Date: May, 2023

Transparent Data Encryption, Every System

Protection for your most sensitive data, everywhere

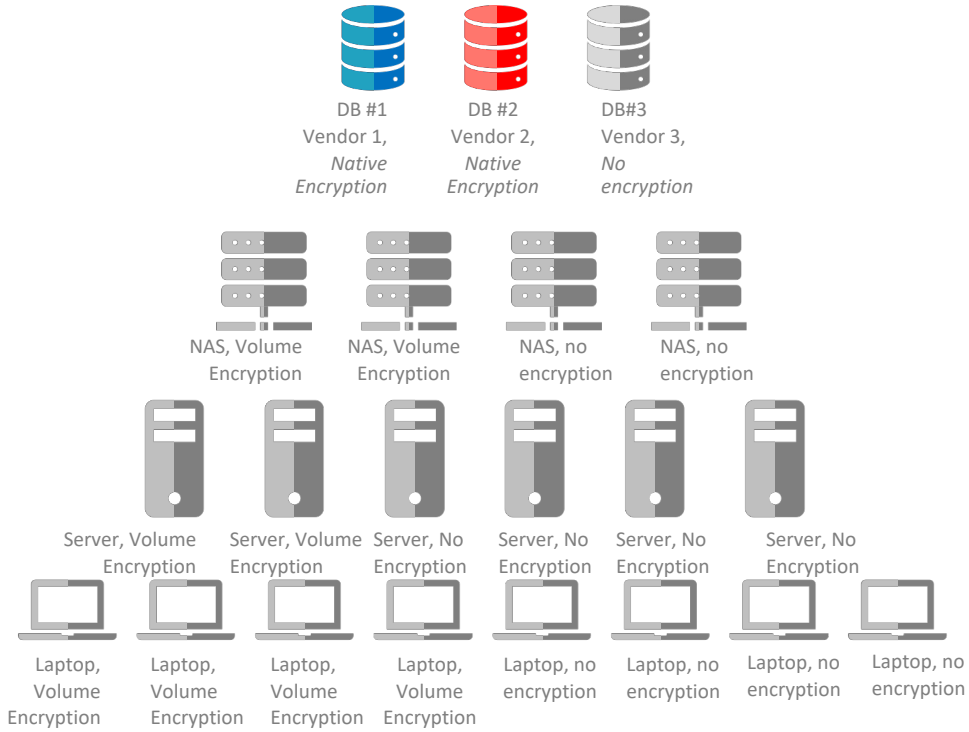
The problem – encryption gaps

Multi-vendor databases with inconsistent protection:

- Training, development, backup databases unencrypted
- Multiple flavors of native encryption specific to DB vendor (if available)

Server environments, NAS & laptops weakly protected:

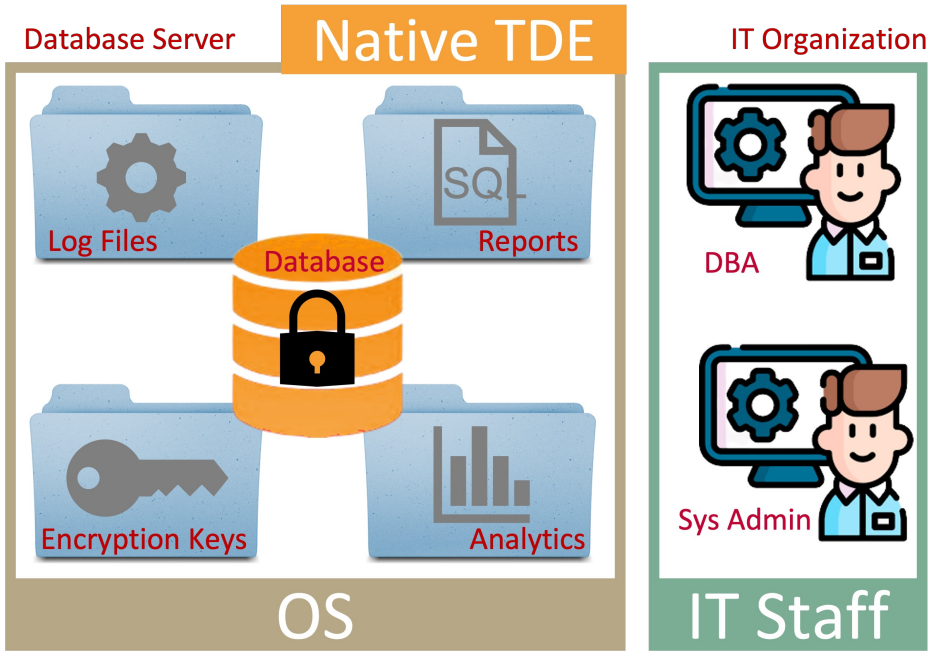
- Volume/ Full disk encryption (if used) ineffective once machine is running
- Native database TDE provides narrow protection, leaves broader DB server environment vulnerable



Native DB TDE - Gaps

- Echos and traces stored outside on the DB server and shared on other devices such as file server, cloud storage and laptops.
- Attackers can dumpster-dive DB, web app and file servers for reports, test data or analytics systems.
- Privileged DBA accounts (if compromised) can extract or change data and cover their tracks by altering log files.
- Privileged Sys Admin accounts (if compromised) can copy entire DBs, along with their TDE encryption keys

Native TDE protects database contents; broader environment is is somebody else's problem.

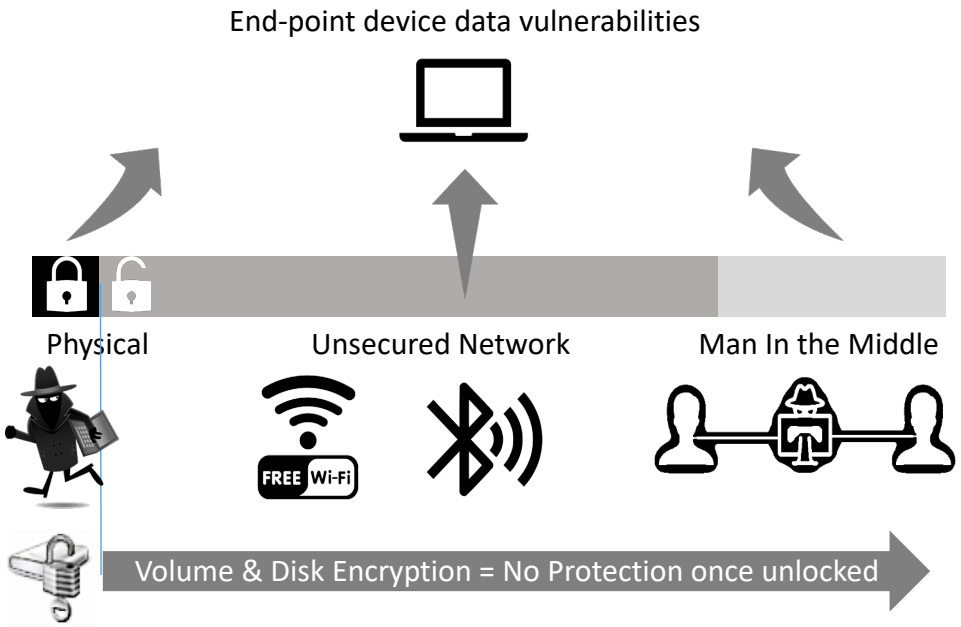


Native TDE = Transparent Data Encryption (TDE) as provided by database vendors

Volume Encryption – Gaps

Volume and Disk encryption provides ‘tick the box’ encryption but not effective protection:

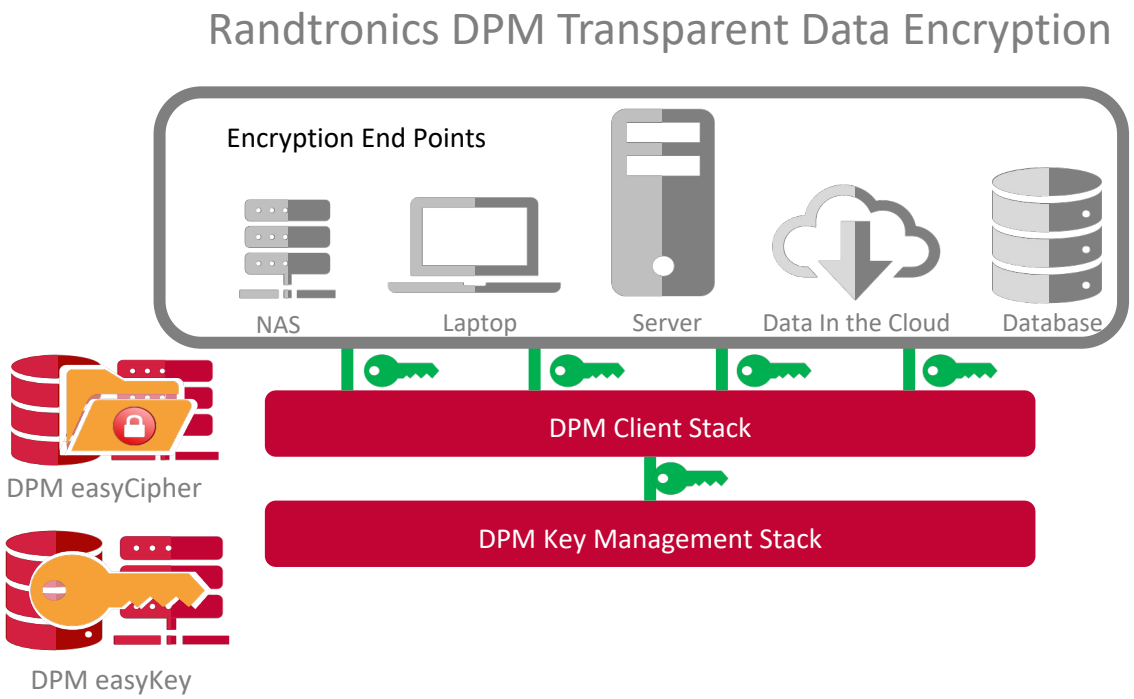
- Inside data center – vulnerable to attack via compromised user
- Mobile workforce via public networks – vulnerable to interception attacks



The Solution

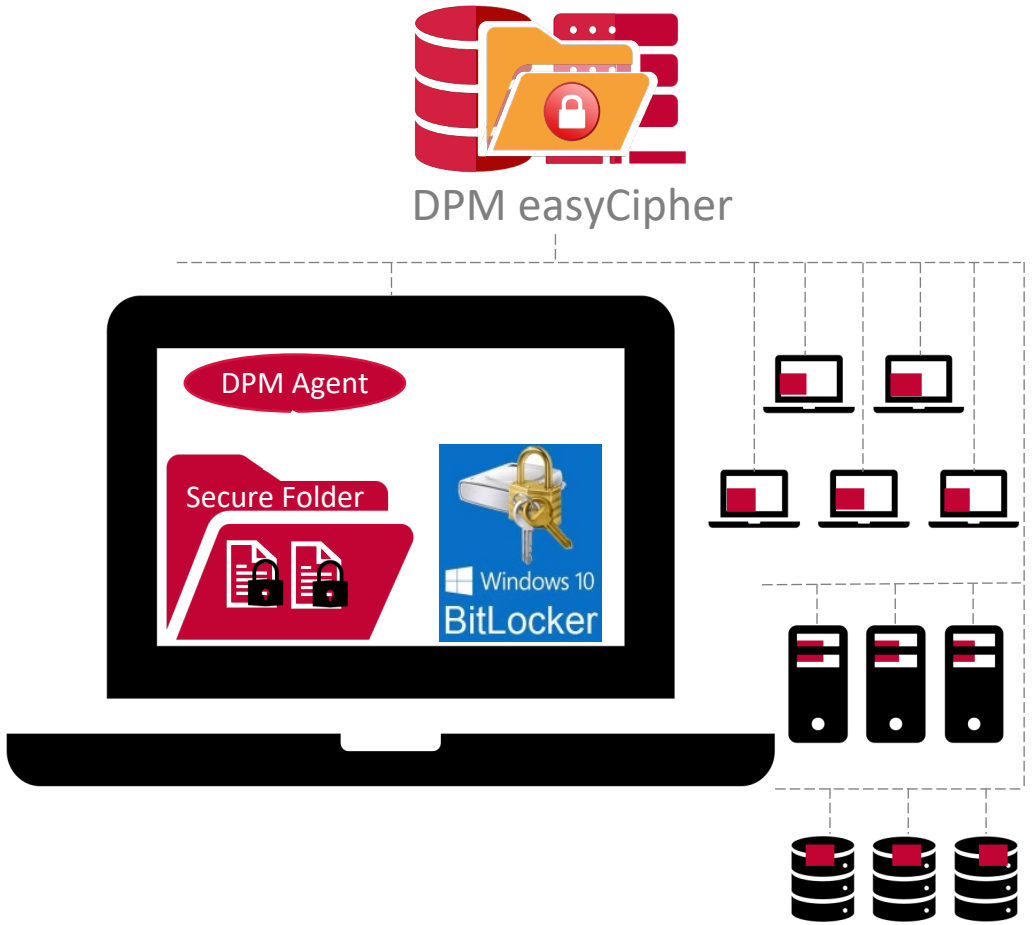
Randtronics enterprise-wide transparent data encryption:

- Protects all Windows/Linux based environments
- Provides TDE for any database
- Support double-encryption:
  - for databases already using native TDE
  - For devices using volume/ disk encryption
- Centrally-managed, policy based:
  - Data privacy controls
  - Lifecycle Key management



Fully Managed encryption

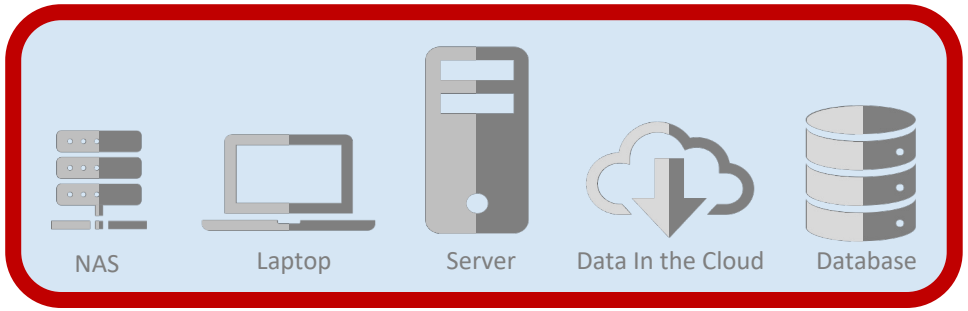
- TDE protection for databases, servers & laptops is delivered by means of local installed DPM agent software.
- The user is able to read and write files when offline.
- Encryption keys are stored and managed centrally
- Data protection policies (who can see what) are also managed centrally.
- Randtronics TDE protection complements and co-exists alongside volume/ disk encryption



Benefits

- Enterprise-wide TDE protection for all Windows/ Linux based systems: databases, servers, NAS, laptops
- Sensitive data protected from IT administrators
- Encryption keys and policies are managed centrally:
  - separation of duties
  - Auditable
  - Resilient & Recoverable

Transparent Data Encryption, Every System

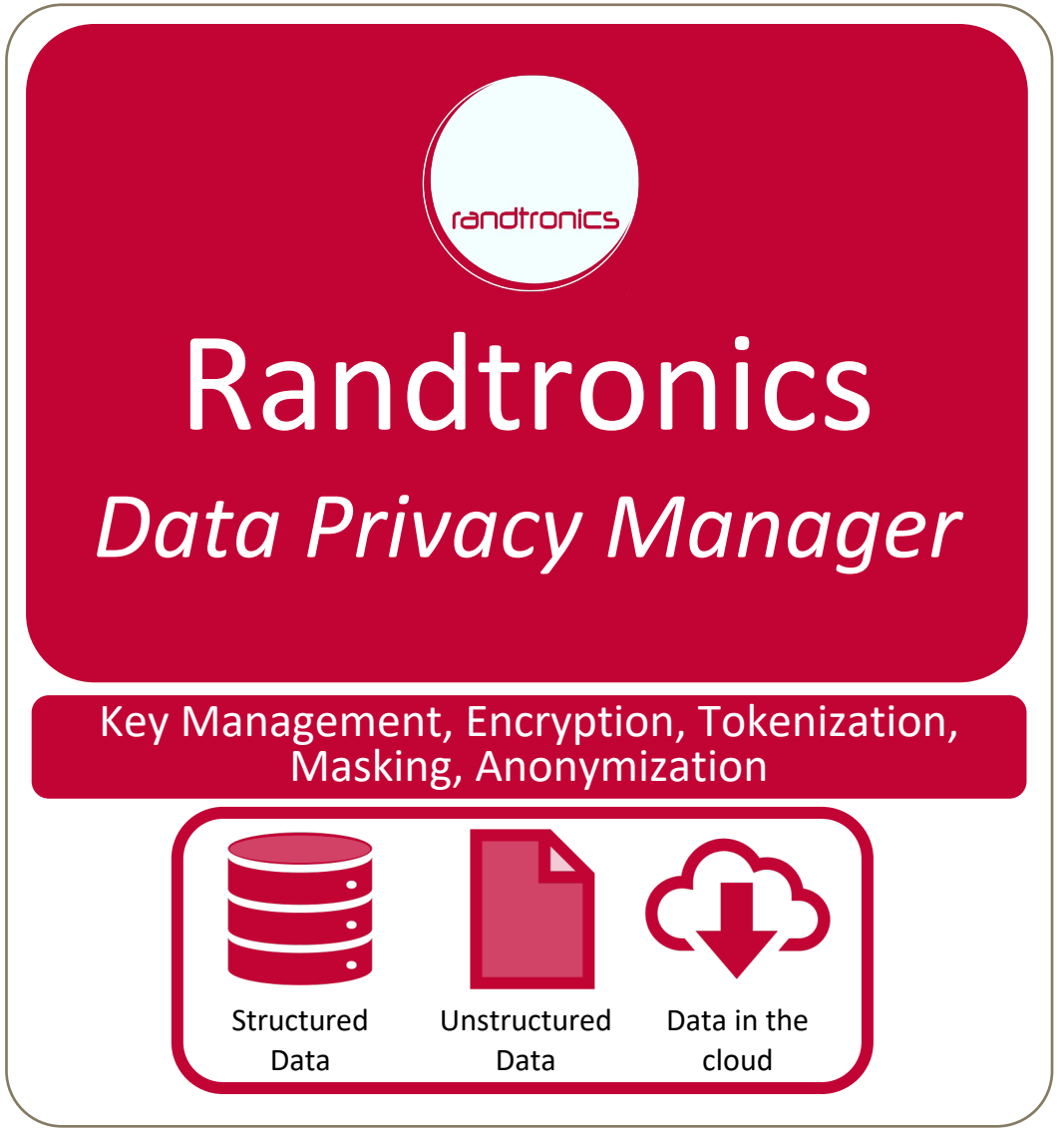


Introducing Randtronics Data Privacy Manager

Randtronics DPM is an enterprise encryption management platform created with the aim of making implementing and managing effective encryption ‘easy’ for organizations

The Transparent Data Encryption, Every System solution features two DPM products:

1) DPM easyCipher – TDE for databases, servers files, folders and laptops and
2) DPM easy2Key – enterprise management of encryption keys and certificates



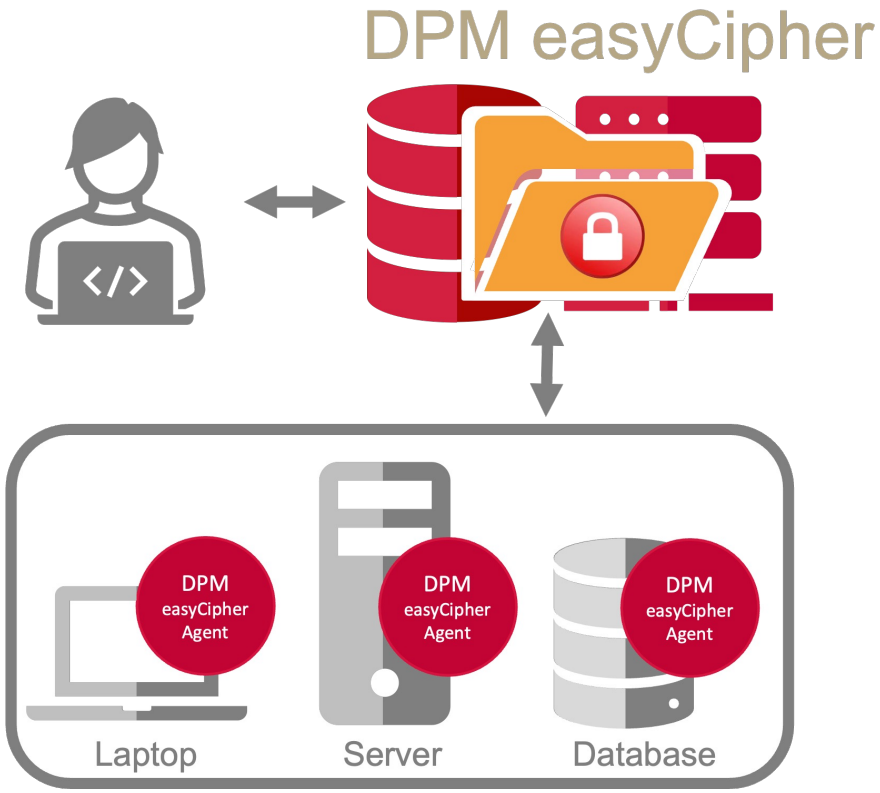
DPM easyCipher

- 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
- Supports encryption on cloud file systems: OneDrive, Box, Dropbox and Google Drive
- Allows transparent data encryption of multi-vendor database data files such as 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

DPM easyCipher

TDE for databases, files stores and laptops

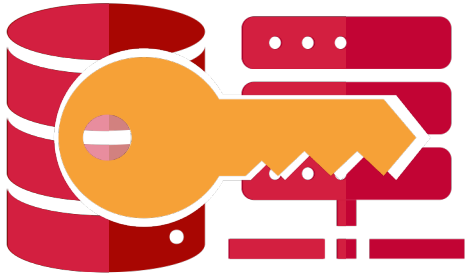
- DPM easyCipher provides transparent data encryption of files on laptops and servers
- Supports encryption on cloud file systems.
- Enables transparent data encryption of multi-vendor database
- Centralized managed of security protections – protect from unauthorized users, system administrators and root users
- Integrates with DPM easyKey if centralized key management is required.



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

DPM easy2Key

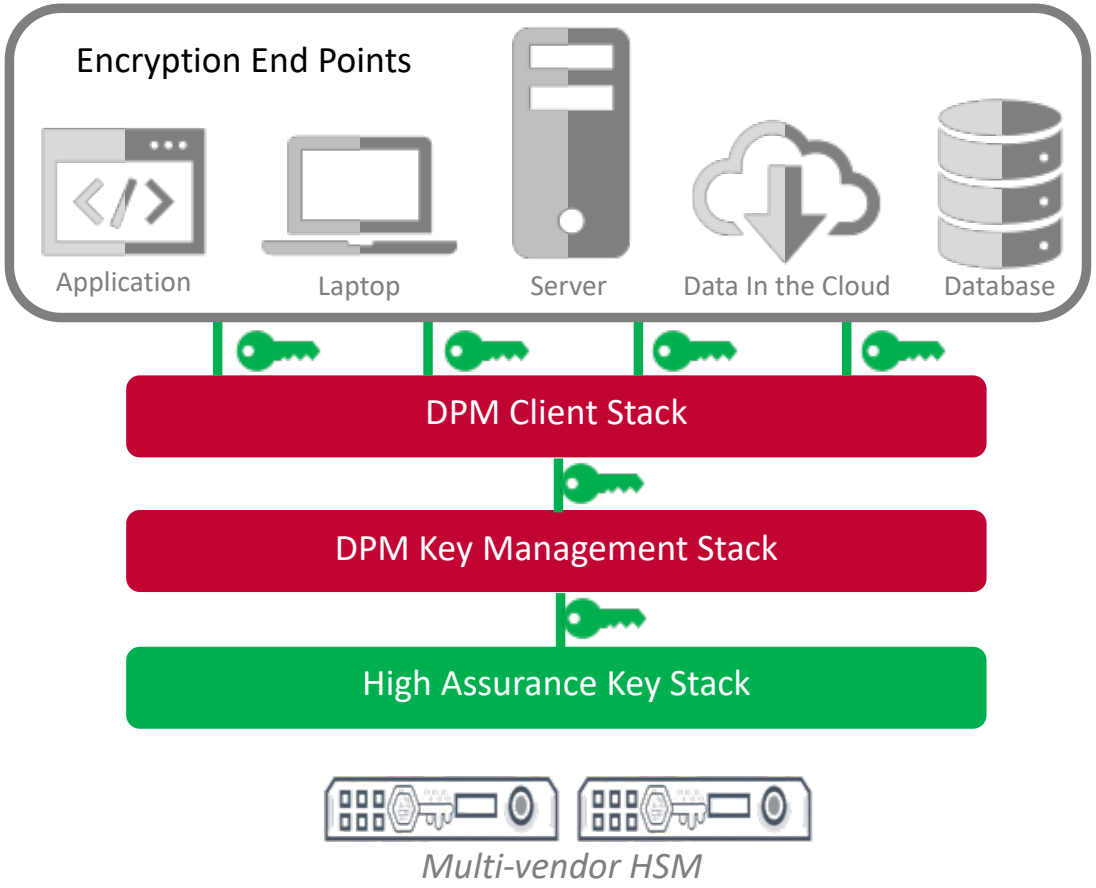
- Policy-based lifecycle management of encryption keys and certificates
- Software only key manager with optional multi-vendor HSM integration
- Simplifies data privacy legislation compliance with full control and auditable history of key storage



DPM easyKey

Multi- vendor HSM Support

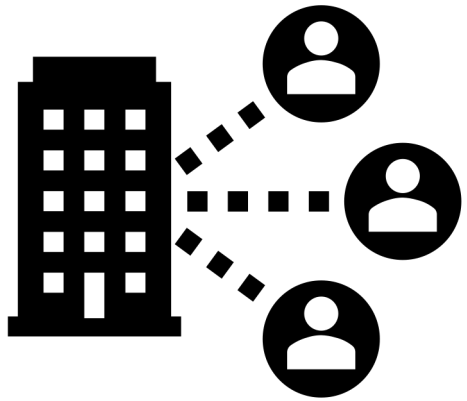
- Choice of software only or HSM based masterkey storage
- Hardware key assurance options – plug'n'play integration of multi-vendor HSMs to protect keys to FIPs140-2 Level 4 & Common Criteria EAL+ certified hardware
- Mix and match multi-vendor HSM's



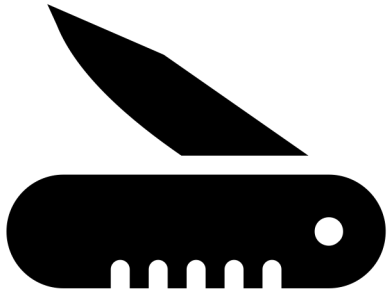
Flexible, quick and simple to Deploy

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