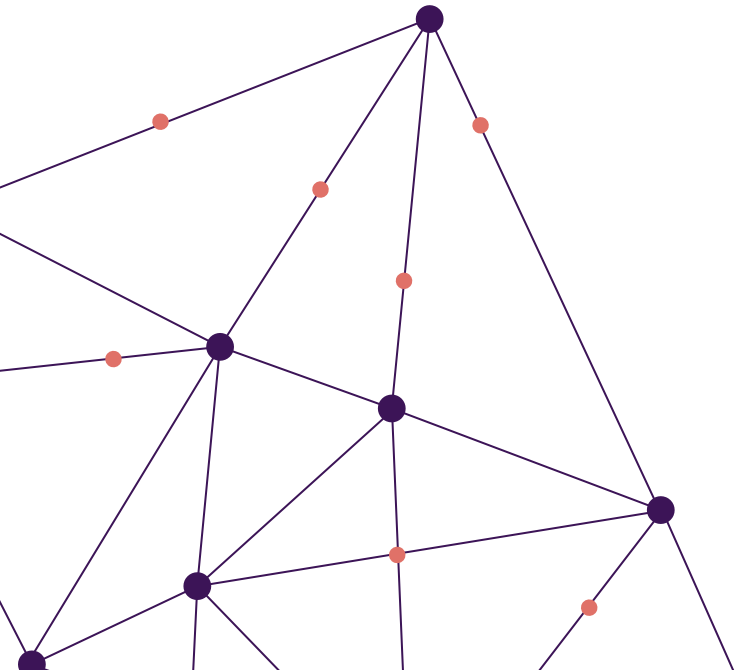
Briefing Paper

Disk Encryption Buyers Guide

Why not all solutions are the same and how to choose the one that's right for you

#becrypt.com



Commercial Sector

Introduction

We have written this guide to help you understand the key factors to consider when purchasing a Full Disk Encryption (FDE) solution.

Although on the face of it, one FDE product may seem much the same as another, there are actually some very significant differences in the features and functionality offered by different products.

The suitability of a particular FDE product depends on a range of factors, including the nature of your organization, your existing IT environment and the value you place on data security.

This guide is intended to help you frame the key questions you should be asking before purchasing FDE, identify some of the trade-offs involved in any decision and, ultimately, make the right decision for your organization.

This page at-a-glance:

- Not all FDE products are the same.
- How to choose the right one.
- How FDE works.

What is Full Disk Encryption?

Full Disk Encryption (FDE) works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" that conversion. Even if the hard drive is removed and inserted into another machine, the data remains inaccessible without a proper authentication key.

FDE is commonly used to protect the data on laptops and other portable computing devices that can be physically lost or stolen. It is also used to protect servers or storage devices holding sensitive data.

FDE provides a greater level of security than File Encryption, which – as the name suggests – encrypts data at the individual file level. Although file encryption products offer greater granularity, they are inherently less secure and require active, ongoing management by the user to ensure secure data is protected.

This page at-a-glance:

- Big variations in degree of disruption.
- Some products lack central deployment.
- Some require user configuration.
- Some depend on in-depth expertise.

What to consider when buying FDE

Ease of implementation

When faced with the question of which FDE product is right for you, a good place to start is to think about how much disruption and risk you're prepared to tolerate when deploying the software. Different products vary considerably in the degree to which they can be implemented easily.

Some free and open-source products lack the ability to be deployed remotely by a central administrator, so their implementation requires physical access to the device. This creates both significant admin overhead and disruption for end-users.

Also, some products are designed for local deployment rather than across an enterprise network. This can mean that you become dependent on your end-users to implement and configure the software. Such a situation creates significant additional risk as end-users can inadvertently or intentionally modify the configuration, thereby weakening protection.

In addition, you should think about the resources you have available to manage the implementation. Some products require in-depth security expertise to configure correctly, while others feature intuitive interfaces and are designed to be simple for IT administrators to deploy.

Key questions to consider:

- Do you want your end-users to have to surrender their devices to your IT staff for them to install FDE?
- Do you need the ability to remotely deploy to home/remote workers?
- Do you want to be dependent on having specialist security experts to correctly configure and deploy the solution?
- Do you want to be dependent on end-user action to ensure your FDE is implemented and configured correctly?

This page at-a-glance:

- Multi-factor authentication matters.
- The limitations of OS-integrated products.
- The value of merging multiple domains.
- Password update issues.
- Multiple users of a single device capability.
- Brute force attacks.

Best practice authentication

Any good FDE solution will feature a robust and flexible authentication capability.

Best practice is to have multi-factor authentication, meaning that more than one method of authentication is required to verify the user's identity. So you should look for an FDE solution that supports a variety of authentication methods.

Some FDE products are integrated with the Operating System. But be aware that this means you're reliant on a single layer of authentication. You need to decide whether you are going to follow best practice and have the security of an additional layer of protection.

You also need to consider how your FDE solution integrates with any existing authentication services that you use (such as Active Directory). If you have a relatively complex environment with multiple Active Directory domains, you'll want to ensure that your chosen FDE product can easily merge multiple domains.

Forced periodic password updates are also widely considered best practice, with many companies now enforcing this as part of their security policies. So take note that some products allow users to keep passwords indefinitely, which increases the risk that those passwords will be compromised.

Another important consideration is whether you ever need to support multiple users on a single device (for example, if a laptop is shared between several users). Some free products only allow one password per device, which needs to be shared between all users as well as admin staff.

And finally, pay attention to how your FDE solution handles a 'brute force attack' – such as repeated attempts to guess the password – in the event of the device being lost or stolen. Some products don't offer protection against brute force attacks. And some that do actually delete data after a set number of attempts, which leaves you open to the possibility of the malicious destruction of data.

Key questions to consider:

- How important is data security to you? Do you need best practice or would you tolerate increased risk to save money?
- Are you happy to rely on an FDE solution built into the OS or do you need an additional level of security that follows best practice?
- Do you need to support multiple users on a single device?
- Do you have existing authentication methods in use that you need your FDE to integrate with?

This page at-a-glance:

- Cost of ongoing management.
- Central administrator control.
- Threats to employee productivity.
- Simplifying administration.
- New threat identification and protection.

Efficient ongoing management

One of the main areas where different encryption products vary is in their management functionality.

The main cost of encryption to a organization is not the software, but the ongoing administration. So you should ensure that your chosen solution supports efficient management, as well as giving you the control you need.

To ensure that you can effectively control your environment without creating a massive cost overhead, it is essential to have FDE that features usable and robust management features and central administrator control.

For example, not all FDE products provide good credential management functionality (such as robust, user-driven password recovery and easy account deletion). This can create a real admin headache in a large organization, damaging employee productivity as well as introducing additional risk. Just imagine, without an easy way to centrally delete accounts, you risk ex-employees continuing to have access to your sensitive data.

It's also important to decide whether you want to simplify administration by having the ability to manage multiple devices and platforms from a single console. The tools available from OS or device vendors will often be lacking in this respect.

And you should look at how good the FDE vendor's solutions are for actively monitoring for new vulnerabilities and automatically applying patches. Any delay in identifying new threats and applying patches could leave you exposed.

Key questions to consider:

- Do you want to be able to centrally apply security policies and lock down configurations?
- Do you need the ability to manage encryption on multiple devices and platforms from a single console?
- Will you need the ability to add and remove devices and users centrally?

This page at-a-glance:

- Devices, platforms and applications considerations.
- Standby mode protection.
- Software and applications conflict.
- VPN compatibility.
- New version updates.

Compatibility with your IT environment

Ensuring your FDE is compatible with your existing IT environment is another key consideration.

You need to make sure that you have a FDE solution that is compatible with the various devices, platforms and applications in use across your organization. If your users have a mix of Windows and iOS devices, for example, you need to ensure the FDE is fully compatible with both.

A common side effect of incompatibility is the failure of FDE to protect devices that are in a hibernation or standby mode. Many free products fall down in this respect. Given that many laptop and tablet users rarely shut down their devices fully, this could render your FDE solution next to useless.

You also need to watch out for potential conflicts between your FDE software and applications that access the hard drive directly – such as disk utilities and asset management programs.

Also, be aware that, if you use Virtual Private Networks for access to your corporate network, not all FDE solutions work seamlessly with VPNs – which can cause potential problems for your users.

Finally, never forget that when it comes to compatibility, nothing in technology is static. So you need to ensure that your FDE vendor has an active program to maintain compatibility as new versions of hardware devices and Operating Systems are released.

Key questions to consider:

- Do you need to support a heterogeneous environment with different devices and platforms in use (such as a mix of Windows and Mac)?
- What apps or utilities do you use within your organization that your FDE product needs to be compatible with?
- Do you use VPNs and, if so, do you want an FDE solution that works seamlessly with your VPN technology?

This page at-a-glance:

- Algorithms and key lengths.
- Third-party certification.
- Secure Encryption Key storage.
- Key recovery process.

Robust encryption standards

For effective protection against a determined attacker, you need to have an FDE product that is based on robust cryptography.

The easiest way to be sure of this is to make sure you select an FDE solution that is both based on an industry-accepted algorithm and uses a key length to industry standard. For peace of mind, the recommendation is to use an Advanced Encryption Standard (AES) algorithm, preferably with a key that is 256 bits long.

You should also ensure that any FDE product you deploy has third-party certification – such as FIPS 140-2 in the US or CPA in the UK – to demonstrate that it has been independently tested.

Also, Secure Encryption Key storage is vital to ensure the integrity of the cryptography. So, when evaluating any FDE product, make sure you find out how keys are stored. Best practice is to store keys across multiple locations, but many products store their keys in one location – traditionally, the Trusted Platform Module – which makes them vulnerable to well-documented power attacks and side load attacks if the perpetrator has the device in hand.

Finally, you need to ensure that any key recovery process (in the event of a lost password or PIN, for example) is very robust. Some FDE products have a static recovery code per device, which never changes; whereas the most robust solutions generate unique recovery codes (that cannot be used again) for each incident.

Key questions to consider:

- Do you need the assurance of industry-standard, fully-certified encryption, or are you prepared to accept a lower standard?
- Do you have data that is of high potential value, providing criminals or other malign agents with the incentive to make concerted efforts to break your encryption?

This page at-a-glance:

- Device performance issues.
- Importance of single sign-in.
- Touchscreen devices.

Minimal end-user impact

Although robust protection is vital, it's also important to ensure that your FDE solution doesn't negatively impact your end-users. The greater the impact of your FDE on end-users, the greater the likelihood that they will find ways to circumvent the technology and thereby introduce new vulnerabilities.

You should consider how your FDE impacts device performance – does it take longer to boot, does it slow the machine down in normal operation? If it does, then it will have a negative impact on user productivity and your users will be motivated to find a way to disable the technology or avoid having it deployed on their device.

Enabling single sign-in to a device is also important. The way some FDE products work requires users to authenticate themselves twice, first with the encryption product and then to login to their Windows account (on a Windows device). This not only frustrates the user, but it also increases the likelihood that they will start writing down their passwords on notes attached to the device, which completely undermines all your security. The best FDE products can link pre-boot and Windows authentication so that the user only needs to sign in once.

You should also consider whether any of your users are using touchscreen devices. Some FDE products can't be used without a keyboard. Given that the onscreen keypad on most tablets is only available after the users have authenticated themselves, this makes the device unusable with FDE installed.

The most flexible FDE products have an onscreen touch keypad at pre-boot for a wide variety of tablet devices, ensuring that users can always authenticate themselves without a separate keyboard.

Key questions to consider:

- How important is single sign-on for you?
- Are you happy for users to be inconvenienced by having to sign in twice to access their devices?
- Would you tolerate a reduction in user productivity in order to purchase a lower cost encryption solution?
- Are some of your users working with touchscreen devices?

This page at-a-glance:

- Safeguarding personal data.
- Government suppliers.
- Applicable standards compliance.
- Importance of audit trails.

Compliance and auditability

Your compliance and auditability requirements must also be considered when deciding which solution is best for you. FDE has an important role to play in keeping organizations compliant in many areas.

For example, general Data Protection legislation as well as some industry regulations – such as HIPAA in Healthcare and the Payment Card Industry Data Services Standard (PCI DSS) – place specific obligations on organizationes to safeguard personal data stored on devices.

In some instances, organizationes that want to act as suppliers to government need to be able to demonstrate compliance with relevant encryption standards – such as Federal Information Processing Standard (FIPS) 140-2 in the US and Commercial Product Assurance (CPA) in the UK.

So you should ensure that the FDE product you select is compliant with the standards applicable to the markets you operate in.

To reduce your exposure to penalties in the event of a security breach, it's important not only that you have appropriate encryption in place, but also that you can provide an audit trail showing how that encryption was deployed and managed. Bear in mind that many basic FDE products are very limited in their ability to produce auditable reporting information.

Key questions to consider:

- What regulatory standards for encryption do you need to comply with?
- How exposed are you to regulatory fines in the event of a data breach?
- How important is good reporting and audit functionality to you?

This page at-a-glance:

- Complementary solutions considerations.
- Controlling data shared via removable media.
- Stand-alone products versus broader offerings.

Eliminating data leakage

The final area to consider is what other solutions you need to implement alongside FDE to minimize the risk of sensitive data being lost or stolen. However good your FDE product is, it can only ever be a partial solution to protecting the data stored on a laptop or tablet.

More breaches probably occur from data being copied onto removable media and devices than from laptops being lost or stolen. Even if the copying is for a genuine organization reason (rather than malicious intent), it still creates increased risk.

So you should think about how you control what data is shared via removable media, and how you protect any data copied to a peripheral device.

Some FDE products operate just as stand-alone products. Others are available as part of broader offerings that incorporate solutions to defend against data leakage via peripheral devices. The advantage of the latter is that they allow you to control all of your data protection solutions via a single management console.

Key questions to consider:

- How exposed are you to data leakage via malicious copying to removable devices?
- Do users commonly share data via USB drives and other portable devices?
- Do you need the ability to control what data can be copied to removable devices?

Summary

Although the central purpose of all FDE products is the same, don't assume that all FDE products are equal.

There are significant differences between the different solutions on the market. The importance of these differences to you will depend on the profile of your users, the size of your organization, the nature of your IT environment and the value of the data you need to protect.

Manageability is probably the key difference across the various products on offer. More basic, free products are typically fine for individuals and one-off systems; but not for networked enterprise deployments where you need central management.

The key trade-offs are typically cost versus usability versus risk. You should draw up the criteria that are most important to you and chose your FDE accordingly. Hopefully, this guide will help make that process easier.

About Becrypt Data Protection Suite

With over 15 years' experience of helping governments and organizationes secure their valuable data, Becrypt has a long heritage of providing enterprise data protection solutions to the most security conscious organizations.

Innovating to provide the highest levels of product assurance, our data protection solutions allow diverse platforms to be adopted within the enterprise with confidence. Working with device manufacturers, we deliver comprehensive mobile security as a seamless user experience that supports productivity without compromising protection.

For quick, straightforward data protection across your device estate, contact:

sales.US@becrypt.com +1 877 221 7775 #becrypt.com/xxx