250-438$^{\text{Q\&As}}$

Administration of Symantec Data Loss Prevention 15

Pass Symantec 250-438 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/250-438.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec Official Exam Center

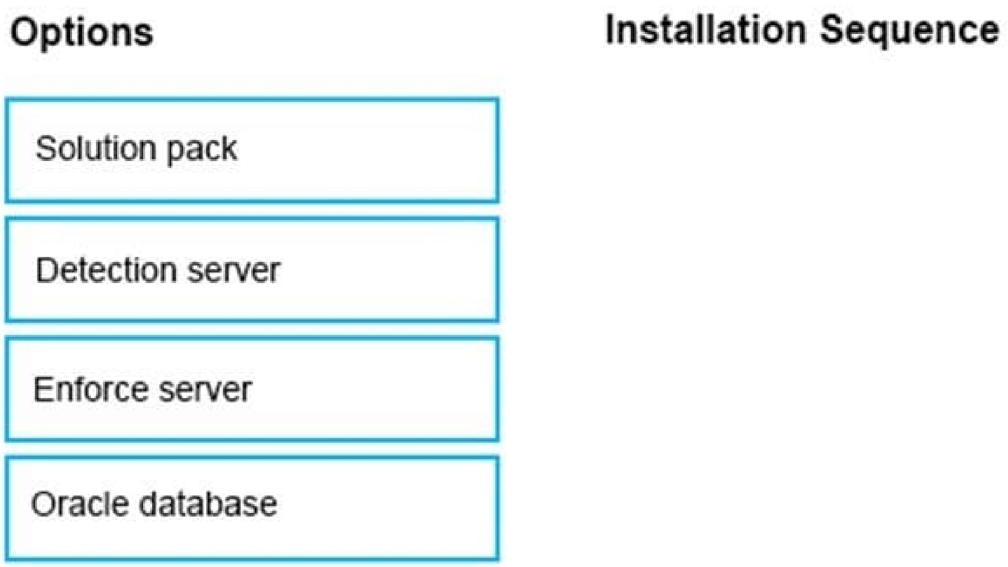
QUESTION 1

DRAG DROP

What is the correct installation sequence for the components shown here, according to the Symantec Installation Guide?

Place the options in the correct installation sequence.

Select and Place:



Options

Installation Sequence

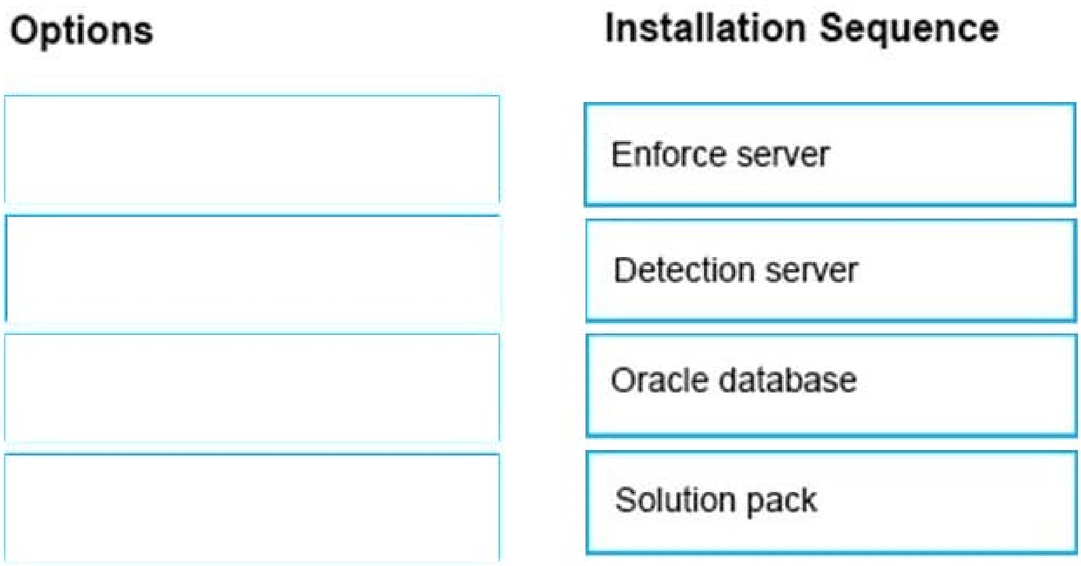
Solution pack

Detection server

Enforce server

Oracle database

Correct Answer:



Options

Installation Sequence

Enforce server

Detection server

Oracle database

Solution pack

QUESTION 2

Which two automated response rules will be active in policies that include Exact Data Matching (EDM) detection rule? (Choose two.)

A. Endpoint Discover: Quarantine File

B. All: Send Email Notification

C. Endpoint Prevent: User Cancel

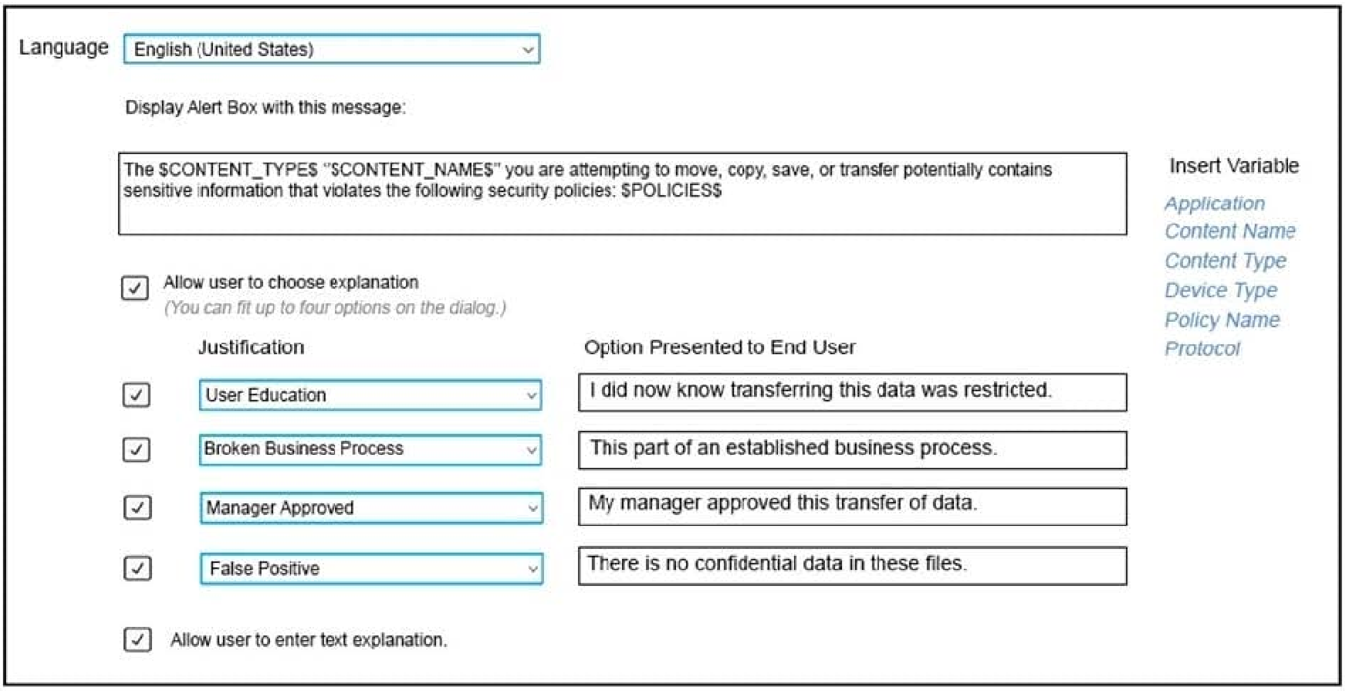
D. Endpoint Prevent: Block

E. Network Protect: Quarantine File

Correct Answer: AD

QUESTION 3

Refer to the exhibit. Which type of Endpoint response rule is shown?



Language: English (United States)

Display Alert Box with this message:

The $CONTENT_TYPE$ "$CONTENT_NAME$" you are attempting to move, copy, save, or transfer potentially contains sensitive information that violates the following security policies: $POLICIES$

Insert Variable

Application
Content Name
Content Type
Device Type
Policy Name
Protocol

☑ Allow user to choose explanation
(You can fit up to four options on the dialog.)

	Justification	Option Presented to End User
☑	User Education	I did now know transferring this data was restricted.
☑	Broken Business Process	This part of an established business process.
☑	Manager Approved	My manager approved this transfer of data.
☑	False Positive	There is no confidential data in these files.

☑ Allow user to enter text explanation.

A. Endpoint Prevent: User Notification

B. Endpoint Prevent: Block

C. Endpoint Prevent: Notify

D. Endpoint Prevent: User Cancel

Correct Answer: B

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v27595430_v120691346/Configuring-the-Endpoint-Prevent:-Block-action?locale=EN_US

QUESTION 4

A DLP administrator is testing Network Prevent for Web functionality. When the administrator posts a small test file to a cloud storage website, no new incidents are reported. What should the administrator do to allow incidents to be generated against this file?

A. Change the "Ignore requests Smaller Than" value to 1

B. Add the filename to the Inspect Content Type field

C. Change the "PacketCapture.DISCARD_HTTP_GET" value to "false"

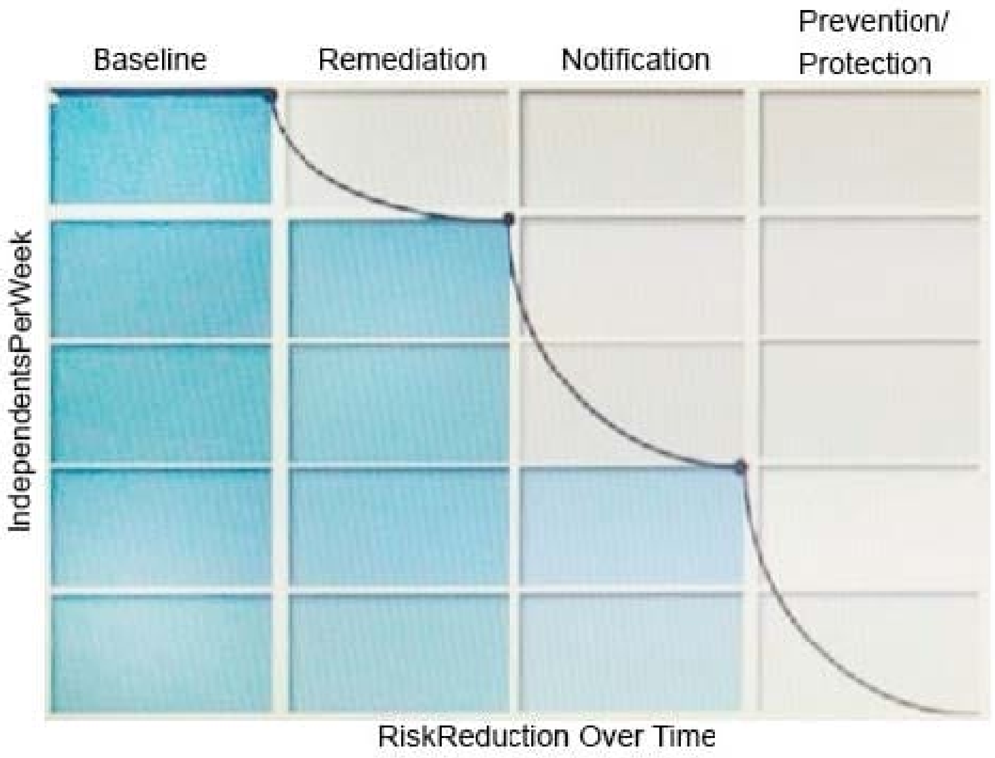
D. Uncheck trial mode under the ICAP tab

Correct Answer: A

Reference: https://help.symantec.com/cs/dlp15.0/DLP/id-SF0B0161467_v120691346/Configuring-Network-Prevent-for-Web-Server?locale=EN_US

QUESTION 5

Refer to the exhibit.



What activity should occur during the baseline phase, according to the risk reduction model?

A. Define and build the incident response team

B. Monitor incidents and tune the policy to reduce false positives

C. Establish business metrics and begin sending reports to business unit stakeholders

D. Test policies to ensure that blocking actions minimize business process disruptions

Correct Answer: C