DUMPSARENA

Endpoint Security Complete Implementation - Technical Specialist

Symantec 250-586

Version Demo

Total Demo Questions: 7

Total Premium Questions: 78

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

A. Exceptions

B. Host Protection

C. Shared Insight

D. Intrusion Prevention

E. Process Control

ANSWER: A D

Explanation:

Exceptions and **Intrusion Prevention** are policy types administered through Symantec Endpoint Protection Manager. An Exceptions policy centrally defines exclusions for endpoint protection technologies. Administrators can use it to exclude specified files, folders, file extensions, processes, or other objects when an exclusion is appropriate for a trusted application or a documented operational requirement. Because the policy is assigned to groups, the exclusion configuration can be consistently applied to the managed endpoint population rather than maintained individually on each device.

An Intrusion Prevention policy is also a standard SEPM policy. It configures endpoint network-intrusion protection behavior, including the signatures and settings used to inspect network traffic and detect or block exploit attempts, malicious protocol activity, and other network-based attacks. SEPM lets administrators create, edit, assign, and enforce this policy across groups of clients, ensuring that endpoint intrusion-prevention settings align with the organization's security requirements.

These policy categories are part of the Endpoint Protection policy-management model described in the Broadcom Symantec Endpoint Protection documentation. Broadcom also provides Endpoint Protection administrative guidance through its Knowledge Base.

QUESTION NO: 2

Which EDR feature is used to search for real-time indicators of compromise?

A. Cloud Database search

B. Endpoint search

C. Domain search

D. Device Group search

ANSWER: B

Explanation:

Endpoint search is the EDR capability designed for actively querying managed endpoints for indicators and artifacts associated with suspected compromise. An analyst can use it during threat hunting or incident investigation to look across devices for relevant endpoint telemetry and evidence, such as files, processes, hashes, command lines, registry-related artifacts, and other observable data. This makes it particularly useful when a newly identified indicator of compromise must be checked against the organization's endpoint population without waiting for a scheduled report or relying only on previously generated detections. Endpoint search helps analysts rapidly establish the scope of potentially affected devices, collect context for triage, and decide whether response actions are needed. In Symantec Endpoint Security Complete, this function supports the EDR workflow by enabling direct investigation of endpoint data from the management console. Broadcom's Endpoint Security documentation describes the product's endpoint detection, investigation, and response capabilities and provides the operational documentation for Endpoint Search and associated EDR functions. See the Broadcom Endpoint Security documentation portal and the Symantec Endpoint Security product page.

QUESTION NO: 3

During Data Gathering, which two items are technical objectives that can directly constrain the SES Complete implementation design? (Select two.)

A. The supported operating systems in the endpoint estate

B. The available WAN bandwidth between sites

C. The desired reduction in incident-response time

D. The customer acceptance of completed deliverables

E. The approval of the project budget

ANSWER: A B

Explanation:

The supported operating systems in the endpoint estate and **the available WAN bandwidth between sites** are correct because they are operational constraints that affect agent deployment, policy design, communication, and content-delivery planning. A desired reduction in incident-response time is a business outcome, while acceptance of completed deliverables and the project budget approval are engagement-governance matters rather than technical environmental constraints.

QUESTION NO: 4

What is the purpose of the Test Plan in the implementation phase?

A. To assess the SESC Solution Design in the customer's environment

B. To monitor the Implementation of SES Complete

C. To guide the adoption and testing of SES Complete in the implementation phase

D. To seek approval for the next phase of the SESC Implementation Framework

ANSWER: C

Explanation:

To guide the adoption and testing of SES Complete in the implementation phase is correct because a Test Plan provides the structured method for validating that the deployed solution operates as intended in the customer environment. It defines the test scope, expected outcomes, prerequisites, test activities, and acceptance criteria used to confirm that configured security capabilities, endpoint communications, policy behavior, and required integrations meet the implementation requirements. The plan also supports a controlled rollout: implementation stakeholders can test representative endpoints and workflows, record results, resolve issues, and confirm readiness before broad production adoption. This validation is especially important because endpoint-security deployments commonly involve customer-specific policies, network conditions, operating systems, and operational processes. A documented testing approach makes those checks repeatable and provides evidence that the implementation satisfies the agreed design and security objectives. Broadcom’s Endpoint Security documentation provides the product configuration and operational guidance that implementation teams use when defining and executing such validation activities. See the Broadcom Endpoint Security documentation portal and the Broadcom Endpoint Security product downloads and documentation resources.

QUESTION NO: 5

An administrator must test a more restrictive firewall and intrusion prevention configuration without changing protection behavior for existing production endpoints. What is the most appropriate approach?

A. Create a separate pilot group and assign the test policies only to that group.

B. Edit the production policy and rely on the next heartbeat to identify issues.

C. Remove all existing policies from the production group before testing.

D. Disable client communication until the production policy has been approved.

ANSWER: A

Explanation:

Create a separate pilot group and assign the test policies only to that group. SEP policy assignment is group based, so a dedicated pilot group isolates the changed configuration from production populations while allowing representative endpoints to be tested. Editing the production policy would expose all assigned production clients to an unvalidated change.

QUESTION NO: 6

When a SEPM is enrolled in ICDm which policy can only be managed from the cloud?

A. Firewall

B. Network Intrusion Prevention

C. LiveUpdate

D. Intensive Protection

ANSWER: B

Explanation:

Network Intrusion Prevention is the policy that can only be managed from the cloud after Symantec Endpoint Protection Manager is enrolled in Integrated Cyber Defense Manager (ICDm). ICDm integration creates a hybrid-management arrangement in which specific protection capabilities are administered through the cloud console rather than through the on-premises SEPM policy interface. Network Intrusion Prevention is among those cloud-managed capabilities, allowing its configuration to be centrally controlled using the cloud service's policy workflow and threat-protection model. This centralized handling supports consistent deployment of intrusion-prevention settings for the enrolled environment and aligns the capability with cloud-delivered security management. Administrators should therefore use the ICDm/Symantec Endpoint Security cloud console when they need to view, configure, or modify Network Intrusion Prevention policy settings for a SEPM that has been enrolled. Broadcom's Endpoint Security documentation provides the product documentation set and hybrid/cloud-management guidance at Broadcom TechDocs: Endpoint Security. The associated technical support knowledge and product documentation resources are available through the Broadcom Support Portal.

QUESTION NO: 7

Before a production rollout, the implementation team must document the selected SES Complete capabilities and their customer-specific settings, and also define repeatable validation activities with expected outcomes. Which two deliverables are required? (Select two.)

A. Solution Configuration Design

B. Test Plan

C. Solution Infrastructure Design

D. Executive Summary

E. Project close-out record

ANSWER: A B

Explanation:

The **Solution Configuration Design** records the selected features, functions, and customer-specific configuration settings that guide rollout. The **Test Plan** defines repeatable validation scenarios, expected outcomes, and acceptance criteria. The Infrastructure Design documents topology and communications, but it does not replace either configuration guidance or functional validation planning.