

# CAS-003<sup>Q&As</sup>

CompTIA Advanced Security Practitioner (CASP+)

## Pass CompTIA CAS-003 Exam with 100% Guarantee

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

<https://www.pass2lead.com/cas-003.html>

100% Passing Guarantee  
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



### QUESTION 1

An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user's accounts is sensitive, and therefore, the organization wants to comply with the following requirements:

Active full-device encryption Enabled remote-device wipe Blocking unsigned applications Containerization of email, calendar, and contacts

Which of the following technical controls would BEST protect the data from attack or loss and meet the above requirements?

- A. Require frequent password changes and disable NFC.
- B. Enforce device encryption and activate MAM.
- C. Install a mobile antivirus application.
- D. Configure and monitor devices with an MDM.

Correct Answer: B

---

### QUESTION 2

A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

- A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.
- B. A DLP gateway should be installed at the company border.
- C. Strong authentication should be implemented via external biometric devices.
- D. Full-tunnel VPN should be required for all network communication.
- E. Full-drive file hashing should be implemented with hashes stored on separate storage.
- F. Split-tunnel VPN should be enforced when transferring sensitive data.

Correct Answer: BD

Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked.

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate

file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

Full-tunnel VPN should be required for all network communication. This will ensure that all data transmitted over the network is encrypted which would prevent a malicious user accessing the data by using packet sniffing.

---

### QUESTION 3

A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization's users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

- A. OTA updates
- B. Remote wiping
- C. Side loading
- D. Sandboxing
- E. Containerization
- F. Signed applications

Correct Answer: EF

---

### QUESTION 4

A security researcher is gathering information about a recent spike in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.

Based on the information available to the researcher, which of the following is the MOST likely threat profile?

- A. Nation-state-sponsored attackers conducting espionage for strategic gain.
- B. Insiders seeking to gain access to funds for illicit purposes.
- C. Opportunists seeking notoriety and fame for personal gain.
- D. Hacktivists seeking to make a political statement because of socio-economic factors.

Correct Answer: A

---

### QUESTION 5

A regional transportation and logistics company recently hired its first Chief Information Security Officer (CISO). The

CISO's first project after onboarding involved performing a vulnerability assessment against the company's public facing network. The completed scan found a legacy collaboration platform application with a critically rated vulnerability. While discussing this issue with the line of business, the CISO learns the vulnerable application cannot be updated without the company incurring significant losses due to downtime or new software purchases.

Which of the following BEST addresses these concerns?

- A. The company should plan future maintenance windows such legacy application can be updated as needed.
- B. The CISO must accept the risk of the legacy application, as the cost of replacing the application greatly exceeds the risk to the company.
- C. The company should implement a WAF in front of the vulnerable application to filter out any traffic attempting to exploit the vulnerability.
- D. The company should build a parallel system and perform a cutover from the old application to the new application, with less downtime than an upgrade.

Correct Answer: C

[Latest CAS-003 Dumps](#)

[CAS-003 Study Guide](#)

[CAS-003 Exam Questions](#)