

# DREM™

## Data at Rest Encryption Module

*As demand for data security continues to increase, organizations are beginning to encrypt critical data inside corporate databases. Industry requirements and the emergence of laws and regulations requiring data protection mean that private information such as medical records, social security and customer credit-card numbers, payroll/benefits data, driver's license numbers and more need to be kept secure...*

### THE DREM SOLUTION

DREM offers an immediate solution that enables organizations to instantly gain the security benefits of encryption while avoiding a massive enhancement project. Developers and users can choose fields within individual files or entire files to be encrypted and decrypted without any programming help from jBASE International! DREM allows them to choose which users are allowed to see the decrypted data within a given file, no matter which tool is used to view that data.

With DREM your company will not lose customers (and lost customers means lost revenue) because of the inability to encrypt jBASE systems in a timely manner. DREM allows a system to be fully and comprehensively encrypted and compliant within hours. There is no programming required. There is no ongoing administration. The DREM methodology allows a company to encrypt their database without having their programs and dictionaries touched which saves them testing time, programming time, development time—all kinds of time!

And how do you encrypt an application if source code for some programs have been lost or destroyed? jBASE's data at rest encryption technology is also the solution to this quickly growing problem. Programs will not need to be recompiled, so the lack of source code is not an issue.

### DREM USES jBASE JEDI TECHNOLOGY

This unique jBASE innovation enables developers to achieve seamless integration with foreign databases and external functions. The published interface provides a common set of rules and syntax to access any database or data source. By means of specific jEDI drivers, jBASE BASIC I/O statements can access and manipulate any jBASE file as well as any other database such as Oracle, SQL Server and DB2 as simply as they can access standard jBASE files or other MV database files (UniVerse, UniData, D3, Cache etc). The encryption and decryption of data files is treated by jBASE as a normal read or write to the standard jPLUS (files greater than two gigabytes) or j4 files.

The jEDI system also provides a number of other useful generic facilities to the application developer, such as transaction boundary support across multiple databases and secondary indexing. The Transaction Journaling product uses the jEDI interface to log transactions to just about any device for any and all data sources. All work *seamlessly* with DREM.

In addition, the jEDI architecture is ideal for sites that require their investment in their application to be maintained while being able to work with DB2, Oracle or other RDBMS and use DREM encryption technology.

DREM functionality is only available in jBASE Release 4.1. For more information speak to your jBASE representative or visit [www.jbase.com](http://www.jbase.com)!

### KEY FEATURES OF DREM

**DREM is scalable.** The algorithms used by DREM include file compression of the encrypted files and the caching of frequently referenced large records. Although a small number of files may increase in size, other files get even smaller.

**DREM is flexible.** DREM offers automatic whole file or field encryption as defined by the user during installation. It also offers selective viewing of encrypted data on a file-by-file basis based on individual users or groups of users.

**DREM deploys quickly and easily.** In most case, the entire set of files that need to be encrypted can be converted within hours without changing any programs or dictionaries. Setting up the policies of which users can see which data within these files takes minutes once user permissions have been determined and the necessary user groups within the Unix or Windows environment have been created.

**DREM doesn't need the program source code to make it work.** This makes the DREM particularly appealing to companies that require encryption yet do not have or have lost the source code. The implementation of data at rest encryption has zero impact on application programming or the modification of dictionary items and deployment is easy.

**DREM does not require ongoing administration.** DREM will not increase administrative overhead. Once the file is encrypted and the access groups are assigned the project is complete.

**DREM doesn't require user intervention.** There is no need for a user to know anything about encryption. Company management can be secure in the knowledge that they are meeting standards that will pass audit requirements.

**DREM is Developer friendly.** There is no need for a developer to understand the encryption process. All the developer needs to know is the fields and/or the files that require encryption and to create those files with the CREATE-EFILE verb.

**DREM allows for individual and/or group designated users.** Companies can choose which users see the decrypted data on a file-by-file basis.

**DREM is value priced.** End users, just compare the cost of changing all programs and dictionary items, delayed new projects, and the use of outside consultants with the competitive price of DREM!



**For more information, visit [www.jbase.com](http://www.jbase.com)!**