The Risk of Highly-Privileged Database Users & DBAs

Integrate your Ticketing System with Guardium to Prevent Abuse

High-level privileges are often required for database administrators (DBA) to conduct maintenance tasks on databases or to fix problems. With these ultimate privileges, DBAs can do whatever they want!

Malicious DBAs (insiders) are a rare phenomenon but there are a lot of careless DBAs who might expose their DBA credentials. Alternatively, DBA credentials may be compromised by an email phishing campaign (outsiders) despite all the cyber security training companies provide.

Strict permission model is virtually impossible to achieve in practice for several reasons: privileges are hierarchical, they contain other privileges and the administrator's permission needs keep changing based on their current task(s). Therefore, the **"trust, but verify"** model is best: review all activities and let DBAs know that their actions are audited. This is where IBM Guardium shines. Guardium simplifies the audit and review of DBA activities.

Hundreds of ad-hoc changes occur on your databases every week. How can you keep track of these changes and know which ones are authorized and which are not authorized? Most companies today have a ticketing system and most DBAs will not touch a production database without a ticket assigned to them. **But what about an instance where the DBA may abuse their privileges and make changes to a database without a ticket!!**

The Missing Link – Report segregates authorized changes from unauthorized changes.

This customized solution captures critical information in ticketing systems (ServiceNow, Remedy or HPSM) such as Database User, Database Systems, time window of the change etc. and importing this ticketing information into Guardium custom domain helps clients to segregate authorized changes from unauthorized changes. Saving the time from follow-ups and seeking documentation from database admin and fulfilling auditor requirements.

This solution can also be extended to policy alerting or correlation alerting and avoid situations where a user has a proper ticket to access or make changes to sensitive information, but an alert gets generated despite that.

KEY FEATURES OF TICKET RECONSILIATION INTEGRATION WITH DB AUDIT & SECURITY

- Both authorized and unauthorized activities are reported -- all activities within the change window are consolidated and reported as authorized changes and activities reported outside of change window will be considered unauthorized.
- This integration compels organization to following best practices.
- Alerts can be issued when a highly privileged user connects and executes privileged actions or queries on sensitive tables without a valid ticket.
- Validation of the actual activity by reporting all audited events that belong to each ticket ID

WHAT WE CAN DO

By combining our domain knowledge in data protection, our hands-on engineering experience with IBM Guardium and our breadth of data management experience we can help transform and adapt our clients to the cyber security era of technological change.

Business Partner IBM

adaptivesystems
Princeton, NJ USA
888-234-4735
www.adaptivesystemsinc.com