RSA® DATA PROTECTION MANAGER

An easy-to-use solution that can manage encryption keys at the database, file server and storage layers

AT A GLANCE

– Lower the overall total cost of ownership associated with encryption with enterprise key management

– Leverage key management to solve a wide array of encryption and data protection needs – hosts, databases, SAN switches, tape libraries, tokenization, etc.

– Increase operational security through enhanced central control of encryption key policies and commands

EXECUTIVE SUMMARY

As an integral part of RSA Data Protection Manager (formerly RSA Key Manager), enterprise key management is an easy-to-use management tool for encrypting keys at the database, file server and storage layers. It is designed to lower the total cost of ownership and simplify the deployment of encryption throughout the enterprise. It also helps ensure that information is properly secured and fully accessible when needed at any point in its lifecycle through a powerful management console and built-in high-availability features. The key manager is part of RSA Data Protection Manager, which, combined with application encryption and tokenization, forms a comprehensive platform for enforcing and managing the security of sensitive data.

REALIZE THE BENEFITS OF ENTERPRISE KEY MANAGEMENT

Traditional approaches to enterprise key management can cause significant challenges. This is because too many administrators rely on the simplest mechanism for key management when implementing their encryption projects. Taking this approach may seem like an easy solution at first, but it leads to a number of problems.

First, key management is an important part of meeting compliance standards and with native solutions it is difficult for administrators to ensure that keys are handled in the proper manner. Second, when keys are managed in silos, the ability to share data across applications is limited. Last, the absence of an enterprise key manager creates the possibility of compromised or lost keys. Enterprise key management with RSA Data Protection Manager directly addresses these challenges with an enterprise key management solution that is easy to use and manage, eliminating the need for point solutions, reducing administrative overhead and improving ROI.

According to a report by Aberdeen Research*, organizations that deploy enterprise key managers are able to support encryption in 40% more applications and are able to manage 11.5 times more encryption keys. In addition, these organizations are able to do so at a significantly lower cost – up to 92% less in terms of average cost per key! Enterprise key management with Data Protection Manager can enable consistent key policies and allow organizations to leverage one key manager for a variety of encryption devices. This increases security, simplifies operations and lowers the total cost of ownership.

Data Sheet

RSA Data Protection Manager is advancing the operational benefits associated with enterprise key management. Many key managers concern themselves only with vaulting the keys and ignore the important management features that allow users to leverage their key management infrastructure. RSA Data Protection Manager has the features and functions necessary to add significant value to any encryption product.

Customers can lower the overall total cost of ownership associated with encryption by simplifying operations for administrators. Key policies, e.g., which clients have permission to generate/rotate/delete keys or tokens, can be defined centrally at the server and then enforced at the clients. These policies can also be defined per device, so that encryption in disk storage may have different permissions than encryption in tape media. In addition, RSA Data Protection Manager has robust server-side management interfaces to help administrators search easily and manage keys when they are vaulted. This can quickly help determine the right key to decrypt a specific piece of media.

The management layer can also help meet audit requirements by logging the appropriate encryption functions, helping to reduce manual processes. RSA Data Protection Manager provides a wide range of integrations to ensure that one key manager can be leveraged across multiple encryption solutions (including application encryption and tokenization). It integrates with host, database, SAN switches and native tape encryption solutions from RSA, EMC and best-of-breed partners such as Brocade®. RSA has also been instrumental in bringing key management standards to the market, which increases the integration capability of Data Protection Manager.

Lastly, Data Protection Manager can enable increased security and protection in encryption environments by giving administrators control of cryptographic key operations from a central device — increasing security by allowing critical functions to remain with the experts. It has the ability to send commands for key generation, rotation or deletion directly to clients to have those commands enforced. This increases security by allowing administrators to meet audit requirements through proper key rotation, and also to respond quickly and delete a key when it is compromised on the client. Data Protection Manager automatically protects the key vault with local clustering for fail-over, and built-in replication for disaster recovery capability between remote sites.

ABOUT RSA

RSA is the premier provider of security, risk and compliance solutions, helping the world’s leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.