IDC
Analyze the Future

## WHITE PAPER

# Oracle Database Security: Preventing Enterprise Data Leaks at the Source

Sponsored by: Oracle Corporation

Charles J. Kolodgy
Brian E. Burke
Gerry Pintal

February 2008

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

## IDC OPINION

Information has become the world's new currency. Databases are the digital banks that store and retrieve valuable information. The growing number of high-profile incidents in which customer records, confidential information, and intellectual property are leaked (or lost/stolen) has created an explosive demand for solutions that protect against the deliberate or inadvertent release of sensitive information. Moreover, numerous information-intensive government and industry regulations are requiring organizations to protect the integrity of customer and employee personal information and corporate digital assets. Security breaches can no longer be "swept under the rug" because of strict breach disclosure laws.

Addressing information protection and control (IPC) is a complex challenge. Today, nearly all corporate information exists in electronic form, typically stored in databases, so it stands to reason that enterprises must secure their databases as part of any IPC strategy to protect sensitive information and comply with policy regulations. As attackers are much more likely to be cybercriminals who are financially motivated, it is more difficult to deter them with a minimal amount of security. Database security represents a preemptive approach to preventing enterprise data theft and regulatory compliance infractions.

IDC believes that no IPC strategy can be effective unless information is properly 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.

## 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 within or outside the enterprise in violation of regulatory or company policies. This white paper also highlights how Oracle provides security products that enterprises can leverage to protect themselves from costly data breaches.

## Approach

IDC developed this paper in January 2008 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 as Currency*

For the vast majority of organizations, some of their greatest assets consist of digital bits of information, intellectual property, and data stored in databases, file management systems, flat files, spreadsheets, and other information storage formats, not their physical holdings. Database servers hosting the data are critical components of a successful business.

The demand for solutions that protect sensitive information was originally fueled by industries (e.g., financial services, banking, healthcare) that needed to comply with various government and industry regulations (e.g., Health Insurance Portability and Accountability Act [HIPAA], Gramm-Leach-Bliley [GLB], Sarbanes-Oxley [SOX]). In 2006 and 2007, a series of high-profile incidents in which customer records and confidential information were leaked (or lost/stolen) created an explosive demand for solutions outside the heavily regulated industries. A privacy failure, or even the mere perceived failure to protect customer data, can result in loss of consumer trust, affect customer retention, and cause significant damage to brand and company reputation.

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, which run 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.

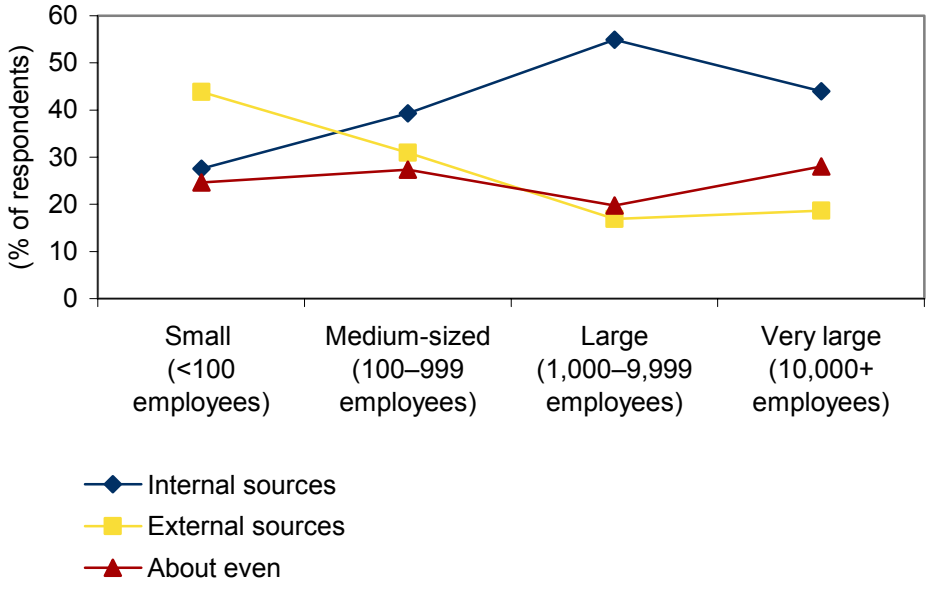
Any organization with sensitive personal or financial data represents a potential target. New attack vectors are going for the "business jugular." Criminal elements are conducting targeted attacks on financial assets, reputation, or sensitive proprietary data from inside the business. In one extreme example, newly hired employees were planted for the specific purpose of stealing customer credit information. These new forms of creative attacks are proving to be difficult to detect in part because they are a blend of interconnected security weakness and because they emanate from individuals believed to be trusted corporate insiders. All of these developments require improved IPC mechanisms.

### *Internal Threats Versus External Threats*

According to IDC's 2007 *Enterprise Security Survey* of 433 North American IT professionals, internal sources are believed to pose a greater threat to the enterprise than external sources. The gap between internal and external threat concerns is much more pronounced within large enterprises, as shown in Figure 1. 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 been growing.

**FIGURE 1**

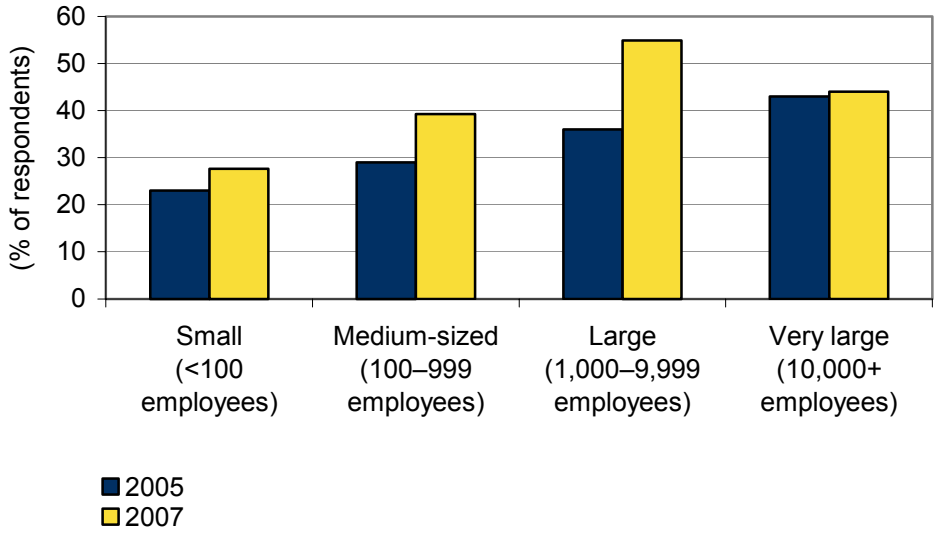
Origin of Most Serious Threats: Internal Sources or External Sources?




Source: IDC's 2007 *Enterprise Security Survey*

**FIGURE 2**

Internal Threats Are Considered Most Serious




Source: IDC's 2007 *Enterprise Security Survey*

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

- 80% of very large organizations (10,000+ employees) and 52% 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 15% of large organizations (1,000–9,999 employees) have prosecuted an employee for internal security violations.

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 in 2006, $900 million was made in the buying and selling of stolen and compromised identities. 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.

1. In 2007, employee error ranked as the greatest threat to enterprise security. 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.

2. Data stolen by an employee or a business partner ranks as the fifth-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.

3. Insider sabotage ranks 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. 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. Figure 3 illustrates the perceptions of the greatest threats enterprises saw in 2007.

**FIGURE 3**

Most Significant Threats to Enterprise Security


Source: IDC's 2007 *Enterprise Security Survey*

### *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 some malfeasance or spectacular failure. Government and industry regulations remain a key driver for IPC implementations, as shown in Table 1. 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 SOX, GLB, HIPAA, European Union Data Protection Directive 95/46, 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 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, which 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 1**

Key Regulations Driving Information Protection and Control

| Regulation | Impact |
|---|---|
| HIPAA | The Health Insurance Portability and Accountability Act of 1996 requires that to ensure privacy and confidentiality, all patient healthcare information be protected when electronically stored, maintained, or transmitted. 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. |
| ISO 17799 | ISO 17799 is a detailed security standard organized into 10 major sections: 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. The objective of ISO 17799:2005 is to provide a common basis and practical guideline for developing organizational security standards and effective security management practices. |
| 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 now 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. CobiT is in its fourth version. |
| PCI | 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 data, 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. |

**TABLE 1**

Key Regulations Driving Information Protection and Control

| Regulation | Impact |
|---|---|
| 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 | 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 anti–money laundering (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. |
| Homeland Security Presidential Directive 12 (HSPD-12) | 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). |

Source: IDC, 2008

## Preemption Is the Best Strategy

### *Database Security Best Practices*

Enterprise systems are exposed to substantial risk from data loss, theft, and 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 four areas:

1. **User management.** Centralized database user management and strong authentication help address compliance and insider threat challenges, especially for organizations with large-scale databases and user populations.

2. **Access control.** Complying with stringent internal control requirements found in regulations requires controlling access to databases, applications, and data from within the database and reducing enforcement at the application level. This also reduces the risk of ad hoc access to application databases bypassing the actual application. When determining who accesses databases, data, and applications as well as when, where, and how databases, data, and applications are accessed, 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 an 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.

   Separation of duties is associated with least privilege and primarily refers to the access granted 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 only be able to perform 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.

3. **Data protection.** Encryption is often the first thing that comes to mind when one thinks of data protection. When done properly, encryption is the best way to prevent unauthorized access to data once it leaves the database either over the network, on backup tape, disk, or export file. If data leaves the database, encryption is the only protection available. Database encryption can be achieved with third-party applications or natively by the database. The key differentiators are transparency, performance, and key management. Does the application have to be changed to call database triggers and reference views? How well does the solution produce, retrieve, archive, change, and destroy encryption keys? Encryption is an indispensable component of data protection if it is transparent, performs well, and provides built-in key management capabilities.

4. **Security policy monitoring and audit.** 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. They must provide the proper guidance to secure the database management systems, and they must be enforceable. The most effective security policies are those that can be set and enforced directly within the database. This helps remove user error and also reduces barriers associated with strong security. Security policy is used to establish parameters, such as defining trusted and privileged users, what their roles are, what they can do with data, how long passwords need to be, how often they need to be changed, the classification of information stored in the database, and whether all data or only sensitive data will be encrypted.

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 the inside threats, and detect problems when they are small, adjusting 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 44.4% market share, which is well ahead of its closest competitor.

## Oracle's Focus on Security

Security has been part of Oracle's heritage since the company's inception. For decades, Oracle has been an innovative force for database security solutions. A nonstop series of industry firsts, including the first network encryption, the first row-level security, the first fine-grained auditing, and the first transparent data encryption, has earned Oracle a reputation for being at the forefront of security. Coupled with an industry-leading 19 independent security evaluations for the database alone, Oracle remains the choice for security-aware organizations.

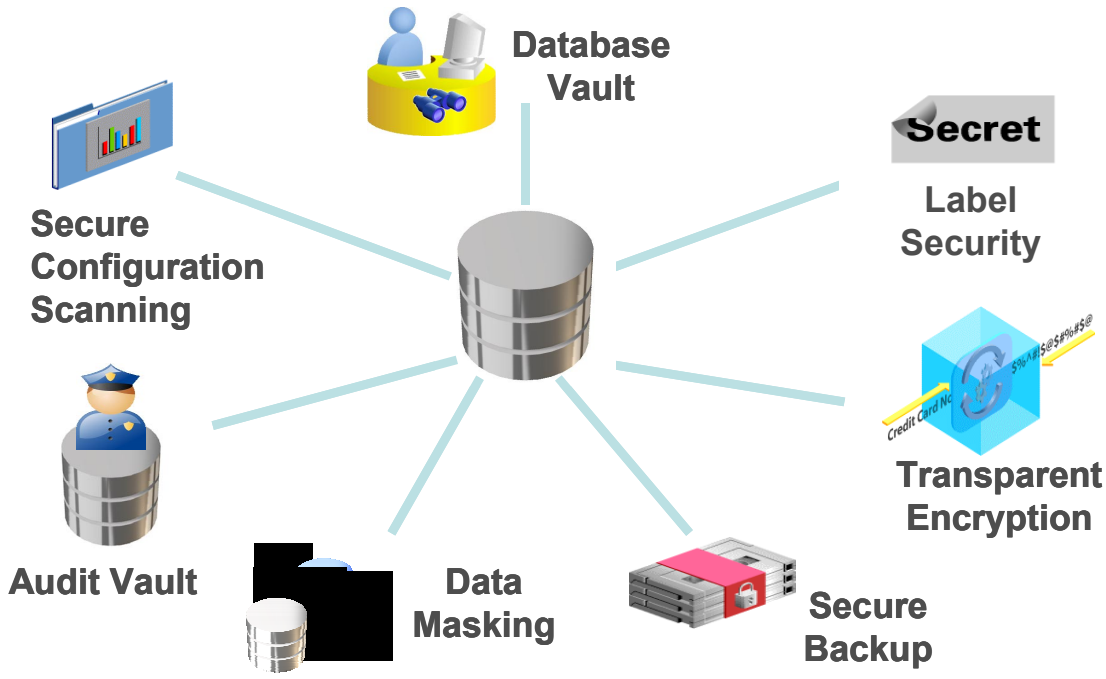
## Oracle IPC Solutions

With solutions spanning user management, access control, data protection, and monitoring/alerting for compliance management, Oracle provides a comprehensive information security architecture and best-in-class products. Figure 4 illustrates Oracle's database security products.

**FIGURE 4**

Oracle Database Security Products




Source: Oracle, 2008

## User Management

Oracle Enterprise User Security simplifies user management by enabling database user accounts to be centrally managed in the Oracle Internet Directory, the core of Oracle's Identity Management suite. Oracle Directory Synchronization Service, part of the Oracle Internet Directory, permits synchronization between Oracle Internet Directory and other directories and user repositories such as Microsoft Active Directory and SunONE, allowing users to authenticate to the database using credentials stored in one of these other repositories. Enterprise User Security provides support for strong authentication based on PKI digital certificates or Kerberos.

Additionally, users can individually authenticate using a password or strong credentials and be mapped to a single database account, thus simplifying database user management and increasing security. For example, a single database account called "Org A" could be defined in the Oracle Database and users in Business Unit A could be mapped to this account once they are individually authenticated external to the database. This reduces the need for creating individual user accounts in the database, greatly simplifying monitoring and audit.

Oracle's Identity Management suite provides a number of other capabilities that can be used to increase security and regulatory compliance.

## Access Control

The 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, accessing the database can be easily restricted based on IP address, time of day, 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, Oracle 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, Oracle Database Vault will create an audit record in a specially protected table inside the Database Vault. The product includes 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 where 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.

## Data Protection

It is imperative that data be protected. The best way to protect the confidentiality and integrity of data is with encryption. Oracle, in supporting strong data leakage protection, provides inherent encryption capabilities.

- **Oracle Advanced Security** helps customers address regulatory compliance requirements by protecting sensitive data on the network, on backup media, or within the database from unauthorized disclosure. Oracle Advanced Security Transparent Data Encryption (TDE) provides the industry's most advanced encryption capabilities for protecting sensitive information without requiring any changes to the existing application. TDE is a native database solution that is completely transparent to existing applications with no triggers, views, or other application changes required. Data is transparently encrypted when written to disk and transparently decrypted after an application user has successfully authenticated and passed all authorization checks. Authorization checks include verifying the user has the necessary read/update privileges. TDE can be used to encrypt columns that contain sensitive data or entire database objects residing

in a tablespace. Tablespace encryption ensures all database objects are encrypted at the file system level. When the database reads data blocks from the encrypted tablespace, it will transparently decrypt the data blocks. 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** also provides strong protection for data in transit with comprehensive network encryption capabilities. Oracle Advanced Security's easy-to-deploy and comprehensive 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)** is Oracle's comprehensive tape backup solution for Oracle Databases and file systems. Tight integration with the Oracle Database provides optimal security and performance, eliminating backup of any associated database UNDO data. 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 but scrubbed data based on masking rules and ensures 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 helps maintain the integrity of the application while masking data. Oracle Enterprise Manager Data Masking Pack provides a comprehensive, easy-to-use 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.

## Monitoring

As previously illustrated, meeting compliance requirements is a key component for data leak prevention. It is important to be able to audit the activities of a database and, when required, alert to policy violations. Oracle has a strong set of auditing capabilities around its database products.

- **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 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: A QUESTION OF TRUST

With the growing concern about insider access to critical information, enterprises need to limit the access provided to insiders, especially to administrators. Oracle Database Vault is a mechanism to protect information from the insider threat. However, limiting permission may cause individuals to feel that they are not trusted by the organization. Oracle must "win over" DBAs who may not be too enthusiastic to implement this security. IDC believes that the DBAs will embrace this technology when they realize it protects them from scrutiny should an incident occur. When a bank is robbed, the tellers are considered suspects and their actions are scrutinized. By utilizing Oracle's Database Vault, strong security features, and products, the DBA is not the first suspect.

## 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. The cost of sensitive information being exposed to deliberate and/or accidental security breaches is too high.

IDC believes that information protection and control contains the solution sets required to protect sensitive information. IDC also believes it will be a major area of investment over the next five years. 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. Nevertheless, we expect to see more examples of high-profile incidents in which customer records, confidential information, and intellectual property are leaked. These incidents will continue to fuel the demand for IPC solutions for data at rest, data in motion, and data in use.

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 effective means an organization has to prevent data leaks.

IDC believes that Oracle offers customers a comprehensive, well-integrated set of security products that address both insider threat mitigation and regulatory requirements. 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. Built-in and transparent solutions such as those offered by Oracle mean that 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 select Oracle as their database management system vendor.

Enterprises looking to improve their competitiveness, regulatory compliance, and overall data security should consider Oracle's offerings.