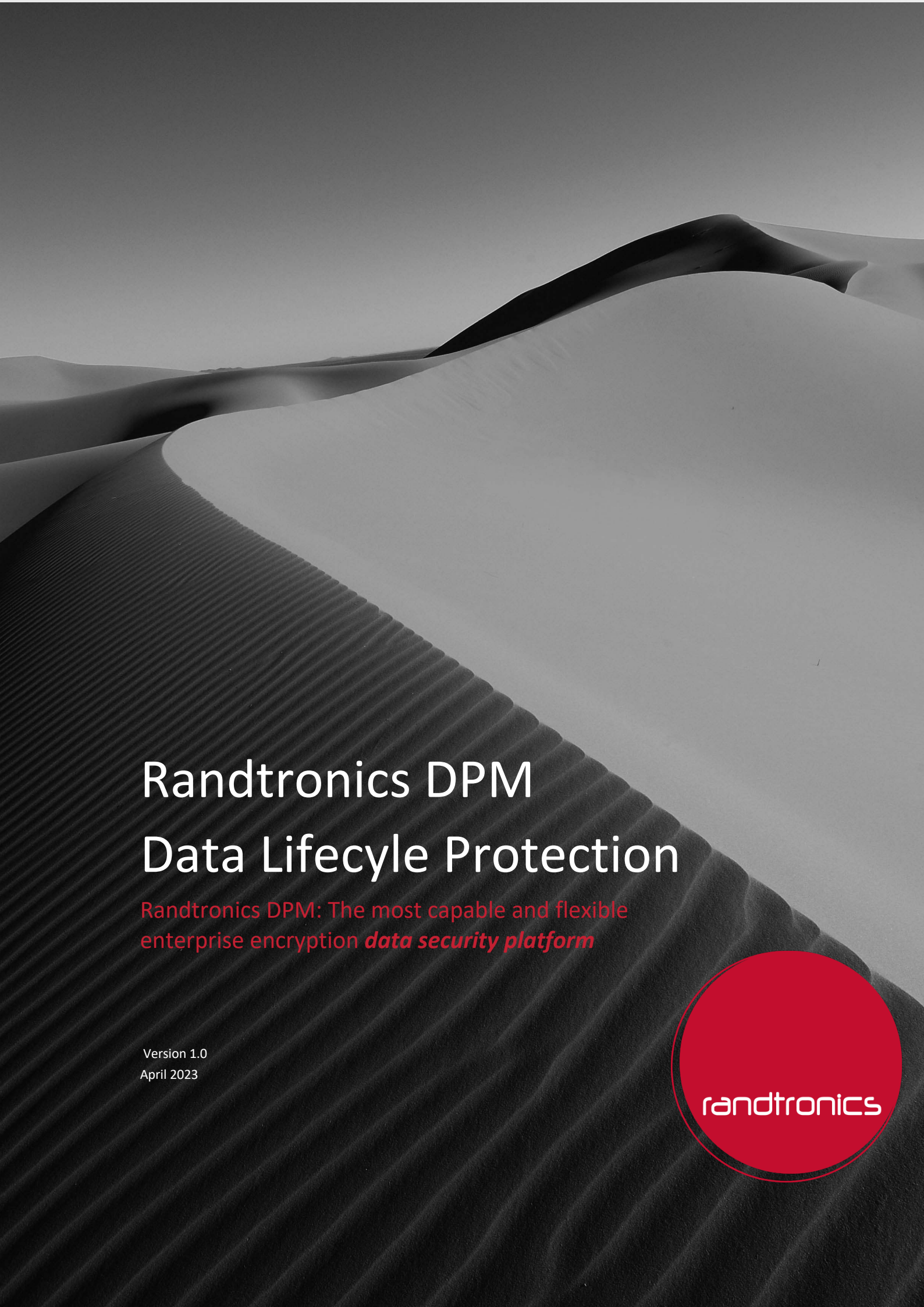


Randtronics DPM
Data Lifecyle Protection

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

Version 1.0
April 2023

randtronics

Randtronics Data Privacy Manager

Data Lifecycle Protection

1. Introduction

One of the upshots of recent high profile data breaches has been a rapid maturation in the attitude towards the treatment of personal data and other sensitive information.

The paradigm that **'data is the new oil'** to be collected, hoarded and mined is being reshaped with an awareness that 'data can be toxic', if a breach occurs and particularly embarrassing if it turns out that the data was be held past the point that organization had a legitimate need to hold it.

Organizations are facing increasing scrutiny over their lifecycle treatment of data

- What data is collected?
- How data is protected?
- How/when data is destroyed?

Figure 1 Data Lifecyle

There is no silver-bullet solution that will guarantee an organization protection against all cybersecurity threats, rather protection comes from a combination of risk reduction measures that together serve to reduce the opportunity for data breach.

Dive into the website of any cybersecurity consultancy and you will quickly come across a washing list of 'sensible easily implemented actions':

- Use strong passwords and multifactor authentication
- Keep your software and operating systems patched and up to date
- Use firewalls and other network protection methods
- Train your staff to be vigilant in opening emails and browsing
- Install anti-virus
- Backup your data

We would also add “use encryption” to this list, on the basis that there are no foolproof measures to prevent data intrusions or internal leaks but organizations that use encryption effectively have a secure backstop in place reducing the risk of data breach that is independent of other protection methods.

The purpose of this whitepaper is to highlight the role that Randtronics Data Privacy Manager products can play in protecting data throughout an organizations data lifecycle.

2. Many flavors of Encryption

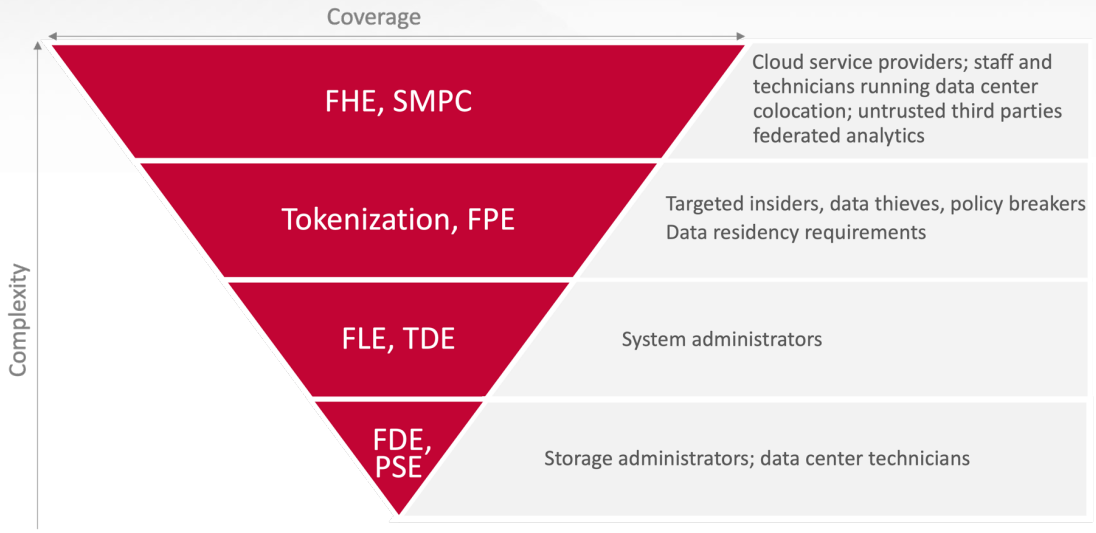
2.1 What type of encryption?

Encryption can seem initially confusing since depending on the context the word refers to general technique of transforming clear text into disguised ‘cipher text’ using a key, but the word encryption is also used as shorthand to refer to many different forms of encryption-based data protection.

To avoid confusion, this section aims to clarify some of the main forms of encryption-based data protection, and without getting to the details provide a short overview as to the different types of risk that these different technologies address.

The inverted triangle diagram below was prepared by the consultancy Gartner, illustrates four level of encryption ranging from:

- FDE/ DSE (Full disk encryption/Primary storage encryption) being the simplest to implement, through to
- FHE, SMPC (Fully Homomorphic Encryption / Secure Multiparty Computation) a significantly more complex technology to implement.



FHE (Fully Homomorphic Encryption); SMPC (Secure Multiparty Computation); FPE (Format-Preserving Encryption); FLE (Field-Level Encryption)
TDE (Transparent Data Encryption); FDE (Full Disk Encryption); PSE (Primary Storage Encryption)

Source: Gartner

In simple terms, the more complex encryption forms have been developed to counter additional threats types that can evade less complex forms of encryption,

Referencing the diagram above:

- FDE, PSE provides some protection, but once the authorised user has unlocked the volume it is open to attack to anyone who can reach the volume via network. Useful, if you are mainly worried about attack by storage administrators, data center technicians or that random stranger who found your laptop on the bus…but pretty easy for a sophisticated attack to evade.

- FLE, TDE (File-level Encryption, Transparent Data Encryption) provides the teeth to enforce Access Control, by denying the ability for unauthorized users to read files. Much harder for an attacker to evade even if they have been able to gain control of an account with system administrator rights. A persistent attacker thwarted this way may then hunt around to find an application that has been granted access.
- Tokenization, FPE (Format-preserved Encryption) provide protection against insiders using by disguising at source the data used by applications. These techniques create a significantly higher bar for potential data thieves but do not address all the vulnerabilities that may arise when data is being shared with third-party applications or being accessed for analytics.
- FHE, SMPC (Fully-homomorphic Encryption, Secure Multiparty Computation) are advanced techniques that enable to data transformed into formats that can safely used for analytic purposes without the risk of disclosing the underlying details. Use cases for these techniques include compliance with obligations to delete individuals information whilst preserving the ability to conduct group level analytics

2.2 Encryption and Access Control

Access control systems such as Active Directory and encryption systems work together to enhance security by providing complementary layers of protection.

Access control systems like Active Directory provide a mechanism for controlling access to network resources such as files, folders, and applications. Active Directory manages user authentication and authorization by verifying a user's identity and granting them access only to those resources for which they have permissions. By controlling access in this way, Active Directory helps prevent unauthorized access to sensitive data and applications.

Encryption systems, on the other hand, protect data by encoding it in a way that can only be decoded by authorized users who possess a decryption key. Encryption can be applied to data at rest (such as files stored on a hard drive or in a database) or in transit (such as data being sent over a network). Encryption helps prevent unauthorized access to sensitive data even if an attacker gains access to the system where the data is stored or transmitted.

Enterprise encryption management systems such Randtronics DPM easyCipher provides a centrally managed mechanism that links encryption protection to user permissions set by Active Directory or other access control systems.

When used together, access control systems and encryption systems provide a layered approach to security. Access control systems ensure that only authorized users can access sensitive data and applications, while encryption systems protect the data itself from unauthorized access even if an attacker gains access to the system where the data is stored or transmitted.

Active Directory in combination with Randtronics DPM easyCipher provide centralised management of user identity and control access to files and folders across the organization and use encryption to enforce the exclusivity of access to files and folders to explicitly authorized users.

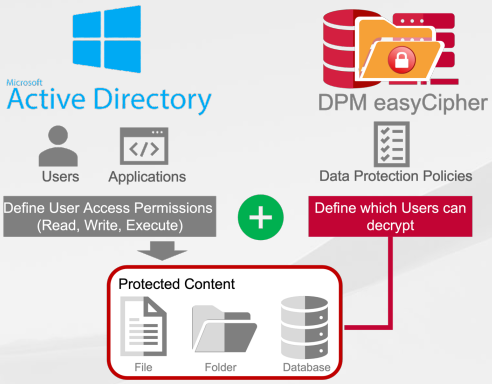


Figure 2 DPM encryption strengthens Access Control measures

One well known avenue for hackers to overcome Access control protection is to gain access to user with system administrator right. A user with system administrator rights holds the keys to the kingdom and can grant themselves access to files and folders independent of permissions set by Active Directory. In this situation, the attacker would still be defeated since the attackers' user still lacks authorization to decrypt.

2.3 Encryption Trade-offs

The reality for most organizations is that they have limited time, budget and a shortage of staff with sophisticated encryption skills and so when it comes to implementing encryption trade-offs need to be made which can be framed as defining and choosing the level of risk they are prepared to accept for a given system or data type in the context of the potential damage that would result if this data was disclosed.

3. Introducing Randtronics DPM

Randronics Data Privacy Manager (DPM) is an enterprise-encryption data security platform. The platform comprises a series of products between them address a wide range of data protection use cases.

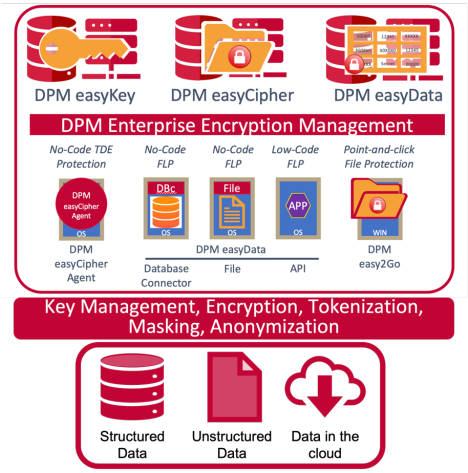


Figure 3 Randtronics DPM Product Suite

Protection Method	Coverage	No Code Change	No Workflow Change	Minimal Perf. Impact	Protection Granularity	Suitable for
TDE for DB, Servers and Laptops						Production Databases, File Servers & App Servers. Protecting laptops & desktops
Transparent Column-level data protection	SQL Server, ORACLE DATABASE					Copies of production Databases for analytics, development or backup
Flat file Redaction	ASCII Any file containing ANSI extended ASCII codes					Automatic redaction of reports or other files
API level protection	Any system platform where code modification is an option					Any application where source code modification is an option

Figure 4 Summary of DPM Components

4. Data Lifecycle Protection

Most organizations who are investigating encryption technologies are looking for immediate solutions for protecting their 'Today' current or legacy systems. As conversations evolve, customers will also become interested in understanding how an investment in Randtronics DPM may assist with future 'Tomorrow' requirements.

The overwhelming requirement that we encounter for 'Today' customers is for effective data protection that can be implemented without code change and hence for the purpose of this whitepaper we have broken out our No-code change solutions and have mapped the use case of solutions against the data lifecyle.

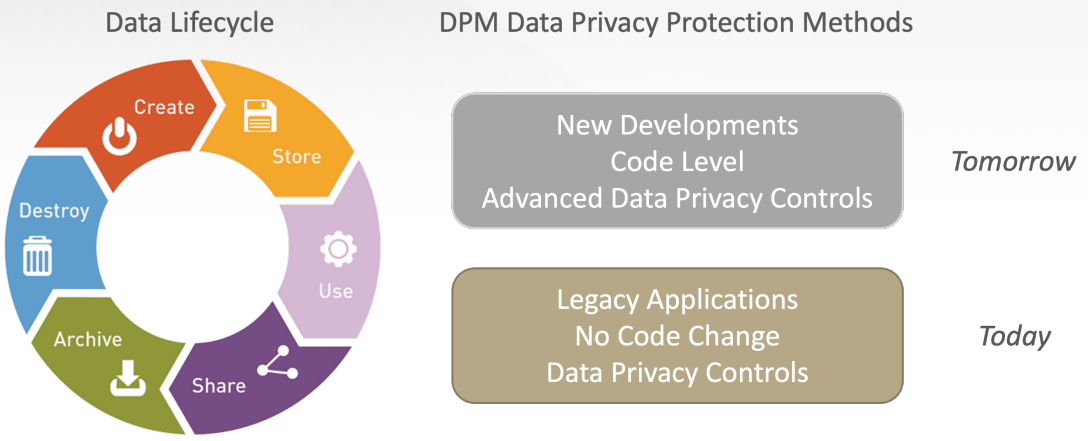


Figure 5 Randtronics DPM data lifecycle protection

4.1 No-Code Change Data Lifecycle Use Cases

Randtronics DPM products enables organizations to significantly reduce their exposure to data breach across the data lifecycle with no initial code changes required

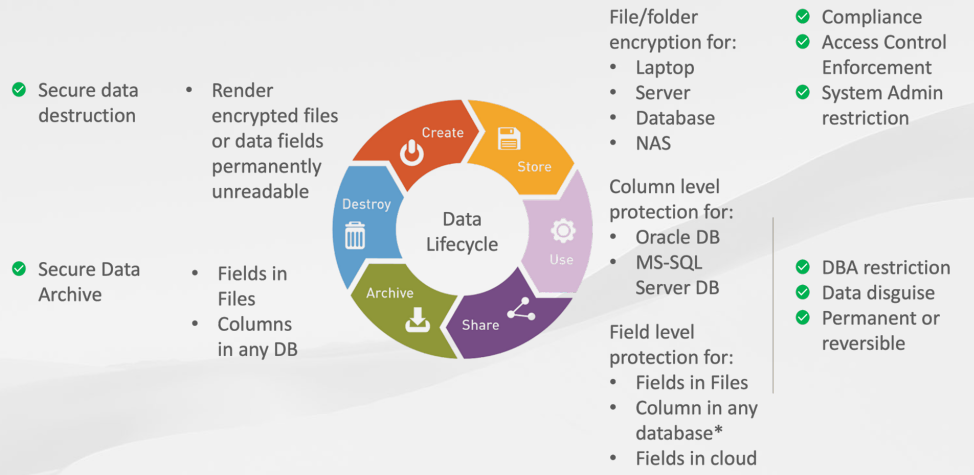
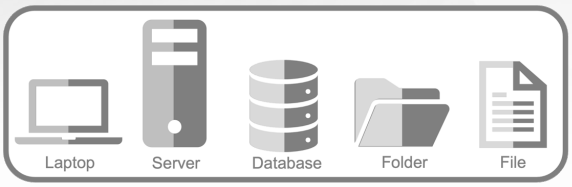


Figure 6 No-Code Change DPM Use Cases by Data Lifecycle Stage

4.1.1 Data in Store

Use Case 1 – TDE File-level protection.

Randtronics DPM easyCipher performs Transparent Data Encryption (TDE) for Windows and Linux environment.



TDE is a no-code change protection solution for protecting files, folders and databases.

Databases protected by TDE are treated a single file or folder.

DPM easyCipher it can be rapidly deployed and easily managed. It works alongside access control systems such as Microsoft Active Directory to deny access to protected content to all but explicitly authorized users (individuals or programs).

DPM easyCipher provides an excellent starting point for organizations seeking to rapidly implement encryption protection without code change to address compliance requirements.

Use Case 2 –Field-Level Protection

Randtronics provides three no-code options for protecting field-level data stored in Database columns and flat files:

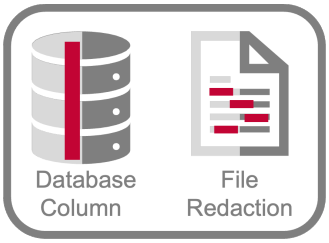


Figure 7 Field-level data protection

a) Static Data Transformation, a one-time operation to disguise data in the column. This is

permanent change and its use case for Data-in-Store relates to disguising sensitive data in duplicate databases used for training or testing i.e. applications that do not need clear-text access to the original data

b) Dynamic Data Transformation, a continuous operation to disguise column data stored in Oracle and MS SQL Server databases. In this scenario a DPM agent intercepts data to and from the database. Data and depending on the requirements the data disguise may be permanent or reversible, in either situation the data stored in the database is disguised and thus eliminating possible breach by a disgruntled database administrator.

Lastly, Randtronics also supports field-level protection of data stored in flat files. Data fields in flat files can be disguised using a permanent or reversible transformation. Even in the case of reversible disguise the means of reversing the operation are centrally controlled and stored away from the data. This use case allows sensitive data to be redacted from flat files reducing the risk of sensitive data breach if the files are stolen.

4.1.2 Data in Use

The DPM protection methods highlighted above for protected Data-in-Store also have some use cases for protecting data-in-use:

a) TDE protection prevents unauthorized users or applications accessing protected data in its storage location even when it is being used by authorized users.

b) Field-level protection used to disguise data presented to users and applications who do not require access to clear data, thus removing unnecessary risk and reducing the organizations attack surface.

4.1.3 Data Shared

Use cases for DPM protection without code change for protecting data in use include:

a) The risk of inadvertent sharing of sensitive data by applications or application program interfaces (API's) can be reduced by through the use of field-level protections and tightly limiting the number of users, applications and API's that are authorized to access clear data

b) the DPM easyCipher utility (separate product within the DPM suite) enables users to encrypt files to be shared via email or other insecure media such as public cloud folders or USB pen drives. Files can be protected with either a password or digital certificate ensuring that only the intended receiving party can read the contents.

4.1.4 Data Archive

Use cases for DPM protection without code change for protecting data in use include:

a) TDE protection of archive folders, with access narrowly limited to archive management program or data administrator

b) Redaction of sensitive fields using DPM field level protection methods to permanently disguise sensitive fields in archive materials

4.1.5 Data Destruction

The DPM platform can also be used to ensure the secure destruction of data through the encryption key lifecycle management process that includes the ability to permanently destroy keys.

4.2 Advanced Data protection for new developments

Having first instigated a program to protect current systems, the next item on the agenda is to consider have data protections are further enhanced for new developments.

DPM supports a full range of advance data protection methods that are easily called via its API, using DPM API offers organizations the opportunity to standardize their data protection methods across and centrally control these data protection methods using the same management platform and administration skills previously implemented to provide no-code change protection for legacy systems,

Figure 8 DPM advanced code-level data protection methods

Over time, encryption key technologies evolve to counter new more sophisticated threats. Organizations that use the DPM platform have the added advantage of frictionless implementation of new key technologies with minimal disruption.

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