

Planning your deployment of Full Disk Encryption (FDE)

Background

ntegra combines world class technical experience with extensive, practical business knowledge across diverse sectors to deliver a complete IT service.

With extensive experience in delivering new capabilities into business, this document has been produced to highlight some of the factors which can produce a successful deployment of Full Disk Encryption, and some of the pitfalls that should be avoided.

CheckPoint FDE

As independent consultants, ntegra are able to work with any technology provider. The details within document are taken specifically from our experience working with CheckPoint FDE on a Windows based estate.

Preparation

The amount of preparation required for deploying FDE varies from company to company, according to how complex or strict your security policies are, how varied your PC estate and user base is, and how you support your user base. From a technical perspective, it would appear that successful deployment would just involve setting your installation policy, and performing thorough testing. However,

there is more to consider..! Let's tackle some of these one by one:

Security policy severity & level of protection

Ok, although anyone considering FDE will obviously have an objective to meet in regard to security and data protection. However, CheckPoint FDE can be configured to be completely transparent to the user, or it can require full separate authentication to the usual windows logon process.

The starting position for CheckPoint is to configure with Windows Integrated Logon (WIL). Doing so still provides full hard drive protection, but pre-boot logon is bypassed and user Windows logon remains as is. However, CheckPoint have added additional protection to the Windows GINA to protect against brute force hacking, so the data is still protected unless the user can logon to Windows.

If this is insufficient protection, Pre Boot Authentication (PBA) can be enabled. This is a separate CheckPoint account logon at pre OS boot stage, which can have pretty much any password policy you require - length, mix and adjacency of characters, password history etc. *Note: If using Single Sign On (SSO) it's important that the policy should be at least as strong as your AD policy, so that any change to be synchronised to AD will meet the AD requirements and not break password synchronisation!*

CheckPoint pre-boot logon supports various authentication methods, including two-factor token authentication. This method eliminates the risks of compromising fixed passwords so can be useful if one of your

departments has particularly sensitive data our security standards to meet. This is the most secure method of authenticating users and protecting your data, but it does require users to carry a token, and will therefore undoubtedly increase your support overheads.

Administration & administrator privileges

Next we'll take a brief look at privileges with CheckPoint FDE.

For larger organisations, or ones with more stringent requirements, CheckPoint can be configured with two administration tiers. For example, your helpdesk / 1st line support group can be empowered to perform password resets and one time logon assistance to users, but not to create new user accounts, uninstall the product or decrypt a PC. This privilege can be retained by a small group of super users only, thus protecting your estate from unauthorised access by staff / ex staff.

If you are going to provide remote password and logon support, consider how you authenticate the end user to your support personnel. Ideally, this should be part of your IT support process already, ensuring only genuine users are given password resets and system access.

Third party GINA

If you are using any 3rd party GINA's to provide self serve password resets for example, these need to be configured in the CheckPoint policy to ensure the correct GINA chain is called following pre boot stage, otherwise PC's will default back to the windows GINA.

Testing

We recommend testing your CheckPoint installation package(s) before deployment on a range of PC models in use through your estate. Some of the things to look out for in testing include pre-boot USB support, password policy correctness & SSO operation and network location permissions for key file and log storage.

Anti spyware and Malware products need to be tested to ensure they don't conflict with CheckPoint.

In addition testing is also crucial for your support teams, providing them with further insight to the installation process, policy settings and recovery process.

Data storage & recovery

One thing to be mindful of is your local data storage and recovery policy. For example, do you stipulate that users are responsible for backing up their local data? If a user has a fault on their PC at present, will your IT support recover data for them? These policies do not necessarily need to change due to rolling out FDE, however, they do become more important to understand, as recovering data from encrypted systems is obviously more time consuming and complex than on non encrypted PC's.

In general, we would recommend that users are provided with secure network storage, or encrypted USB media to allow them to back up their data. Any recovery requirements can therefore be kept to a minimum.

CheckPoint does provide a number of ways to recover systems & data. For example, if there is a major OS problem, and an encrypted PC won't boot, CheckPoint can

create bootable media specific to the PC, and therefore provide access to run windows repair utilities.

In addition, it is possible to slave a hard drive onto another machine. This can be useful if Windows is beyond repair, and user data needs to be transferred off the drive.

Note: This requires enabling specific settings in CheckPoint policy.

Hardware

Look out for old (~ over 5 years), full & heavily fragmented hard drives. CheckPoint does require an amount of contiguous space to perform the encryption, and faulty drives can obviously cause problems as FDE fully exercises hard drives during the initial encryption process. Performing a scandisk and defragmenting hard drives on older PCs prior to encryption can be a good way to check & prepare these PC's for encryption. Avoid any PC's with known hard drive issues!

Deployment

CheckPoint FDE installation files include the main MSI, the installation profiles you have built and a set of supporting install folders. These can be incorporated in a package from a deployment tool such as SMS or RADIA (look out for restrictions on MSI transforms), or can be stored on a network location. CheckPoint has a number of folders defined in the installation profile – Installation, update, recovery, log etc. Permissions should be set individually on these folders, the installation, update and log folders should be read only to general users, recovery should be read/write. Note the log and recovery files are encrypted so remain secure.

It's worthwhile sending out a communication to all your users in advance of the deployment – particularly if you are using PBA without SSO as your users will need to know about the changes to their PC logon's. This will also give you a chance to provide users with more information if they require, plus a chance to request assistance in backing up their data, or an in person install.

I would also recommend scheduling the installs in increasing sized batches – starting with 10 users, moving up to 25, 50, 100, 250 etc for example. Allow sufficient time between batches to ensure any problems are captured and resolved before the deployment goes too far.

If you don't have a package deployment tool, then you can monitor the recovery folder on the network for progress. Each PC will write a recovery file here once CheckPoint has been installed, *prior* to the encryption process starting. Note, the encryption process will not start until this file has been written to ensure that recovery is not compromised.

Conclusions

Every organisation is different, and although you may think this is overkill, planning your deployment carefully ensures best practice is followed and ensures every last detail is thought through and catered for, and ultimately will save you time and money.