

ORACLE DATABASE SECURITY

Oracle Database security features help ensure regulatory compliance, protect from insider threat, promote information consolidation and sharing, and protect sensitive information on media.

Fine-Grained Auditing

DBAs specify the conditions necessary to generate an audit record.



Oracle Secure Backup

Data-to-tape encryption protects against the misuse of sensitive information if backup tapes are lost or stolen.

Oracle Audit Vault

Administrators can consolidate and protect audit information, enabling centralized analysis and reporting on audit data.



Oracle Identity Management

Sysadmins manage the lifecycle of user identities within and beyond the firewall. Strong authentication lowers risk of security breaches. With Oracle Identity Management, DBAs manage database users and authorizations in one central place.

Transparent Data Encryption

Protect information without change to the application by transparently encrypting data and decrypting it when it is read back to the user.

Oracle Label Security

Control access to critical business data using data classification and label-based access control.

Virtual Private Database

Customized security policies support security when standard object-level privileges and database roles don't meet application security requirements.



Oracle Database Vault

Managers control access to data and applications, even among administrators, protecting against insider threat from malicious intent, negligence, or oversight. The Command Rules and Realms features add "rules" and "protection zones" through which users access the restricted information. Multifactor authorization enforces how, when, and where applications can be accessed by verifying IP address, authentication method, and time of day.