Case Study - Data Privacy for Databases

Using DPM to protect sensitive column data with no code changes

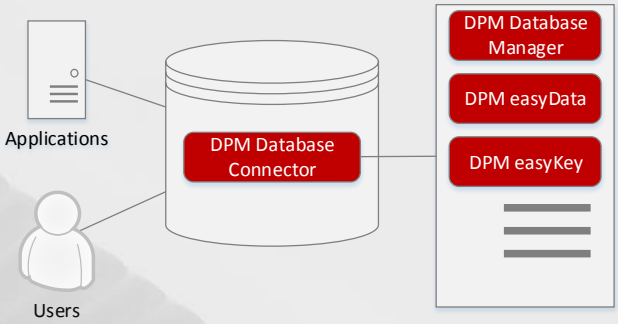
The Challenge

The banking client needed to transparently protect sensitive data stored in Oracle database columns without having to make application code changes. The data needed to be protected so that only authorized users could see the data and all other users would see de-identified data based on different user policies.

The Solution

Data Privacy Manager (DPM) was used to tokenize and protect the sensitive column data

The DPM encryption keys, de-identification of data and database connector were configured for the protection policies



The Benefits

- No code changes were required – DPM transparently protected the database columns
- Database protection is managed by the security admin and not the DBA
- As new data was inserted or updated, the DPM Database Connector tokenized the new values automatically
- Authorized users could see clear data and all other users could see only de-identified data
- The solution seamlessly worked with the existing backup architecture with no configuration changes required
- Upgrade path for protecting additional columns with masking and encryption for future use