

# Tamper-proof database privacy

*Enhance, extend or replace native protection with Randtronics Transparent Data Encryption*

## Top five reasons to choose Randtronics DPM Transparent Data Encryption

**1 Air-gap sensitive data from your IT Organization:**

Native TDE alone doesn't protect your DB from a compromised privileged DBA or Sys Admin user

**2 Standardize DB Protection:**

Replace multiple flavors of native TDE and standardize on a single skillset and technology

**3 Expand protection beyond TDE:**

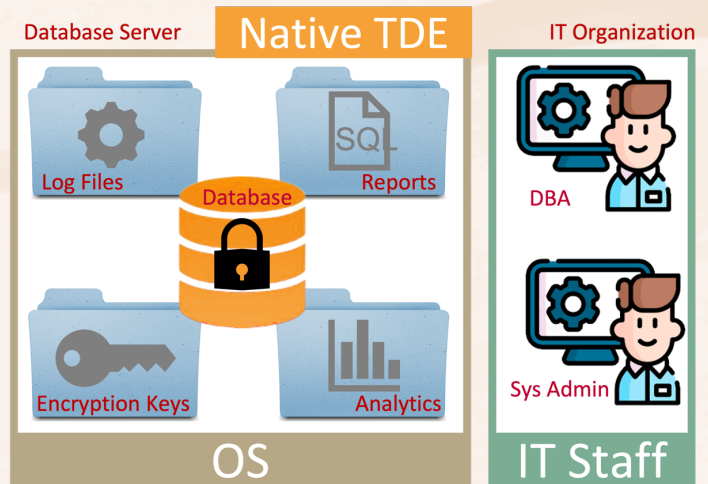
Protect databases, field-level data, file and web servers. Single protection solution that provides tamper-proof TDE, enterprise key management and field-level protection

**4 Protect sensitive data in and around the Database:**

Randtronics TDE goes beyond native TDE to also protect your DB Log Files, Encryption Keys, SQL reports and other materials co-residing on DB server or other file stores

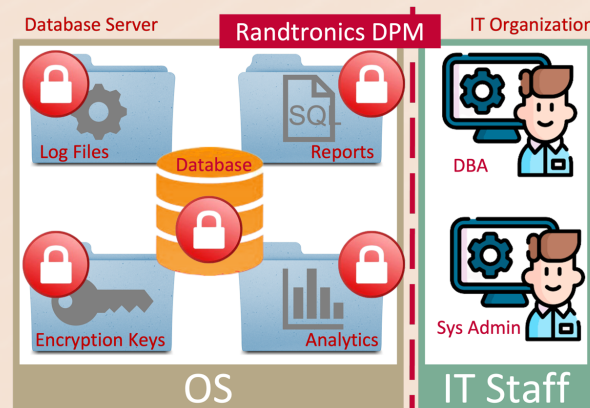
**5 Protect DB when native TDE is not supported:**

Randtronics TDE protects any database including those that don't support native TDE



*Tamper-proof database privacy and more with Randtronics*

Randtronics DPM is a data security platform for managing enterprise encryption and protecting your databases wherever they reside:



- ✔ Zero-trust encryption management system
- ✔ Air-gap separation between your IT organization and your sensitive data
- ✔ Standardize encryption management across multiple DB vendor technologies, web/app servers; all Windows & Linux VM or Kubernetes container environments
- ✔ Enhance, extend or replace native TDE

*Visit our website to learn more or contact us to discuss your data protection requirements*



# Randtronics Data Privacy Manager

*Standardize your organizations data privacy protection with Randtronics DPM*

Randtronics Data Privacy Manager (DPM) is a 100% software-only data security platform that manages encryption protections for structured and unstructured data on-premise and on-cloud.

The diagram illustrates the DPM Enterprise Encryption Management architecture. At the top, three main components are shown: DPM easyKey (represented by a key icon), DPM easyCipher (represented by a folder with a lock icon), and DPM easyData (represented by a database icon with a table showing masked data like '00000', '12345', 'XXXXX', 'Hidden', 'XOXOXO', '12345', 'XXX', 'Secret', '00000'). Below these is a central banner for 'DPM Enterprise Encryption Management'. Underneath the banner, five categories are listed: 'No-Code TDE Protection' (DPM easyCipher Agent on OS), 'No-Code FLP' (Database Connector on OS), 'No-Code FLP' (File on OS), 'Low-Code FLP' (API on OS), and 'Point-and-click File Protection' (DPM easy2Go on WIN).

## Encryption, Spoofing, Masking, Anonymization

The diagram shows three data types supported by DPM: 'Structured Data' (represented by a database icon), 'Unstructured Data' (represented by a document icon), and 'Data in the cloud' (represented by a cloud with a downward arrow icon).

Contact us to today to discuss your data protection requirements at [www.randtronics.com](http://www.randtronics.com)

