

Success Story

Leading global GSM operator secures production, training and non-production environments with ActiveBase Security™



Background

A leading global GSM operator was required to protect personal identifiable information across various production, clones, training and non-production environments, including Billing systems, CRM (both Siebel and Clarify), legacy and custom applications.

These applications are accessed daily by thousand of business users, newly recruited employees, IT personnel, production support teams, developers and DBAs.

Various security approaches were tested before contacting ActiveBase, but none could provide the level of privacy protection required:

In production environments encryption could not be used due to the performance impact and implementation complexities experienced, as it required changes to applications that were not possible in many closed packaged applications the customer was using.

In non-production environments, physical masking was used to some extent, yet it was not applicable in protecting training environments due to the complexity and the need to train end-users with real-life scenarios changing frequently in accordance with the dynamic nature of the business.

In addition, in development environments certain data items were simply too complex to mask physically (due to referential integrity; data flowing between billing, CRM and ERP applications and external data batch validations against external production systems that could not be masked).

“Within several weeks, ActiveBase transparently masked personal information on our Billing, CRM and custom application screens and packaged reports in production and non-production environments from both end-users and IT personnel, becoming a vital component in our privacy compliance endeavor”
CISO, Global GSM operator

ActiveBase Security™ Dynamic Data Masking

The security team has installed ActiveBase Security™, and within a couple of weeks implemented Dynamic Data Masking across production, training and non-production environments.

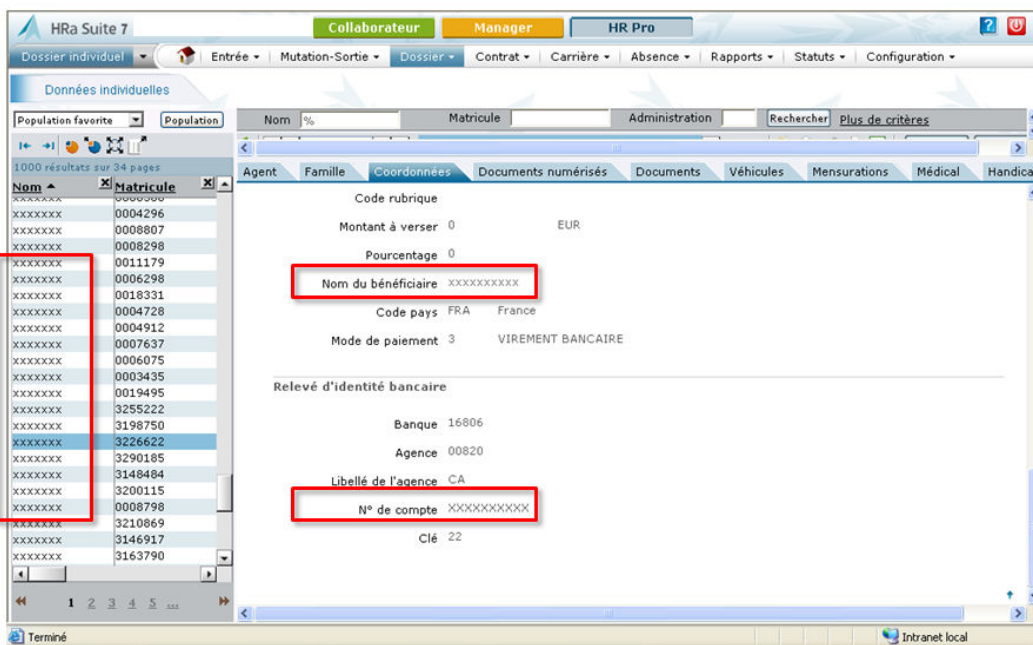
Neither application nor database changes were required to protect the privacy of customer names, SSN, account information, outgoing call numbers, credit card information and other private data items.

First, ActiveBase Security™ was quickly and transparently installed on one of the Sun Enterprise servers. A fully replicated production environment was configured to point to the ActiveBase Security server. The security team worked with one of the application trainers, with the following implementation methodology, called ‘Screen based implementation’:

1. The trainer opened several screens presenting personal information that was required to be anonymized.

2. The SQL requests submitted by the screens in order to retrieve information from the databases were audited and saved.
3. Based on the full SQL requests, the columns and tables containing personal information were identified – and a masking rule was created and added to the ActiveBase Security™ server.
4. The trainer accessed the screens again – this time to ensure that the masking was working properly and personal information is indeed anonymized.

Using this methodology, and with no changes to the actual data stored on the database, the applications were quickly protected, and rules were propagated between different environments, and applied on different use cases. As no changes to either the applications or the databases were required, the process has been successfully completed for the entire maze of applications, interfaces and batches within only several weeks by the internal security team.



ActiveBase Security™ transparently secures personal information in application screens, packaged reports and Development tools

The Results

ActiveBase quick implementation across applications and environments resulted in:

1. ActiveBase simple visual implementation methodology enabled the security team to secure a plethora of personal identifiable information quickly in several of the most complex and demanding business applications, including billing and CRM applications.
2. Rule propagation provided quick protection across production, training and non-production environments.
3. Personal information was now secured from business users, newly recruited and existing employees, part-time workforce, outsource and IT staff – allowing them to access it only on a need-to-know basis.
4. Quick compliance with various privacy regulations was achieved with no costly changes to application.

www.active-base.com

400-00101-191 | 3/5 | © 2011 ActiveBase, Ltd. All rights reserved. All other third-party trademarks are the property of their respective owners.

