May 6, 2011

The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011

by Noel Yuhanna
for Application Development & Delivery Professionals

May 6, 2011

The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011

IBM, Imperva, And Sentrigo Lead, With Application Security, Oracle, And Fortinet Close Behind

by Noel Yuhanna
with Stephanie Balaouras and Adam Knoll

EXECUTIVE SUMMARY

In Forrester's 147-criteria evaluation of database auditing and real-time protection vendors, we found that the market is rife with mature products. IBM, Imperva, and Sentrigo lead the pack because of their strong user activity auditing, policy management, real-time protection, and application support capabilities as well as their forward-thinking strategies. Application Security, Oracle, and Fortinet are Strong Performers; their products have reporting, real-time detection and protection, and user-activity auditing capabilities that are slightly weaker than capabilities of the Leaders' offerings. However, all of the products we evaluated are mature database auditing and real-time protection solutions. Given this, rather than basing their choice of database auditing and real-time protection product on traditional auditing functions, application development and delivery professionals should base their decision on the more cutting-edge functionality, such as real-time attack activity blocking, privileged-user monitoring, drilldown analytics, and centralization repository.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester conducted product evaluations in October 2010 and interviewed 20 vendor and user companies to evaluate the database auditing and real-time protection offerings of Application Security, Fortinet, IBM, Imperva, Oracle, and Sentrigo.

Related Research Documents

"Creating An Enterprise Database Security Plan" July 29, 2010

"Your Enterprise Database Security Strategy 2010" September 28, 2009

"Market Overview: Database Security" February 27, 2009

DATABASE AUDITING AND REAL-TIME PROTECTION ADOPTION HAS GROWN

Database auditing has become critical to all enterprises for dealing with various regulatory compliance and security requirements. Database auditing focuses on answering data access questions such as: "Who accessed the credit card numbers?"; "When did someone change a customer's address?"; "What was the old content prior to the change?"; and "What application was used to access the sensitive data?" Although the fundamental approach to database auditing has not changed in decades, the focus has now shifted to more-in-depth, granular data audit analysis, centralized audit administration across hundreds and thousands of databases, comprehensive audit reporting, role separation, and real-time protection. In addition, the need to audit database administrators and other privileged users has grown, especially as auditors and security groups look at nailing down sensitive data to meet various regulatory compliance requirements such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and the Sarbanes-Oxley Act (SOX). Stopping attacks in real time has become vital to all organizations, especially as these attacks have become sophisticated and difficult to detect. It takes a hacker less than 20 seconds to execute a query and retrieve sensitive information once he has broken into an application or database. Because it is not possible for a human to detect such attacks, the need for real-time database protection has become critical.

The database auditing and real-time protection products evaluated in this Forrester Wave™ help organizations:

- **Meet regulatory compliance requirements.** Database auditing is a best practice that all enterprises that deal with sensitive data such as credit card numbers, Social Security Numbers, personally identifiable information (PII), personal health information (PHI), or any other company confidential data should deploy. If you are dealing with any of the compliance requirements related to PCI, HIPAA, GLBA, or SOX, enabling database auditing for databases that deal with sensitive data has become a necessity. Today, most auditors emphasize turning on database auditing to track each and every activity related to sensitive data.

- **Secure databases from attacks and data theft.** Most enterprises today are dealing with hundreds if not thousands of databases in their environment, and many of those databases contain company confidential data. It's very difficult to manually detect suspicious database activities and block data access in real time. Database auditing and real-time protection solutions can proactively monitor database access, alert database administrators (DBAs) and security professionals, and block connections and sessions in real time.

- **Build a more comprehensive data security strategy.** A critical component in building a successful data security strategy is database auditing and real-time protection, along with data-at-rest encryption, data masking, entitlement management, and vulnerability assessment.[1]

The Database Auditing Market Is Mature And Consolidating

When it comes to security, databases are not intelligent enough to differentiate a user from a hacker or determine if data is sensitive in nature. Besides helping organizations meet regulatory compliance requirements, database auditing and real-time protection solutions also enhance their security. Three years ago, enterprises were looking to audit and protect a few critical databases that held sensitive data. Today, the focus has shifted to protecting hundreds and thousands of databases across the enterprise, with many organizations looking for an enterprise database auditing and real-time protection solution that offers centralized administration, role separation, policy management, high performance, data discovery, and classification and simplified management.

Forrester estimates the database security market — which including new licenses, support, and services — at approximately $650 million and expects it to double by 2015 as more enterprises look at an enterprisewide auditing strategy. Today, the top database auditing and real-time protection vendors include Application Security, Fortinet, IBM, Imperva, Oracle, and Sentrigo.[2] The database security market is mature but has consolidated over the years, with acquisitions such as: Sentrigo by McAfee, IPLocks by Fortinet, Tizor Systems by Netezza, Netezza by IBM, Guardium by IBM, and Secerno by Oracle. Some large vendors have even tried entering the database security space on their own but didn't fare well and eventually had to kill the product line. These include Symantec Database Security and Quest Software's InTrust product for databases.

The enterprise database auditing and real-time protection market breaks down into two major segments:

- **Native database management systems (DBMSes) offer basic auditing capability.** Every major DBMS product — including those from IBM, Ingres, MarkLogic, Microsoft, Oracle, and Sybase — offers native auditing capabilities to support producing basic audit trails on access and changes. Although these features are good enough for small and less-complex implementations, they lag when it comes to reporting, role separation, real-time protection, and supporting a large farm of databases. Forrester believes that DBMS vendors will continue to add more-advanced native auditing features in the coming years, bridging the gap between their offerings and those from leading third-party vendors.

- **Third-party vendors offer comprehensive auditing solutions.** Today, a dozen vendors offer database auditing and real-time protection solutions. Some of these vendors are very large, such as Fortinet, IBM, and Oracle, and others are startup companies, such as Application Security, Imperva, and Sentrigo. The vendors primarily offer two types of architecture: 1) network-based appliance, and 2) software-based. Most of the adoption today has been around the software-based type of architecture; these solutions are either agentless or agent-based, and they read audit information from database shared memory, database logs, and process connections. Regardless of their architecture, third-party vendor solutions focus strongly on simplification, role separation, policy management, centralized administration, and compliance reporting.

DATABASE AUDITING AND REAL-TIME PROTECTION EVALUATION OVERVIEW

To assess the state of the database auditing and real-time protection market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of six of the top database auditing and real-time protection vendors.

Evaluation Criteria: Current Offering, Strategy, And Market Presence

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 147 criteria, which we grouped into three high-level buckets:

- **Current offering.** To assess product strength, we evaluated eight high-level categories of current offering criteria: database auditing, user and application auditing, audit policies, auditing repository, reporting and analytics, real-time protection, architecture, and manageability.
- **Strategy.** We reviewed each vendor's strategy and considered planned enhancements for positioning products to meet future customer demands. We also looked at the financial resources available to support the company's product, go-to-market pricing, and corporate strategy.
- **Market presence.** To establish a product's market presence, we combined information about each vendor's installed base, financial performance, services, employees, technology partners, and international presence.

Evaluated Third-Party Vendors Have Credible Deployments And Enterprise-Level Solutions

Forrester included six third-party vendors in the assessment: Application Security, Fortinet, IBM, Imperva, Oracle, and Sentrigo. Each of these vendors has (see Figure 1):

- **An enterprise-class database auditing solution.** We included only those third-party vendors that have recognized the growing need to support database auditing requirements with a special focus on products that offer high performance and scalability, reporting, policy management, and ease of use beyond native DBMS auditing features. The product had to be readily available as of August 15, 2010.
- **Visibility in the auditing space.** We included only those third-party database auditing and real-time protection vendors that customers mentioned in Forrester inquiries at least 10 times during the past year.
- **A credible installed base.** We evaluated third-party vendors that had a customer base of 100 or more enterprise customers. All of the evaluated vendors met this criterion.

Figure 1 Evaluated Vendors: Product Information And Selection Criteria

Vendor	Product evaluated	Product version evaluated	Version release date
Application Security	DbProtect	Version 6.1	June 2010
Fortinet	FortiDB	Version 4.1	July 2010
IBM	InfoSphere Guardium	Version 7.0	July 2008
Imperva	SecureSphere Data Security Suite	Version 8.0	July 2010
Oracle	Audit Vault	Version 10.2.3	June 2008
Sentrigo	Hedgehog Enterprise	Version 4.0	August 2010

Vendor selection criteria
The product offers a comprehensive enterprise-class database auditing solution that can help meet regulatory compliance requirements and protect data against theft, including offering compliance reporting, role separation, real-time data protection, storage of audit trails, and automation of auditing process and procedures.
The product was mentioned by Forrester clients in 10 or more inquiries in the past 12 months.
The product must have a customer base of 100 or more enterprise customers.
The product must be readily available as of August 15, 2010.

Source: Forrester Research, Inc.

MOST DATABASE AUDITING VENDORS ARE NOW OFFERING COMPREHENSIVE SOLUTIONS

The evaluation uncovered a market in which (see Figure 2):

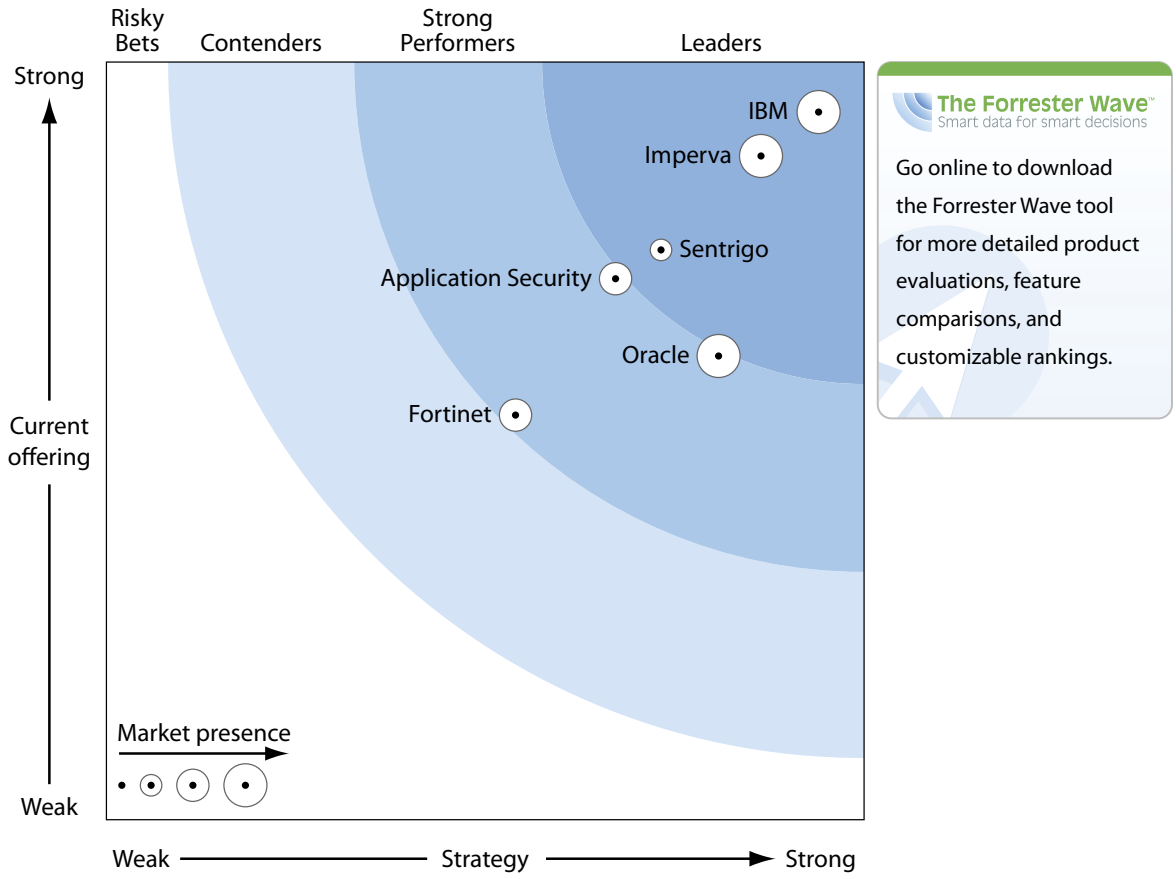
- **IBM, Imperva, and Sentrigo lead the pack.** These vendors offer strong support for most database auditing features and functionality to meet any enterprise auditing requirements. IBM InfoSphere Guardium offers support for almost any of the features that one might find in an auditing and real-time protection solution. InfoSphere Guardium offers strong support for database-access auditing, application auditing, policy management, auditing repository, and real-time protection. Imperva's SecureSphere Data Security Suite offers strong real-time protection, reporting and analytics, user-activity auditing, and policy management. Sentrigo Hedgehog Enterprise is strong in audit policies, performance, ease of use, compliance reports, and policy management.

- **Application Security, Oracle, and Fortinet offer competitive options.** Application Security DbProtect has done well considering that the vendor has focused primarily on vulnerability assessments for years. DbProtect has good features around audit policies, compliance reporting,

ease of use, performance, centralized repository, and user and privileged-user auditing. Oracle continues to extend its security focus each year; it has done well with its Audit Vault and Database Vault products and is now filling the gap in its database firewall capability with the acquisition of Secerno. Oracle is strong in data auditing, auditing repository and access, notification and alerting, and user activity and privileged-user auditing. Fortinet FortiDB gained entry into the database security market with the acquisition of IPLocks in 2008 and has done well over the years, offering enterprises a lower-cost solution that can support any small to moderately sized auditing requirements.

This evaluation of the database auditing and real-time protection market is intended to be a starting point only. We encourage readers to view detailed product evaluations and adapt the criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

Figure 2 Forrester Wave™: Database Auditing And Real-Time Protection, Q2 '11



Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Database Auditing And Real-Time Protection, Q2 '11 (Cont.)

	Forrester's Weighting	Application Security	Fortinet	IBM	Imperva	Oracle	Sentrigo
CURRENT OFFERING	50%	3.57	2.67	4.67	4.38	3.06	3.76
Database auditing	10%	3.81	3.51	4.88	4.40	3.92	4.12
User and application auditing	15%	3.08	2.56	4.68	4.44	2.68	3.56
Audit policies	10%	3.90	3.30	5.00	4.60	3.20	4.60
Auditing repository	10%	3.80	3.24	5.00	4.04	4.52	4.28
Reporting and analytics	10%	4.46	3.44	4.76	4.64	3.40	3.56
Real-time protection	15%	2.70	1.10	4.80	4.80	2.20	4.20
Architecture	15%	3.57	3.00	4.19	4.15	3.17	2.94
Manageability	15%	3.80	2.15	4.40	4.04	2.29	3.35
STRATEGY	50%	3.36	2.70	4.70	4.32	4.04	3.66
Product strategy	60%	2.80	2.50	4.50	4.40	3.40	3.30
Corporate strategy	40%	4.20	3.00	5.00	4.20	5.00	4.20
Cost	0%	0.00	0.00	0.00	0.00	0.00	0.00
MARKET PRESENCE	0%	3.69	3.49	4.92	4.18	4.88	2.64
Installed base	20%	3.00	2.00	5.00	5.00	5.00	2.00
Revenue	10%	2.60	4.00	4.20	2.40	3.80	2.60
Services	20%	3.60	5.00	5.00	2.90	5.00	2.20
Employees	20%	4.05	4.25	5.00	4.30	5.00	2.40
Technology partners	20%	5.00	1.70	5.00	5.00	5.00	3.68
International presence	10%	3.00	5.00	5.00	5.00	5.00	3.20

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders: IBM, Imperva, And Sentrigo

- **IBM's acquisition of Guardium helps it move to a Leader position.** IBM was a Strong Performer in the Q4 2007 Forrester Wave evaluation of the database auditing and real-time protection market, in which we evaluated IBM Consul InSight and IBM DB2 Audit Management Expert (AME). However, IBM's acquisition of Guardium in 2009 changed everything, making IBM one of the leading players in this market. IBM InfoSphere Guardium continues to demonstrate its leadership in supporting very large heterogeneous environments, delivering high performance and scalability, simplifying administration, and performing real-time database protection. IBM continues to focus on innovation and extending the Guardium product to integrate with other IBM products such as InfoSphere Discovery and InfoSphere Optim. Today, IBM InfoSphere Guardium has been deployed across many large enterprises

and hundreds of mission-critical databases. In addition, IBM offers comprehensive professional services to help customers with complex environments as well as those who need assistance implementing database security across their enterprise.

- **Imperva remains close on IBM's heels.** Imperva has done extremely well over the years despite now competing against bigger giants such as Fortinet, IBM, and Oracle. Imperva is a Leader with a strong-performing and scalable database auditing solution that received high scores in most of the areas we evaluated. Imperva has strong support for auditing and compliance reporting, transaction and query auditing, real-time discovery, user-level and privileged-user auditing, policy definition and compliance policies, notification and alerting, and real-time protection. Imperva also has a strong product and corporate strategy, and its strong market presence should help it further increase growth in the coming years. Imperva continues to be one of the most aggressive vendors in the database auditing space. Besides database security, Imperva also offers web application and file security solutions. Forrester believes that Imperva is likely to be a target for acquisition by a large security vendor in the coming years.

- **Sentrigo does extremely well to gain a spot as a Leader.** Sentrigo was recently acquired by McAfee as this Forrester Wave was being published. The Sentrigo Hedgehog Enterprise product is now known as McAfee Database Activity Monitoring, and the Sentrigo Hedgehog DBscanner product is now known as McAfee Vulnerability Manager for Databases. Sentrigo, founded in 2006, offers several database security solutions, including database auditing, vulnerability assessment, data discovery, virtual patching, and real-time protection. Sentrigo received strong scores for its audit policies, ease of use, real-time attacks detection, end-to-end analysis, and compliance reporting. It also has strong product vision, commitment, and partners. Although Sentrigo does not have as many customers as IBM or Imperva, it has some very large Fortune 1000 companies that are using its product to support hundreds of critical databases.

Strong Performers: Application Security, Oracle, And Fortinet

- **Application Security offers a viable database auditing solution at an attractive price.** Application Security, founded 10 years ago, leads in database vulnerability assessments and continues to extend its DbProtect product that supports database auditing and real-time protection. However, Application Security has faced stiff competition from vendors such as IBM, Imperva, and Oracle over the years. Application Security is a Strong Performer across the board in our evaluation. It received strong scores for its user activity monitoring, compliance reporting, drilldown analytics, real-time attacks detection, and performance.

- **Oracle offers a comprehensive database security solution that goes beyond auditing.** Oracle is the vendor offering the most comprehensive database security solution; the Oracle solution includes database auditing, data masking, vulnerability assessment, data discovery, label security, data-at-rest encryption, entitlement management, and patch management. Oracle is a Strong Performer across the board in our evaluation and continues to remain committed to security

solutions. In addition, Oracle is the only DBMS vendor with a solution that offers protection of sensitive data from DBAs at the database level (the Oracle Database Vault product). Oracle recently released its Database Firewall product, which offers real-time protection and strong user and access auditing; this product is a good complement to Oracle's Audit Vault and Database Vault product line. Because our cutoff date for production evaluation was set as August 15, 2010, we did not evaluate the Oracle Database Firewall product.

- **Fortinet offers a viable solution for database security at a low cost.** Fortinet acquired IPLocks in 2008 to enter the database security market. Overall, Fortinet has done well since the acquisition, and today it has more than 100 customers, half of which are large Fortune 500 companies. Although, Fortinet's core focus is network security appliances and unified threat management (UTM), database security remains an important focus. Fortinet's strong capabilities lie in its integration with native database security, reporting, proactive alerting, custom policies, and user-level and transaction-level auditing. Fortinet is likely to face stiff competition ahead as vendors further consolidate. Fortinet needs to remain focused and innovate in order to stay competitive.

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of two data sources to assess the strengths and weaknesses of each solution:

- **Product demos.** We asked vendors to conduct demonstrations of their product's functionality. We used findings from these product demos to validate details of each vendor's product capabilities.

- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with two of each vendor's current customers.

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 we encourage readers to adapt the weightings to fit their individual needs through 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] For more research on building a comprehensive database security strategy, see the September 28, 2009, "Your Enterprise Database Security Strategy 2010" report.

[2] Sentrigo was recently acquired by McAfee as this Wave was being published.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Forrester has research centers and sales offices in more than 27 cities internationally, including Amsterdam; Cambridge, Mass.; Dallas; Dubai; Foster City, Calif.; Frankfurt; London; Madrid; Sydney; Tel Aviv; and Toronto.

For a complete list of worldwide locations visit www.forrester.com/about.

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 27 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

FORRESTER®