Date: September, 2023

Townsend Security Alliance Key Manager EOL Migration

Protection for your most sensitive data, everywhere

The problem

Alliance Key Manager customers need a replacement:

- Alliance Key Manager are Townend Security's range of Hardware Security Modules and virtual appliances
- Marketed as a secure key manager Microsoft SQL Server Transparent Data Encryption (TDE)[1] and other encryption key applications[2]
- End-of-Life[3] announced effective from 30 November, 2023

Townsend customers need an alternative means of securely protecting their database that ideally:

- Requires minimum change or disruption;
- Is cost effective; and
- Offers the basis for extending protection to a wider range of systems to further reduce potential attack surface

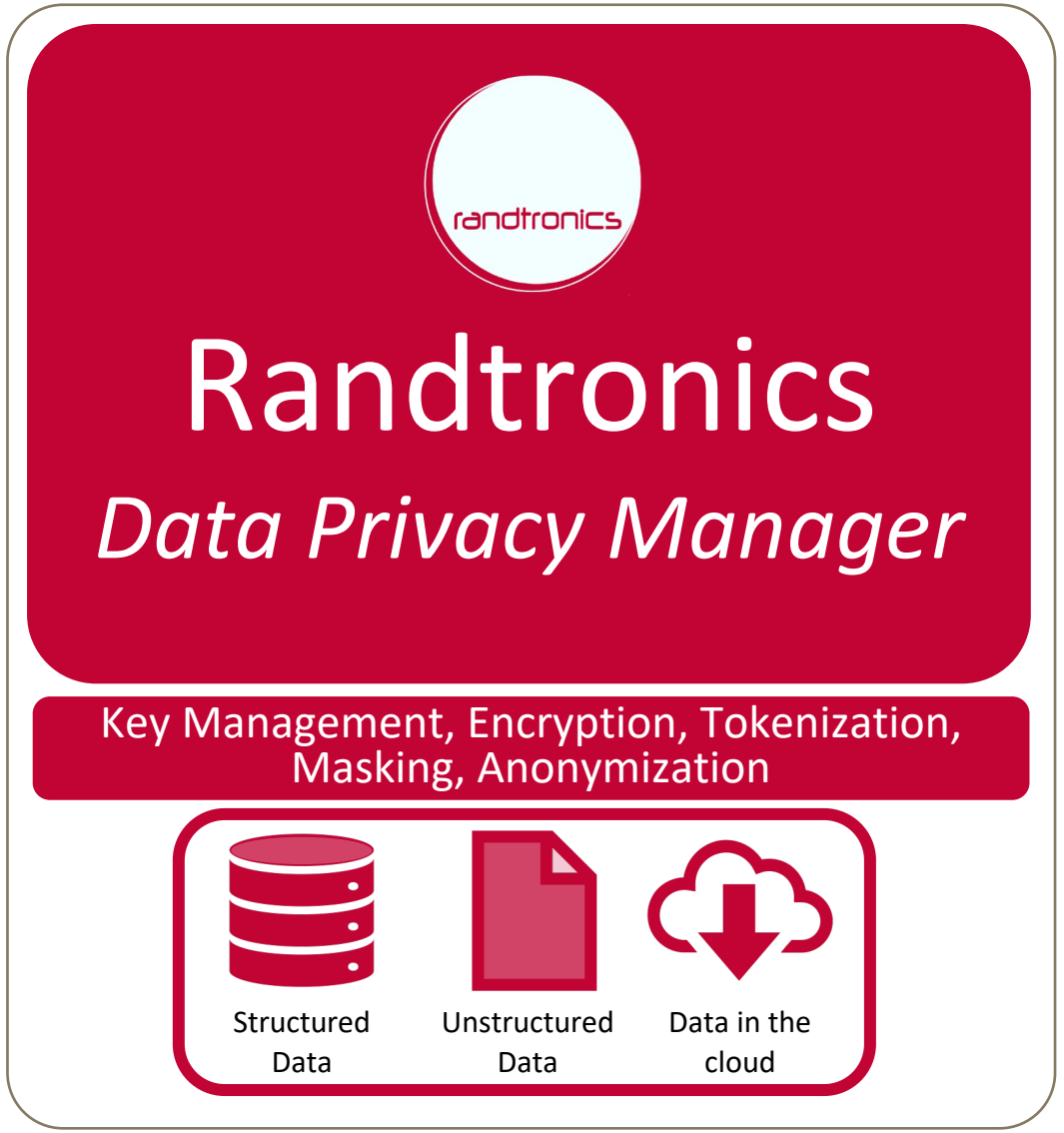
End of Life

30/11/23

1. Internal TDE feature of MS SQL Server
2. Other key management applications includes MySQL TDE, MongoDB TDE
3. https://info.townsendsecurity.com/

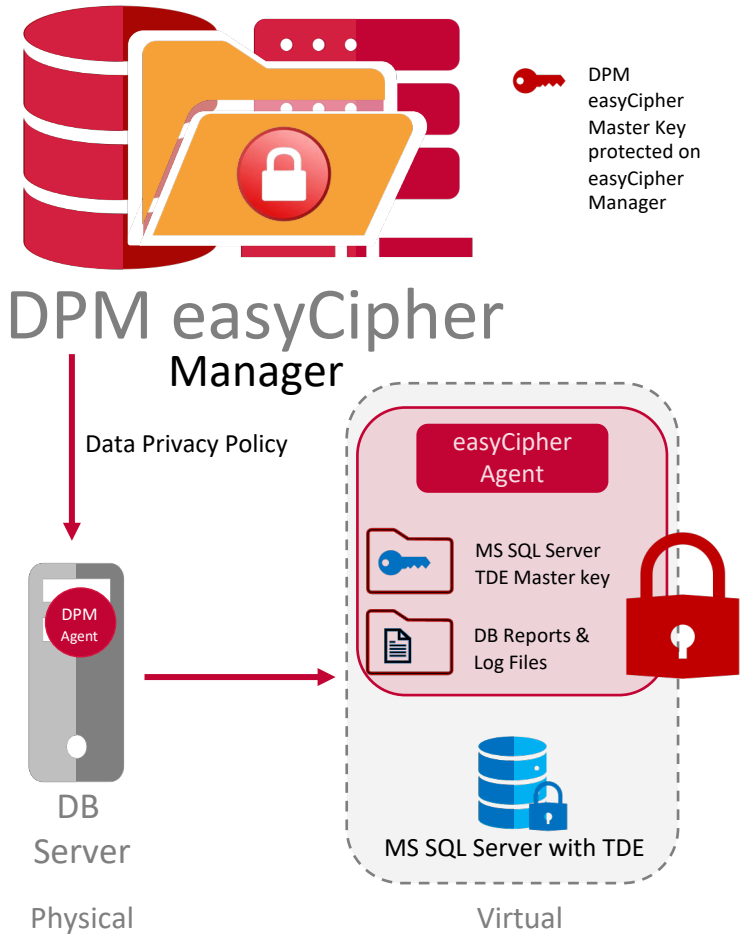
Solution

- Replace Alliance Key Manager with Randtronics DPM data privacy manager
  - 100% software replacement for your HSM or virtual appliance
  - Cost effective means of delivering key and data separation
- Choose to keep or replace MS SQL TDE
  - Double encryption is also an option
- Option to increase protection now or in future
  - Extend TDE protection to all laptops & servers
  - Add column-level data protection
  - Add API tokenization
  - Option to add HSM for high-assurance root of trust as and when demanded by compliance standards



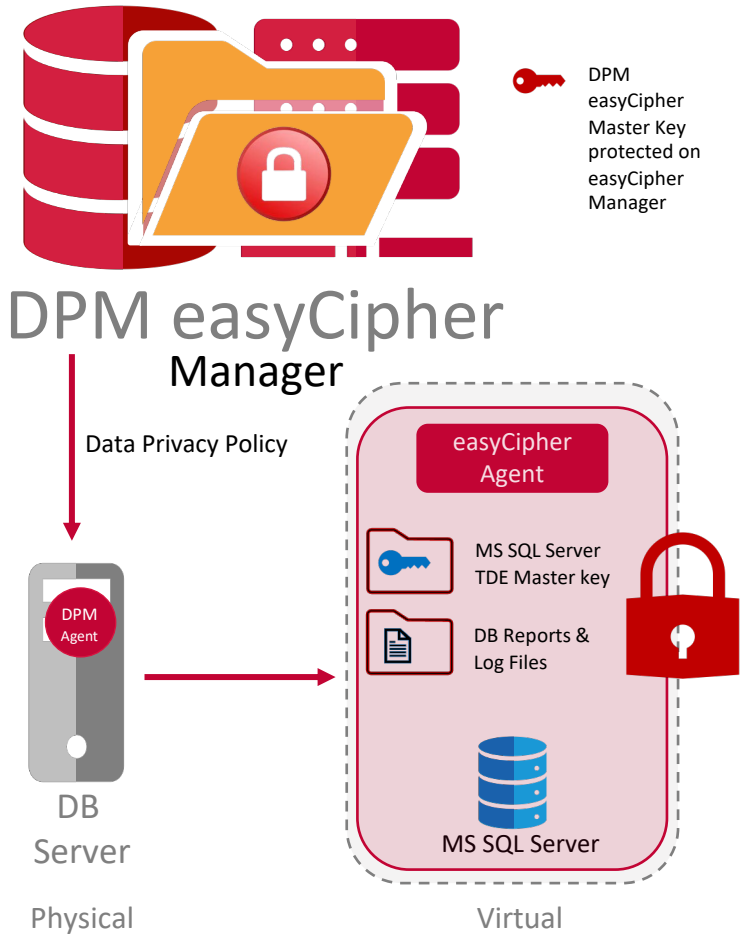
Option 1 – Retain MS SQL TDE

- MS SQL Server TDE is retained to protect DB contents
- Balance of DB server environment protected by DPM easyCipher TDE
  - Protect MS SQL TDE master key, DB reports/log files, lock down other applications
  - Separation of duties, prevent DBA changing log files, control access for all OS users & Sys Admin
  - Root of trust protected by DPM easyCipher manager
  - Audit log for all access to DPM protected data



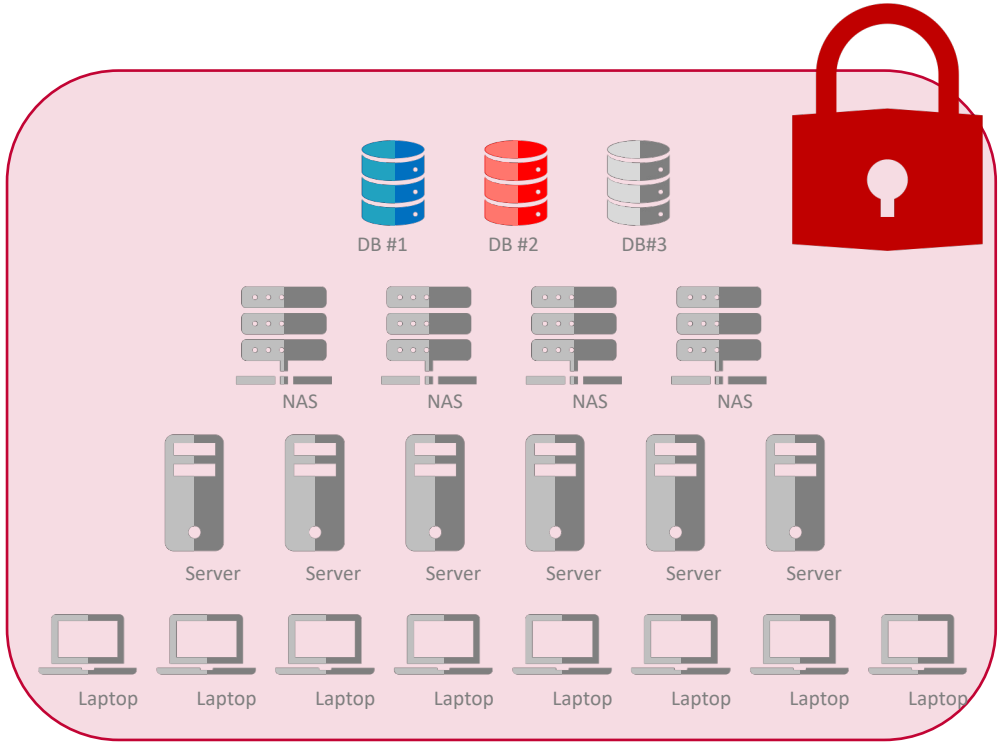
Option 2 – Replace MS SQL TDE

- Entire DB server environment protected by DPM easyCipher TDE
  - Protect MS SQL DB, DB reports/log files and lock down other applications
  - Separation of duties, prevent DBA changing log files, control access for all OS users & Sys Admin
  - Sys admin protection
  - Add user and application ACL and encryption, application white and black list
  - Audit log for all access to protected data
  - Root of trust protected by DPM easyCipher manager



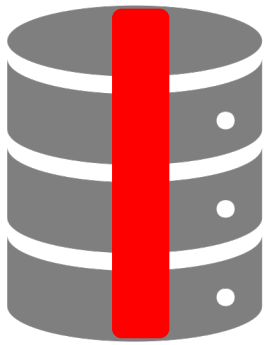
Extend TDE Protection

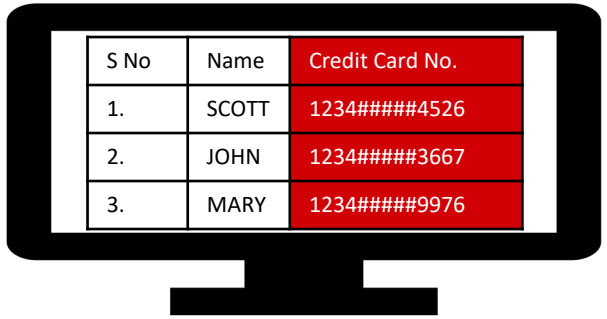
- Extend your data protection scope to prepare for more stringent compliance requirements
- Minimize data breach attack surface by encrypting all databases, servers and laptops
- Centrally administered, policy-based data protection covering all systems



Column-level data protection

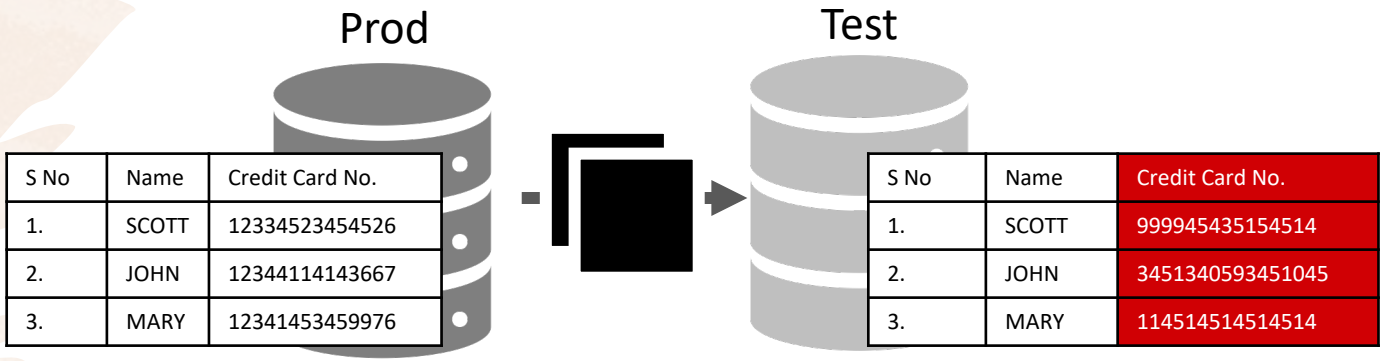
- Column level de-identification with no code changes for MS SQL Server
  - Options include tokenization, format preserving encryption, masking
- API based data protection available
  - Standardize your code-level data protection methods
  - Standardized policy-based data protection for TDE and Tokenization





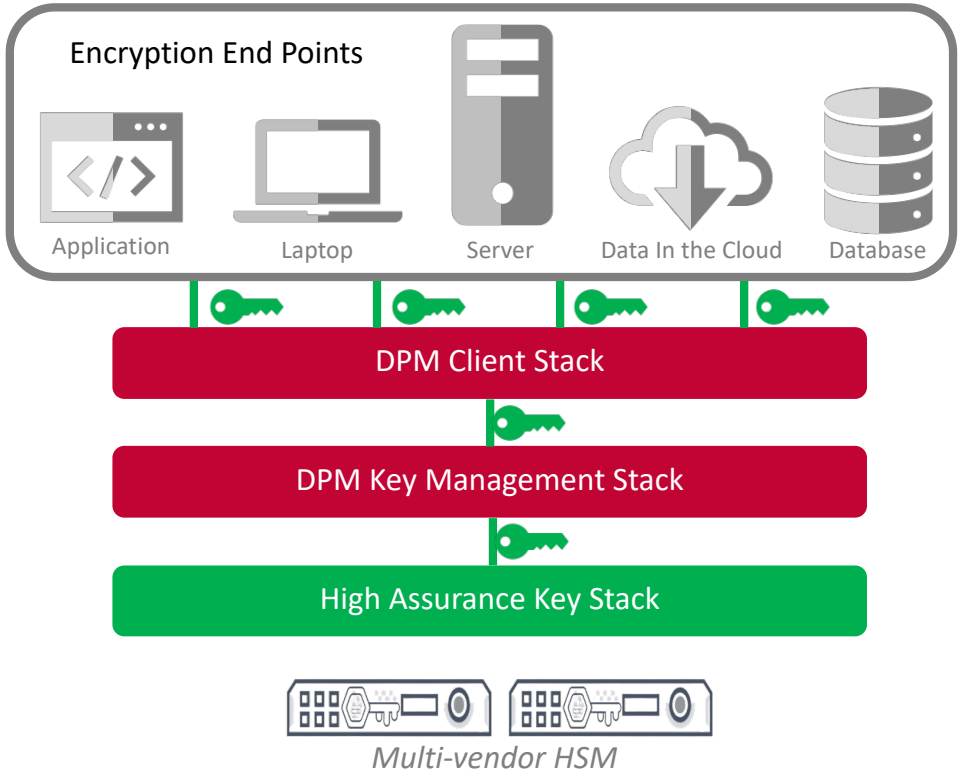
Sanitize data sets for test or analytics

- Reduce risk of data breach from copies of production data
- Implement simple, standardized methods for creating regular sanitized copies of production data
  - For representative test data sets
  - For analytical data sets that can be safely shared



High key assurance protection

- Enterprise key & certificate management DPM easyKey
  - easily manage key & certificate policy usage enterprise wide
  - Policy-based lifecycle management of keys & certificates
- Option to elevate key assurance security level if required via HSM
  - Choice of HSM vendor
  - Option to protect keys to FIPs140-2/3 Level 3/4 & Common Criteria EAL4+ certified hardware



White-glove Migration Service

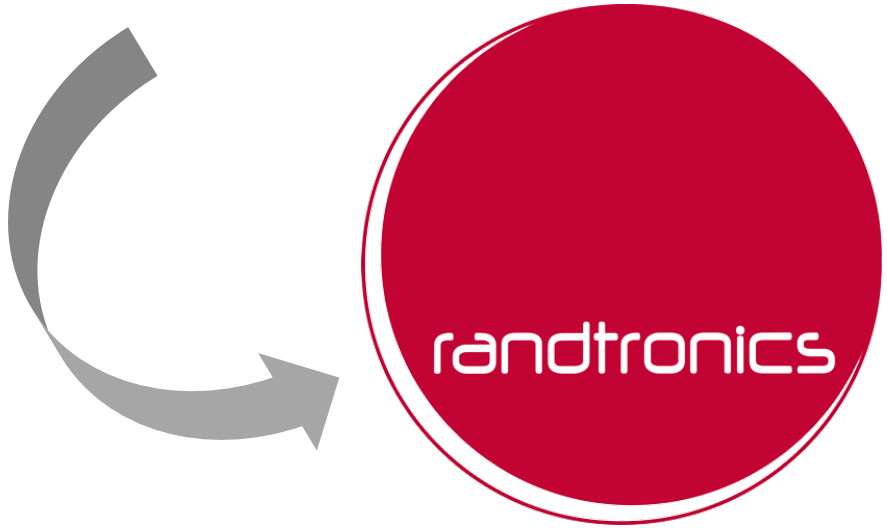
Randtronics offers customers the option of an end-to-end migration service:

- Start with an initial scoping review, obtain indicative costing & timeline.
- Conduct a POV in your environment:
  - DPM protection of your key data types
  - Optimal migration methods for your mix of systems
  - Detailed product and end-to-end migration services quote

Indicative Migration Timeline

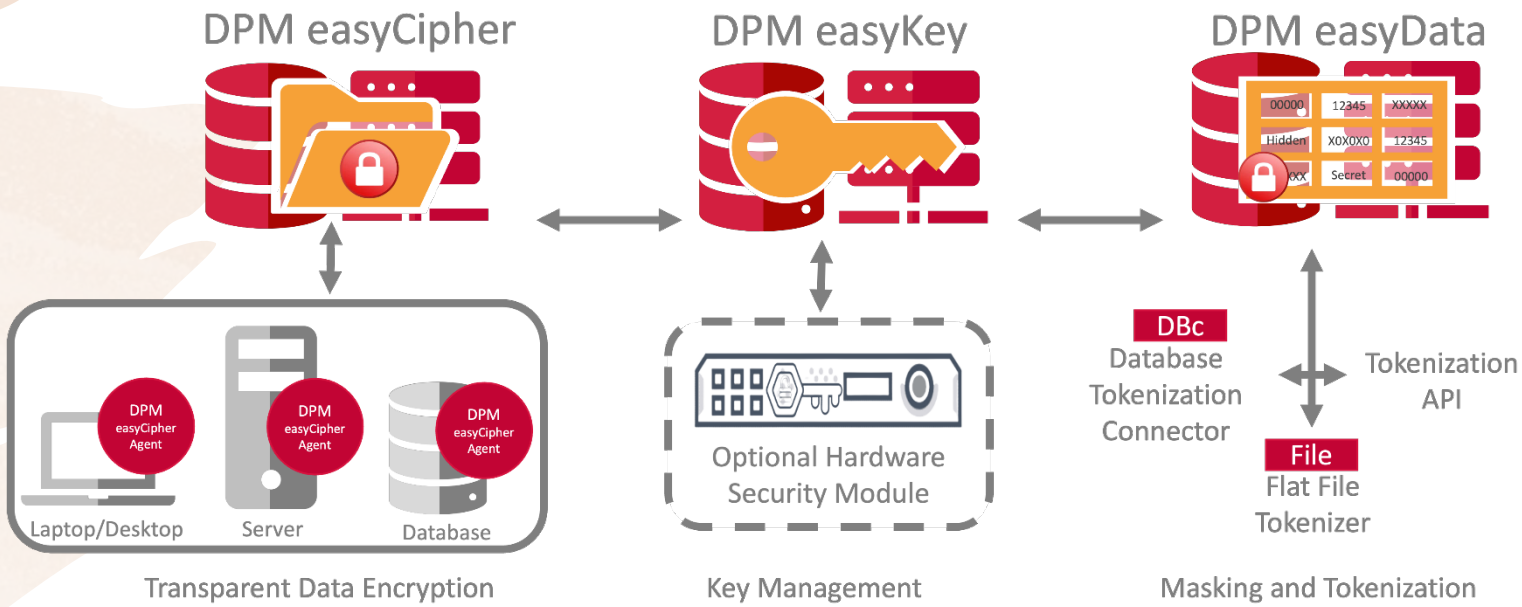
Benefits

- Drop-in replacement for your current database TDE solution using Alliance Key Manager
- Cost savings:
  - Lower maintenance costs
  - Rationalize HSM costs:
    - Software only key management option
    - Choice of multi-vendor HSM integration
- Future-proof solution with options to further tighten your data privacy measures to address future compliance requirements



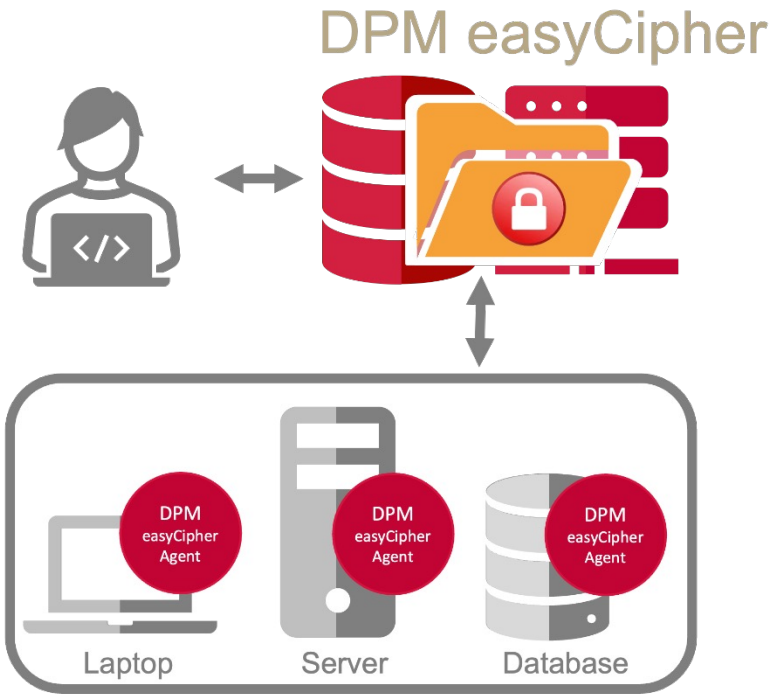
Introducing Randtronics DPM

- Protects all Windows/Linux based environments
- Transparent Data Encryption
- Masking & Tokenization
- Key Management
- Centrally-managed, policy based:
  - Data privacy controls
  - Lifecycle Key management



DPM easyCipher

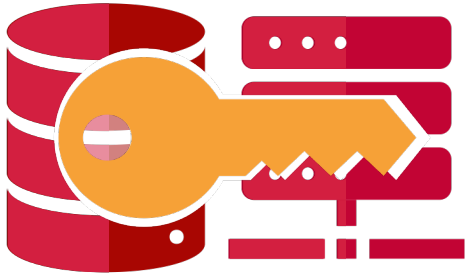
- Runs in a Windows or Linux environment on premise or in multi-vendor cloud (Windows/Linux Virtual Machine instances)
- Provides transparent data encryption of files (MS office, video, images, structured, unstructured, etc.) on laptops and servers
- Allows transparent data encryption of multi-vendor database (editions & versions) including Oracle, MS SQL Server, DB2, MySQL, Maria, Postgres
- Security protection policies are managed from a central point by administrators
- Protection from unauthorized users, system administrators and root users
- Application white and black list access control to sensitive files
- Encryption keys are stored and managed centrally



Enables users to transparently encrypt files, folders, applications and databases in real time without any code changes

DPM easyKey

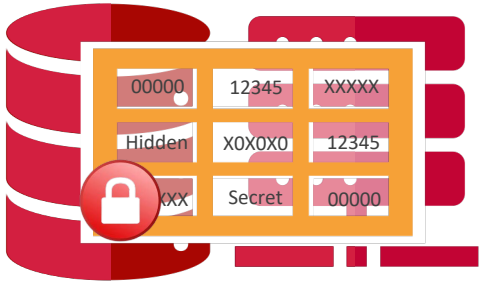
- Policy-based lifecycle management of encryption keys and certificates
- Software only key manager with optional multi-vendor HSM integration
- Simplifies data privacy legislation compliance with full control and auditable history of key storage



DPM easyKey

DPM easyData

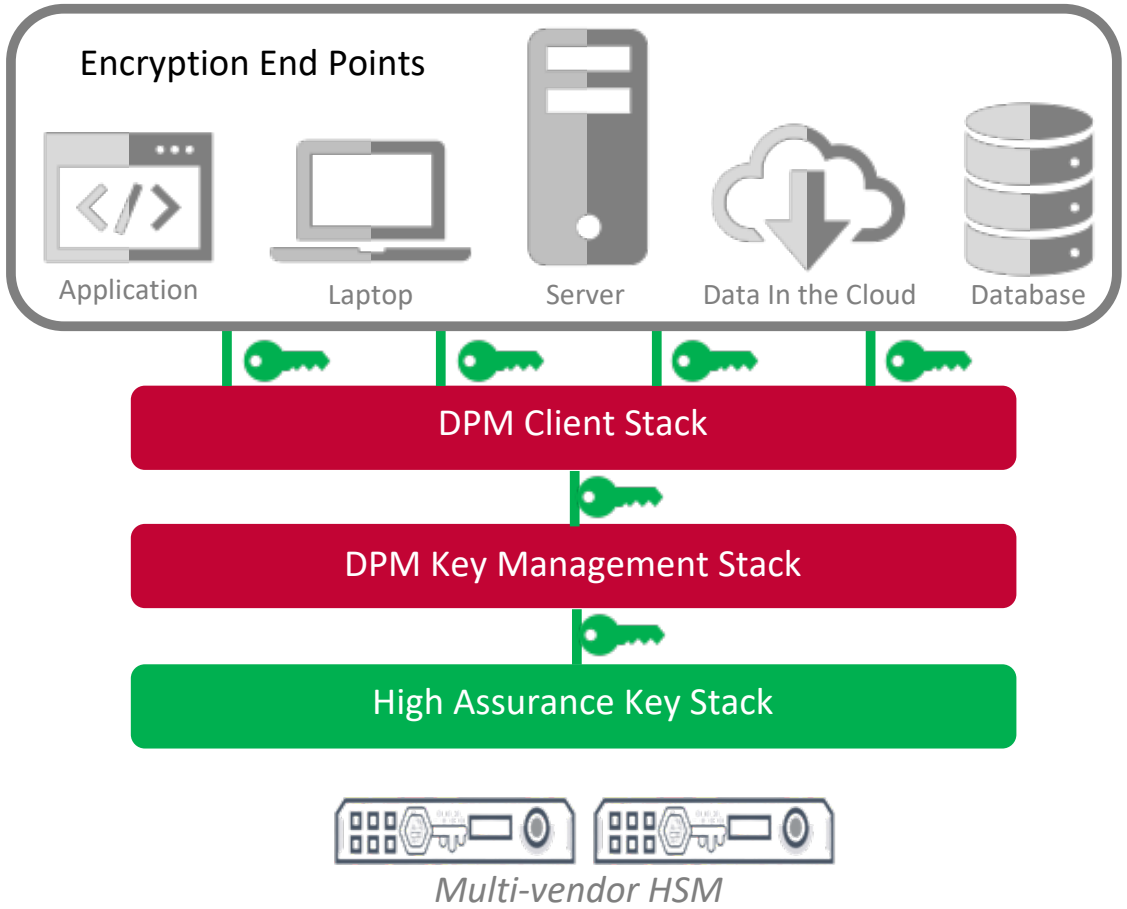
- Runs in a Windows or Linux environment on premise or in multi-vendor cloud (Windows/Linux Virtual Machine instances)
- Provides field-level data de-identification services: Masking, Tokenization, Anonymization, Pseudonymization and Encryption,
- Security protection policies are managed from a central point by administrators
- Pre-built agents offer no-code change field-level protection for
  - Column data in MS-SQL and Oracle databases
  - Flat files
- API (priced same as an agent) offers low-code, standardized access to centrally managed data protection services



DPM easyData

Multi-vendor HSM options

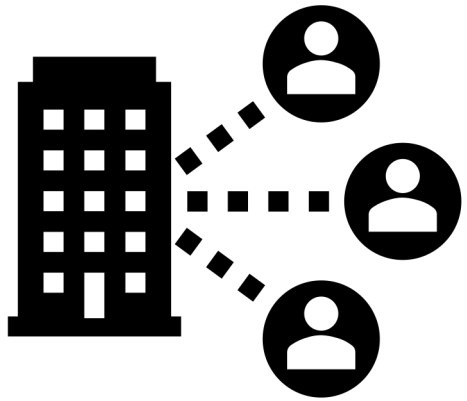
- HSM not required, software key management solution
- HSM masterkey storage available as an option
- Freedom to mix and match multi-vendor HSM’s



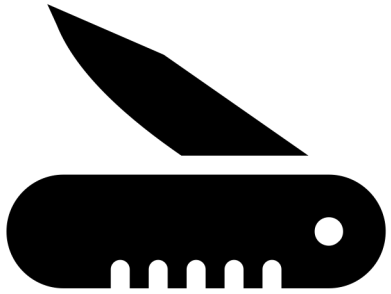
Flexible, quick and simple to Deploy

DPM components are ‘standard’ Windows/Linux/DB apps and as such, are quick and, simple to deploy and cost-effective to manage:

- Lightweight local agents/utilities easy to add to standard build configurations
- Management modules available via SaaS or on-prem installation
- No special skills required (standard Windows / Linux/ database)
- No special architecture (standard methods for backup, n-tier separation and scalability)



Management Modules



Locally deployed agents and utilities

Randtronics LLC

Milpitas CA 95035 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

Thank you for your time

email: bob.adhar@randtronics.com

Cell: +614 18 226 234 or +1 650 241 2671