

ActiveBase Security™ Competitive Landscape

Comparison document



Comparing ActiveBase Security with Physical Masking

Players include Oracle Masking, Informatica and IBM Optim

Functionality

- Masks the actual data stored in the database by changing the real data into fictitious values
- Only applicable in Development environments, as physical masking changes the database columns irreversibly, making it impossible to use in Production, replications and training and User Acceptance Testing (UAT) environments
- Requires in-depth application knowledge into the data model
- Changing data columns might cause the application to break and stop working
- Requires long implementation (months compared with days for ActiveBase Dynamic Masking)

ActiveBase Security in non-production environments:

1. Provides physical masking by masking ETL EXPORT processes that extract data from production databases, ensuring that only secured personal information leaves production. This is achieved by routing the EXPORT processes through ActiveBase Listener port.
2. Complements physical masking by dynamically masking data that is too complex or is impossible to mask physically (e.g., when trying to mask referential data such as account numbers and SSN that flows across various business applications or credit card numbers that require validation with external applications that physically changing the data will prevent).

Comparing ActiveBase Security with Database Encryption Solutions

Functionality and limitations

Organizations worldwide are trying to minimize the number of columns they have to encrypt because each encrypted table column requires changing all reference application source-code while adding severe performance penalties to any transaction accessing the encrypted column (due to the encrypt/decrypt function duration and resources)

- Encryption protects against infrastructure DBAs that have access to database files and backup tapes
- It does not prevent end-users from accessing personal information, as applications decrypt the values presented within screens and packaged reports
- Complex to implement, requires application source-code or database changes
- Performance overhead caused by the encryption/decryption algorithm

ActiveBase Benefits

- ActiveBase protects against application end-users as well as from privileged users
- Implemented within days with no need for prior in-depth application knowledge into the data model
- Application and database transparent
- No database performance overhead
- Can be implemented in databases along encryption solutions to secure sensitive information that is not encrypted such as names, SSN, addresses and account details
- No need to encrypt the personal data for protecting its privacy, avoiding application changes, database complexities and performance penalties

Comparing ActiveBase Security with Database Access Monitoring (DAM) Solutions

Players include Imperva, Guardium and Application Security

Functionality and limitations

- Monitors and audits past occurrences of users accessing personal and sensitive information
- Protects databases from SQL Injection
- Unauthorized SQL can be killed without any notification to the user, causing time and productivity loss

ActiveBase Benefits

- ActiveBase Security restricts end-users, IT support, outsourced developers and DBA teams from accessing personal information when it is not required to enable them to perform their job
- It actively secures packaged application screens, packaged reports, development and DBA tools by masking, scrambling or hiding sensitive information, delivering real-time row and column level security and restricting number of rows retrieved, proactively preventing data leakage
- It can also block requests that retrieve personal information without killing user sessions while notifying the user accordingly (ActiveBase Informed Block™), eliminating any risk of time or productivity loss
- ActiveBase Dynamic Data Masking enables to manage security necessities and operational requirements. By masking and scrambling sensitive and personal information access while allowing the performance of all required remedies, the information is kept out of the preying eyes of IT operations and outsourced support teams, while allowing them required access to solve production problems

Comparing ActiveBase Security with Oracle VPD (Virtual Private Database) and RLS (Row Level Security)

Functionality and limitations

- Cannot mask personal information within application screens and packaged reports (it can only return null values, causing errors in application screens and packaged reports)
- Policies applied only on the object level, lacking policy enforcement on individual SQL requests (e.g., restricting row level access, yet allowing for aggregations and summary reports) and multi-tier application user context
- Complex to implement and requires experienced DBAs, in defiance with the requirement for separation of duties
- Performance overhead

ActiveBase Benefits

- ActiveBase uniquely provides the ability to mask, scramble and block (not only hide) sensitive fields within application screens, packaged reports and development/DBA tools
- Policies can be applied selectively based on context, including SQL, session, object context, application user, ActiveDirectory and grants maintained in ILM/IDM systems
- ActiveBase ensures separation of duties, as it can be configured exclusively by security officers
- Implemented within days with no need for prior in-depth application knowledge into the data model
- Application and database transparent
- No database performance overhead

Comparing ActiveBase Security with Oracle Database Vault

Functionality and limitations

- Restricts access to privileged users by using powerful access controls built into the Oracle database
- Does not secure privileged user's direct access to database files in the OS level
- Does not block unauthorized access to the database server (not a database firewall)
- Database Vault access restriction to sensitive data can substantially delay or hurt problem resolution, as root cause analysis can be blocked

ActiveBase Benefits

- ActiveBase complements Database Vault implementations by adding Dynamic Data Masking that enables DBAs and developers to access applications and screens containing personal information in order to perform their job and fix production problems for operational purposes, while being exposed to only masked, scrambled or hidden personal and sensitive information in a secured and controlled way
- It also provides a database firewall that can block requests (Informed Block™) while notifying the end-user (database firewall is a compliance requirement for certain regulations)

Detailed comparison between Oracle Row Level Security and ActiveBase

Feature	Oracle Database Vault	Oracle Virtual Private Database (VPD)	ActiveBase Security
1. Database Access control			
a. Block access to objects	Yes	Yes	Yes
b. Context Sensitive Block (e.g. between hours)	Yes	Yes	Yes
c. Notify user with customized message when blocking	No	No	Yes
d. Flexible and gradual implementation	No	Limited	Yes
2. Protecting Sensitive and Personal Identification Information (PII)			
a. Restricting row level access	No	Yes, adding 'where' clause conditions	Yes, adding 'where' clause conditions
b. Restricting column level access	No	Limited	Yes – Dynamic Data Masking
c. Hiding results of sensitive columns	No	Limited	Yes

d. Masking results of sensitive columns (for verifying data quality and quick bug fixing)	No	No	Yes
3. Privileged user access control			
a. Control access to sensitive information	Yes	No	Yes
b. Control connections bypassing listener	Yes	Yes	Limited
c. Control SYS privileges	Yes	Limited	Limited
4. Separation of duties	Yes	No	Yes
5. Auditing	Complex to write audit script that defines the exact access for each specified user.	No	Easy, centralized
6. Maintainability	Medium	Difficult	Easy
7. Version support	Oracle10g and higher for most features and performance reducing functions (cache)	Oracle 9i and higher, limited functionality	Oracle8.0 and higher, all functions operate on all versions
8. Performance penalty on production systems	Medium to Heavy	Heavy	None
9. Implementation time	Weeks	Months	Days
10. Cost	Very high > \$20K Per CPU core	Based on modules	Low and flexible pricing per CPU core or per user

Why is our blocking better and safer than blocking provided by other solutions?

Only ActiveBase software enables to block specific SQL requests in any application (2, 3 or n-tier applications) without killing sessions or touching application code, while returning a customized notification to the user (multi-language supported) – ActiveBase Informed Block™.

Application connections are not torn and sessions are not killed - only the specific request is blocked, protecting productivity. Other requests from different users using the same connection (using connection pool) continue with no application abstraction whatsoever, eliminating any risk of time or productivity loss.

Can ActiveBase Security be deployed in training environments?

Short answer: Yes. Training environments are especially compatible for ActiveBase Security which can be very easily deployed there, whereas it is impossible to use physical masking to mask all columns. And when later on you consider securing production with ActiveBase, the same rules are simply propagated into production applications!