The Smart Choice: IPLocks Information Risk Management Platform with Oracle Database

January 2005

IPLocks, Inc.

441-A W. Trimble Road, San Jose, CA 95131 USA

www.iplocks.com

IPLocks Information Risk Management Platform with Oracle:

The Smart Choice

Background

In the face of increased insider theft and a proliferation of government regulations on information privacy and financial statement integrity, organizations face increasing pressure to effectively secure their critical databases, and monitor the use of the databases to assure that they are being accessed in an appropriate and expected manner.

To help you protect your databases, Oracle provides a comprehensive collection of information security tools that include:

- Identity Management (identifying and authenticating users through single sign-on);
- Access Management (controlling user access to privileges and objects, and security labeling);
- Policy Management (using security labels and the Virtual Private Database)
- Privacy protection (through layered security and encryption);
- Extended Enterprise protection (employing Oracle Advanced Security)
- Detail and Selective Auditing (policy-based triggers, event-handlers, alerts)

These are competent, industry-leading tools that can help an organization competently secure its databases and information. Even so, there is opportunity for significant improvement through complementary and alternative tools that use advanced vulnerability assessment, auditing, and analysis techniques. The key factors that drive the need for enhanced tools are:

- The insider threat
- Information privacy and financial integrity regulations
- The scope and scale of other potential security threats
- Volume and complexity of transactions and information
- Challenges to effective information security implementation

We explain each of these factors in the sections that follow. What becomes clear is that as it becomes more difficult and less productive to establish and maintain effective access restrictions, there is an increasing need for sophisticated, automated computer-based tools to empower and enable an organization to frequently reassess database vulnerabilities, monitor your Oracle databases non-stop for appropriate access and use, and alert you to unusual or suspicious events.

The Insider Threat

It is well documented that insiders cause and have been causing most computer-based crime (crimes against computers or using computers as a tool). It is clear that insiders either exploit the privileges that they are given to do their jobs, or they exploit weaknesses in the organization's business process and information security controls. Enhanced auditing and analysis tools are your best defense to protect your databases from insider tampering.

Information Privacy and Financial Integrity Regulations

The recent flood of regulations provides organizations with an abundance of guidelines on what they should accomplish. However, the regulations provide precious little specifics on how the guidelines should be achieved. This can place the I.T. organization and the database administrator in the center of conflicting objectives to restrict access and accessibility on the one hand, and to enable and empower the organization through information access and integration on the other. This suggests that a balance needs to be established between restrictive access management and information empowerment. Wherever the balance-line is drawn, the empowerment side of that line will leave opportunities for exploitation and, again, increased vigilance is necessary to guard against misuse of privileges.

The Scope and Scale of Other Threats

Today's database environments are incredibly complex, and can extent outward to customers, partners, suppliers and other third parties through Web applications and remote access solutions. There is your database, and then there is the rest of the world with all of its risks, vulnerabilities, threats, and layers of information security controls. Your last line of defense is at the doorway to your Oracle database. While you want to be able to rely on your established information security controls to protect your database, you can greatly increase the effectiveness of those controls by closely watching the changes taking place directly in the database.

The Volume and Complexity of Transactions and Information

We've long ago gone beyond measuring our information in kilobytes and megabytes. Now, we've moved beyond terabytes and into petabytes. The amount of information that we retain in our databases is staggering and confounds the imagination. To get all of this information and put it to good use for the organization, we are seeing transaction counts in the millions and higher, and analytical reporting requirements that drive query volume off the scale. An organization cannot invest in enough people to establish effective vigilance over this volume of activity and information. Automated, computer-based and intelligent tools must be deployed to do the job.

The Information Security Implementation Challenge

There exist a number of real and practical challenges to the implementation of effective Oracle security using the controls provided. Effective security implementation requires a comprehensive understanding of the organization's Oracle environment, resources, relationships and security requirements; a sound and comprehensive security strategy and plan; the implementation of identity and access controls that provide and maintain sufficient security without unnecessarily restricting valid business activities; and continued monitoring to assure that controls remain effective without inhibiting valid functionality. To meet these challenges requires full management support, a standardized and well-documented database environment and, more particularly, a database environment that has been designed with security top of mind. Beyond these operational requirements, you will need knowledgeable security leadership and adequate staffing to perform the full range of security analysis, design, implementation, administration, and monitoring activities. There can be breakdowns in any or all of these requirements in most organizations, and only few companies may manage to achieve competence in all of them. As a result, even with the best controls available, most organizations can fall well short of fully effective Oracle security.

IPLocks Information Risk Management Platform

IPLocks is designed to Complement and Enhance Oracle Security

Oracle security provides information security capabilities such as Identity Management, Access Management, and Security Labeling to enable you to implement your information security strategy and policy, balancing security requirements against the organization's need for access and accessibility. Oracle security also provides logging, auditing and alert capabilities to help you maintain vigilance over your database and how it is accessed and used.

IPLocks Information Risk Management Platform does not attempt to duplicate the functionality provided by Oracle security. Instead, we provide capabilities that independently complement and enhance those controls, taking the capabilities to a more advanced state, as illustrated by the following features:

- ***Independent Auditing***: IPLocks auditing capabilities enhance and extend Oracle security in several ways:
  - First, IPLocks auditing is independent of the Oracle platform both in physical implementation and operation. Independence makes the audit environment more "tamper-proof" thereby increasing both the completeness and the credibility of audit results, providing a neutral audit capability cannot be easily repudiated.
  - Second, IPLocks does not burden the Oracle database environment with additional writes to Oracle log files. IPLocks "listens" to and records the SQL traffic to your databases and independently logs to IPLocks own secure Oracle database.
- ***Best Practices Auditing***: While Oracle's auditing capability enables you to focus your audit activities, IPLocks takes this quite a bit further and our Vulnerability Assessment tool performs a "best practice" assessment of the Oracle DBMS and recommends Oracle best practices, and other best practices established by IPLocks own consulting group. Using IPLocks Vulnerability Assessment (CVA) tool, best practice auditing can be performed in a consolidated approach across geographically dispersed Oracle databases.

IPLocks best practice auditing includes Oracle database configurations, privileges, and the database architecture. Common configuration vulnerability assessments in IPLocks include: Over 40 database configuration settings and conditions; more than 20 Oracle database vulnerabilities including password vulnerabilities (default passwords, blank passwords, etc.); database patches; unencrypted DBLink password; NO ADMIN OPTION; and sensitive permissions such as permissions to modify system tables, or to PUBLIC; permissions to execute system procedures; and direct user permissions.

Other tests and assessments include:

- ***Penetration Testing***: Using the IPLocks database auto-discovery capability, brute force attacks can be launched against each database to identify weak passwords that could be easily compromised.
- ***Privileges Monitoring***: IPLocks monitors privilege changes using a comparison of database catalog snapshots to enable you to identify unauthorized changes. Pre-defined rules are referenced to identify acceptable and inappropriate privilege settings and privilege roles for Oracle system and schema object privileges as set in the Oracle data dictionary views.
- ***Meta Data Monitoring***: IPLocks monitors changes to database schema objects, using a comparison between system catalog snapshots in time. Changes to all schema objects are identified and reported including tables, views, triggers, synonyms, packages, and tablespaces.

- ***Behavioral Analysis***: Well-beyond simple auditing and event tracking, IPLocks provides a unique, full behavioral and intelligent analysis of users and their actions against the database, establishing patterns of normal behavior. This powerful User Behavior Monitor (UBM) capability enables IPLocks to learn how your database is accessed, uses this “intelligence” to identify unusual activities and behaviors, and alert the security officer and auditor for follow-up investigation. This monitoring is targeted to specific objects, users, and sessions that you deem sensitive due to corporate policy or regulations. The UBM relieves the security officer and auditor of the need to sift through mountains of data and transactions to try to manually identify those events of interest and, within those, the events that are unusual or out of norms. Oracle access violation events (violation, suspicious OS or DB user, location, or multiple dimension object rule) and access frequencies (time violation, OS or DB user and time, terminal and time, and multiple dimension object rule) can be set to further customize the monitor.
- ***I.T. Policy Development***: IPLocks provides tools to assist the security officer in the formation of database use policies through examination of standard and non-standard database transactions and activities. By identifying specific representative objects that are sensitive from a Sarbanes-Oxley or privacy standpoint, the security officer can perform targeted analysis of access to those objects to identify access patterns, review the access patterns with business process owners, and help in the identification of appropriate and inappropriate access activities in terms of who, what, when, and where. This information enables the definition of relevant security policies to specifically allow appropriate activities and prohibit those that are deemed inappropriate.

About IPLocks

IPLocks, Inc. protects business continuity, safeguards company brand reputation and eases the pain of corporate governance by securing critical information assets from negligent and malicious acts.

The IPLocks Information Risk Management Platform alerts management to information risks from security and business policy violations, attacks on data, compromised structural integrity and information theft, which other security solutions fail to detect.

IPLocks secures business critical data for financial services, telecommunications, media services, healthcare, public utilities and other industries. Founded in 2002, San Jose, California-based IPLocks is a privately held global corporation with customers throughout North America, Asia Pacific, South America and Europe. For additional information, visit www.iplocks.com.