



Business Challenge

A leading international telecommunications organization needed a cost effective means to protect the privacy of its customer data and comply with regulatory requirements.

Solution

InfoSphere Guardium provided a fine grained audit trail of all sensitive data access, along with automated reporting and compliance workflow, satisfying the needs of auditors. Real-time blocking and alerts ensured privacy policies were strictly enforced.

Data Privacy in Telecommunications

Case Study: Implementing Database Activity Monitoring for a Major International Telecommunications Company

The organization wanted to:

- Monitor access to private customer data located in thousands of databases across a wide geographical area.
- Implement the solution for both Operational Support Systems (OSS) and Business Support Systems (BSS).
- Create a centralized audit trail for all database instances across:
 - Multiple DBMS platforms: Oracle, SQL Server, Sybase
 - Multiple OS platforms: Solaris, OpenVMS and Windows
 - Multiple data center locations: OSS in 11 locations, BSS in five locations
- Monitor privileged user access via local protocols such as Oracle BEQ, shared memory and Sybase TLI.
- Produce detailed compliance reports for their auditors.
- Implement proactive security via real-time alerts for critical events, based on both corporate security policies and anomaly detection (comparison to baselines).
- Monitor application end-users for fraudulent activities via enterprise applications such as Business Objects.
- Provide granular logging (to a single DB column) with detailed information about users (username, IP address, MAC address, application name, protocol, etc.).
- Log all security exceptions such as failed logins and SQL errors.
- Log all query results for sensitive data.
- Provide separation of duties and non-repudiation of audit data; ensure that data cannot be modified by anyone, even authorized administrators, via access at any level (e.g. system GUI, root access to OS, physical access to storage).
- Support cross-analysis (correlation) of log information from different databases.
- Easily integrate the solution with their existing environment (LDAP, Kerberos, SNMP/SMTP, etc.) and manage it remotely.
- Implement a solution that does not rely on database-resident functions (such as triggers, trace or transaction logs) since these can affect database performance and stability.
- Select a solution that provides strong 2-factor authentication such as RSA SecurID.
- Implement a solution that incorporates appliances with high-availability features (RAID, fail-over, etc.).



The customer’s systems are managed by a well-known global systems integrator. After inquiring with Gartner and Forrester Research, the systems integrator evaluated multiple database auditing vendors (including Oracle) and chose the InfoSphere Guardium solution.

InfoSphere Guardium’s appliance-based technology allows companies to secure their enterprise data and rapidly address compliance requirements without affecting performance or requiring changes to databases or applications.

Environment

The company’s infrastructure includes thousands of databases in Production, Staging, Test, and Development environments, that need to be monitored for unauthorized or suspicious access. These databases support a range of OSS and BSS applications.

The following table summarizes how InfoSphere Guardium addressed the stringent requirements typically defined by telecommunication organizations.

Customer required	InfoSphere Guardium provided
The means to produce information required for national data privacy laws.	The InfoSphere Guardium solution creates a continuous, fine-grained audit trail of all database activities – including the “who, what, when, where, and how” of each transaction. It continuously analyzes and filters this granular data in real-time to produce the specific information required by auditors.
Customizable reporting	The system ships with 150+ pre-configured templates for security and privacy regulations. Reports can easily be customized via a drag-and-drop interface.
Automated compliance reporting and workflow	Capabilities to automatically generate compliance reports and distribute them to oversight teams for electronic sign-off or escalation, reducing compliance costs and effort.
Support for all DBMS platforms installed in their environment	Support for all major database platforms – including Oracle, Microsoft SQL Server, IBM DB2, IBM Informix, Oracle MySQL, Teradata, Netezza, PostgreSQL, Sybase ASE, and Sybase IQ – on all major OS platforms (Windows, Solaris, HP-UX, AIX, Linux, Tru64, z/OS).
Easy integration into the existing environment	InfoSphere Guardium’s non-invasive approach has virtually zero impact on performance (typically less than 2%) and does not require any changes to databases or applications. Customers can monitor traffic via SPAN ports, network TAPs, or lightweight host-based probes – or any combination that best fits their environment.
A solution that does not rely on database-resident functions that affect performance or stability, such as triggers, trace or transaction logs, or native auditing	InfoSphere Guardium’s architecture is database-independent. It works by continuously monitoring and analyzing all database traffic – including both network and local traffic – for suspicious or unauthorized activities, without relying on database trace or transaction logs. This non-invasive approach provides 100% visibility into all database activities without impacting performance or enabling any database-resident functionality.
Monitoring of all data definition modifications (DDL)	InfoSphere Guardium monitors all database schema changes such as inserting or removing tables or columns. This is required to enforce change control policies.
Monitoring of all data manipulation (DML) actions (SELECT, INSERT, UPDATE, DELETE, etc.)	InfoSphere Guardium monitors all SQL statements including DML. This is required to monitor access to sensitive data as well as to enforce change control policies for critical data values.
Monitoring of all exceptions	InfoSphere Guardium monitors security exceptions such as failed logins, permission denied on selects, and SQL errors.
Automated reconciliation of DB changes with approved change control requests	InfoSphere Guardium reduces staff time to address auditors’ requirements by automatically creating reports that compare all detected changes with approved change requests (from Peregrine, Remedy, etc.). It generates real-time alerts when unauthorized changes are detected, including changes to configuration files and environment variables.
A means to provide proactive security	InfoSphere Guardium is a policy-based system that provides a number of automated actions that customers use to respond to policy violations, including real-time alerts, blocking, and customized actions. This allows the security organization to immediately detect potential intruders in a proactive approach, rather than rely on reactive “after-the-fact” actions obtained after reviewing traditional logs.

A system that provides full information about originators of database transactions	InfoSphere Guardium identifies the user via a number of values including username, OS username (Domain login), MAC address, hostname and IP address of client system. It also identifies the application used to access the database, so it can enforce policies regarding the use of unauthorized applications such as Microsoft Excel or SQL developer tools.
A system that identifies application user IDs in connection pooling (Application Server) environments; does not simply show generic database login ID	InfoSphere Guardium positively identifies application user IDs associated with database queries and activities. Unlike other approaches, InfoSphere Guardium's approach supports both pure HTML applications as well as applications that use other presentation-layer technologies such as ActiveX controls and applets (e.g., Oracle). It also supports Single Sign On (SSO) environments.
A system that provides complete auditing with no "back doors" (e.g., local access)	In addition to monitoring all database traffic at the network level, InfoSphere Guardium provides a lightweight software probe (called S-TAP™) that monitors privileged local traffic at the operating system IPC layer (such as console access, terminal services, shared memory, and named pipes). The probes minimize any effect on server performance because they simply relay traffic to InfoSphere Guardium appliances for processing and analysis.
A system that tracks changes to DB configuration files that can affect DB security posture	InfoSphere Guardium's Change Auditing System (CAS) tracks all changes to DB configuration files and other external objects such as environment/registry variables, shell scripts, OS files, and executables such as Java programs. To accelerate deployment, the system includes 200+ pre-configured templates for all popular OS/DB configurations.
Support for SQL Server SSL Encryption and Kerberos Authentication	Encryption support is built-in and never requires keys to be uploaded to the InfoSphere Guardium system.
Secure, tamper-proof audit repository with data mining tools for forensics	All audit data is stored in a single centralized repository that cannot be modified by privileged users. This provides the "verifiable audit trail" for auditors and forensic investigations. There is no root access to the device. A rich set of data mining tools is provided for forensic investigations.
Efficient storage of auditing information to reduce storage costs	InfoSphere Guardium uses patented, intelligent storage algorithms to minimize the capacity required to store massive amounts of transaction data. These algorithms store audit data in 20-100x less space than traditional logging solutions.
Management Requirements	InfoSphere Guardium provided
Support for centralized management	A scalable, multi-tier architecture with centralized policy management and aggregation/normalization of audit data for enterprise-wide compliance reporting, forensics and incident management. Appliances are remotely managed via a graphical Web console interface.
Integration with existing management systems (Cisco MARS, IBM Tivoli, etc.)	Support for standard interfaces including SNMP and SMTP as well as data export via CSV files. Additionally, information from other systems can easily be imported into the InfoSphere Guardium system for incorporation in reports and queries.
Integration with identity management systems	Support for LDAP and Kerberos systems for identifying DB users. Also supports LDAP and RSA SecurID for authentication by system administrators to the system itself.
Role-based administration	The ability to be administered by non-DBAs such as Information Security or Compliance professionals. Can also be tailored to support different permissions and views based on role.
Integration with archiving systems	Each appliance includes self-contained storage for 6-9 months (typically) of audit information. It also integrates to standard archiving devices (file servers, NAS, IBM TSM, EMC Centera) for periodic, scheduled archive processes.
Power-down protection	The ability to protect itself from unexpected power-downs and shut-downs of the local probe via security alerts.

Other Telecom Installations

InfoSphere Guardium technology is currently being used to protect the privacy of sensitive data for many telecommunications companies around the world. Other installations include:

- Several global telecommunications and mobile wireless operators based in Europe
- Several mobile wireless telecommunications operators in the southern hemisphere
- Several US-based telecommunications operators
- Several Japanese telecommunications operators

About IBM InfoSphere Guardium

InfoSphere Guardium is the most widely-used solution for preventing information leaks from the data center and ensuring the integrity of enterprise data. It is installed in more than 400 customers worldwide, including 5 of the top 5 global banks; 4 of the top 6 insurers; top government agencies; 2 of the top 3 retailers; 20 of the world's top telcos; 2 of the world's favorite beverage brands; the most recognized name in PCs; a top 3 auto maker; a top 3 aerospace company; and a leading supplier of business intelligence software. InfoSphere Guardium was the first solution to address the core data security gap by providing a scalable, cross-DBMS enterprise platform that both protects databases in real-time and automates the entire compliance auditing process.

Guardium is part of IBM InfoSphere; an integrated platform for defining, integrating, protecting and managing trusted information across your systems. The InfoSphere Platform provides all the foundational building blocks of trusted information, including data integration, data warehousing, master data management, and information governance, all integrated around a core of shared metadata and models. The portfolio is modular, allowing you to start anywhere, and mix and match InfoSphere software building blocks with components from other vendors, or choose to deploy multiple building blocks together for increased acceleration and value. The InfoSphere Platform provides an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster.



© Copyright IBM Corporation 2010

IBM Corporation
Route 100
Somers, NY 10589

US Government Users Restricted Rights - Use, duplication of disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Produced in the United States of America
May 2010
All Rights Reserved

IBM, the IBM logo, ibm.com, Guardium and InfoSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

¹ *The Forrester Wave: Enterprise Database Auditing and Real-Time Protection, Q4 2007* by Noel Yubanna, October 2007.



Please Recycle