MENTIS

Data Minimization

iRetire™ Data Sheet

Reduce the risk of carrying inactive sensitive data

info@mentisinc.com

www.mentisinc.com

Reduce Compliance and Security Risk by Retiring Inactive Sensitive Data

Automate your data retention policy in enterprise systems.

iRetire™, the industry's first data retirement software, allows IT organizations to de-identify and tokenize aged, inactive data within a production environment, ensuring compliance and reducing risk.

iRetire™ enables organizations to "retire" non-current sensitive data within the IT environment without losing the value of that retired data. A complete integration with MENTIS suites for discovery, masking, and monitoring means intelligence from your security efforts is put to work for you across your security programs.

Sensitive Data Retirement

Every organization generates and captures sensitive data in its enterprise databases. Sensitive data may include personally identifiable information (PII) such as credit card information, social security numbers, and other sensitive data; and corporate sensitive data such as intellectual property, location codes, product formulas, negotiated contracts, etc.

Although reasons to retain sensitive data range from legal mandates to active use, a significant percentage of data housed in enterprise systems is not current. Retiring this non-current data from production systems allows organizations to minimize the risks associated with a potential breach.

A case for sensitive data retirement

44% Average percentage of employee records that are not current.

$221 Cost of sensitive data breach record.

$972 Cost in thousands for data breach related to non-current sensitive information.

10,000
EMPLOYEES

SOURCES:
Ponemon Institute.
The True Cost of Compliance Study (2015) Cost of a Data Breach Report (2015)

How Does iRetire Work?

iRetire™ allows an organization's IT department to construct data retirement policies based on the organization's specific parameters and data retention policies. Candidate data is then identified, allowing IT to review and approve the data flagged for retirement. Once approved, iRetire™ uses MENTIS' proprietary and patent-pending process to securely tokenize the sensitive data within the application and underlying database.

Even after the sensitive data within a record is retired, the valuable market, demographic, and operational data associated with the retired data remains intact and usable by the system of origin. Additionally, the retired data can be reinstated if deemed necessary. And when the time comes to archive or delete the records from the application, the token link to the **iRetire**™ repository is removed, and the data is permanently deleted from the underlying database.

iRetire™ by MENTIS

Our innovative approach ensures flexibility, integrity, and security.

Flexibility to define parameters based on corporate data retention policies

Integrity of application and underlying table structures

Security of sensitive information within application and iRetire repository

Analyst Recognition :

" Mentis innovates in securing sensitive data by offering the retirement of inactive sensitive data "

- Gartner

Why Retire Sensitive Data?

Compliance

- Payment Card Industry Data Security Standard (PCI DSS)
- UK Data Protection Act of 1998
- Family Education Rights and Privacy Act (FERPA)
- BASEL
- Right to be Forgotten
- Breach Notification Laws Security
- Intellectual Property
- Trade Secrets
- Credit card numbers
- Contracts
- Personally Identifiable Information (PII) Best Practices
- Sensitive Data Management
- Corporate Governance

About MENTIS

iMask™ is part of a complete enterprise sensitive data security software suite from MENTIS.

iDiscover™ finds ALL sensitive data locations and user access across all data sources. The templates from iDiscover™ are used by downstream applications for masking, monitoring and retirement across non-production, production and pre-production environments.

Non - Production

iDiscover™ Find ALL sensitive data across all sources and metadata based on data classifications and sophisticated search.

iScramble™ Static data masking that supports 54 different masking methods, with full referential integrity and high performance scrambling across heterogeneous databases and unstructured data.

iSubset™ Creates subsets of production data for masking.

Production

iDiscover™ Find ALL sensitive data across all sources and metadata based on data classifications and sophisticated search.	**iMask**™ Dynamic data masking for databases and applications with unique role based, conditional and location-aware masking.	**Monitor**™ For continuous monitoring of connections and statements of sensitive data access by authorized users. Both iMask™ and iMonitor™ have minimal latency.
iProtect™ Offers intrusion protection at the database level as additional security.	**iRetire**™ A tokenization solution for retiring sensitive data in production.	

Pre-Production

MENTIS' unique shared enterprise sensitive data intelligence and integrated architecture combines both static (**iScramble**™) and dynamic (**iMask**™) data masking.

Code scan at preproduction for any changes in sensitive data access can be embedded as security acceptance testing as part of pre-deployment checks and approval.