Randtronics DPM Product Overview

Randtronics DPM: The most capable and flexible enterprise encryption ***data security platform***

Version 2.2
October 2024

Randtronics Data Privacy Manager

The most capable and flexible enterprise encryption data security platform

1. Introduction

Randtronics DPM is a suite of software products providing enterprise wide data privacy management and protection using key management, encryption, tokenization, masking, anonymization and access control.

DPM is a 100% software-only data security platform that manages encryption protections for structured and unstructured data on-premise and on-cloud.

DPM is typically used by large organizations to centralize and manage their data privacy protections effectively consistently across all platforms.

Customers use DPM products to create a centralized Data Security Platform that performs some or all of the following:

a) **Standardizes encryption key management and data privacy controls** through centrally controlled policies

b) **Standardizes encryption protection for files, databases and folders** for all Windows and Linux systems across the organization

c) **Standardize and centrally control, data protection methods** built in to all new applications

d) **Role separation** – separate the control and management of data privacy protections outside the reach of Database, Systems and Application Administrators such as to deny these privileged users the ability to see sensitive data in the clear on the systems they are administrating.

Common motivations that drive customers to consider DPM products include:

1) **Compliance** – introduction of new stringent personal data protection legislation such as GDPR, CCPA or HIPAA that impose significant penalties for organization that suffer a data breach resulting in the disclosure of personal data. Organizations that use encryption both lessen the risk of a data breach and lessen the penalties imposed if a breach occurs.

2) **Ransomware Resilience** – Organizations that have good backups and have encrypted sensitive data across the organization are much less vulnerable to ransomware coercion.

3) **Technical Skill Shortages** – Skilled cybersecurity staff are in short supply, it makes little sense to have these people performing basic encryption related administration tasks when DPM can manage the complexity and can be administered by staff with basic technical skills.

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 product features:

- Universal, centralized key management to FIPs 140-3 Level 3 and EAL 4+ assurance level
- Encryption, format preserved encryption, tokenization and masking
- No-code change Transparent Data Encryption (TDE) for Windows and Linux environments
- No-code change field-level protection (FLP) for MS-SQL Server, MySQL, Maria, Postgres, Oracle database and flat files
- Low-code API protection for any field-level protection (FLP) for any application-database stored anywhere
- Shared file encryption to protect files shared across Dropbox, email, OneDrive, Google Drive, FTP

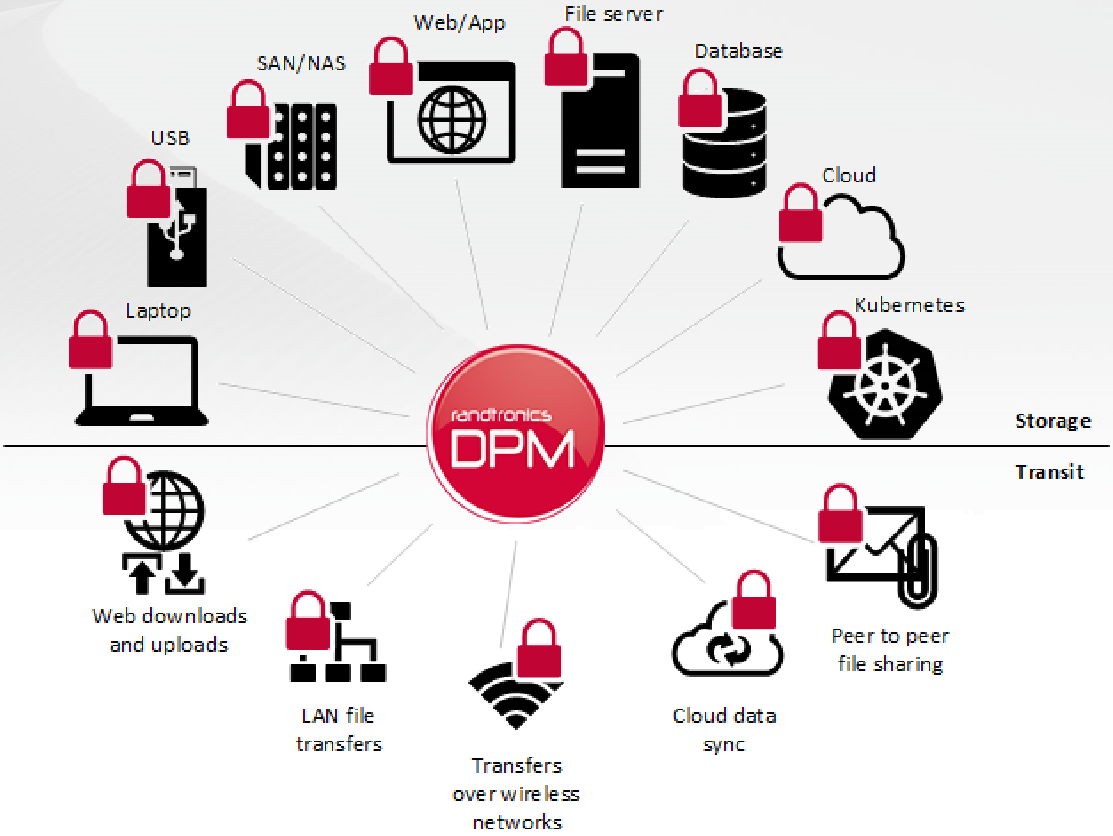


Figure 1 DPM encryption protecting structured and unstructured data on-premise and on-cloud

Randtronics DPM is designed to meet the needs of customers seeking to centrally manage all of their encryption protections across all of their platforms, ideally without any code changes or as few code changes as possible.

Randtronics DPM addresses this need for universal, centrally managed protection in the following ways:

- No-code agent-managed TDE on Windows and Linux physical or virtual machines
- No-code agent-managed FLP for supported Databases on Windows or Linux physical or virtual machines
- No-code utility for flat file data de-identification
- Low-code API managed protection for any field, record, file stored anywhere
- Point-and-click encryption for sharing files over insecure mediums and media
- Addition of centralized key management and tamper-proof data-privacy protection on top of Native TDE
- Software key assurance to FIPs140-3 Level 1
- Key assurance to FIPs 140-3 Level 3/4 and Common Criteria EAL 4+/5+ via third party HSM from France, Germany, USA, Switzerland to meet country specific geo-political needs.

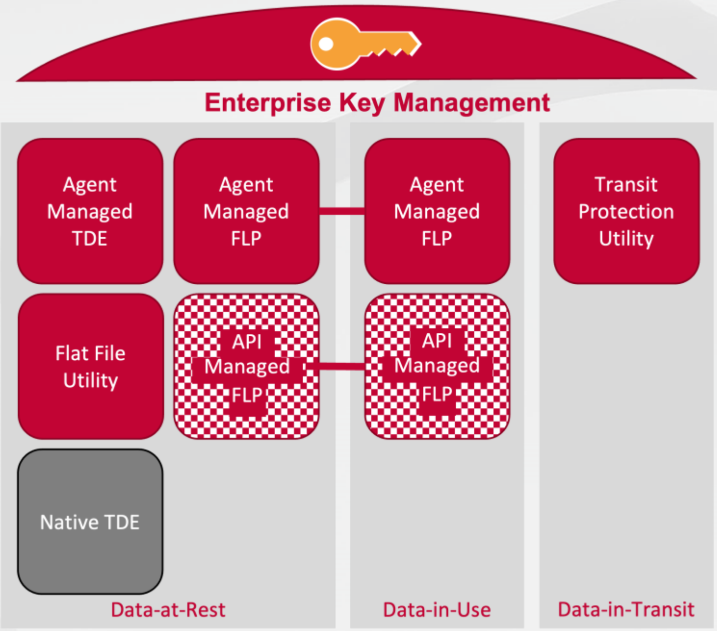


Diagram Key:		*Policy-base Key Management*	*Policy-based Data Protection Management*	*No Code Changes*	*Activity Logging (audit trial)*
***No-code** function via DPM agent or DPM utility*	🟥	✓	✓	✓	✓
***Low-code** DPM API-based function*	▨	✓	✓	Low Code	✓
DPM Managed Key function (only)	■	✓	N/A	✓	✓

Terms:
TDE – Transparent Data Encryption
FLP – Field Level Data Protection
API – Application Programming Interface
Native TDE – Non-Randtronics TDE solution from DB vendor
N/A – Not applicable i.e. Policy-based data protection not possible with Native TDE

Figure 2 DPM centralized management of enterprise encryption

2. DPM Product Suite Overview

The Randtronics DPM software products together provide a comprehensive centrally managed enterprise encryption platform whilst offering flexibility for customers to mix and match to meet their specific requirements:

- Standalone no-code TDE with automated key management
- Standalone enterprise key management
- No-code TDE with key management
- FLP with key management
- Point & Click protection for file sharing via insecure medium & media (with or without centralized key management)
- All of the above: no-code TDE, FLP and centralized key management.

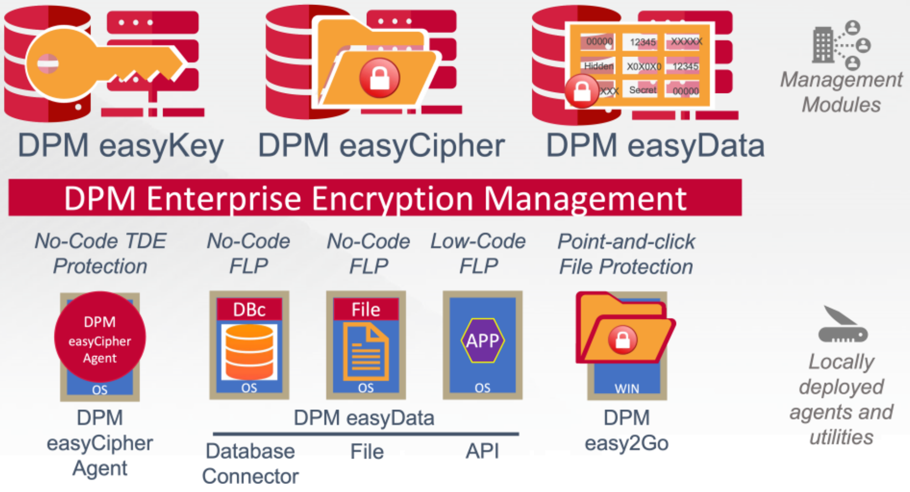


Figure 3 DPM product suite (shown in Red)

The DPM Product Suite comprises:

- **Management modules** – centrally deployed components that manage key and encryption activities
- **Agents and Utilities** – deployed on Linux or Windows environments
- **Standalone software** – easy2Go is a standalone file encryption solution for Windows workstations (works with or without centralized certificate management).

The individual components of the DPM Product Suite are:

- **DPM easyKey** – management module, providing a central place for key and certificate management. Allows generation of keys internally in software or via a cluster of multi-vendor hardware security modules
- **DPM easyCipher** – management module that enables transparent data encryption and access control of files, applications, databases stored on laptops, Windows or Linux servers and Kubernetes containers
- **DPM easyCipher agent** – agent deployed on Windows or Linux workstation and server environments: Database servers, File servers, Web/App servers, Desktops and Laptops
- **DPM easyData** – management module that tokenizes, encrypts and anonymizes data using a web service interface for any web, app and database

- **DPM easyData Database Connectors** – agent deployed on MS-SQL Server or Oracle Database environments for de-identification of live databases
- **DPM easyData Agentless Database** – agentless de-identification for MS-SQL Server, Oracle database, Maria, MySQL and Postgres environments
- **DPM easyData File** – utility to access the services of DPM easyData management module to provide de-identification and redaction of data inside flat files
- **DPM easyData API** – program level access to data de-identification services
- **DPM easy2Go** – utility that provides end to end encryption of any files shared across an insecure medium such as FTP, email, public cloud and other networks
- **DPM easyCloudPlus** – Randtronics offers customers the option of deploying the DPM easyKey, DPM easyCipher and DPM easyData management modules, on-premise or accessing these services via Randtronics' DPM easyCloudPlus encryption-as-a-service SaaS offering.

3. DPM easyKey

Randtronics **DPM easyKey** is an enterprise key manager product for centrally managing encryption keys and certificates.

- DPM easyKey is a 100% software only key manager product that can centrally manage encryption keys for a wide range of software application
- For customers requiring the highest levels of assurance such as FIPs140-3 Level 3/4 Common Criteria EAL4+, DPM easyKey optionally uses a mixed-vendor fleet of HSM's[1] from USA, Germany, France and Switzerland by linking encryption keys used throughout the organization to a central root of trust.

The software has a web browser-based interface for administrators to maintain the encryption keys and a KMIP interface and RESTful API for client applications to use the encryption keys.

Encryption keys are either generated and protected internally on the DPM easyKey, or an HSM if optionally installed.

DPM easyKey provides Root of Trust services for applications. When DPM easyKey provides the option of auto-generating keys in software or sourcing key HSM products. In this latter case the HSM becomes the source of Master Key, System Keys, Key Encryption Keys and Data Encryption Keys.

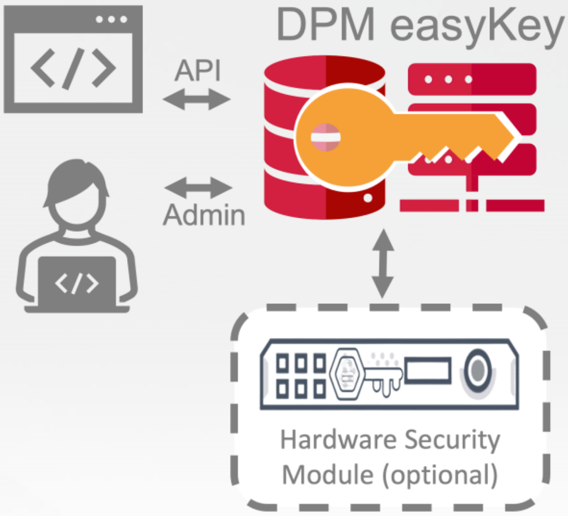


Figure 4 DPM easyKey API & Web browser Admin

Supported backend databases: • *Microsoft SQL Server 2016 and up* • *MySQL 8.0*	***Supported third-party key management:*** • *Multi-vendor HSMs (Utimaco, Entrust, Thales, Fortanix, Securosys, Futurex and Engage) and Microsoft Azure key vault* • *KMIP supported enterprise key manager*
Supported environments: • *Windows Server 2016 and up* • *RedHat Linux, CentOS, Oracle Linux* • *Ubuntu*	***Supported client interfaces:*** • *Transparent data encryption using easyCipher agents* • *APIs using RESTful and KMIP* • *Field level protection using easyData*

[1] Hardware Security Modules (HSM) are specialized hardware key protection devices

4. DPM easyCipher

Randtronics **DPM easyCipher** is an enterprise encryption product that provides transparent data encryption (TDE) for files, databases and folders on Windows and Linux environments.

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

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
- Integrates with DPM easyKey, enabling centralized key management.

The DPM easyCipher product has two components:

- **DPM easyCipher Manager** – provides a central place for administrator to configure security policies and to distribute those policies to end user agents.
- **DPM easyCipher Agent** – runs on each laptop, desktop or server in order to transparently encrypt and enforce access control policy. Is designed to run in the background – users do not need to change anything in order to start using the software.

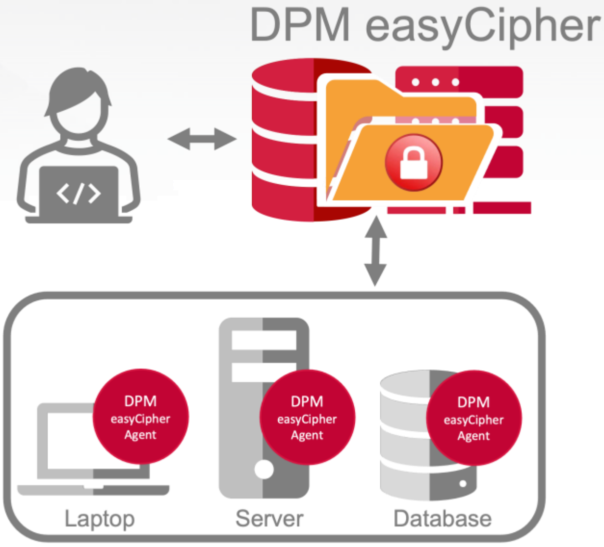


Figure 5 easyCipher Manager & Agent

DPM easyCipher

Supported backend databases:

- *Microsoft SQL Server 2016 SP1 and up*
- *MySQL 8.0*

Supported environments:

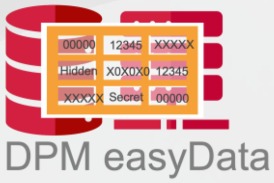
- *Windows 8.1, 10, Server 2012R2 and up, Microsoft Hyper V*
- *RedHat, CentOS, Oracle Linux, SUSE and Ubuntu*
- *Any physical or virtualized environment, multi-vendor cloud, Kubernetes containers and NAS*

Supported clients:

- *Any Windows and Linux based file servers, database servers, web and application servers*
- *Any Windows and Linux laptops and desktops*
- *Secure container with encryption and access control for master keys, configuration files, passwords*
- *Any application is supported with whitelist and blacklist enforcement*
- *Kubernetes containers*
  Up to 5,000 agents supported per manager

5. DPM easyData

Randtronics **DPM easyData** is a high-performance data-de-identification engine. It allows flat files, web and app server applications and databases to encrypt, FPE, tokenize, mask and anonymize data using centrally controlled data privacy policies.



- Multi-language tokenization and anonymization
- Format-preserving or standard encryption
- Masking, encryption and tokenization of column level data with no application code changes
- Protection from DBAs, software developers, outsourced workers, cloud administrators
- Protection from DBAs, software developers, outsourced workers, cloud administrators
- High performance
- Web service API for client applications to perform masking, tokenization/detokenization, encryption and anonymization
- Agentless de-identification of database columns for test databases
- Full auditing of access to protected data.

Data de-identification is the process of replacing sensitive data with fake data based on privacy policy. DPM easyData allows flat files, web and app server applications and databases to encrypt, tokenize, mask and anonymize data using centrally controlled data privacy policies.

Organizations using DPM easyData have the ability to ensure all access and usage to confidential data is centrally managed and subject to audit tracking.

- Web service API for client applications to perform masking, tokenization/ detokenization, encryption and anonymization
- Full auditing of access to protected data.

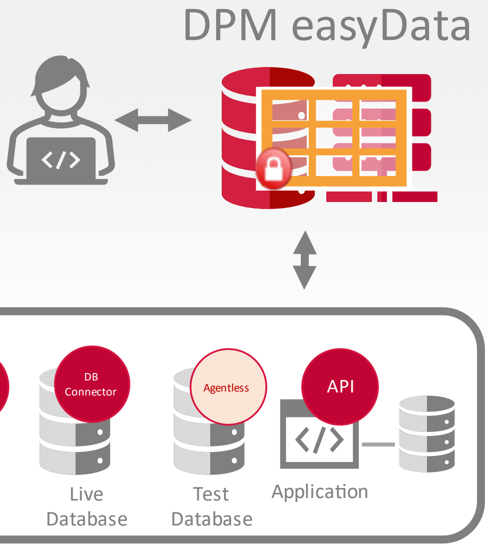


Figure 6 easyData and integration options

The DPM easyData product has four components:

- **DPM easyData** - provides a central place for administrator to configure data protection policies for applications, files and databases. Web service APIs are provided for integrating any application
- **DPM easyData Database Connector** – runs on MS-SQL or Oracle databases to provide tokenization, encryption or masking of column level data. A connector is required on each database containing data to be protected
- **DPM easyData Database Agentless** - de-identification of MS SQL Server, Oracle, MySQL, Postgres and Maria database columns for testers, developers and analytic purposes
- **DPM easyData File** – runs on target machines providing data de-identification for flat files.

Supported databases for DB Connector:

- *Oracle 19c*
- *Microsoft SQL Server 2016 and up*

Supported databases for agentless Test data protection:

- *Oracle 19c*
- *Microsoft SQL Server 2016 and up*
- *MySQL 8.0*
- *MariaDB 10*

Supported environments for DB Connector:

- *Windows*
- *Linux*

Supported clients for API integration:

- *Any legacy and current applications supporting web services*

Supported environments for easyData File:

- *Windows*
- *Redhat Linux, CentOS, Oracle Linux*

Supported backend databases for DPM easyData:

- *MySQL 8.0*
- *MS SQL Server 2016 and up*

Supported environments for DPM easyData:

- *Windows Server 2019 and up*
- *RedHat Linux, CentOS, Oracle Linux*
- *Physical and virtualized environments*

5.1 DPM easyData File

DPM easyData File de-identifies data inside any flat file using centralized policy managed by easyData. Command line interface allows integration with existing scripts.

The product has the following features:

- Policy based data de-identification using DPM easyData
- Masking, tokenization, format-preserving encryption
- Data types supported include numeric, alpha and alphanumeric of various formats including bank account numbers, emails, names, addresses, etc.
- Text file format supported include delimited type such as CSV, space or tab delimited or based on a position within the file
- Search and replace of sensitive data based on regular expression.

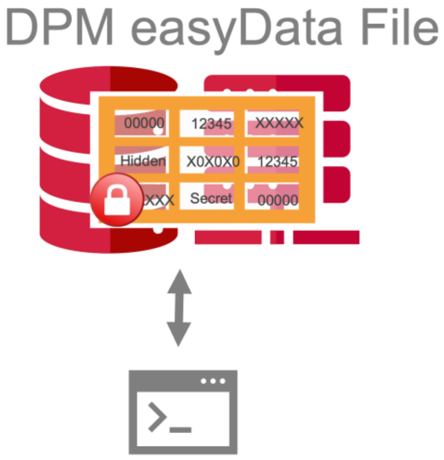


Figure 7 easyData File, flat file protection

6. DPM easy2Go

DPM easy2Go encrypts files as they are transmitted end to end and only provide decryption control to authorized parties. DPM easy2Go ensures persistent encryption that follows the files.

The product has the following features:

- Any file type and size are supported
- Single file or folder
- Protection options are password, digital certificate or centrally managed symmetric key
  - Password – both sender and recipient use an agreed password for encryption and decryption of files
  - Digital certificate – a file is protected with X.509 public certificate. Only nominated recipients can decrypt the file using their private key
- Works with DPM easyKey for centralized generation and management of policy based digital certificates
- Vault to store frequently used passwords and public certificates
- Integration with Windows File Explorer and CLI option
- Restriction of start and end date for decryption (Enterprise license)
- Receiving party also required to install a copy of DPM easy2Go
- Forever free download for DPM easy2Go reader edition.

Figure 8 easy2Go data-in-transit protection

Supported environments:	***Environments in-development:***
Windows Laptops 10 and 11	***Linux***
Windows Servers 2016 and up	***IOS***
Apple Macs	***Android***

7. DPM easyCloudPlus

DPM easyCloudPlus is hosted and managed SaaS offering for use by customers.

The product has the following features:

- Always available, backed-up and optional redundant manager
- Self managing encryption policies and keys
- Data resides with customer
- Data sovereignty assurance option
- Supported features are as per easyKey and easyCipher
- Option to outsource day to day encryption key and policy management to Randtronics and its global certified partners.

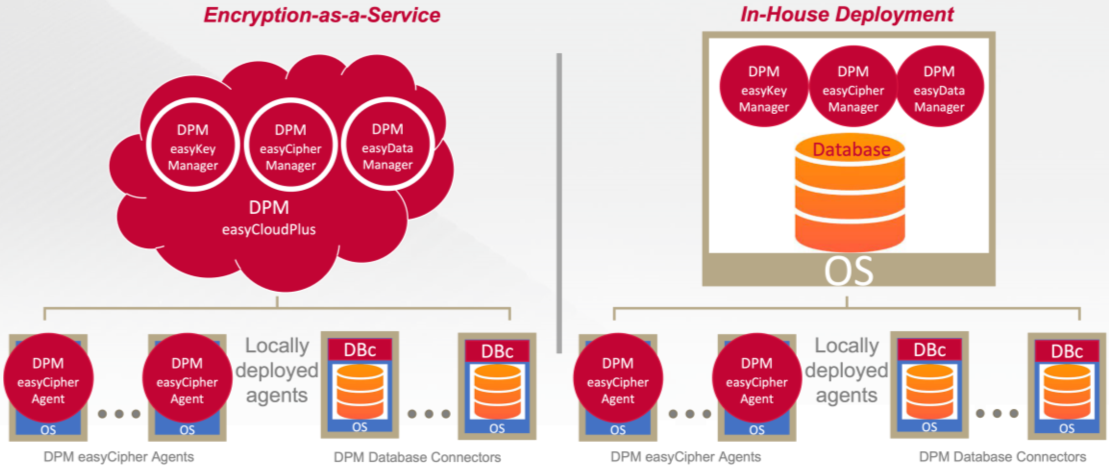


Figure 9 easyCloudPlus encryption-as-a-service available as an alternative to on-premise deployment

8. Summary

Randtronics DPM is designed to make encryption easy. Our products are easy to deploy and manage.

Our Encryption-as-as-Service DPM easyCloudPlus service offers customers the option for near-instant deployment with minimum fuss.

Our easy to download and install DPM management modules offers customers the option to implement and control every aspect of their enterprise encryption solutions within their own familiar standard operating environments.

Randtronics DPM provides customers flexibility, convenience and the freedom to change as their business grows:

- DPM management modules via in-house instance or SaaS
- Design a solution tailored to meet your specific needs for scale, redundancy and role segregation
- Flexibility to design an architecture whose data sovereignty, data-privacy enforcement, resilience, and performance parameters are aligned to your specific business needs
- Support of industry-standard server and database elements enabling you to cost-effectively deploy your design using existing in-house skills, familiar tools and existing IT support arrangements.

Copyright Information

Contact Randtronics to arrange an evaluation download - **enquiry@randtronics.com**

Randtronics

America: Milpitals, CA. Ph: +1 650 241 2671
Australia: North Ryde, NSW. Ph: +614 1822 6234

www.randtronics.com