

WHITE PAPER

Oracle Database Security: Cost-Effective Data Leak Prevention Starts at the Source

Sponsored by: Oracle

Charles J. Kolodgy
August 2009

IDC OPINION

Data, data everywhere. Organizations are awash in information. Data has been growing at an incredible rate. The growth in storage capability is a bellwether for the growth in information. Over the past few years the annual capacity growth rate for data in traditional enterprises increased at about 45%. The information being collected, created, and stored is valuable to the everyday operations of organizations. This information drives most business activities, and the information creates value in its use; thus it represents a type of currency within the marketplace.

Gathering, organizing, managing, finding, and analyzing information has been and remains a core imperative for most businesses. As information proliferates and creates value, it must be available to those who need it. The expanded sharing of information leads to decentralized data management. Decentralization vastly reduces dependence on the keepers of central files. Databases are the digital banks that store and retrieve valuable information. As the repository in which critical information, such as customer records, business transactions, and intellectual property, is stored, databases must be protected, and the protection must not stifle access to the information by those who need it. IDC believes information security is most effective when information is protected and controlled at the source — the database. In addition, enterprises must adopt database security best practices to protect the mission-critical enterprise data repositories that represent their lifeblood. The security must be able to prevent the mistaken and inappropriate release of data and foil attackers who are financially motivated and won't be deterred by minimalist security. Database security represents a preemptive approach to data security.

Database security is a critical component of what IDC calls information protection and control (IPC). IPC, like most security efforts, is a multifaceted challenge. It must protect against the deliberate or inadvertent release of sensitive information, must ensure compliance with regulations, must not interfere with the proper usage of information, and must meet these challenges in a cost-effective manner.

In This White Paper

This IDC white paper presents a preemptive approach to IPC. It discusses the growing internal threats to business information, the impact of government regulations on the protection of data, and how enterprises must adopt database security best practices to prevent sensitive customer data or company information from being distributed internally or externally in violation of regulatory or company policies.

This white paper also highlights how Oracle provides security products that enterprises can leverage to protect themselves against costly data breaches.

Approach

IDC developed this paper in June 2009 using a combination of existing market research and our knowledge base of primary research. This research includes a range of quantitative surveys and in-depth interviews about enterprise security conducted with IT executives at companies in a variety of industries, including healthcare, financial services, public services, and manufacturing. In addition, IDC met with the Oracle product development team to understand Oracle's database security product offerings.

INFORMATION PROTECTION AND CONTROL

Motivators

Information Explosion

Some of the greatest assets of the vast majority of organizations consist of digital bits of information, not their physical holdings. Increasingly, data stored in databases, file management systems, flat files, spreadsheets, and other information storage formats is the linchpin for enterprise success. Intellectual property, transactions, and records to name a few are fueling business because that information is the currency upon which business operations function. Organizations are creating and using data at an unprecedented level, as represented in the demand for storage capacity. The annual capacity growth rates for the storage of data within enterprises grew 47% in 2008. The creation and processing of critical information won't let up anytime soon. Mandates for electronic health records and smart utility grids are just a few examples of what will accelerate the information explosion in the years ahead.

Businesses have become more dependent on information. The gathering, organizing, managing, finding, and analyzing of information are now crucial to most businesses. Information manipulation can make a business more flexible and better able to address emerging business trends. As information usage proliferates among more and more users, organizations must deliver data to only those who require it for their jobs. Data accessibility, to authorized users, is at the heart of business processes. The proper management of the data is the purview of databases.

Data Breaches

As the value of information collected, organized, manipulated, and analyzed grows, so do the threats to that data. Any organization with sensitive personal or financial data represents a potential target. New attack vectors are aimed at siphoning off the critical data while avoiding detection. Criminal elements are conducting targeted attacks on the "information business jugular" of financial assets, sensitive proprietary data, or resalable personal data. Authorized insiders also contribute to data breaches by either intentionally taking data or inadvertently releasing data.

No matter how the data is lost or exposed, it is costly for an organization. In response to an IDC research survey, almost half of the companies reported that the "total" impact of financial loss was over \$100,000, while 8.5% of the companies reported financial loss of over \$1 million. No matter the size of the breach, be it a few hundred records or tens of millions of records, data loss has a significant negative impact on a business. Any privacy failure, or even the mere perceived failure to protect customer data, can result in loss of consumer trust, affect customer retention, cause significant damage to brand and company reputation, or lead to civil penalties. Organizations have slowly been investing in IPC solutions. On average they have been spending \$35,000 to improve their data protection profile. However, to fully reduce risk of data exposure, organizations are working to strengthen their overall infrastructure to prevent data breaches. Since the majority of breaches are inadvertent, ensuring proper access control and accountability for protected information can greatly reduce a company's exposure, and investments will have a significant return.

Table 1 provides some representative data breaches, both large and small, and describes how they can impact organizations in many different sectors.

TABLE 1		
Database Data Loss Incidents		
Date Reported	Vertical	Impact
May 2009	Manufacturing	Personal information (name, title, Social Security number, and salary) was accessed from a company database. The breach was from internal sources. It was reported by an employee who had seen the employee list.
February 2009	Healthcare	An attacker accessed 17 servers that contained a database with sensitive personal information of university medical patients. 37,000 records that contained the names, addresses, birth dates, and Social Security numbers of each person who had lab work, such as a blood or urine test, done at the facility since 1994 were exposed. It was reported that a forensic investigation concluded that the hacker was not in the system long enough to retrieve any confidential information.
January 2009	Education	Attackers broke into a university database and illegally obtained personal information about students and sent the information to an off-campus IP address. About 450 Social Security numbers and other unspecified personal information were exposed.
October 2008	Government	Lottery winners, lottery commission employees, retailers, and vendors were the victims of a data breach by a former employee at a state lottery commission. More than 100,000 records that included names, Social Security numbers, addresses, and prize amounts were exposed when a former computer analyst copied the data onto computer disks.
September 2008	Retail	Nearly 99,000 payment cards used by customers at several retail stores may have been compromised in a series of data thefts dating back to August 2004. The compromised data included credit and debit cards, expiration dates, and "other card data" but did not include customer names or addresses. The data breach was uncovered following the arrest of three individuals for credit card fraud.

TABLE 1

Database Data Loss Incidents

Date Reported	Vertical	Impact
August 2008	Government	A retired employee improperly emailed himself the contents of a database containing the personal information of 13,000 retired police officers. Information exposed included names, addresses, and Social Security numbers. Officials said they did not see malicious intent, so no charges were filed.
August 2008	Financial services	A computer was accessed by a hacker between November 2007 and February 2008. As a result, the names, addresses, birth dates, and Social Security numbers of the company's more than 92,000 online credit seekers may have been exposed.
April 2008	Healthcare	The personal information, including names, addresses, and some health information and Social Security numbers, of thousands of clients and patients of a regional medical center was potentially compromised when a database was illegally accessed. The breach resulted in the immediate shutdown of the database.
January 2008	Financial services	The database of a financial services company was breached, and the names and Social Security numbers of virtually all of the company's clients were obtained by the attacker. The database included information such as account numbers and balances. Information on 226,000 current and former clients was exposed.
September 2007	Financial services	A database was hacked, and contact information for more than 6.3 million customers was stolen. It was reported that sensitive information in the same database, including Social Security numbers and account numbers, was not compromised. Names, email addresses, phone numbers, and home addresses were taken in the data breach, which resulted in customers receiving unwanted spam.
July 2007	Financial services	A database analyst stole customer records containing credit card, bank account, and other personal information. A total of 8.5 million records were affected. The perpetrator was arrested and pleaded guilty to federal fraud and conspiracy charges in connection with the theft of data.

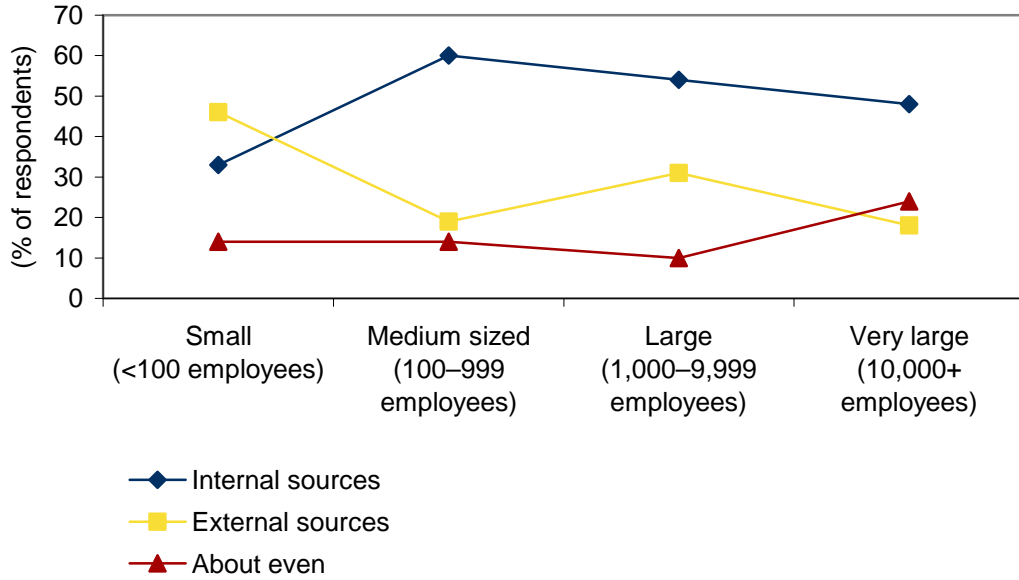
Source: IDC, 2009

Internal Threats Versus External Threats

Threats to protect information are generated from both external and internal sources. According to IDC's 2008 *Enterprise Security Survey* of 333 North American IT professionals, internal sources are believed to generate a greater threat to the enterprise than external sources. As shown in Figure 1, the gap between internal and external threat concerns is much more pronounced among companies with between 100 and 1,000 employees, although all but the smallest organizations view internal threats as more serious. The growing concern with internal security threats comes as no surprise as enterprises have focused their attention on strengthening perimeter defenses, designed to keep people out, while having considerably weaker or even nonexistent defenses on information repositories such as databases. Those already on the inside can have nearly unfettered access to information. The need to improve information protection from insider threats appears to be a growing concern. Figure 2 illustrates how concerns about internal threats have changed from 2005 to 2008.

FIGURE 1

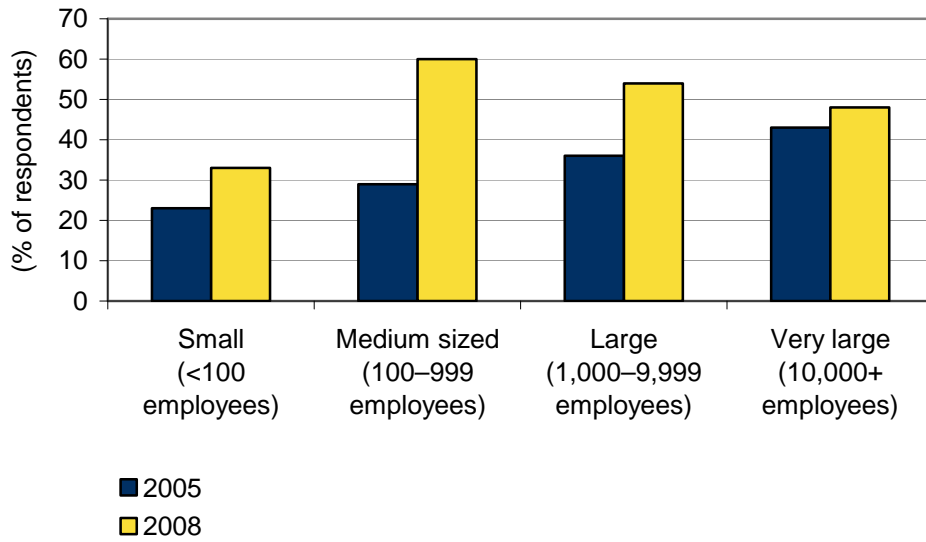
Origin of Most Serious Threats to the Enterprise by Company Size



Source: IDC's *Enterprise Security Survey*, 2008

FIGURE 2

Internal Threats Are Considered Most Serious



Source: IDC's *Enterprise Security Survey*, 2008

Additional IDC survey findings that illustrate the risks to information from internal threats include:

- ☒ 73% of very large organizations (10,000+ employees) and 54% of large organizations (1,000–9,999 employees) have terminated employees or contractors for internal security violations.
- ☒ 31% of very large organizations (10,000+ employees) and 22% of large organizations (1,000–9,999 employees) have prosecuted an employee for internal security violations.

Table 2 illustrates the perceptions of the greatest threats enterprises saw in 2007 and 2008; concerns regarding threats increased markedly in 2008. Internal threats are rapidly climbing the priority list of enterprise security threats and now account for three of the top 10 most serious threats facing corporations today.

TABLE 2

Top Threats to Enterprise Security (Most Significant), 2007 and 2008
(% of Respondents)

	2007	2008
Trojans, viruses, other malware	46	54
Employees exposing information	49	52
Spyware	41	48
Application vulnerabilities	32	44
Hackers	34	41
Equipment misconfiguration	34	41
Spam	45	39
Data stolen by trusted party	37	38
Insider sabotage	29	34
Wireless LANs	27	33

Source: IDC's *Enterprise Security Survey*, 2008

In 2008 employee error ranked as the greatest threat to enterprise security for companies with over 10,000 employees and is a close second for all companies. This is up from the fourth-greatest threat in 2006. IDC believes the majority of information leaks and compliance violations come from employee error. Organizations are extremely concerned with employees inadvertently violating corporate policies and/or complying with government and industry regulations.

Data stolen by an employee or a business partner ranked as the eighth-greatest threat to enterprise security. Although the majority of insider violations are inadvertent, IDC believes the most costly incidents are from malicious insiders. IDC believes malicious action by a trusted source with access to corporate databases and network resources will continue to rise up the priority list in organizations. Malicious employees potentially facing financial hardship are increasingly looking for ways to use corporate information to commit fraud.

Insider sabotage ranked as the ninth-greatest threat to enterprise security. As with data stolen by an employee, insider sabotage by trusted employees poses a significant risk to organizations.

For organized attackers, the ultimate payoff comes from selling the ill-gotten data, not from conducting fraud using that data. Trafficking in stolen credit cards and other identity information has become big business. IDC estimates that the buying and selling of stolen and compromised identities has become a billion-dollar industry.

In all cases, organizations are facing a growing number of information leaks containing confidential data from insiders as well as increasing incidents of insider fraud. The vast majority of insider incidents are caused by human error, so systems that can reduce human error will provide a significant return to the enterprise.

Government and Industry Regulations

A major change in the way security is handled is that many of the activities associated with security aren't necessarily done to prevent attackers from breaching the network but rather are being driven by government regulations and industry standards. These rules have sprung up as a result of malfeasance or spectacular failure. Government and industry regulations remain a key driver for IPC implementations. Table 3 provides a list of the key regulations or standards with which organizations need to comply. The increasingly complex environment of regulations and standards drives concerns about the accuracy and protection of an organization's data and information, not only with employees but also with customers, partners, and contractors. Organizations are faced with addressing compliance issues surrounding Sarbanes-Oxley (SOX), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the European Union Data Protection Directive 95/46, the Japanese Personal Information Protection Act (JPIPA), and state public disclosure laws. Additionally, the Payment Card Industry Data Security Standard (PCI DSS), although not a regulation, has considerable impact on those companies that handle credit cards. Further impetus for executives to push their organizations to comply with these regulations includes personal liability and the threat of criminal and/or civil penalties. Civil prosecution can carry substantial financial penalties and damage a company's reputation with its customers.

Regulations governing privacy have been passed worldwide and vary from country to country. Organizations doing business internationally are struggling to cope with the effort to comply across borders. In the United States, complying with federal regulations that have recently come into effect is not as straightforward as executives would have hoped because many of the laws by their nature are written with vague directives. Building best practices and industry standards is an ongoing process, but it has been

slow and often painful for many organizations that find themselves learning from the financial loss and public humiliation that typically accompany noncompliant actions.

As outlined, privacy regulations have surfaced worldwide, and the trend shows no signs of abating. IDC expects the risk of compliance infractions and lawsuits from customers and/or patients to continue as many enterprises have not yet implemented the requisite technology capabilities needed to safeguard regulated data.

IDC research has identified the pitfalls that lead to compliance failures. They include:

- Unresolved separation of duties that inadvertently enables accounts with "superuser" access rights
- Failure to control the number of users with superuser access to production databases
- Failure to adequately secure data in custom applications
- Inability to properly document manual processes and reconcile these processes to the IT systems used
- Inability to adequately secure access to operating systems and databases that support corporate financial applications and transactions
- Failure to monitor the activities of privileged users

TABLE 3

Key Regulations Driving Information Protection and Control

Regulation	Impact
HIPAA	The Health Insurance Portability and Accountability Act of 1996 requires that all patient healthcare information be protected when electronically stored, maintained, or transmitted to ensure privacy and confidentiality. It also mandates that each user be uniquely identified before being granted access to confidential information. It specifies that access to personal health information (PHI) be restricted to only those individuals who need access as part of their role.
Sarbanes-Oxley	In the wake of recent financial scandals, the Sarbanes-Oxley Act of 2002 (SOX) requires public companies to validate the accuracy and integrity of their financial management. IDC believes this act will have long-term effects on federal securities regulation, corporate governance, and the regulation of auditors. SOX requires that businesses not only document and assess their internal controls but also control access to financial systems. Section 404 covers internal control activities during the creation of financial reports and points to compliance risks that can be addressed by identity and access management (IAM) solutions.
Gramm-Leach-Bliley	The Gramm-Leach-Bliley Act mandates privacy and the protection of customer records maintained by financial institutions. These security requirements include access controls on customer information systems, encryption of electronic customer information, procedures to ensure that system modifications do not affect security, and monitoring systems to detect actual attacks or intrusions.

TABLE 3

Key Regulations Driving Information Protection and Control

Regulation	Impact
ISO/IEC 27000 series	ISO/IEC 27000 series is a collection of information security standards published jointly by the International Organization of Standardization and the International Electrotechnical Commission. These standards provide best practice recommendations on information security management, risk, and controls. They provide a common basis and practical guideline for developing organizational security standards and effective security management practices. ISO/IEC 27002, which was previously known as ISO 17799, provides a code of practice on business continuity planning, system access control, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, computer and network management, asset classification and control, and security policy.
ITIL	The IT Infrastructure Library (ITIL) has seven sets of processes providing a framework for businesses in the following areas: service support, service delivery, planning to implement service management, ICT infrastructure management, applications management, security management, and business perspective.
CobiT	Control Objectives for Information and Related Technology (CobiT) was developed as a generally applicable and acceptable standard for good information technology security and control practices for management, users, auditors, and security practitioners. It was issued by the IT Governance Institute and is in its third edition. CobiT contains 34 processes and provides the tools to assess and measure an organization's ability to deliver on those processes. It was originally published in 1996, with versions 2 and 3 appearing in 1998 and 2000, respectively. Version 4 has just been released.
PCI/DSS	The Payment Card Industry (PCI) Data Security Standard was developed by MasterCard and Visa. It contains 12 requirements grouped into six areas: build and maintain a secure network, protect cardholder, maintain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy.
SB 1386	California's Information Protection Act requires companies to report security breaches involving private consumer information. Personal information is defined as Social Security number, driver's license or California ID card number, account number, or credit or debit card number in combination with a required security code, access code, or password that permits access to an individual's financial account.
PIPEDA	Much like HIPAA, PIPEDA prohibits the collection, storage, and disclosure of personal information related to an individual without that person's explicit consent. Personal information is any factual or subjective information, recorded or not, about an identifiable individual. PIPEDA provides the individual with the right to know what is being collected and change the information if it is inaccurate. Interestingly enough, U.S. and U.K. businesses may also be bound by the rules protecting Canadian citizens' personal information.
European Union (EU) Data Protection Directive	Member countries are mandated to adopt standards for the collection, storage, and disclosure of personal data. This directive also outlines individuals' rights concerning their personal data. It is described as the most ambitious and stringent data privacy initiative, and the guidelines to ensure that data is transferred outside the EU only when it is adequately protected have extraterritorial implications for businesses. The U.S. Department of Commerce worked closely with the European Commission to develop a "safe harbor" framework to enable U.S. businesses to meet EU privacy regulations.
USA PATRIOT Act, Title III (anti-money laundering [AML] regulations)	Section 352 requires financial institutions to develop internal policies, procedures, and controls to guard against money laundering. Institutions are required to track and report suspicious activities and conduct regular independent audits to test AML programs. Additional rules designed to establish a customer identification program also came into effect recently and require financial institutions to document the methods they utilize to verify a customer's identity. A consortium of global financial institutions is looking to define business processes that can be shared among networked members and invoked using Web services and a service-oriented architecture (SOA). AML has been identified as one of the key initiatives that would enable member firms to accomplish compliance at a lower cost.

TABLE 3**Key Regulations Driving Information Protection and Control**

Regulation	Impact
Homeland Security Presidential Directive 12 (HSPD-12) (policy for a common identification standard for federal employees and contractors)	The primary objectives of HSPD-12 are the development and deployment of a federal government-wide common and reliable identification verification system that will interoperate among all government agencies and serve as the basis for reciprocity between those agencies. In response to HSPD-12, the NIST Computer Security Division initiated the Personal Identity Verification (PIV) project and established the Federal Information Processing Standard (FIPS PUB 201).
Massachusetts' Standards for the Protection of Personal Information	This state regulation, which goes into effect on January 1, 2010, is a very detailed, all-encompassing set of rules designed to keep consumers' personal data safe. These regulations go beyond notification and instead define what protections businesses must employ to protect the data. Entities must identify all records used to store personal information, and they are also required to be vigilant when dealing with terminated employees so that their access to data is "immediately" denied.

Source: IDC, 2009

The stakes are extremely high for organizations that manage patient health information, Social Security numbers, credit card numbers, and other types of protected personal data; they are being forced by government and industry regulations to implement security measures to address leakage of personal information. The loss of confidential personal information can materialize into compliance infractions, lawsuits from customers and/or patients, potential identity theft, and significant and often irreparable harm to an organization's credibility and reputation.

Similarly, financial institutions must protect their consumers from fraud and identity theft. Such protection runs the gamut from authentication and securing private consumer data to making consumers whole in the event of a fraudulent loss. If consumers lose confidence in an institution's ability to adequately secure sensitive information, they will defect from both online banking and the institution. The same can be said for many other industries as well, especially retail, where customer trust and brand reputation are critical.

Preemption Is the Best Strategy

Database Security Best Practices

Enterprise systems are exposed to substantial risk from data loss, theft, or manipulation. Efforts to manage this risk are expensive and complicated because threats change quickly. As part of a preemptive IPC strategy, many enterprises are consolidating their electronic assets into database management systems. Databases allow better protection and control of access to these assets. Securing these databases is critical to protect sensitive information and comply with policy regulations.

Database security must address the following three areas: encryption and masking, access control, and monitoring and auditing.

Encryption and Masking

Encryption and masking are important for protecting data outside the access control perimeter of the database. Data sitting on disk underneath the database and applications, data in test and development environments, data traveling over the network, and data on backup media needs protection that only encryption and masking can offer. Discarded disk drives and the presence of superusers on the operating system leave open the possibility of unimpeded access to sensitive data that bypasses the authentication and access controls within the database. Movement of production data to other departments for testing and development purposes unnecessarily exposes sensitive data to individuals without a true "need to know." Data traveling over the wire is perhaps the most at risk of unauthorized access.

Access Control

Access controls beyond the application level are now vital to enabling organizations to achieve the benefits of data consolidation, offshoring, and cloud computing. Historically, applications have been designed to scale to Internet requirements and provide role-based functional access. Today, however, regulations and privacy laws require limited access to application data, even by the database administrator and especially from ad hoc tools that can be used to bypass the application.

When determining when, where, and how databases, data, and applications are accessed and by whom, enterprises must follow the least privilege principle.

Least privilege requires that users and applications have the minimal privileges required to function properly. In a database environment, this might mean that a user or application can read the data out of a specific database table but is not authorized to modify that data or even be aware of other tables in that database. This greatly improves the security of a system because there will be considerably fewer users or applications that can perform the functions attackers exploit to penetrate the system.

Associated with least privilege is separation of duties, which primarily refers to the access granted to privileged users, such as administrators. Normally administrators have full access to the systems and the underlying data they administer. They can create accounts and monitor the access logs. With separation of duties, a database administrator will be able to perform only administrative tasks and possibly not even be able to access the underlying data. It is also possible to require multiple database administrators to perform certain sensitive tasks, thus removing the ability of any one administrator to bypass the database security controls.

Monitoring and Auditing

While encryption and access control are key components for protecting data, even the best security systems are not complete without a monitoring system in place. Just as video cameras supplement audible alarms in homes and businesses, monitoring provides the corresponding who, what, and when that complements the encryption, masking, and access control systems.

Security policy must be clear and well defined at both a strategic level and a tactical implementation level. A security policy can have hundreds of components, so it is difficult to delineate what is right for any given environment. Policies work best when they are created in response to enterprise-specific needs and requirements.

To know if a security policy is working requires constant awareness. Security policies aren't effective if they are not enforced and updated to new attack vectors. Transaction logging and auditing must be enabled and reviewed proactively through alerting. In this way, it is possible to stay ahead of inside threats, detect problems when they are small, and adjust security policies as required. Full audit information is essential in demonstrating regulatory compliance.

ORACLE

Overview

Oracle (NASDAQ: ORCL) is the world's largest enterprise software company and the overall leader in the worldwide relational database management systems (RDBMS) software market. According to IDC research, Oracle has a 44% market share, well ahead of its competitors.

Oracle's Focus on Security

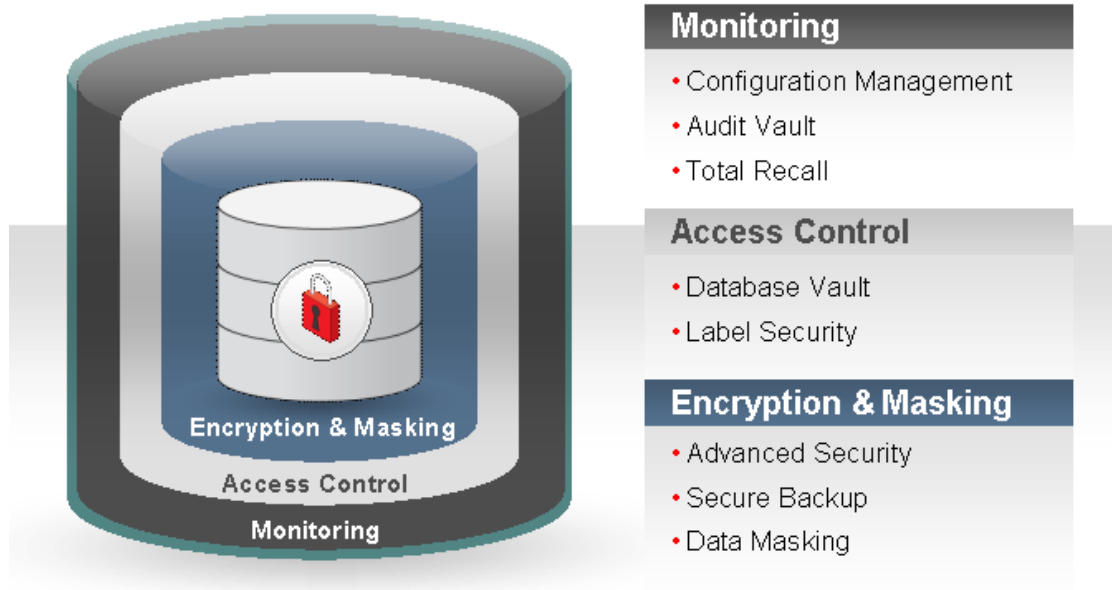
Security has been part of Oracle's heritage since the company's inception. Built upon 30 years of security experience, the Oracle Database provides defense-in-depth security controls that enable organizations to transparently protect data. Additionally, with more than 20 independent security evaluations for the database alone, Oracle remains the choice for safeguarding mission-critical enterprise information.

Oracle IPC Solutions

With solutions spanning data encryption, access control, monitoring, and auditing, Oracle provides a comprehensive information security architecture and best-in-class products. Figure 3 illustrates Oracle's database security products.

FIGURE 3

Oracle Database Defense-in-Depth



Source: Oracle, 2009

Encryption and Masking

☒ Oracle provides robust encryption solutions to safeguard sensitive data against unauthorized access at the operating system level or through theft of hardware or backup media. **Oracle Transparent Data Encryption (TDE)**, part of **Oracle Advanced Security**, addresses privacy and PCI requirements by encrypting personally identifiable information such as Social Security numbers and credit card numbers.

Oracle supports transparently encrypting specific sensitive columns with TDE column encryption or encrypting entire applications with TDE tablespace encryption. Using **Oracle Enterprise Manager**, a column can be quickly and easily encrypted or an entire encrypted tablespace can be created to store all application tables. TDE is transparent to existing applications and does not require any triggers, views, or other application changes. Data is transparently encrypted when written to disk and transparently decrypted after an application user has successfully authenticated and passed all authorization checks. Existing database backup routines continue to work, with the data remaining encrypted in the backup. For encryption of entire database backups, TDE can be used in combination with **Oracle RMAN** to encrypt backups to disk. Both TDE column encryption and TDE tablespace encryption have been certified with Siebel, PeopleSoft, and Oracle E-Business Suite applications.

TDE also supports storing the TDE master encryption key on a hardware security module (HSM) device. This provides an even higher level of assurance for protecting the TDE master key and provides centralized key management in a clustered environment.

Oracle Advanced Security provides strong protection for data in transit with comprehensive network encryption capabilities. Oracle Advanced Security's network encryption provides both native network encryption and SSL/TLS-based encryption. In addition, it can be configured to accept or reject communication from clients not using encryption, providing optimal deployment flexibility. Configuration of network security is managed using the Oracle Network Configuration administration tool, allowing businesses to easily deploy network encryption without any changes to applications.

- ☒ **Oracle Secure Backup (OSB)** encrypts tapes and provides centralized tape backup management for the entire Oracle environment and protects Oracle Database and the associated Unix, Linux, Windows, and network-attached storage (NAS) file system data. Tight integration with the Oracle Database provides optimal security and performance. OSB achieves faster backups than comparable media management utilities with less CPU utilization.

A centralized administrative server provides a single point of control for enterprisewide tape backup and any associated encryption keys. The administrative server maintains a tape backup catalog and manages security policies for distributed servers and tape devices. OSB encrypts data before the data leaves the database, resulting in continuous security for the data when in transit to the tape drive unit. OSB also provides the ability to back up and encrypt file systems directly to tape.

- ☒ **Oracle Enterprise Manager Data Masking Pack** can help organizations comply with privacy and confidentiality laws by masking sensitive or confidential data in development, test, or staging environments. The Data Masking Pack uses an irreversible process to replace sensitive data with realistic-looking values based on masking rules, ensuring that the original data cannot be retrieved or recovered.

The Data Masking Pack provides out-of-the-box mask primitives for various types of data, such as random numbers, random digits, random dates, constants, as well as built-in masking routines such as shuffling, which shuffles the value in a column across different rows. The Data Masking Pack maintains referential integrity so that applications continue to work just as they would using the original data. Oracle Enterprise Manager Data Masking Pack provides a comprehensive solution to share production data with internal and external entities while preventing sensitive or confidential parts of the information from being disclosed to unauthorized parties.

Access Control

Oracle Database provides the industry's most advanced access controls. Over the past 30 years, Oracle has innovated powerful access control features such as Virtual Private Database based on Oracle Label Security and the recently released Database Vault.

☒ **Oracle Virtual Private Database (VPD)** was introduced to address the application bypass problem and enforce row-level security. The application bypass problem exists when security is built into the application and someone accesses the application tables by using any tool other than the approved application. VPD uses the notion of a policy or function, written in PL/SQL, that returns a "where" clause. Once attached, the policy is invoked whenever the table is accessed and the resulting "where" clause is appended to the statement attempting to access the table. Database-enforced security is paramount in addressing the application bypass security problem. VPD gives customers the flexibility to program their own access control policies. Application developers can create custom application context variables that can then be referenced inside a VPD policy function and used to restrict access to specific application data no matter how the database is accessed. VPD is one of Oracle's most popular built-in security features.

☒ **Oracle Database Vault** provides enterprises with protection from insider threats and inadvertent leakage of sensitive application data. Access to application data by users and DBAs is controlled using Database Vault realms, command rules, and multifactor authorization. Database Vault addresses least privilege by separating access to application data from traditional database administration responsibilities and security administration. Database Vault realms block ANY-type privileges (SELECT ANY) commonly associated with DBAs from being used to access application data. Using multifactor authorization, access to the database can be easily restricted based on IP address, time of day, authentication type, etc. Command rules enable the Database Vault security administrator to associate rule sets or policies with Oracle Database commands. Combined with multifactor authorization, command rules allow powerful policies to be deployed inside the database, further reducing the risk associated with insiders bypassing the application.

Oracle Database Vault separation of duty enables a systematic approach to security that strengthens internal controls within the database, enabling customers to address the least privilege problem transparently. For example, customers can use Database Vault to restrict user account creation to the DBA responsible for account management. This enforcement overrides any previous account creation privileges granted to other DBAs. Thus, even if a DBA with previously granted account creation privileges attempts to create a new account, Oracle Database Vault will prevent this from happening, enforcing the separation of duties established around account creation.

Additionally, Database Vault's numerous out-of-the-box reports provide the ability to report on such things as attempted data access requests blocked by realms. For example, if a DBA attempts to access data from an application table protected by a realm, Database Vault will create an audit record in a specially protected table inside the Database Vault. Oracle Database Vault reports include a realm violation report that makes it easy to view these audit records.

The transparent nature of Oracle Database Vault is important because many customers are not in a position to make significant changes to legacy applications or analyze existing user and application privilege models.

- ☒ **Oracle Label Security (OLS)** is the industry's most advanced data classification and label-based access control solution. OLS transparently mediates access to application data by comparing the user label authorization with the sensitivity label assigned to data rows. Only if the user label authorization is equal to or greater than the data sensitivity level will access to the data be allowed. OLS was developed, in part, based on Oracle's long history of working with government customers for whom protection of classified information is a matter of national security. Application tables can contain data ranging from company confidential to highly sensitive, and restricting access to data at the row level based on data classification is becoming increasingly important, especially as data is consolidated into fewer applications. Oracle Label Security has been evaluated to the Common Criteria at EAL4. User label authorizations can be managed within the Oracle Database or centrally using Oracle Directory Services.

OLS user label authorizations can be used as powerful factors in Oracle Database Vault multifactor authorization, helping address regulatory compliance requirements and separation of duty. For example, Database Vault command rules can use OLS to determine whether a DBA should be able to execute a specific command.

Monitoring

- ☒ **Oracle Audit Vault** reduces the cost and complexity of compliance and the risk of insider threats. Oracle Audit Vault transparently collects and consolidates audit data from multiple Oracle and non-Oracle databases across the enterprise, providing valuable insight into who did what to which data when — including privileged users who have direct access to the database. Oracle Audit Vault leverages Oracle's industry-leading database security and data warehousing technology for managing, analyzing, storing, and archiving large volumes of audit data. The integrity of audit data is ensured by using sophisticated controls, including Oracle Database Vault and Oracle Advanced Security. Access to the audit data within Oracle Audit Vault is strictly controlled. Privileged DBA users cannot view or modify the audit data, and even auditors are prevented from modifying the audit data.

Oracle Audit Vault provides proactive threat detection through alerting. Event alerts help mitigate risk and protect from insider threats by providing proactive notification of suspicious activity across the enterprise. Oracle Audit Vault continuously monitors the inbound audit data, evaluating audit data against alert

conditions. Alerts can be associated with any auditable database event, including system events such as changes to application tables, role grants, and privileged user creation on sensitive systems. Oracle Audit Vault provides graphical summaries of activities causing alerts. In addition, database audit settings are centrally managed and monitored from within Audit Vault to ensure consistent auditing policies across the enterprise.

- ☒ **Oracle Enterprise Manager Configuration Management Pack** provides a policy-based vulnerability detection solution. With over 250 built-in policy rules or "best practices," it provides automated assessments for secure configurations through XML-based policy solutions for security checklists, configuration benchmarks, automated compliance testing, and compliance scoring. Example policies include checking password complexity and password reuse settings. The latest release of Oracle Enterprise Manager enables security administrators to define their own policy rules, thus strengthening their ability to monitor the enterprise configuration. The evaluation results are converted into compliance scores (based on a weighted average), and the overall scores can be presented in a compliance dashboard. The dashboard presents summaries of key indicators, with the ability to drill down to details, allowing users to continuously monitor and verify their compliance posture. Support for trend analysis provides the ability to track progress toward compliance over time for the entire IT environment.

CHALLENGES: LOOKING BEYOND CONVENTIONAL WISDOM

IPC is something all industry professionals agree is needed. Data is too important not to be protected, and it needs to go to only those who are supposed to receive it. The issue is how best to protect it. IDC research shows that most people focus on the avenues of data dissemination (email, instant messaging, or Web postings) or lost devices (laptops, smartphones, and thumb drives) when they consider IPC. The vast majority of spending on IPC is to monitor network traffic for protected information or for encryption devices. Ensuring that data isn't lost in these manners is an important consideration, but IDC believes that part of the equation is being overlooked. Database management systems must also be a component of the IPC strategy. Protecting the database through access controls, activity monitoring, and encryption makes it harder for individuals and especially attackers to access information they are not authorized to receive.

ESSENTIAL GUIDANCE

Enterprises carry high-value information within their IT systems in general and in their databases in particular. Given the high risks of not being in compliance with applicable regulations as well as internal policies, enterprise management must demand the highest levels of information security for their information systems. Organizations need to ensure that the infrastructure, including the database management system, provides strong security features. The cost of sensitive information being exposed to deliberate and/or accidental security breaches is too high for security to just be bolted on and not incorporated into the infrastructure.

IDC believes that IPC contains the solution sets required to protect sensitive information. IDC also believes that IPC will be a major area of investment over the next five years as there continue to be high-profile incidents in which customer records, confidential information, and intellectual property are leaked. The ever-growing list of government and industry standards and regulations is forcing organizations of all sizes and vertical markets to investigate, deploy, and use IPC solutions.

Organizations must move from a reactive compliance stance to proactive and cost-effective information protection and control. Enterprises must go beyond the minimum requirements of regulatory compliance to internal policy compliance at a higher level of assurance. The ability to stop malicious and noncompliant actions before they occur requires a preemptive approach that starts with protecting and controlling information *at the source* — especially the database management systems. Increasing database security is one of the most efficient and cost-effective measures an organization can take to prevent data leaks. By utilizing the data protection, access control, account management, encryption, log management, and other security controls inherent in the database management system, entities can institute first-level control over the widest range of protected information. As a central repository for unstructured data, which is growing at leaps and bounds, the database should be the first layer providing information leakage protection.

Oracle's security solutions meet customer requests for security that is natively provided within the database management system. Although complementary security components can be utilized with the database, poorly matched product pairings delivered by multiple vendors can be problematic. The better solution is to have native security that is integrated with the application without changing it. Integrated security has a better risk profile and maintains system performance, scalability, and stability. Providing security as part of the underlying database management system provides the most benefits to customers. By utilizing Oracle's encryption, access control, and monitoring solutions, customers are able to meet their goal of consolidating vendors.

IDC believes that Oracle, already the largest relational database management system vendor, with over 44% of the market in 2008, offers a comprehensive, well-integrated set of security components. Its solutions provide considerable customer value by mitigating insider threats, making regulatory compliance easier, and protecting data through better data management. Oracle's innovative security capabilities, especially in the areas of data protection and access control, can be applied today and are some of the most advanced solutions available. With built-in and transparent solutions, such as those offered by Oracle, enterprises do not have to trade performance for security or settle for lowest-common-denominator capabilities designed to work across different vendor databases. Oracle's security solutions represent the best in breed for Oracle databases and provide a strong incentive for organizations to continue to select Oracle as their database management system vendor.

Any enterprise looking to improve its competitiveness, regulatory compliance, and overall data security should consider Oracle's offerings, not only because of their database management capabilities but also because they provide tools that are the first layer of information leak prevention.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2009 IDC. Reproduction without written permission is completely forbidden.