

March 29, 2005

Comprehensive Database Security Requires Native DBMS Features And Third-Party Tools

by Noel Yuhanna

MARKET OVERVIEW

MARKET OVERVIEW



March 29, 2005

Comprehensive Database Security Requires Native DBMS Features And Third-Party Tools

by **Noel Yuhanna**

with Randy Heffner and Carey Schwaber

EXECUTIVE SUMMARY

With increasing attention on data privacy and security, IT shops must enforce strict DBMS security policies and procedures to protect their critical databases. Achieving comprehensive DBMS security requires ensuring that database security policies are aligned with IT security policies and taking strong advanced security measures to harden the database environment. Major DBMS products offer only basic security features; at present Oracle has the most advanced security features. Small specialist vendors such as Application Security, Guardium, IPLocks, Lumigent, and Protegrity offer solutions that help firms ensure that their DBMS environments meet their security requirements. The future of DBMS security will focus on increased automation, tighter integration with technology stack components, and intelligent features. Although most DBMS security requirements will be met by native DBMS features and functionality, firms should consider adopting specialized solutions in the areas of vulnerability assessment, encryption, and intrusion detection prevention to achieve comprehensive DBMS security.

TABLE OF CONTENTS

- 2 Database Security Is Critical To IT Security**
- 5 The Independent DBMS Security Market Is Small But Growing**
- 6 Authentication And Authorization Are Minimum Requirements**
- 7 Database Hardening Is Crucial For All Types Of Applications**
- 9 Database Auditing Is Challenging For Now**
- 11 The Future Of DBMS Security: Automation, Integration, And Intelligence**

RECOMMENDATIONS

- 13 Start With Native DBMS Features, Then Supplement With Specialist Products**
- 14 Supplemental Material**

NOTES & RESOURCES

Research for this report included market analysis and ongoing discussions with DBMS vendors and third-party DBMS tool vendors, including: Application Security, Guardium, IBM, IPLocks, Lumigent, Microsoft, Oracle, Protegrity, and Sybase. Forrester also surveyed 24 IT decision-makers at user companies with more than \$500 million in revenue to understand their DBMS security implementations.

Related Research Documents

“DBMS: Foundation Of Application Infrastructure”
July 30, 2004, Market Overview

DATABASE SECURITY IS CRITICAL TO IT SECURITY

Enterprises often focus on perimeter-based security, but with the growing complexity of environments and applications, firms need to take a broader view, considering security as it relates to the entire technology stack. A survey conducted by *CSO* magazine found that some of intrusions occur internally, indicating that enterprises need more than perimeter security to ensure full protection of their data.¹ DBMS security, which is the last line of defense for enterprise data, needs to focus specifically on policies and procedures that will minimize the risk and the impact of various kinds of attacks. All databases — even those with advanced security measures — can be vulnerable. While all enterprise DBMS products offer basic security — comprising authentication, authorization, and access control — firms still need strong policies and procedures to protect data. DBMS security is not about software or hardware; it's about establishing solid security policies and procedures and ensuring that they are supported by the DBMS security infrastructure and are well integrated with other elements of IT security.

Enterprise Concern Grows As DBMS Security Threats Continue To Grow

Forrester surveyed 24 enterprises with more than \$500 million in annual revenue about their DBMS security implementations; 22 of the 24 were concerned about database security in their organizations. Of these, nine were extremely concerned (see Figure 1-1).² However, most enterprises feel that they have taken sufficient measures to protect against intrusions (see Figure 1-2). Data is important to any business, but private data matters most — especially financial and medical data. Twenty-one of the 24 enterprises Forrester surveyed stated that they understand at least some of the applicable regulatory compliance requirements like Gramm-Leach-Bliley (GLB), HIPAA, and Sarbanes-Oxley (SOX) (see Figure 2-1). All but one of the enterprises we surveyed are confident that their databases meet applicable regulatory compliance requirements; five were extremely confident (see Figure 2-2). This reflects the fact that enterprises are taking regulatory requirements seriously and taking measures to secure their databases. At the same time, Forrester has seen a notable uptick in clients asking about advanced security options to secure their DBMS environments. We believe that the demand for encryption, auditing, and assessment will grow in the coming years, driven largely by regulatory compliance requirements.

With growing incidence of intrusions across industries and strong regulatory requirements to secure private data, enterprises need to make DBMS security a top priority.³ A single intrusion that compromises private data can cause immense damage to the reputation of an enterprise — and in some cases financial damage as well. Bank of America was recently the victim of a security breach, losing critical computer data tapes containing the personal information of 1.2 million federal employees, including some members of the US Senate. The lost data included social security numbers and other sensitive account information. Last November, Wells Fargo informed some of its 5.8 million mortgage and student-loan customers nationwide that their names, addresses, and

social security numbers had been stolen from a third-party processing center in Georgia. And more recently, ChoicePoint made headlines when it disclosed that a security breach on its server storing personal information of at least 145,000 people was comprised.⁴ These are just a few of the intrusions that continue to make headlines, and they are unlikely to stop anytime soon. Hackers will find new ways to break into corporate environments — either to disrupt businesses or to steal private data. Enterprises therefore need to be more vigilant and take proactive measures to safeguard their data.

The Three Major Categories Of DBMS Security

The key to a successful DBMS security implementation is knowing what you are protecting, why you're protecting it, and how best to secure the data, especially when dealing with private data. In accordance with overall corporate information protection policies and IT security policies, the business determines policies for protection of major data sources. Database security managers translate these policies into appropriate yet cost-effective technical and procedural solutions for DBMS security. Feature/function options for DBMS security fall into three major categories:

- **Authentication and authorization (access control).** This category answers questions like, “Can I log in?” or “What privileges do you have?” or “Can I access this data?” Authentication and authorization are key requirements for any database deployment and are even more important when dealing with private data. User account management, single sign-on, role management, and password administration are the key functions.
- **Administration.** This category covers functions required to harden a database environment against attacks that bypass authentication and authorization. Key functions include security assessment to flush out vulnerabilities, backup protection, patch management, and data encryption for both data-at-rest and data-in-motion.
- **Auditing.** This answers questions like, “What happened?” or “Who changed this data?” or “Why is a user repeatedly trying to access private data?” Key functions include intrusion-detection prevention, data auditing, management reporting, real-time auditing, and proactive security monitoring.

Each of the key functions listed above is discussed in more detail in the following sections.

Figure 1 Most Enterprises Are Concerned About Database Security

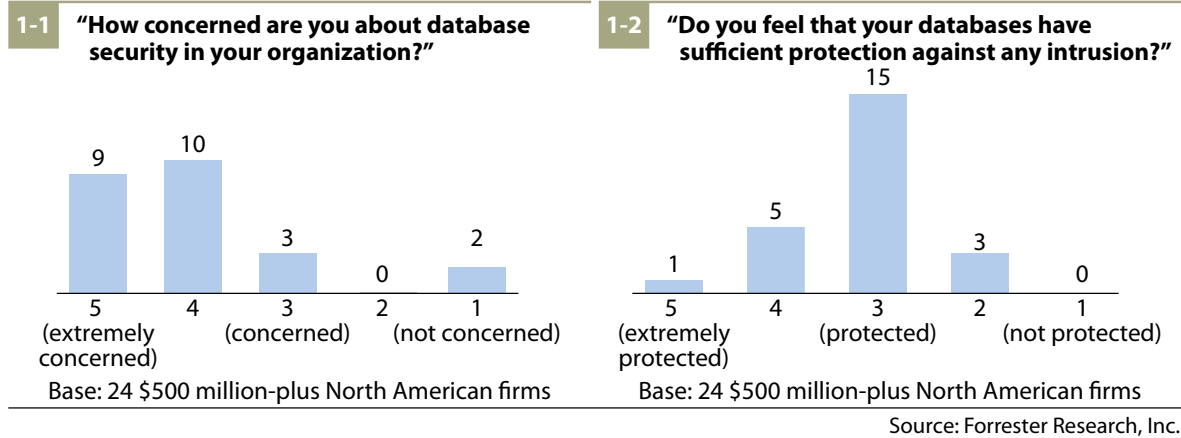
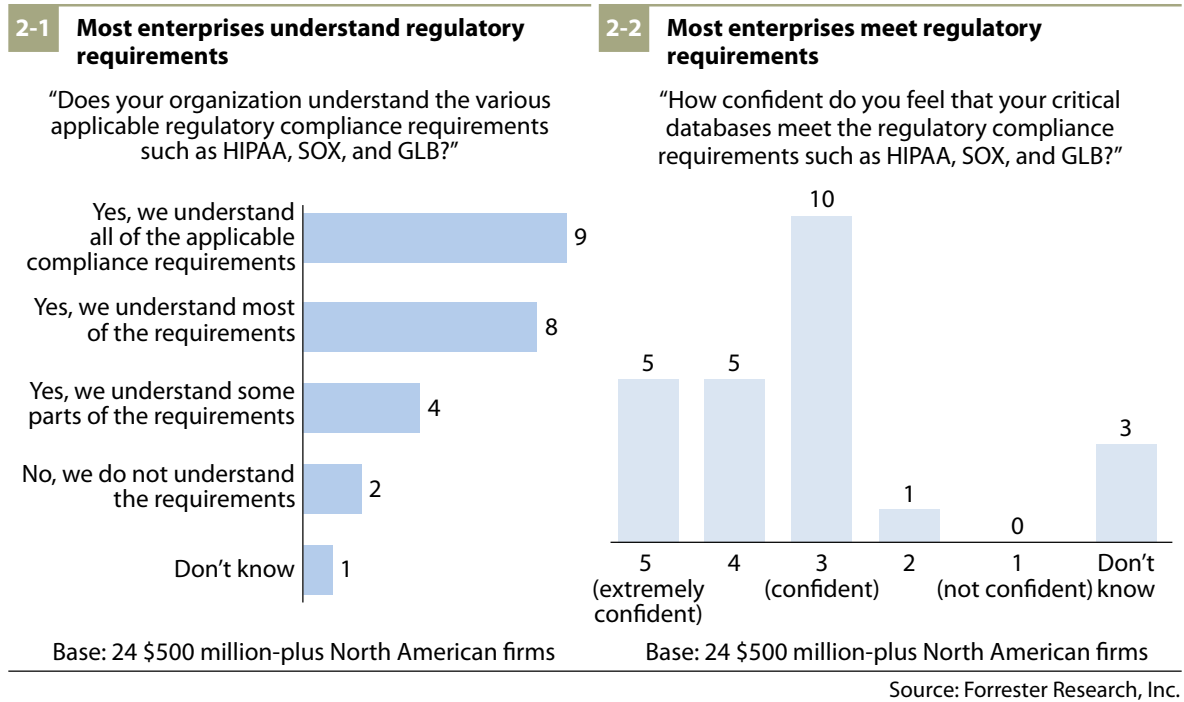


Figure 2 Regulatory Requirements Remain A Top Priority For Enterprises



THE INDEPENDENT DBMS SECURITY MARKET IS SMALL BUT GROWING

The major DBMS products on the market provide many — but not all — of the key functions within the three major DBMS security categories. Thus, growing concerns about security vulnerabilities and regulatory requirements have created a market opportunity for specialized DBMS security vendors, particularly in the areas of encryption, vulnerability assessment, intrusion detection and prevention, and monitoring. The current DBMS security tool market is around \$135 million and is likely to more than double to \$280 million by 2008.⁵

Comprehensive DBMS Security Requires Both Native DBMS Features And Specialized Tools

When looking for comprehensive security options, first consider your DBMS's native features, then look at areas in which the DBMS itself does not meet your requirements and specialized tools might be able to help. In the current DBMS security landscape:

- **DBMS vendors meet most security requirements.** Although most DBMS security requirements will be met by native DBMS features, many DBMSes do not offer a comprehensive set of advanced security options; notably, many DBMSes do not have security assessment, intrusion detection and prevention, data-in-motion encryption, and intelligent auditing capabilities. Oracle continues to lead in database security solutions, with many advanced DBMS security features like virtual private databases, LDAP integration, fine-grained auditing, and label security. Oracle Database 10g Release 2, which is scheduled for later this year, will extend the data-at-rest encryption feature by making it more tightly integrated with the DBMS kernel and more transparent to the application. Microsoft continues to expand on database security, and SQL Server 2005 will support data-at-rest encryption with integrated key management infrastructure, DDL-level auditing, Windows-like full user management capability, and a secure-by-default approach that enables only limited features by default. The recent IBM DB2 Universal Database V8.2 now supports data-in-motion encryption, two-part user names for improved user identity, and Windows Local System Account functionality.

While these advanced security requirements are good to have, the basic DBMS product functions for authentication, access control, administration, and auditing are a critical foundation. Start by addressing core requirements using native DBMS security features, understanding that you may well need to supplement with a specialized DBMS security solution. Over the next three to four years, the DBMS vendors are likely to expand their offerings to include advanced security solutions in the areas of encryption, auditing, and intelligent tools, so it is important to understand your vendor's future plans before heavily investing in a specialist vendor's product.

- **Top DBMS tools vendors lag behind — at least for now.** Three vendors dominate the database tools market — BMC Software, Computer Associates International, and Quest Software. But when it comes to database security, these vendors lag behind. Most of their current database

security solutions are focused on authentication and access control, and some offer basic auditing capabilities. None of them provides advanced data protection solutions such as data-at-rest encryption, security assessment, or database intrusion detection and prevention. Although BMC partnered with IPLocks last year to address advanced security areas like auditing and vulnerability assessment, it is still behind in delivering a comprehensive and integrated security solution. Computer Associates offers authentication, authorization, and auditing capability, but it still lags in the areas of encryption, vulnerability assessment, and database intrusion detection and prevention. Quest Software has so far shown no sign of extending its database security presence beyond authentication and authorization capabilities. With more customers demanding simplified, integrated, and automated database security solutions, the market for advanced solutions will continue to expand. As a result we are likely to see these DBMS tools vendors either acquire or partner with more strategic specialized vendors to extend their presence over the next one to two years.

- **Small specialized tool vendors fill in the gaps.** Today most of the advanced DBMS security functions are provided by small specialized vendors such as Application Security, Guardium, IPLocks, Lumigent Technologies, nCipher, NetLib, Protegrity, and Vormetric. These vendors focus primarily on addressing functional gaps around data-at-rest encryption, backup encryption, security assessment, granular auditing, and intrusion detection and prevention. Application Security offers the most comprehensive database security solution, covering data-at-rest encryption, assessment, auditing, and intrusion detection and prevention. Although DBMS vendors will continue to extend their security solutions in the near term, we believe that the specialized vendors are likely to maintain their edge with simplified and more innovative, integrated, and intelligent security solutions.

AUTHENTICATION AND AUTHORIZATION ARE MINIMUM REQUIREMENTS

All DBMSes have the basic authentication and authorization features, which are key requirements for any application. Nineteen of the 24 enterprises Forrester surveyed found user and password management to be challenging (see Figure 3-1). This is no surprise, because today authentication and authorization can be implemented at the application or database level, making them more complex. The key functions of basic security are:

- **Database authentication.** Authentication is the process of determining whether the identity of someone or something is in fact as it is claimed to be. A database identity can be linked to the operating system authentication module or LDAP so users don't have to enter their credentials again if they have already been authenticated. Alternatively, many applications use a generic database identity through which many users access the database. Passwords can be stolen, forgotten, or broken, presenting an opportunity to pursue more stringent authentication policies and deeper integration with application-level security.

- **Database authorization (access control).** Authorization is the process of giving someone or something permission to do something. Authentication precedes authorization, but authenticated users still must be given explicit authorization to access various database objects and functions, such as creating a table or accessing some data. Role management helps in managing authorization policies by clustering related functions together as a role and then authorizing the role for specific access rights.

Native DBMS Features Meet Most Authentication And Authorization Requirements

DBMS authentication and authentication works fine out of the box, but they still require enforcing strong policies to make the process secure. Some DBMSes offer advanced password management features like automatic checks for poor passwords or checks of various user accounts and roles; these are important for critical applications. DBMS tools vendors like BMC, Computer Associates, and Quest Software offer support for the authentication and authorization process through centralized administration using a GUI tool.

DATABASE HARDENING IS CRUCIAL FOR ALL TYPES OF APPLICATIONS

While authentication and authorization establish a foundation for database use by trusted users, many of the database intrusions over the past three years have bypassed DBMS trust mechanisms. Database hardening aims to protect against these sorts of attacks. Additional levels of data protection include protection for backups; encryption for data-at-rest and data-in-motion; and granular object-level protection, especially for private data. Restricting physical access to the server is foundational to DBMS security.⁶ Key functions for database hardening include:

- **Ensuring security patches are applied in a timely fashion.** Thirteen of the 24 enterprises Forrester surveyed stated that finding and patching DBMS software vulnerabilities is challenging. Database security patches remain critical and needs the highest level of attention. Patch deployments are a manual task today, but DBMS vendors are working toward automating them in the near future.
- **Protecting backups.** Backups of databases should be given the same level of security focus as operational databases, especially when dealing with private data.⁷ What if a hacker does a string search of the backup data files? What if an insider walks away with backup tapes? Backup data is as good as production data, so it should be given the same level of security focus. Because backups involve multiple groups (the server group, the database group, and the business group), the task of formulating secure procedures for managing backups often falls through the cracks.
- **Performing regular security vulnerability assessments.** Database configurations are not secure by default, and they often require specialized knowledge and extra effort to ensure that configuration options are set in the most secure manner possible. Administrators must ensure

that: 1) only required database options are installed; 2) default user accounts are removed; 3) poor passwords are flushed out; 4) connectivity to and from other applications and programs is minimized; 5) all database files and directories are well protected; and 6) all objects have proper privileges. Although these things can be checked manually, hundreds of databases and a constantly changing environment make it a very challenging task. If this task is not performed, security breaches can result.

- **Encrypting data when and where appropriate for each application.** Only four of the 24 enterprises Forrester surveyed use data-at-rest encryption to protect their databases. Ten out of the 24 enterprises find data encryption to be challenging. While some DBMS products offer data-at-rest encryption, they still lack in simplicity and transparent integration with applications, making their encryption features difficult to use. Also, because encryption leads to higher system resource use, impacting the applications response time, it is often difficult to judge the cost/benefit of encryption; this can put the application teams at odds with the security group. While data-in-motion encryption is supported by most DBMSes, and data-at-rest encryption by some, no DBMS product today supports backup encryption at the database file level.

Specialized DBMS Security Vendors Fill Gaps In Database Hardening

Only a few DBMS products offer advanced security features that help deploy additional measures to harden the database, such as data-at-rest encryption, backup encryption, vulnerability assessment, and fine-grained auditing capability. Limiting administrator-level access on private data still remains challenging, since there are no DBMSes currently available that support this.⁸ Since none of the DBMS security tools vendors have any solution around security patch deployments, enterprises must continue to rely on native patch management tools. Most DBMS products offer backup and recovery features, but they lack in advanced measures, such as encrypting the data, putting new passwords on backups, and tracking all backup tapes. Enterprises looking for strong backup solutions should look at EMC, Network Appliance, Veritas Software, and Vormetric for backup solutions. Security assessment tools can help check environments to identify vulnerabilities and weak configurations. None of the top DBMS products offer security assessment features today, so consider third-party tools from vendors such as Application Security, Internet Security Systems, IPLocks, Next Generation Security Software, and Symantec. Security vendors such as Application Security, nCipher, Protegrity, and Vormetric lead in database encryption solutions, supporting heterogeneous DBMSes and simplified administration to minimize the effort required to implement encryption.

DATABASE AUDITING IS CHALLENGING FOR NOW

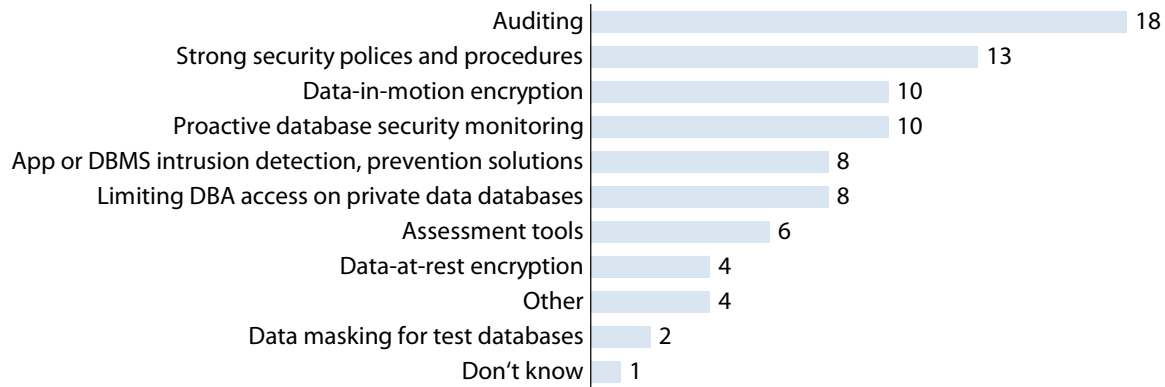
Auditing helps to answer questions like “Who changed data?” and “When was the data changed?” and “What was the old content was prior to the change?” Your ability to answer such questions is very important for regulatory compliance. Sometimes it may be necessary to review certain audit data in greater detail to determine how, when, and who changed the data. When planning for auditing requirements, consider that: 1) not all databases need deep auditing; 2) only some tables or columns need auditing; 3) automated auditing can save much time; 4) auditing analysis is most effective when it is integrated in a centralized way across multiple audit targets; 5) audit logs should be stored separately from production databases; and 6) auditing should include user logins and sessions, particularly when dealing with very sensitive data. Key functions of auditing include:

- **Logging the right data so it is available at audit time.** Database auditing is the process of detecting and recording security-related events, such as attempts to update, delete, insert, or view data. The audit records are stored in an audit log and can provide useful information about who, what, and when related to the data. Eighteen of the 24 enterprise Forrester surveyed use auditing in their environment, but 12 of the 24 find it to be challenging (see Figure 3-2 and see Figure 3-3). Enabling the auditing feature is usually straightforward, but it’s knowing what to look for that can be challenging, especially when the audit log can contain many log entries. Therefore, auditing tools should not only capture and present to you the audit data, but they should also alert you on activities and quickly identify records that are needed for an audit.
- **Intrusion detection and prevention can help with real-time auditing.** A database can be accessed in many ways, including ODBC, JDBC, native database calls, third-party applications, and other database tools. If a user has the necessary privileges, the DBMS typically does not do any further analysis and simply gives the authority to access or change data as appropriate. But if the user is an insider collecting large amounts of private data, a hacker who stole a password, or a hacker exploiting vulnerabilities, the DBMS will not prevent access. Intrusion detection and prevention solutions check for suspicious activities. For example, they might ask why a user is trying to access all of the data in a table or why a user is trying to look at the schema definition.

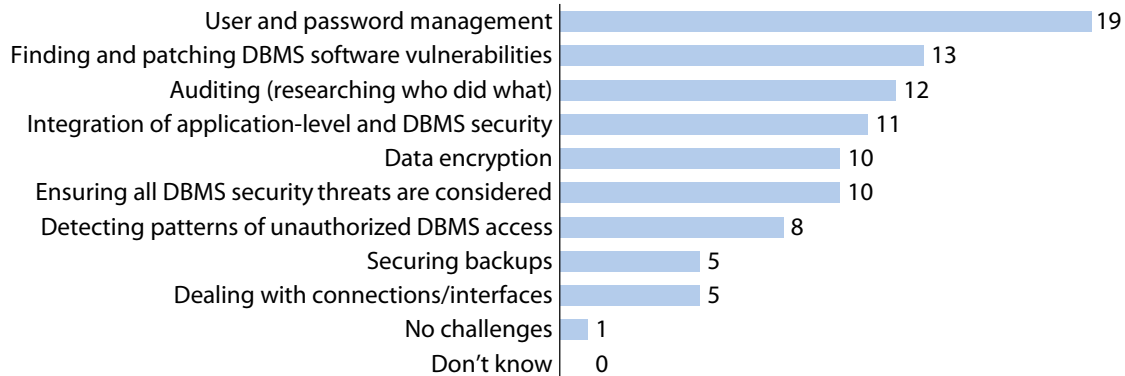
Specialized DBMS Security Vendors Provide Comprehensive Auditing Solutions

At present, most DBMS vendors lag in intelligent auditing tools that can help in the audit process. Also, we find that not all enterprises enable auditing because of the system overhead associated with capturing the relevant information. Small specialized vendors that offer auditing functionality include Lumigent, Guardium, and Application Security; these vendors focus on a centralized yet heterogeneous auditing capability (see Figure 4). Today, only a few DBMS vendors offer features that can help track security threats in real time. Small vendors supporting real-time vulnerability monitoring include IPLocks, Guardium, and Lumigent. Guardium offers a unique product that monitors network streams, checking for suspicious activities.

Figure 3 Database Security Remains Challenging

3-1 “What advanced DBMS security measures are being taken in your organization?”


Base: 24 \$500 million-plus North American firms
(multiple responses accepted)

3-2 “What are the key DBMS-related security challenges your organization faces?”


Base: 24 \$500 million-plus North American firms
(multiple responses accepted)

3-3 “What are the various obstacles that you face in addressing DBMS security issues?”


Base: 24 \$500 million-plus North American firms
(multiple responses accepted)

Source: Forrester Research, Inc.

Figure 4 DBMS Security Market Landscape

Vendor	Authentication	Authorization	Security patch deployment	Vulnerability assessment	Data-at-rest encryption	Data-in-motion encryption	Database auditing	Intrusion detection
Application Security			✓	✓		✓	✓	
BMC Software	✓	✓				✓		
Computer Associates	✓	✓				✓		
Guardium						✓	✓	
IBM	✓	✓	✓		✓	✓	✓	
IPLocks				✓		✓	✓	
Lumigent Technologies						✓	✓	
Microsoft	✓	✓	✓			✓	✓	
nCipher					✓			
NetLib					✓			
Next Generation Security Software				✓				
Oracle	✓	✓	✓		✓	✓	✓	
Quest Software	✓	✓						
Protegrity					✓			
Sybase	✓	✓	✓			✓	✓	
Symantec	✓	✓		✓				✓
Vormetric					✓			

Source: Forrester Research, Inc.

THE FUTURE OF DBMS SECURITY: AUTOMATION, INTEGRATION, AND INTELLIGENCE

Twelve of the 24 enterprises Forrester surveyed indicated that their lack of DBMS security features or products is an obstacle in addressing their DBMS security issues. Forrester expects that DBMS vendors will continue to expand their security offering over the next three to four years and will be able to meet most of the requirements. The specialized DBMS security vendors will continue to focus on innovative security solutions around encryption, assessment, and auditing, making the products simpler, more automated, and more tightly integrated with other technology stack components. Enterprises should update their DBMS security strategy every six to 12 months to reflect the new features offered by DBMS vendors and third-party vendors. In the near future, vendors will focus on:

- **Automation to simplify security implementations.** Thirteen of the 24 enterprises we surveyed find it challenging to deal with database security patches, which is no surprise since patch deployments take a lot of time and effort and require production outages. We are likely to see DBMS vendors and third parties come out with highly automated security solutions in patch management that will require no planned outages within the next three to four years.
- **Integration to support more robust and comprehensive solutions.** Most of today's security products focus on delivering a piecemeal solution relevant to a part of the technology stack. There is no integrated end-to-end security in which a transaction can be tracked from the user's device down to the disk block where the data resides. In the near future, specialized vendors might address this issue with innovative products that will be able to track all activities (transactions and users) across the technology stacks in a more integrated manner. These products will extend data encryption, assessment, and detection and prevention solutions to focus on queries and transactions from a client to the database and to be aware of what programs and applications are being used to access the database and what infrastructure is being used, such as laptop, PDA, server, or desktop.
- **Intelligent solutions to deliver real-time data protection.** DBMSes are not intelligent when it comes to security: For example, if a user has privileges, the DBMS does not stop the user or even determine why he or she might be trying to query the schema repeatedly or trying to access all private data. What if the user is a hacker or a disgruntled employee? In the future, DBMS vendors and specialized vendors are likely to roll out innovative security solutions that will be intelligent enough to automatically detect and prevent hackers from accessing private data.

RECOMMENDATIONS

START WITH NATIVE DBMS FEATURES, THEN SUPPLEMENT WITH SPECIALIST PRODUCTS

Enterprises must focus on:

- **Auditing all critical databases.** All DBMS products offer basic auditing features, which should be sufficient in most cases. But firms looking to centralize auditing for heterogeneous DBMSes should consider specialized DBMS security solutions.
- **Using intrusion detection and prevention for Internet-based applications.** For databases that need the highest level of protection, such as Internet-based database application, consider using specialized intrusion detection and prevention tools to track and eliminate suspicious activities.
- **Using data encryption to secure sensitive databases.** Not all DBMS vendors offer comprehensive data encryption solutions, so consider specialized products when existing products fall short. Look for solutions that are easy to implement, scalable, and require no application changes.
- **Performing security assessment to flush out vulnerabilities.** When trying to secure many critical databases, consider using security assessment tools that can check for various types of vulnerabilities. With DBMS vendors lagging in security assessment tools, look at specialized solutions.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Document

Application Security	Lumigent Technologies
Computer Associates International	Microsoft
Guardium	MySQL
IBM	Oracle
IPLocks	Sybase

ENDNOTES

- ¹ CSO magazine's 2004 E-Crime Watch survey conducted in cooperation with the US Secret Service and the Carnegie Mellon University Software Engineering Institute's CERT Coordination Center found that 29% of intrusions were internal. See <http://www.cert.org/about/ecrime.html> for details.
- ² Forrester surveyed 24 large companies in North America in February 2005 to find out their database security implementation.
- ³ IT security incidents reported to CERT numbered 137,529 in 2003 and 82,094 in 2002. CERT publishes security related statistics on a regular basis. For details, please see http://www.cert.org/stats/cert_stats.html.
- ⁴ ChoicePoint made headlines recently when it began the incident disclosure and notification process of a security breach that compromised the personal information of at least 145,000 people. See the March 1, 2005, Quick Take "ChoicePoint Security Breach Will Lead To Increased Regulation."
- ⁵ Growing numbers of security vulnerabilities and security-centric regulatory requirements combine with DBMS vendors' security inadequacies to create a second fertile market for third-party tool vendors. See the September 28, 2004, Market Overview "DBMS Tools Market: Modest Growth To 2008."
- ⁶ Database servers should reside in a data center or a secure room to minimize unauthorized access. See the September 25, 2003, Planning Assumption "DBMS Security Issues."
- ⁷ Forrester finds that most enterprises have strong security measures for critical product environments but often overlook database backup security. See the September 30, 2004, Best Practices "Database Backup Security Matters."
- ⁸ Eight of 24 enterprises surveyed indicated that limiting DBA access on private data to be challenging.

FORRESTER®

Helping Business Thrive On Technology Change

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

*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.