DUMPSARENA

Administration of Symantec Endpoint Protection 14

Symantec 250-428

Version Demo

Total Demo Questions: 10

Total Premium Questions: 131

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

An organization created a rule in the Application and Device Control policy to block peer-to-peer applications.

What two other protection technologies can block and log such unauthorized application? (Choose two.)

A. Memory Exploit Mitigation

B. Virus and Spyware Protection

C. Custom IPS Signatures

D. Host Integrity

E. Firewall

ANSWER: C E

Explanation:

Reference: https://support.symantec.com/us/en/article.tech122597.html

QUESTION NO: 2

A Symantec Endpoint Protection Manager (SEPM) administrator notices performance issues with the SEPM server. The Client tab becomes unresponsive in the SEPM console and .DAT files accumulate in the “agentinfo” folder.

Which tool should the administrator use to gather log files to submit to Symantec Technical Support?

A. collectLog.cmd

B. LogExport.exe

C. smc.exe

D. ExportLog.vbs

ANSWER: A

Explanation:

References: https://support.symantec.com/en_US/article.TECH105955.html

QUESTION NO: 3

An organization has a small group of servers with large drive volumes.

What setting in the Virus and Spyware Protection policy can the organization utilize when scheduling scans on these servers?

A. Use resumable scans

B. Use Shared Insight Cache

C. Adjust Auto Protect Settings

D. Randomize scheduled scans

ANSWER: A

Explanation:

Reference: https://support.symantec.com/us/en/article.HOWTO80934.html

QUESTION NO: 4

Which two are policy types within the Symantec Endpoint Protection Manager? (Select two.)

A. Intrusion Prevention

B. Exceptions

C. Process Control

D. Shared Insight

E. Host Protection

ANSWER: A B

Explanation:

References: https://support.symantec.com/en_US/article.TECH104434.html

QUESTION NO: 5

Which tool should the administrator run before starting the Symantec Endpoint Protection Manager upgrade according to best practices?

A. CollectLog.cmd

B. DBValidator.bat

C. LogExport.cmd

D. Upgrade.exe

ANSWER: B

Explanation:

References: https://support.symantec.com/en_US/article.TECH240591.html

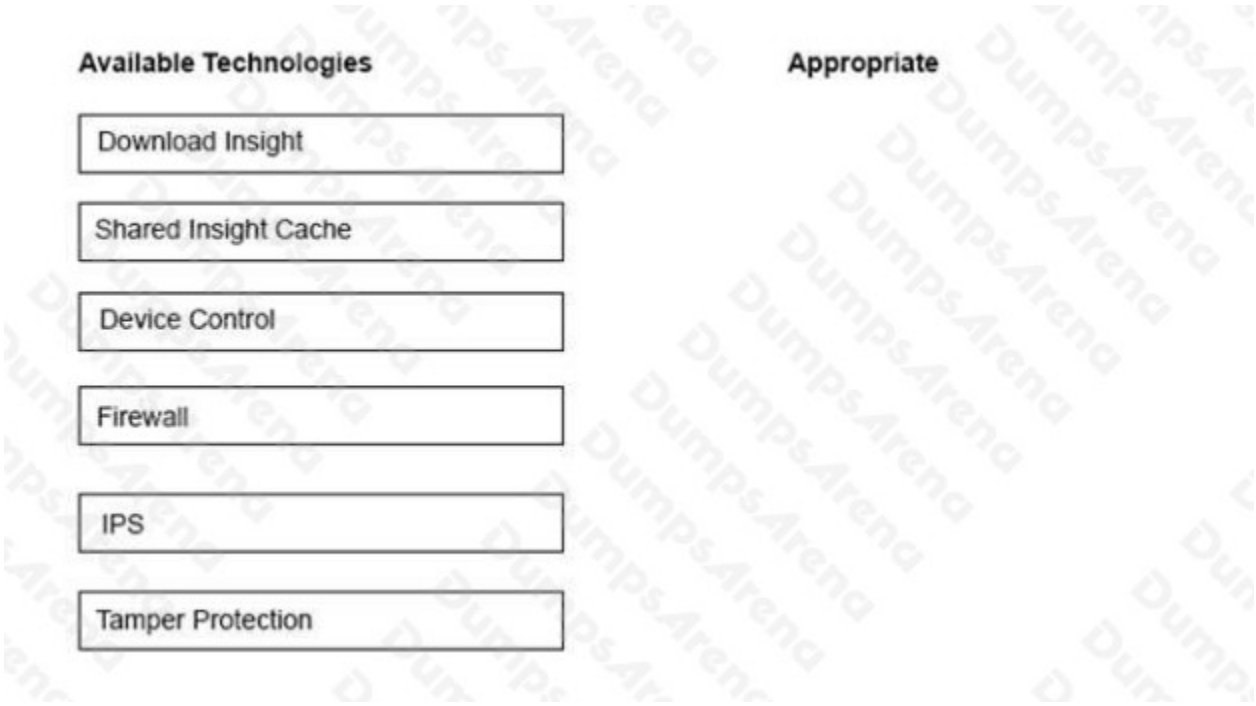
QUESTION NO: 6 - (DRAG DROP)

DRAG DROP

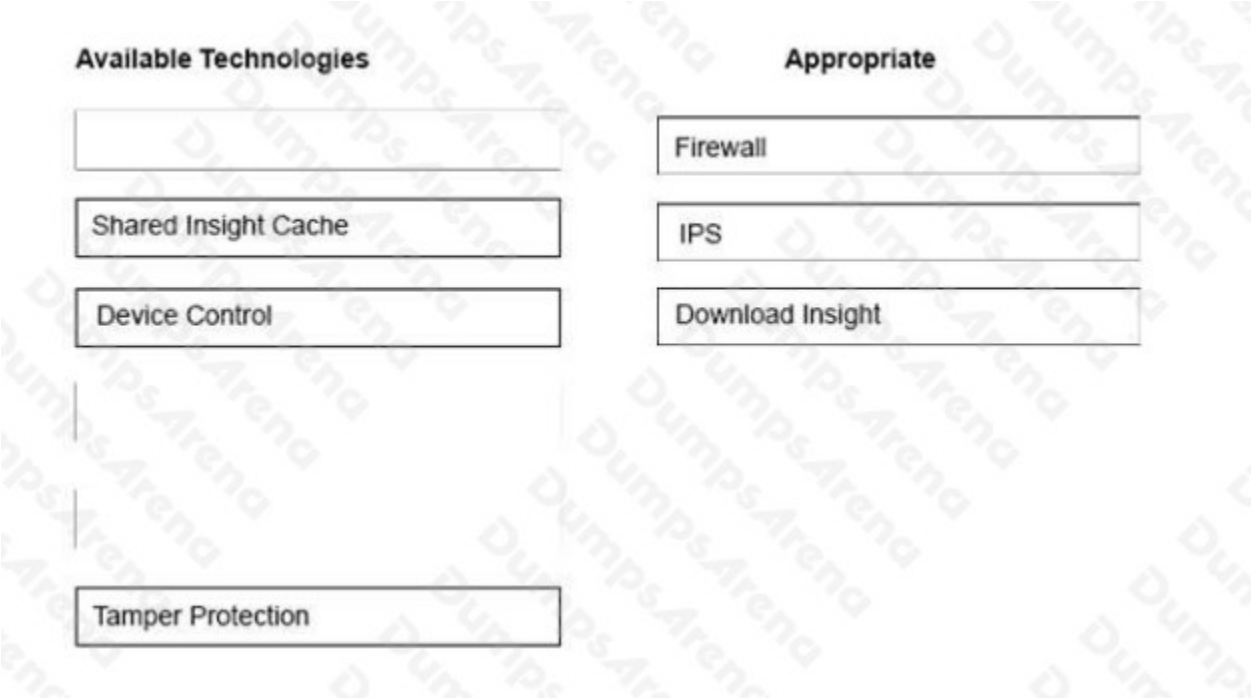
An administrator is unknowingly trying to connect to a malicious website and download a known threat within a .rar file. All Symantec Endpoint Protection technologies are installed on the client's system.

Drag and drop the technologies to the right side of the screen in the sequence necessary to block or detect the malicious file.

Select and Place:



ANSWER:



Explanation:

QUESTION NO: 7

Which two options are available when configuring DNS change detections for SONAR? (Select two.)

A. Log

B. Quarantine

C. Block

D. Active Response

E. Trace

ANSWER: A C

QUESTION NO: 8

An administrator needs to increase the access speed for client files that are stored on a file server. Which configuration should the administrator review to address the read speed from the server?

A. Enable Network Cache in the client's Virus and Spyware Protection policy

B. Add the applicable server to a trusted host group

C. Enable download randomization in the client group's communication settings

D. Create a Firewall allow rule for the server's IP address.

ANSWER: A

QUESTION NO: 9

A company deploys Symantec Endpoint Protection (SEP) to50 virtual machines running on a single ESXi host.

Which configuration change can the administrator make to minimize sudden IOPS impact on the ESXi server while each SEP endpoint communicates with the Symantec Endpoint Protection Manager?

A. Reduce number of content revisions to keep

B. Increase download randomization window

C. Reduce the heartbeat interval

D. Increase Download Insight sensitivity level

ANSWER: B

QUESTION NO: 10

In which two areas can host groups be used? (Select two.)

A. Locations

B. Download Insight

C. IPS

D. Application and Device Control

E. Firewall

ANSWER: C E