Protect mainframe data with encryption and access controls

Safeguard data with IBM Guardium Data Encryption for Db2 and IMS Databases

Highlights

- Provide segregation of duties and access controls to meet data privacy regulatory compliance
- Ensure data privacy throughout database processing to ensure that clear text results are presented only to authorized users
- Retain encryption when database is backed up, loaded into memory buffers, or written out to database and systems logs
- Achieve granular encryption in IBM® Db2® for z/OS® and IBM IMS™ databases for fine-tuned access controls and optimized performance
- Utilize IBM Z® cryptographic hardware and key management to protect data on Db2 and IMS databases

Businesses and governments alike are experiencing an alarming rate of malicious activity from both external and internal actors. Usually, bad actors hack into systems (or trigger an internal data breach) because they want to steal, modify or delete sensitive data—whether customer data, healthcare information, proprietary business plans, top-secret algorithms or something else.

So long as attackers seek inroads to data, security and privacy will continue to be vital issues—and if dangers are left unaddressed, they will stand in the way of business innovation, putting enterprise-critical data at risk of exposure, and companies at risk of liability.

Strong perimeter security is a necessary protective step to help stop intruders from reaching crucial systems, but sensitive data itself must also be protected for compliance and security purposes. Perimeter security provides extremely limited data control, and as the threat of security breaches—from external attacks as well as from insider threats—continues to grow, sensitive data has become ever more vulnerable to compromise.

Mainframe environments in particular have become increasingly desirable targets for data thieves, who know that enterprises have trusted mainframes with their most vital data. Many mainframe-equipped businesses

are leveraging mobile initiatives, big data initiatives, social initiatives and more to drive their businesses forward. This can mean exposing mainframe-hosted data over the network to new vulnerabilities and new endpoints, from ATMs to mobile devices and even browsers.

Meeting mainframe challenges with encryption

For many enterprises, nearly 80 percent of all active code still runs on the mainframe, and 80 percent of enterprise data also is housed on the mainframe—much of it containing customers' sensitive personal data. Further, some security challenges are specific to the mainframe:

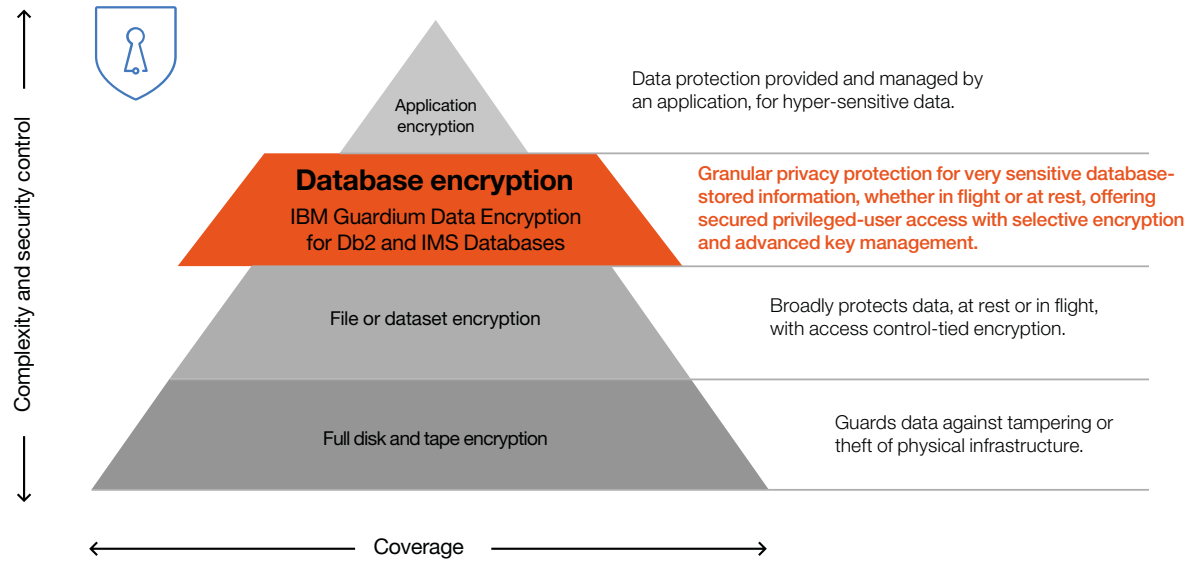
- Mainframe security administration is typically managed by privileged system programmers, and mainframe IT management is often siloed and independent of other enterprise operations, limiting security, compliance and ownership visibility
- The mainframe contains the most critical elements of many large business services, making security threats even greater risks
- Inconsistent security enforcement and management controls can give mainframe data uneven protection or incomplete access records

Regardless of the type of environment—distributed or mainframe—it's crucial to protect the sensitive data itself when it comes to defending against data breaches—and data encryption is an excellent, efficient means to protect data. Encryption works most effectively if it is part of a comprehensive, pervasive encryption strategy that includes the ability to protect sensitive data inside databases. To gain maximum benefit from encryption, security-conscious enterprises employ intelligent encryption protocols, employing access controls that ensure that data is decrypted only in results presented to authorized users, such as to a customer making a bank account balance inquiry or a human resources manager accessing sensitive employment details. To help secure the entirety of a mainframe environment, it is crucial to address the risks to mission-critical mainframe databases. IBM Guardium® Data Encryption for Db2 and IMS Databases helps protect sensitive enterprise data on IBM z/OS while supporting efficiency and performance.

Guardium Data Encryption for Db2 and IMS Databases provides granular database encryption, honors existing fine-grained access controls on the mainframe and database, and supports a range of keys available on z/OS. It can use available IBM Z cryptographic facilities and hardware to protect sensitive data.

Compliance as a driver for mainframe encryption

Along with the skyrocketing incidence of data exposures (malicious or unintentional) comes heightened efforts from legislators and regulators to safeguard sensitive enterprise data. Numerous regulations now require executive officers to ensure the privacy, protection and confidentiality of electronically stored data. These directives include the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the European Union's General Data Protection Regulation (GDPR), and a multitude of other breach-notification laws, as well as industry standards such as the Payment Card Industry Data Security Standard (PCI DSS). Many specify data encryption as a requirement or best practice. Guardium Data Encryption for IBM Db2 and IMS Databases is designed to help organizations comply with those regulations and legislative acts, and to help ensure that private and confidential data is secure.



IBM Security Guardium Data Encryption for Db2 and IMS Databases is part of a comprehensive, layered approach to data encryption—pervasive encryption—helping organizations secure the privacy of sensitive database content in IBM Z mainframe environments.

Maintaining security even for data in use and in transit

Standard methods of encryption are no longer enough to protect against viewing of sensitive data by unauthorized users. Full-disk encryption provides protection against someone making a copy of the disk, or someone removing the disk altogether. File encryption is good protection against bad actors who make a copy of the file and see the sensitive data without authorization. However, neither of these approaches protects against unauthorized access once the sensitive data is loading into an application or the database for processing and stored in system memory. Any database administrator or other privileged user will be able to view database records—including sensitive data—during database processing. Guardium Data Encryption for Db2 and IMS Databases can help guard against unauthorized access by maintaining encryption of the sensitive data throughout database processing, including for data stored in memory and data written out to system logs or backups. Even at this stage, customers can further protect the sensitive data by using encrypted communications, such as HTTPS or TLS, to secure the sensitive data during transmission.

Advanced data encryption and decryption capabilities

To help reduce the risk to sensitive data in mainframe environments, Guardium Data Encryption for Db2 and IMS Databases provides advanced encryption and decryption.

These capabilities are made possible by the Advanced Encryption Standard (AES) algorithm, in addition to Triple Data Encryption Algorithm (TDEA), and ANSI Data Encryption Algorithm. The IBM solution provides encryption routines that are transparent to applications accessing the databases, so they require no costly application development.

To continue to get value from your encrypted sensitive data, you must be able to decrypt that data on demand. To meet this need, Guardium Data Encryption for Db2 and IMS Databases uses Db2 edit routines and IMS exit routines to encrypt only the sensitive data you are concerned about protecting. This provides fine-grained access controls and optimizes for performance. You can choose to encrypt sensitive data fields, rows, columns and tables to ensure that data privacy is protected while maintaining performance.

Guardium Data Encryption for Db2 and IMS Databases uses IBM Z cryptographic hardware that is Federal Information Processing Standard (FIPS) 140-2 compliant along with Integrated Cryptographic Service Facility (ICSF) capabilities to support robust encryption. Key management is essential to ensure data access protection, and Guardium Data Encryption for Db2 and IMS Databases supports a range of encryption methods to support your needs.

A multi-layered data-centric defense

Organizations often focus their security efforts on the edges of their data holdings, watching their network perimeter for malware, unauthorized access or anomalous data transfers. Because sensitive information stored in mainframe environments often constitutes the "crown jewels" of an organization's data, though, protecting that mainframe data is an equally important component of a comprehensive, multi-layered approach to security. And because the same data may exist in more than one place (because of backups and in-memory or cached copies) that same information can be vulnerable at different points in its lifecycle—or even to different threats at the same time.

Employing pervasive encryption—a capability built into IBM Z to protect databases as well as other data whenever possible—and utilizing real-time activity monitoring are two of the strongest methods for ensuring that mainframe data remains accessible only to authorized, accountable users, even if an attacker penetrates an organization's firewall or strikes from within.

Protects against internal and external threats

Organizations face a multitude of rapidly evolving threats to sensitive and private data. Guardium Data Encryption for Db2 and IMS Databases is designed to protect against not only unauthorized attempts to view sensitive data, but also attacks on the database operating environment that could lead to a compromise of sensitive data.

To help protect against internal and external threats, Guardium Data Encryption for Db2 and IMS Databases integrates the following data security features:

- Persistent and granular database encryption, not only for data at rest but also in in-memory buffers, in logs and even in dumps
- Access controls to enforce segregation of duties
- Encryption policies to help meet data privacy regulations
- Flexible key management options available from z/OS
- ICSF hardware assistance
- Encryption for database backups

These features help organizations enforce policy-based data security rules to satisfy data privacy mandates and other compliance needs.

IBM Guardium Data Encryption for Db2 and IMS Databases	
Data at-rest encryption	✓
Data in-memory encryption	✓
Supports IBM Db2 and IBM IMS	✓
Transparent to applications	✓
Fine grained control of encryption	✓
Segregation of duties	✓
Protects data in logs	✓
Protects data in memory dumps	✓

IBM Security Guardium Data Encryption for Db2 and IMS Databases provides comprehensive control and integration features that are tuned to the needs of today's enterprise security teams

Guardium Data Encryption for Db2 and IMS Databases: At a glance

Guardium Data Encryption for Db2 and IMS Databases provides the following key features:

- Advanced data encryption and decryption, for data security and privacy as well as to support low system overhead
- Interactive System Productivity Facility (ISPF) front-end and exit drivers, for optimizing efficiency, encryption, and compression capabilities
- Application transparency, without requiring costly application modifications
- Segregation of duties, allowing only authorized users to see decrypted sensitive data
- *IBM Resource Access Control Facility* (IBM RACF®) and Db2 fine-grained access control, to limit access to sensitive data
- Sensitive data encryption at the Db2 table level and at the IMS segment level, to support performance and contribute to low system overhead
- Data-in-use protection for in-memory buffers
- "Clear text" data protection, preventing unauthorized access even with DBMS access methods; clear text protection also for in-memory buffers, logs and dumps

Database transaction log encryption, image copy datasets encryption and direct-access storage device (DASD) volume backup encryption.

Why IBM?

IBM offers an industry-leading mix of experience and capabilities that come together in Guardium Data Encryption for Db2 and IMS Databases. This solution helps deepen security for mainframe-hosted data held in Db2 for z/OS and IMS databases. It represents valuable real-world expertise in IBM Z mainframe technology and decades of IBM experience in data storage, database technology, enterprise security and encryption.

For more information

To learn more about IBM Guardium Data Encryption for Db2 and IMS Databases, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/guardium-data-encryption-for-z/OS

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2017

WGS03116-USEN-00