15/02/2022

randtronics

Data Privacy Platform for Databases

Case Study

Using DPM to protect sensitive column data with no code changes

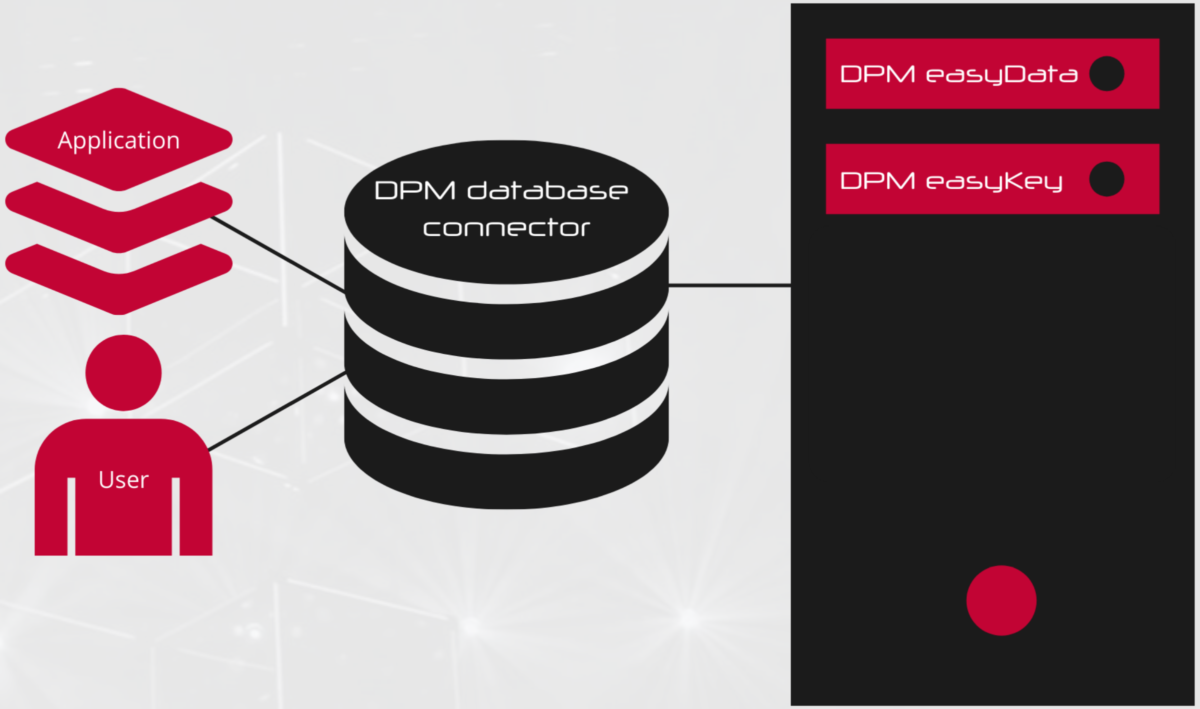
The Challenge

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 centrally managed privacy policies.

randtronics

The Solution

- Data Privacy Manager (DPM) was used to tokenize, mask and protect the sensitive column data
- The DPM encryption keys, de-identification of data and database connector were configured for the protection policies
- Privacy policies for encryption key and regulated data was centrally enforced



The Benefits

- No database, file server, network systems, architecture and application changes were required – DPM transparently protected the databases with AES256

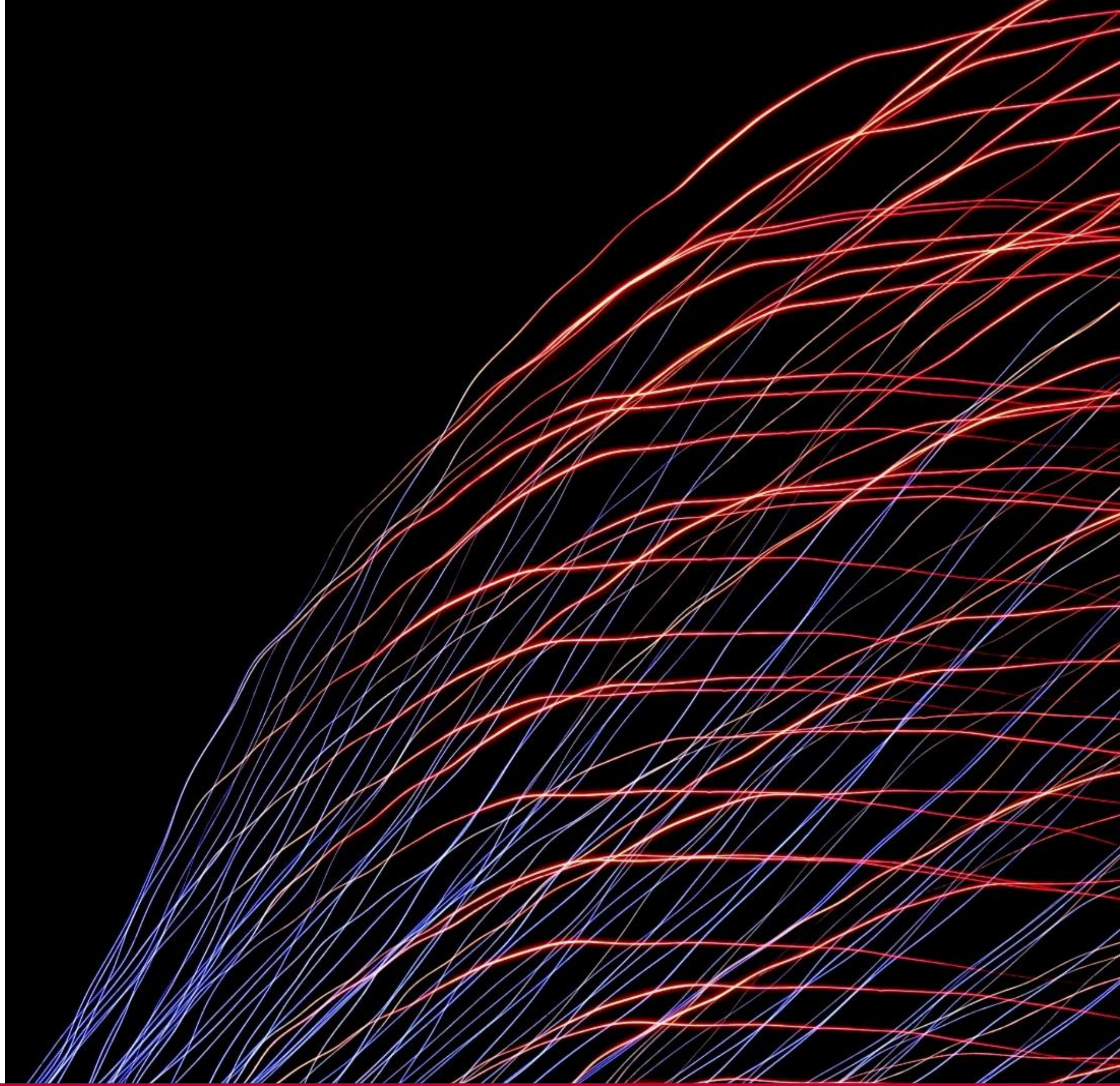
- Database protection is managed by the security admin and not the DBA

- Protection from all users, including the admin user. Only the database process user is allowed to access the database column and decrypt the field data

- The same method was applied to the SQL Server 2012 and 2019 databases and 2019 file servers. In the future, the same method would apply to newer versions and different database vendors

- High performance – application impact was negligible

- No changes needed for existing database and system backup



Randtronics LLC

Redwood City CA 94065 United States
+1 (650) 241 2671
enquiry@randtronics.com

Randtronics Pty Limited

S1.1, Level 1, Building A 64 Talavera Road
North Ryde, NSW 2113 Australia
+61 418 226 234