DUMPSARENA

# Securing Cisco Networks with Sourcefire FireAMP Endpoints

## Cisco 500-275

**Version Demo**

**Total Demo Questions: 10**

**Total Premium Questions: 50**

**Buy Premium PDF**

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, FireAMP Overview and Architecture | 9 |
| Topic 2, Outbreak Control Menu Items | 5 |
| Topic 3, Enpoint Policies | 5 |
| Topic 4, Groups and Development | 6 |
| Topic 5, Analysis and Reporting | 9 |
| Topic 6, Private Cloud | 5 |
| Topic 7, Accounts | 3 |
| Topic 8, FireAMP Connector | 3 |
| Topic 9, Console Interface | 5 |
| Total | 50 |

**QUESTION NO: 1**

The FireAMP connector monitors the system for which type of activity?

**A.** Vulnerabilities

**B.** Enforcement of usage policies

**C.** File operations

**D.** Authentication activity

**ANSWER: C**

**QUESTION NO: 2**

Where is the File Fetch context menu option available?

**A.** anywhere a filename or SHA-256 hash is displayed

**B.** only from the Filter Event View page

**C.** from the Audit Event page

**D.** from the configuration in the Business Defaults page

**ANSWER: A**

**QUESTION NO: 3**

What do policies enable you to do?

**A.** specify a custom whitelist

**B.** specify group membership

**C.** specify hosts to include in reports

**D.** specify which events to view

**ANSWER: A**

**QUESTION NO: 4**

A default FireAMP Private Cloud installation can accommodate how many connectors over which period of time?

**A.** 100 connectors over a 15-day period

**B.** 1000 connectors over a 45-day period

**C.** 5000 connectors over a 10-day period

**D.** 500 connectors over a 30-day period

**ANSWER: D**

**QUESTION NO: 5**

Which of these can you use for two-step authentication?

**A.** the Apple Authenticator app

**B.** the Google Authenticator app

**C.** a SecurID token

**D.** any RFC 1918 compatible application

**ANSWER: B**

**QUESTION NO: 6**

Which question should be in your predeployment checklist?

**A.** How often are backup jobs run?

**B.** Are any Linux servers being deployed?

**C.** Who are the users of the hosts on which you will deploy?

**D.** Which applications are installed on the hosts on which you will deploy?

**ANSWER: D**

**QUESTION NO: 7**

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: 8

Which option represents a configuration step on first use?

**A.** Verify, Contain, and Protect

**B.** User Account Setup

**C.** System Defaults Configuration

**D.** Event Filtering

**ANSWER: A**

## QUESTION NO: 9

Which statement describes an advantage of the FireAMP product?

**A.** Signatures are pushed to endpoints more quickly than other antivirus products.

**B.** Superior detection algorithms on the endpoint limit the amount of work the cloud must perform.

**C.** It provides enterprise visibility.

**D.** It relies on sandboxing.

**ANSWER: C**

## QUESTION NO: 10

Which statement is true about the Device Trajectory feature?

**A.** It shows where the endpoint devices have moved in your environment by displaying each IP address that a device has had over time.

**B.** A "plus" sign on the File Trajectory map indicates that you can execute the file inside FireAMP.

**C.** In the File Trajectory map, you can view the parent process for a file by selecting the infected system.

**D.** It shows hosts that display Indications of Compromise.

**ANSWER: C**