IBM Security Guardium Data Encryption

Highlights

- Granular data protection with centralized security policies
- Consistent security and compliance support across environments
- Flexibility and extensibility enable fast support of additional use cases
- Integrate with supported HSMs, other 3rd-party sources for encryption keys

As devastating security breaches continue with alarming regularity and compliance mandates become increasingly stringent, your organization needs to extend data protection controls across numerous environments, systems, applications, processes, and users. For organizations considering the development of a data protection program, encryption is a core technology to help safeguard data across a wide variety of environments and use cases—while still being easy to deploy and maintain.

IBM Security Guardium Data Encryption (GDE) offers a modular set of encryption solutions that help security teams to effectively enable data-at-rest security across the entire organization. GDE is composed of an integrated set of products built on a common, extensible infrastructure with efficient, centralized key and policy management designed to help your security teams reduce administration effort and address data security policies and compliance mandates, in keeping with encryption best practices.

CORE USE CASES FOR IBM SECURITY GUARDIUM DATA ENCRYPTION

Strength, security, and compliance. Guardium Data Encryption offers capabilities for protecting and controlling access to databases, files, containers, and applications. It can help protect assets residing in cloud, virtual, big data, and physical environments. This set of scalable data security solutions enables you to address pressing requirements and to prepare your organization to respond when the next security challenge or compliance requirement arises.

GDE's comprehensive capabilities help you address a range of security and privacy mandates, including the Payment Card Industry Data Security Standard (PCI DSS), the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), and regional data protection and privacy laws. GDE equips organizations with powerful tools to help combat external threats, guard against insider abuse, and establish persistent controls, even when data is stored in the cloud or an external provider's infrastructure.

Maximize staff and resource efficiency. GDE helps make administration simple and efficient through an intuitive web-based interface. With this solution, you can apply data-at-rest security quickly and consistently to help maximize staff efficiency and productivity. In addition, this high-performance solution enables efficient use of virtual and physical server resources, reducing the load on the service delivery infrastructure.

Reduce total cost of ownership. Instead of having to use multiple isolated products scattered across your organization, you can take a consistent and centralized approach across files, databases, applications, and big data environments with GDE—reducing the pain associated with integrations and the need for specialized knowledge of point solutions.

GUARDIUM DATA ENCRYPTION DATA SECURITY MANAGER

IBM Security Guardium Data Encryption is comprised of a suite of integrated products that are all administered via a common management server known as the Data Security Manager (DSM).

Unified management and configuration across the hybrid enterprise. The DSM centralizes key management and platform policy for all GDE products under a single console. The DSM and the products it manages integrate with user and group identity management systems such as LDAP, Active Directory, local user databases, Hadoop, and container environments. Strong separation-of-duties policies can be enforced as well. The DSM features remote administration, multi-factor authentication, and an internal HSM.

Key features:

- Multi-tenancy support
- Proven scale to 10,000+ agents
- Data protection policy definition
- Easy integration with existing authentication infrastructure
- RESTful API support

GUARDIUM FOR FILE AND DATABASE ENCRYPTION

Guardium for File and Database Encryption encrypts data-at-rest with centralized key management, privileged user access control, and detailed data access audit logging that can help organizations address compliance reporting. This solution helps protect structured databases, unstructured files, and linked cloud storage accessible from systems on-premises, across multiple cloud environments, and even within big data

and container implementations.

Support compliance requirements and granular access control. Guardium for File and Database Encryption delivers the controls to help address compliance and data privacy standards (including PCI DSS, HIPAA/Hitech, GDPR and many others) without operational or business process changes. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop, and containers. Controls include access by process, file type, time of day, and other parameters.

Non-intrusive, scalable, and easy to deploy across environments. GDE agents are deployed on servers at the file system or volume level and include support for Linux, Unix, Windows, SAP HANA, and Teradata file systems, as well as cloud storage environments like Amazon S3 and Microsoft Azure. Deployment requires no changes to applications, user workflows, business practices, or operational procedures, and administrators perform all policy and key administration through the DSM.

GDE FOR FILES AND DATABASES WITH LIVE DATA TRANSFORMATION

Deployment and management of data-at-rest encryption can present challenges when transforming clear-text to ciphertext, or when rekeying data that has already been encrypted. GDE for Files and Databases with Live Data Transformation eliminates these hurdles, enabling encryption and rekeying with unprecedented uptime and administrative efficiency.

The solution helps administrators to encrypt data with decreased disruption to users, applications, or workflows; users and processes continue to interact with databases or file systems as usual while encryption is underway. Seamless, non-disruptive key rotation allows users to perform key rotation without having to duplicate data or take associated applications off-line. In case of a data recovery operation, archived encryption keys recovered from the Data Security Manager are automatically applied to an older data set and the restored data is encrypted with the current cryptographic keys.

Key benefits:

- Reduce costs associated with encryption implementation and maintenance
- Minimize encryption's impact on the user experience
- Accelerate recovery of data encrypted with older keys
- Real-time encryption of unprotected data during initial deployment

GUARDIUM FOR CONTAINER DATA ENCRYPTION

Guardium for Container Data Encryption delivers container-aware data protection and encryption capabilities for granular data access controls and data access logging in containerized environments. This solution enables security teams to modify encryption, access controls, and data access audit logging on a per-container basis, both to data inside of containers and to external storage accessible from containers.

This solution secures container volumes, protects against root, privileged, or

unauthorized user access within containers, and helps protect against privilege escalation attacks from other containers. Users can isolate data access between containers and establish granular access policies based on specific users, process, and resource sets. With this solution, you can address compliance mandates for data access controls and container level auditing.

Key features:

- Provides encryption, granular data access controls, and data access audit logging, both for Docker and OpenShift hosts and images
- Offers controls that address data stored within containers, as well as data accessible from containers
- Enables container-specific granular data access controls for specific users, processes, and resource sets
- Doesn't require any changes to applications, containers, or infrastructure
- Uses the same agents and infrastructure set as Guardium for File and Database Encryption

GUARDIUM FOR TOKENIZATION

Guardium for Tokenization dramatically reduces the cost and effort required to comply with security policies and regulatory mandates. This solution provides data tokenization and dynamic display security, safeguarding and anonymizing sensitive assets. It allows users to leverage cloud, big data, and outsourced models more fully—without increased risk.

Dynamic data masking. This solution allows administrators to establish policies that tokenize an entire field or dynamically mask parts of a field.

Non-disruptive implementation. Users can restrict access to sensitive assets without changing the existing database schema. The solution's RESTful API implementation helps make it fast, simple, and efficient for application developers to institute sophisticated tokenization capabilities.

Simplified compliance. Guardium for Tokenization helps simplify the process of addressing compliance with regulations such as GDPR, that require protection of personally identifiable information (PII); it also helps minimize servers requiring audit and control.

Key features:

- Virtual appliance enables fast increase and decrease in capacity
- Deploys in AWS, Microsoft Azure, virtualized, and bare-metal environments
- Granular, policy-based dynamic data masking
- Role-based access control
- Strong safeguards to protect sensitive assets from cyber-attacks and insider abuse

GUARDIUM FOR APPLICATION ENCRYPTION

Guardium for Application Encryption streamlines the process of adding encryption into existing applications, delivering standards-based APIs that power high-

performance cryptographic and key management operations. When encryption occurs at the application level, data is encrypted across multiple (including disk, file, and database) layers. Guardium for Application Encryption delivers key management, signing, and encryption services, enabling comprehensive protection of files, database fields, big data selections, and so on. The solution is FIPS 140-2 Level-1 certified, based on the PKCS#11 standard, and fully documented with a range of practical, use-case based extensions to the standard. It supports Windows, Linux, and Teradata environments (available through Guardium for Teradata Encryption).

Enforce granular controls. With NIST-approved format-preserving encryption (FPE) capabilities, users can encrypt sensitive records without altering their format or field schemas. In addition, dynamic data masking enables users to present various levels of decryption and presentation of data to different users.

Streamline encryption implementations. Developers can use RESTful APIs, or C-, .NET- or Java-based applications linked with a local PKCS#11 library, to easily add standards-based secure key management and data encryption services to customized data security solutions.

Secure cloud, database, and big data. Address policies and compliance mandates that require granular encryption at specific layers, protecting sensitive data before being stored in database, big data, or cloud environments.

GUARDIUM FOR BATCH DATA TRANSFORMATION

Guardium for Batch Data Transformation provides static data-masking services that enable secure, fast, and efficient use of modern digital transformation initiatives such as data warehouses, big data on-premises, and in the cloud, sharing databases with DevOps and outsourced data analysis.

Flexible data masking. When installed on a server already equipped with Guardium for Application Encryption and Guardium for Tokenization, Batch Data Transformation utilizes Guardium for Application Encryption locally for encryption and key management and communicates with the Guardium for Tokenization server for tokenization and data masking services. Guardium for Batch Data Transformation accelerates deployment of Guardium for Tokenization or custom applications based on Guardium for Application Encryption.

Data security for digital transformation. Transformation options include either encryption or tokenization for files or supported databases. Use cases include:

- Rapid data rekeying
- Secure database or data extract sharing with big data consumers, DevOps, or third parties
- Preparing data for safe cloud migration
- Preparing a database for tokenization or application level encryption

GUARDIUM FOR CLOUD KEY MANAGEMENT

Guardium for Cloud Key Management allows customers to own and control the keys to their encrypted data, thanks to its Bring Your Own Key (BYOK) and Keep Your Own Key (KYOK) capabilities. This offering reduces key management complexity and operational costs by giving customers full lifecycle control of encryption keys with centralized management and visibility.

Customer key control. BYOK-based customer key control allows for the separation, creation, ownership, and control, including revocation, of encryption keys or tenant secrets used to create them. The solution can be deployed rapidly on-premises to help address more stringent compliance requirements, offering up to FIPS 140-2 certified cryptographic key generation and protection.

Strong encryption key security. Customer key control requires secure key generation and storage. This solution leverages the security of the DSM or supported HSMs to create and store keys.

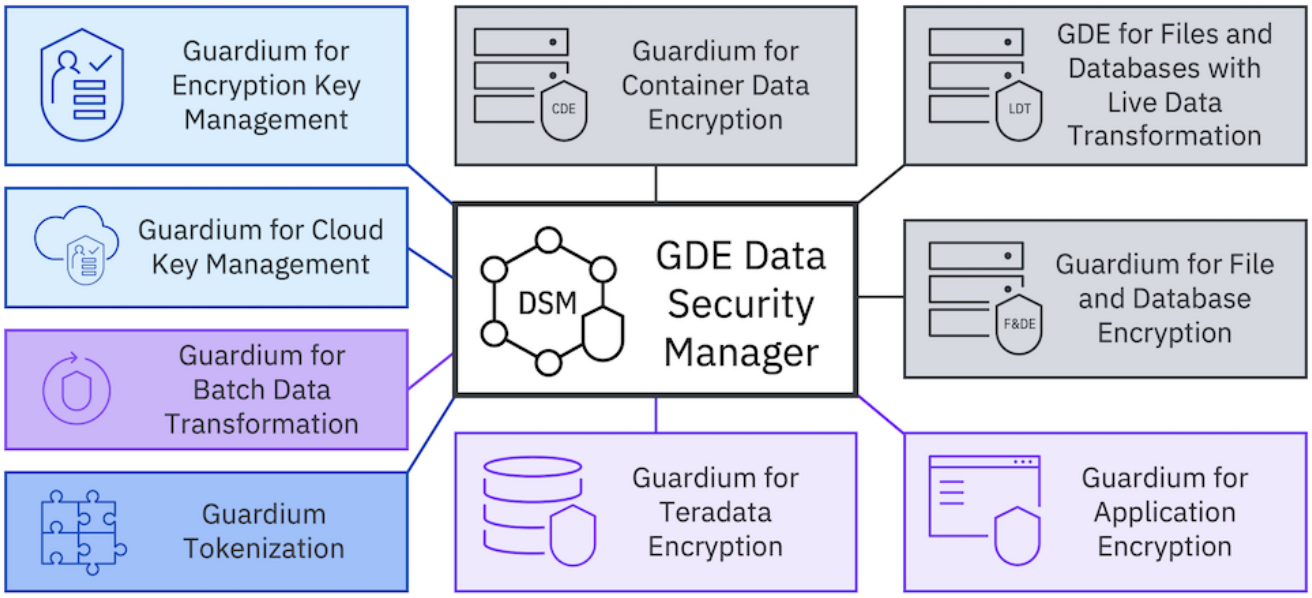
IT efficiency and compliance tools. Centralized key management for multiple cloud providers combined in a single browser window, automated key rotation, federated login, and management of native cloud keys help to enhance IT efficiency. Cloud-specific logs and prepackaged reports can help you to address compliance reporting requirements.

GUARDIUM FOR DATA ENCRYPTION KEY MANAGEMENT

Guardium for Data Encryption Key Management allows customers who already have a Data Security Manager deployed to manage encryption keys for external, KMIP-compatible data repositories and databases provided by third parties such as Oracle, VMware, or SQL. Consolidating key management fosters consistent policy implementation across multiple systems and reduces training and maintenance costs.

Key benefits:

- Secure storage of certificates and keys
- Expiration notifications for certificates and keys
- Reports provide status and audit support
- Secure replication of keys across multiple appliances with automated backups



The IBM Security Guardium Data Encryption Data Security Manager allows for flexible, centralized policy and key management across your entire Guardium Data Encryption deployment.

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 our offerings, 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/products/guardium-data-encryption

© Copyright IBM Corporation 2020.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at https://www.ibm.com/legal/us/en/copytrade.shtml, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM Security Guardium Data Encryption

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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