# Broadcom

## 250-604

## Symantec Endpoint Security Complete Admin R3 Technical Specialist

For More Information – Visit link below:

https://www.examsboost.com/

## Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

# Latest Version: 6.0

## Question: 1

**Scenario:**

An organization is deploying SES Complete to multiple branch offices globally. Some branches have low IT staff presence and no on-premise infrastructure. The security team wants to ensure continuous protection, visibility, and minimal configuration effort.

What should a security analyst consider when enrolling remote endpoints into SES Complete from different geographies with limited infrastructure support? (Choose three)

A. Leverage ICDm for centralized policy deployment
B.Use SEP Mobile agents for remote deployment
C.Utilize agent packages with auto-enrollment capabilities
D.Schedule weekly offline syncs for policy enforcement
E.Enable automatic policy updates via cloud communication

**Answer: ACE**

## Question: 2

Which consideration is most relevant when integrating SEPM with the ICDm platform in a hybrid environment?

A. Only cloud-licensed devices can participate in the hybrid structure.
B.Devices cannot report to both SEPM and ICDm simultaneously.
C.Endpoint devices must be manually re-enrolled with each policy update.
D.Certain features must be manually enabled to support co-management.

**Answer: D**

## Question: 3

When securing Android and iOS devices in a modern enterprise using SES Complete, which approaches allow administrators to manage threats effectively without interrupting device functionality? (Choose two)

A. Allowing passive threat detection without enforcement
B.Sending policy updates only when the user is connected to Wi-Fi
C.Using behavior analytics to detect rogue applications
D.Applying threat defense rules through configurable app control policies

**Answer: CD**

## Question: 4

What is the recommended first step when planning a migration of SEPM policies to the ICDm platform within a hybrid deployment?

A. Immediately disconnect SEPM from all managed endpoints.
B.Export all device group configurations and import into ICDm.
C.Review and map existing SEPM policies to ICDm equivalents for consistent functionality.
D.Disable all SEPM firewall rules and recreate them in ICDm.

**Answer: C**

## Question: 5

**Scenario:**
Your organization operates field devices using mobile hotspots. Employees often connect through untrusted Wi-Fi networks. You are asked to minimize the risk of data exfiltration via these connections using SES Complete.
Which two actions should be taken using SES Complete mobile security capabilities? (Choose two)

A. Block all app installations on field devices
B.Disable App Control in monitor mode
C.Enforce real-time scanning of mobile app behavior
D.Configure Network Integrity to detect rogue networks

**Answer: CD**

## Question: 6

Which component of ICDm allows administrators to initiate remediation actions such as isolating an endpoint or deleting a malicious file?

A. Incident Response Actions Panel
B.Alert Management Dashboard
C.Asset Management Console
D.Device Inventory

**Answer: A**

## Question: 7

What must be understood about policy precedence when managing both SEPM and ICDm in a hybrid Symantec Endpoint Security Complete environment?

A. Policy precedence is always based on alphabetical rule order.
B.SEPM policies will override all ICDm settings regardless of the device group.
C.Policies applied via ICDm take precedence unless explicitly overridden by SEPM-assigned policies.
D.Whichever policy was created most recently will override the older one.

**Answer: C**

## Question: 8

Which key features of SES Complete's mobile technologies assist administrators in securing corporate data on user-owned devices operating on untrusted networks? (Choose two)

A. Ability to block all background app updates permanently
B.Real-time malicious network detection and isolation
C.Continuous scanning of application permissions for suspicious access
D.Policy-based enforcement of threat remediation actions

**Answer: BD**

## Question: 9

What is the primary role of LiveShell within the EDR framework in ICDm?

A. Patching vulnerabilities in endpoint firmware
B.Updating policy changes across isolated endpoints
C.Automating system restarts after malware cleanup

D.Initiating real-time command-line investigation on remote devices

**Answer: D**

## Question: 10

When should administrators configure automatic quarantine rules for endpoints in ICDm?

A. When endpoints are connected via VPN only
B.When endpoints are consistently offline
C.When a high-severity threat is detected based on predefined behavioral triggers
D.When bandwidth utilization crosses a set threshold

**Answer: C**