DUMPSARENA

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

Checkpoint 156-536

Version Demo

Total Demo Questions: 12

Total Premium Questions: 122

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Harmony Endpoint Overview	44
Topic 2, Deployment	57
Topic 3, Policy Management	15
Topic 4, Threat Prevention	6
Total	122

QUESTION NO: 1

What happens to clients that fail to meet the requirements?

A. They have unenforced protections

B. They have encryption issues

C. They do not receive FDE protections

D. They receive incomplete protections

ANSWER: C

Explanation:

They do not receive FDE protections. Harmony Endpoint Full Disk Encryption uses a deployment process in which the endpoint must meet the required conditions before encryption protection can be fully applied. These prerequisites are essential because Full Disk Encryption must be able to install and operate its protected pre-boot environment reliably. When a client does not meet them, Harmony Endpoint cannot protect that computer through Full Disk Encryption, and the pre-boot environment cannot open. Consequently, the device does not obtain the intended FDE protection state; it is not merely a partial-encryption condition or a generic warning about encryption health. This distinction matters operationally: administrators should identify why the endpoint did not satisfy the deployment requirements and remediate that condition before treating the computer as protected by FDE. Until the prerequisites are fulfilled and the deployment completes successfully, the endpoint should not be considered covered by the Full Disk Encryption policy. Check Point's Harmony Endpoint documentation describes Full Disk Encryption configuration, deployment, and the protected pre-boot capability in its administration guidance. See the Harmony Endpoint Administration Guide: Full Disk Encryption and the Check Point Harmony Endpoint product page.

QUESTION NO: 2

An Endpoint client has completed initial registration and received its first policy synchronization from the Endpoint Security Management Server. What communication behavior begins next as part of normal managed operation?

A. A periodic client-initiated heartbeat connection

B. A periodic server-initiated connection to the client

C. A one-time Full Disk Encryption recovery request

D. An LDAP synchronization with the client operating system

ANSWER: A

Explanation:

The client begins its **periodic heartbeat communication** after the first synchronization. The heartbeat is initiated by the client and provides regular management connectivity, status reporting, and opportunities to receive relevant updates.

The heartbeat is not a server-initiated random connection and does not occur before the endpoint has established its initial managed relationship through synchronization.

QUESTION NO: 3

What do the machine's Endpoint Client GUI Overview page, Web Management, and debug logs show?

A. The status of the client's FDE system setup only

B. The deployment status of the client's policy download, user acquisition, FDE system setup, and encryption phases.

C. The status of the client's policy downloads only

D. The status of the client's encryption phases only

ANSWER: B

Explanation:

The deployment status of the client's policy download, user acquisition, FDE system setup, and encryption phases. is correct because Full Disk Encryption deployment is a staged process that must be visible to both the endpoint user and the administrator. The Endpoint Client GUI Overview page provides local progress and status information, while Harmony Endpoint Web Management and diagnostic/debug logging provide administrative and troubleshooting visibility into the same deployment workflow. This includes receiving the applicable policy, acquiring the relevant user information, preparing the computer for Full Disk Encryption, and reporting the encryption progress/state. Viewing these phases together is important because encryption cannot be treated as an isolated event: the endpoint must first obtain its configuration and complete the prerequisite setup activities before the drive-protection process can proceed and be monitored. Check Point's Harmony Endpoint documentation describes Full Disk Encryption as an integrated endpoint capability managed through policy and endpoint status reporting, and its administration guidance covers monitoring and troubleshooting endpoint deployment behavior. See the Check Point Harmony Endpoint Administration Guide and the Check Point Harmony Endpoint product overview.

QUESTION NO: 4

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

A. Remote Operations

B. Node Management

C. Remote Help

D. Push Operations

ANSWER: D

Explanation:

Push Operations is the Endpoint Security Management Server feature intended for sending an immediate administrative action to selected endpoint computers without requiring a policy installation. An administrator can select endpoints in the Endpoint Security management interface and issue operational commands such as restart or shutdown. These are on-demand management actions rather than persistent configuration changes delivered through a policy package, which makes the feature useful for maintenance, troubleshooting, and controlled endpoint administration.

Push Operations are handled through the established Endpoint Security client-management communication channel. The endpoint must therefore be managed and able to receive the operation; if it is temporarily offline, the requested action is performed when connectivity and applicable operational conditions permit. This separation between an immediate push action and a full policy installation lets administrators carry out necessary device operations while avoiding an unnecessary policy deployment cycle. Check Point documents Push Operations as part of Endpoint Security administration and distinguishes these administrative commands from policy management workflows. See the Check Point Endpoint Security R81.20 Push Operations documentation and the Endpoint computer management documentation.

QUESTION NO: 5

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 technique 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: D

Explanation:

Video editing is a disk-intensive workload: large media assets are read, written, rendered, cached, and moved continuously. Full Disk Encryption operates transparently beneath the file system, so its encryption and decryption processing applies to this sustained storage activity. XTS-AES 128 bit provides the appropriate balance for this use case because it uses the XTS mode designed for storage encryption while reducing cryptographic processing overhead relative to a larger AES key. This helps preserve the disk throughput and responsiveness needed during high-bandwidth multimedia production.

Check Point Full Disk Encryption protects data at rest through pre-boot protection, boot authentication, and encryption of the device's storage. The selected algorithm should therefore account for both the required protection and the endpoint's expected performance profile. For a workstation whose primary role is demanding video processing, XTS-AES 128 bit is the recommended practical choice among the listed algorithms. Check Point's Harmony Endpoint documentation describes Full Disk Encryption and its policy configuration in the Harmony Endpoint Administration Guide. Background on the XTS-AES mode used for storage devices is available in NIST SP 800-38E.

QUESTION NO: 6

How does FDE add another layer of security?

A. By offering media encryption

B. By offering pre-boot protection

C. By offering port protection

D. By offering encryption

ANSWER: B

Explanation:

By offering pre-boot protection is correct. Check Point Full Disk Encryption (FDE) protects a device before the operating system starts. At startup, the user must successfully authenticate at the pre-boot environment before the encrypted drive can be unlocked and the operating system can load. This creates a security boundary that operates independently of the normal Windows sign-in process. Consequently, a person who has physical possession of a powered-off or restarted endpoint cannot simply boot the installed operating system or access its protected information without satisfying the FDE authentication requirement. The pre-boot stage is therefore an additional layer of access control: it verifies the authorized user before granting access to the encryption keys needed to read the disk. This is particularly important for lost or stolen laptops, because data remains protected even when the endpoint is not connected to the corporate network. Check Point documents Full Disk Encryption as a Harmony Endpoint capability and describes pre-boot authentication as part of its disk-encryption protection workflow. See the Check Point Harmony Endpoint overview and the Harmony Endpoint documentation portal for product documentation and administration guidance.

QUESTION NO: 7

Full Disk Encryption (FDE) protects data at rest stored on a Hard Drive.

A. RAM Drive

B. SMB Share

C. NFS Share

D. Hard Drive

ANSWER: D

Explanation:

Full Disk Encryption protects data at rest on the endpoint's local hard drive. In Harmony Endpoint, Check Point Full Disk Encryption combines pre-boot protection, boot authentication, and encryption so that information stored locally on desktops and laptops remains inaccessible unless an authorized user successfully authenticates. This is specifically intended to protect the contents of an endpoint if the computer is lost, stolen, powered off, or otherwise accessed outside the normal operating-system session.

The protection applies to the physical disk and, where configured, its volumes. Encryption is performed transparently for authorized users after authentication, while the stored data remains encrypted when it resides on the drive. This addresses the data-at-rest risk associated with local endpoint storage rather than data held only in volatile memory or accessed remotely through a network resource. Check Point's Harmony Endpoint documentation describes Full Disk Encryption as a capability that safeguards information on endpoint computers through pre-boot authentication and strong encryption. See the Harmony Endpoint documentation portal and Check Point's Harmony Endpoint product overview for the Full Disk Encryption feature context.

QUESTION NO: 8

External Policy Servers are placed between the Endpoint clients and the Endpoint Security Management Server. How many Policy Servers are supported per environment?

A. From 1 to 25 Policy Servers are supported

B. From 1 to 15 Policy Servers are supported

C. From 1 to 20 Policy Servers are supported

D. From 1 to 5 Policy Servers are supported

ANSWER: C

Explanation:

From 1 to 20 Policy Servers are supported. In a Check Point Harmony Endpoint deployment, an External Policy Server acts as an intermediary between Endpoint clients and the Endpoint Security Management Server. This architecture is intended for distributed or large-scale environments where direct client connectivity to the management server may be inefficient or unavailable. Policy Servers provide local client communication services, including policy distribution and reporting-related connectivity, while remaining centrally managed through the Endpoint Security Management Server.

The platform supports deploying up to 20 External Policy Servers in one environment. Administrators can use this capacity to place servers near major geographic locations, network segments, or remote offices and to spread Endpoint-client load appropriately. The exact number deployed should be based on client population, network topology, resiliency requirements, and the sizing guidance for the relevant Harmony Endpoint release. This documented maximum is an environment-level limit, rather than a recommendation that every deployment requires 20 servers. See the Check Point Endpoint Security R81.20 Administration Guide and the Harmony Endpoint product documentation overview for deployment and architecture information.

QUESTION NO: 9

What does Endpoint's Media Encryption (ME) Software Capability requiring authorization accomplish?

A. Protects sensitive data and encrypts storage media

B. Controls ports and encrypts storage media

C. Controls ports and manages ports

D. Decrypts and blocks access to specific ports

ANSWER: B

Explanation:

Controls ports and encrypts storage media is correct. Check Point Harmony Endpoint's Media Encryption and Port Protection capability is designed to control how endpoint users interact with removable-media interfaces and to protect data when it is written to authorized removable storage. Administrators can apply policy to device and port usage, such as USB-connected storage, while requiring encryption for media that is permitted for use. This combination helps prevent unprotected copies of organizational data from leaving managed endpoints and supports secure use of removable devices in environments where such media is necessary. The authorization aspect is important because it allows the organization to enforce centrally managed access and encryption policy rather than relying on individual users to protect media manually. Check Point describes Harmony Endpoint as providing unified endpoint protection and data protection controls, including protection for data on endpoint devices and removable media. See the Check Point Harmony Endpoint product page and the Harmony Endpoint datasheet for product capability information.

QUESTION NO: 10

Endpoint's Media Encryption (ME) Software Capability protects sensitive data on what, and how?

A. Storage devices, removable media, and other input/output devices by requiring authorization before a user accesses the device

B. Input/output devices using Anti-Malware

C. Removable media and other input/output devices by using encryption methods

D. Storage devices by requiring multi-factor authorization

ANSWER: A

Explanation:

Storage devices, removable media, and other input/output devices by requiring authorization before a user accesses the device is correct because Harmony Endpoint's Media Encryption and Port Protection capability combines protection for data-bearing media with device and port access control. The policy is not limited to encrypting a file after it has been copied; it can enforce whether a user or endpoint is authorized to use a connected storage device or peripheral in the first place. This provides a preventative control point for sensitive data, particularly when users connect USB storage, optical media, or other external input/output hardware. Administrators define rules for device classes and individual devices, then apply access permissions and encryption requirements through the Harmony Endpoint policy. Authorized use can therefore be controlled centrally while protected media remains suitable for legitimate business use. This approach helps reduce the risk of unapproved removable media becoming a path for data exposure or transfer. Check Point documents Media Encryption and Port Protection as an Endpoint capability for managing removable media encryption and controlling access to ports and devices. See the Check Point Harmony Endpoint overview and the Harmony Endpoint Administration Guide: Media Encryption and Port Protection.

QUESTION NO: 11

Where are the Endpoint Policy Servers located?

A. Between the Endpoint clients and the EPS

B. Between the Endpoint clients and the EMS

C. Between the Endpoint clients and the NMS

D. Between the Endpoint clients and the SMS

ANSWER: B

Explanation:

“Between the Endpoint clients and the EMS” is correct because an Endpoint Policy Server acts as an intermediary communication component between managed endpoint computers and the Endpoint Management Server. It is commonly deployed when endpoints cannot directly reach the Endpoint Management Server, such as when devices are on remote networks, in perimeter segments, or across locations with restricted connectivity. The Endpoint Policy Server accepts client connections and relays the required management communication to the Endpoint Management Server, enabling clients to receive policy updates, report status, and maintain management connectivity without exposing or directly connecting every endpoint to the management server. This architecture also helps organizations scale endpoint communications and place connection points closer to remote endpoint populations. The Endpoint Policy Server therefore does not replace central endpoint management; instead, it extends the Endpoint Management Server’s reach by functioning as the managed communication path for clients. Check Point’s Endpoint administration documentation describes the Endpoint Policy Server role and its deployment in the endpoint-management architecture: Check Point Endpoint Policy Server documentation. Additional product architecture context is available from Check Point Harmony Endpoint.

QUESTION NO: 12

A user works from a hotel network and must access internal corporate resources securely from a managed endpoint. The organization needs to protect the traffic between the endpoint and the corporate network. Which Harmony Endpoint capability addresses this requirement?

A. Compliance

B. Full Disk Encryption

C. Media Encryption and Port Protection

D. Remote Access VPN

ANSWER: D

Explanation:

Remote Access VPN provides secure remote access from the Endpoint Security Client to corporate networks over an IPsec VPN connection. It protects traffic while the user connects from an untrusted network.

Full Disk Encryption protects locally stored data at rest. Media Encryption and Port Protection controls removable media, while Compliance evaluates whether endpoint requirements are met.