Vendor: Check Point

Exam Code: 156-536

Exam Name: Check Point Certified Harmony Endpoint Specialist - R81.20 (CCES)

Version: DEMO

QUESTION 1
Which option allows the Endpoint Security Management Server to modify client settings such as shutting down or restarting the client computers without installing policy?

A. Remote Operations
B. Node Management
C. Remote Help
D. Push Operations

Answer: A
Explanation:
Remote Operations enable the management server to directly execute commands (e.g., shutdown, restart) on client devices without requiring a policy installation. This is used for immediate, on-demand actions.

QUESTION 2
What information does the Endpoint Client provide end users?

A. Overview summary of all machines and their status.
B. Overview summary of the protections deployed on the machines and the status of each protection.
C. Overview summary of security breaches.
D. Overview summary of traffic logs.

Answer: B
Explanation:
The Check Point Endpoint Security Client provides end users with a comprehensive overview of the security protections deployed on their machines, including the status of each protection. This allows users to monitor and manage their security settings effectively.
https://sc1.checkpoint.com/documents/R80.40/SmartEndpoint_OLH/EN/Topics-EPSG/ClientUI.html

QUESTION 3
Name one way to install Endpoint Security clients:

A. Third-party deployment tools
B. Automatic using the server deployment rules
C. Package import
D. Manual deployment using the internet

Answer: B
Explanation:
Harmony Endpoint allows for the automatic deployment of Endpoint Security clients through server deployment rules. These rules enable the automatic download and installation of pre-configured packages on endpoint devices, streamlining the deployment process.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_EndpointWebManagement_AdminGuide/Topics-HEP/Automatic-Deployment-of-Endpoint-Clients.htm

QUESTION 4
How many Endpoint Security Client Package types exist?

A. There are two main package types. Initial Client Package and Endpoint Security Client Packages.
B. There are two packages. One for Windows and one for MacOS
C. The administrator has to download all the appropriate packages from the UserCenter.
D. There is only the initial package.

Answer: A
Explanation:
Initial Client Package (NEWDA):
This is a minimal package designed for initial software deployment. It contains no components and serves as a lightweight entry point for installing additional features later.
Endpoint Security Client Packages:
These include various specialized packages tailored to different security needs and operating systems. Examples from the search results include:
Master_FULL_E1/x64: Complete client for 32/64-bit Windows (includes Anti-Malware).
Master_FULL_NO_NP/x64: Complete client without Anti-Malware.
Master_SBA/x64: SandBlast Agent for threat prevention.
Master_ENCRYPTION/x64: Full Disk Encryption and Media Encryption.
Dynamic Package (EXE for Windows, ZIP for macOS): A self-extracting executable recommended for most deployments, containing all components.

QUESTION 5
How can an administrator tell when the MAC OS Harmony Endpoint client is successfully installed?

A. The Apple device will automatically reboot when the installation is complete. This is confirmation that the client is installed.
B. The MAC OS will generate a pop-up message to notify the administrator.
C. When the client is successfully installed, the Endpoint icon will appear in the computer's menu bar.
D. The Harmony management portal will generate a pop-up in the portal to notify the administrator.

Answer: C
Explanation:
After installing the Harmony Endpoint client on macOS, users can confirm a successful installation by locating the Endpoint icon in the menu bar. This icon indicates that the client is active and functioning properly.

QUESTION 6
Harmony Endpoint offers Endpoint Security Client packages for which operating systems?

A. Unix, WinLinux and macOS
B. Windows, macOS and Linux operating systems
C. macOS, iPadOS and Windows
D. Windows, AppleOS and Unix operating systems

Answer: B
Explanation:
Harmony Endpoint provides Endpoint Security Client packages for the following operating systems:
Windows: Supported versions include Windows 11 (Enterprise and Pro editions) and Windows 10 (various versions).

macOS: Supported versions include macOS Sequoia (15), macOS Sonoma (14), macOS Ventura (13), macOS Monterey (12), macOS Big Sur (11), and macOS Catalina (10.15).
Linux: Supported distributions include Amazon Linux, CentOS, Debian, OpenSUSE, Oracle Linux, RHEL, SUSE Linux Enterprise Server (SLES), and Ubuntu.
These packages ensure comprehensive endpoint protection across a wide range of operating systems.
https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Endpoint-Admin-Guide/Topics-Common-for-HEP/Supported-Operating-System-for-the-Client.htm

QUESTION 7
On which desktop operating systems are Harmony Endpoint Clients supported?

A. Windows, MacOS, Linux and Unix
B. Only Windows and MacOS
C. Windows Servers and Clients, MacOS and Linux
D. Windows Client, MacOS and Linux

Answer: C
Explanation:
Check Point Harmony Endpoint supports Windows Server editions, Windows Client editions, macOS, and Linux. Unix is not explicitly supported in this context.

QUESTION 8
You must make a decision of which FDE algorithm to be used by one of your clients who specializes in multimedia video editing. What algorithm will you choose?

A. The implementation of a Secure VPN with very strong encryption will make your data invisible in cases of live internet transmission.
B. In Multimedia applications you do not need to implement any kind of Full disk encryption. You can use software like 7Zip in order to encrypt your data.
C. Any kind of data is very important and the Full Disk Encryption technic must be used with the strongest secret key possible. Your client has to use strong encryption like XTS-AES 256 bit.
D. Video processing is a high bandwidth application which utilizes a lot of HDD access time. You have to use a FDE algorithm with small secret key like XTS-AES 128 bit.

Answer: C
Explanation:
In the context of Full Disk Encryption (FDE) for a client specializing in multimedia video editing, it's crucial to prioritize data security due to the sensitive nature of the content being handled. Utilizing a robust encryption algorithm like XTS-AES 256-bit ensures a high level of protection against unauthorized access.
Why XTS-AES 256-bit?
Strong Security: XTS-AES 256-bit encryption offers a high level of security, making it suitable for protecting sensitive data, including multimedia content.
Performance Considerations: While stronger encryption algorithms may introduce some performance overhead, modern hardware often mitigates this impact. For high-performance applications like video editing, it's essential to balance security with performance needs.

QUESTION 9
What does pre-boot authentication disable?

A. Workarounds to computer security
B. Identity theft
C. Incorrect usernames
D. Weak passwords

Answer: D
Explanation:
Pre-boot authentication is designed to enforce strong security measures before the operating system loads. It disables the use of weak passwords by requiring users to authenticate before booting into the operating system. This ensures that the device is secured from unauthorized access, particularly in situations where data protection, like Full Disk Encryption, is in place. By requiring robust authentication, it prevents attackers from bypassing security with weak or easily guessable passwords.

QUESTION 10
Does the Endpoint Client GUI provide automatic or manual prompting to protect removable storage media usage?

A. Manual Only
B. Either automatic or manual
C. Automatic Only
D. Neither automatic or manual

Answer: B
Explanation:
The Endpoint Security Client's Media Encryption & Port Protection component offers both automatic and manual methods to protect removable storage media:
Automatic Protection: When a removable device is connected, the client can automatically prompt for encryption or access authorization, ensuring that sensitive data is protected without user intervention.
Manual Protection: Users can manually initiate encryption or access controls through the client interface, providing flexibility based on organizational policies and user preferences.
This dual approach allows organizations to balance security requirements with user convenience.

QUESTION 11
Full Disk Encryption (FDE) protects data at rest stored on_____.

A. RAM Drive
B. SMB Share
C. NFS Share
D. Hard Drive

Answer: D
Explanation:
Full Disk Encryption (FDE) is a security method that encrypts all data on a disk drive, including the operating system, applications, and user files. This comprehensive encryption ensures that unauthorized users cannot access the data, even if the physical device is lost or stolen.
FDE operates at the disk level, encrypting the entire disk, which includes all data stored on it. This approach differs from file-level encryption, which encrypts individual files or folders. By encrypting the entire disk, FDE provides a higher level of security, as it protects all data, including system files and temporary files, from unauthorized access.

In contrast, data stored on network shares like SMB or NFS shares is typically protected by network-level security measures, such as access controls and encryption protocols, rather than by FDE. Similarly, data stored in RAM drives is volatile and does not persist after a system reboot, making it less relevant to FDE.
https://www.techtarget.com/whatis/definition/full-disk-encryption-FDE

QUESTION 12
What does FDE software combine to authorize accessibility to data on desktop computers and laptops?

A. post-logon authentication and encryption
B. OS boot protection with pre-boot authentication and encryption
C. OS boot protection and post-boot authentication
D. Decryption

Answer: B
Explanation:
Full Disk Encryption (FDE) software combines OS boot protection, which ensures that the system is secure from the moment it's powered on, with pre-boot authentication. This forces the user to authenticate before the operating system loads, ensuring that only authorized users can access the encrypted data. The encryption protects the data at rest, making it unreadable without proper authentication.

QUESTION 13
What does pre-boot protection require of users?

A. To authenticate before the computer will start
B. To answer a security question after login
C. To authenticate before the computer's OS starts
D. To regularly change passwords

Answer: C
Explanation:
Pre-boot authentication (PBA) requires users to authenticate before the operating system (OS) starts. This process ensures that the device is protected from unauthorized access, even if the OS is compromised. By requiring authentication at the pre-boot stage, the system prevents unauthorized users from accessing the OS and its data.
In contrast, post-boot authentication occurs after the OS has loaded, which may not provide the same level of security against unauthorized access.
https://en.wikipedia.org/wiki/Pre-boot_authentication
https://www.trentonsystems.com/en-us/resource-hub/blog/pre-boot-post-boot-authentication

QUESTION 14
What does the Data protection/General rule contain?

A. Actions that define user authentication settings only
B. Actions that define decryption settings for hard disks
C. Actions that restore encryption settings for hard disks and change user authentication settings
D. Actions that define port protection settings and encryption settings for hard disks and removable media

Answer: D
Explanation:
The Data Protection/General rule includes actions that define both port protection settings and encryption settings for hard disks and removable media. This rule helps to manage the protection of data both at rest (through encryption) and in transit (via port protection), ensuring the security of sensitive information on the device.

QUESTION 15
The Harmony Endpoint solution includes which three Data Security Software Capability protections?

A. - Full Disk Encryption
   - Media Encryption
   - Anti-Malware
B. - Passwords and Usernames
   - Port Protection (MEPP)
   - Security Questions
C. - Media Encryption
   - Media Decryption
   - Remote Access VPN
D. - Full Disk Encryption
   - Media Encryption & Port Protection (MEPP)
   - Remote Access VPN

Answer: D
Explanation:
Check Point Harmony Endpoint provides Data Security Software Capabilities to protect sensitive information and prevent data leaks. The three key data security features included are:
Full Disk Encryption (FDE) – Encrypts the entire hard drive to protect data at rest, ensuring that unauthorized users cannot access data even if the device is lost or stolen.
Media Encryption & Port Protection (MEPP) – Encrypts external media devices (USB, external drives) and restricts unauthorized peripheral devices to prevent data leakage.
Remote Access VPN – Provides secure remote access to corporate resources by encrypting network traffic, preventing unauthorized data interception.

QUESTION 16
What is the default encryption algorithm in Full Disk Encryption tab under Advanced Settings?

A. AES-CBC 128 bit
B. AES-CBC 256 bit
C. XTS-AES 256 bit
D. XTS-AES 128 bit

Answer: B
Explanation:
In Check Point's Full Disk Encryption (FDE) settings, the default encryption algorithm under the Advanced Settings is AES-CBC 256 bit. This algorithm employs the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode with a 256-bit key length, providing robust data protection for full disk encryption.
https://sc1.checkpoint.com/documents/R80.40/SmartEndpoint_OLH/EN/Topics-EPSG/VolumeEncryption.html?

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**