Guardium Data Encryption

As security breaches continue with alarming regularity and regulations become increasingly stringent, your organization needs to extend data protection controls across the hybrid multicloud environment. IBM Security Guardium Data Encryption (GDE) offers a unified and modular set of encryption solutions built on a common, extensible infrastructure with centralized key and policy management. It is designed to help reduce administrative effort through an intuitive web-based interface.

Guardium Data Encryption can help protect assets residing in cloud, virtual, big data, and physical environments, offering capabilities to encrypt and control access to files, databases, and applications. You can define policies to outline which users or groups have certain privileges and manage encryption keys separately from the data.

GDE enables organizations to safely secure their cloud migration. With advanced multicloud Bring Your Own Encryption (BYOE) solutions, as well as centralized, independent encryption key management, you can avoid cloud vendor encryption lock-in and enable data mobility to efficiently secure data across multiple cloud vendors. Consistent policy enforcement can be extended from on-premises to the cloud. And for added security, GDE can work with your existing security infrastructure by integrating with on-premise or cloud hardware security modules (HSMs) to ensure unified data protection.

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

Highlights

- Granular data protection with centralized key and policy management
- Consistent security and compliance support across hybrid multicloud environments
- Compatible with your existing security tools including supported HSMs and 3rd party sources for encryption keys

Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), and other regional data protection and privacy laws. Obscure data-at-rest with format-preserving tokenization and use dynamic data masking to protect data-in-use. GDE helps address compliance with strong data encryption, robust user access policies, data access audit logging, and key management capabilities.

Whether the data is stored in the cloud or on-premises, GDE equips organizations with powerful tools to help combat external and internal threats and establish persistent controls.

Guardium Data Encryption portfolio components

CipherTrust Manager (formerly Data Security Manager or DSM)

Guardium Data Encryption is comprised of a suite of integrated products that are all administered via a common management server known as CipherTrust Manager or CM. It is the central management point, providing key and data access policy management across the hybrid multicloud enterprise, and is available as a virtual appliance.

CM simplifies key lifecycle management including activities such as generation, backup and restore, deactivation, and deletion. Role-based access to keys and policies, multi-tenancy support, and robust auditing and reporting of key usage and operational changes are core features of the console.

Additional key features include:

- Self-service licensing, streamlining connector license provisioning and ongoing management
- Secrets management, providing the ability to create and manage secret and opaque objects

- Multi-tenancy provides capabilities required to create multiple domains with separation of duties
- REST APIs to automate repetitive tasks
- Robust auditing and reporting, including tracking key state changes, administrator access, and policy changes
- Easy integration with existing security authentication

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 cloud storage services such as Amazon S3. Policies can be applied by users and groups from systems, LDAP/Active Directory, and Hadoop, and you can enable controls by parameters such as process, file type, and others. Access policies can be defined to create a permitted list of “trusted” applications to prevent any untrusted binaries (e.g., ransomware) from accessing data stores.

Guardium for File and Database Encryption can be used in physical, virtual, cloud, and big data environments – regardless of the underlying storage technology. Deployment requires no changes to applications, user workflows, business practices, or operational procedures. Agents can run at the file system or volume level on a server, and is available for Microsoft Windows Server, many variants of Linux, and IBM AIX operating systems. SAP HANA and Teradata file systems are also supported. Your administrators will perform all policy and key administration through CipherTrust Manager.

Live Data Transformation: Live Data Transformation is an addition for Guardium for File and Database Encryption that enables encryption and rekeying with unprecedented uptime and administrative efficiency during initial encryption or subsequent maintenance. 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. Security best practices and regulatory mandates require periodic key rotation, and Live Data Transformation addresses this through online key rotation and data rekeying. It also supports faster backup and archive recovery.

Guardium for Container Data Encryption: This extension to Guardium for File and Database Encryption delivers container-aware data protection and encryption capabilities for granular data access controls and data access logging in containerized environments (e.g., Docker and OpenShift hosts and images). 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. It secures container volumes, protects against root, privileged, or unauthorized user access within containers, as well as 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.

Guardium for Tokenization

Guardium for Tokenization provides application-level tokenization and dynamic display security. It secures and anonymizes sensitive assets — whether they reside in the data center, big data environments, or the cloud. Tokenization protects data-at-rest while the policy-based dynamic data masking capability protects data-in-use. A RESTful API in combination with centralized management and services enables tokenization with a single line of code per field.

Tokenization is provided by dedicated, distributed-cluster-capable Tokenization Servers, offering full separation of duties. Tokenization

management and configuration are available through an operational dashboard with convenient workflows.

Dynamic data masking policies define whether a tokenized field is returned fully or partially masked based on user identification controlled by an AD or LDAP server. For example, the policies could enable customer service representatives to see only the last four digits of credit card numbers, while account receivables staff could access the full credit card number.

Format preserving tokenization protects sensitive data without changing the database schema. Guardium for Tokenization requires minimal software engineering, leveraging standard protocols and environment bindings. It can be deployed as an appliance in your virtual format of choice.

Guardium for Application Encryption

Guardium for Application Encryption offers DevSecOps-friendly software tools for application-level encryption of sensitive data. The solution is flexible enough to encrypt nearly any type of data passing through an application. Protecting data at the application layer can provide the highest level of security, as it can take place immediately upon data creation or first processing and can remain encrypted regardless of the state – during transfer, use, backup, or copy.

Development flexibility is delivered with REST, C, .Net Core, Net, and Java cryptographic libraries to enable creation of crypto applications for the widest range of programming skills.

Operational flexibility is twofold. First, a broad range of cryptographic providers are available including native C, PKCS#11, the Cryptographic Service Provider (CSP) and Crypto Next Generation (CNG) Providers for Windows, and the Java Crypto Engine (JCE). Second, encryption operational flexibility is delivered by the choice to

encrypt locally or on CipherTrust Manager, without changing any code. The choice is implemented with a simple configuration change. Supported environments include Windows, Linux, AIX, Teradata, and others, including all major cloud platforms.

Guardium for Batch Data Transformation

Guardium for Batch Data Transformation provides static data-masking, which transforms selected data to unreadable forms in order to utilize data sets while preventing misuse of sensitive data. As an addition to Guardium for Tokenization and Guardium for Application Encryption, Batch Data Transformation protects vast quantities of data quickly. Use cases include masking data in preparation for sharing with third parties, development, QA, R&D, as well as before adding a data set to a big data environment, preparing data for safe cloud migration, and others.

Guardium for Cloud Key Management

For organizations to safely store sensitive data in the cloud, Guardium for Cloud Key Management offers advanced multicloud centralized and independent encryption key management. It supports Bring Your Own Key (BYOK) lifecycle management for many Infrastructure-, Platform- and Software-as-a-Service cloud providers, who offer data-at-rest encryption capabilities. Many data protection best practices indicate that encryption keys be managed remote from the cloud service provider. 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. You can gain higher IT efficiency by leveraging automated key rotation and expiration management. With BYOK API’s, Guardium reduces key management complexity and operational costs with full lifecycle control of encryption keys and centralized management and visibility.

Achieve additional IT efficiency with centralized access to each cloud provider from a single browser window, management of native cloud keys, and automated synchronization that ensures that cloud console operations are centrally visible. Key activity logs and prepackaged reports enable faster compliance reporting, and logs may be directed to multiple syslog servers or SIEM systems.

Guardium Cloud Key Management is available as a standalone virtual appliance. CipherTrust Manager provides secure key generation, and for additional layers of security, supported HSMs such as IBM Cloud Hyper Protect Crypto Services, can offer key generation security and storage.

Guardium for Data Encryption Key Management

Guardium for Data Encryption Key Management centralizes key management for Guardium Data Encryption solutions as well as 3rd party devices, databases, cloud services, and applications. It supports KMIP – an industry-standard protocol for encryption key exchange between clients (appliances and applications) and a server (key store). Standardization facilitates external key management for storage solutions including SAN and NAS storage arrays, self-encrypting drives, and hyper-converged infrastructure solutions. KMIP simplifies the requirement of separating keys from the data being encrypted, allowing those keys to be managed with a common set of policies. Guardium operates in the KMIP server role for a broad range of third party applications and devices acting in the KMIP client role, which can include third parties such as Microsoft SQL TDE and Oracle TDE.

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 IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

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

For more information

To learn more about IBM Security Guardium Data Encryption, please contact your IBM representative or IBM Business Partner, or visit the following website: https://www.ibm.com/products/guardium-data-encryption