

iMonitor

Access Monitoring and Documentation for Production Databases

iMonitor provides next-generation security access monitoring and documentation for sensitive data residing in production databases. iMonitor documents the detailed data needed to comply with privacy legislation, and has actionable alerts including intrusion detection, attack termination, victim notification, and internal controls.

The Power to Terminate Attacks

When suspicious activity is detected, iMonitor's alert engine verifies that the access is unauthorized, and then sends actionable alerts to designated pagers, hand-held computers, or email inboxes - in real time. The alerts are flexible and can be scheduled from 1-180 minute intervals. With timely, accurate information in hand, your staff can determine the right course of action and even stop an intrusion already in progress.

Rock Solid Compliance & Internal Controls

iMonitor's continuous tracking and alerting systems enable your company to demonstrate thorough and independent controls over private data access. iMonitor's logs are comprehensive and can pinpoint the exact database areas that the intruder accessed down to the actual row, and, in some cases, the SQL statement or database program used. You will be able to determine:

- Who accessed the information
- What information was accessed
- When the information was accessed
- How the information was accessed (SQL, Export, Copy Table, Connection Type such as ODBC, etc.)
- From where the information was accessed (Workstation, Server, Web Port, etc.)

iMonitor will satisfy Internal IT auditors, the Privacy & Security Office, and multiple, legislative mandates.

Notify Your Customers with Confidence

Until iMonitor, determining what specific data was actually breached made compliance with new privacy legislation slow, and accurate victim notification impossible. With speed, accuracy, and detail, iMonitor assesses the intrusion, and then records the specific rows, columns, and timestamp of the data accessed. Instead of the cost and exposure of notifying untold numbers of victims, your organization can narrow the notifications to only those that were truly affected. If you add iMask and iScramble to your suite of products, you can also see if the data the intruder accessed was something they could use or not, further narrowing the notification list and adding the power of knowledge about the attack. This is a differentiation that your customers will appreciate. iMonitor, when used with iMask and iScramble, will help your Publicity Department. A formerly weak position is now one of strength.

iMonitor Benefits

- Detect intruders 24/7 with automated, continuous monitoring
- Stop an intrusion in its tracks with actionable, real-time alerts
- Record the specific rows, columns and timestamp of the data accessed with speed and accuracy
- Determine the specific information actually breached
- Save cost and reputation by narrowing customer notifications to only those that were truly affected
- Add iMask and iScramble to your suite of products, and see if the data the intruder accessed was something they could use or not, further narrowing the notification list
- Demonstrate thorough and independent controls
- Comply with privacy legislation
- Provide log reports and alerts that are readily usable by IT, Audit, and Security Teams without customization

Do You Know...

- When an intrusion occurs while it is happening?
- Who accessed the information?
- What information the intruder saw?
- How the information was accessed?
- From where data was accessed?
- The names of privacy victims to notify?



Efficient, Low-Cost Architecture. One Solution.

When combined with iMask and iScramble, iMonitor offers a complete solution for protecting enterprise databases, both production and non-production. Simple, easy-to-use interfaces allow collaboration between IT, Audit, Security & compliance groups within your organization, streamlining compliance, audit costs, and efforts.

iMonitor uses the existing database technology stack; no additional software licensing is required. iMonitor, iScramble, iProtect, and iMask 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.

Industry Based Compliance: Metadata, Data Classifications, and Access Rules.

iMonitor's metadata simplifies the process of locating and delineating your organization's sensitive information. Pieces of data from different data base areas that could be combined into a privacy record, or hidden data that might not be obviously private, can be defined by IT and non-IT personnel alike. Therefore, privacy & security officers or IT can easily create stakeholder-defined contents - groupings of tables and columns based on industry, business practice, or stakeholder type. With iMonitor, organizations have a portal through which they can take action on customer, employee, vendor, partner, or corporate data that could be exposed. IT can also define content based on the purpose of the database itself and easily delineate and document access rules. MENTIS' iMonitor product offers unique industry-based compliance with the most granular and accurate detection and documentation tools on the market.

Support for Hybrid Systems

Most organizations have several database and application types that store and give access to sensitive information, creating hybrid systems. MENTIS' development schedule includes an aggressive plan to help organizations protect their company across various database architectures. MENTIS supports Oracle database customers with PeopleSoft HR, PeopleSoft Financials, and Lawson. In 2008, MENTIS will also support SQL-Server and Enterprise DB.

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.



MENTISoftware
SECURITY • COMPLIANCE • BEST PRACTICES

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

sales@mentissoftware.com

www.mentissoftware.com