

COLUMN-LEVEL DATABASE ENCRYPTION SECURED BY nCIPHER

SecureDB is a database security solution that delivers column-level encryption of data at rest. It provides a simple and cost-effective deployment option, requiring minimal integration at the application level, while delivering granular access control.

Column-level encryption selectively protects the most sensitive information within the database, not only securing against external attack, but also protecting the database from legitimate database users attempting to access restricted records. This ensures a robust separation of duty between administration and security functions.

DATA AT RISK

Most companies rely upon cryptographic security controls to protect data as it passes over IP networks. However, they often depend solely on physical security controls to protect the data where it is stored for 99% of the time. Hackers regularly penetrate perimeter defences and focus their efforts where sensitive information is most concentrated; the place where an attack would have the most devastating effect – the database. Credit card numbers, social security numbers, health records, HR records, trade secrets, proprietary source code and other sensitive information often lie virtually unprotected in databases.

However, risk management is not the only reason behind a reassessment of database security; increasingly privacy and compliance regulations such as HIPAA (Health Insurance Portability and Accountability Act) and the Gramm-Leach-Bliley Act (GLBA, public law 106-102) are driving organisations to deploy robust database controls.

THE CHALLENGE OF DATABASE SECURITY

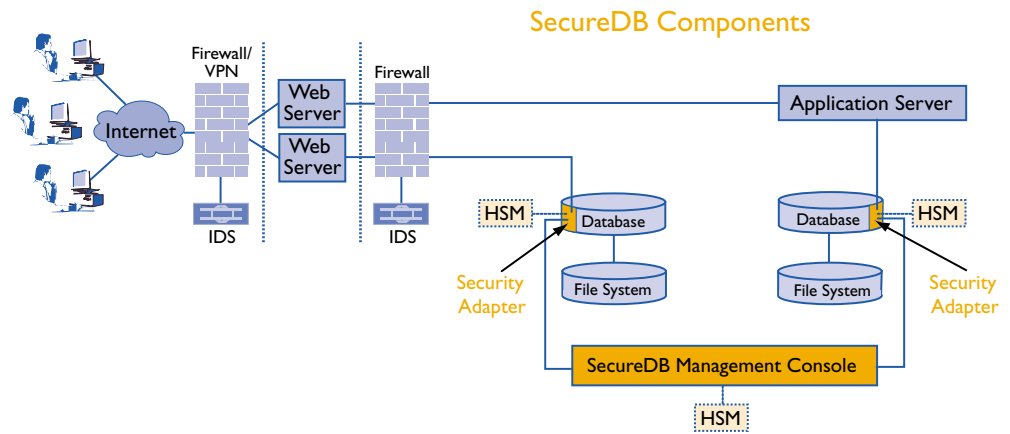
At first glance the obvious solution is simply to protect against the theft of files. However, encrypting data at the file level is an all-or-nothing solution; it provides no additional security to the database itself. Anyone with rights to access the database will then be able to view all the information within that database. This creates a security risk, giving super-users unlimited access with no separation of security management and database management.

Alternatively data can be encrypted by the application before it's stored in the database. With this approach, database queries return encrypted data for decryption by the application. While this approach provides for role-based security policies and provides end-to-end security, it also demands significant application-level modifications. This can be a major barrier for organisations that deploy multiple applications that may span databases from several vendors.

COLUMN-LEVEL DATABASE ENCRYPTION

SecureDB addresses the traditional challenges of database encryption without necessitating complex application-layer or database modifications. SecureDB combines multiple levels of authentication for role-based users to provide fine-grained control over the encryption and decryption of data elements. This level of control delivers separation of duty, ensuring there are no super-users. Even system administrators and security personnel can be prevented from viewing unauthorized data.

By selectively protecting the most sensitive data, robust security can be deployed without burdening the entire database or impacting the wider business process. Used in conjunction with SSL, SecureDB can ensure that data is encrypted at each stage, protecting the channels between Web server, application server and database, without the need for costly application-level customization. Optionally, nCipher Hardware Security Modules can be deployed to strengthen the key management facilities through the use of tamper-resistant, FIPS 140 validated cryptographic hardware.



SecureDB Overview and Architecture

SecureDB consists of a centralized Management Console and lightweight database Security Adapters installed on each database server. The system architecture is designed to manage multiple database types, ensuring that your investment in database security for one database vendor is leveraged to achieve the same level of security for another database type. New databases can be included simply by remotely adding a new adapter for each new database server and updating the centralized Management Console.

SecureDB Security Adapters

SecureDB Security Adapters are lightweight processes for particular databases and are deployed from the remote SecureDB Management Console. The Adapter performs local encryption and decryption of data on demand as authorized users access protected database records. Requests to access unencrypted fields pass transparently through the Adapter ensuring that there is minimal performance impact.

SecureDB Management Console

The SecureDB Management Console offers a centralized deployment, management, debug and extensibility platform and is the core of the solution. Each SecureDB Security Adapter can be configured for a specific database type and remotely deployed into the target database from the Management Console. Administrator access rights, role-based security privileges and the configuration of each SecureDB Security Adapter are controlled using an intuitive user interface.

Hardware Security Module Support

Any encryption-enabled database is only as secure as the security of the digital keys used to encrypt the database. SecureDB supports the deployment of nCipher's Hardware Security Modules (HSM) for robust key management. Management of the cryptographic keys inside the nCipher

SecureDB Components

nShield HSM delivers a significant improvement in the security, manageability and scalability of the software key hierarchy. Managing the keys in FIPS 140 validated cryptographic hardware allows for the secure generation, storage, disposal, archival and recovery of the key.

Security administration functions such as key back up and recovery are controlled through a set of administrator smart cards. This means responsibility can be split between multiple security officers, avoiding an over-reliance on a single individual. Two-factor authentication is also supported through the use of threshold sets of smart cards, where 'k of n' operator cards must be presented by security officers or administrators to authorize a specific function.

SYSTEM REQUIREMENTS

SecureDB Management Console:

- Operating Systems:
 - Windows NT
 - Windows 2000/XP
 - Windows 2003
- 20 MB free disk space
- Oracle Net8 Client (for Oracle Database only)
- nShield HSM support

SecureDB Security Adapter:

- Oracle:
 - Solaris
 - AIX
 - HPUX
 - Linux
 - Windows
- IBM DB2:
 - AIX
 - Linux
 - Windows
- Microsoft SQL Server