KEY MANAGEMENT

Alliance Key Manager Cloud HSM
Solution Brief

Enterprise Encryption Key Management

On the road to protecting sensitive data assets in the cloud, data encryption remains one of the most difficult goals. A major barrier to achieving encryption has been the lack of an affordable Enterprise encryption key management solution.

Alliance Key Manager (AKM) Cloud HSM is provides Enterprise customers, OEMs, and ISVs with a secure method of managing encryption keys for their data security applications with an HSM in the cloud. Alliance Key Manager deploys as a key server appliance in any data center environment. With built-in key replication, key retrieval, encryption and administrative controls, Alliance Key Manager is a secure, reliable, and affordable key management solution for a wide variety of applications.

About Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, and Linux. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.

Townsend® SECURITY

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

FIPS 140-2 Level 1 compliance (certificate #1449)

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

Reliable
Hardware and software redundancy insure that you will never lose encryption services or encryption keys. Redundancy is provided through:

- Dual RAID controlled disk drives and dual power supplies
- Real time, bi-directional key mirroring
- On demand and scheduled backups
- High availability hot failover
- Load balancing support

www.townsendsecurity.com

Hosted Encryption Key Management

The Townsend Security Alliance Key Manager Cloud HSM offering helps you meet compliance and contractual requirements for data security in cloud environments using a dedicated Hardware Security Module (HSM) designed to create and protect encryption keys through the entire key lifecycle.

Townsend's Alliance Key Manager Cloud HSM deploys the Townsend Security Alliance Key Manager HSM in a secure validated cloud infrastructure to help you meet the most stringent requirements for encryption key management. The solution is NIST compliant to FIPS 140-2 Level 1 (certificate 1449) and is the same HSM solution that customers deploy in their own data centers. Enterprise customers can now safely migrate applications to the cloud without deploying key management in their own data centers. The Townsend Security Key Manager Cloud HSM offers fully redundant, NIST validated encryption key management for cloud applications running in Amazon Web Services, Microsoft Azure, Rackspace, Hosting.com, and many other cloud environments. You maintain full control over your encryption keys through the entire key lifecycle, the keys are only accessible by you, and you are not locked into your cloud vendor's key management facility.

Features and Benefits

With Townsend Security Alliance Key Manager Cloud HSM you can:

- Create, protect, store, and distribute encryption keys with tamper-evident HSM appliances. Only your security administrators have access to the HSMs.
- Access encryption keys and encryption services securely from any cloud environment such as Amazon AWS, Microsoft Azure, Rackspace, and other cloud providers.
- Deploy your own key retrieval software or leverage Townsend Security's rich library of sample code for key retrieval and on-device encryption. Developer resources are available for Java, PHP, Perl, Python, C/C++, C#, VB.NET, PL/SQL, COBOL, and RPG. Database samples include MySQL, Microsoft SQL Server, Oracle Database, and others.
- At no extra charge, deploy Townsend Security's ready-to-use security applications for Microsoft SQL Server Transparent Data Encryption (TDE) and Cell Level Encryption, Microsoft SharePoint encryption, and other applications. There are never extra fees for deploying client-side applications.
- Meet compliance regulations for system log collection without interference by your cloud vendor. Key server system logs can be sent to your own log collection server, or you can deploy a Townsend Security combined log collection server and key backup server under your control.
- Achieve true Separation of Duties and Dual Control that are mandatory for regulatory compliance and security best practices.
- Deploy fully redundant, highly available, mirrored key servers with geographic separation for the highest possible uptime for any data protection need. You can even integrate key management HSMs with key servers hosted in your data center.

Service Highlights

Secure Key Storage

You have dedicated control over key server HSM functions in the cloud. Townsend Security Alliance Key Manager Cloud HSM protects your cryptographic keys with HSM appliances in a secure data center. You retain full control of your keys and cryptographic operations on the HSM while Townsend Security provides hardware service and monitoring.

Contractual and Regulatory Compliance

By deploying Townsend Security's NIST FIPS 140-2 compliant solution, you will always meet the most stringent regulatory requirements for encryption key management. Please see Hosting.com's statement of compliance regarding the certifications of their network.

Reliable and Redundant Key Management

Townsend Security Alliance Key Manager Cloud HSM is deployed as a pair of key servers - a production key server and a high availability failover key server in geographically separate data centers. Data center redundancy includes geographic separation, redundant power sources in each data center, and redundant and segmented network connectivity. Your encryption keys are mirrored in real time to the failover key server over a secure connection. HSM hardware redundancy reduces the risk of server failures and includes hot-swappable RAID disk drives, dual power supplies, and multiple NICs.

Simple and Secure Connectivity

Alliance Key Manager HSMs are deployed in a secure, locked, dedicated rack in a secure data center with 24/7 physical access control and monitoring. All encryption key management, key retrieval, and encryption services are performed over mutually authenticated, TLS encrypted connections. Encryption keys are never retrieved in the clear, and encryption services are never performed in the clear - your keys and data are never exposed.

A Strong and Defensible Security Posture

By placing Alliance Key Manager Cloud HSM in a facility separate from your cloud applications, you can achieve the full control over your encryption keys in a way that meets Cloud Security Alliance recommendations for cloud key management, and help insure that you always meet compliance regulations for separate encryption key management. Key servers are dedicated hardware security modules that do not share memory, storage, or hardware resources with any other customer's HSM implementation. Cloud Security Alliance recommendations for encryption key management (Domain 11) can be found here.

Intended Use

The Alliance Key Manager Cloud HSM offering complements other Townsend Security key management offerings including HSMs installed in user data centers, VMware virtualized key management, and other key management offerings. The Alliance Key Manager Cloud HSM will be attractive to cloud customers who do not have traditional IT infrastructure but who also need an affordable, dedicated, validated encryption key management HSM to meet compliance regulations. Cloud applications in Amazon AWS, Microsoft Azure, Rackspace, and many other cloud platforms can use the Alliance Key Manager Cloud HSM solution to protect sensitive data.

Pricing

Unlike other Cloud HSM offerings, Alliance Key Manager Cloud HSM includes two key servers (production and high availability failover) at no additional charge and at a substantially lower cost, and you won't pay additional client-side license or usage fees.

Perpetual License

The perpetual license and annual maintenance option provides you with ownership of the Alliance Key Manager HSM hardware and a perpetual license to the key management software. Subject to reasonable notification and shipping times, you can request to have the key management HSMs shipped to your location (additional fees may apply). While installed at the hosting facility, Townsend Security will monitor the key server hardware and software and will provide any needed hardware service. An annual hardware and software support agreement is available that provides 24/7/365 response (subject to terms and conditions).

Subsription License

A subscription license provides you with a cost effective way to use the Alliance Key Manager HSM hardware and software without long-term purchase commitments. During the subscription period you have the same dedicated access and control over the Alliance Key Manager HSMs. Under the subscription license Townsend Security will monitor the key server hardware and software and Townsend Security will provide all hardware maintenance. A subscription license requires a minimum one year commitment, and then monthly subscription fees apply. Software support is included in the subscription cost and provides 24/7/365 response (subject to terms and conditions).

Order Processing

Orders for key servers can normally be filled very quickly. Additional time may be required for organizations that need more than two key servers.

Continuous Monitoring

Alliance Key Manager HSMs are monitored for hardware and key server application failures. In the event a production or high availability failover HSM encounters a problem, both you and the Townsend Security support team are notified of the event. In most cases a failing hardware component can be replaced without any interruption of cryptographic services. Townsend Security works with the hosting provider service team to replace any defective hardware.

Client-side Applications and SDKs

Alliance Key Manager includes a rich set of ready-to-use client-side applications, and a library of sample source code to assist developers. A partial list of client-side applications include:

- Microsoft SQL Server Transparent Data Encryption (TDE)
- Microsoft SQL Server Cell Level Encryption
- Microsoft SharePoint Transparent Data Encryption
- Microsoft Windows Volume and Folder Encryption
- IBM i (AS/400) DB2 Field Procedure (FIELDPROC) application support
- Developer resources include shared libraries and sample source code including:
- Microsoft SQL Server Standard and Web Edition SDK
- Microsoft .NET Assembly for Key Retrieval
- Oracle Database PL/SQL sample application code
- Java JAR files for key retrieval and encryption, and sample code

- Microsoft C# and VB.NET key retrieval sample code
- PHP, Perl, and Python sample key retrieval sample code
- MySQL Database Encryption sample code

Locations

Townsend Security key managers are available in two data centers. One is located in Newark, Delaware (East) and the other is located in Denver, Colorado (West). You can choose to locate your production key server HSM in either data center, and the high availability failover key server HSM will be located in the other data center.

Firewall

The Alliance Key Manager HSM runs on an Enterprise Linux platform and provides access to full Linux firewall facilities. Out of the box firewall protections limit inbound and outbound access to ports and services. You can add additional firewall rules to further protect access to your key server HSMs.

Optional Backup & Logging Server

Good security practice and PCI Data Security Standards dictate that you should make secure backups of your encryption keys and key server configurations on a regular basis. You may also wish to collect key server system logs and key server key retrieval and encryption usage logs to meet compliance regulations. You can provide your own backup and log collection servers, or you can deploy Townsend Security's server within the same data center as your high availability key server. Built on the same resilient hardware base as the key server HSM, the Townsend Security log collection and backup server provides extensive storage for system logs and backups. The optional backup and logging server is priced separately.

Evaluations

Townsend Security makes it easy for you to evaluate the Alliance Key Manager HSM solution. Our evaluation options give you the ability to fully evaluate the full set of key management and on-device encryption functions and client-side applications. There is no charge for evaluation versions of the key manager.

Security Best Practices

Separation of Duties

Separation of duties is inherent in the design of the Alliance Key Manager Cloud HSM. Key management functions are fully independent of key retrieval and encryption operations giving you full separation of duties between security administration of keys and your application's use and consumption of keys. Townsend Security monitors the health of the HSMs but does not have server administration access, nor any access to your encryption keys. All security functions are fully under your control, and separated from Database Administrators and Application Developers.

Dual Control

Encryption key management operations can be implemented under key server-enforced Dual Control. When this feature is activated two independent security administrators must authenticate to the key server in order to manage encryption keys. All key management functions are fully logged, and logs are transmitted to your log collection server or SIEM solution.

Split Knowledge

Encryption keys are never exposed during the key generation, transmission, loading, storage, or destruction obviating the need for Split Knowledge. Encryption key security administrators never handle key material in the clear during any phase of key management.

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 3000 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. Learn more at www.townsendsecurity.com or by phone at (800) 357-1019.