**Oracle** – Oracle has two popular features that they deem as “Advanced Security Database Features”. *Transport Data Encryption* (TDE) and *Data Redaction*. TDE protects data-at-rest by encryption in the database layer. Data Reduction then aids TDE by reducing unauthorized data exposure preventing data leakage.

**Microsoft SQL Server** – Microsoft SQL Server offers your standard encryption at-rest with TDE. It offers access with *SQL Server Logins* and Active Directory (*AD*) integration. It supports secure application access with *dynamic data masking* and *row-level security*. It also offers monitoring and insights with *SQL Server Auditing* and *Windows Server Anti-malware.*

**MySQL** – MySQL like most databases offer encryption at-rest but also offers OpenSSL capabilities at the SQL level. This allows applications to add public-key asymmetric cryptography. It allows for the creating of public/private keys along with digital signatures. It also allows for dynamic data masking and encrypted connections via TLS and the X.509 standard.

All three products offer row-level encryption along with the ability to encrypt tables along with the database as a whole. They all also offer a Public Key Infrastructure, Oracle with the Java KeyStore, Microsoft SQL using its Extensible Key Management, and MySQL using their Keyring feature. They all can offer bilateral security, this can be achieved with data-at-rest using the encryption implemented when the database is not being used. When data is in-transit, they all offer the capability to encrypt the traffic that is being exposed. This is what creates the bilateral security of both data in-transit and at-rest being encrypted to secure databases.

<https://www.oracle.com/database/technologies/security/advanced-security.html>

<https://www.microsoft.com/en-us/sql-server/data-security>

<https://dev.mysql.com/doc/refman/5.7/en/enterprise-encryption.html>

<https://dev.mysql.com/doc/refman/5.7/en/data-masking.html>

<https://dev.mysql.com/doc/refman/5.7/en/encrypted-connections.html>