Randtronics DPM Product Overview

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

Version 2.6
September 2025

randtronics

Randtronics Data Privacy Manager

The most capable and flexible enterprise encryption data security platform

1. Introduction

Randtronics DPM is a suite of integrated software products providing enterprise wide data privacy management and protection using key management, encryption, tokenization, masking, anonymization and access control. Enhanced with database discovery, column classification, and reporting, DPM enables organizations to identify, classify, and protect high-value data while maintaining compliance with regulatory requirements.

DPM is a comprehensive, 100% software-based data security platform designed to provide robust encryption for structured and unstructured data across on-premises and cloud environments. Trusted by large organizations, DPM streamlines the centralization and consistent management of data privacy protections across all platforms, ensuring security and compliance with ease.

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. HYOK and BYOK to Azure, Google, AWS and Alibaba (beta) as well as multi-vendor HSMs are supported

b) **Standardizes encryption protection for files, databases and folders** for all Windows and Linux systems across the organization without code changes

c) **Standardize and centrally control, data protection methods** built into 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, PCI DSS 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 masking and 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, DB2 LUW, DB2 IBMi, Oracle database and flat files
- Low-code API protection for any field-level protection (FLP) for any application-database stored anywhere
- Database discovery, column level classification, graphical insight and reporting without installing agent and code changes for production, HA, Dev, Test, marketing databases
- Shared file encryption to protect files shared across Dropbox, email, OneDrive, Google Drive, FTP. Windows, Apple Mac, iPhone/iPad iOS and Android phone/tablet
- Support cryptographic acceleration on Intel, AMD and IBM platforms for high performance
- Interoperability certification on demand for SAP, Azure and AWS.

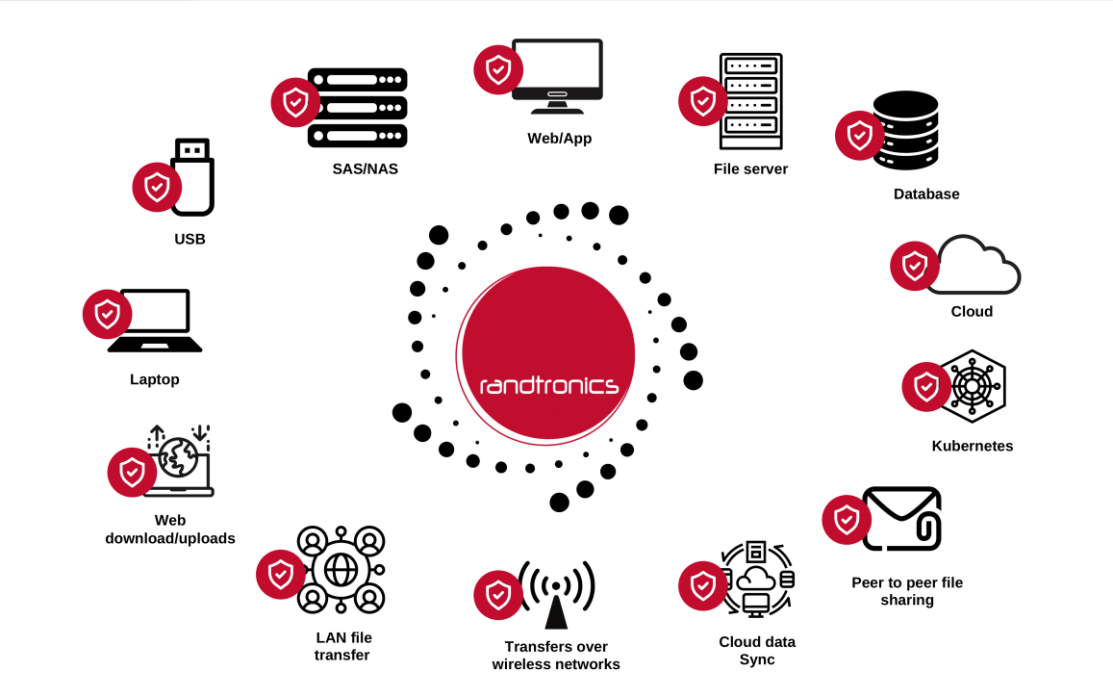


Figure 1 DPM encryption protecting structured and unstructured data on-premise and on-cloud

Randtronics DPM simplifies the needs of customers seeking to centrally manage encryption and masking protections across all platforms enterprise wide, with minimal or no code changes. Designed for seamless integration with existing infrastructure, it empowers organizations to utilize their current IT personnel or trusted service providers efficiently. For added flexibility, Randtronics offers a comprehensive encryption and key management outsourcing service, enabling customers to delegate these critical functions entirely to Randtronics for an additional fee, ensuring expert handling and peace of mind.

Randtronics DPM addresses the 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
- No-code agentless FLP for supported databases
- 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
- Database discovery, column classification and reporting
- Centralized key management and tamper-proof data-privacy protection. HYOK and BYOK AWS, Azure, GCP support
- Using industry standard algorithms such as AES-128 and 256, RSA 2048/4096, SHA-256
- 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 geo-political needs.

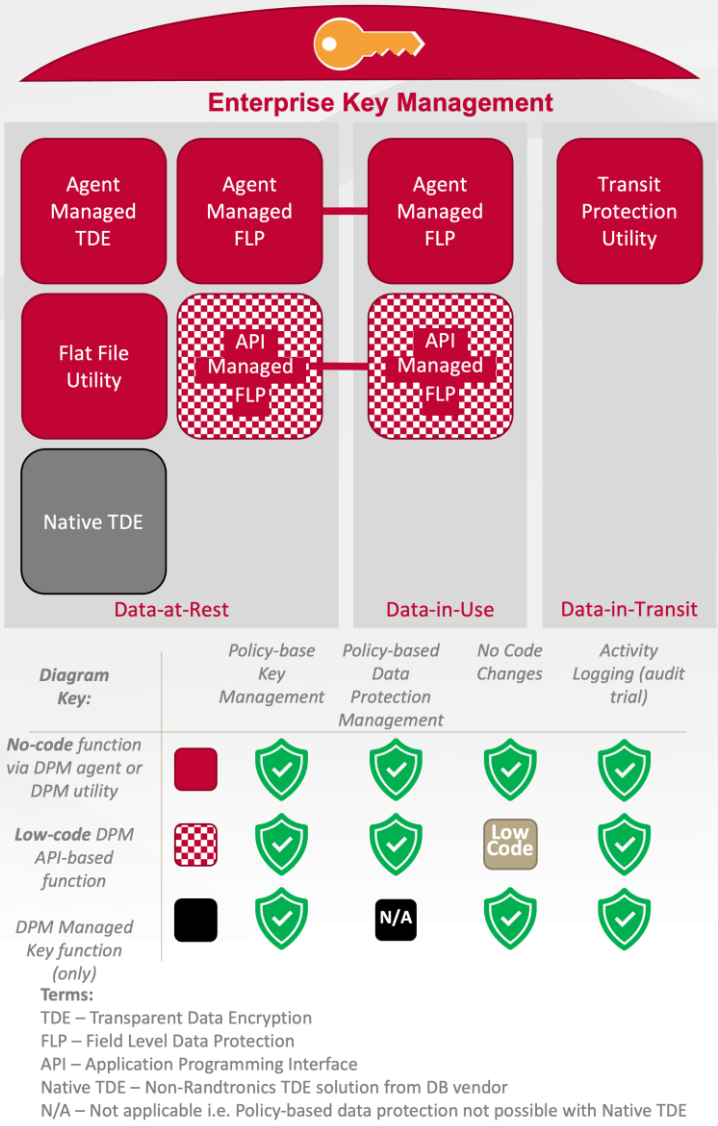


Figure 2 DPM centralized management of enterprise encryption, discovery and classification

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:

- No-code TDE with automated key management or with separation of duties for key management
- Standalone enterprise key management
- FLP with key management
- Database discovery, database column classification and reporting

- Point & Click protection for file sharing via insecure medium & media (with or without centralized key management)
- All of the above: no-code TDE, FLP, database discovery, column level classification and centralized key management.

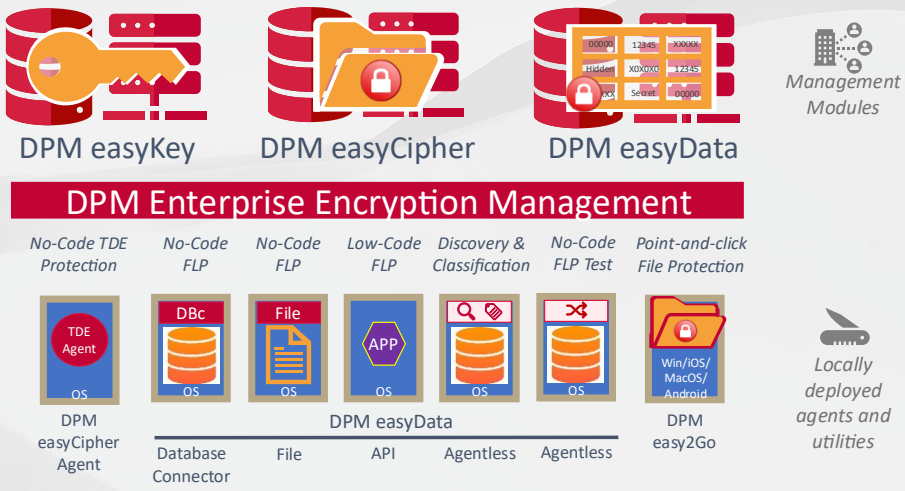


Figure 3 DPM product suite

The DPM Product Suite comprises:

- **Management modules** – centrally deployed components that manage key and encryption activities with separation of duties and full audit for all management operations to meet various security standards and compliance regulations such as PCI DSS, GDPR, HIPAA and others. All managers support high availability architecture using standard OS/DB/mirroring/load balancing tools for active-passive or active-active setup
- **Agents and Utilities** – deployed on Linux or Windows environments
- **Standalone software** – easy2Go is a standalone file encryption solution for Windows, Apple Mac, Apple iPhone/iPad, Android phones/tablets (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, masks and anonymizes data using a web service interface for any web, app and database
- **DPM easyData Database Connectors** – agent deployed on MS-SQL Server, IBM DB2 or Oracle Database environments for de-identification of live databases
- **DPM easyData Agentless Database** – agentless de-identification for MS-SQL Server, IBM DB2, 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 for data de-identification services
- **DPM easyData Discovery Agentless** – agentless and no-code database discovery, database column classification and reporting services for Oracle, MS SQL Server, MySQL, Maria, IBM DB2 (LUW & IBMi) and Postgres databases
- **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. Supports Windows, Apple Mac, Apple iPhone/iPad & Android phone and Tablets
- **DPM easy2Go CLI** – command line interface for application integration for end to end encryption of any files shared across an insecure medium such as FTP, email, public cloud and other networks.
- **DPM easy2Go Reader** – utility that enables decryption of DPM easy2Go encrypted files without requiring a license purchase
- **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 DPM modules and a wide range of software application
- For customers seeking the highest levels of assurance, such as FIPS140-3 Level 3/4 Common Criteria EAL4+, DPM easyKey offers optional integration with a mixed-vendor fleet of HSM's from USA, Germany, France and Switzerland. This ensures that encryption keys used across the organization are securely linked to a central root of trust, providing robust and reliable protection
- HYOK and BYOK to Azure, Google, AWS and Alibaba (beta) are supported.

- The software has a web browser-based interface for administrators to maintain the encryption keys. It provides role-based access control and ensures separation of duties for key management operations so no database administrator or system administrator has full control of the protected data
- Provides KMIP interface and RESTful API for client applications to use the encryption keys. All connections are protected by TLS security
- Provides full lifecycle key management for AES (128, 192, 256); RSA (2048, 3072, 4096), ECDSA (256, 384, 512), PQC ML-KEM (512, 768, 1024) keys; with support for rotation, revocation, and destruction, tracking previous and current versions and actions

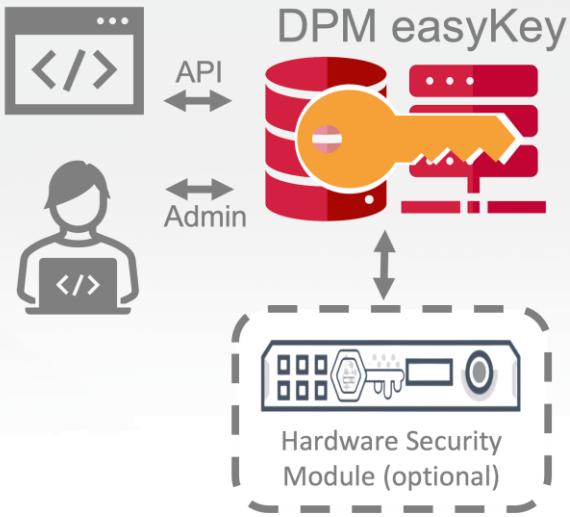


Figure 4 DPM easyKey API & Web browser Admin

- 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 with architecture flexibility to meet data sovereignty needs. DPM easyKey provides the option of auto-generating keys in software or sourcing key from multi-vendor HSM products. In this latter case the HSM becomes the source of Master Key, System Keys, Key Encryption Keys and Data Encryption Keys.
- Full auditing of key management operations and key history

Manager supported backend databases:

- *Microsoft SQL Server 2016 SP1 and up*
- *MySQL 8*
- *MariaDB 10*

Manager supported OS:

- *Windows Server 2016 and up*
- *RedHat, CentOS, Oracle Linux, Ubuntu*

Supported environments:

- *Any physical or virtualized environment (HyperV, VMWare, cloud IAAS)*
- *Multi-vendor cloud: Azure, AWS, GCP, Oracle cloud and other*

Supported third-party key management:

- *Multi-vendor HSMs (Utimaco, Entrust, Thales, Fortanix, Securosys, Futurex and Engage)*
- *HYOK and BYOK for clouds Microsoft Azure, AWS, GCP and Alibaba (beta)*
- *DPM easyKey integrates to existing and new HSMs supporting PKCS11, KMIP, JCE and REST*
- *KMIP supported enterprise key manager*

Supported client interfaces:

- *Transparent data encryption using easyCipher agents*
- *APIs using RESTful and KMIP*
- *Field level protection using easyData*

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:

- 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
- High performance transparent encryption with negligible performance overhead for database transactions
- Utilizing hardware cryptographic acceleration to achieve high performance for encryption/decryption operations on Intel and AMD platforms
- Allows transparent data encryption of multi-vendor database data files such as Oracle, MS SQL Server, DB2, MySQL, Maria, Postgres, SAP Hana, DataStax, Couchbase
- Protection of database native TDE keys for databases Oracle, MS SQL Server, DB2, SAP Hana, MySQL, Postgres, Maria and others without any code changes or writing scripts
- 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 with executable hash verification access control to sensitive files
- Integrates with DPM easyKey, enabling centralized key management
- Full auditing of access to protected folders and files
- Initial data transformation (CLI, GUI, Multi-threading) with adjustable completion time
- Rotation of key encrypting key is performed without taking applications and databases offline
- Supports authentication and user synchronization with Microsoft Active Directory and LDAP

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.

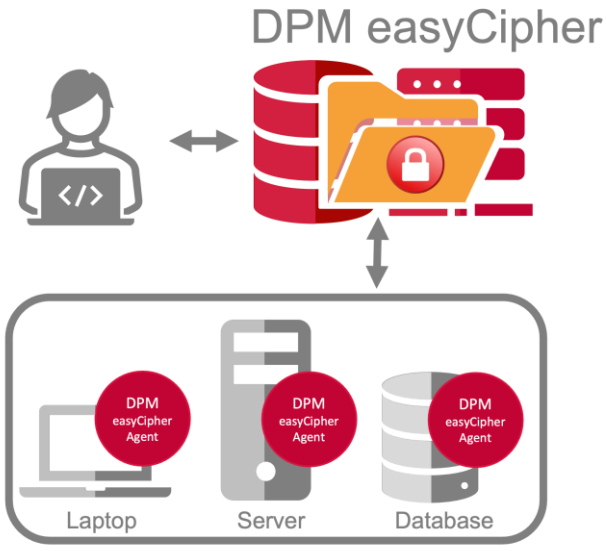


Figure 5 easyCipher Manager & Agent

DPM easyCipher

Manager supported backend databases:

- *Microsoft SQL Server 2017 and up*
- *MySQL 8*
- *MariaDB 10*

Manager supported OS:

- *Windows Server 2016 and up*
- *RedHat, CentOS, Oracle Linux, Ubuntu*

Supported environments:

- *Any physical or virtualized environment*
- *Multi-vendor cloud: Azure, AWS, GCP, Oracle cloud and other*

Supported clients:

- *Windows 8.1, 10, 11*
- *Windows Server 2012R2 and up*
- *RedHat, CentOS, Oracle Linux, SUSE, Ubuntu*
- *x86-64 architecture, IBM s390x*
- *File servers with NAS and SAN storages*
- *Application servers (IIS, Apache, Weblogic and other, SAP, Oracle, Dynamics CRM)*
- *Multi-vendor databases: Oracle, MS SQL Server, DB2, MySQL, MariaDB, Postgres, SAP Hana, MongoDB, NoSQL databases and other*
- *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. Database discovery, column classification, and reporting enables organizations to identify, classify, and protect high-value data easily.

- Format-preserving (FF1), BYO FPE Characters or standard encryption (AES)
- Multi-language tokenization and anonymization
- Masking, encryption and tokenization of column level data with no application code changes
- Comprehensive tokenization policies with numeric, alphanumeric, alpha, dates formats, single or multi-use tokens. Allows randomly generate tokens or use pre-defined dictionaries, preserve certain parts of original data or characters.
- Dynamic masking for tokenized data based on a policy
- Options of vaulted random tokenization of vaultless mathematically computed tokens
- Protection from DBAs, software developers, outsourced workers, cloud administrators
- High performance
- Web service API (REST and SOAP) for client applications to perform masking, tokenization/detokenization, encryption, and format-preserving encryption allowing integration with applications written in popular programming languages such as Java, C/C++, .Net, Python
- Agentless de-identification of database columns for production, HA, DR, dev, marketing and test databases
- Full auditing of access to protected data
- Discovery of databases and columns
- Classification of sensitive data
- Full auditing of access to protected data
- Supports authentication with Microsoft Active Directory and LDAP
- Provides highly scalable architecture by utilizing underlying CPU, RAM, Disk, virtualization specs to achieve desired performance

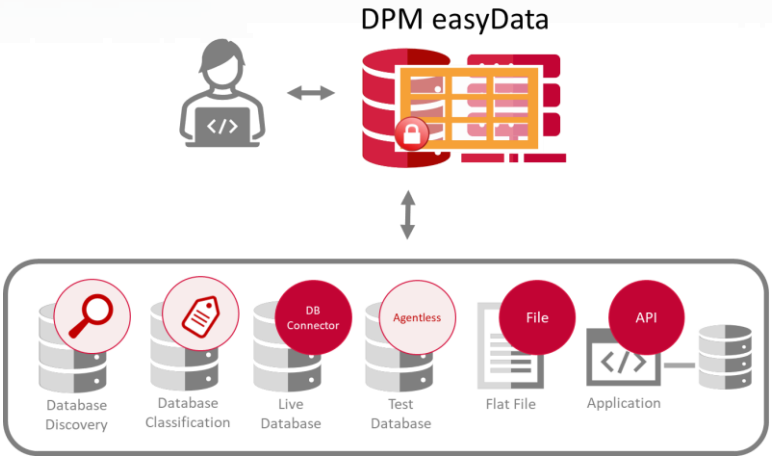


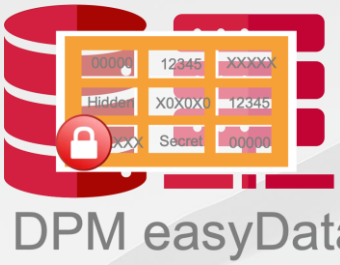
Figure 6 easyData and integration options

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 discover, classify and ensure all access and usage to confidential data is centrally managed and subject to audit tracking.

The DPM easyData product has five 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, IBM DB2 (LUW and IBMi) and Maria database columns for testers, developers and analytic purposes without installing and agent and without requiring code changes
- **DPM easyData Database Discover Agentless** – discovery, classification and reporting of database columns for MS SQL Server, Oracle, MySQL, Postgres and Maria databases used in production, HA, DR, test, dev and analytic. Node code changes or deployment of agent is required
- **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*
- *IBM DB2 (LUW 11.1 and IBMi 7.3) and up*

Supported databases for agentless Test data protection:

- *Oracle 19c, MySQL 8*
- *Microsoft SQL Server 2016 and up*
- *PostgreSQL 14 and up*
- *MariaDB 10*
- *IBM DB2 (LUW 11.1 and IBMi 7.3) and up*

Supported environments for DB Connector:

- *Windows*
- *Linux*
- *IBMi 7.3 Release and up*

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*
- *MS SQL Server 2017 and up*
- *MariaDB 10*

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, JSON, space or tab delimited or based on a position within the file
- Search and replace of sensitive data based on regular expression.

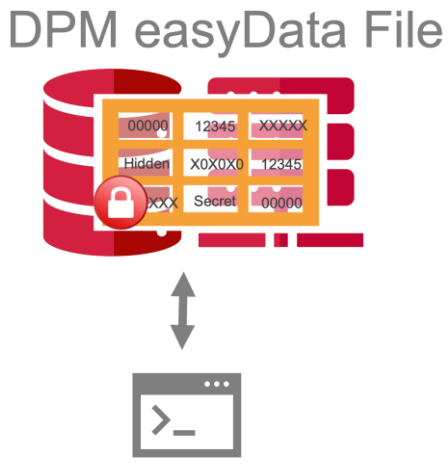


Figure 7 easyData File, flat file protection

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***	
• ***Apple MacOS 13.x and up***	
• ***Apple iPhone and iPad***	
• ***Android Phone and Tablets***	

7. DPM easyCloudPlus

DPM easyCloudPlus is hosted and managed SaaS offering for use by customers and partners wanting to build their own SaaS offering.

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.

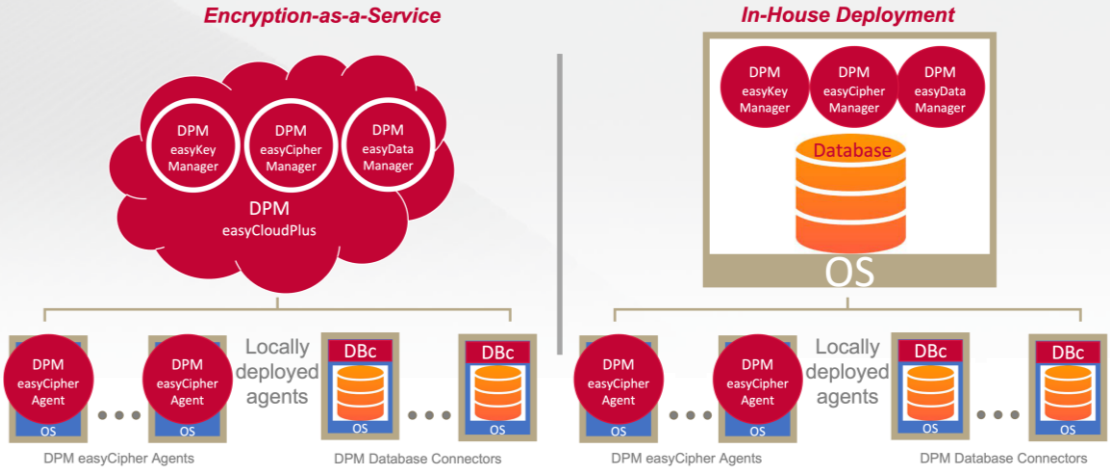


Figure 9 easyCloudPlus encryption-as-a-service available as an alternative to on-premise deployment

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.

Disclaimer on Specifications

Randtronics reserves the right to modify specifications without prior notice.

Copyright Information

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

Randtronics

America: Milpitals, CA, USA
Australia: North Ryde, NSW, Australia
Germany: Frankfurt, Germany
India: Noida, UP, India
South Korea: Mapo-gu, Seoul,South Korea
Thailand: Bangkok, Thailand

www.randtronics.com