Guardium

BlueCross BlueShield

Case Study: Implementing Database Auditing, Monitoring and Security in a Leading Blue Cross and Blue Shield Organization

Overview

A leading Blue Cross and Blue Shield organization with more than 500,000 members needed to implement database auditing in order to comply with SOX and HIPAA regulatory requirements.

The organization wanted to:

- Monitor access to all critical databases, including access by privileged insiders.
- Create a centralized audit trail for all their database systems.
- Produce detailed compliance reports (SOX and HIPAA) for their auditors.
- Implement proactive security via real-time alerts for critical events.
- Acquire a solution that integrated easily with their existing environment (LDAP, SIM/SEM, Cisco switches, MOM, etc.) and could be managed remotely.
- Select a solution that does not rely on database-resident functions (such as triggers, trace or transaction logs, etc.) which can affect database performance and stability.

After inquiring with Gartner and Forrester Research, the BC BS organization evaluated multiple vendors and chose the Guardium solution.

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

Environment

The BC BS infrastructure includes nearly 50 database instances in Production, Staging, Test, and Development environments, that need to be monitored for unauthorized or suspicious access. These databases support a range of financial, customer, and patient applications.

The Guardium solution is complementary to existing security investments such as perimeter firewalls, SSL VPNs, identity management, SIM/SEM, IDS, and configuration policy management. The following table summarizes how Guardium addresses the stringent requirements typically defined by BC BS organizations.

Functional Requirements

Customer required	Guardium provided
Produces information required for SOX, HIPAA, FISMA, CMS, DISA S-TIG, data privacy laws, and PCI	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 SOX and data 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.
Integrates easily into the existing environment	Guardium's non-invasive approach has virtually zero impact on performance (<5%) and does not require any changes to databases or applications.
Does not rely on database-resident functions that affect performance or stability, such as triggers, trace or transaction logs, or native auditing	The company's Data Security At-the-Switch™ architecture is network-based and database-independent. It continuously monitors a mirrored network stream – by simply connecting to standard SPAN ports on network switches or network taps – and analyzes all database traffic for suspicious or unauthorized activities. It does not require 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 polices 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 are detected, including changes to external database 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 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 relevant traffic to Guardium appliances for processing and analysis.
Secure, tamper-proof audit repository	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.

Management Requirements

Supports centralized management	The Guardium solution is based on a scalable, multi-tier architecture with centralized policy management and aggregation of audit data. All appliances are managed via a graphical Web console interface.
Integrates with existing management systems (Microsoft MOM, Cisco MARS, IBM Tivoli, etc.)	Supports standard interfaces including SNMP and SMTP as well as data export via CSV files.

Integrates with identity management systems	Supports LDAP and other authentication systems.
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.

About Guardium

Guardium, the database security company, develops the most widely-used solution for database activity monitoring, security and auditing. Founded in 2002, Guardium was the first company to address the core data security gap by delivering a practical, appliance-based platform that both protects databases in real-time and automates the entire compliance auditing process – without impacting performance or requiring changes to databases or applications. The company's blue-chip customer base includes organizations in all major geographies and industries.

Guardium's investors include Cisco Systems and leading venture capital firms. The company has partnerships with IBM, EMC, HP, Microsoft, Oracle, and Sybase and is a member of IBM's Data Governance Council.

230 Third Avenue • Waltham, MA 02451 • T: 781-487-9400 • F: 781-487-7900 • www.guardium.com