

Technical solution overview

CheckPoint Full Disk Encryption SME deployment

Introduction

This document is aimed at customers interested in deploying Check Point Full Disk Encryption (FDE).

ntegra have partnered with Castleforce IT Security to provide a single point of contact to purchase and deploy Check Point FDE. This document provides an overview of the solution we have developed to successfully deploy Check Point FDE into small to medium sized enterprises.

Aside from many years experience of technical deployments, ntegra have also performed and managed a number of Check Point implementations. These include small deployments to 5 users, through to European wide deployments of over 1000 users.

Using our deployment solution ensures best practices are fully exploited, providing a solid foundation to ensure your encryption and security requirements are met without business disruption.

ntegra & Castleforce

ntegra is a dynamic, growing IT consultancy and services organisation – We have developed our business by delivering high quality solutions to customers in many sectors, including Telecommunications, IT and Finance.

Our services are designed to help our clients increase the value they gain from their IT investments. Our services are built on the quality, pragmatism and experience of our consultants, who bring expertise in:

- Solutions Architecture, Analysis, Design and Development
- Business Change, Programme and Project Management
- Infrastructure Design and Implementation
- Application Testing and Assurance
- Data Migration, Implementation and Release Management
- System, Environment Support and Service Desk
- Vendor management and engagement

Castleforce IT Consultancy Ltd are IT Security and Business Continuity specialists helping businesses choose the best products that meet the diverse requirements needed to protect against the current threat landscape and which satisfy the specific requirements of compliance guidelines and regulations.

CheckPoint FDE

Check Point Software Technologies is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions.

The Full Disk Encryption solution from Check Point has proven itself in enterprises and government agencies around the world, delivering the highest level of data security by providing a strong, full-disk encryption solution for PCs and laptops as well as access control. It has the most and highest-level of certifications, works with Linux or Windows and Apple MAC, and provides centralised management of PC data security.

Our solution

We have developed a rapid deployment model, providing a risk averse & pragmatic approach, whilst ensuring costs and lead times are kept to a minimum.

Deployment of Check Point FDE needs to be carefully planned because:

- You need a smooth roll out, minimising disruption to users
- Impact on support overheads need to be kept to a minimum within the organisation
- Unplanned scenarios could preclude to at least excessive support overheads, if not actual loss of data and business disruption

Depending on complexity of the business & security policy, adopting our approach ensures this preparation can usually be completed in one day. Roll out can then be performed as aggressively as required/appropriate. One of our delivery managers will discuss your requirements, and agree whether the solution is suitable for your needs. Even if your requirements are more adhoc or complex, this solution still provides a good foundation for your project.

Day 1 Agenda – Preparation & Testing

Technical workshop

Attendees: ntegra consultant, Helpdesk manager, Desktop support team lead, Security officer

Duration: 2-4 hours depending on complexity

Review of requirements, company security policy and support capabilities to complete the CheckPoint solution design from our template, which when completed will contain all information required to build, test and deploy CheckPoint FDE, as well as record the

necessary information for your support personnel. The agenda includes a short discussion on CheckPoint FDE and high level business requirements and drivers, and then a structured walkthrough of the design template to review information such as:

- Security policy requirements (ie, two factor authentication, SSO etc)
- Administration roles & responsibilities and tiering of privileges
- Data recovery policy
- Password & 1st line support
- 2nd line support
- Package deployment method

Testing workshop

Attendees: ntegra consultant, Desktop support team lead +1 team member (inc. Packaging contact)

Duration: 4-6 hours

Develop the template installation profile for Check Point & test installation on a set of PC models/builds used in the business

- Define new installation profile settings
- Test installation
- Test removal
- Test privileges
- Test updates
- Test install package

Performance testing (optional, extra time required)

Data recovery testing (optional, extra time required)

Deployment options

We usually recommend using a hybrid deployment model of remote and in person installs.

In general, providing users are informed in advance, remote installations obviously provide the quickest deployment. However, in person installs can provide additional reassurance to VIP's and/or for persons who may require assistance with backing up data.

A drop in centre can be setup for users to have their data backed up and install completed.

Or, floor walker(s) can be sent to the required users.

A suitably secure backup volume will be required to temporarily store the backups to ensure users are comfortable and company security policy is not impacted.

Access to a package deployment model such as Hp's RADIA obviously speeds up deployment. There are restrictions on amending the Check Point MSI (transforms etc).

Pre-requisites

Prior to start of any engagement, we recommend a holding a short discussion on a checklist of pre-requisites to ensure the project starts smoothly. This also provides an opportunity to make introductions prior to start of the engagement, and discuss CheckPoint FDE features or questions you may have. The following are examples of pre-requisite items that should be discussed

- Project sponsor & security mandate to the business
- Engagement of required resources in the business
- Access to test PC's as required

- Network share for log & key storage
- Audit of company PC's / clear list of PC's to be encrypted
- Clarification of users data storage policy