



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

Overview

A leading international telecommunications organization needed to implement database activity logging in order to protect the privacy of its customer data and comply with regulatory requirements.

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 users 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 solution with their existing environment (LDAP, Kerberos, SNMP/SMTP, etc.) and manage it remotely.
- 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.
- A solution that provides strong 2-factor authentication such as RSA SecurID.
- 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, the systems integrator evaluated multiple auditing vendors (including Oracle) and chose the Guardium solution.

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 Guardium addresses the stringent requirements typically defined by telecommunication organizations.

Customer required	Guardium provided
Produces information required for national data privacy laws.	The 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 100+ pre-configured templates for security and privacy regulations. Reports can easily be customized via a drag-and-drop interface.
Automated compliance reporting and workflow	Reduces compliance costs and effort by automatically generating compliance reports and distributing them to oversight teams for electronic sign-off and escalations.
Supports all DB platforms installed in environment	Supports all major database platforms -- including Oracle, Microsoft SQL Server, IBM DB2, Informix, Sybase ASE, and Sybase IQ – on all major OS platforms (Windows, Solaris, HP-UX, AIX, Linux, OpenVMS, z/OS).
Integrates easily into existing environment	Guardium's non-invasive approach has virtually zero impact on performance (<5%) 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.
Does not rely on database-resident functions that affect performance or stability, such as triggers, trace or transaction logs, or native auditing	Guardium's architecture is network-based and 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.
Monitors all data definition modifications (DDL)	Guardium monitors all database schema changes such as inserting or removing tables or columns. This is required to enforce change control policies.
Monitors all data manipulation (DML) actions (SELECT, INSERT, UPDATE, DELETE, etc.)	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.
Monitors security exceptions	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	Reduces staff time to address auditors' requirements by automatically creating reports that compare all detected changes with approved change requests (from Peregrine, Remedy, etc.). Generates real-time alerts when unauthorized changes detected, including changes to configuration files and environment variables.
Provides proactive security	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.
Provides full information about originators of database transactions	Guardium identifies the user via a number of values including username, OS username (Domain login), MAC address, and 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.
Identifies application user IDs in connection pooling (Application Server) environments; does not simply show generic database login ID	Guardium positively identifies application user IDs associated with database queries and activities. Unlike other approaches, 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.
Provides complete auditing with no "back doors" (e.g., local access)	In addition to monitoring all database traffic at the network level, 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 Guardium appliances for processing and analysis.

Tracks changes to DB configuration files that can affect DB security posture	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.
Supports SQL Server SSL Encryption and Kerberos Authentication	Encryption support is built-in and never requires keys to be uploaded to the 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	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

Supports centralized management	The Guardium solution is based on 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.
Integrates with existing management systems (MOM, Cisco MARS, IBM Tivoli, etc.)	Supports 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 Guardium system for incorporation in reports and queries.
Integrates with identity management systems	Supports 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	Can 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.
Integrates 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 management	The system protects itself from unexpected power-downs and shut-downs of the local probe via security alerts.

Other Telecom Installations

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 Guardium

Guardium, the database security company, develops the most widely-used solution for database activity monitoring, security and auditing. Recognized as "A Leader across the board" in *The Forrester Wave™: Enterprise Database Auditing And Real-Time Protection, Q4 2007*, Guardium was the first company to address the core data security gap by delivering a scalable enterprise platform that continuously protects databases in real-time and automates the entire compliance auditing process.

Guardium has partnerships with Oracle, Microsoft, IBM, Sybase, BMC, EMC, RSA, Accenture, NetApp and McAfee, with Cisco as a strategic investor, and is a member of IBM's prestigious Data Governance Council and the PCI Security Standards Council.



230 Third Avenue • Waltham, MA 02451 • T: +1-781-487-9400 • www.guardium.com