IBM Security Guardium Data Encryption

Highlights

- *Extend data protection to files, databases, applications and big data environments with the modular Guardium Data Encryption suite*
- *Address core use cases including strengthening security and compliance, maximizing staff and resource efficiency, and reducing total cost of ownership by leveraging encryption*
- *Understand core components of the Guardium Data Encryption suite, including the Data Security Manager, Guardium for File and Database Encryption, Guardium for Application Encryption, Guardium for Teradata Encryption, and Guardium for Tokenization, and how these pieces fit together to provide integrated protection capabilities*

As devastating security breaches continue to happen 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 any organization considering the development of a data protection program, encryption emerges as a core technology that can 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 suite of encryption solutions to enable security teams to effectively manage data-at-rest security across the entire organization. Built on an extensible infrastructure, GDE is composed of an integrated collection of products built on a common infrastructure with efficient, centralized key and policy management. As a result, your security teams can address data security policies and compliance mandates in keeping with encryption best practices, while reducing administrative effort and total cost of ownership.

CORE USE CASES FOR GDE SUITE

Strengthen Security and Compliance

Guardium Data Encryption offers capabilities for protecting and controlling access to databases, files, and applications—and can secure assets residing in cloud, virtual, big data and mainframe environments. By leveraging GDE, security teams can address a broad set of use cases and protect sensitive data across the organization. The platform delivers comprehensive capabilities that enable teams to address the demands of 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 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

Guardium Data Encryption makes administration simple and efficient, offering an intuitive web-based interface. With this solution, you can apply data-at-rest security quickly and consistently to maximize staff efficiency and productivity. Plus, 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

Guardium Data Encryption makes it simpler and less costly to protect data at rest through enabling IT and security organizations to quickly safeguard data across your organization in a uniform and repeatable way. Instead of having to use a multitude of 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 pains 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 several different products that provide specific capabilities based on user needs – Guardium for File and Database Encryption, Guardium for Tokenization with Dynamic Data Masking, Guardium for Application Encryption, and Guardium for Teradata Encryption – that are all accessed via a common management server known as the Data Security Manager.

Unified Management and Configuration Across the Hybrid Enterprise

The Data Security Manager (DSM) centralizes management and policy for all Guardium Data Encryption products, and enables organizations to efficiently address compliance requirements, regulatory mandates and industry best practices, and to adapt as deployments and requirements evolve. It features an intuitive, web-based console and APIs for managing policies, auditing, and encryption keys to enable flexibility and ease of use.

Security users and groups can be integrated with LDAP and Active Directory for best practice management of security policies and deployments, and the solution also provides the logs needed to support the various compliance requirements. To minimize costs, the DSM also provides central management of heterogeneous encryption keys for the GDE agents.

Secure, Reliable and FIPS-Certified System

To maximize uptime and security, the DSM features redundant components and the ability to cluster appliances for fault tolerance and high availability. Strong separation-of-duties policies can be enforced to ensure that one administrator does not have complete control over data security activities, encryption keys or administration. In addition, the DSM supports two-factor authentication for administrative access.

Key Features of the Data Security Manager

- Single console for all platform policy and key management
- Multi-tenancy support
- Proven scale to 10,000+ agents
- Clustering for high availability
- Toolkit and programmatic interface
- Easy integration with existing authentication infrastructure
- RESTful API support
- Multi-factor authentication

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

GUARDIUM FOR FILE AND DATABASE ENCRYPTION

Guardium for File and Database Encryption (GDE for Files and Databases) delivers data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging that helps organizations meet compliance reporting and best practice requirements for protecting data, wherever it resides.

This solution's transparent approach protects structured databases and unstructured files, and is designed to meet data security requirements with minimal disruption, effort, and cost. Implementation is seamless – keeping both business and operational processes working without changes, even during deployment and roll out.

Support Compliance Requirements and Granular Access Control

Encryption, access controls and data access logging are basic requirements or recommended best practices for almost all compliance and data privacy standards and mandates, including PCI DSS, HIPAA/HITECH, GDPR and many others. Guardium Data Encryption delivers the controls required without operational or business process changes.

GDE for Files and Databases allows security professionals to apply granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop and containers. Controls also include access by process, file type, time of day, and other parameters.

Enable Scalable Encryption Across All Your Environments

The Guardium Data Encryption agent runs at the file system or volume level on a server. The agent is available for a broad selection of Windows, Linux and Unix platforms, and can be used in physical, virtual, cloud, and big data environments— regardless of the underlying storage technology. Administrators perform all policy and key administration through the Data Security Manager (DSM).

Encryption takes place on the server, eliminating bottlenecks that plague legacy, proxy-based solutions. Performance and scalability are further enhanced by leveraging cryptographic hardware modules that are built into such modern CPUs, such as Intel AES-NI, IBM Power8 in-core and Oracle SPARC.

Non-Intrusive and Easy to Deploy

Guardium Data Encryption agents are deployed on servers at the file system or volume level and include support for Linux, Unix, Windows file systems as well as cloud storage environments like Amazon S3 and Azure Files. Deployment requires no changes to applications, user workflows, business practices or operational procedures

Key Features of GDE For Files and Databases

- **Broad platform support:** Windows, Linux and Unix operating systems
- **High performance encryption:** Uses the hardware encryption capabilities built into host CPUs - Intel and AMD AES-NI, PowerPC 8 AES, and SPARC encryption
- **Suite B protocol support**
- **Log all permitted, denied and restricted access attempts** from users, applications and processes
- **Role-based access policies:** Control who, what, where, when and how data can be accessed
- **Enable privileged users** to perform their work without access to clear-text data
- **Extensions** offer added capabilities, including more granular container support and zero-downtime data encryption capabilities

GUARDIUM DATA ENCRYPTION FOR FILES AND DATABASES WITH LIVE DATA TRANSFORMATION

Deployment and management of data-at-rest encryption can present challenges when transforming clear-text to cipher-text, or when rekeying data that has already been encrypted. Traditionally, these efforts either required planned downtime or labor-intensive data cloning and synchronization efforts. Guardium Data Encryption Live Data Transformation Extension eliminates these hurdles, enabling

encryption and rekeying with unprecedented uptime and administrative efficiency.

The Live Data Transformation add-on to Guardium Data Encryption for Files and Databases delivers these key capabilities:

- **Zero-downtime encryption deployments:** The solution enables administrators to encrypt data without downtime or disruption to users, applications or workflows. While encryption is underway, users and processes continue to interact with databases or file systems as usual.
- **Seamless, non-disruptive key rotation:** Both security best practices and many regulatory mandates require periodic key rotation. Live Data Transformation makes it fast and efficient to address these requirements. With the solution, you can perform key rotation without having to duplicate data or take associated applications off line.
- **Intelligent resource management:** Encrypting large data sets can require significant CPU resources for an extended time. Live Data Transformation provides sophisticated CPU use and I/O rate management capabilities so administrators can balance between the resource demands of encryption and other business operations. For example, an administrator can define a resource management rule specifying that, during business hours, encryption can only consume 10% of system CPU, while on nights and weekends, encryption can consume 70% of CPU.
- **Versioned backups and archives**: With key versioning management, Live Data Transformation offers efficient backup and archive recovery that enable more immediate access. In a data recovery operation, archived encryption keys recovered from the Guardium Data Security Manager are automatically applied to an older data set. Restored data is encrypted with the current cryptographic keys.

With these capabilities, Guardium for File and Database Encryption with Live Data Transformation extends the capabilities of GDE files and databases by allowing the encryption of files and databases without taking them offline to do so – bringing significant performance and operational benefits.

GUARDIUM TOKENIZATION WITH DYNAMIC DATA MASKING

Guardium Tokenization with Dynamic Data Masking enables organizations to substitute a "token" for sensitive data which can be mapped to the original value via tokenization, and also facilitates masking to desensitize personal information and make it unreadable from the original form while still preserving format and referential integrity. These capabilities can dramatically reduce the cost and effort required to comply with security policies and regulatory mandates like the Payment Card Industry Data Security Standard (PCI DSS). Now, organizations can efficiently address objectives for securing and anonymizing sensitive assets—whether they reside in the data center, big data environments or the cloud.

Easily Protect Against Internal and External Threats

Guardium Tokenization makes it easy to use format-preserving tokenization to protect sensitive fields in databases and to add policy-based dynamic data masking to applications. The solution delivers the following core capabilities:

- **Dynamic data masking:** Administrators can establish policies to return an entire field tokenized or dynamically mask parts of a field. For example, a security team could establish policies so that a user with customer service representative credentials would only receive a credit card number with the last four digits visible, while a customer service supervisor could access the full credit card number in the clear.
- **Non-disruptive implementation:** With the solution's format-preserving tokenization capabilities, you can restrict access to sensitive assets without changing the existing database schema. The solution's RESTful API implementation makes it fast, simple and efficient for application developers to institute sophisticated tokenization capabilities.

- **Batch data transformation:** With this optional utility, you can tokenize high volumes of sensitive records without lengthy maintenance windows and downtime. You can mask sensitive columns in production databases and in copies of databases before they are sent to third-party developers and big data environments.

Through leveraging Guardium for Tokenization with Dynamic Data Masking, organizations can safeguard against both external attacks and insider abuse, while also taking full advantage of flexibility afforded by the cloud without fear of unauthorized sensitive data access by CSPs.

GUARDIUM FOR APPLICATION ENCRYPTION

Guardium for Application Encryption (GDE for Applications) delivers key management, signing, and encryption services enabling comprehensive protection of files, database fields, big data selections, or data in platform-as-a-service (PaaS) environments. 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. GDE for Applications accelerates development of customized data security solutions.

Streamline Encryption Implementations

Guardium for Application Encryption solution simplifies the process of adding key management and encryption to applications. Developers use RESTful API's, or C- or Java-based applications linked with a local PKCS#11 library, to add standards-based secure key management to customized data security solutions. The solution allows security teams to address policies and compliance mandates that require encryption of specific fields at the application layer, securing sensitive data before it is stored in database, big data, or cloud environments.

GUARDIUM FOR TERADATA ENCRYPTION

By aggregating massive volumes of enterprise data in Teradata environments, businesses can gain unprecedented insights and strategic value. Unfortunately, this very aggregation of data can also present heightened risks. Without proper protections, the sensitive assets compiled in these environments can inadvertently be exposed by privileged administrators, or be the target of theft by malicious insiders and external attackers – and storing exponentially greater amounts of data together in one place makes the threat of exposure greater. Now, Guardium Data Encryption for Teradata Databases (GDE for Teradata) enables your organization to guard against these risks through employing robust data-at-rest security capabilities in your Teradata environments.

Strengthen Security While Minimizing Disruption and Costs

GDE for Teradata simplifies the process of securing sensitive records, enabling encryption of specific fields and columns in Teradata databases. The solution also offers NIST-approved format-preserving encryption (FPE) capabilities, so teams can encrypt sensitive records without altering their format or field schemas. Not only does this minimize the potential impact of encryption on associated applications and workflows, but it helps avoid the increased storage requirements associated with conventional encryption approaches. Through leveraging this approach, organizations can improve their security posture without compromising the value of big data analytics.

Streamline Encryption Deployment and Usage

The solution reduces complexity for developers by offering documented, standards-based application programming interfaces (APIs) and user-defined functions (UDFs) that can be employed to perform cryptographic and key management operations. With the solution, Teradata users can set up their own easily configurable profiles for submitting encryption and decryption requests, including choosing from standard AES encryption and FPE.

WHY IBM SECURITY SOLUTIONS?

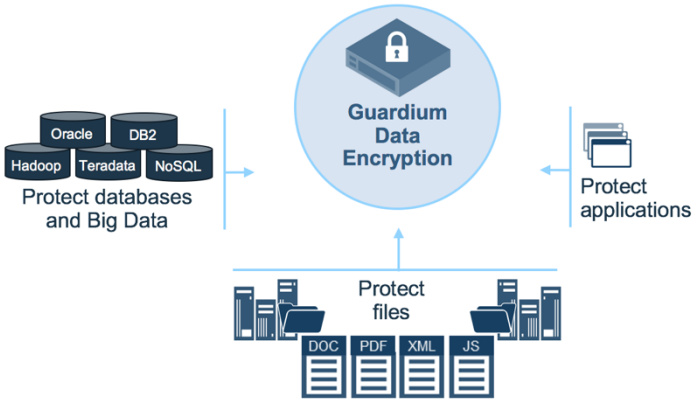
IBM Security solutions, including encryption solutions for heterogeneous environments, are trusted by organizations worldwide for advanced data protection. Proven IBM Security technologies enable organizations to safeguard their most critical resources. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions.

Leveraging the IBM Security Guardium Data Encryption suite, organizations can take a modular approach to encryption in which they select the specific capabilities they need including encryption for files and databases with or without live data transformation, Teradata encryption, application encryption, and tokenization, all centrally managed through the GDE Data Security Manager console.

IBM offers decades of leadership with encryption as part of an overall security environment, and with this technology can help protect your intellectual property. The IBM Data Security portfolio can help prevent cybercriminals from accessing and abusing your sensitive data, reduce the chances that compromised data can cause material harm, help your organization achieve compliance with regulatory mandates, and provide a modular approach for dealing with changes to the regulatory environment.

IBM has worldwide security expertise in some of the most highly regulated industries, including government, healthcare, transportation, energy production and financial services. IBM is trusted by companies of all sizes to secure today's data environments as well as plan for the future.

As a strategic partner, IBM empowers organizations to reduce security vulnerabilities and manage risk across the most complex IT environments. With proven, standards-based technologies, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions.



The IBM Security Guardium Data Encryption Suite enables organizations to encrypt data across a wide variety of environments and data sources, including databases, files, big data repositories, and applications.

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/guardium-file-and-database-encryption

IBM Security
75 Binney St
Cambridge, MA 02142

Produced in the United States of America
July 2018