

# Cisco

## Exam 500-275

### Securing Cisco Networks with Sourcefire FireAMP Endpoints

Version: Demo

[ Total Questions: 10 ]

**Question No : 1**

How many days' worth of data do the widgets on the dashboard page display?

- A. the previous 5 days of data
- B. the previous 6 days of data
- C. the previous 7 days of data
- D. the number of days you set in the dashboard configuration

**Answer: C**

**Question No : 2**

From the Deployment screen, you can deploy agents via which mechanism?

- A. push to client
- B. zip install file
- C. user download from Sourcefire website or email
- D. precompiled RPM package

**Answer: C**

**Question No : 3**

The FireAMP Mobile endpoint connector currently supports which mobile OS device?

- A. Firefox
- B. HTML5
- C. Android
- D. iPhone

**Answer: C**

**Question No : 4**

When a user initiates a scan, which types of scan are available as options?

- A. scheduled scan, thorough scan, quick scan, network scan
- B. jiffy scan, overnight scan, scan when available, vulnerability scan
- C. flash scan, custom scan, full scan
- D. none, because user-initiated scans are not allowed

**Answer: C**

**Question No : 5**

If a file's SHA-256 hash is sent to the cloud, but the cloud has never seen the hash before, which disposition is returned?

- A. Clean
- B. Neutral
- C. Malware
- D. Unavailable

**Answer: B**

**Question No : 6**

The Update Window allows you to perform which action?

- A. identify which hosts need to be updated
- B. email the user to download a new client
- C. specify a timeframe when an upgrade can be started and stopped
- D. update your cloud instance

**Answer: C**

**Question No : 7**

Which feature allows retrospective detection?

- A. Total Recall
- B. Cloud Recall
- C. Recall Alert

**D. Recall Analysis**

**Answer: B**

**Question No : 8**

Where does an administrator go to get a copy of a fetched file?

- A. the Business Defaults page
- B. the File menu, followed by Downloads
- C. the File Repository
- D. the Search selection in the Analysis menu

**Answer: C**

**Question No : 9**

What is the first system that is infected with a particular malware called?

- A. Patient Zero
- B. Source
- C. Infector
- D. Carrier

**Answer: A**

**Question No : 10**

Which pair represents equivalent processes whose names differ, depending on the connector version that you are running?

- A. immuneset\_protect and iptray
- B. agent.exe and sfc.exe
- C. TETRA and SPERO
- D. ETHOS and SPERO

**Answer: B**

