

Technical solution overview

Check Point Media Encryption Deployment

Introduction

This document is aimed at customers interested in deploying Check Point Media Encryption.

ntegra have partnered with Castleforce IT Security to provide a single point of contact to purchase and deploy Check Point Media Encryption. This document provides an overview of the solution we have developed to successfully deploy the product 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.

Check Point Media Encryption

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.

Check Point Media Encryption secures sensitive corporate data and blocks incoming malware by encrypting removable media such as USB storage devices, CDs and DVDs and controlling activity (read, write and execute) on ports and devices. All device content is automatically encrypted in the background for a transparent end-user experience. Unique to Check Point, users can access encrypted media securely on unmanaged computers with no client installation.

Our solution

We have developed a pragmatic deployment model, designed to efficiently deploy the product in one day whilst preventing undue disruption to users.

Deployment of Check Point Media Encryption needs to be carefully deployed because:

- Users need to be well informed, so they can adjust their working practices for the new restrictions with external devices
- Poorly designed policy WILL generate significant level support calls and cause disruption for users.

1 – Kick off

Firstly, a kick off session will be held with representatives from your support team and security department if applicable. The following type of points need to be considered:

- Devices in use through the estate – inc, external media, 3g modems, mp3 players
- Devices to be prohibited or controlled
- Communications required to end users

2 – Installation and training

Once we have discussed the desired configuration, we will move on to install the product on a central workstation / administration PC, and run through the features of the management console.

We will then create the required computer and user groups, ready for the policy definitions.

There are then two recommended ways of proceeding – full roll out and staged lock down, or full lock down with staged roll out.

3a – Full roll out & staged lock down

This option involves setting the most basic level of policy designed not to implement any impact to end users as this stage. The product will

be rolled out to all users with full auditing enabled. We can then begin to identify the various types of devices from the auditing logs, and show you how to incorporate gradual policy changes accordingly.

This option is perhaps most suitable for ensuring no user impact, and if you have sufficient time to make repetitive reviews of the audit logs and policy settings.

3b – Full lock down with staged roll out

This option involves setting strict policies to block every device – short of any devices available on hand for testing at this point. The product is then rolled out to pilot or ‘friendly’ users and adjustments made as required until the final policy has been confirmed and the product rolled out to all users. This option is perhaps more suitable if the set of pilot users are truly representative of the user estate, and you wish to make fewer visits to policy settings.

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 Check Point media encryption 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
- Audit of authorised portable devices.
- Communication to users, regarding the impending media encryption roll out & clarification of company policy for removable media.