- 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

57

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.

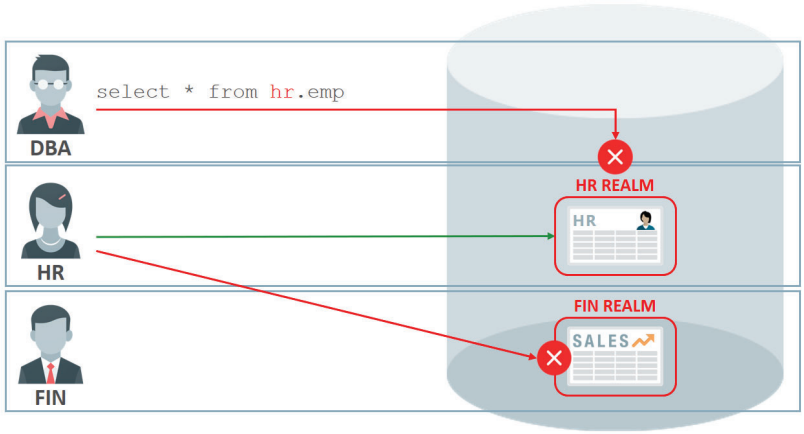


Figure 1. Oracle Database Vault for privileged accounts

**Table 1-1 Regulations That Address Potential Security Threats**

| Regulation | Potential Security Threat |
|---|---|
| Sarbanes-Oxley Section 302 | Unauthorized changes to data |
| Sarbanes-Oxley Section 404 | Modification to data, unauthorized access |
| Sarbanes-Oxley Section 409 | Denial of service, unauthorized access |
| Gramm-Leach-Bliley | Unauthorized access, modification, or disclosure |
| Health Insurance Portability and Accountability Act (HIPAA) 164.306 | Unauthorized access to data |
| HIPAA 164.312 | Unauthorized access to data |
| Basel II – Internal Risk Management | Unauthorized access to data |
| CFR Part 11 | Unauthorized access to data |
| Japan Privacy Law | Unauthorized access to data |
| EU Directive on Privacy and Electronic Communications | Unauthorized access to data |
| Payment Card Industry Data Security Standard (PCI DSS) | Unauthorized changes to data |

## 1.5 How Oracle Database Vault Protects Privileged User Accounts

Many security breaches, both external and internal, target privileged database user accounts to steal data from databases.

57

Oracle Database Vault helps to protect against compromised privilege user account attacks by using realms, factors, and command rules. Combined, these provide powerful security tools to help secure access to databases, applications, and sensitive information. You can combine rules and factors to control the conditions under which commands in the database are allowed to execute, and to control access to data protected by a realm. For example, you can create rules and factors to control access to data based on IP addresses, the time of day, and specific program, such as JDBC, SQL Developer, or SQL*Plus. These can limit access to only those connections that pass these conditions. This can prevent unauthorized access to application data and access to the database by unauthorized applications. For example, you could define a rule to limit execution of the `DROP TABLE` statement to a specific IP address and host name.

## 1.6 How Oracle Database Vault Allows for Flexible Security Policies

Oracle Database Vault helps you design flexible security policies for your database.

For example, any database user who has the `DBA` role can use the `DROP ANY TABLE` system privilege granted to that role. Suppose an inexperienced administrator believes they are on a non-production database when they execute a `DROP TABLE` command and is instead on the production system and drops a critical application table. This will probably cause an application outage, data loss, and hours to recover from. With Oracle Database Vault, you can create a command rule to prevent this user from making such modifications by limiting their usage of the `DROP TABLE` statement. Furthermore, you can attach rule sets to the command rule to restrict activity further, such as limiting the statement's execution in the following ways: