Enterprise Security Auditing

Data Privacy

iMaxsoft Corporation

June 2007

Version 1.0

WE'LL ALWAYS BE HERE

Industry Leader in Enterprise Security Compliance Products
Based in Cupertino, CA since 1987

Table of Contents

Executive Summary

Federal policies and regulations have become an increasing and more pervasive burden upon today's organizations. The success of your business depends on how quickly and effectively it responds to new policies and regulations. Responding quickly is not sufficient, however; you need to know that your company is moving in the right direction. Compliance requires an information technology (IT) infrastructure that delivers solutions that meets today's regulations while being flexible enough to enable your company to rapidly adopt future additions to policies.

The typical IT infrastructure is a complex mix of technology from different vendors that is difficult and costly to maintain. Your challenge is to make it all work together faster and at a lower cost. iMaxsoft's answer to this challenge is the VerticoData solution, a complete software offering that helps customers comply with Privacy Requirements with ease. VerticoData provides auditing tools to make rapid enhancements to your existing production environment without costly additions your infrastructure. VerticoData provides a detailed audit trail of all read and write transactions that are defined as sensitive data. It records which user access or change sensitive data at any point in time and stores the audit trail data into a relational database.

How can VerticoData Help?

In today's fast pace industries where technology is rapidly advancing, security takes the highest priority among corporations due to vast amounts of data stored electronically. Lots of measures have been taken to safeguard and block un-authorized access to private data banks. As that technology advanced, there seemed to have been something that was overlooked. What we have been lacking is a universal and secure way of preventing potential security breaches from the corporate back-office computing environment.

There is an ever growing necessity in modern day business to log and prevent security violations from *authorized* personnel. Federal policies and regulations such as HIPAA and Sarbanes-Oxley are becoming an increasing and more pervasive burden upon organizations in all industries. Pressures from both the government and consumers are forcing businesses today to find new ways in protecting sensitive data from not only outside intruders but inside trespassers as well while not hindering their existing IT infrastructure.

IMAXSOFT is a provider of cutting-edge technology for comprehensive enterprise security solutions. We offer highly efficient methods of securing sensitive data to help companies:

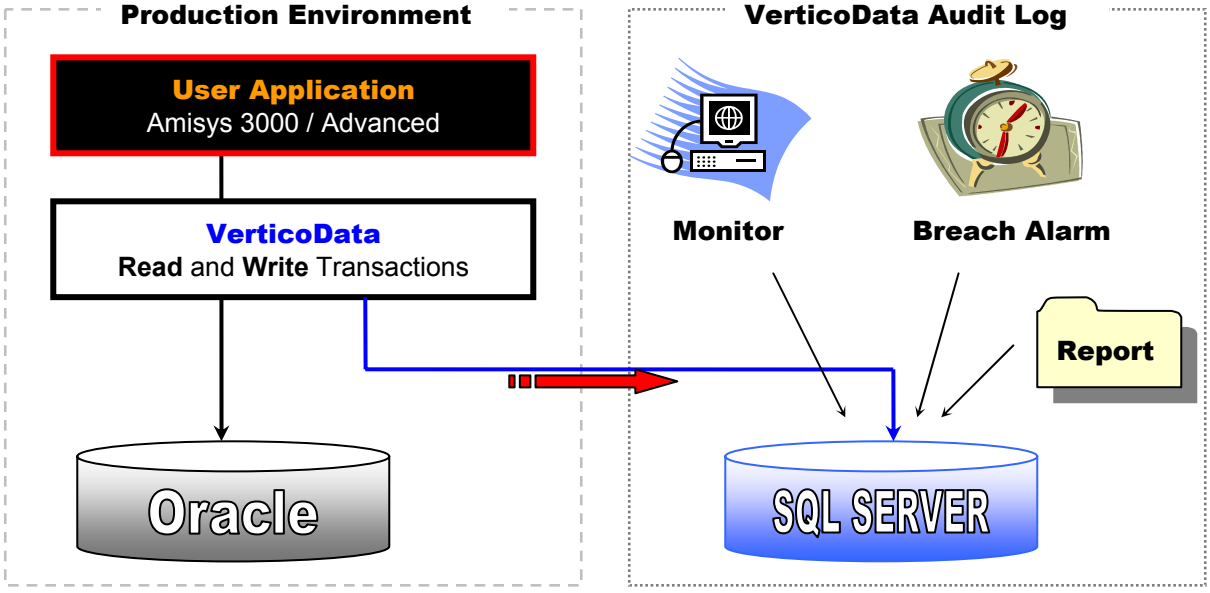
- Secure and monitor confidential and sensitive data
- Analyze and improve day-to-day operations based on data access
- Prevent any internal or external security violations
- Comply with legislative policies and regulations
- Log and audit application critical data

Our comprehensive security solution allows you to stay ahead and differentiate yourself in the highly competitive and rapidly advancing industry of security.

Securing Your Data

iMaxsoft's goal is to be able to provide secure and efficient transaction logs for your private and confidential data while remaining transparent to the data sources and applications themselves. Due to the scope of legacy applications running on proprietary systems, a solution that can be easily integrated into existing legacy environments also becomes critical to our technology. This powerful engine offers a secured and high-performance logging facility and dispatching system.

VerticoData Auditing Technology



VerticoData offers an industry specific role based transaction monitoring solution that allows you to make detailed analysis of all read, write, and update transactions. Not only will this system record and safeguard any illegal or abnormal access to your sensitive data, it enables extensive capabilities to analyze day-to-day operations based on who is accessing your data at what time.

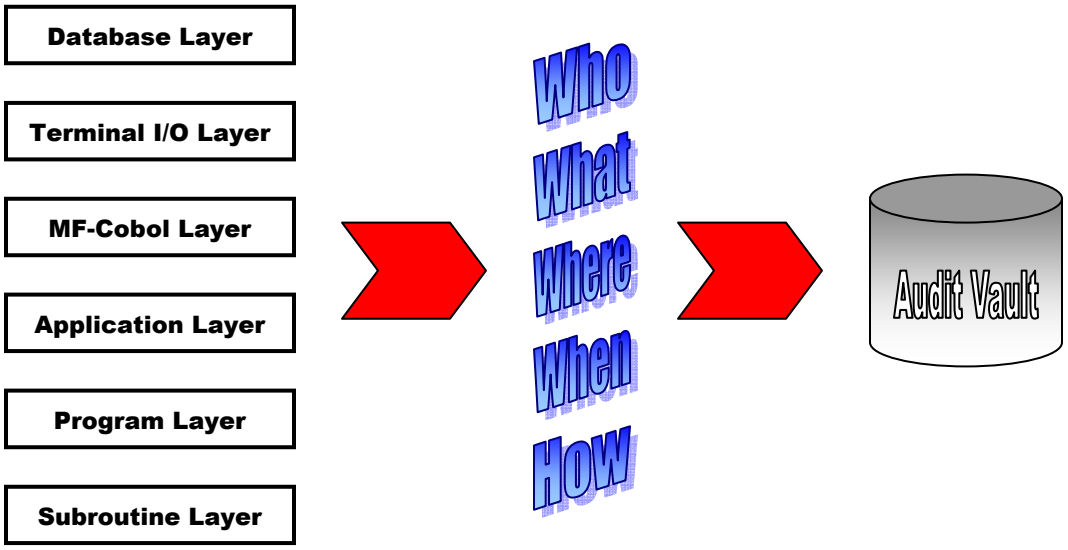
Proven Solution

VerticoData sits on top of iMaxosft's proven, patent pending technology that has been *deployed by top Fortune 1000* companies occupying a variety of industries around the world. This powerful engine is designed for performance and has been used in many critical applications *for over 20 years*. Diverse applications such as airline ticketing, on-line sale, shipping logistics, automobile manufacturing, telecoms, HMOs, hospital management, among others have

benefited from the iMaxsoft technology in developing best in class applications to address their customer needs.

VerticoData Technology

VerticoData is a complete enterprise audit-trail solution. Its intent is to log *who* and *how* they accessed *what* data from *where* at what time (*when*). Who is defined by which application user was used to access sensitive data. How is customized information defining through what medium the user accessed the sensitive data. What is defined by the actual sensitive data that has been accessed. Where is defined by the physical location of the sensitive data. When is defined by the timestamp when the sensitive data transaction took place.



Its broad and flexible technology allows its users to span across their application and data through different layers of access. Each layer functions independently and has its own uniqueness. Audit logs from the different layers are consolidated and stored into the audit-trail in real-time. Audit trails can be set in the following layers:

- The Database layer – OCI
- The Terminal I/O layer – Screen I/O
- The MF-Cobol File System layer – File I/O
- The Application layer – Amisys, ASI, SAP, Oracle
- The Program layer – ProC, ProCobal
- The Subroutine layer – C/C++, Cobol Subroutine

Not only can VerticoData audit database transactions, through these layers it can also monitor file system I/O, terminal screen/form fields, subroutine calls inside individual ERP, and also safeguard database utilities i.e. SUPRTOOL, SQLPLUS, and QUIZ.

VerticoData can also be customized for seamless integration with your current application environment. Screen ID's, private data fields, and managed user logins can all be incorporated into the audit log process.

VerticoData consists of a security platform, a sensitive data definition and policy builder, and a role based security analyzer.

Security Platform

Secure audit-log facility that controls and manages all transactions pertaining to back-office security. This powerful engine captures specific transactions in-between the application layer and data source layer. Due to its unique placement, there is no need for any modification to your existing applications, data sources, or your infrastructure. Its quick and efficient design proves to have minimal impact on performance yet can analyze and log thousands of transactions with no visible consequences to your application.

The core of the Security Platform consists of technology that trace and log Oracle read and write transactions, terminal I/O, Micro-Focus Cobol flat file transactions, and any shared library subroutines.

First Industry Read Transaction Monitoring Solution

VerticoData records both read and write activity of sensitive data. While write transaction audit-trail monitoring has been implemented in some application, read transaction audit-trail monitoring is rarely built in due to performance consideration. VerticoData technology suffers from none of the performance issues experienced by other implementations. All transactions are logged to the relational database of your choice (SQL Server, Oracle or DB2) and can be analyzed using our viewer/analyzer tool that allows you to:

- Identify specific user access patterns
- Pinpoint specific records accessed, created, or updated by a given user during particular dates and times
- Locate potential breaches
- Identify any abnormal access
- Prevent any security violations

Write Transaction Monitoring

For write transactions, VerticoData supports auditing from the database layer by taking advantage of Oracle's redo and archive log functionality. Using log miner, a tool Oracle provides for reading its archive log, we can scan and filter through all write transactions that occurred by a specific tool. Programs such as DBAQ, QUERY, and QTP can all be specified as a target. We can retrieve who, what, where, when, and how all from the archive log in addition to the session id and serial# we need to correlate with our read transactions. This process is completely offline and has zero impact on the production environment.

Utilities Safeguard

VerticoData Utilities Safeguard uses its terminal I/O logging capabilities as a foundation to centrally log who and when a utility is used, i.e. SUPRTOOL, Sqlplus, and Quiz. In addition, it can log the entire user session in a log file for later analysis. This unique option allows you to see exactly what commands (inputs) and results (outputs) your IT staff is executing in your production environment.

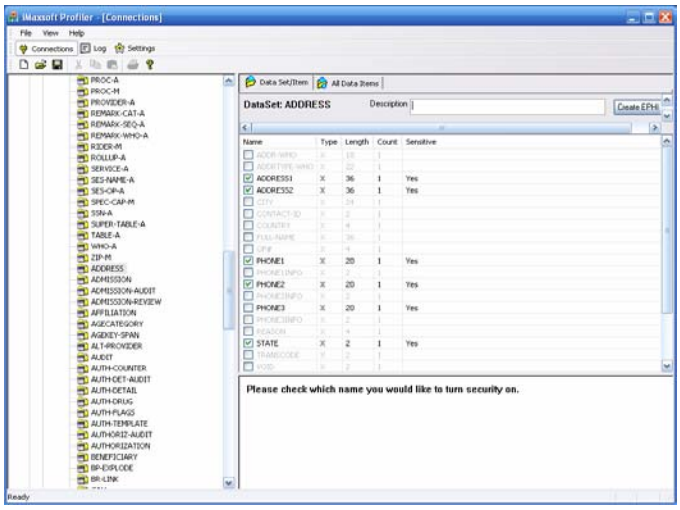
One of our customers decided to monitor Sqlplus from DBA and IT teams in addition to standard Oracle security. VerticoData Utilities Safeguard limited Sqlplus access to a designated user group. When authorized users attempt to run Sqlplus, they are routed through VerticoData Utilities Safeguard first, which in turn executes Sqlplus as the designated user group and audits the entire session. Session logs are then stored on the system for further analysis.

Amisys Integration

VerticoData has been integrated into and now supports both Amisys 3000 and Amisys Advance products on HP3000 and HP9000 Servers. Its rich functionalities and flexibilities can be configured dynamically to meet the most sophisticated auditing requirements without any interruptions to your day-to-day operations. Our technology does not modify or alter Amisys standard source code.

Sensitive Data Definition and Policy Builder

Helps you to easily create and manage sensitive data definitions and policies for enterprise data sources. These policies act as a filtering mechanism that enables you to select and define specific sets or sub-sets of your data source for you to track. Sensitive data definitions and policies provide the necessary information to and interface with the security platform which triggers the secured audit-trail logging. Pre-defined policies within each industry are available which allows you to leverage proven industry standard policies into your system.



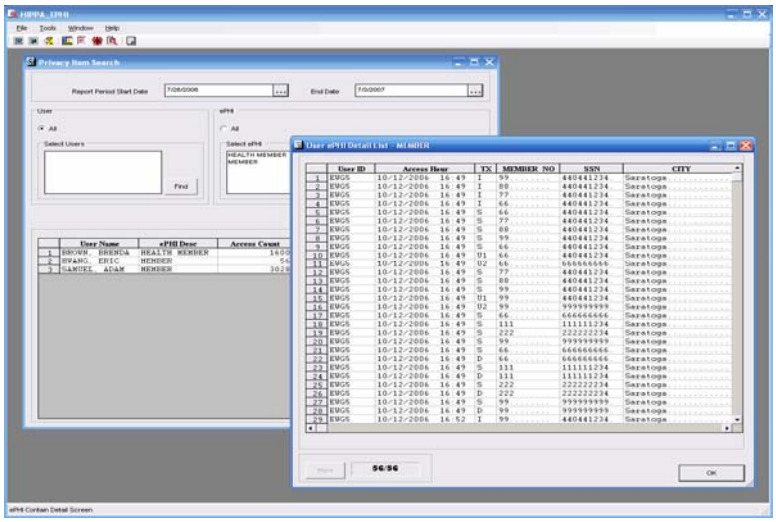
This Windows based application connects to the VerticoData audit vault using iMaxsoft middleware technology. The iMaxsoft secured middleware has a built-in 128 encryption algorithm to protect data in local area networks that travel to and from the database.

Once connected, the Policy Builder will display your entire database schema, its tables, and columns. Through this easy to use interface, you will be able to navigate through and select the sensitive data columns from your database to define policies that will be used by the VerticoData Security Platform for filtering data transactions.

There is also a CLI version available for the Unix/Linux environment. This version takes in a well defined set of policy structures and processes and stores them into the audit vault.

Role Based Security Analyzer

Analyze audit-logs based on pre-set alarm roles to report potential security breaches. Once all the critical transactions have been logged, this tool can mine through the raw data collected and identify specific or suspicious user access patterns, locate potential breaches and weaknesses within your operations, and pinpoint specific data that has been viewed or modified by any given user at anytime. With this analyzer, you will be able to trace and safeguard any security violations within your entire operation.



VerticoData provides four distinct ways to analyze data access patterns.

Abnormal Data Access

Some operations are only allowed access to the database between certain “normal” working hours. This tool allows you to filter through and find all the users who have accessed certain sensitive data at an abnormal time.

Let's say that Company A has employees processing claims between 8am thru 5pm. Nobody is allowed to process any claims before 8am or after 5pm. After scanning the audit vault with VerticoData, we find that John has been entering in claims at 9pm. It turns out John was stealing member information at night when nobody else was in the office.

Excessive Data Access

Excessive activities on sensitive data usually triggers suspicion and may lead to potential security breaches. This tool allows you to filter through and find all the users who have accessed certain sensitive data excessively compared to their individual average.

Let's assume Jane's average daily volume is 40, which translates into 400 transactions. After scanning the audit vault with VerticoData, we find that on a particular day, Jane's activities increased to 1,000 truncations. It turns out that Jane was leaving the company in a month and stealing all the member data for her next job.

Member Data Access

Every single member record in a company's database is required to be securely protected. Very important and private data are stored such as SSN, Credit Cards, and Health Information. This tool allows you to filter through and find all the users who have accessed a certain member's sensitive data.

Let's say Company B receives an unexpected call from Diane, an alarmed customer who had their credit card information leaked out. Diane demands that the company do something or else she will take legal actions. Under the formal HIPAA Formal Rules and Laws, a company will be held responsible for leaking private information unless they can provide a log pinpointing who, when, and how the information was leaked. A quick scan of the audit vault with VerticoData and we find a list of employees that have accessed Diane's credit card information within the last month. It seems that Joe has been the only person during that timeframe who has looked at Diane's credit report. After a detailed investigation, we find out that Joe was indeed stealing credit card numbers from the company and selling them to a credit fraud organization.

Privacy Item Search

There must be a way to directly correlate between your application user and the sensitive data policy. This tool allows you to filter through and find all the users who have accessed a certain sensitive data, or vice versa.

Let's assume Company C is currently in a legal lawsuit of which someone's private health information was leaked. Jack, an employee of Company C, is the brother of Chris, a publisher for the daily newspaper. Chris has been trying to find dirt on the local governor for months. He finally was able to obtain a diagnosis from his brother and published it in his article. In this situation, Company C needs to prove that it was indeed Jack who leaked the information out. After scanning the audit vault with VerticoData, we directly linked Jack to the governor's patient record and were able to prove the case.

Minimal Performance Impact

VerticoData guarantees high performance. It has minimal effect on application performance and is invisible to your end users. Past benchmark tests have shown our solution offers huge gains in business efficiency and features with *less than 2% increase in overall performance overhead*.

With an application level design, process and memory are in the user's domain. There is no direct impact to the Oracle database. Only end results of a query will be logged, which dramatically reduces excessive logging and improves the precision of the logs.

VerticoData has a powerful and condensed rule definition capability that significantly reduces the number of policies. The less policy defined the faster the auditing process is. During the data transaction filter process, policies only need to be evaluated once and then cached for the duration of the entire process life.

IT has the ability to disable VerticoData for those batch programs and reports they do not wish to audit. The support of a mixed environment is essential for high performance. Batch processes that alter but does not display sensitive data, report programs that access but does not print sensitive data, online programs that accesses sensitive data from invoking common routines but do not present it to the end user are all good candidates for disabling VerticoData auditing.

Seamless Integration

VerticoData is easy to integrate with your environment. Generally all that is required to enable it is a simple XL list change to your MPE/XL startup UDC. The Unix/Linux equivalent would be a quick change in your shared library path. We will assist in the setup of your entire environment along with helping your team to create, configure, and maintain your RDBMS infrastructure. If necessary, iMaxsoft can also design custom solutions to the specifics for your infrastructure.

The VerticoData technology is transparent to your application and database. This means there is exactly zero modifications that need to be made to your production environment.

Customized Security Solution

Due to the flexible nature of VerticoData, it is easy to log additional audit information and implement alternative methodologies. Certain application specific information can be build into VerticoData to accommodate individual needs. Some examples include but are not limited to the following:

- Custom reporting to satisfy auditing requirements
- Unique transaction identification logging
- Specialized performance tuning
- Interface with operation consoles through callback routines

Why Choose VerticoData?

Existing data audit security tools such as Oracle FGA, Oracle Audit-Vault, and other third party tools *do not* log the final results of a read transaction to the audit-trail. They are designed to restrict access at the table level safeguarding the data but preventing user applications to function properly. In order to perform data level audit-trail analysis, the replaying of audited queries is required. This is not technically feasible because in a multi-user environment, even at the same moment the exact same query from 2 concurrent users have 2 different data views. ORACLE uses SCN (System Change Number) to ensure consistent data views for each user. SCN, however, uses Rollback Segments to accomplish this but the Audit-log doesn't store any SELECT transactions. Let us look at an example from Oracle Fine-Grained Auditing:

> *"SELECT CLAIM_NO, MEMBER_NO, DIAG_CODE, TOTAL_AMT FROM CLAIM WHERE PROVIDER_NO = :PROVIDER_NO"*

In this example, If *MEMBER_NO*, *DIAG_CODE* and *TOTAL_AMT* are both ePHI, then having the above query logged only tells us that *:PROVIDER_NO* 440004 from *DBA_FGA_AUDIT_TRAIL* column *SQL_BIND* is accessed by a particular user at a specific time. We would need to replay the query in order to find the actual data of *MEMBER_NO*, *DIAG_CODE* and *TOTAL_AMT*. The problem is that Oracle cannot re-produce the exact same data view that was used at the time the query was executed. Tools like these are not specifically designed for dynamic transaction analysis required by federal regulations. They do however provide a powerful rule-based engine that safeguards your data from un-authorized access.

Other alternative tools provide agents set at the network layer that analyzes incoming and outgoing data. This method of auditing does not capture local or direct data access and proves to be a heavy burden to your runtime performance. Internally developed tools using triggers or application modification do not capture all data transactions. They are time-consuming and costly to implement and maintain. Most importantly, none of the existing solutions provide a useful and realistic approach in auditing read activities for your data sources.

Conclusion

Most back-office security measurements are only built around the concept of preventing data from being accessed through the internet, which only controls un-authorized access of sensitive data but doesn't manage authorized access. Due to recent years of explosive technologic advances, faster processors, bigger networking bandwidths, and larger storage spaces are becoming ever easier to obtain. Huge enterprise data are accumulating and being accessed every second of the day. Privacy and sensitivity become a major challenge not only to IT but also to the entire corporation. The time to track "*who updates what*" has passed. Today, "*who is reading what*" is more valuable to the business than ever before. A robust security platform with well-defined security policies and standard monitoring rules for back-office computing environment is essential to all industries.

Why doesn't ORACLE, SAP, or IBM do it themselves? Any complete solution is required to be generic enough to integrate with all applications and all data sources. Individual vendors can only provide solutions tailored to its own applications or data sources which are not sufficient to those corporations who operate in a heterogeneous computing environment.

Any service provider, software and hardware vendor, or enterprise IT can develop a custom security solution to fulfill their own specific needs. This, however, does not mean that they should. Today's computing environment is changing so rapidly that a custom solution is simply too costly to maintain and too slow to implement in order to satisfy the growing business needs and regulatory requirements. Rather than derailing from their core business to spend time in an unfamiliar field, why not focus on current objectives and plug in a security system that is guaranteed to work?

As a result, neither a vendor specific nor a custom solution is strategically viable for satisfying a quick and on-demand application model with a fast time-to-market business approach. A plug and play system that is platform independent and can be quickly deployed is the key to a successful solution. IMAXSOFT is the only independent integrator that provides a cost-effective internal security solution that is comprehensive and transparent to applications and its data sources.

For More Information:

Visit us at: www.imaxsoft.com

Email us at: support@imaxsoft.com

iMaxsoft Corp.

20410 Town Center Lane #295
Cupertino, CA 95014

Phone (408) 253-8808
Fax (408) 253-4008

www.imaxsoft.com