Volume/Disk-level encryption is good but insufficient means of data protection

Encryption whether applied to Disks, Volumes, Folders or Databases are components but not a complete data privacy protection strategy

A Randtronics reseller walks into a bar (*at an IT conference*)…

Randtronics sells Data Privacy protection products

You mean encryption?

More like a data-security platform managing encryption

We already have encryption

But does your encryption protect everything and provide nuanced control over who can see what?

Pretty sure we have encryption on every device

But do you have centralized and audited control over who gets to unlock data every time data is accessed?

Aren't all encryption products the same?

So glad you asked…

Our typical customers already know their encryption 101, and understand that encryption is a standard technique that can be applied to:

- Hard Disks
- Logical Volumes (many to a hard disk)
- File/ Folder
- Database (whole of database i.e. as file/folder)
- Database or File (at an individual column/field level)
- Platform (mainframe, server, cloud file store)
- Environment (everything)

Whilst our dream customer wants to encrypt everything day one, back in the real world most customers have more specific requirements and sometimes the distinction between encryption types can be confusing.

Read on to learn more about the different types of encryption and their strengths and weakness.

Full Disk Encryption (FDE)

FDE is a data privacy protection technique that encrypts the entire hard drive or storage device, protecting data at rest.

Strengths:

- **Comprehensive Protection:** FDE provides comprehensive protection of data, including the operating system, applications, and user files. This means that even if someone steals your computer or hard drive, they won't be able to access your data without the encryption key.
- **Easy to Use:** FDE is relatively easy to use, requiring minimal user interaction once it's set up. In most cases, users only need to enter a password or passphrase to unlock the drive.
- **Transparent:** FDE is transparent to the user, meaning that it does not interfere with normal computer use. Once the drive is unlocked, the user can access their data and use their computer as they normally would.
- **Protection Against Malware:** FDE can protect against malware attacks by preventing unauthorized modifications to the operating system or boot sector.

Weaknesses:

- **Performance Impact:** FDE can impact system performance, as the encryption and decryption of data require additional computing resources. While modern computers have become faster, FDE can still slow down older or less powerful computers.
- **Single Point of Failure:** FDE relies on a single encryption key, which can be a point of failure. If an attacker gains access to the key, they can decrypt the entire hard drive. This is why it's essential to choose a strong password and keep it secure.
- **Data Recovery Difficulties:** If the encryption key is lost or forgotten, there is no way to recover the data. This means that

backups are essential for preventing data loss in the event of a lost key.

- **Limited Protection:** FDE only protects against data theft when the computer is turned off or the hard drive is removed. If the computer is turned on and logged in, the data is vulnerable to theft by attackers who gain access to the system.
- **Compatibility Issues:** Some hardware configurations or operating systems may not support FDE, making it difficult or impossible to implement on those systems.

Volume Encryption (VLE)

VLE is a data privacy protection technique that encrypts everything within a logical volumes (of which their may be many on a single hard drive or storage device), protecting data at rest. VLE acts the same as FDE if the drive only contains a single volume.

Strengths:

- **Comprehensive Protection:** VLE provides comprehensive protection of data, that may include some or all of the operating system, applications, and user files. This means that even if someone steals your computer or hard drive, they won't be able to access your data within your protected volume without the encryption key.
- **Easy to Use:** VLE is relatively easy to use, requiring minimal user interaction once it's set up. VLE support come built-it to most modern operating systems. In most cases, users only need to enter a password or passphrase to unlock the drive.
- **Transparent:** VLE is transparent to the user, meaning that it does not interfere with normal computer use. Once the volume is unlocked, the user can access their data and use their computer as they normally would.
- **Protection Against Malware:** VLE can protect against malware attacks by preventing unauthorized modifications to the operating system or boot sector.
- **Performance Impact:** VLE operating as striped and RAID-5 volumes have a lower performance impact than FDE.
- **Scope:** VLE allows multiple users to share a hard drive and still only see the files within their volume.

Weaknesses:

- **Performance Impact:** VLE can impact system performance, as the encryption and decryption of data require additional computing resources. While modern computers have become faster, FDE can still slow down older or less powerful computers.
- **Single Point of Failure:** VLE relies on a single encryption key, which can be a point of failure. If an attacker gains access to the key, they can decrypt the entire volume.
- **Data Recovery Difficulties:** If the encryption key is lost or forgotten, there is no way to recover the data. This means that backups are essential for preventing data loss in the event of a lost key.
- **Limited Protection:** VLE only protects against data theft when the computer is turned off, the volume is unmounted, the user logs off or the hard drive is removed. If the computer is turned on and the user logged in, the data is vulnerable to theft by attackers who gain access to the system.
- **Compatibility Issues:** Some hardware configurations or operating systems may not support VLE, making it difficult or impossible to implement on those systems.

What role can FDE play as part of your organizations Data Privacy protection strategy?

FDE alone offers only limited data privacy protection, but it has a role to play as part of a broader Data Privacy protection strategy.

- Useful for protecting data stored on devices that can be easily stolen or lost such a laptops.
- Straightforward to implement and a sensible starting point for building a multi-layered data privacy protection – contributes to your defence-in-depth strategy
- Contributes to GDPR / PDPL/ other international personal data protection compliance obligations. Use of FDE is recommended.
- Organizations using an enterprise key management system such as DPM easyKey can compensate for the issues of Single Point of Failure and Data Recovery Difficulties.

Why FDE is only offers partial protection.

As soon as a computing device protected with FDE is powered up and a password has been entered, all encryption protection falls away.
Data is open to all and any user or application that can reach the computing device physically or via a network.

What extra protection does DPM easyCipher provide over FDE.

Randtronics DPM easyCipher provides an extended form of Transparent Data Encryption (TDE) that prevents unauthorized users or applications from decrypting data contents stored on servers and devices.

DPM easyCipher is a centrally managed data security platform, it provides:

- a standardized means for an organization to encrypt all databases (regardless of vender, edition or version), database servers, file stores, application servers and laptops
- centralized policy-based fine-grained access control to sensitive data to whitelisted users and applications
- role separation for data privacy control, in accordance with best practice guidelines.

In summary, the use of FDE is recommended by GDPR/PDPL and other personal data protection frameworks however it offers only partial protection its use in isolation still leaves and organization vulnerable to data breach and falling short of the broader best practice obligations imposed by global personal data privacy laws.

Visit our website today or talk to your local Randtronics reseller to learn how Randtronics DPM can help you control, simplify & strengthen data privacy – right across your organization