KEY MANAGEMENT

Alliance Key Manager
HSM, VMware, & the Cloud

Manage Risk and Meet Compliance

Alliance Key Manager is an encryption key manager that is available as a hardware security module (HSM), cloud HSM, virtual appliance (VMware), or in the cloud (Microsoft Azure, Amazon Web Services, vCloud, etc.) Alliance Key Manager easily integrates with your databases/applications and enables you to address audit requirements for encryption and key management as found in PCI-DSS, HIPAA, HITECH and other privacy regulations, as well as meets emerging key management standards without putting business continuity at risrisk.

Certified. Comprehensive. Cost Effective.

Alliance Key Manager helps organizations affordably meet compliance requirements with FIPS 140-2 compliant encryption key management. The symmetric encryption key management solution creates, manages, and distributes 128-bit, 192-bit, and 256-bit AES keys for any application or database running on any Enterprise operating system (Windows, Linux, IBM i (AS/400), IBM z).

Townsend SECURITY

Compatible
Alliance Key Manager works with all major business platforms, cloud platforms, and leading encryption applications

FIPS 140-2 compliant

OASIS KMIP (Key Management Interoperability Protocol) compliant

Cost-Effective
Affordable key management solution for any size Enterprise.

Easy to Use
Ready-to-use client software speeds deployment and reduces IT costs.

Deployment Options
- Hardware Security Module (HSM)
- Cloud HSM
- VMware
- Cloud (AWS, Microsoft Azure)

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360 357 9047

Encryption Key Management

Hardware Security Module (HSM)

Hackers don't break encryption. They find your keys. Encryption keys should never reside on your server with encrypted data. Alliance Key Manager allows you to easily and affordably meet encryption key management compliance requirements with a FIPS 140-2 compliant encryption key manager. Wherever your data is, Alliance Key Manager can protect it.

Available as a hardware security module (HSM), cloud HSM, virtual appliance (VMware instance), or in the cloud (AWS, Azure, etc.), Alliance Key Manager provides full life-cycle management of encryption keys to help organizations meet PCI DSS, HIPAA, and PII compliance. With built-in key replication, key retrieval, and administrative controls, Alliance Key Manager is a secure, reliable, and affordable key management solution for a wide variety of applications. Additionally, Alliance Key Manager supports on-appliance encryption and decryption services so that your encryption key is always kept separate from the data it protects. [LEARN MORE]

Cloud HSM

Consisting of a pair of production and high availability (HA) key servers, Alliance Key Manager Cloud HSM is hosted in geographically dispersed data centers under an ITIL-based control environment independently validated for compliance against PCI DSS and SOC frameworks. This option allows customers to meet the most stringent data security standards without having to deploy the key management solution in their own data center. Key servers are pre-positioned in the hosting data center for rapid deployment. [LEARN MORE]

VMware

Alliance Key Manager is available as a VMware virtual appliance. Using exactly the same software as the Hardware Security Module (HSM) with FIPS 140-2 compliance, the VMware instance can be deployed in your IT Data Center or in a cloud environment that supports the vCloud architecture. Alliance Key Manager in VMware can help you meet PCI Data Security Standards for encryption key management when deployed according to the PCI virtualization guidelines. The VMware ESX, vSphere (ESXi), and vCloud platforms are supported by this option. [LEARN MORE]

Amazon Web Services (AWS)

Deployed as an AMI in Amazon Web Services, Alliance Key Manager for AWS relies on the same FIPS 140-2 compliant technology as the company's flagship Alliance Key Manager HSM that is in use by over 3,000 customers worldwide. When Alliance Key Manager for AWS 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, Oracle, SharePoint, MySQL, and other applications you run in Amazon Web Services. [LEARN MORE]

Microsoft Azure

The same FIPS 140-2 validated key management solution available in Townsend Security's hardware security module (HSM) can also run as a virtual machine in Microsoft Azure. You can easily deploy the best encryption key management solution for your cloud applications directly in Microsoft Azure and leverage all of the management options provided by Microsoft.
[LEARN MORE]

Microsoft Azure

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 validated solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, SOX, and other regulatory compliance requirements.

At Townsend Security we believe that everyone should be able to afford and easily deploy data protection that provably meets industry standards. Available at no extra charge, Townsend Security includes ready-to-use security applications (SQL Server, Drupal, more), SDKs, and sample code (Java, C#, IBM i, more) for developers. Additionally, there are never extra fees for deploying client-side applications.

Web: www.townsendsecurity.com
Phone: 360.359.4400 / 800.357.1019
Email: info@townsendsecurity.com
Twitter: @townsendsecure