IBM Security Guardium Key Lifecycle Manager

Highlights

- Modernized architecture for deployment on containerized platforms
- REST-based key serving multi-cloud and hybrid-cloud use-cases
- Align with industry regulations and reduce operational expense
- Simplify and automate key management process for self-encrypting media
- Centrally manage encryption keys to enhance data security
- Gain flexibility with support for encryption-key management standard, KMIP

Business data is growing at exponential rates, driving the demand to secure data on-premises and in the cloud. Enterprises have responded by implementing encryption at various layers: in hardware, on network and in applications. This response can result in a series of encryption silos within organizations—some of them containing confidential customer data—with inconsistent approaches to managing security, keys and domains. Key management for these encryption approaches is often similarly fragmented. In some cases, there is no formal key management process in place. Regardless of whether the key management process is fragmented or non-existent, organizations are at risk of losing control of their data.

In order to encrypt all data at rest and centralize the management of encryption keys, organizations need a solution that integrates with multiple data encryption systems, uses standard protocols, supports National Institute of Standards and Technology (NIST) guidance, is certified to Federal Information Processing Standard (FIPS) 140-2, and imposes little or no burden on IT operations and processes.

Deploy a simple solution to a complex problem

IBM® Security Guardium Key Lifecycle Manager provides a simple solution to the complex problem of key management. As encryption becomes more widely adopted, an increased number of keys require management throughout their lifecycles, and the keys have their own lifecycles that are separate from the data they're protecting. Guardium Key Lifecycle Manager can help you manage key lifecycles

from initialization and activation through expiration and destruction, allowing you to simplify, centralize and automate your organization's key management processes and reduce operational costs.

As data becomes more mobile, there are enormous direct and indirect risks of data loss or compromise. To reduce this risk, data should be encrypted and the organization should control the keys. Together with the IBM Guardium Data Encryption (GDE) set of products, Guardium Key Lifecycle Manager helps users ensure their sensitive information is protected in the event that media goes for repair, becomes misplaced or is stolen, or needs to be erased from the cloud. Additionally, support for the latest key management interoperability protocol (KMIP) standard allows Guardium Key Lifecycle Manager to manage encryption keys not only for GDE products, but also for a number of non-IBM encryption solutions, enabling efficient management of encryption keys for the entire organization.

Centrally manage encryption keys

Guardium Key Lifecycle Manager serves keys at the time of use to allow for centralized storage of key material in a secure location, a unique approach that supports multiple protocols for serving symmetric and asymmetric keys. Users can centrally create, import, distribute, back up, archive and manage the lifecycle of those keys using a customizable graphical user interface (GUI).

Because Guardium Key Lifecycle Manager enables keys to be generated and served from a centralized location, the embedded encryption engine in IBM's GDE offerings encrypts and decrypts data as it enters and leaves your data encryption environment, which can improve the secure handling of data.

Guardium Key Lifecycle Manager can be deployed with an optional hardware security module (HSM) to store the master key that is used to protect all keys stored in the Guardium Key Lifecycle Manager keystore. This capability can be enabled for installs with existing data or for new installations of Guardium Key Lifecycle Manager.

Guardium Key Lifecycle Manager supports the device-specific encryption requirements for a wide range of data encryption solutions.

Guardium Key Lifecycle Manager provides broad support for encryption keys, using a combination of proprietary and internationally standardized protocols to support:

- A broad range of IBM tape storage as well as Quantum and Spectra Logic tape drives and libraries
- A wide range of IBM disk storage systems (including IBM System Storage DS series storage controllers)

- Network storage devices from NetApp
- Grid-scale storage solutions designed for cloud storage implementations, such as IBM Spectrum Accelerate™
- High-performance enterprise file management systems, such as IBM Spectrum Scale
- Data warehouse appliances, such as those from IBM PureData® Systems
- Servers with self-encrypting disk drives, such as Lenovo System x servers
- Virtual systems such as VMware® vSAN and vCenter

Guardium Key Lifecycle Manager enables users to group devices into separate domains, allowing multiple administrators with different roles and permissions to be defined. By default, the groups of devices have access only to encryption keys defined within their group. These role-based access control features enable segregation of duties, mapping of permissions for actions performed against objects, and enforcement of data isolation and security in a multi-tenancy environment. Organizations can also define which administrators can perform custodial actions on keys and limit the permissions of operations staff to only the functions they require to perform their jobs.

For scenarios in which keys need to be created more frequently, Guardium Key Lifecycle Manager works with your existing high-availability and disaster-recovery solutions to create and replicate your keys. Furthermore, it has multi-master capabilities for real-time synchronization of up to 21 instances of Guardium Key Lifecycle Manager, helping to eliminate the chance of losing updates.

Support strong authentication and security

These rich multi-master and integration capabilities are made possible by strong authentication between IBM Security Guardium Data Encryption solutions and Guardium Key Lifecycle Manager. Each solution is registered with Guardium Key Lifecycle Manager prior to managing the encryption keys of the device. Each time an encryption device reconnects to request a key, the solution verifies its identity and cryptographically authenticates using the device's identifying certificate. Any unknown device is rejected or placed into a queue to be approved by the administrator. With this strategy, a rogue device cannot be deployed on the network and used to intercept enterprise organizational keys.

In addition to strong authentication, there is also strong security between the data encryption device and Guardium Key Lifecycle Manager. Temporary session keys are used to encrypt the encryption key and all of the traffic to the device. This approach to encryption can improve data security while simplifying encryption key management. The impact on performance is minimal, and each encryption solution performs cryptographic tasks instead of reaching across the network. Not having to change other processes, install more hardware or reconfigure software to support hardware means that security is simplified and streamlined.

Leverage a wide range of implementation options

Guardium Key Lifecycle Manager can be applied at different levels to simplify key management while helping to meet the unique needs of your organization:

- For organizations that manage keys within separate silos, Guardium Key Lifecycle Manager can simplify complex key distribution and management, reducing administrative burdens within each silo.
- For organizations that want centralized control and policy-driven key management, Guardium Key Lifecycle Manager offers consolidated management of keys across domains, supports standards that extend management to both IBM and non-IBM products, and integrates well into existing security-team methodologies.
- For organizations that want high availability and support for disaster recovery, Guardium Key Lifecycle Manager works with a wide variety of clustering, replication and failover implementations in their environments, leveraging current investments.
- The multi-master capability of Guardium Key Lifecycle Manager allows customers to deploy up to 21 masters across data centers, clouds, and across environments, with real-time synchronization of keys.
- While the cryptography inside of Guardium Key Lifecycle Manager is validated to FIPS 140-2 Level 1, users also have the option to leverage FIPS 140-2 Level 2- or 3-validated hardware to enhance key security.

Simplify key configuration and management tasks

Guardium Key Lifecycle Manager provides an easy-to-use, web-based GUI that helps simplify key configuration and management tasks. With this GUI, administrators can easily create keystores, assign keys and manage the lifecycle of both from a centralized console.

The software itself is typically installed on an organization's most secure and highly available server, as a virtual machine, or on a dedicated workstation. Once installed, the GUI allows administrators to perform basic local key lifecycle management on the drives and offers not only configuration and setup tools, but also audit and compliance support. The software provides three ways to add encryption-enabled devices: Auto-discovery of encryption-capable devices, discovery with administrator's approval, or manual addition. Once added, keys are assigned automatically per configured policy.

The GUI also enables administrators to implement key retention for backed-up data and to address rules for regulatory compliance and legal discovery. Guardium Key Lifecycle Manager also provides numerous methods for key backup and recovery in case of disaster. Administrators can configure rules for automated rollover of groups of keys so that new encryption keys are used automatically based on a configurable schedule. In this way, administrators can limit the amount of data encrypted with particular keys, minimize exposure when a key is compromised and

perform cryptographic erasure of data by deleting relevant keys when data is set to expire. The end result is the ability to configure automated key assignments over time such that the operations team has to interact with key management very infrequently.

Wizard-based assistance expedites deployment

Guardium Key Lifecycle Manager uses a wizard-based guide to help administrators through a series of simple, task-based screens that demonstrate key and device creation and the handling of new device requests. Administrators can also configure different devices to use certain communication protocols including Key Management Interoperability Protocol (KMIP).

Once registered, encryption devices appear in the Guardium Key Lifecycle Manager key administration section and are ready for use as a secure endpoint. The keys associated with the devices can then be managed through the GUI, including making updates, expiring or destroying the keys. The Guardium Key Lifecycle Manager key administration welcome page provides critical notices to administrators, including information about last backups and available protocols.

Benefit from lightweight, flexible deployments

Guardium Key Lifecycle Manager is an application that can be deployed on a variety of Microsoft Windows, UNIX and Linux operating systems. Its design and architecture do not require extensive RAM or processing resources; in fact, the solution can typically be deployed with 8 GB of RAM and a dual processor core.

Thanks to the application’s small footprint and the ability to be deployed as a virtual machine, organizations are easily able to manage multiple instances of Guardium Key Lifecycle Manager for redundancy and high availability or alignment with organizational structure.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitoring greater than 60 billion security events per day in more than 130 countries, and the corporation holds more than 3,700 security patents.

Next steps

→ For more information on this offering, please click here.

→ Contact us for pricing.

For more information

For more information

To learn more about this offering, contact your IBM representative or IBM Business Partner or visit:

https://www.ibm.com/us-en/marketplace/ibm-security-key-lifecycle-manager

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM Security Key Lifecycle Manager

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.