Full Disk Encryption

Introduction to Full Disk Encryption (FDE)

Full disk encryption (FDE) is a security safeguard that protects all data stored on a hard drive from unauthorized access using disk-level encryption. With FDE, all data is encrypted by default, taking the security decision out of the hands of the user. The most common use case for implementing FDE is to protect data loss due to lost or stolen laptops, which is often sufficient enough to avoid costly data breach notification requirements.

The purpose of this guide is to provide worthwhile strategies for implementing full disk encryption throughout your organization, and to identify common pitfalls to avoid. The following topics are covered on this page:

- Defining the Scope
- Developing Policies and Procedures
- Choosing Software, Hardware, and Configuration
- Implementation and Support
- Understanding the Limitations
- Dos and Don'ts
- Additional Resources in the Guide

Define the Scope

- Determine what your goals are for the FDE project. Are you simply trying to protect personally identifiable information and avoiding data breach notification requirements? Are you trying to protect other data?
- Are you only concerned about lost laptops and opportunistic thefts? Are you also concerned about attackers targeting your institutions data?
- Are you interested in protecting all managed laptops? Only faculty and staff laptops? Only certain employees or divisions? Only those who have access to the data you are trying to protect?
    - *Consider protecting both Windows, Macs and mobile devices.*
- Are you interested in protecting only laptops? What about desktops or servers?
    - *Consider enabling FDE on desktops or servers that house confidential data in areas where theft may be possible and more likely.*
- Are you interested in protecting only the primary device, or are you also concerned about removable media such as removable media and backup drives?

Top of page

Develop Policies and Procedures

- Create a standard of which systems to protect with FDE. Will you require that all laptops are encrypted, or only those who belong to faculty and staff? Do you have desktops or servers that are at risk of theft that should also be protected?
- Determine incident response policies and procedures for lost equipment that is protected by FDE. Consider federal, state, and local regulations applicable to your institution. Are you exempt from data breach requirements if FDE is in place? Do you need to provide some level of assurance that FDE was active on the device?
- Determine who has access to encryption recovery tokens and how that access will be audited.

Top of page

Choosing Software, Hardware, and Configuration

- Select the appropriate software for your goals, environment, and culture. Common solutions include:
    - *BitLocker – Windows Vista/7 (Enterprise Edition or Ultimate Edition only)*
        - Included with operating system at no extra cost
        - Use with Microsoft Active Directory to centrally storing encryption keys and to manage BitLocker settings via Group Policy
        - Used with Microsoft System Center Configuration Manager to validate that BitLocker is continuously enabled
    - *PGP Whole Disk Encryption – Windows, Mac OS, Linux*
        - Best if used with PGP Universal Server
    - *TrueCrypt – Windows only*
        - Note: TrueCrypt provides system encryption for for Windows, Mac OS, and Linux. However it only provide full disk encryption for Windows operating systems.
    - *FileVault2 – Mac (Lion 10.7 only)*
    - *A more complete list of solutions can be found on the following Wikipedia page: http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software#Features*
- Consider purchasing laptops that include Trusted Platform Module (TPM). TPM is an integrated security processor that handles encryption keys and other security tokens in a more secure manner, and can provide additional flexibility when determining the user login experience. TPM is available with most modern, mainstream laptops vendors, including Acer, Dell, HP, Lenovo, Sony, and Toshiba.
- Select the required login method when booting the computer. For BitLocker, options include requiring a passphrase or PIN, a USB token, the TPM module (if applicable), or a combination of the three.
    - *Consider the threats you're looking to protect against. If you're only concerned with lost laptops and thefts of opportunity, TPM only may be sufficient. This will provide a more desirable user experience as users will not be required to enter a PIN, passphrase, or USB token at boot up.*
    - *If you have a particularly high risk asset, or if you're concerned that a user or system may be specifically targeted, consider requiring a PIN, passphrase, or USB token at boot up for an additional layer of protection.*
    - *If TPM is not an option, the use of a PIN, passphrase, or USB token is required at boot up.*

- Determine if enterprise management capabilities are needed for the scope of your implementation. This can greatly ease software updates, key recovery and assurance of encryption status.

Top of page

Implementation and Support

- Carefully plan, test, and pilot your infrastructure and system before deploying a FDE solution.
- Ensure you have a system in place for key management.
- Create procedures for how to enable, recover from, and service encrypted laptops.
- Educate Help Desk and User Support staff on how to address potential FDE issues users may face.
- Integrate your deployment plan with planned service, such as laptop upgrades.
- Prevent users from disabling encryption, or look for ways to verify and prove that full disk encryption has not been disabled.

Top of page

Understand the Limitations

- FDE does not protect data within a running operating system from malware or physical access.
- FDE is only effective when coupled with other security controls, such as screensaver passwords, disabling auto-logon and strong account passwords.

Top of page

Dos and Don'ts

- Do choose a FDE technology that's as ubiquitous across your OS platform as possible.
- Do decide early on if you will be escrowing keys for FDE recovery, and if so, how it will be managed.
- Do verify the polices that will cover encryption/decryption of drives (all, some, none).
- Do use hardware encryption such as TPM to avoid USB drives that may fail, get lost, or stolen.
- Don't wait for a "holy grail" technology to appear that will solve all your FDE issues.
- Don't constantly change vendors implementations of FDE.
- Don't allow for end user decision on escrowing.
- Don't take FDE as "ad-hoc" security measure without any policy or procedures backed by IT.
- Don't allow recovery keys to be stored with the laptop/desktop.

#Top of page

Additional Resources in the Guide

- Encryption 101

Top of page
