# The Role of Database Encryption in Enterprise **Security**

## Why data at rest is data at risk

Today, the majority of data security measures — such as firewalls and intrusion detection systems — focus on data in transit. But most data remains at rest in databases for more than 90% of its life. Hackers know this, so when they probe and monitor networks it is not to intercept proprietary application data, but rather to steal passwords and other information that will allow them to breach the servers and systems containing the data stores. In fact, it is possible for hackers to exploit application bugs and configuration errors, intercept user passwords, or gain administrative rights to operating systems without ever compromising a single firewall. But no matter what method hackers use to penetrate others' data stores, the results are usually the same: disastrous.

## Where current security falls short

Most companies currently protect data using a combination of perimeter security and access controls. These measures attempt to keep unauthorized users from accessing data. They are part of what is commonly referred to as a "defense in depth" or "layered security" approach. These measures include:

- Firewalls, which are designed to prevent unauthorized access to the network. Unfortunately, firewalls cannot protect against malicious access to data by authorized (internal/employee) or seemingly authorized (spoofed) users.
- Intrusion detection, which offers notification of a breach, but no prevention.
- OS hardening, which restricts access to the operating system to prevent exploitation. While hardening protects against root attack, it does nothing for misuse of authorized access.
- Access control and authentication at the application, network, database, and/or operating systems level. This can be difficult to maintain in large organizations, and may not provide adequate compliance with domestic and international data-sharing and privacy requirements.
- DBMS security features, such as SSL, LDAP or enhanced authorization, which mask data in transit but do not secure the data at rest in database tables.

***These outward facing security measures fall short in several areas:***

- They do not prevent DBAs from accessing the database or the data residing within it.
- They do not provide data-level encryption, leaving data vulnerable to physical theft (of laptops, disk drives or backup tapes) or users with root access to the system.
- Their auditing facilities, if present, cannot catch authorized users who alter and delete log files to cover their tracks.
- They do not restrict data sharing or enforce data separation and separation of duties at the administrator level.

## The smart approach to data encryption

Data encryption is the only way to absolutely protect sensitive data, eliminate potential data sharing issues, ensure that privacy is maintained, minimize the potential for identity theft and ultimately meet data-privacy compliance requirements. There are three basic approaches to encryption of stored data:

1. The entire database can be encrypted: There are two problems with this approach. First, it allows anyone with access to the database to decrypt all data stored therein. Second, it exacts a substantial performance penalty because all requests — whether for sensitive data or not — require data to be decrypted and re-encrypted.

2. Individual database applications can be modified to encrypt sensitive data. This requires the use of crypto "toolkits" to reengineer in-house applications, a costly and inflexible application-by-application proposition that does not offer a scalable and uniform approach to data privacy. In addition, this approach does not provide essential key-management functions and may actually increase the number of people requiring access to databases for development and maintenance purposes.

3. Security middleware can be installed. This is the integrated **Secure.Data**™ approach, developed in close cooperation with the leading database providers for tight interoperability with database systems. The Secure.Data solution selectively targets only the sensitive information residing in databases, limits access to those who are specifically authorized to see the data and minimizes encryption/decryption overhead. The Secure.Data solution is transparent to most applications, so customization and hard coding are not required. In addition, Secure.Data gives organizations the flexibility to adjust or change data-privacy policies and protection parameters as needed, without changing their applications. Security policies and access rights can even be configured in real-time.

Secure.Data represents the most flexible, quickly deployed and cost-effective approach to enterprise data protection and privacy enforcement. With strong security controls and robust key management, Secure.Data provides organizations with a single, uniform approach to data privacy without additional application development and maintenance. Plus, total cost of ownership for a Secure.Data solution is far lower than application-by-application development.

## Benefits of Secure.Data

- Fast deployment and low maintenance via middleware design
- Strong, granular column-level encryption of data at rest
- Enhanced role-based and workgroup-based access controls
- Comprehensive key-management facilities
- Enforced separation of duties between database and security administrators (dual control)
- Secure audit and reporting capabilities
- Robust database and security compatibility and interoperability

protegrity

**Protegrity, Inc.**
1177 Summer Street
Stamford, CT 06905 USA
solutions@protegrity.com
www.protegrity.com

**Eastern United States**
+ 1.888.776.8347
**Western United States**
+ 1.408.366.0417
**Canada**
+ 1.416.693.7233
**Europe**
+ 46.31.755.2520