

ALLIANCE KEY MANAGER

Secure, compliant and affordable key management

Encryption Key Management in VMware

By deploying Alliance Key Manager for VMware as a virtualized encryption key manager, enterprises are able to reduce hardware costs, lower operational costs, minimize the IT footprint, and have a clear path for a future move to the cloud. Using the same FIPS 140-2 compliant technology that is in our hardware security module (HSM) and in use by over 3,000 customers worldwide, Alliance Key Manager for VMware is VMware Ready, brings a proven and mature encryption key management solution to VMware environments, with a lower total cost of ownership.

Secure, Compliant, and Affordable Key Management

In addition to supporting vSphere and vSAN encryption, Alliance Key Manager supports application and database encryption in deployed VMware virtual servers. The solution allows businesses to protect VMware images and digital assets while deploying a secure, compliant and affordable key manager. VMware customers can deploy multiple, redundant key servers as a part of the KMS Cluster configuration for maximum resilience and high availability.

When Alliance Key Manager for VMware is launched for the first time, it will automatically generate a certificate authority, client-side credentials, and create encryption keys that you can immediately use with SQL Server, MongoDB, Oracle, SharePoint, MySQL, and other applications you run in VMware.

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.

Meet Compliance Requirements

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.

“Townsend Security was extremely easy to work with - from the sales process to deploying our proof of concept to post-sales support.”

— ADAM BELL
SR. DIRECTOR OF IT
CITIZENS SECURITY LIFE INSURANCE



VMWARE VSPHERE

vSphere is the industry-leading server virtualization software and the heart of a modern SDDC, helping you run, manage, connect, and secure your applications in a common operating environment across clouds

PROTECT SENSITIVE DATA

In addition to supporting vSphere and vSAN encryption, Alliance Key Manager supports application and database encryption in deployed VMware virtual servers.

“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>

Only You Have Access to Your Keys

Whether you deploy Alliance Key Manager on premises or in the cloud, only you have access to your encryption keys because they are managed with a dedicated key management solution. This means that your keys will never reside within a multi-tenant key manager and only you have access to your encryption keys – something that cloud-based key management services are unable guarantee.

How it Works

The Alliance Key Manager client-side applications, software libraries, and software development kits (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 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.

Learn More

To learn more about how Townsend Security and Alliance Key Manager for VMware can better secure your encrypted data, download a free trial at <https://tsec.io/VSX> or contact Townsend Security or VMware partner or sales representative.

