PassQueen
a.k.a dumpsqueen.com

CyberArk Defender - EPM

CyberArk EPM-DEF

Version Demo

Total Demo Questions: 8

Total Premium Questions: 85

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which capabilities can be managed using CyberArk EPM User Policies? (Choose two.)

A. Just-In-Time endpoint access and elevation

B. Access to removable drives

C. Threat intelligence source licensing

D. EPM Set creation and ownership

ANSWER: A B

Explanation:

Just-In-Time endpoint access and elevation and **access to removable drives** are correct. User Policies can apply endpoint controls in the context of users or user groups. Just-In-Time controls provide temporary administrative access or elevation without granting standing local administrator membership. Removable-drive controls allow organizations to govern user access to removable storage devices.

User Policies can also be used for controls such as filesystem and registry access, Windows Services access, and User Account Control monitoring. Threat-intelligence source configuration and EPM Set administration are managed elsewhere in the EPM console.

For current administration guidance, see the CyberArk Documentation Portal.

QUESTION NO: 2

What are the predefined application groups?

A. Developer group, Administrator group

B. Run as Administrator, Run as Developer, Block

C. Elevate, Allow, Block, Developer Applications

D. Block Only

ANSWER: C

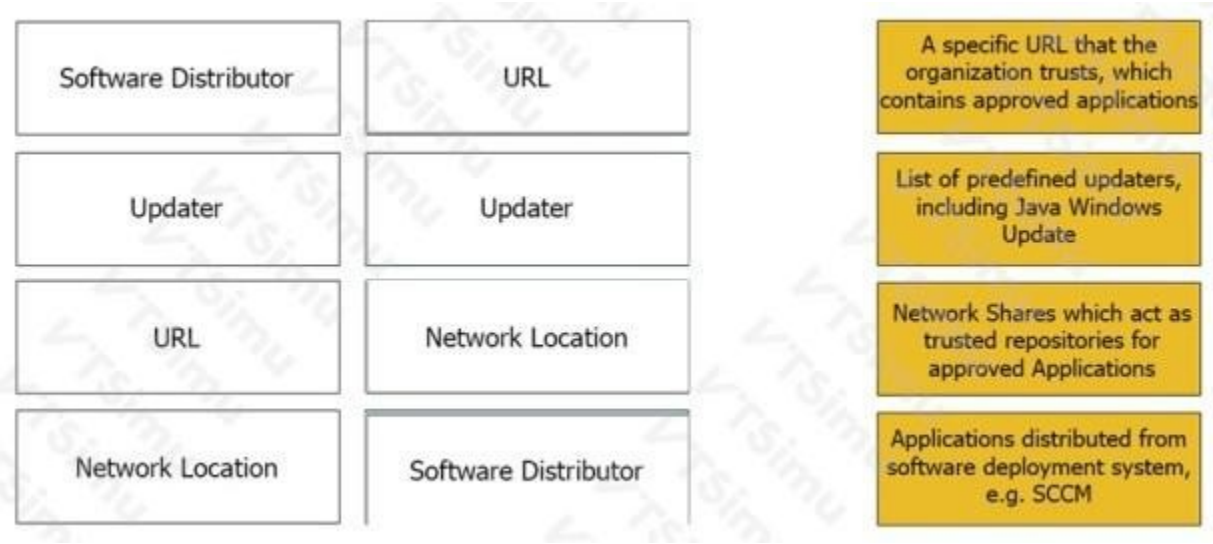
Explanation:

Elevate, Allow, Block, Developer Applications is correct because CyberArk Endpoint Privilege Manager provides these built-in application groups as the core classification categories for application control and privilege management. Administrators use them to define the intended treatment of applications: applications in the Elevate group can receive elevated privileges under policy control; Allow supports approved execution without elevation; Block identifies software that must not run; and Developer Applications supports development-related workflows where developers may require controlled access to tools and applications. These predefined groups provide a standard policy framework that can be used immediately and can be supplemented with custom application groups when an organization needs additional classification or targeting criteria. This organization lets EPM apply least-privilege principles while preserving productivity for approved business and development software. CyberArk's EPM documentation describes application-group management and the policy capabilities that use these groups to control application execution and elevation. See the CyberArk EPM application-group documentation and the CyberArk Endpoint Privilege Manager product page.

QUESTION NO: 3 - (DRAG DROP)

Match the Trusted Source to its correct definition:

ANSWER:



Explanation:

CyberArk EPM Trusted Sources identify recognized origins from which applications may be installed, updated, or otherwise treated as trusted under endpoint policy. The correct matches follow the type of origin represented by each trusted-source category. **URL** is the appropriate trusted source for a specific web address that the organization trusts and that hosts approved applications. This lets policy identify an approved application source by its exact online location.

Updater applies to a predefined list of recognized update mechanisms, including Java Windows Update. This trusted-source type is designed for legitimate software update activity, allowing approved updaters to deliver changes without being treated like unknown installation sources. **Network Location** applies to network shares used as trusted repositories for approved applications. In this case, the trusted origin is the shared network path from which the endpoint obtains the software.

Software Distributor applies when applications are deployed through an enterprise software-distribution platform, such as SCCM. The relevant trust is associated with the managed deployment channel, enabling centrally administered application rollouts to be recognized appropriately. Together, these mappings distinguish trusted web locations, update technologies, network repositories, and managed distribution systems so EPM policy can apply trust according to the actual delivery method. CyberArk's EPM documentation describes how application control and trusted sources support policy-based handling of authorized software: CyberArk Endpoint Privilege Manager documentation. Additional product context is available at CyberArk Endpoint Privilege Manager.

QUESTION NO: 4

When deploying EPM and in the Privilege Management phase what is the purpose of Discovery?

A. To identify all non-administrative events

B. To identify all administrative level events

C. To identify both administrative and non-administrative level events

D. To identify non-administrative threats

ANSWER: C

Explanation:

In the Privilege Management phase, Discovery is used to establish a complete picture of endpoint activity before privilege policies are finalized. Therefore, **To identify both administrative and non-administrative level events** is correct. EPM gathers event telemetry for applications, processes, installers, scripts, and user activity, including events that run with elevation as well as those executing in a standard-user context. This broad visibility matters because a least-privilege policy cannot be designed safely from elevated activity alone: standard-context events can reveal application dependencies, child-process behavior, and workflows that may later require controlled elevation or policy handling.

Discovery data enables administrators to understand which applications and tasks are in use, determine where elevated privileges are actually needed, and create appropriately scoped policies without unnecessarily disrupting normal user productivity. It supports the transition away from standing local administrative rights by supplying evidence for policy decisions, rather than making assumptions about application behavior. CyberArk describes Endpoint Privilege Manager as providing visibility and control over endpoint privilege use, which aligns with collecting activity across both privilege contexts during discovery. See the CyberArk Endpoint Privilege Manager documentation and CyberArk's Endpoint Privilege Manager product overview.

QUESTION NO: 5

Which statements describe appropriate uses of EPM Sets? (Choose two.)

A. Target an application-specific policy to computers that use the application

B. Apply a new policy to a pilot endpoint population

C. Store local administrator passwords for endpoints

D. Replace the EPM agent on unmanaged computers

ANSWER: A B

Explanation:

EPM Sets are centrally maintained groups of managed endpoints that can be used to scope policies. An administrator can use a Set to apply an application-specific Threat Protection policy only to computers where the protected application is installed. Sets can also be used to stage a new policy with a pilot population before expanding the policy to broader endpoint groups.

Using Sets supports controlled rollout, targeted enforcement, and simpler policy administration. A Set does not replace the need to define the policy action or application criteria; it defines the endpoint scope to which the policy applies. See the CyberArk EPM documentation.

QUESTION NO: 6

What are valid policy options for JIT and elevation policies?

A. Grant temporary access for all users, Policy name, Restart administrative processes in admin approval mode, Collect audit information

B. Grant temporary access for, Policy name, Terminate administrative processes when the policy expires, Collect audit information

C. Grant administrative access, Policy name, Log off to apply policy, Collect policy violation information

D. Terminate administrative services, Grant policy access for, Policy name, Collect audit reports

ANSWER: B

Explanation:

Grant temporary access for, Policy name, Terminate administrative processes when the policy expires, Collect audit information is correct because these are relevant configuration elements for CyberArk Endpoint Privilege Manager just-in-time access and elevation policy workflows. A policy needs a meaningful name for administration and reporting, and temporary access duration is fundamental to JIT access because privileges must be granted only for a defined, limited period. EPM can also terminate administrative processes when that period ends, preventing an elevated process from continuing after the authorized access window has expired. Collecting audit information provides the visibility required to investigate privileged activity, demonstrate accountability, and support compliance reporting. Together, these settings implement the core JIT principle of granting the minimum required privilege for the minimum required time while retaining an auditable record of activity. CyberArk describes Endpoint Privilege Manager as a platform for enforcing least privilege and controlling application elevation on endpoints. See the CyberArk Endpoint Privilege Manager product page and the CyberArk documentation portal for product documentation and administrative guidance.

QUESTION NO: 7

On the Default Policies page, what are the names of policies that can be set as soon as EPM is deployed?

A. Privilege Escalation, Privilege Management, Application Management

B. Privilege Management, Application Control, Threat Protection

C. Privilege Management, Threat Protection, Application Escalation Control

D. Privilege Management, Privilege Threat Protection, Local Privileged Accounts Management

ANSWER: B

Explanation:

Privilege Management, Application Control, Threat Protection is correct. CyberArk Endpoint Privilege Manager provides these default-policy areas so an organization can establish its initial endpoint security posture immediately after deployment. Privilege Management defines how users and applications receive elevated privileges, supporting least-privilege operations while allowing approved administrative tasks. Application Control establishes which applications are permitted to run and under what conditions, helping reduce exposure to unauthorized or untrusted software. Threat Protection applies endpoint-focused protections that identify and prevent risky behavior and malicious activity. Together, these policy categories cover the essential initial controls for elevation, application execution, and endpoint threat defense. Administrators can use the Default Policies page as a starting point, then tailor rules, exceptions, and targeting to their organization's users, devices, and operational requirements. CyberArk's Endpoint Privilege Manager documentation describes policy configuration and the available policy-management capabilities in the CyberArk EPM documentation. Additional product information is available on the CyberArk Endpoint Privilege Manager product page.

QUESTION NO: 8

An organization uses third-party antivirus and EDR products together with the EPM agent. Which configuration practices help avoid interoperability and performance issues? (Choose two.)

A. Add existing security application files to Files to Be Ignored Always

B. Add EPM agent components to the third-party security tool exclusions

C. Disable the EPM agent whenever antivirus scans run

D. Create an Elevate policy for every antivirus process

ANSWER: A B

Explanation:

CyberArk recommends adding the existing security product executables to **Files to Be Ignored Always** in EPM where appropriate. This reduces unnecessary processing of the security product by EPM.

The organization should also configure the third-party security tools to exclude the relevant EPM agent components. Reciprocal exclusions reduce the likelihood that antivirus or EDR software will block, quarantine, or repeatedly inspect EPM agent files and processes. Exclusions should be tightly scoped and maintained according to vendor guidance. See the CyberArk documentation portal and the CyberArk Support Portal.