

Enterprise Rights Management: Comprehensive User Discovery

The business demands placed on today's enterprise organizations require that a wide range of users have access to company data. Users include internal employees, external consultants, partners, and clients.

As the scope of projects at large organizations expand, employee roles and groups often change. With these changes, it is not uncommon to see the emergence of toxic combinations of access controls to sensitive information. These inappropriate user entitlements often violate separation of duties controls and increase the risk of a potential breach.

The more conduits to data that exist on a corporate network, the more opportunities there are to exploit those access points—resulting in a greater risk of internal and/or external attack.

Malicious insiders are prevalent in today's enterprises. Research indicates that 48 percent of data breaches can be attributed to an insider attack¹. In addition, 48 percent of breaches are the result of privilege misuse, meaning that employees with certain levels of privileges to sensitive data are not adhering to the policies and controls set forth by organizations.

As a result, enterprises now face increasing data security, risk, and compliance challenges. In many cases the cause of this increased risk is a lack of understanding of the number of people with access to sensitive data – or the failure to implement proper controls to ensure that those with access,

have the appropriate levels of access on an ongoing basis. Unfortunately, most organizations rely on manual and time-consuming processes to conduct user entitlement reviews—the process by which an organization examines its overall data access privileges. These manual processes are not only insufficient - they are often error prone and inaccurate. Most companies cannot afford to stretch their resources with a time-consuming project that will not produce the desired result. It has become critical for organizations to proactively implement user entitlement best practices to ensure that appropriate access and ownership rights are assigned to critical data. The failure to conduct a full user rights review increases an organization's risk of data access abuse.

At the database level, there are vulnerabilities and configuration issues that exist across database applications that can be exploited. And there are specific processes that organizations should implement in order to effectively manage user rights.

This paper will discuss those processes, provide context of existing vulnerabilities, and present a best practices approach for ensuring continuous compliance through an effective rights management process.

¹ Verizon Business Data Breach Report, 2010

² Verizon Business Data Breach Report, 2010

ROLES AND RIGHTS – WHO, WHAT, WHEN, WHERE AND HOW?

In large enterprises, managing user rights ensures that appropriate data privileges have been assigned. In many organizations, rights management is a manual and reactive process.

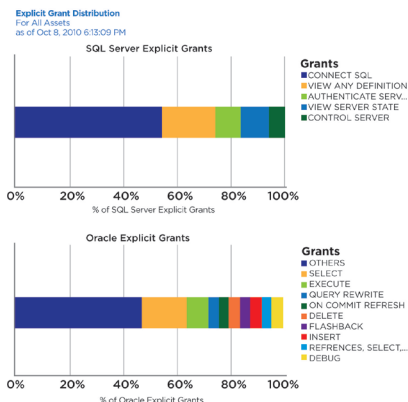
The process is typically undertaken as a requirement of a compliance audit, or as a reaction to a security breach. As part of the process, an IT organization is saddled with having to identify users, examine data access, and determine appropriate privileges. This is typically undertaken as a manual process which significantly increases the odds of human error resulting in inaccurate findings and controls.

Common sense dictates that the fox should not be left to watch the henhouse, but adhering to that dictate in regard to database security can be a major challenge for even the most sophisticated organization. End users require access to database applications to perform their jobs. The more they are responsible for, the greater the access privileges they require. The greater level of access privilege they are granted, the less control organizations are able to exercise.

This reality raises the following three key questions:

- How much business risk is acceptable for a given degree of access privilege?
- What controls are appropriate to govern access to specific types of sensitive data?
- What level of privilege should be granted to each type of sensitive data?

Rights Management
Are there excessive rights?



Explicit Grant Distribution

- Managing security best practices- granting to roles
- Find who has been given direct access

To manage these access control challenges, audit firms recommend implementing the Principle of Least Privilege, which suggests that employees be entitled only to as much database access as is required to perform their job. The concept of least privilege makes perfect sense, but in reality, this implementation is much more difficult than it appears. Database utilities lack appropriate reporting tools to manage least privilege implementations. As a result, entitlement reviews are typically complex and time-consuming.

It is estimated that a manual entitlement review of a typical database can take in excess of 80 man-hours to complete. Streamlining this process through the use of an automated solution allows organizations to discover, manage, and eliminate excess permissions in a manner that is consistent with business and compliance requirements.

DbProtect Rights Management

Inventory All Users with DBA Privileges

IP/PORT	Database Type	Role Type	Role
192.168.2.63:1521	Oracle® Database	Oracle Role	AQ_ADMINISTRATOR_ROLE
192.168.2.63:1521	Oracle® Database	Oracle Role	AQ_USER_ROLE
192.168.2.63:1521	Oracle® Database	Oracle Role	CONNECT
192.168.2.63:1521	Oracle® Database	Oracle Role	CTXAPP
192.168.2.63:1521	Oracle® Database	Oracle Role	DBA
192.168.2.63:1521	Oracle® Database	Oracle Role	DELETE_CATALOG_ROLE
192.168.2.63:1521	Oracle® Database	Oracle Role	EXECUTE_CATALOG_ROLE
192.168.2.63:1521	Oracle® Database	Oracle Role	EXP_FULL_DATABASE
192.168.2.63:1521	Oracle® Database	Oracle Role	HS_ADMIN_ROLE
192.168.2.63:1521	Oracle® Database	Oracle Role	IMP_FULL_DATABASE
192.168.2.63:1521	Oracle® Database	Oracle Role	JAVA_ADMIN
192.168.2.63:1521	Oracle® Database	Oracle Role	JAVA_DEPLOY
192.168.2.63:1521	Oracle® Database	Oracle Role	JAVADERUGPRIV
192.168.2.63:1521	Oracle® Database	Oracle Role	JAVADPRIV

Role Type	Role
Oracle Role	AQ_ADMINISTRATOR_ROLE
Oracle Role	AQ_USER_ROLE
Oracle Role	CONNECT
Oracle Role	CTXAPP
Oracle Role	DBA
Oracle Role	DELETE_CATALOG_ROLE

Oracle User	SCOTT
Oracle User	SYS
Oracle User	SYSTEM
Oracle User	VIKING

WHO SHOULD I BE CONCERNED WITH?

CSO's must be concerned with employees within their organization, but they must also be concerned with individuals outside the organization.

Employees with inherited roles that grant a certain level of access to a database or group of database instances are often overlooked by IT and IT Security organizations. It is often forgotten that this granular level of access control could represent a major set of vulnerabilities in the security process.

New employees may be credentialed as if they were a former employee. Although the new employees' roles and responsibilities may be different or evolving, simply assigning inherited privileges assumes those credentials are essential for job performance.

Another example is an employee who has access to data that is non-essential to perform his job. It could be confidential customer data or transaction data at a brokerage house. Or it could be electronic health records (EHR's) at a hospital or provider. This is an unacceptable scenario because access to non-essential information leaves data vulnerable to compromise.

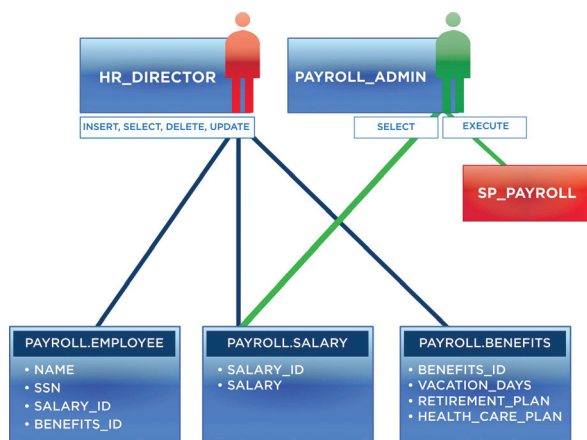
Many organizations don't have the time or resources to deal with these seemingly simple problems. And many fail to take the time to define a comprehensive process to determine roles and privileges related to database access. With attacks increasingly targeting the database, and with insider attacks on the rise, this poses a threat not just to the integrity of the data, but to the viability of the company.

The Malicious Insider

- Typically has privileges providing excessive access to information that exceeds those necessary to perform their duties
- Could be a disgruntled employee, or an employee working in concert with a criminal organization. Information typically not stolen in a single attack, but compromised over time.

The Inherited Role

- Employee replacement (permanent or temporary) may have inherited excessive privileges through the inheritance of a database role that grants access to specified databases and specified sets of data.
- Through this inherited role, the employee may have excessive privileges. They may not need as much access as they now have, or rights to a specialized data set.



Separation of Duty is the principal that requires that the certifier and the implementer of an action be different entities.

Inappropriate Access

- Misassigned access levels providing excessive privilege based on responsibilities. For example, if an HR Director is assigned privileges such as SELECT, INSERT, UPDATE, DELETE, or DENY on a payroll database despite the fact that this level of access is not necessary or appropriate.

EXAMPLES OF EXCESSIVE PRIVILEGES IN THE DATABASE (FROM THE TEAMSHATTER KNOWLEDGEBASE)

Database management systems are highly sophisticated applications that demand constant attention. Businesses demand uptime, but when a security breach occurs, administrators typically disable the database to limit further damage.

When databases are not properly secured, they are vulnerable. And when organizations don't properly assign appropriate access privileges, risk is increased.

It is important for organizations to know what vulnerabilities exist on database applications. The following are a few samples from the SHATTER knowledgebase of database vulnerabilities and misconfigurations that are commonly present in enterprise database systems.

1. BUILTIN\Administrators member of SYSADMIN fixed server role

The SYSADMIN fixed server role grants all database privileges to assigned members. The BUILTIN\Administrators group of the host server should not be granted the SYSADMIN role. Doing so inappropriately provides all local administrators on the Windows host DBA privileges on the database server and separation of duty controls are not appropriately enforced.

Security should be enforced by revoking DBA privileges from all operating system users. This is accomplished by revoking the sysadmin role from the BUILTIN\Administrators group. Instead, create a separate Windows group containing the appropriate DBAs and grant the group the sysadmin role in the database.

2. Account can grant any role

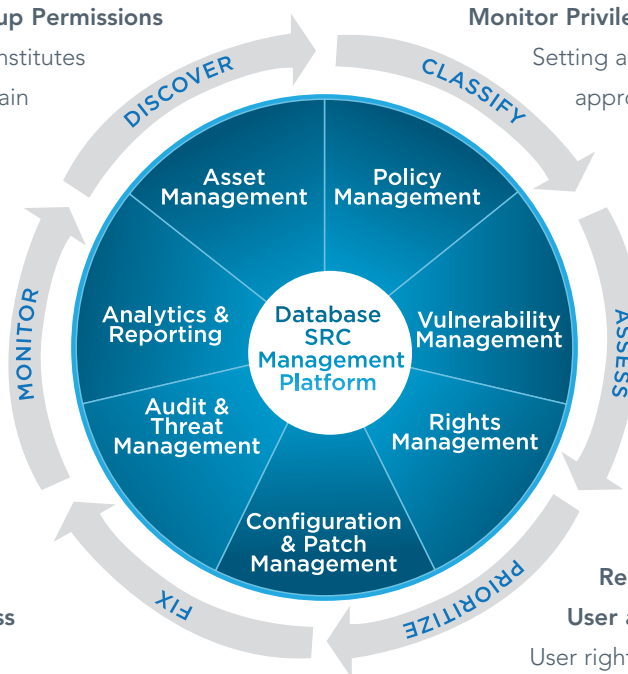
External applications spawned by the DBMS process may be executed under OS accounts which

Identify Appropriate User and Group Permissions

Organizations should define what constitutes appropriate access to the data. Certain users and groups of users who might be responsible for special database projects require robust levels of access while other users need permissions only for specific types of data. Defining what's appropriate and assigning privileges judiciously enables an organization to be ready to deploy technology that can automate the process.

Implement Appropriate Data Access

Setting the appropriate access levels for internal employees is just as important as establishing controls for external users. Once the internal and external access policies are established and users are informed, companies should maintain consistent enforcement of these standards to prevent violations and minimize human errors.



Monitor Privileged User Access

Setting access controls, establishing what's appropriate, and identifying all users is not enough. The probability of data misuse always exists. Activity monitoring should be used to identify any potential misuse. Deploying a scalable database monitoring solution allows an organization to identify users, establish appropriate permissions, and locate excessive or unusual database activity.

Regularly Update Policies Based on User and Organizational Changes

User rights management is a continuous process and is a critical component of the database security risk and compliance lifecycle. As individuals are hired, terminated, or leave willingly, roles will change, and access controls should be adjusted accordingly. The database environment is not static and it is essential that users and policies be continuously reevaluated and reinforced.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSec is a pioneer and leading provider of database security, risk and compliance (SRC) solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSec supports the database lifecycle for some of the most complex and demanding environments in the world across more than 2,500 commercial and government customers.

Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, [TeamSHATTER](#), AppSec products help customers achieve unprecedented levels of data security from nefarious or accidental activities, while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: www.appsecinc.com | www.teamshatter.com

For a free database vulnerability assessment visit: <http://www.appsecinc.com/downloads/appdetectivepro>

Follow us on Twitter: [www.twitter.com/appsecinc](https://twitter.com/appsecinc) | [www.twitter.com/teamshatter](https://twitter.com/teamshatter)

**APPLICATION
SECURITY, INC.**[®]

www.appsecinc.com