

Data privacy for the hybrid workplace

Protect sensitive content on laptops wherever people are working

Top five reasons to choose Randtronics DPM easyCipher Laptop Encryption

- 1** **Transparently protects anywhere, anytime**

Protects content even whilst user is logged in a working via public or other insecure network. Protection works both when online and off. Data protection is transparent to authorized users and applications.
- 2** **Complements Bitlocker protection**

Bitlocker volume protection comes free with Microsoft Windows and protects contents in the case of laptop loss/theft but ceases to play a role once user is logged in, in contrast easyCipher file/folder protection is 24/7
- 3** **Centralized Policy-based Access Control**

Data security policies defined in easyCipher manager determine which users and applications can access protected files, when and from where. Authorization can be remotely reset or revoked.
- 4** **Protects data from privileged users**

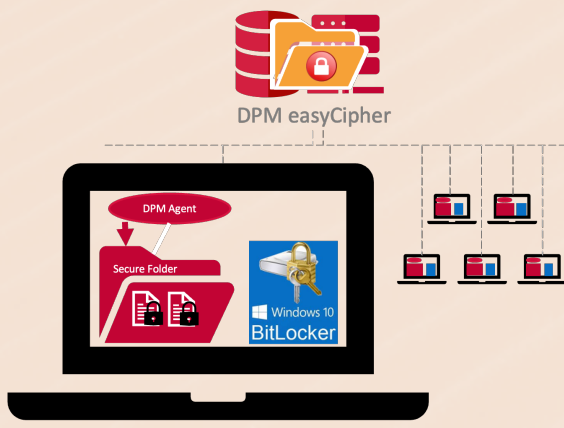
Enables data to be protected against unauthorized users even if they have elevated privileges (such as System Administrator)
- 5** **Protect and manage keys**

easyCipher encryption keys are always stored separate from data. Options available to provide policy-based, full lifecycle key management and/or root-of-trust in hardware



Tamper-proof laptop data protection and more with Randtronics

Randtronics DPM is a data security platform for managing enterprise encryption and protecting your sensitive data wherever it resides:



- ✓ **Zero-trust encryption** management system
- ✓ **Air-gap separation** between your IT organization and your sensitive data
- ✓ **Standardize encryption management**
DPM offers a standardized means of managing data protection for laptops, servers, containers and databases across all Windows & Linux environments
- ✓ **Enhance, extend or replace** native TDE

Visit our website to learn more or contact us to discuss your data protection requirements



Randtronics Data Privacy Manager

Standardize your organizations data privacy protection with Randtronics DPM

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 diagram illustrates the DPM Enterprise Encryption Management architecture. At the top, three main components are shown: DPM easyKey (represented by a key icon), DPM easyCipher (represented by a folder with a lock icon), and DPM easyData (represented by a database icon with a table of masked data). Below these is a central banner for 'DPM Enterprise Encryption Management'. Underneath the banner, five categories are listed: 'No-Code TDE Protection' (DPM easyCipher Agent on OS), 'No-Code FLP' (Database Connector), 'No-Code FLP' (File), 'Low-Code FLP' (API), and 'Point-and-click File Protection' (DPM easy2Go on WIN). Each category includes a representative icon and the name of the associated DPM component.

Encryption, Spoofing, Masking, Anonymization

The diagram shows three data types supported by DPM: 'Structured Data' (represented by a database icon), 'Unstructured Data' (represented by a document icon), and 'Data in the cloud' (represented by a cloud with a downward arrow icon).

Contact us to today to discuss your data protection requirements at www.randtronics.com

