MENTIS Meets Your Challenges.

CxO

- **Create a Comprehensive GRC strategy.** No need to manage multiple application and database security vendors.
- **Build Collaboration & Visibility for GRC Teams.** Bridge dangerous communication and role gaps that could create security liabilities.
- **Stay Ahead of Changing Legislation.** Comply with today's legislation, and respond to changes rapidly.
- **Be Market Savvy.** Measure industry and compliance standards against the technology stack for continuous compliance monitoring.
- **Free IT & Business.** Streamline for more value-added work and innovation.
- **Protect Reputation & Bottom Line.** Save costs and gain customer confidence.
- **Be Audit-Ready.** Period.

IT

- **Keep Performance Humming.** Zero performance load. Single point installation. Zero overhead. You can reduce the complexity of multiple management tasks.
- **Implement & Deploy Quickly.** Installs within days and re-deploys with a push of a button to greatly improve your security posture.
- **Reduce IT Exposure.** Improve your security posture with airtight data integrity and controls.
- **Get Granular Control.** Satisfy auditors, business, and users.
- **Meet Your Needs Your Way.** Products installed individually or as an entire suite.

Audit, Risk & Compliance

- **Achieve High Visibility.** Create consistent compliance strategy and complete compliance record across the enterprise.
- **Gain Independence.** Conduct review in business language, not technical language.
- **Affirm Separation of Duties.** Find conflicts in applications and databases.
- **Produce Granular Documentation.** Know the "who, what, when, where, and how" across the enterprise – then compare to applicable legislation.
- **Review Code.** Identify compliance breaches before code is migrated to production.
- **Adjust your Risk Matrixes.** Create fresh, point-in-time documentation.
- **Automate.** Take the manual effort out of internal controls, testing, and reporting.
- **Address Insider Threat.** Independently and effectively.

"You have a lot of different options as to how you want to protect your system... We are going above and beyond what we have to."

Anna Goff,
Senior Oracle DBA, South Mississippi Electric Power Association

"[MENTIS] describes what we are protecting and how we are protecting it - who can access the database and who can't. It [MENTIS] gives us the granularity. ... For auditors, we can show the rules and responsibilities - the who, what, when and where of what has been done."

Carl Lindau,
Director of IT, South Mississippi Electric Power Association

ACCOLADES & AWARDS

- "Cool Vendor in Risk & Compliance" – *Leading Analyst Firm*
- "Security Industry Leader" – *Standard & Poor's*
- "Rising Star in Corporate Governance" – *Yale University, Millstein Center*

MENTiSOFTWARE
SECURITY • COMPLIANCE • BEST PRACTICES

311 East 72nd Street, Suite 9A
New York , NY 10021
212.861.2235

sales@mentisoftware.com

www.mentisoftware.com

MENTiSOFTWARE
SECURITY • COMPLIANCE • BEST PRACTICES

Data Loss Prevention & Compliance

Sensitive Data is Everywhere.

Database and application environments are highly dynamic and complex. The data itself brings business to life; it becomes tangible, usable, shareable – and open to abuse. Thus, even though data is stored, it is not "out of sight, out of mind." It is an active, often sensitive element of everyday business. Not only is it propagated and hidden throughout the enterprise; it also has access points that are increasingly difficult to control.

The Critical Intersection of Data Security and GRC.

Compliance is among the top three initiatives of many organizations – and data security plays a fundamental role. However, in those same organizations, data protection is seen as the responsibility of IT, since the core IT team understands both the database and its technical language. Though IT "owns" the data, it is the Compliance group that has the expertise to understand the law and what is needed to comply with that law. Moreover, other stakeholders have key responsibilities. Risk Management creates the policy necessary to mitigate possible loss or damage. Auditors demand independence; and also expect documentation proving that the entire technology stack is protected. The result: each group speaks a different language at a critical intersection where communication gaps could equal security gaps.

MENTIS bridges dangerous security gaps by helping all stakeholders speak the same language. With MENTIS, your security posture can be made visible at any point in time with highly granular documentation that everyone understands.

Assess Risk. Analyze Exposure. Act Decisively.

MENTIS' preventive and detective strategy automates compliance and security across the database and application architecture. A deep scan finds sensitive data anywhere within an enterprise database by evaluating the data patterns stored in tables and columns. MENTIS then classifies this data and translates it into a common business language so all stakeholders can work toward the same goal.

In addition, out-of-the-box metadata, security rules, and a library of separation-of-duties conflicts allow companies to comply with the changing industry laws and automate complex processes.

In other words, we've done the tough thinking, so you can assess your risk comprehensively, analyze exposure intelligently, and act quickly and decisively.

www.mentisoftware.com sales@mentisoftware.com 212.861.2235

"A single, cost-effective solution to protect all our enterprise Oracle databases. Helps us on our path to Best Practices."

Bob Peck
VP, Accounting - Top 10 Multiple Services Organization (MSO)

AUTOMATE

- **Crawling –** pattern recognition that helps you find sensitive data you didn't know you had.
- **Data Classification**
- **Data Masking**
- **Activity Monitoring**
- **Intrusion Prevention & Access Control**
- **Risk & Exposure Assessments**
- **Code Review & Source Code Library**

DEFENSE IN DEPTH

- Production & Non-Production Databases
- Enterprise & Custom Applications

A Clear Path to Data Loss Prevention and Compliance.

1. ASSESS RISK

DATABASES - *Where does sensitive data reside?*

Identify where sensitive data is stored

Classify Data – turn technical language into a shared business language.

MENTIS FRAMEWORK
Our products and services are built on the same technical framework, and share a metadata and data classification engine.

Metadata and data classifications are pre-built, with an automated method for customized extensions, and pattern recognition. A deep scan finds the most hidden sensitive data with ease.

Templates help organize work according to a particular law, group of laws, type of database – or whatever you choose.

A single user interface presents both business and technical teams with clear visibility into your organizations data security and compliance posture.

MENTIS IS DIFFERENT.

Because of the MENTIS Framework, our products implement in days, not weeks or months, and can be deployed to multiple databases with a push of a button. You don't have to re-do your work, or reinvent the wheel.

APPLICATIONS - *Where is sensitive data exposed?*

Catalog Application Source Code

Catalog exposure from changes in code to application forms and reports

iCatalog determines if specific code could inappropriately expose users to sensitive data – a valuable change control tool and testing step for compliance. Conduct a quick, dynamic review of the code written into every application object (forms, reports, and JSP, .Net, PL-SQL, etc.). The detailed, pre-built library can be extended to custom applications.

2. ANALYZE EXPOSURE

DATABASES - *Who logged on? What can they see? What can they do?*

Review Database Access – of privileges, roles, and schemas

iDocument retrieves all privileges and roles within and across all enterprise databases at any point in time. Easily see who has inappropriate levels of access, from where they are logging on, and which programs they are using. With an at-a-glance, visual representation, compare your access controls to relevant legislation.

APPLICATIONS - *Who logged on? What can they see? What can they do?*

Review Access to Sensitive Data – for separation of duties conflicts within one or between multiple applications

iAudit automatically reviews access privileges to application forms and reports – across the enterprise. The complexity of password, role, and responsibility management is reduced to a simple, at-a-glance report. A library of common separation of duties conflicts helps validate that users are assigned access appropriate for their work – no matter how many applications or forms they log onto.

MENTIS IS DIFFERENT.

MENTIS products can be owned by Non-IT personnel for absolute separation of duties.

3. ACT DECISIVELY

PRODUCTION DATABASES - *What is appropriate access to data – for each user, according to the responsibilities of their job?*

Prevent Intrusions – keep unauthorized connections out of Production

iProtect tightly controls access to your production environment. Prevent unnecessary access, and assign and manage appropriate access for all users. Authorize the program, terminal, and time of day that access is allowed for each user, even if they use a schema to gain entry.

Mask Data – for legitimate connections that do not need access to sensitive data

iMask for Databases protects sensitive data with authorization rules when direct connections are made. iMask maintains complete database functionality so users see only the data they need to do their jobs. It provides all of the safeguards that encryption can and more, but without the performance penalty, or the need to re-engineer or retrofit your applications.

Monitor privileged users, document details, and stop intrusion in progress.

iMonitor has actionable alerts including intrusion detection, attack termination, and internal controls. iMonitor documents the specific rows, columns, and timestamp of the data that was breached. Your organization can narrow victim notifications to only those that were truly affected, saving cost and reputation, and gaining customer confidence.

NON-PRODUCTION DATABASES - *Do contractors, global partners, developers, and others have access to Production copies?*

Eliminate Risk and scramble data

iScramble masks (obfuscates) sensitive data and maintains complete functionality in non-production databases. It provides safeguards that encryption cannot and without the performance load.

APPLICATIONS - *Do end-users have the data access appropriate for the work that they do?*

Mask Sensitive Fields from end users based on the user and/or responsibility.

iMask for APPS creates granular and dynamic rules for application forms. iMask for Apps masks sensitive information by user and responsibility, without the security loopholes that can result from custom-developed code. Lock down sensitive data so that each user sees only the information necessary to do their job – at the field, row, column, and form event level.

NOTES:

"iScramble is an important tool in helping us keep our commitment to doing what's right to protect sensitive information of our students, employees, partners and vendors."

Grant Gasson,
VP, Financial & HR Systems
Apollo Group