SOLUTION BRIEF

Alliance Key Manager for IBM Cloud for VMware

Encryption Key Management for IBM Cloud for VMware

Cloud automation and server virtualization has been a game changing technology for IT, providing efficiencies and capabilities that have previously been impossible for organizations constrained within a physical world. Using the same FIPS 140-2 compliant technology that is in Townsend Security's hardware security module (HSM) and in use by over 3,000 customers, Alliance Key Manager for IBM Cloud for VMware enables enterprises to lower operational costs, meet compliance requirements, deploy encryption key management in the cloud, and accelerate deployment of mission critical security technology through a native VMware virtual encryption key manager.

Townsend SECURITY

Cost-Effective
Affordable key management solution for any size organization. Leverages current investment in encryption technologies via vendor-neutral solution.

Compliant
Meet data security requirements found in PCI DSS, HIPAA, CCPA, and more.

Compatible
Accessible from any Enterprise platform including Windows, Linux, IBM i, IBM z, and others. OASIS KMIP (Key Management Interoperability Protocol) compliant. Works with vSphere version 6.5 and later, and vSAN version 6.6 and later.

Easy to Use
Ready-to-use client software and SDKs speed deployment and reduce IT costs.

Secure Administration
Protects against key loss through secure and authenticated administration.

Partner Friendly
Extensive partner program insures successful and compliant results for your end customers.

105 8th Ave SE, Suite 301, Olympia, WA 98501 | www.townsendsecurity.com | 800 357 1019 +1 360 359 4400

Alliance Key Manager for IBM Cloud for VMware

Alliance Key Manager generates symmetric encryption keys for all AES key sizes including 128-bit, 192-bit, and 256-bit encryption keys; and asymmetric keys for all RSA key sizes. Encryption keys are generated using a cryptographically secure pseudo-random number generator (CSPRNG), and are stored in a secure database. All encryption keys are protected by two layers of encryption as well as SHA-256 hash verification to prevent key corruption and key substitution. Encryption keys can be either expiring or non-expiring to enforce key use policies as defined by the security administrator. Additionally, encryption keys can be created in advance of use and only available at a predetermined future date. Encryption key management is restricted to the security administrator and all key management activity is logged to the system log audit trail.

Securing Private Information in IBM Cloud for VMware

As VMware users turn to IBM Cloud for VMware, 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 IBM Cloud, 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 IBM Cloud for VMware, 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 IBM Cloud for VMware, customers can achieve their security and efficiency goals in a cloud environment. Alliance Key Manager for IBM Cloud for VMware brings a proven and mature encryption key management solution to IBM Cloud for VMware, 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 IBM Cloud for VMware is an easy to deploy, native centralized key management solution for IBM Cloud for VMware users.

Encrypt VMs and vSAN Storage

Alliance Key Manager can encrypt your VMs and vSAN storage that are managed by vSphere. Leveraging the KMIP interface in vSphere you can define one or more key managers to protect the encryption keys used to encrypt VMs and vSAN. Encrypting VMs and vSAN storage provides a rapid path to meeting security best practices and compliance regulations. There is no limit to the number of VMs or vSAN storage pools that you can protect.

Secure, Compliant, and Affordable

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 IBM Cloud for VMware can also help businesses meet other compliance regulations such as GDPR, HIPAA, CCPA, FFIEC, etc.

With subscription and perpetual licensed options for the Alliance Key Manager for IBM Cloud 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.