



October 26, 2007

Oracle Is A Strong Performer In Enterprise Database Auditing; Tops Native DBMS Auditing

The Forrester Wave™ Vendor Summary, Q4 2007

by Noel Yuhanna

with Jonathan Penn and Katie Smillie

EXECUTIVE SUMMARY

Oracle is a Strong Performer across the board in our evaluation, and tops the native DBMS auditing solutions. Oracle is the technology leader when it comes to databases, and Oracle gives database security and auditing the same level of commitment and focus as other database features. Although Oracle's native auditing does not offer strong support for integration with applications, policy management, reporting, or centralized administration, it is nevertheless freely bundled with Oracle database management system (DBMS) making it an attractive option for enterprises. We find that with every new release of Oracle DBMS, Oracle continues to expand its auditing capabilities, specifically around performance, simplification, and auditing coverage, narrowing the gap with pure-play auditing vendors. Besides Oracle's native auditing, Oracle recently released the Audit Vault product, which offers more advanced auditing features including the ability to centralize auditing for large environments that deal with many databases.

ORACLE IS BEST SUITED TO SMALL TO MODERATE AUDIT REQUIREMENTS

Oracle, with annual revenue of approximately \$18 billion and 74,674 full-time employees as of May 31, 2007, has more than 250,000 mostly database customers. Besides its native auditing solution, Oracle offers the recently rolled out Audit Vault product that transparently collects and consolidates audit data to support large enterprise auditing requirements. Audit Vault offers enterprises wanting a more comprehensive auditing solution more reports, granular alert notification, and centralized repository and policy management. This is not freely bundled with the DBMS, but is an add-on option. Oracle Audit Vault was not evaluated in this Forrester Wave™ because it was just released in June 2007.

Forrester evaluated Oracle's current offering and strategy for enterprise database auditing and real-time protection against 116 criteria (see Figure 1). The product has strong support for alerting and notification, monitoring user activity, and integrating with other compliance solutions, but it lacks strong support for integrating with applications, policy management, reporting, centralized administration, and real-time database protection. This makes the Oracle native auditing solution an especially good fit for buyers that:

- **Are looking for simple auditing for their not too large or complex Oracle databases.** Although Oracle's native auditing solution does not have all the features normally provided by pure-play vendors' products, it offers basic auditing capabilities that suffice for many enterprises. In addition, Oracle's native auditing can be customized using scripts and SQL to satisfy more elaborate auditing requirements, but not without additional manual effort.

- **Don't have a huge budget for auditing.** Oracle's native auditing comes freely bundled with Oracle DBMS software, therefore it remains an attractive option for enterprises that don't have a huge budget. Forrester finds that many enterprises deploy both the native auditing and third-party vendor solutions to balance the audit requirements and maintain cost control.

To see how Oracle stacks up against 13 competitors, see the Forrester Wave evaluation of the enterprise database auditing and real-time protection market.¹

Figure 1 Oracle Native Auditing Evaluation Overview

CURRENT OFFERING

Levels of auditing	Oracle supports row-level, column-level, table-level, database-level, and DDL-level auditing and monitoring. Oracle supports basic and complex SELECT and DML queries. It can also audit triggers, stored procedures, and database views. Oracle provides the ability to monitor statements issued by any user or statements issued by a specific list of users from within the Oracle database. Oracle can audit if a packaged application runs on top of an Oracle database.
Application level support	The same Oracle database audit commands are used to audit application tables, as well as individual user access. Oracle provides a client identifier functionality for packaged applications to integrate with the database server to perform end user auditing.
Audit policies	Oracle does not have predefined policies; however, these can be created. In 11g, auditing is enabled by default and provides a script to audit security-related SQL statements and privileges. Oracle database auditing can be customized to address specific compliance and privacy requirements; however, they are not installed out-of-the-box. Oracle auditing, when enabled, generates an audit record during the execute phase of statement execution.
Monitoring and notification (alerting)	Oracle's auditing, when enabled, generates an audit record during the execute phase of statement execution. Oracle FGA provides the ability for a security officer to be notified via a custom procedure call to the database. Oracle audits all activity if it is executed over the network or directly on the host. Privileged user activity can be audited with a single "audit user" command.
Auditing repository	Oracle's audit records can be stored in the database audit tables or in files on the OS. Oracle's audit trail records can be written into an Oracle table. Oracle's native auditing does not support a centralized repository, unless implemented manually.
Reporting	Oracle's database does not provide out-of-the-box reports for audit trail data. Oracle's audit trail records can be stored in a database table. Reports to support SOX regulations such as failed logins, privileged user activity, and database changes may be created. Customers using Oracle Audit Vault can use the published data warehouse schema in conjunction with any reporting tool such as SQL*Developer or Oracle BI Publisher to create customized reports. Oracle Audit Vault is a separate product included for information only and has no effect on the score for this criteria.
Analytics and intelligence	Oracle's database does not analyze end-to-end transactions. However, Oracle database auditing writes all audit trail data defined by the security officer's policies, which is executed within the database. Oracle's database auditing monitors data access, which can be used to prevent future malicious activity.
Performance and scalability	Oracle claims that it performed an in-house testing on a two-CPU Linux x86 Server on Oracle Database 10g Release 2 (10.2.0.3). The internal tests showed that database auditing added an additional 1% CPU overhead when 1,000 or more audit trail records were created per second.

Source: Forrester Research, Inc.

Figure 1 Oracle Native Auditing Evaluation Overview (Cont.)

CURRENT OFFERING

Architecture	Oracle's database auditing is built into the Oracle kernel and does not require an agent. With non-native auditing solutions, agents may fail and audit records can be lost. Oracle's database auditing is native to the database; therefore, all platforms that the Oracle's database supports can collect audit trail data. Oracle's database auditing only supports Oracle databases.
Usability	Oracle's database auditing is controlled by a single database parameter. Once database auditing is turned on, a security officer can run the script to set up the audit policy. Oracle's auditing is native therefore administration efforts are minimal. The user can create policies and manage audit logs. Enterprise Manager Grid Control provides a centralized browser facility for managing database audit policies. Oracle Audit Vault provides a centralized browser console to verify and update audit policies for all managed databases. Oracle Audit Vault is a separate product included for information only and has no effect on the score for this criteria.

STRATEGY

Product strategy	Oracle is continuing to add more audit features including support for Audit Vault and default audit policies in Oracle Database 11g. Oracle Database 11g Release 1 will provide certifications. Oracle has more than 19,500 partners. Oracle Audit Vault is a separate product included for information only and has no effect on the score for this criteria.
Corporate strategy	Oracle is very committed to delivering auditing solutions, and recently released two products, Audit Vault and Oracle Database Vault, that extend the auditing and monitoring capabilities. These products are not part of our evaluation and have no effect on the score for this criteria.
Cost	Oracle's database auditing is native to the database and is included as part of the licensing cost. However, Audit Vault is a priced option and not included in this evaluation.

MARKET PRESENCE

Installed base	Forrester estimates that 40% of Oracle enterprise customers are using the native DBMS auditing solution. Oracle has 250,000 customers, of which the majority are database customers.
Revenue	Oracle's revenue is \$17.996 million. Oracle's total company revenue grew by 25% from FY 2006 to FY 2007.
Services	Oracle offers classroom, Web-based, and on-site training for database auditing. Oracle has a large consulting organization with expertise in many industry verticals.
Employees	Oracle has 18,130 employees in R&D. Oracle has 74,674 full-time employees as of May 31, 2007.
Technology partners	Oracle has more than 19,500 partners.
International presence	Oracle has offices in 126 countries all over the world.

Source: Forrester Research, Inc.



Go online to download additional in-depth data and scores for this vendor and other vendors included in this Forrester Wave evaluation.

SUPPLEMENTAL MATERIAL

Online Resource

The underlying spreadsheet for Figure 1 is available online. The spreadsheet includes more detailed data and scores for this vendor.

This detailed data and scores for this vendor are also available online through an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and readers are encouraged to adapt the weightings to fit their individual needs using the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

ENDNOTES

- ¹ Forrester's evaluation of leading enterprise database auditing and real-time protection vendors across 116 criteria found Guardium and Imperva to have established leadership positions thanks to their enterprise database auditing capabilities, breadth of focus, and strong product and corporate strategy. Tizor Systems, Application Security, and Lumigent Technologies also emerged as Leaders able to handle and support most enterprise database auditing requirements. Symantec, IBM Consul InSight (recently rebranded Tivoli Compliance Insight Manager), RippleTech, Embarcadero Technologies, and Oracle are Strong Performers best suited, because they lack a comprehensive set of auditing, real-time protection, and other features and functionality, to basic to moderate auditing requirements. Oracle's database management system (DBMS) tops other DBMS vendors by having the best set of native auditing features; Microsoft, Sybase, and IBM DB2 trail, largely because they have only basic auditing capabilities. Although IBM Audit Management Expert (AME) offers only basic auditing capabilities, it integrates well with IBM's DB2 and IMS DBMSes running on the mainframe. See the October 26, 2007, "[The Forrester Wave™: Enterprise Database Auditing And Real-Time Protection, Q4 2007](#)" report.