The Problem

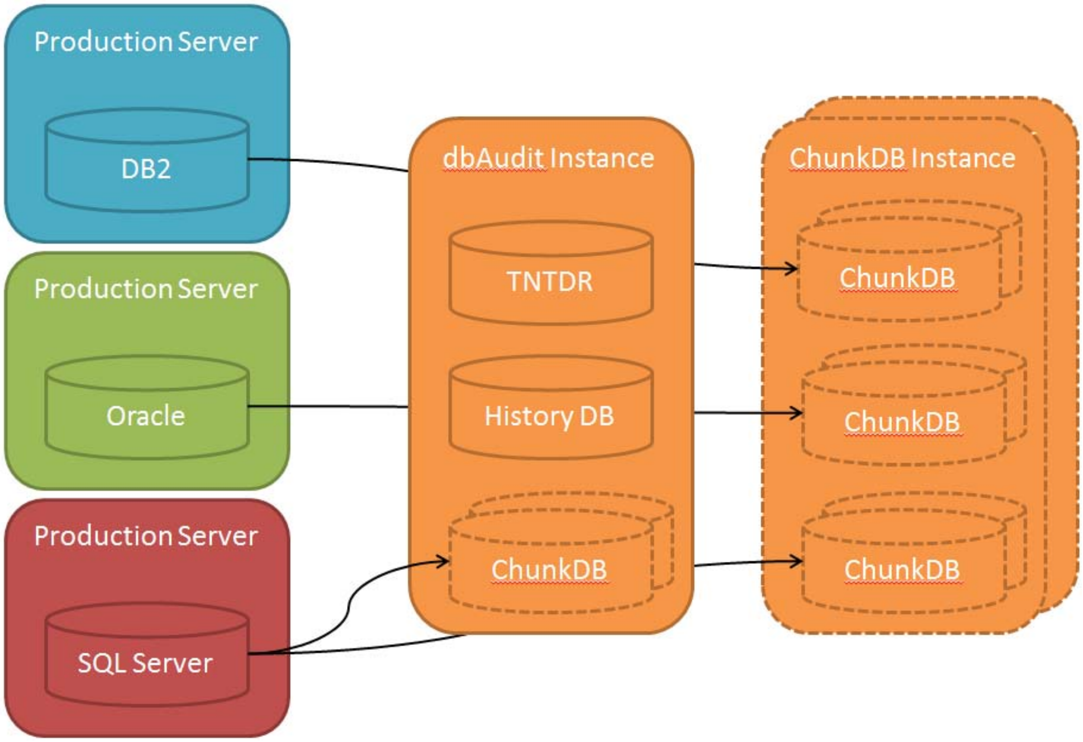
When you are responsible for the integrity of your database — be it banking information, insurance details, or customer information — the threat of a data breach can keep you awake at nights. Data integrity and security breaches have increasingly become front-page news and a chronic headache for IT professionals.

If you had to produce a history of every record change in a database, could you do it?   If the bank you work for is involved in accounts litigation, could you produce a forensic analysis of an account record and what values it contained at any given moment? Your ability to prove that a record had certain values and when it had those values can make or break a case in litigation.

Data security is often left to corporate programmers who create solutions specific to their applications. These solutions demand maintenance — an ongoing cost for the organization. RDBMS providers can offer features with which you, as a programmer, can implement data recording. But these features are reserved for enterprise editions of those databases, and they come with the enterprise price tag that very quickly runs into 6 or 7 figures for systems such as Oracle, Microsoft SQL Server, and IBM’s DB2.

The Solution

DBDefend’s DbAudit product offers data recording for any size database. DbAudit uses the intrinsic technologies that come with all major database management systems and can, therefore, be easily and quickly adapted to your database. It easily captures all change data for a wide range of database systems, including Oracle, Microsoft SQL server, DB2, Sybase, MySQL, MariaDB, and PostgreSQL.



dbAudit tracks INSERT/DELETE/UPDATE operations for fields/tables you configure:

- who made the change (i.e. the DB login)
- when the change happened
- what terminal/server made the change
- the before and after values of each field changed

The dbAudit GUI allows users to:

- configure which tables and columns are audited
- select predefined, application-specific data capture scenarios for easy setup
- start and stop auditing
- set alert conditions
- specify whether alert notifications are sent by email or text message, and to whom

With dbAudit, you can:

Create a history of single records. DbAudit tracks every event that occurs to the records in a database, making it easy to audit the trail of a record from creation to termination or archiving.

Helps meet SOX, HIPAA, and PCI requirements. DbAudit can be configured to monitor all changes to sensitive data, thus meeting requirements for many regulatory laws.

Optionally block any transaction that attempts to alter data above a configurable limits. The product can be configured to block SQL statements/transactions which modify over X sensitive fields, or change sensitive data values (e.g. a dollar balance) by more than Y percent.

Restore a single data record. With the data browser in DbAudit, you can choose exactly what version of a record should be restored to the production database.

Restore a single table. You can restore single tables, or all the tables, to the production database.

Restore a point in time. With DbAudit's restore feature, you can restore an entire database to a date and time you specify.

Produce a forensic analysis. All data captures receive a timestamp, which you can use to document the sequence of change events for each user and workstation.

Store data long-term. You can export historic data into immutable, encrypted files for later review or for use in forensic investigations.

Reporting for all sensitive record changes, including summaries by date/time with the ability to drill-down to individual events.

Use templates for data capture. DbAudit provides application-specific templates that you can use to capture data from the database. No need to know which of the 86000+ tables that an SAP installation includes are worth auditing. You can customize these templates for a specific application your company uses. In addition, you can set capturing criteria for these templates; set rules that will flag certain data; and send alerts to specific personnel when data is flagged.

Furnish delta data. DbAudit captures everything from single table columns, to all table columns, to all tables of the database. With this information, you can provide delta data for processing in a data warehouse.

Integrate custom applications. With the API feature of DbAudit, you can integrate your own applications.

dbAudit also comes with an API allowing controlling dbAudit and displaying/analyzing historic data from other applications.

Technical requirements:

Minimum RAM: 1 GB

Minimum free disk space: 20 GB

Operating systems supported for control and history databases
Windows 7 and higher

Windows Server 2008, and higher
License requirements: None. dbAudit operates on free SQL Server 2014 Express, but can also operate on any higher license

Supported production databases:

Microsoft SQL Server 2008 or higher

MySQL 5.0 and higher

Oracle 10g and

PostgreSQL 8.0 and higher (available 2017)

DB2 Ver. 9.1 and higher (available 2017)

Supported production operating systems:

Windows 7 and higher

Windows Server 2008 and higher

Linux, Unix

System capacities:

Databases monitored: 2^{31}-1 (roughly two billion) being operated on a maximum of 32,766 server

Maximum number of production server supported: 32,766

Maximum number of history instances (server or virtual server): 32,766

Maximum size of history database: 10,238 PetaByte

Maximum duration of data history: User definable

Minimum time between synchronization events: one second