October 26, 2007

The Forrester Wave™: Enterprise Database Auditing And Real-Time Protection, Q4 2007

by Noel Yuhanna
for Security & Risk Professionals

FORRESTER® Making Leaders Successful Every Day

October 26, 2007

The Forrester Wave™: Enterprise Database Auditing And Real-Time Protection, Q4 2007

Guardium And Imperva Lead, With Tizor Systems, Application Security, And Lumigent Technologies Following Closely; Oracle Tops Native Auditing

by Noel Yuhanna
with Jonathan Penn and Katie Smillie

EXECUTIVE SUMMARY

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 renamed 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.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester conducted product evaluations from June to August 2007 and interviewed 12 vendor and 22 user companies including Application Security, Embarcadero Technologies, Guardium, IBM, Imperva, Lumigent Technologies, Microsoft, Oracle, RippleTech, Sybase, Symantec, and Tizor Systems.

Related Research Documents

"Enterprise Databases Need Greater Focus To Meet Regulatory Compliance Requirements" January 24, 2007

"The Forrester Wave™: Database Encryption Solutions, Q3 2005" August, 8, 2005

DATABASE AUDITING AND REAL-TIME PROTECTION HAVE BECOME NECESSITIES FOR ALL

Database auditing focuses on answering fundamental data access questions like "Who changed the data?", "When was the data changed?", and "What was the old content prior to the change?" In the past, database auditing was focused primarily on ensuring the accuracy of financial data and largely driven by the requirements of external auditors. Today's requirements have expanded to embrace auditing all types of data including personal data that contains credit card and Social Security numbers, financial and health-related information, and company confidential information. The need to audit privileged users like database administrators (DBAs) and IT professionals has also increased over the years as external auditors and security groups look to more completely guard access to private data. Although the approach to database auditing has not changed in decades, the focus has shifted to more in-depth data access analysis, higher performance and greater scalability, comprehensive audit reporting, role separation, and centralized audit administration across hundreds of databases.

There is as well a growing need for real-time data protection to meet regulatory compliance requirements and mitigate risk against various types of threats to enterprise databases. Because hackers will always find new ways to breach security, enterprises must keep abreast of the latest security technologies including real-time protection. It takes a hacker less than 20 seconds to execute a query and retrieve confidential data once an application or database is broken into. Because it is not humanly possible to detect such attacks, the need for real-time database protection has become a critical requirement, and adoption will further grow as enterprises look to automate their auditing and real-time protection environments.

Database auditing and real-time protection products help organizations:

- **Meet compliance requirements.** Although many legislative mandates do not explicitly spell out data security options, database auditing is always viewed as a best practice that should be employed for enterprises' critical databases. Some compliance requirements like PCI Data Security put special emphasis on cardholder data, requiring a complete audit trail not only of which data was changed and by whom, but also of who accessed the data. In addition, the HIPAA regulation requires that enterprises not only secure personal healthcare related information, but also track unauthorized access to such information including access by DBAs and others.

- **Secure critical databases from data theft.** In many enterprises, databases manage hundreds and thousands of data access requests per minute. It is next to impossible to manually detect suspicious activities and block services in real time. Auditing and real-time protection cannot only alert DBAs and IT professionals, but also block connections and sessions in real time.

- **Meet internal and external audit requirements.** Internal and external auditors are now requiring complete nail down of all private data in applications and databases. Forrester estimates that in most industries fewer than 15% of enterprise databases contain private data, but in some (like financial services) the figure can be as high as 80%. Auditing is one of the

recommended measures that often satisfies auditors' data security requirements. The ability to look at historical audit data to determine who changed it and, when helps keep data protection and management under a magnifying glass.

- **Reduce the risks of data breach.** Any breach of security can have a potentially huge impact on a business in the form of fines, lawsuits, effect on stock prices, and revenue loss. Although advanced database security measures do not guarantee freedom from attacks, they can minimize risks. They're like your car insurance, the value of which typically isn't realized until your car is damaged or stolen.

Database Auditing Market Is Hot

Today, most enterprises face a daunting task in trying to secure their enterprise databases in order to meet regulatory compliance requirements and prevent unauthorized break-ins. Because DBMS technology is still evolving with respect to being able to prevent all kinds of attacks, for now enterprises need to rely on advanced database security measures like data-at-rest encryption, auditing, vulnerability assessment, and real-time monitoring to mitigate risk. Two years ago, enterprises were looking to audit and protect one or two critical databases that held private data. Today, the focus has shifted to protecting hundreds of databases across enterprises giving rise to a pressing need for centralized administration, role separation, policy sharing, private data discovery, and simplified installation.

Forrester estimates the value of the database auditing and real-time protection market, which includes new licenses, support, and services, at approximately $450 million, and expects it to double by 2010 as enterprises look to automate and secure even more of their enterprise databases. The market size includes revenue from DBMS vendors that charge for auditing and monitoring products, third-party solutions, and consulting organizations that provide customized services. Companies in this space, from the smallest to the largest, all claim to cure enterprises' database security woes. The enterprise database auditing and real-time protection market breaks down into two major segments:

- **Native DBMS auditing solutions offer some auditing and real-time protection capabilities.** Although native DBMS auditing solutions are less functional than pure-play vendor solutions, they remain an attractive option, especially since they are freely bundled with the DBMS product. Some third-party vendors build on the native DBMS auditing features to provide a more comprehensive auditing solution. A major customer concern around native auditing solutions is the performance impact on database servers, an issue still in evidence today in very large or complex database environments. But DBMS vendors will continue to add more advanced native auditing features over time, bridging the gap that leading third-party vendors enjoy today.

- **Pure-play vendor solutions offer comprehensive features, but at a price.** Database auditing solutions are currently offered by more than two dozen vendors, mostly small startup companies with few customers. There are primarily two types of architectures being offered by third-party solutions: 1) network-based appliances, and 2) software-only solutions. Network-based appliances sniff SQL packets coming into the database and store them in a repository. Software-only solutions, which can be agentless or agent-based, read audit information by polling the database shared memory, pulling the database transaction logs for change activity, using host-based agents to track requests for database access, or all three. Some vendors like Guardium and Imperva complement their network appliance with a host-based agent that captures activity not initiated over the network like local DBA access. Regardless of the architecture, third-party vendor solutions focus more strongly on automation, simplicity, role separation, policy management, centralized administration, compliance reporting, and reduced performance impact.

ENTERPRISE DATABASE AUDITING AND REAL-TIME PROTECTION EVALUATION OVERVIEW

Forrester assessed the state of the enterprise database auditing and real-time protection market and evaluated the strengths and weaknesses of top enterprise database auditing and real-time protection vendors to see how they stacked up against each other.

Evaluation Criteria: 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 (see Figure 1). Ultimately, we evaluated vendors against 116 criteria grouped into three high-level buckets:

- **Current offering.** To assess product strength, we evaluated each offering against ten groups of criteria: levels of auditing, application level support, audit policies, monitoring and notification, auditing repository, reporting, analytics and intelligence, performance and scalability, architecture, and usability.

- **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 strategies.

- **Market presence.** To establish a product's market presence, we combined information about each vendor's financial performance, installed base, technology partners, and international presence.

Figure 1 Evaluation Criteria

CURRENT OFFERING	
Levels of auditing	How strong is the vendor's support for various levels of database auditing including data level, stored procedures, triggers, views, and user/database administrator (DBA) activity?
Application level support	How strong is the vendor's support for applications? Can the product audit access per individual application user, even when a pooled connection method is used to access the database?
Audit policies	How strong is the vendor's audit policies? Does it offer predefined policies out of the box? What about custom policies? How strong is the product's ability to support advanced policies? Does it support compliance policies for SOX, PCI, HIPAA, and GLBA?
Monitoring and notification (alerting)	How strong is the product's support for auditing data collection for real-time monitoring and auditing? Can it monitor all of the user activity that comes over the network or is executed on the host? Does it support monitoring privileged users? How strong is the product's ability to support notification/alerts?
Auditing repository	How strong is the vendor's audit repository? What are the storage requirements? How strong is the product's ability to secure and back up audit data? Does it offer a centralized repository?
Reporting	How strong is the vendor's support for audit reports? Does it offer predefined reports? How strong is the product in customized reporting? How strong is the product's ability to support compliance reports such as SOX, PCI, GLBA, and HIPAA?
Analytics and intelligence	How strong is the vendor's support for analytics and intelligence? Can it detect fraud and provide response data auditing? Does it provide support for known attacks and vulnerabilities? Does it offer automated data discovery of sensitive data?
Performance and scalability	Can the product support very large volumes of database activity? How many activities per second can the product monitor? What is the impact of adding additional policies on the performance of the solution? What is the impact of native DBMS auditing on the solution?
Architecture	How strong is the vendor's integration with the environment, i.e., operating system, DBMS, network, and application? How strong is the vendor's integration with the server? What operating systems does it support? What DBMS does it support?
Usability	How strong is the product's ease of use and deployment? How strong is the product in ongoing administration? Does it support centralized administration?

Source: Forrester Research, Inc.

Figure 1 Evaluation Criteria (Cont.)

STRATEGY	
Product strategy	How strong is the vendor's product strategy? What major certifications does it have? Who are the key technology partners?
Corporate strategy	How committed is the vendor? Does it have the financial resources to support the strategy? Does it have the ability to execute?
Cost	How much does the tool cost on average?
MARKET PRESENCE	
Installed base	How large is the vendor's installed base of customers for this product and for all products?
Revenue	What was the vendor's total revenue during the most recent four quarters? At what rate has the vendor's product revenue grown?
Services	How strong are the vendor's implementation and training services?
Employees	How many engineers does the vendor have dedicated to this platform? How big is the vendor's sales presence?
Technology partners	How strongly do technology partners support this product?
International presence	How is the vendor's international presence?

Source: Forrester Research, Inc.

Evaluated Vendors Met Enterprise Auditing Requirements With Credible Deployments

Forrester included 12 vendors in the assessment: Application Security, Embarcadero Technologies, Guardium, IBM, Imperva, Lumigent Technologies, Microsoft, Oracle, RippleTech, Sybase, Symantec, and Tizor Systems. Each of these vendors has (see Figure 2):

- **Enterprise-class database auditing capability.** We included 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, user management, and ease of use.
- **Native auditing capability in their DBMS offerings.** We included the top DBMS vendors, Oracle, Microsoft, Sybase, and IBM, to compare theirs' with third-party vendor products' native database auditing and real-time protection capabilities.
- **Credible installed base.** We evaluated third-party vendors that had a customer base of 40 or more customers. Application Security, Embarcadero Technologies, Guardium, Imperva, Lumigent Technologies, RippleTech, Symantec, and Tizor Systems met this criterion.

ENTERPRISE DATABASE AUDITING CAN BE IMPLEMENTED IN DIFFERENT WAYS

The evaluation uncovered a market in which (see Figure 3):

- **Guardium, Imperva, Tizor, Application Security, and Lumigent lead the pack.** These vendors offer strong support for most database auditing features and functionality to meet any enterprise auditing requirements. Guardium offers strong application integration as well as analytics and intelligence. Imperva's SecureSphere offers strong audit policies, reporting, and behavioral and intelligent analysis. Tizor's Mantra has strong file auditing integration, end-to-end security analysis, and response data collection. Application Security and Lumigent, software-only vendors, have a database transactional log, network, and shared memory to capture complete audit information, and an extremely flexible architecture that supports integration with native auditing solutions.

- **Symantec and RippleTech are hot on the heels of the Leaders.** Symantec came out with Symantec Database Security (SDS) solution about a year ago and has done reasonably well to gain a spot in the Strong Performer's category, especially considering that the product was developed from the ground-up and positioned to compete against the products of well-established pure-play vendors. RippleTech has good features and functionality in general, and at a very attractive price, but lacks strong integration with packaged applications, response data analysis, and end-to-end auditing analysis capability across the technology stack.

- **Embarcadero and IBM Consul InSight offer competitive options.** Although the products of these vendors do not have all the capabilities found in those of vendors in the Leader's category, they offer good auditing options with sufficient features to audit databases. Embarcadero offers credible capabilities around repository management, compliance reports, performance, and ongoing administration, but does not support predefined policies, blocking user connections and know attacks, or integrating with file-level auditing. IBM Consul InSight (now named IBM Tivoli Compliance Insight Manager), has strong capabilities around policies and audit and compliance reporting, but lags in fraud detection, response auditing, and end-to-end analysis.

- **Oracle offers a competitive option; it leads DBMS native auditing.** Oracle has done well in gaining a spot in the Strong Performer's category considering that it is a native DBMS auditing solution. Although Oracle now has a more advanced auditing solution called Audit Vault as an add-on option, we did not evaluate it because it became generally available only in June 2007.

- **IBM DB2 AME must improve features to compete with pure-play vendors.** IBM DB2 Audit Management Expert (AME) currently supports only the mainframe environment. It offers basic support for reporting, policies, and alerting, but lacks advanced features such as analytics and intelligence, integration with packaged and file-level auditing, and integration with other compliance solutions.

- **Microsoft, Sybase, and IBM DB2 lag in native auditing.** These vendors offer only auditing capabilities for low to moderate requirements, and often require manual efforts to administer, alert, and report. Most of these vendors tend to rely on third-party vendors to offer more complete auditing solutions. Microsoft's SQL Server native database auditing offers basic-level functionality around monitoring user and DBA activity, and some reporting capability, but lags in comprehensive policy management, integration with applications, alerting and notifications, centralized administration, and fraud analysis. Sybase's native database auditing solution offers some level of support for auditing user and DBA activity, but provides no support for alerting and notifications, predefined reports and policies, and analytics and intelligence. Sybase also has a product called Sybase Data Auditing, which is a rebranded Lumigent product. IBM DB2 native auditing offers basic database auditing features, and IBM promotes IBM TCIM and AME products when customers want a more comprehensive auditing solution.

This evaluation of the enterprise database auditing and real-time protection market is intended to be a starting point only. Readers are encouraged to view detailed product evaluations and adapt the criteria weightings to fit their individual needs using the Forrester Wave™ Excel-based vendor comparison tool.

Figure 2 Evaluated Vendors: Product Information And Selection Criteria

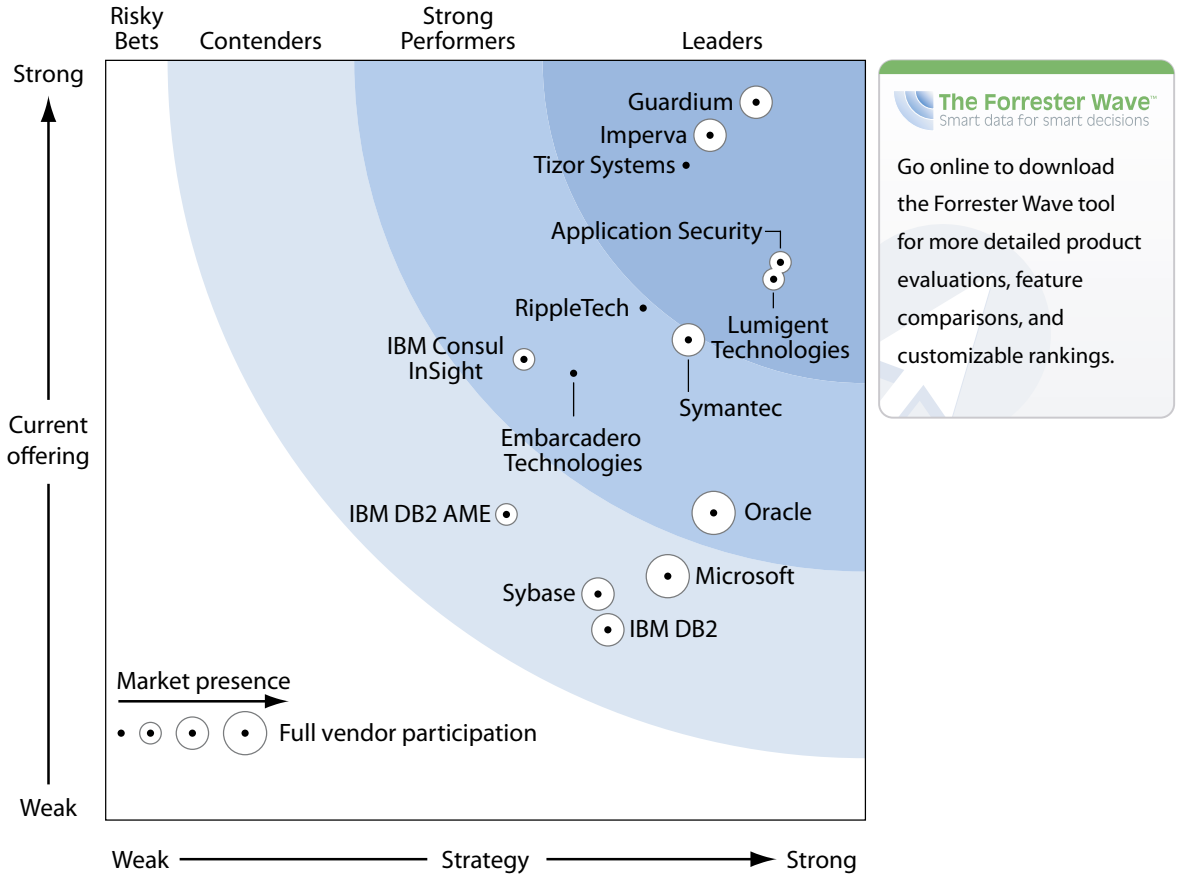
Vendor	Product evaluated	Product version evaluated	Version release date
Application Security	DbProtect	2007.0	February 2007
Embarcadero Technologies	DSAuditor	4.1	April 2007
Guardium	SQL Guard	6.0	April 2007
IBM	Consul InSight*	7.0	May 2007
IBM	DB2 Audit Management Expert	1.1	September 2006
IBM	DB2	9.0	July 2006
Imperva	SecureSphere	6.0	June 2007
Lumigent Technologies	Audit DB	6.0	May 2007
Microsoft	SQL Server	SQL Server 2005	November 2005
Oracle	Oracle Database	10.2.0.3	February 2007
RippleTech	Informant†	2.5	December 2006
Sybase	Sybase Data Auditing	ASE 15.0.2	June 2007
Symantec	Symantec Database Security	2.0	October 2006
Tizor Systems	Mantra	5.4	June 2007

*As of July 3, 2007, Consul InSight 7.0 became IBM Tivoli Compliance Insight Manager 8.0
† Version 3.0 was release in August 2007

Vendor qualification criteria
The product focuses on database security and auditing solutions and its version was released prior to June 30, 2007.
The product has enterprise-class auditing capability in the areas of performance, scalability, reporting, and user management.
The product has been deployed by 25 or more enterprise customers in mission-critical deployments.

Source: Forrester Research, Inc.

Figure 3 Forrester Wave™: Enterprise Database Auditing, Q4 '07



Source: Forrester Research, Inc.

Figure 3 Forrester Wave™: Enterprise Database Auditing Q4 '07 (Cont.)

	Forrester's Weighting	Application Security	Embarcadero Technologies	Guardium	IBM Consul InSight	IBM DB2	IBM DB2 AME	Imperva	Lumigent Technologies	Microsoft	Oracle	RippleTech	Sybase	Symantec	Tizor Systems
CURRENT OFFERING	50%	3.67	2.94	4.72	3.03	1.25	2.01	4.50	3.56	1.60	2.02	3.37	1.48	3.16	4.31
Levels of auditing	8%	4.46	3.81	5.00	3.36	2.24	3.22	4.30	4.91	3.17	3.71	4.06	2.80	4.51	4.60
Application level support	10%	1.80	1.80	5.00	3.00	1.00	1.80	3.80	3.00	1.00	1.00	1.80	1.00	1.80	3.80
Audit policies	12%	4.70	2.58	4.76	3.12	1.45	2.01	4.82	3.41	1.15	2.07	4.52	1.15	3.14	4.76
Monitoring and notification	10%	4.60	3.76	5.00	3.76	1.20	2.50	5.00	5.00	1.74	3.80	5.00	1.60	3.76	4.16
Auditing repository	8%	3.80	3.56	3.80	3.62	2.22	2.64	3.56	3.80	2.46	2.40	3.56	2.22	3.44	3.80
Reporting	10%	3.08	2.80	4.52	4.20	1.28	1.12	5.00	3.48	2.12	1.76	3.80	1.28	2.28	4.20
Analytics and intelligence	12%	3.48	1.38	4.40	0.48	0.00	0.00	4.64	0.90	0.00	0.39	1.59	0.21	3.24	3.60
Performance and scalability	10%	3.00	5.00	5.00	3.00	1.00	3.00	5.00	3.00	1.00	1.00	3.00	1.00	3.00	5.00
Architecture	8%	3.10	1.93	4.60	3.58	1.48	1.60	3.26	3.75	1.68	2.40	3.46	1.63	1.81	3.98
Usability	12%	4.44	3.24	5.00	3.00	1.24	2.76	5.00	5.00	2.44	2.44	3.24	2.44	4.44	5.00
STRATEGY	50%	4.44	3.08	4.28	2.76	3.30	2.64	3.98	4.40	3.70	4.00	3.54	3.24	3.84	3.82
Product strategy	40%	3.90	3.20	4.70	3.00	1.95	2.10	4.70	4.25	2.95	3.70	2.85	2.10	3.75	3.55
Corporate strategy	30%	4.60	3.00	5.00	4.20	3.40	3.00	5.00	5.00	3.40	3.40	3.00	3.00	3.80	5.00
Cost	30%	5.00	3.00	3.00	1.00	5.00	3.00	2.00	4.00	5.00	5.00	5.00	5.00	4.00	3.00
MARKET PRESENCE	0%	2.34	1.35	3.66	2.64	3.14	2.89	3.78	2.49	4.34	4.54	1.82	3.34	3.67	1.85
Installed base	25%	1.00	1.00	4.00	3.00	5.00	4.00	3.00	5.00	5.00	5.00	2.00	5.00	2.00	2.00
Revenue	20%	2.40	0.60	4.20	3.20	3.20	3.20	4.20	0.00	3.20	3.80	0.00	3.20	5.00	3.00
Services	15%	2.20	1.00	3.60	3.50	3.50	3.50	3.60	2.30	5.00	5.00	2.90	3.80	5.00	1.60
Employees	15%	4.10	3.20	3.40	1.50	1.50	1.50	4.10	2.20	3.00	5.00	1.50	1.20	4.60	2.40
Technology partners	15%	2.40	0.60	2.60	0.00	0.00	0.00	3.80	3.50	5.00	3.50	2.10	1.30	1.50	0.70
International presence	10%	3.00	2.60	3.80	5.00	5.00	5.00	4.60	0.40	5.00	5.00	3.40	5.00	5.00	0.40

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

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders

- **Guardium: Has dominance and momentum on its side.** Guardium is a Leader across the board in our evaluation of enterprise database auditing and real-time protection, a result of the broad range of features and functionality built into the product and the company's strong product and corporate strategy and growing market presence. Guardium scored strong in most of the areas of functionality we reviewed, demonstrating its dominance in this space. We expect Guardium to maintain its leadership in supporting large heterogeneous environments, delivering high performance and scalability, simplifying administration, and performing real-time database protection. It continues to be the most aggressive vendor, with innovation and

strong marketing initiatives. Guardium has come a long way in understanding customer needs with respect to database auditing, delivering a solution that not only meets but often exceeds requirements.[1]

- **Imperva: An aggressive vendor**. Imperva is a Leader with a strong performing and scalable auditing solution that scored high in most areas that we evaluated. Imperva has strong support for audit and compliance reporting, end-to-end audit analysis, fraud detection, response auditing, monitoring and alerting, policy management, and administration. Imperva also has a strong product and corporate strategy; its modest 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, and one of the few focusing on integrating databases and applications to deliver a complete end-to-end auditing solution.[2]

- **Tizor Systems: Focuses on innovation and end-to-end auditing.** Tizor Systems is a Leader in the enterprise database auditing and real-time protection market because it provides strong support for alerting, audit and compliance reporting, performance, policy administration, the discovery of private data, integration with files and custom applications, auditing of structured and unstructured data, and end-to-end audit analysis. Its major shortcoming is the inability to block connections in real time. To capitalize on this market-leading product and grow its market presence, Tizor must quickly remedy the deficiencies and increase innovation. Tizor has done well in our evaluation with a strong, credible offering that should meet most enterprises' auditing requirements.[3]

- **Application Security: Offers good auditing solution at an attractive price.** Application Security surprised us by taking a Leader's position in database auditing and real-time protection because it also offers other database security solutions like encryption, vulnerability assessment, and monitoring. The company has enhanced its DbProtect auditing product significantly over the past 18 months by adding several new features, one of the key reasons for its strong showing and market uptake. Application Security is already well known in the vulnerability assessment space, and is now effectively leveraging its existing reputation and market presence to extend its footprint in database auditing. Although Application Security has balanced well across its product portfolio, it is likely to face stiff competition ahead as vendors consolidate and large vendors increase their stakes in this space. Application Security needs to remain focused, increase integration among its various product offerings, and innovate in order to stay competitive.[4]

- **Lumigent Technologies: Flexible and easy-to-use solution.** Lumigent's Leader position was no surprise given that it offers a comprehensive audit solution that meets a broad range of customers' requirements. Lumigent is one of the few vendors we evaluated that offers a flexible architecture capable of reading audit data from three sources: transaction logs, network activity, and native database auditing. It also offers strong support for policy management, monitoring

and alerting, and integration with packaged and custom applications, but lacks strong support for predefined policies, the ability to block connections in real-time, and the discovery of private data in databases. Overall, Lumigent has a strong audit product, good market presence, and a robust road map that should help the company grow apace with the market.[5]

Strong Performers

- **Symantec: Leveraging its market presence.** Although Symantec Database Security (SDS) is a late arrival to the database security game, it has done extremely well to gain a spot in the Strong Performer's category within a year after its general availability. SDS offers a good balance of features and functionality and is especially strong around repository management, activity monitoring, custom policy creation, and ease of use. A key shortcoming is the inability to integrate with packaged applications or files. To make SDS more competitive, Symantec needs to take the product enhancements to the next level by adding more advanced features and functionality to compete against the products of leading vendors like Guardium and Imperva. SDS is a good start for Symantec, but much work remains to be done before it can aspire to take a top spot.[6]

- **RippleTech: Good solution but lacks momentum.** RippleTech's Informant solution is a Strong Performer in the enterprise database auditing market because it offers good features and functionality at an attractive price. It has strong support for compliance reporting, monitoring and notification, role separation, and policy management. It also has two shortcomings: the product does not offer response data analysis, or integration with packaged applications for end-to-end audit analysis. Although RippleTech has a well-defined and credible auditing solution, it is likely to face stiff competition ahead as vendors consolidate and increase their stakes in this space. To stay competitive, RippleTech will need to integrate the Informant product with LogCaster and roll out advanced auditing and real-time protection features.[7]

- **Embarcadero Technologies: Still has a ways to go before it can compete against Leaders.** What a difference 24 months make. Prior to October 2005, Embarcadero never had a database auditing solution, but the acquisition of Ambeo put it on the map. Although Embarcadero's DSAuditor does not top the features and functionality race, it offers a well-balanced solution at a low price. Embarcadero has good support for database auditing, monitoring, and audit repository management, but lacks strong support for applications, intelligent auditing, and predefined policies. As native database management system (DBMS) auditing solutions continue to expand their auditing features and functionality, and as the market consolidates, Embarcadero is likely to face pressure, which it would have to address through innovation and integrating DSAuditor with other Embarcadero products like DBArtisian and ER/Studio.[8]

- **IBM Consul InSight: Part of the Tivoli Security solution**. IBM acquired the privately-held company Consul Risk Management in December 2006. With this acquisition, IBM got a database auditing tool called Consul InSight, recently rebranded Tivoli Compliance Insight

Manager (TCIM). Although Consul InSight does not have top scores compared to leading vendors such as Guardium and Imperva, it offers a reasonably rich auditing solution suitable for most small to moderate auditing environments. Consul InSight's core strengths are in mainframe auditing and the ability to capture audit data from various files, devices, and servers. To expand the penetration of this product, IBM would have to improve features that support integration with packaged and custom applications, offer fraud detection and real-time session block capability, and focus on centralized administration to support large-scale deployments.[9]

- **Oracle: Top native DBMS auditing.** 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.[10]

Contenders

- **IBM AME: Basic-level auditing for mainframe platform.** IBM DB2 Audit Management Expert (AME) currently supports only the mainframe environment, with support for other platforms planned for the future. Overall, AME offers basic support for reporting, policies, and alerting, but lacks advanced features like analytics and intelligence, integration with packaged and file-level auditing, and integration with other compliance solutions. DB2 AME offers more features and functionality than the native DB2 database auditing, but it's not free. For even more advanced auditing, IBM offers a product called IBM Consul Insight, recently rebranded Tivoli Compliance Insight Manager (TCIM). This product is also in the Forrester Wave evaluation of the enterprise database auditing and real-time protection market.[11]

- **Microsoft: Partners count.** Microsoft's SQL Server native auditing solution is basic, but it's free. It offers a good level of support for monitoring user and DBA activity, but lags in policy management, reporting, monitoring and alerting, and analytics. Although Microsoft has improved database security and auditing features in SQL Server 2005, it is still behind Oracle on a feature-by-feature comparison. Microsoft's approach to advanced auditing is to let partners address the gaps, and Forrester does not see this position changing any time soon. But Microsoft remains committed to improving database security with every new release of SQL Server, with the ultimate goal of making SQL Server completely self-securing from all types of threats and vulnerabilities.[12]

- **Sybase: Focuses on Lumigent partnership.** Sybase's native database auditing solution is basic, which is why Sybase itself recommends that customers with advanced auditing requirements use third-party vendor solutions. In fact, Sybase resells Lumigent's AuditDB product under the Sybase Data Auditing brand name. Although Sybase's native database auditing solution does offer some level of support for auditing user and DBA activity, it provides no support for alerting and notifications, predefined reports and policies, or analytics and intelligence. A key strength found in the Sybase native auditing is the ability to build your own auditing solution using Sybase's SQL interface, but this can entail a considerable effort depending on the complexity of the auditing requirement.[13]

- **IBM DB2: More products available to fill gaps.** IBM DB2 native auditing provides basic-level auditing at no additional product cost. Although DB2 native auditing offers some level of support for auditing users and DBA activity as well as database objects, it provides no support for notification and alerting, predefined policies and reports, analytics, and real-time database protection. Most enterprises that use the DB2 native auditing solution write their own scripts and reports to support their auditing requirements. DB2 native auditing lags behind Oracle native auditing, but IBM often promotes both the IBM Tivoli Compliance Insight Manager (formerly Consul InSight) and IBM Audit Management Expert for DB2 for advanced level auditing requirements.[14]

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 3 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 three 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.
- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.

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] View the vendor summary for more detailed analysis of how Guardium fared in this evaluation. See the October 26, 2007, "Guardium Is A Leader In Enterprise Database Auditing And Real-Time Protection" report.

[2] View the vendor summary for more detailed analysis of how Imperva fared in this evaluation. See the October 26, 2007, "Imperva Is A Leader In Enterprise Database Auditing And Real-Time Protection" report.

[3] View the vendor summary for more detailed analysis of how Tizor Systems fared in this evaluation. See the October 26, 2007, "Tizor Systems Is A Leader In Enterprise Database Auditing And Real-Time Protection" report.

[4] View the vendor summary for more detailed analysis of how Application Security fared in this evaluation. See the October 26, 2007, "Application Security Is A Leader In Enterprise Database Auditing And Real-Time Protection" report.

[5] View the vendor summary for more detailed analysis of how Lumigent Technologies fared in this evaluation. See the October 26, 2007, "Lumigent Technologies Is A Leader In Enterprise Database Auditing And Real-Time Protection" report.

[6] View the vendor summary for more detailed analysis of how Symantec fared in this evaluation. See the October 26, 2007, "Symantec Is A Strong Performer In Enterprise Database Auditing And Real-Time Protection" report.

[7] View the vendor summary for more detailed analysis of how RippleTech fared in this evaluation. See the October 26, 2007, "RippleTech Is A Strong Performer In Enterprise Database Auditing And Real-Time Protection" report.

[8] View the vendor summary for more detailed analysis of how Embarcadero Technologies fared in this evaluation. See the October 26, 2007, "Embarcadero Technologies Is A Strong Performer In Enterprise Database Auditing And Real-Time Protection" report.

[9] View the vendor summary for more detailed analysis of how IBM Consul InSight fared in this evaluation. See the October 26, 2007, "IBM Consul InSight Is A Strong Performer In Enterprise Database Auditing" report.

[10] View the vendor summary for more detailed analysis of how Oracle fared in this evaluation. See the October 26, 2007, "Oracle Is A Strong Performer In Enterprise Database Auditing; Tops Native DBMS Auditing" report.

[11] View the vendor summary for more detailed analysis of how IBM AME fared in this evaluation. See the October 26, 2007, "IBM AME Is A Contender In Enterprise Database Auditing And Real-Time Protection" report.

[12] View the vendor summary for more detailed analysis of how Microsoft fared in this evaluation. See the October 26, 2007, "Microsoft Is A Contender In Enterprise Database Auditing And Real-Time Protection" report.

[13] View the vendor summary for more detailed analysis of how Sybase fared in this evaluation. See the October 26, 2007, "Sybase Is A Contender In Enterprise Database Auditing And Real-Time Protection" report.

[14] View the vendor summary for more detailed analysis of how IBM DB2 fared in this evaluation. See the October 26, 2007, "IBM DB2 Native Auditing Is A Contender In Enterprise Database Auditing And Real-Time Protection" report.

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

Australia
Brazil
Canada
Denmark
France
Germany
Hong Kong
India
Israel
Japan
Korea
The Netherlands
Switzerland
United Kingdom
United States

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

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866.367.7378, +1 617.617.5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 24 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.

FORRESTER®