IMPERVA®

User Rights Management for Databases (URMD)

Audit and Validate User Access Rights to Sensitive Data

User Rights Management for Databases Benefits

- Enables automated, repeatable process for reviewing access rights (SOX, PCI 7, and PCI 8.5)
- Automates the process of aggregating user rights across all corporate databases into a single repository
- Streamlines reporting and analysis of user access rights to sensitive data
- Supports comprehensive investigation of excessive user rights and validates user access rights are on a need-to-know basis
- Identifies dormant accounts and un-used access rights which can be disabled or removed

User Rights Management for Databases (URMD) enables security, database administrators, and audit teams to focus on rights associated with sensitive data and identify excessive or dormant rights based on organizational context and actual usage. Using URMD, organizations can demonstrate compliance with regulations such as SOX, PCI 7, and PCI 8.5 and reduce the risk of data breach.

Audit: Aggregate and Report on Access Rights Across Databases

URMD streamlines the process of aggregating, consolidating, and reporting on user access rights across heterogeneous enterprise databases. The automated audit process significantly reduces the time and resources required for gathering user rights. Consolidated reports provide a full overview of user rights across all databases and enable reviewers to focus on changes since the last review.

Investigate: Does the User have Access to Sensitive Data?

SecureSphere database security solutions enable organizations to map out databases and discover where sensitive data resides on the corporate network. Data Classification provides insight into the different types of sensitive data that are stored in database objects. URMD correlates the user rights with information about the object's sensitivity, allowing organizations to focus on analyzing access rights to sensitive data which represents the highest business risk.

Validate: Should the User Have Access to Sensitive Data?

Access to sensitive objects needs to be granted based on 'Need-To-Know' which is typically defined by the users' organizational context. By adding details such as the user role and department, reviewers have full visibility into the user job function and the type of data he/she can access. URMD's analytical views provide reviewers with the ability to determine if the user access rights are appropriately defined and enable the removal of excessive rights that are not required for the users to do their job.

Mitigate: Remove Excessive Rights and Dormant Users

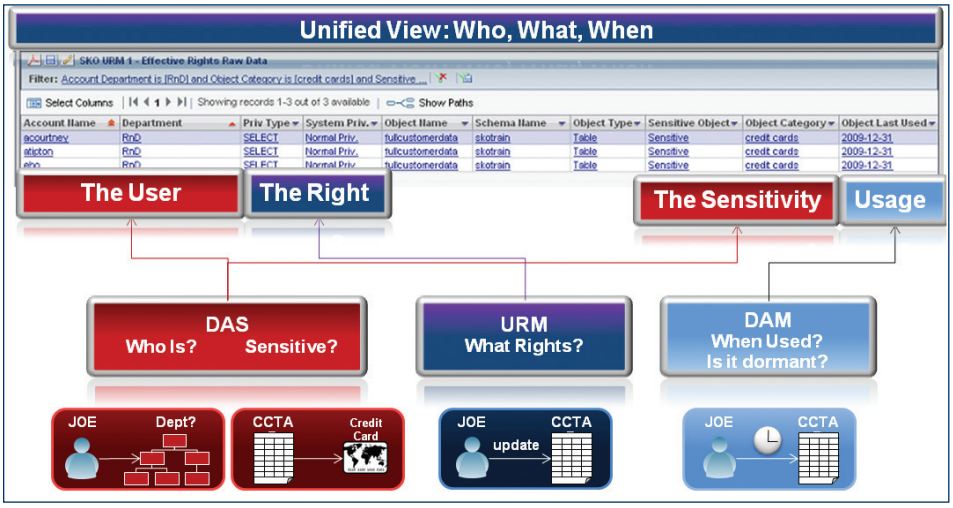
When SecureSphere Database Activity Monitoring (DAM) is deployed in conjunction with URMD, it is possible to track the actual usage of database objects by different users. A combined report showing the user, their organizational role, the type of data the user is allowed to access, and the actual usage of that data, helps identify dormant users and un-used access rights. Such rights can now be safely removed from the database and reduce the risk of exploitation.

Comprehensive User Rights Reports and Analytical Views

Pre-defined reports and analysis views consolidate details about user rights across all enterprise databases. User rights details can be presented per user or group, per database, or per database object. Using these views, it is easy to compare user rights, identify excessive rights, validate changes to rights, and pin-point dormant accounts.

Built-In Workflow for Reviewing and Approving User Rights

With Imperva URMD organizations can easily demonstrate an automatic, repeatable process for reviewing access rights as required by regulations like PCI-DSS and SOX. Imperva URMD includes a work-flow framework to support user rights review and authorization processes. URMD provides a full audit trail of the rights granted/revoked including the grantee and granted details. Administrators can accept or reject privileges and add comments to explain the decision. When further action is required, a task can be assigned and its status is tracked within SecureSphere.



Imperva User Rights Management: Review and document user access rights to sensitive data,validate access is based on a 'need-to-know' and actual usage.

About Imperva

Thousands of the world's leading businesses, government organizations, and service providers rely on Imperva solutions to prevent data breaches, meet compliance mandates, and manage data risk. Underscoring Imperva's commitment to data security excellence, the Imperva Application Defense Center (ADC) is a world-class security research organization that maintains SecureSphere's cutting edge protection against evolving threats.

www.imperva.com