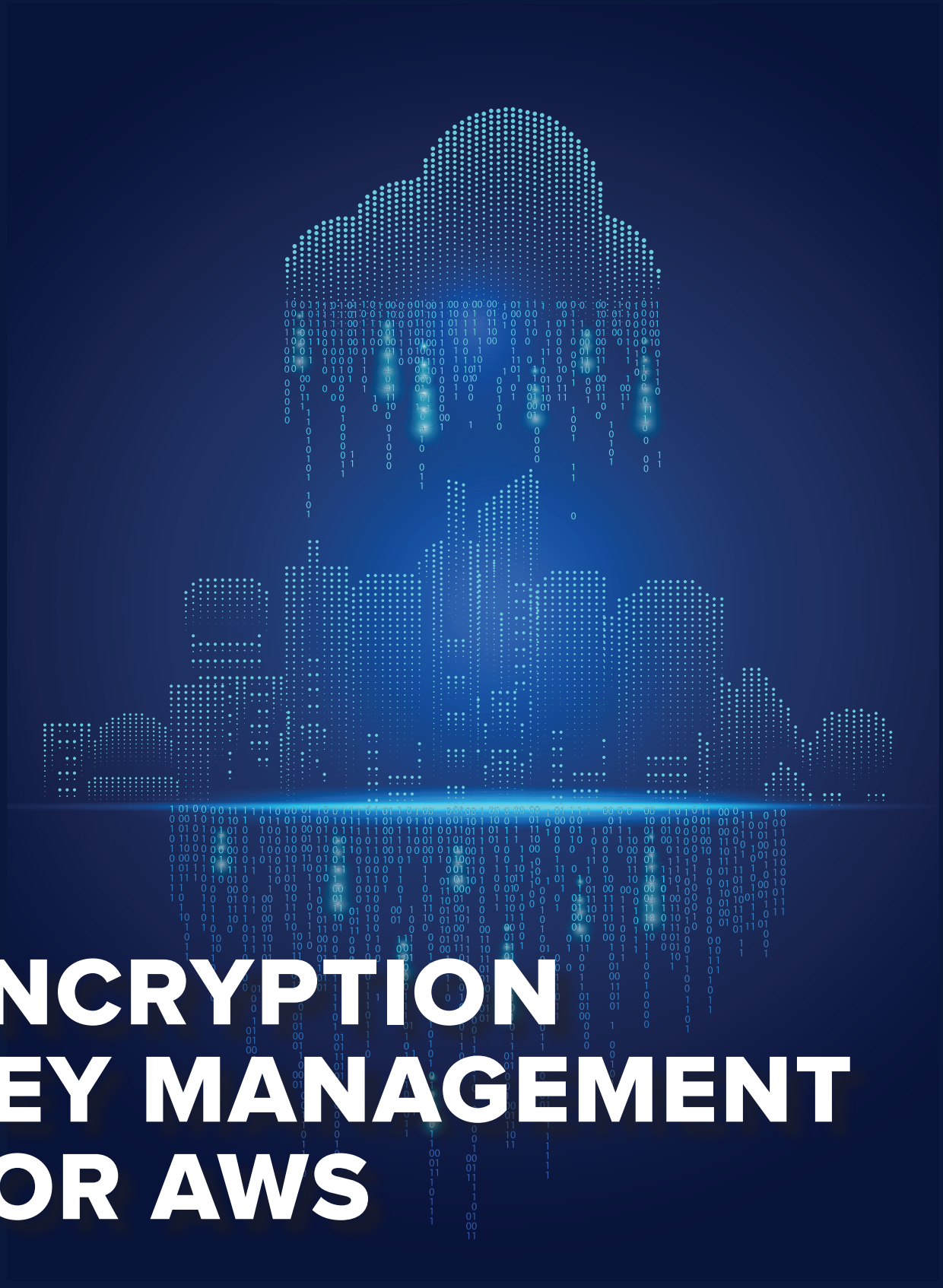


ENCRYPTION KEY MANAGEMENT FOR AWS

THE DEFINITIVE GUIDE

Townsend® SECURITY

Security is the biggest barrier to cloud adoption, and encryption of sensitive data is the hardest part of security. Once an organization decides to encrypt their sensitive data, getting encryption key management right can be a significant hurdle. As encryption key management options for AWS users grow, there are a few ways to distinguish a key management solution that meets industry standards and one that will leave you with a breach notification on your hands. Considerations that should be considered include: standards and certifications, who has access to encryption keys, key management best practices, cloud service provider (CSP) lockin, and finally, cost. This guide will explore the key concepts of encrypting data in AWS and protecting the encryption keys using proper encryption key management without cloud lock-in.

CONTENTS

INTRODUCTION

AT THE AMAZON RE:INVENT SUMMIT OF 2014 the Amazon Web Services (AWS) group announced a new AWS Key Management Service (AWS KMS). Positioned as a cost effective method of generating encryption keys and the enablement of an encryption service, the AWS Key Management Service helps some AWS customers better protect their sensitive data in the AWS cloud. However, it does not meet minimum standards and security requirements for many organizations. For users who have even more stringent key management requirements (and a healthier budget), AWS offers their dedicated CloudHSM. The CloudHSM is a cloud-based hardware security module (HSM) that allows users to generate and use their own encryption keys on the AWS cloud.

Alternatively, Enterprises can choose to deploy third-party encryption key management solutions in AWS. This a very attractive option because it guarantees an Enterprise that they are the sole owners of their encryption keys (AWS will not have administrative access), removes customers and partners from AWS lock-in, and can be more cost-effective for dedicated solutions.

Selecting a key management system is the most important part of an encryption strategy. To provide insight on how to best deploy encryption and encryption key management in AWS, this comprehensive guide covers the landscape for securing data in AWS. If you'd like to first learn the fundamentals of encryption and key management before diving in, view The Definitive Guide to Encryption Key Management Fundamentals.

CLEARING THE CONFUSION: KMS VS. KMS

THINGS CAN GET CONFUSING FOR END-USERS when the same acronym can be used to describe two completely different types of key managers. A cloud service provider's Key Management Service, such as AWS KMS, is a multi-tenant, encryption key storage service managed by AWS that provides a subset of encryption key lifecycle management. Administrative duties for encryption keys are a shared responsibility of the cloud service provider and the organization that uses the keys. This means that the organization is sharing custody (ownership and access) to encryption keys.

Conversely, for companies who think about centralized key management spanning multi-cloud, application, and databases, the term KMS refers to Key Management System. An Enterprise Key Management System is a security appliance (hardware or software) that manages encryption keys through their entire lifecycle - key creation, key activation, key use, key expiration or retirement, key escrow, and key destruction. The "Enterprise" part of this descriptive phrase is often dropped, and these types of system are often referred to as Key Management Systems. The word "Enterprise" is often used to indicate that the key management system can be used for a wide variety of purposes within an organization.

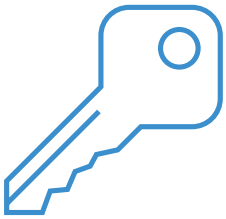
Key Management Systems may be hardware devices (usually hardware security modules, or HSMs), software appliances (think VMware virtual machines), or cloud instances such as AMIs that run in AWS EC2. Their use is dedicated to a single organization and usually managed by security professionals within that organization providing the organization exclusive custody of the encryption keys. Key Management Systems are usually validated to the FIPS 140-2 standard by the National Institute of Standards and Technology (NIST).

"Things can get confusing for end-users when the same acronym can be used to describe two completely different types of key managers."

WHO OWNS ENCRYPTION KEYS IN AWS?

WHEN EXPLORING CLOUD-BASED ENCRYPTION key management, one of the first questions that Enterprises ask themselves is, “who owns my encryption keys?”

The answer to this question is different depending on whether you deploy AWS KMS, CloudHSM, or a third-party encryption key manager like Townsend Security’s Alliance Key Manager.



For the purposes of this question, we can put AWS’s Cloud HSM and third-party key managers in the same category. These solutions are either a physical hardware security module (HSM), VMware instance, or Amazon Machine Image (AMI) that are dedicated to your organization and are virtually or physically located in an AWS regional cloud data center.

Amazon is clear on the topic of encryption key ownership with the CloudHSM service: Only you have access to the keys - with that said, it should be understood that Amazon has physical access to the HSM device in their data center and you do not.

The answer is a bit different for AWS Key Management Service (KMS). This is a multi-tenant service provided by Amazon which is backed by an Amazon hardware security module. That is, Amazon creates a key that is only used by you, but that key is protected (encrypted) by an Amazon managed HSM. When you create a key in KMS it is called a Customer Master Key, or CMK. The CMK is actually a data structure that contains your symmetric key and metadata about the key. The CMK is protected by an Amazon HSM key. So, the answer to the question about who owns your key is straight-forward: You and Amazon share ownership of the encryption key and that ownership is equal. You both can access the raw encryption key.

WHO HAS ACCESS TO MY ENCRYPTION KEYS IN AWS?

THIS IS THE NEXT QUESTION THAT ENTERPRISES generally ask themselves. It is a natural question to ask and it can be hard to determine the answer to this question with the various key management solutions available to cloud users - especially when considering the options available from AWS.

For the purposes of this guide, we will discuss Alliance Key Manager running as a stand-alone EC2 instance in Amazon Web Services, but is worth noting that there are other key managers that take a similar approach to being deployed in the AWS cloud.

There is no component of Alliance Key Manager that is shared by other users of AWS, and there is no component of Alliance Key Manager that uses encryption key management services provided by Amazon in AWS. Neither Amazon nor Townsend Security hold any credentials that grant access to the key manager solution, and there are no “backdoors” to the key manager. You, the AWS customer, solely and exclusively manage it.

Encryption keys in Alliance Key Manager are managed by the Alliance Key Manager Administrative Console. This is an application that you install on your PC or Mac and which accesses one or more instances of Alliance Key Manager in AWS. You maintain full control over the application used to manage keys - with no access ever by AWS.

Lastly, if an unauthorized user gains access to the Alliance Key Manager encryption key database they will not have access to the actual encryption keys. Data encryption keys (DEK) are encrypted by key encryption keys (KEK) which are stored separately. A stolen copy of the key database file will be insufficient to gain access to the encryption keys.

You should be aware that any cloud service provider has low level access to your virtual machines and storage. That is true of Amazon’s cloud platform as it is with any other cloud platform. You should also be aware that Amazon and other cloud service providers must obey the laws and regulations of the countries in which they operate. You cannot exclude the possibility that Amazon will provide access to your key management EC2 instance if required to do so under the law. In some countries this means that law enforcement organizations, national security agencies, and other governmental actors may have access to your encryption keys. And, while very unlikely, you cannot exclude the chance that an Amazon employee might make an unauthorized access to the EC2 instance of your key server. If these possibilities make you feel uncomfortable you should consider hosting your key management server outside of AWS.

PCI CLOUD GUIDANCE AND KEY MANAGEMENT

IN APRIL OF 2018 THE PAYMENT CARD INDUSTRY Security Standards Council (PCI SSC) released a document on cloud guidance called "Information Supplement: PCI SSC Cloud Computing Guidelines". It was an update of the first version of the guidance issued in 2013. While this is not a set of mandatory rules, it is a core guidance document and recommendations in PCI guidance documents often end up as requirements under the PCI Data Security Standard (PCI-DSS) and PCI Payment Application Data Security Standard (PCI PA-DSS). So it is worth understanding the guidance and it is wise to align your IT and business processes with the guidance.

Further, there is another reason to pay attention to the PCI cloud guidance - the PCI standards often set the expectations for security best practices in other regulations, and reflect evolving industry standards such as those developed by the National Institute of Standards and Technology (NIST). Even if you are not processing credit card payments, you should be paying attention to this guidance.

Take a look at appendix E.10 "Data Encryption and Cryptographic Key Management".

Appendix E.10 starts by describing the shared, multi-tenant architecture of cloud services (pretty much states the obvious). And then makes this statement:

"If a Customer shares encryption keys with the Provider, or engages the Provider as a key custodian, details of Provider access permissions and processes will also need to be reviewed and verified.

This consideration is particularly critical if cryptographic keys are stored or hosted by a third-party Provider that also hosts the encrypted data. If Provider personnel have access to a Customer's keys and the Customer's encrypted data, the Customer may have unintentionally granted the Provider ability to decrypt its sensitive data."

By using a service such as AWS Key Management Service (KMS), perhaps unknowingly, you **HAVE** granted your cloud provider the ability to decrypt your sensitive data.

Further, pointing back to the perceived risks of the cloud provider, here is the key point in the PCI guidance document:

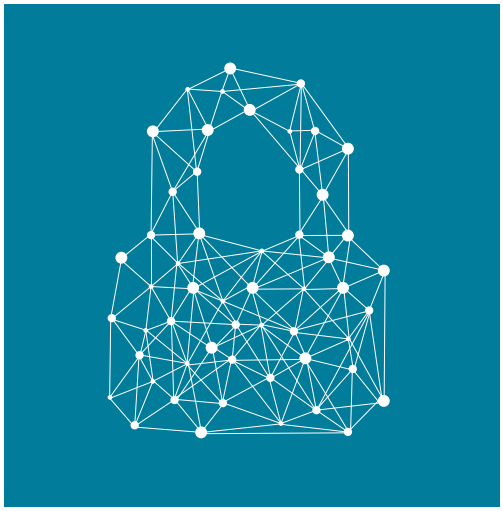
Because compromise of a Provider could result in unauthorized access to multiple data stores, ***it is recommended that cryptographic keys used to encrypt/decrypt sensitive data be stored and managed independently from the cloud service*** *where the data is located.*

PCI CLOUD GUIDANCE AND KEY MANAGEMENT (CONT)

The Cloud Guidance Computing Guidelines document provides some very strong, clear recommendations as what NOT to do. Fortunately, there are several approaches that an Enterprise can take to manage their encryption keys in the AWS cloud.

1. Deploy your own dedicated key manager in your own on-premise data center

It is fairly easy to deploy an encryption key manager in your own data center and enable its use by cloud applications. Most Enterprise key managers use a secure TLS-encrypted session to interoperate with the key manager. Once you enable an outbound cloud TCP port to your key manager, you can easily use the on-premise key manager. Note that this could be a hardware security module (HSM) or a virtual key management appliance running in VMware.



Remember that you probably do not have to retrieve the encryption key from the key server to your cloud application - most key managers support on-board encryption and decryption services. This alleviates the risk of an exposure of the encryption key in cloud memory. Performance will be the important factor to weigh in this regard. While the key manager may be quite efficient in the encryption or decryption operation, the communications lag times may mitigate against this approach.

2. Deploy your own dedicated key manager in a hosted platform

If your organization does not have on-premise infrastructure for a key manager, don't despair. It is really straightforward to deploy a key manager in a hosted environment. A hosting provider can provide a home for a hardware security module, or for a software appliance. Establishing the firewall rules may take a bit more work, but this is an approach that has worked well for our customers.

3. Deploy your own dedicated key manager in a different cloud

One creative option to separate the encryption keys from the protected data is to deploy the key manager in a different cloud platform. You could, for example, deploy your application data in Amazon Web Services, and deploy the key manager in Microsoft Azure. This helps mitigate the risk of one cloud service provider having access to both your encryption keys and your protected data - one of the key concerns expressed in the PCI guidance.

Note that this solution will probably require that you work with the firewall rules in both cloud provider platforms. The good news is that this is not complicated - we have customers doing this today.

PCI CLOUD GUIDANCE AND KEY MANAGEMENT (CONT)

4. Deploy your own dedicated key manager in a separate cloud instance

Lastly, it is possible to deploy a dedicated key management solution in the same cloud as your protected data, but completely avoid the use of the cloud provider's encryption key management infrastructure. The key server runs in its own virtual machine or EC2 instance and encryption key management is exclusively dedicated to you. If you take this approach, but sure that your key management vendor is not using the cloud provider's encryption key management infrastructure! Encryption keys and key management should only be accessible to you and not to your vendor or cloud provider.

> "Because compromise of a Provider could result in unauthorized access to multiple data stores, it is recommended that cryptographic keys used to encrypt/decrypt sensitive data be stored and managed independently from the cloud service where the data is located."

INTEGRATING WITH DATABASES AND APPLICATIONS

WITHOUT DEPLOYING A STRONG ENCRYPTION key management solution, encryption of sensitive data on its own is considered ineffective. The same goes for deploying a key storage solution that stores the key alongside your data in the Cloud. Therefore, having options for where you deploy key management is an important factor in your key management strategy. An effective key management solution should not only centralize your key management, it should protect your data wherever it is located, whether in the Cloud, a virtual environment, or on-site hardware.

In combination with a robust database encryption solution such as that from MongoDB, MySQL, or Microsoft SQL Server, your encryption key management solution will elevate your security position and total level of control.

For databases and applications who support the key management interoperability protocol (KMIP), the decision was likely a deliberate strategy to help users either leverage the Enterprise key management solution they already own, or use a new KMIP-compatible key management solution.

KMIP enables users to truly achieve centralized key management. A historical problem surrounding key management was the difficulty of an organization to store and manage encryption keys across multiple platforms, operating systems, and often departments. KMIP also enables AWS customers to choose their own KMIP compliant key management solution to maintain complete custody of the key management server, and therefore the keys. Whether deploying the key manager in the cloud, in a virtual environment, or on-site, owning a third-party KMIP compliant key manager allows users to retain total control of their keys without sharing access with cloud service providers or software vendors.

While AWS KMS services do not natively support KMIP, Enterprise databases and applications such as VMware vSphere/vSAN, MySQL and MongoDB do support KMIP, providing customers with an easy, standards-based method for protecting private data.

For Enterprises who want to encrypt their private data in AWS at the application level, they can take advantage of client side applications or software developer kits (SDKs). Enterprise level key management solutions will support a suite of languages that include Java, .NET, PHP, Python, C/C++, Perl, Cobol, JCL, and RPG. While not all key management vendors include SDKs and client connections as part of their key management license, vendors like Townsend Security do.

ENCRYPTION KEYS FOR APPLICATIONS

THE IDEAL KEY MANAGEMENT SOLUTION provides high availability, standards-based Enterprise encryption key management to a wide range of applications and databases.

MICROSOFT SQL SERVER

Data can by encrypted in a SQL Server database. In standard edition, you'll need to encrypt at the application level. In Enterprise edition, SQL Server has Transparent Data Encryption (TDE), Extensible Key Manager (EKM), and Cell Level Encryption (CLE). Townsend Security has an EKM provider. You need two things: A key management solution to protect the critical encryption keys, and an encryption solution for the SQL Server database. And they have to talk to each other. For the first part, the Alliance Key Manager for AWS provides a fully functional, Enterprise key management solution that protects SQL Server databases as well as other databases and other OSs. For encrypting SQL Server, the Alliance Key Manager solution comes with a full Microsoft SQL Server Extensible Key Management Provider, called the Key Connection for SQL Server. It's a module that our key management customers receive without paying additional license fees. Key Connection for SQL Server provides the encryption and integration with the key server to provide a complete end-to-end solution for encrypting data in the SQL Server database with compliant key management.

MONGODB

MongoDB offers AES encryption as part of the WiredTiger Storage Engine in the Enterprise edition of their offering. There are two options for storing encryption keys: In the database, in the clear; Or by using KMIP and a key manager. MongoDB strongly recommends the use of a key manager to protect the database keys. Alliance Key Manager is certified by MongoDB for use with the MongoDB Enterprise database on both Intel and IBM Power architectures.

DRUPAL

There is no native encryption in Drupal. Users need to install modules, such as Key, Encrypt, and Townsend Security's Key Connection For Drupal to encrypt private data in Drupal.

WINDOWS

Encryption needs to be done at the application level. This can be facilitated through the use of the Alliance Key Management Windows .NET SDK.

SOFTWARE DEVELOPER KITS (SDKS)

Encryption needs to be done at the application level. This can be facilitated through the use of the Alliance Key Management Windows .NET SDK.

JAVA, .NET, PHP, PYTHON, PERL, ETC.

VMware offers release notes, developer guides, API references, and other documentation for current and past versions of API and SDK sets. Businesses that

ENCRYPTION KEYS FOR APPLICATIONS (CONT)

aren't able or don't want to encrypt at the database level have options to encrypt at the application level. Good key management vendors (such as Townsend Security) offer SDKs and sample code to make encryption at the application level easy.

WINDOWS

Alliance Key Manager protects Windows .NET Client software with encryption and key management for applications. You can add the Windows .NET Client Assembly to your Windows projects to encrypt data at the application level.

LINUX

Linux applications use a variety of database and storage methods that include MySQL, MongoDB, PostgreSQL, Amazon S3 and RDS, and many others. Like any application deployed on any operating system and storage mechanism, Linux applications need to protect sensitive data at rest using strong encryption.

> "Townsend Security collaborates with developers and IT professionals around the world. We know that developers use a wide variety of languages and platforms to accomplish their work."

CLOUD PROVIDER LOCKIN

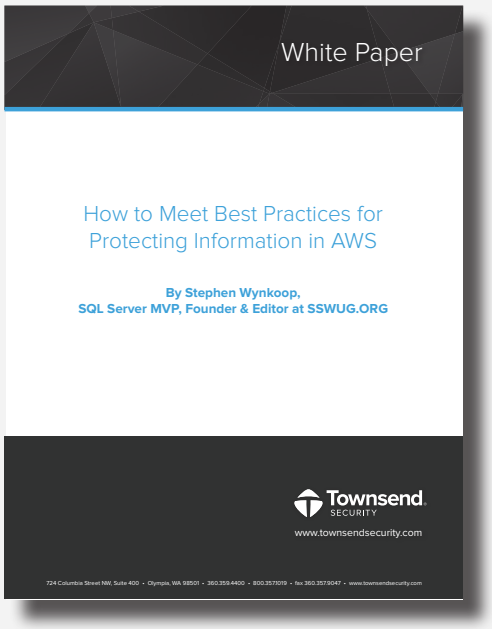
AS KMIP BECOMES MORE WIDELY ADOPTED, businesses are increasingly less likely to invest in technology that isn't standards based. Unfortunately, key management services such as AWS KMS and Azure Key Vault have not yet adopted the KMIP standard. Because CSP provided key management isn't based on standards, it leaves Enterprises with CSP lockin, and channel partners siloed into a single cloud. However, this doesn't mean that KMIP based key management in the cloud is unavailable. A quick search in the cloud marketplace will find other cost-effective alternatives. With KMIP key management, businesses can operate over hybrid cloud deployments and channel partners can offer solutions on their customers' cloud of choice. KMIP key management solutions found in CSP marketplaces provide businesses with a strong, multi-cloud offering that does not limit cloud scalability.

VMWARE ON AWS CLOUD

Recently, VMware has partnered with several cloud service providers to provide support for easy deployment and migration of VMware infrastructure and workloads to the cloud. This new initiative provides VMware customers with an easy path for cloud migration, and protection of their investment in human resources to manage the VMware environment. Unlike other cloud service provides, the AWS platform does not support the full stack of VMware capabilities. In the area of encryption key management for encrypted VMs and vSAN, AWS does not allow definition of a KMS Cluster in vSphere for encryption key management solutions. VMware customers migrating to the cloud should be aware of this limitation and the impact it has on security and a multi-cloud, cross-cloud, and hybrid strategy.

WHITE PAPER:

How to Meet Best Practices for Protecting Information in AWS



DOWNLOAD

AVAILABILITY ZONES / HIGH AVAILABILITY / HYBRID DEPLOYMENTS

MANY ORGANIZATIONS ARE PUTTING THEIR mission critical applications in the cloud. This means that the cloud deployment must match the same resilience and high availability as their on-premise deployments. Cloud service providers vary a great deal in how the provide geographic redundancy and in how they implement high availability for your applications. One big challenge is achieving your high availability goals for encryption key management. Many cloud service provider key storage solutions do not support geographic redundancy across cloud regions and availability zones. Be sure that you understand these limitations.

Townsend's Alliance Key Manager fully supports HA deployments across regions and availability zones, and even to customer on-premise data centers.

TO MAINTAIN AVAILABILITY OF ENCRYPTED data, businesses should have control over key backup and restore. While Enterprise level key managers support these functions, businesses should be aware that not all do. In the event of catastrophic loss of your application, your keys should be fully backed up to external storage that you specify. When comparing key management solutions, make sure that you are able to have real-time mirroring of encryption keys and access policies to one or more failover key servers.

MORE READING

WHITE PAPER:
INDUSTRY MUST-HAVES FOR EFFECTIVE ENCRYPTION KEY MANAGEMENT

DOWNLOAD

FIBBING ABOUT FIPS

WHEN DEPLOYING A KEY MANAGEMENT solution it is important to be sure that the key manager has been validated to the NIST FIPS 140-2 standard. Governments and large Enterprises require this type of validation. Never accept a vendor's claims about FIPS 140-2 compliance. Unfortunately there is a fair amount of deception in the vendor community on this topic. Use the NIST website to verify a vendor's claims of FIPS 140-2 compliance. The web site is here.

Another area to check: What FIPS 140-2 overall level does the vendor claim? A vendor may claim compliance with Level 3, for example. But a review of the Security Policy on the same NIST website may show an overall level of Level 1. Making assumptions about FIPS compliance can have bad consequences for your sales and strategic development. Be careful, it's a jungle out there!

"Never accept a vendor's claims about FIPS 140-2 compliance. Unfortunately there is a fair amount of deception in the vendor community on this topic."

VENDOR CONSIDERATIONS

GENERALLY, THE CONSIDERATIONS FOR key management for AWS will be similar to any relationship you develop with a vendor. The limited number of vendors in this space can limit the choices you have, but there are good solutions to choose from.

LICENSING

Vendors take a variety of approaches to licensing their key management solution. The main difference is in licensing constraints on the AWS side. You may start your first AWS encryption project with a rather limited scope. But as you continue to encrypt more sensitive data you may need to scale. Some encryption key management vendors license software based on the number of keys used, AWS instances or databases that you place under protection. Others provide unlimited numbers of client-side licenses after you acquire the key manager. Be sure you understand the licensing terms of each solution you evaluate, and be sure to understand your long-term needs. Naivete about vendor licensing can lead to big budget surprises later! With Alliance Key Manager, there are no extra licensing fees based on the number of keys, additional clients, number of virtual machines, or number of databases. Organizations should not have to pick and choose what data to protect.

DOCUMENTATION

Documentation on your AWS implementation will be crucial for long-term success. In addition to documentation on the installation and configuration, be sure your vendor provides documentation on key rotation, applying patches to the key manager, upgrading the key manager to new versions, and problem determination. All of these aspects should be covered in vendor documentation.

TRAINING

While key management solutions have become much simpler over time, you should still expect to receive some operational and technical training from your encryption and key management vendor. Gone are the days when this meant a lot of on-site consulting and educational expense. Modern encryption and key management solutions may require little or no time of coaching and training to deploy and maintain. Be sure your encryption and key management vendor has a program to deliver training in a timely fashion.

CUSTOMER SUPPORT

Many vendors have devalued their customer support experience, which can be a problem for all key manager users. When you have a problem with encryption or key management, it's likely to affect your application service levels. Before acquiring your key management solution be sure to schedule time with the customer support group. Do they have a formal problem tracking system? Do you have access to all problem tickets you raise? Does the customer support group respond in a timely fashion? Is there a 24/7 response number? All of the normal customer support questions you might ask are relevant to an AWS key management solution. We all know what really bad customer support feels like, so be sure there is a good team standing behind the solution you deploy.

VENDOR CONSIDERATIONS (CONT)

SERVICES

The modern Enterprise is often geographically distributed, which can make deployment and training difficult. While AWS encryption key management solutions can be simple to deploy and configure, you may want to be sure your vendor can send staff on-site for support.

> “Be sure you understand the licensing terms of each solution you evaluate, and be sure to understand your long term needs.”

MORE INFORMATION

WEBINAR:

Securing Data in the Cloud with Encryption & Key Management

VIEW WEBINAR

SUMMARY

THE CLOUD HAS BEEN A GAME CHANGER FOR organizations of all sizes, providing efficiencies and capabilities that have previously been impossible for organizations constrained within traditional IT data center worlds. Amazon Web Services provides organizations with reliable, scalable, and inexpensive cloud computing services. With the addition of encryption with key management under your control, you can deploy secure environments where there is less risk of data loss in the event of a breach.

The Alliance Key Manager client-side applications, software libraries, and SDKs fully integrate with Alliance Key Manager for key protection, and work naturally with your SQL Server, MongoDB, MySQL, Windows, and Linux deployments. This solution offers unparalleled security, flexibility, and affordability for all AWS cloud users. With no client-side software to install, customers can deploy Alliance Key Manager and install the PKI certificates on the database server to easily begin retrieving encryption keys.

By deploying as a virtualized encryption key manager, Enterprises are able to reduce hardware costs, lower operational costs, minimize the IT footprint, and a clear path for a future move to the cloud. Using the same FIPS 140-2 compliant technology that is in our HSM and in use by over 3,000 customers, Townsend Security's Alliance Key Manager for AWS brings a proven and mature encryption key management solution to AWS with a lower total cost of ownership.

The solution is available as an HSM, VMware instance on-premise, VMware instance on AWS, and in the cloud (Amazon Web Services, Microsoft Azure, and VMware vCloud), allowing organizations to meet compliance requirements (PCI DSS, HIPAA, GDPR, etc.) and security best practices. Townsend Security offers a 30-day, fully-functional evaluation of Alliance Key Manager.

RESOURCES

SOLUTION BRIEF

Alliance Key Manager for AWS

WHITE PAPERS

Encryption Key Management in the AWS Cloud

How to Meet Best Practices for Protecting Information in AWS

DEFINITIVE GUIDES

The Definitive Guide to Encryption Key Management

The Definitive Guide to SQL Server Key Management

The Definitive Guide to MongoDB Encryption Key Management

The Definitive Guide to VMware Encryption Key Management

Shift Left: Designing Applications for Encryption & Key Management

ALLIANCE KEY MANAGER

"A very cost effective solution in terms of performance, manageability, security, and availability. As a result, my company was quickly able to implement full database encryption leveraging the AKM as our key management solution in weeks. Comparable solutions could have taken months."

- CERTAIN

ALLIANCE KEY MANAGER FOR AWS OFFERS unparalleled security, flexibility and affordability for all users of AWS. As an agent-less solution with no client-side software to install, customers can deploy Alliance Key Manager and install the PKI certificates on the database server or within applications to easily begin retrieving encryption keys.

Alliance Key Manager is FIPS 140-2 compliant and in use by over 3,000 organizations worldwide. The solution is available as a hardware security module (HSM), VMware instance, and in the cloud (Amazon Web Services, VMware Cloud on AWS, and Microsoft Azure). Townsend Security offers a 30-day, fully-functional evaluation of Alliance Key Manager.

30-DAY EVALUATION

ALLIANCE KEY MANAGER

- FIPS 140-2 and KMIP compliant Enterprise key manager
- Available as an HSM, VMware, or in the cloud (AWS, Microsoft Azure)
- Affordably priced, with no restrictions on server connections or client side applications
- Meet compliance regulations like PCI DSS, HIPAA, GDPR, and more

REQUEST EVALUATION

ABOUT TOWNSEND SECURITY

"Townsend is a full service security provider that remains on the cutting edge and has demonstrated exceptional customer service."

- CSU FRESNO

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 organizations 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, SOX, GDPR and other regulatory compliance requirements.

CONTACT TOWNSEND SECURITY

www.townsendsecurity.com
@townsendsecure

105 8th Avenue SE, Suite 301
Olympia, WA 98501

360.359.4400

aws partner network

Advanced Technology Partner

Townsend SECURITY