

Solution Brief

Security Solutions for Non-Production environments

Data Leakage Prevention

Challenge:

Non-production databases contain personal data that was extracted from production databases, where regulations and compliance requires organizations to ensure that this personal data is not exploited by current and former consultants and employees, QA and trainers on any of these instances. Personal Information leakage is a major threat to organizations with high cost of remediation.

Masking personal data in the database ('masking at rest') by executing masking functions on personal data columns has limitations such as:

1. Creating the masking scripts takes a long time and requires professionals to analyze where and how to apply the masking since application's data model is very complex and in some cases not available
2. It takes a long time to apply the masking functions on large personal data volumes
3. Masking data requires modifying all testing scripts that have been created with data entry values before data masking occurred

ActiveBase Security Solution

ActiveBase Security provides a unique approach "**Data-in-motion masking**"

ActiveBase Security is built on a unique SQL*Net Proxy. It transparently intercepts SQL requests coming from application screens, interfaces or canned reports and applies Security Rules.

Rules apply masking, scrambling, blocking or hiding sensitive information on-the-fly, preventing access in non-production from unauthorized personnel without having to physically mask the data.

*For example, instead of masking SSN (Social Security Number) in many tables in the database, a single rule masks all 'Select' requests retrieving SSN information, by rewriting the SSN column in the 'select list' of these requests with '*****' (e.g., **select ... SSN..from...** is rewritten with **select ...'*****'..from...**)*

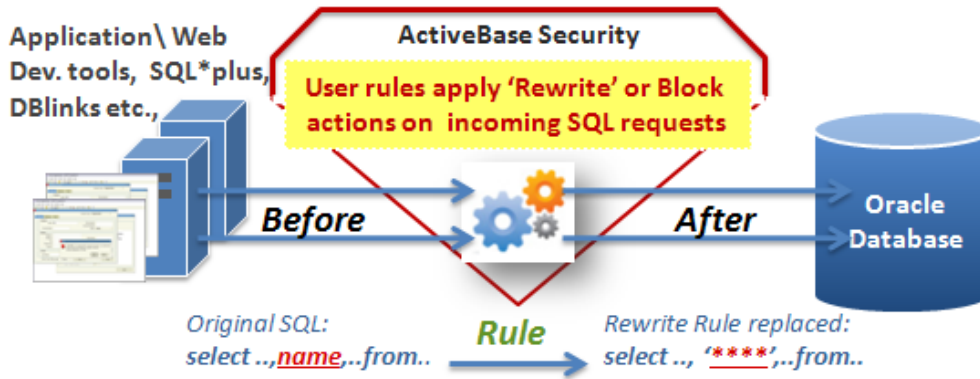
Benefits

- ✓ Prevent leakage of Sensitive and Personal Information from non-production environments
- ✓ Mask "on-motion" in about 1/10 the costs of "data-in-rest" masking
- ✓ The integrity of database relationships is always preserved

Save costs required to:

- Explore data model and object dependencies
- Adapt all test scripts with the new masking
- ✓ Reuse ActiveBase Security rules to mask access to personal information in testing and QA environments as well as in Production





Masking Rules:	Scrambling Rules:	Hiding Rules:															
<p>Original SQL: <code>Select name,..from..</code></p> <p>After Rule: <code>Select substr(name,1,2) '****'</code></p> <p>Result:</p> <table border="1"> <thead> <tr><th>Name</th></tr> </thead> <tbody> <tr><td>Tiger</td></tr> <tr><td>Nelson</td></tr> <tr><td>Rogers</td></tr> <tr><td>Rosen</td></tr> </tbody> </table>	Name	Tiger	Nelson	Rogers	Rosen	<p>Original SQL: <code>select name,..from..</code></p> <p>After Rule: <code>Select scrmbl(name)..</code></p> <p>Result:</p> <table border="1"> <thead> <tr><th>Name</th></tr> </thead> <tbody> <tr><td>Tiger</td></tr> <tr><td>Nelson</td></tr> <tr><td>Rogers</td></tr> <tr><td>Rosen</td></tr> </tbody> </table>	Name	Tiger	Nelson	Rogers	Rosen	<p>Original SQL: <code>select ..,name,..from..</code></p> <p>After Rule: <code>select ..,'..'from..</code></p> <p>Result:</p> <table border="1"> <thead> <tr><th>Name</th></tr> </thead> <tbody> <tr><td>Tiger</td></tr> <tr><td>Nelson</td></tr> <tr><td>Rogers</td></tr> <tr><td>Rosen</td></tr> </tbody> </table>	Name	Tiger	Nelson	Rogers	Rosen
Name																	
Tiger																	
Nelson																	
Rogers																	
Rosen																	
Name																	
Tiger																	
Nelson																	
Rogers																	
Rosen																	
Name																	
Tiger																	
Nelson																	
Rogers																	
Rosen																	

Highlights

- ✓ A single rule can mask, scramble, hide or block all SQL requests that retrieve personal information across applications
- ✓ Adding or changing security rules are applied immediately
- ✓ **NO NEED FOR CHANGES TO THE APPLICATIONS OR THE DATABASE**
- ✓ Supporting all applications running on Oracle8.0 – 11 on all common operating systems

All security rules can be applied selectively, based on condition values relating to specific applications, modules, screens, transactions and users (for example, applying different rules on DBAs and QA).

Customer Experience

A large Telecom company wanted to mask personal information data in their lab, testing and preproduction environments. Applications include CRM (Vantive and Siebel), Billing, Oracle Applications ERP suite and more. Because of the amount of personal data and the complexities of the data model, masking the data within budget constraints and time limitations was not feasible.

ActiveBase Security was quickly installed, and masking rules defined to mask personal information retrieved by these applications (on-motion), without having to mask the actual data.

In less than two week access all masking and scrambling objectives were met.