Alliance Key Manager for VMware Cloud on AWS

Dedicated key management in AWS – with no access to encryption keys by cloud service provider (CSP).

Bringing together best-of-breed technologies and capabilities that create a seamless and flexible hybrid cloud future for customers, VMware and AWS enable services that easily grow and evolve as enterprise needs change. Whether expanding services on-premises or in the public cloud, the VMware Cloud on AWS eliminates the need to make changes to operating models or architectures. The result is the most flexible approach to evolving enterprise cloud strategies to keep pace with digital transformation in business environments.

Securing Private Information in AWS

As VMware users turn to VMware Cloud on AWS, they bring their sensitive data with them – customer names, email addresses and other personally identifiable information (PII). While key management solutions offered by CSPs provide convenience, they leave your keys accessible to third-party administrators – increasing the risk to your security posture.

As discussed in PCI SSC's *Information Supplement: Cloud Computing Guidelines*, "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."

With the flexibility and security of a native VMware encryption key manager in AWS, enterprises can be confident that their data is safe and that they can meet evolving compliance requirements.

Encryption Key Management for Your Databases and Applications

As enterprises adopt VMware Cloud on AWS, there has been a growing demand for VMware native encryption key management. When storing and managing encryption keys with a CSP provided service, an organization's attack surface increases, and therefore the risk of a data breach. Further, by allowing a CSP to administer your encryption keys, you are indirectly giving them access to your customer information, intellectual property, and other personally identifiable information (PII) – increasing your exposure to potential data loss.

By deploying Alliance Key Manager for VMware Cloud on AWS, customers can achieve their security and efficiency goals in a cloud environment. Alliance Key Manager for VMware Cloud on AWS brings a proven and mature encryption key management solution to VMware Cloud on AWS, with a low and predictable total cost of ownership. The solution is FIPS 140-2 and KMIP compliant, supports all major enterprise platforms and offers a wide variety of client side applications. With over 3,000 customers worldwide protecting information in Microsoft SQL Server, MongoDB, Oracle, and other databases, Alliance Key Manager for VMware Cloud on AWS is an easy to deploy, native centralized key management solution for VMware Cloud on AWS users.

vmware®

"When choosing a key management solution, it needed to be 1) KMIP compliant and 2) affordable. Alliance Key Manager was both."

— JONATHAN GANUCHEAU
SYSTEM ARCHITECT
SEED COMPANY

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, GDPR, HIPAA/HITECH, and other regulatory compliance requirements.

USE CASES

Alliance Key Manager helps businesses within regulated industries meet data privacy compliance requirements. Whether you are in the finance industry and need to protect private information or in the technology industry and need to protect intellectual property, encryption and key management is the best way to keep data safe.

Top Solution Verticals:

- Finance
- Healthcare
- Government
- Retail

SEE OUR SOLUTIONS IN THE VMWARE SOLUTION EXCHANGE (VSX)

https://solutionexchange.vmware.com/store companies/ townsend-security-inc

Secure, Compliant, and Affordable Key Management

More than just secure key storage, Alliance Key Manager manages encryption keys through their entire lifecycle. For VMware users who need to meet compliance, the solution has been validated for PCI DSS in VMware by Coalfire, a PCI-qualified QSA assessor and independent IT and audit firm. Enterprises across all industry verticals, regardless of where they deploy VMware, are subject to PCI DSS compliance if they process electronic payments. For VMware customers, FIPS 140-2 compliant encryption and key management are a key defense for data security. Additionally, Alliance Key Manager for VMware can also help businesses meet other compliance regulations such as GDPR, HIPAA, GLBA/FFIEC, FISMA, etc.

With subscription and perpetual licensed options for the Alliance Key Manager for VMware, there are licensing options to fit the needs and budgets of our customers. Additionally, there are never extra fees for deploying additional nodes, databases or applications - giving your encryption strategy the freedom to scale without having to come up with budget for added licenses.

How it Works

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 Windows and Linux VMware virtual machines. Additionally, Alliance Key Manager for VMware Cloud on AWS is KMIP compatible, which allows for interoperable communication between cryptographic environments and encryption key managers – reducing the operational, training, and infrastructure costs for businesses.

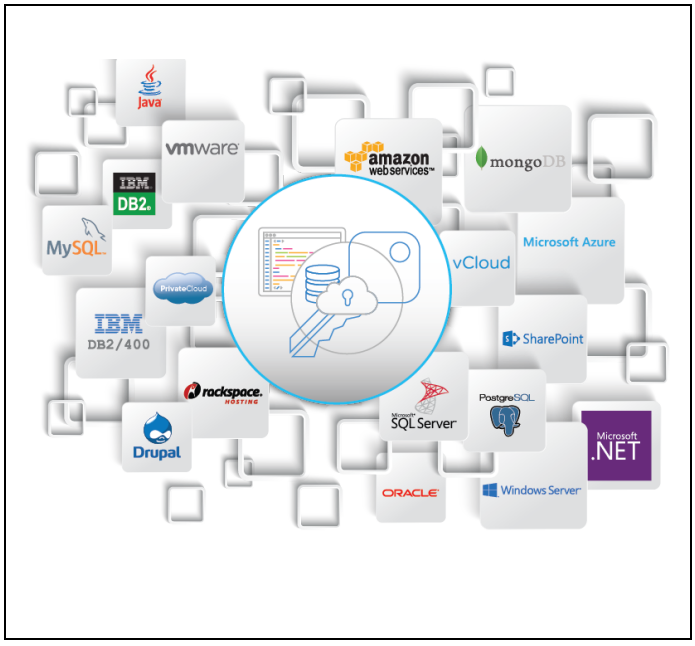

Figure 1: Alliance Key Manager is a centralized encryption key management server (KMS) that allows businesses to store and manage encryption keys separately from their private data.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.