MENTIS
SENSITIVE DATA LIFECYCLE MANAGEMENT™

iScramble

Context Sensitive Masking for Non-production Databases

iScramble is the only enterprise-class, full-security data scrambling product that maintains complete functionality in non-production databases. Also a cost-effective solution for compliance, it provides safeguards that encryption cannot - and without the performance load.

Common Security Risk.

Non-production (or "cloned") databases contain all of the sensitive data that was in the production database at the time of their creation. Since clones are used in secondary functions — such as test, development, research, training, and so forth — they are not perceived as sharing or maintaining valuable information.

Savvy hackers and opportunistic insiders understand and exploit such vulnerabilities. Sheer chance can also expose this information to unknown sources.

Protection for clones is a major gap in most overall IT security strategies. iScramble covers that gap.

Sensitive Data from Production Databases is Often Overlooked When Cloned.

- Personally Identifiable Information (PII)
- Credit Card Numbers
- Pricing, Customer & Supplier Information
- Salary & Benefits

- Social Security Numbers
- Marital Status
- Address & Telephone
- Bank Routing Numbers

- Medical Records
- Payroll Account Numbers
- Tax ID
- Etc., Etc., Etc.

A New Approach.

Typically, security protections are employed at the network and application layers. iScramble protects your information assets at the most basic and critical level – the database where the information actually resides. It works by replacing sensitive data with similarly-constructed and meaningless values.

BEYOND ENCRYPTION: An iScrambled database has no performance degradation, needs no code or migration methodologies, and does not require the distribution of decryption keys.

MAINTAINED FUNCTIONALITY: iScrambled data maintains its functionality so your developers, programmers, and trainers can do their jobs. No coding or encryption is needed, as the data is meaningless to the intruder.

AUTOMATED INTELLIGENCE: The software uses sophisticated, context-sensitive, scrambling methods. iScramble intelligence automatically determines the information to be scrambled. It can be easily customized to your environment or industry. The iScramble process can either be initiated on demand, or as an automated part of the cloning process.

STRONG INTERNAL CONTROLS: iScramble has built-in best practices that address multiple levels of security. Also imbedded are unique data rules that comply with all legislative acts applicable to your industry. Your IT team has a quick catalogue of every area where sensitive information resides within the ERP framework, catching both the obvious and the most obscure piece of sensitive data. iScramble proactively fulfills certain IT audit requirements – with a little guidance from you.

iScramble Benefits

- Easily customized to industry or environment
- Quick catalog of every database area where PII resides
- Built-in data classification engine
- Low cost of ownership
- No need for encryption or decryption keys
- No performance degradation
- No need for change to your code or migration methodologies
- Maintains full database functionality
- Automatically determines information to be scrambled
- Initiated on demand or as an automated process
- Built in best practices
- Multiple levels of security

Efficient, Low-Cost Architecture. One Solution.

Combine iScramble with iMask, iMonitor, and iProtect to comprehensively protect both production and non-production enterprise databases Simple, easy-to-use interfaces allow collaboration between IT, Audit, Security, and Compliance groups within your organization, streamlining compliance, audit costs, and efforts.

iScramble uses the existing database technology stack; no additional software licensing is required. iScramble, iProtect, iMask, and iMonitor reside on a single server and are maintained via a shared administrative console with a common interface. All four products also share a common metadata, content authoring, and data classification engine. The engine resides on a unified framework using a single installation.

iSCRAMBLE Data Example

	BEFORE	AFTER
Name:	Jane Doe	John Gif
SSN:	345-00-9999	134-98-3719
Phone Number:	(212)-555-1212	(546)-213-4530
Salary	48000	37651
Date of Birth	3rd July, 1967	1st January, 1951
Address	12 Jane Street, New York, NY 10001	

A Comprehensive GRC Solution.

- **iProtect** ensures that only authentic users have access to your databases. iMask allows users to see only the data they need to do their job.

- Use **iMask** with **iScramble** to apply the same high-quality preventive controls to production and non-production databases.

- **iMonitor** provides continuous monitoring, which includes intrusion detection, attack termination, victim notification, and internal controls.

- Add **iDocument** to evaluate database-level access controls, including critical functions.

- Use **iCatalog** as a valuable step in compliance testing. iCatalog provides a quick, dynamic review of code written into application access objects (such as forms, reports, jsp, .net, etc.) before the code can expose sensitive data. Automate code migration from development to production.

- Maximize ROI and Audit readiness. Find out how your database security compares to industry standards and applicable legislation through an **S.O.S. (State of Security)** engagement.

- The **iAutomate** service creates entirely dynamic, custom applications for organizations whose labor intensive processes make compliance difficult, less cost-effective, or both.

"iScramble is the most comprehensive and cost-effective solution to a major loophole in the security architecture of databases that we have seen."

**Director of IT,
Leading Nutritional
Distribution Company**

Though 98 percent of U.S. companies use firewalls, more than 74 percent of U.S. corporate financial losses are from four main security sources:*

- Virus attacks
- Unauthorized access to networks
- Lost or stolen laptops, or mobile hardware
- Theft of proprietary information or intellectual property

*According to the 2006 study conducted by the Computer Security Institute (CSI) with the participation of the San Francisco FBI's Computer Intrusion Squad

Do You Know...

How many cloned production instances have been made?

Who has access to information in these databases?

How many current and former consultants & employees have access to them?

How many times these instances get copied, ftp'd, wired overseas, exposed to trainees... and by whom?

How confident your IT team is that breaches have not been made via any of these instances?

¿Quiere realizar una prueba gratuita del producto?