

Use Cases

ActiveBase Security™ Role Based Access Control and Dynamic Data Masking

Control access and dynamically mask personal information from end-users who do not require accessing it in order to perform their jobs while ensuring compliance with ever changing regulations.

The PCI, GLBA, SOX, BASEL II, EU Personal Data Protection Directive and other privacy regulations were created in response to the growing problem of sensitive and personal information theft.

Today's regulations require organizations to verify that the level of access granted to application users is based on the user's business function, including full and part-time workers, outsourced workforce, IT personnel, developers, database administrators and outsourced support teams.

In most cases, the time and cost of restricting access to personal information within packaged and home-grown applications, development and DBA tools is prohibitive and other, more cost effective means should be used.

ActiveBase Security™ Solution overview

ActiveBase, winner of the Gartner prestigious Application Security Cool Vendor award, was named a pioneer in the Dynamic Data Masking market.

Dynamic Data Masking provides CISOs with an effective way to ensure sensitive and personal information is not exposed to IT personnel or to full and part-time employees, customers, partners and outsourced workforce.

Two types of security risks are mitigated using ActiveBase **in both production and non-production environments:**

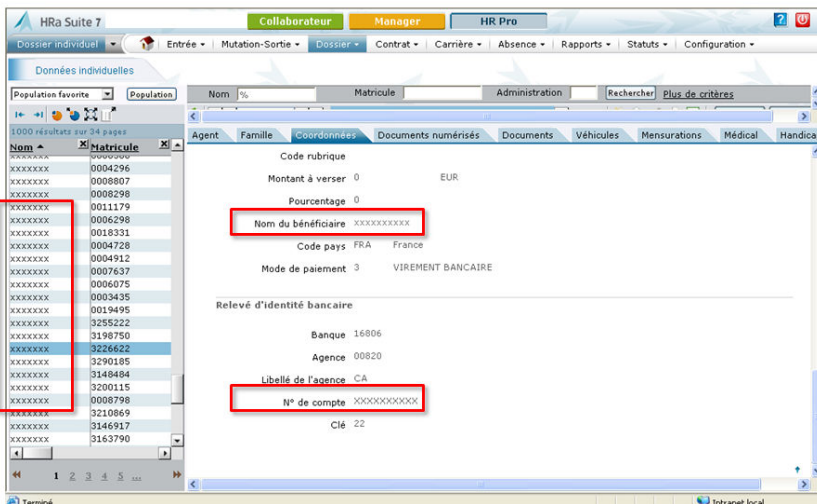
1. Protecting personal information from business users, including full and part-time employees, partners and offshore workforce.
2. Protecting personal information from IT personnel, developers, database administrators and outsourced support teams.

ActiveBase offers the only enterprise-class product on the market where IT and Compliance can determine who sees "masked", "unmasked", "scrambled" or "unscrambled" production data and when access is audited or completely blocked, with no changes to application source-code or databases.



Benefits

1. Dynamically masks, scrambles or hides access to sensitive and personal information.
2. ActiveBase quick installation and unique Implementation methodology enables to secure complex business applications WITHIN DAYS.
3. Prevents Sensitive and Personal Information leakage to part-time and offshore workforce or business partners as well as to production support, outsourced teams, developers and DBAs.
4. Enforces application security policies across applications and tools.
5. Reuses ActiveBase Security production rules to secure training, testing and development environments.
6. Administered by security operators that are not required to be DBAs.
7. Centralized management.
8. No need for changes to applications or databases.



Protecting Production Environments from privileged IT personnel

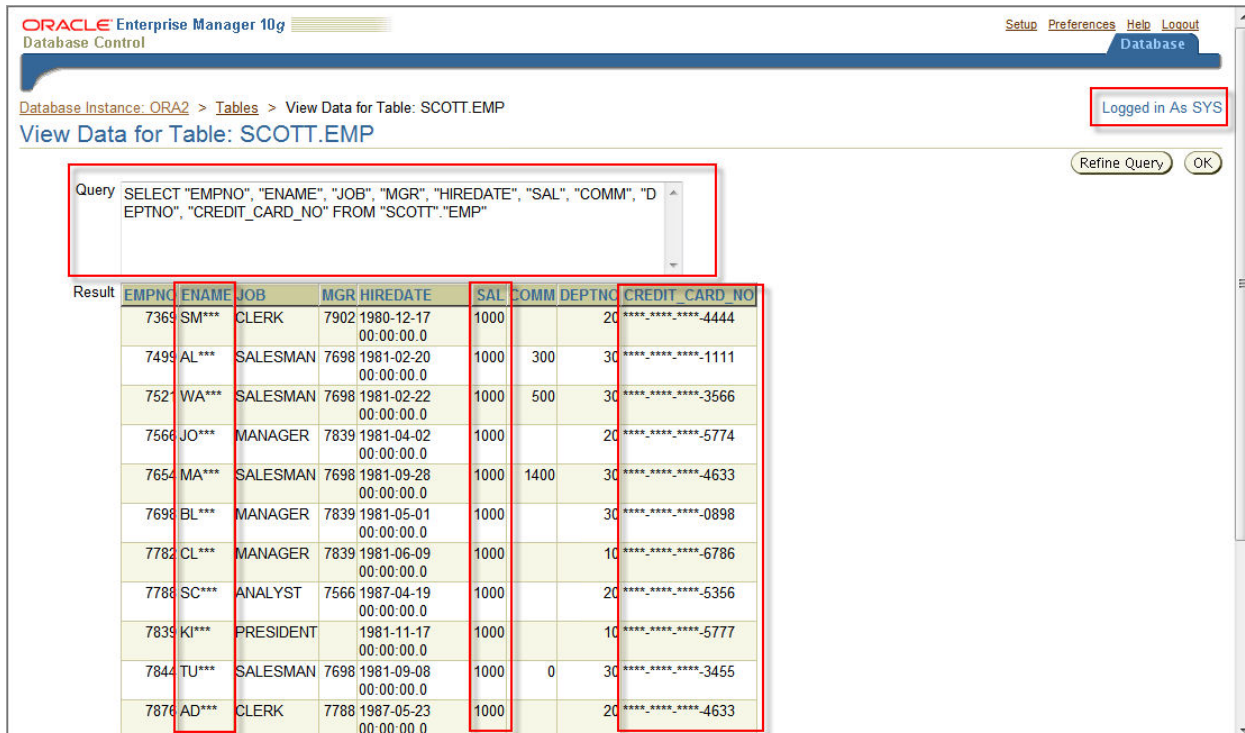
Developers, DBAs, application designers and consultants access production applications and databases daily in order to ensure their performance and availability.

Required to resolve critical production problems quickly, production support teams have unlimited access to credit card numbers, personal data, and sensitive business and financial information.

PCI-DSS, California Senate Bill No. 1386, EU Personal Derivative, GLBA, and HIPAA, among others, require that production support teams DO NOT have access to sensitive data.

Existing solutions merely audit access or offer access limitations that prevent critical production problem identification and resolution.

>> ONLY Dynamic Data Masking provides a full audit trail on all privileged user access (required for SOX, GLBA and other regulations), ensuring that production support teams' access to personal and sensitive data is completely masked or scrambled. It allows production support teams full access for immediate production problem resolution, while preventing data leakage and ensuring compliance with all privacy regulations.



ActiveBase Security™ transparently secures names, salaries and credit card information accessed by production support personnel in application screens, packaged reports and development tools

Securing personal information from outsourced, offshore and on-site consultants

With a market size reaching \$40 Billion, CISOs in large outsourcing organizations are faced with the challenge of ensuring that their most valuable asset – information - is not exposed to outsourced and offshore workforce.

For example, in one of the world's largest telecom companies, thousands of outsourced personnel access production databases daily using application screens, packaged reports, development and DBA tools. Furthermore, it has been required by law and privacy regulations, such as EU personal derivative, that names and contact information of US and European residents found in their production databases are not exposed to offshore workforce.

>> ONLY Dynamic Data Masking ensures that offshore and outsourced teams' access to personal and sensitive data is simply masked or scrambled with no changes to applications or databases.

Protecting personal information within business applications and reporting environments

Regulations are growing on a yearly basis, imposing fines and criminal penalties for every breach. These regulations require stricter security means, audit and granular access control on proprietary business applications and packaged reporting tools – all of which were programmed years ago and lack these capabilities.

For example, a very large Insurance Company is using a core insurance application that was programmed 10 years ago, with extremely basic User Right Management.

Recoding application source-code to enable modern security rolls within proprietary applications is very expensive and a risky endeavor, as the source-code is not available or is too complex.

>> ONLY Dynamic Data Masking adds a protective layer on top of proprietary business applications and packaged reports, masking unauthorized access to personal information, restricting by rows and columns as well as restricting number of rows returned – without changing a single line of code or the database.

The screenshot shows a web browser window displaying the GANJIS insurance application. The page title is "契約一覧照会(火災)" (Contract List Inquiry (Fire)). The search criteria section includes fields for certificate number (07100030), branch, contract status, and other details. The search results table shows one entry with a masked name.

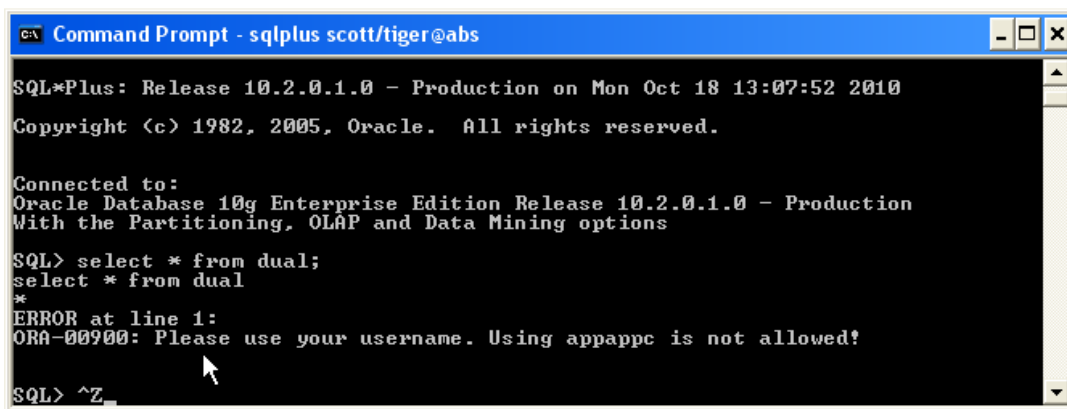
項番	証券番号	扶番	契約状況	保険種類	契約者名	課所	代理店	満期日	承認種類	処理
1	07100030			住宅総合	齋藤	0710	01256	平成32年04月28日		照会

Masking Japanese Insurance applications

Protecting global account usage and access right provisioning

With one of our customers, developers and DBAs access production databases and business applications using generic login accounts (e.g., APPS, Billing) in order to monitor production databases. After failing their security audit the customer has turned to ActiveBase for a solution that will prevent general account usage while ensuring that batches and scripts that use the same generic accounts are not failing.

>> By using ActiveBase unique Informed Block™, all users accessing the databases using global accounts are blocked, and a clear message is returned to them asking to re-enter with their own dedicated user name. Jobs and batches automatically bypass these audit and security enforcement rules. ActiveBase provides detailed SQL audit information to comply with SOX.

A screenshot of a Windows Command Prompt window titled "Command Prompt - sqlplus scott/tiger@abs". The window shows the output of a SQL*Plus session. It starts with the release information: "SQL*Plus: Release 10.2.0.1.0 - Production on Mon Oct 18 13:07:52 2010". Below that is the copyright notice: "Copyright (c) 1982, 2005, Oracle. All rights reserved." The user is connected to an Oracle Database 10g Enterprise Edition. The user enters the command "select * from dual;". The output shows the first row of the dual table. Then, the user enters another "select * from dual" command, which results in an error: "ERROR at line 1: ORA-00900: Please use your username. Using appappc is not allowed!". The prompt is now "SQL> ^Z_".

```
Command Prompt - sqlplus scott/tiger@abs
SQL*Plus: Release 10.2.0.1.0 - Production on Mon Oct 18 13:07:52 2010
Copyright (c) 1982, 2005, Oracle. All rights reserved.

Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> select * from dual;
select * from dual
*
ERROR at line 1:
ORA-00900: Please use your username. Using appappc is not allowed!

SQL> ^Z_
```

Informed Block™ returns a clear message and guidance to the user

Access Control

With one of our customers - a telecom world leader, a developer with access to a billing production database deleted a table by mistake. The result was a \$2M direct loss of revenue as well as frustrated customers that have lost confidence in the company services.

The customer has tried to implement a "kill" on unauthorized user sessions – causing IT productivity loss and dissatisfaction (killing sessions causes the application to abort with all recent changes lost, and the user does not even know why – can the session kill be caused by his program? Server?, Database?), as well as a maintainability problem caused by the lack of central management.

>> ONLY ActiveBase Informed Block™ controls all production database changes. Whenever a change is performed in production, a predefined message is presented to the user within the application screen/tool/report (Multilanguage is supported).

Another ActiveBase product (ActiveBase Priority™) enables to set resource profiles that automatically constrain the amount of server resources that is consumed by production support and online activities, as well as batches during high-peaks. It also includes a dashboard for immediate intervention and resource management.

www.active-base.com