IBM InfoSphere Guardium Data Encryption

Protect sensitive data against theft, misuse and exposure

Highlights

- Protects structured and unstructured data at rest
- Deploys easily and operates transparently to the network, storage or applications
- Provides database file- and tablespace-level encryption without affecting database structure and schema; operates transparently to the DBMS and other applications
- Enforces strong separation of duties
- Provides a unified policy and key management system to centralize and simplify data security management from a single database to multiple databases

Secures and protects data

Global enterprises and governments alike are experiencing an alarming rate of malicious activity from both external and internal sources directed at sensitive data such as corporate financials, credit card transactions, medical records, intellectual property, and private consumer and employee information.

Different types of information have different protection and privacy requirements. Therefore, organizations must take a holistic approach to protecting and securing their business-critical information:

- **Discover where the data exists:** You can't protect sensitive data unless you know where it resides across your enterprise and how it's related.
- **Safeguard sensitive data, both structured and unstructured:** Structured data contained in databases must be protected from unauthorized access. File-level data encryption helps make this information unusable or unviewable except by those with specific rights. Unstructured data in documents and forms requires encryption to protect against malicious use, and privacy policies to redact (remove) sensitive information while still allowing needed business data to be shared.
- **Protect nonproduction environments:** Data in nonproduction, training and quality assurance environments needs to be protected so that sensitive information is not revealed inadvertently, yet it must still be in usable form during the application development, testing and training processes.
- **Secure and continuously monitor access to the data:** Enterprise databases require real-time insight to help ensure data access is protected and audited. Policy-based controls are required to rapidly detect unauthorized or suspicious activity and alert key personnel.

IBM® InfoSphere® Guardium® Data Encryption is a key piece of this holistic strategy and the focus of this document. It is designed to help organizations safeguard structured data and unstructured data in file systems.

Encrypts without enterprise changes

InfoSphere Guardium Data Encryption can be quickly deployed to secure data, yet requires no changes to applications, the underlying database or hardware infrastructure. This approach enables enterprises to meet data governance requirements without disrupting the enterprise.

Secures and encrypts database files

InfoSphere Guardium Data Encryption can also protect database files by encrypting and controlling access to those files. InfoSphere Guardium Data Encryption helps ensure that sensitive data is protected against privileged IT staff with a significant amount of system access.

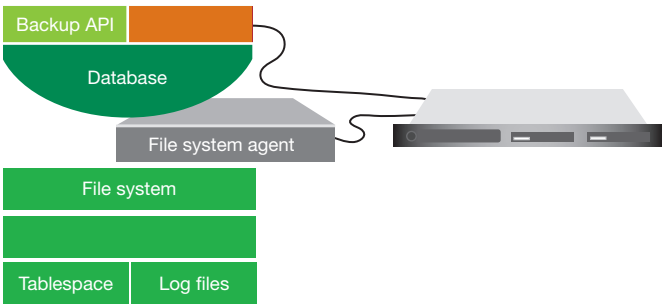

Figure 1: InfoSphere Guardium Data Encryption provides database file- and tablespace-level encryption without affecting database structure and schema.

Secures and encrypts unstructured documents

InfoSphere Guardium Data Encryption can automatically encrypt any sensitive file, anywhere in the distributed enterprise. Patented encryption technology keeps sensitive data encrypted while enabling system administrators to perform their duties. High-performance file-based encryption supports the business process, and granular auditing of data access policies supports monitoring and regulatory compliance initiatives.

Helps support compliance

Along with the skyrocketing rate of data exposure comes heightened activity from legislators and regulators to safeguard sensitive enterprise data. A number of regulations now require executive officers to ensure the privacy and confidentiality of electronically stored data. These directives include the Health Insurance Portability and Accountability Act (HIPAA), PCI Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act (GLBA), the European Union Data Protection Directive, Korea's Personal Information Protection Act and the multitude of state breach notification laws. Many specify data encryption as a requirement or best practice.

InfoSphere Guardium Data Encryption is designed to help organizations comply with those regulations and legislative acts to help ensure that private and confidential data is secure. Data encryption can also enable safe harbor provisions.

Protects against internal and external threats

Organizations must contend with a multitude of rapidly evolving threats to sensitive and private data. InfoSphere Guardium Data Encryption is designed to protect against external hackers as well as internal threats such as malicious or accidental abuse of privileged accounts.

The threat matrix below illustrates common data security threats and the corresponding countermeasures provided by InfoSphere Guardium Data Encryption:

Threat	Encryption	Host access control	Audit and forensics
Root/system user	x	x	x
Direct access to file	x	x	x
Unauthorized viewing/log file tampering	x	x	x
Stolen/lost media	x		
Access by unauthorized application		x	x

InfoSphere Guardium Data Encryption integrates the following data security controls:

1. Access control to data by user and application
2. Security for the database operating environment
3. Secure and proven key management
4. Audit accesses to protected data
5. Encryption of files, such as configuration, log and backup files

Those controls help organizations enforce policy-based data security rules that satisfy data privacy-based compliance needs.

Capabilities include:

- **High-performance encryption**—Performs encryption and decryption operations with minimal impact to database and application performance
- **Context-aware access control**—Helps ensure that only authorized applications and processes can access protected data, and supports established data classification and acceptable use policies
- **Strong separation of duties**—Supports separate database management system (DBMS) and security administration

About IBM InfoSphere

InfoSphere Guardium is a key part of the IBM InfoSphere portfolio. InfoSphere software is an integrated platform for defining, integrating, protecting and managing trusted information across your systems. The InfoSphere platform provides the foundational building blocks of trusted information, including data integration, data warehousing, master data management and information governance, all integrated around a core of shared metadata and models. The portfolio is modular, allowing you to start anywhere and mix and match InfoSphere software building blocks with components from other vendors, or choose to deploy multiple building blocks together for increased acceleration and value. The InfoSphere platform offers an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster.

For more information

To learn more about IBM InfoSphere, contact your IBM sales representative or visit: **ibm.com**/software/data/infosphere

To learn more about IBM InfoSphere Guardium Data Encryption, contact your IBM sales representative or visit: **ibm.com**/software/data/optim/database-encryption-expert

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
January 2012

Please Recycle

IMD11887-USEN-03