

Solution Brief

Security Solutions for Production environments

Dynamic Data Masking and Data Leakage Prevention

The Challenge:

The increasing compliance and regulations requirements for protecting sensitive and personal information on production CRM, ERP, Billing and Proprietary applications has become a corporate imperative.

In most cases, the time and cost of enhancing the security within packaged and proprietary applications is too high or even impossible, and other means should be used.

Moreover, existing security built in applications do not cover development, QA and DBA tools, neither do they protect from external workforce, outsourced DBAs and support teams accessing production data.

Securing databases using Database Vaults has limitations such as:

1. Blocking access privileges to database tables and modules that contain personal information might cause productivity loss, since DBAs and developers cannot access application data they need in order to fix a production problem!
2. Maintaining database security during database changes, upgrades and updates is very costly and complex.

ActiveBase Security Solution

ActiveBase Security provides a unique approach - **“Dynamic Data Masking”** - the only enterprise-class product on the market where IT and Compliance can determine who sees “masked”, “unmasked”, “encrypted” or “decrypted” production data and when access is blocked.

Allowing “masked” access to all tables ensures that personal information is de-identified, that external support teams, outsourced DBAs and IT productivity is not affected, and production availability is ensured.

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, encrypting, blocking or hiding sensitive information on-the-fly, preventing access in production from unauthorized personnel -- without having to physically revoke access rights to the data.

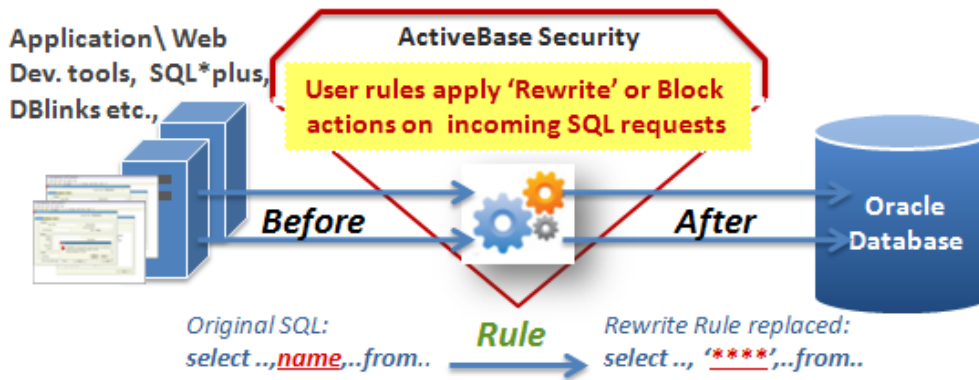
Benefits

- ✓ Dynamically masks, scrambles, encrypts or hides “on-motion” access to sensitive and personal information in 1/10 the costs and time of applying other solutions.
- ✓ Prevents leakage of Sensitive and Personal Information from production environments.
- ✓ Enforces application security policies across applications and tools accessing production database.
- ✓ Reuses ActiveBase Security production rules to mask and protect unauthorized access in testing and QA environments.
- ✓ Administered by security operators that are not required to be DBAs.



Rules can have a broad scope, so a single rule will apply to all similar SQL requests that retrieve personal information.

☞ For example, a rule that masks Social Security Number will automatically mask results retrieved by all 'Select' requests generated from external development tools BUT NOT from legitimate application requests.



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

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 protect access to personal information data in their production environments, including billing, ERP, Datawarehouse and CRM applications

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

www.active-base.com

400-00101-101 | 02/09 | © 2009 ActiveBase, Ltd. All rights reserved. All other third-party trademarks are the property of their respective owners.

Highlights

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

