- Threats to sensitive data during maintenance window from the application administrators
- Threats that exploit weaknesses in the application to escalate privileges and attack other applications on the same database
- Oracle Database Vault with Oracle Database 19c is installed by default, enabling efficient setup, configuration and deployment.

CONTROLS FOR PRIVILEGED ACCOUNTS

Privileged user accounts are commonplace in all databases and are used by DBAs for daily tasks such as user management, performance tuning, replication, patching, backup and recovery, space management, startup, and shutdown. Many Oracle predefined system users such as SYSTEM and roles such as DBA role can access any application data in the database. Due to their wide ranging access, most organizations enforce strict processes and internal rules on who can be granted privileged access or DBA access to the databases. These accounts and roles, however, have also been a prime target of hackers because of their unimpeded access inside the database. They have frequently been misused by insiders to gain access to confidential information.

Privilege User Access Controls on Application Data with Realms

Increasing controls on privileged and DBA accounts is vital to improving security. Oracle Database Vault creates a highly restricted application environment ("Realm") inside the Oracle Database that prevents access to application data from privileged accounts while continuing to allow the regular authorized administrative activities on the database. Realms can be placed around all or specific application tables and schemas to protect them from unauthorized access while continuing to allow access to owners of those tables and schemas, including those who have been granted direct access to those objects.

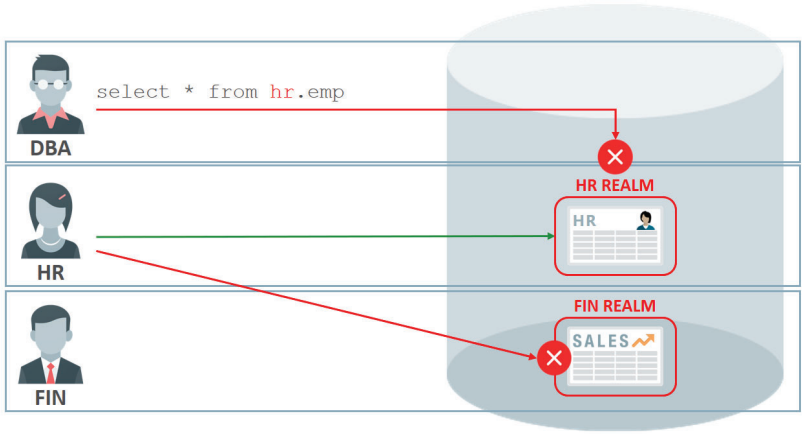

Figure 1. Oracle Database Vault for privileged accounts