Date: May, 2023

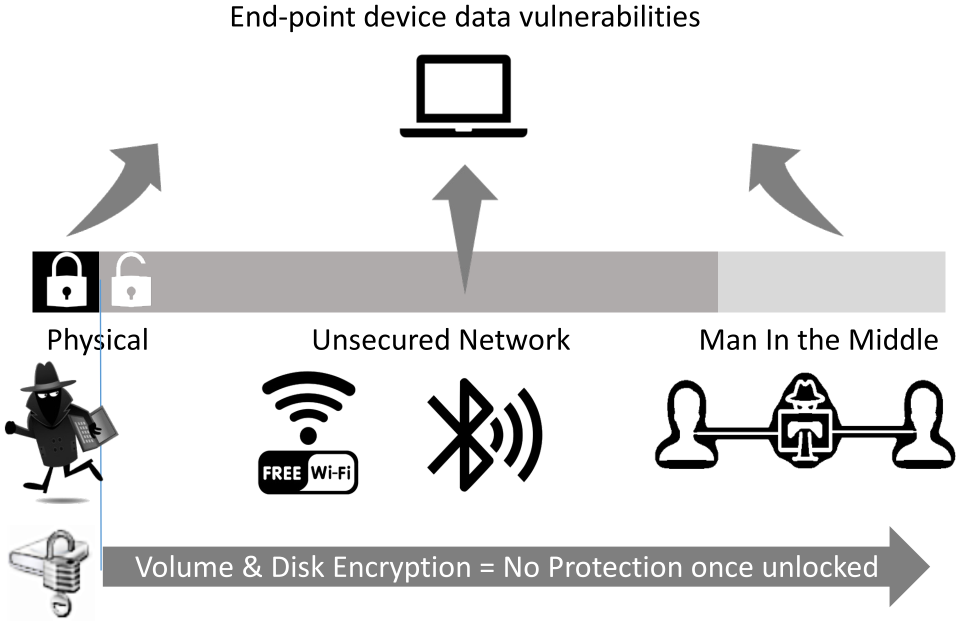
Boosting Volume and Disk Laptop Protection

Protection for your most sensitive data, everywhere

The problem – protecting data at rest

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

- Useful to protect data if machine is physically stolen, however
- Likelihood of physical theft – ***low***
- Time spent working on unsecured public WiFi or 5G Networks – ***High***


End-point device data vulnerabilities
Physical
Unsecured Network
Man In the Middle
FREE Wi-Fi
Volume & Disk Encryption = No Protection once unlocked

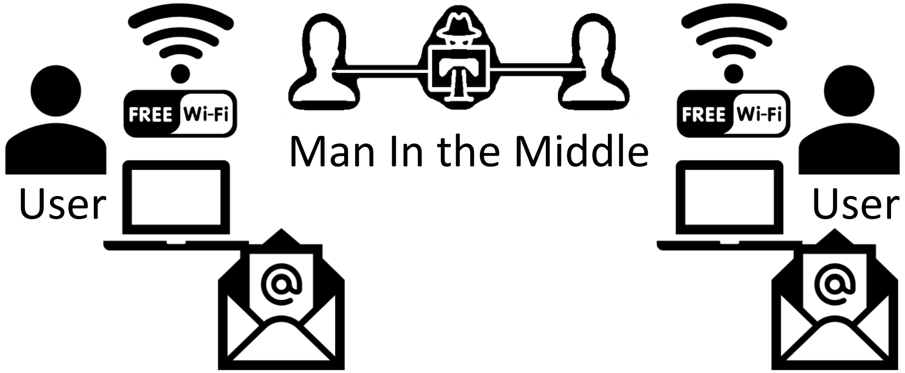
The problem – protecting shared data

Emails and file attachments face potential risks on unsecured networks:

- ‘built-in’ encryption dependent integrity of every server on the email path
- Mistyped name – wrong recipient

Dropbox / cloud folder sharing

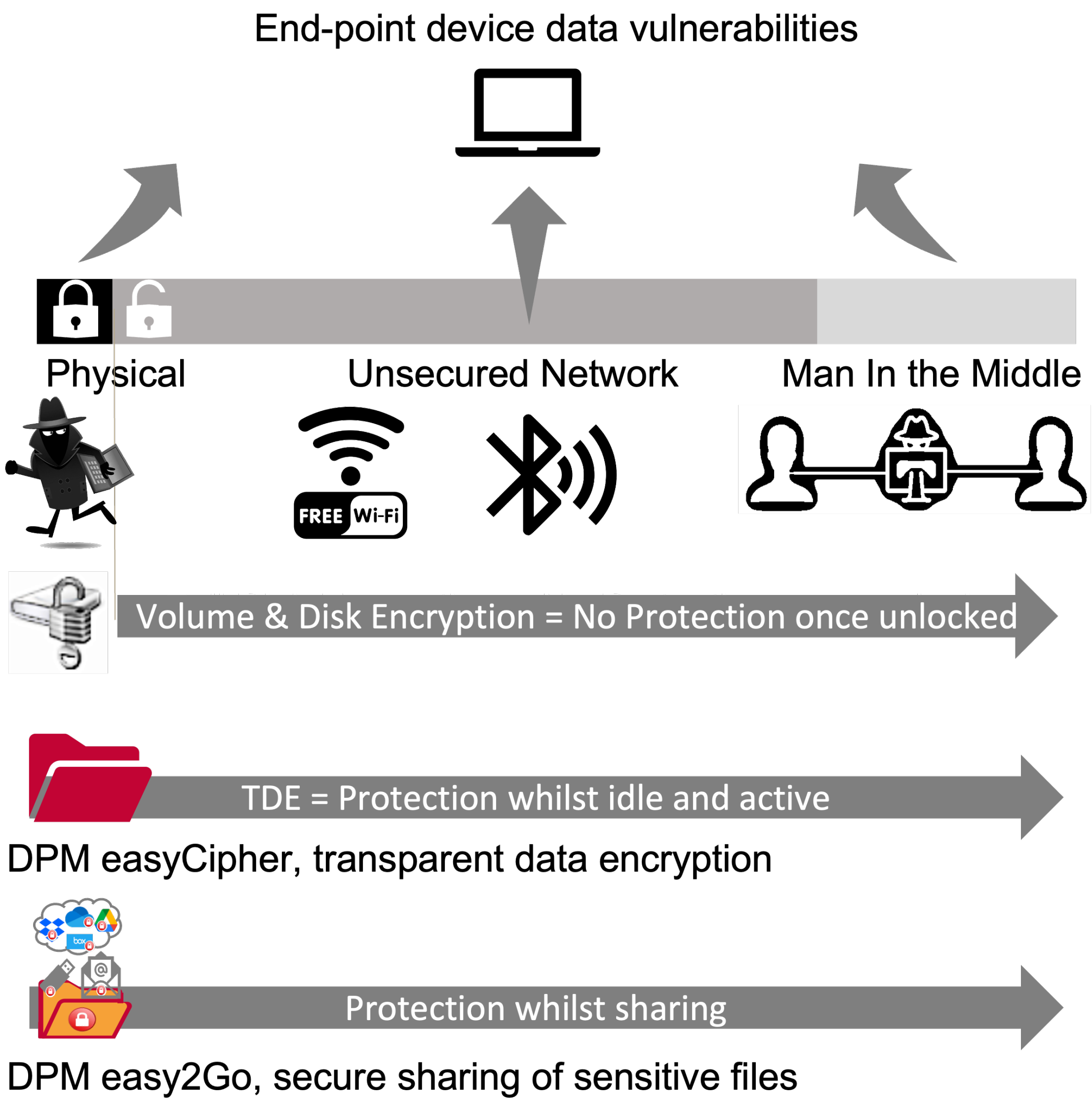
- Downloaded files – vulnerable if destination machine been compromised



The Solution

Supplement existing volume/disk encryption with DPM encryption-based protections to protect data whilst using and sharing data

- File/folder transparent data encryption (TDE)
  - Can only be read by authorized user
  - Sensitive data protected from IT Administrators
  - Access can be granted / denied by changes to centrally-managed policy
- Protect files being shared via email/Dropbox
  - Limit readability to target recipient
  - File remains encrypted after download



End-point device data vulnerabilities

Physical

Unsecured Network

Man In the Middle

Volume & Disk Encryption = No Protection once unlocked

TDE = Protection whilst idle and active

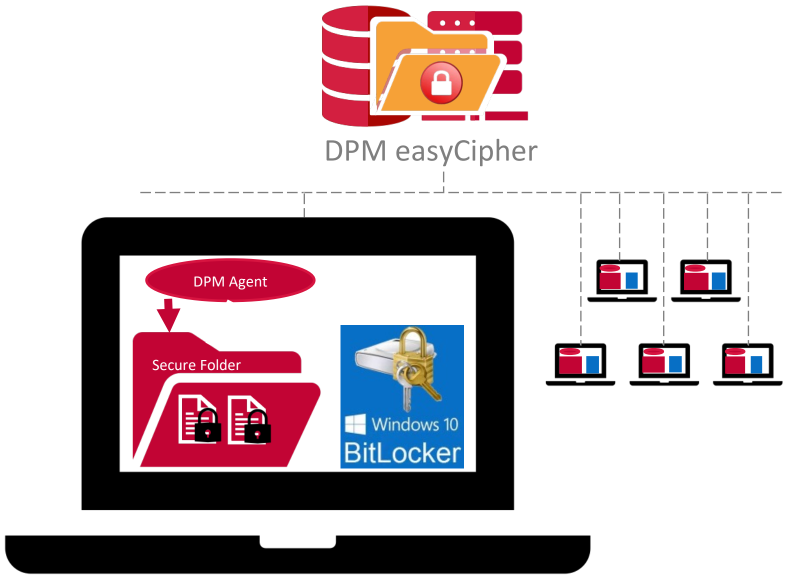
DPM easyCipher, transparent data encryption

Protection whilst sharing

DPM easy2Go, secure sharing of sensitive files

DPM easyCipher TDE for Laptop

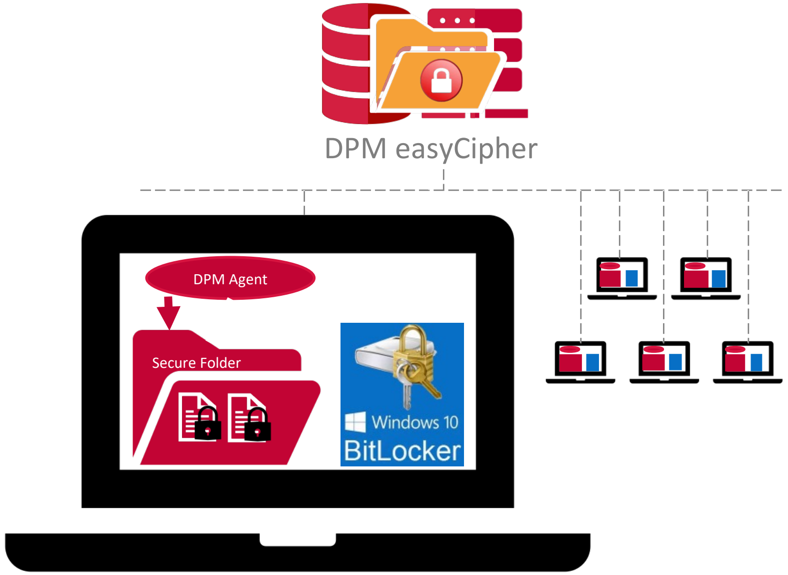
- DPM easyCipher agent installed on Laptops
- easyCipher agent provides TDE encryption protection for local files/folders
- TDE encryption protected data even whilst user is logged in
- TDE Encryption keys are stored and managed centrally
- TDE Data protection policies (who can see what) are managed centrally via DPM easyCipher manager
- Solution works when user is on, or off-line*



* encrypt/decrypt works offline, however data-protection policy changes will only update when online

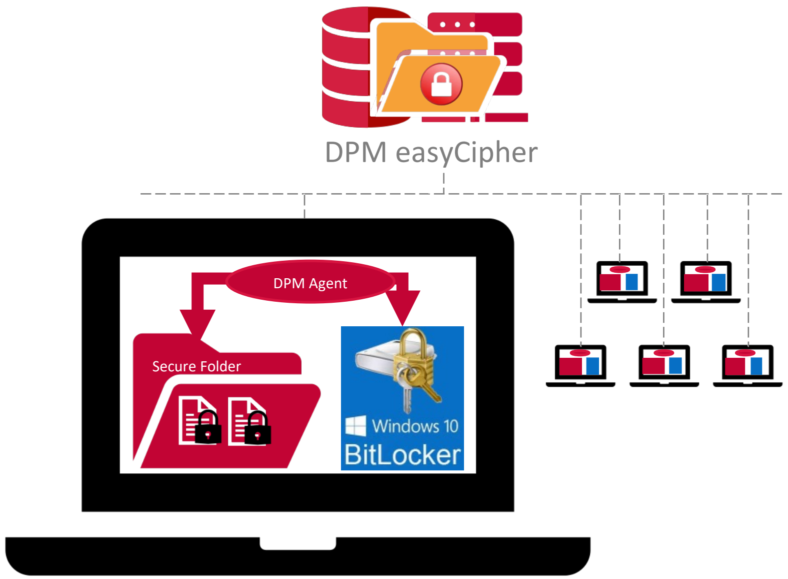
Option 1: TDE and unmanaged Bitlocker protection

- DPM easyCipher laptop agent runs in parallel to Bitlocker
- Bitlocker is not controlled by easyCipher
- Bitlocker provides protection when device is stolen up until the point the user logs on
- TDE encryption protects files/folders all the time, even when user is logged on



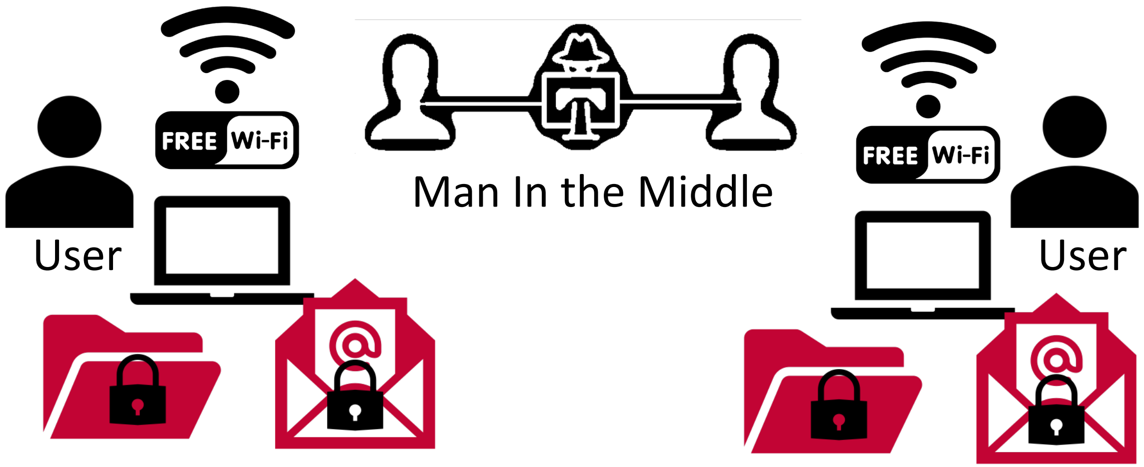
Option 2: TDE and managed Bitlocker Protection

- DPM easyCipher laptop agent manages TDE encryption and Bitlocker administration
- Centralized administration enables security admin to manage local Bitlocker instances
- Security admin able to use easyCipher Manager to remotely turn-on/off and reset Bitlocker passwords:
    - enable/disable
    - recovery password
    - change password



Use Case Example

- Our user is working on a public network that has been compromised by an attacker.
- The attacker sees all traffic from the user and has been able to gain access to the laptop.
- Our user has sensitive files on the laptop and is sending sensitive files to others via email.
- Fortunately, the sensitive files are encrypted on the laptop so the attacker can not access them despite having gained remote access to the laptop.
- The attacker is also foiled in their attempt to sell sensitive files sent via email attachments since the user has encrypted them either with a pre-agreed password or digital certificate.



Benefits

- ✓ 360º protection for mobile workers on public insecure networks
- ✓ Sensitive data protected from IT administrators
- ✓ Encryption keys and policies are managed centrally – no more risk of data loss due to user forgetting password

randtronics

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 Boosting Bitlocker Laptop Protection solution features two DPM products:

1) DPM easyCipher – TDE for databases, files, folders and laptops   and
2) DPM easy2Go – secure sharing over insecure media

Randtronics

Data Privacy Manager

Key Management, Encryption, Tokenization, Masking, Anonymization

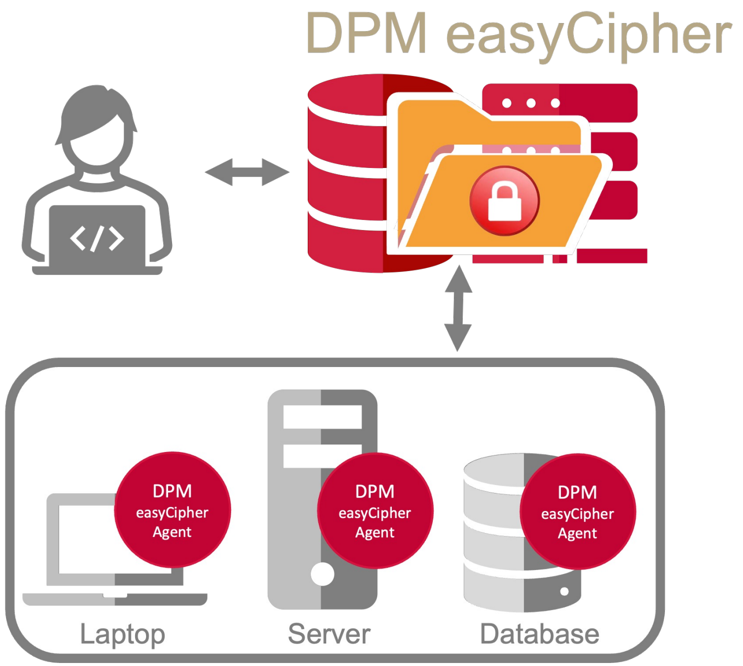
Structured Data

Unstructured Data

Data in the cloud

DPM easyCipher

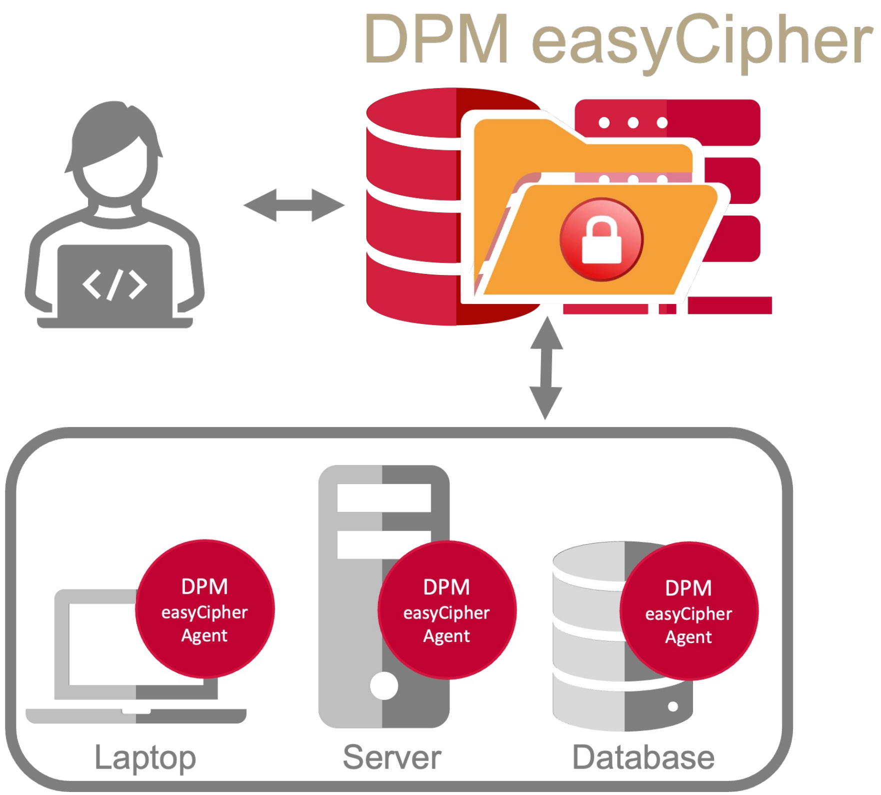
- Runs in a Windows or Linux environment on premise or in multi-vendor cloud (Windows/Linux Virtual Machine instances)
- Provides transparent data encryption of files (MS office, video, images, structured, unstructured, etc.) on laptops and servers
- Allows transparent data encryption of multi-vendor 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



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

TDE for databases, files stores and laptops

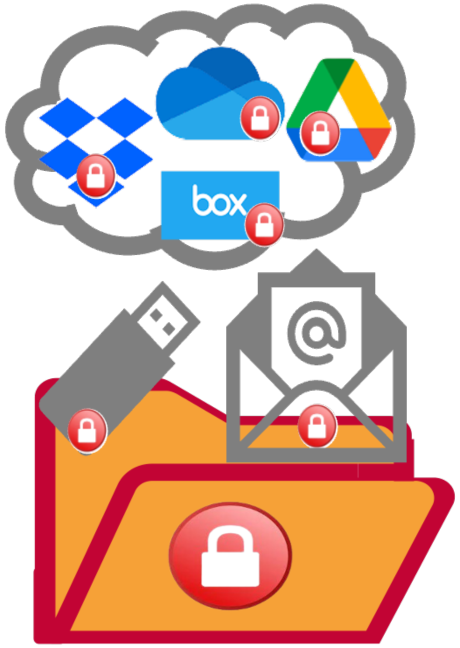
- DPM easyCipher provides transparent data encryption of files on laptops and servers
- Supports encryption on cloud file systems.
- Enables transparent data encryption of multi-vendor database
- Centralized managed of security protections – protect from unauthorized users, system administrators and 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 easy2Go

- Protect any file type or folder via password, digital certificate or centrally managed symmetric key
- Works with DPM easyKey for centralized generation and management of policy based digital certificates
- Receiving party also required to install a copy of DPM easy2Go
- Free download for DPM easy2Go reader edition



DPM easy2Go

DPM easy2Go for persistent encryption that follows the file

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