

Data Access Monitoring (DAM) Solutions and ActiveBase Security™ Comparison

General

- ActiveBase Security™ complements DAM solutions, creating immediate upsale opportunities for DAM resellers within existing DAM customers. Several new ActiveBase customers have bought ActiveBase Security™ after buying a DAM solution.

- ActiveBase Security™ is the only solution in the market today (according to Gartner) providing Dynamic Data Masking.

DAM solutions audit and block access to PII, yet a growing threat comes from within application screens and reports, giving employees, external work force, IT and outsourced support teams unnecessary access to PII.

Dynamic Data Masking provides is the first solution to directly address these threats by limiting and controlling who sees what across applications and environments.

- A few examples of common security threats resolved only by ActiveBase:

> Why should thousands of call center workers have access to credit-card and bank account details on Siebel screens?

IT answer before introducing ActiveBase “...because we cannot mask the screens of this application”

> Why should trainees access PII while learning how to use CRM applications?

IT answer before introducing ActiveBase: “...because it is too complex to physically mask the training environments”

> Why should HR reports enable clerks to access PII not needed for doing their job?

IT answer before introducing ActiveBase “...because we cannot touch the reports in this application”

> Why should an outsourced admin see personal information on his development tools?

IT answer before introducing ActiveBase: “...he must have full application access in order to support production”

> Why should external developers view HR information?

IT answer before introducing ActiveBase: “...because they need to access production HR data in order to fix critical production problem...”

Unlike DAM solutions, ActiveBase can MASK, SCRAMBLE, HIDE OR BLOCK PII – creating a security layer within these applications – in a fully transparent way, with no changes required to either applications or databases (see Image 1 for a real-life example)

ActiveBase enables to return warning messages back to the end users within the application screens and reports. DAM solutions can only kill the user without any warnings or notifications, leaving the user confused while hurting productivity.

ActiveBase is also suited for customers who wish to mask PII within development and DBA tools such as Toad, PL/SQL developer, SQL*plus, excel etc.

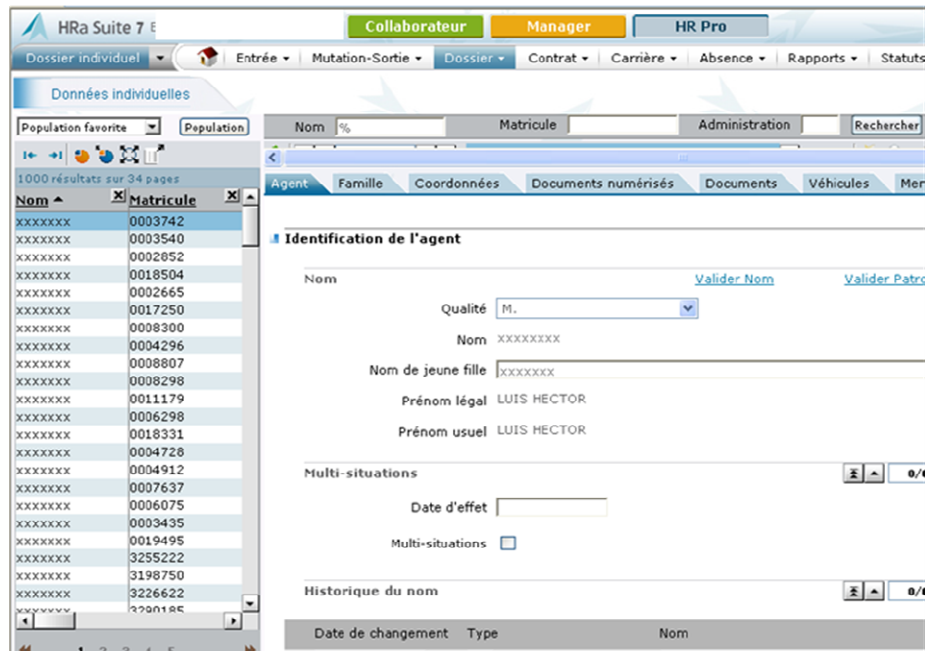


Image 1: Only ActiveBase can mask PII within screens when accessed by an IT support personnel.

DAM solutions are only used in production environments, whereas ActiveBase Security™ is often used both in **production and non-production environments**, dynamically masking developer access to testing and QA environments, complementing physical masking solutions.

Summary

Feature	DAM	ActiveBase Security
Block access to objects		
1. Context Sensitive Block (e.g. within a time frame)	Yes	Yes
2. Notify user with customized message when blocked	No – killing sessions	Yes
3. Flexible and gradual implementation	No – all database traffic is 'sniffed'	Yes – can be implement gradually based on specific application and/or host name
Alert and report on access to PII	Yes	Yes
Protect Sensitive and Personal Identification Information (PII)		
1. Restricting row level access	No	Yes, adding 'where' clause conditions
2. Restricting column level access	No	Yes – Dynamic Data Masking
3. Hiding results of sensitive columns	No	Yes
4. Masking results of sensitive columns (for verifying data quality and quick bug fixing)	No	Yes