

- Expert Verified, Online, Free.

■ MENU

Q

Microsoft Discussions

Exam AZ-900 All Questions

View all questions & answers for the AZ-900 exam

Go to Exam

EXAM AZ-900 TOPIC 1 QUESTION 249 DISCUSSION

Actual exam question from Microsoft's AZ-900

Question #: 249

Topic #: 1

[All AZ-900 Questions]

HOTSPOT -

You plan to implement several security services for an Azure environment. You need to identify which Azure services must be used to meet the following security requirements:

- **→ Monitor threats by using sensors**
- ⇒ Enforce Azure Multi-Factor Authentication (MFA) based on a condition

Which Azure service should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Monitor threats by using sensors:

Azure Monitor
Azure Security Center
Azure Active Directory (Azure AD) Identity Protection

•

*

Enforce Azure MFA based on a condition:

Azure Monitor Azure Security Center Azure Active Directory (Azure AD) Identity Protection

Azure Advanced Threat Protection (ATP)

Azure Advanced Threat Protection (ATP)

Show Suggested Answer

by \(\text{\text{\text{Success101}}}\) at \(Dec. 31, 2019, 11:11 \, a.m.\)

Comments

Type your comment...

Submit

☐ ♣ fgrion Highly Voted • 3 years, 5 months ago

guys, can you please comment only if you think an answer is wrong and why? reading 20 comments of people saying correct doesn't help at all and you always open it. let's put the comments to the minimum pls

upvoted 131 times

■ Jem12124321423 2 years, 11 months ago

Seeing something is correct helps too

upvoted 27 times

asas12321 3 years, 3 months ago

correct answer!!

upvoted 19 times

■ wmoras 11 months ago

correct

upvoted 1 times

□ 🏜 Nvoisn 1 year, 9 months ago

You are correct

upvoted 5 times

Load full discussion...

□ Success101 Highly Voted 4 years, 9 months ago

Both are correct.

Sources:

- 1. https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-architecture
- 2. https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

upvoted 48 times

"Azure ATP" and "Azure AD Identity Protection" is the answer.

https://learn.microsoft.com/en-us/defender-for-identity/what-is

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#azure-ad-mfa-registration-policy

Identity Protection can help organizations roll out Azure AD multifactor authentication (MFA) using a policy requiring registration at sign-in. Enabling this policy is a great way to ensure new users in your organization have registered for MFA on their first day. Multifactor authentication is one of the self-remediation methods for risk events within Identity Protection. Self-remediation allows your users to take action on their own to reduce helpdesk call volume.

upvoted 4 times

🗖 🚨 QBB 1 year, 11 months ago

Given answer is correct

upvoted 2 times

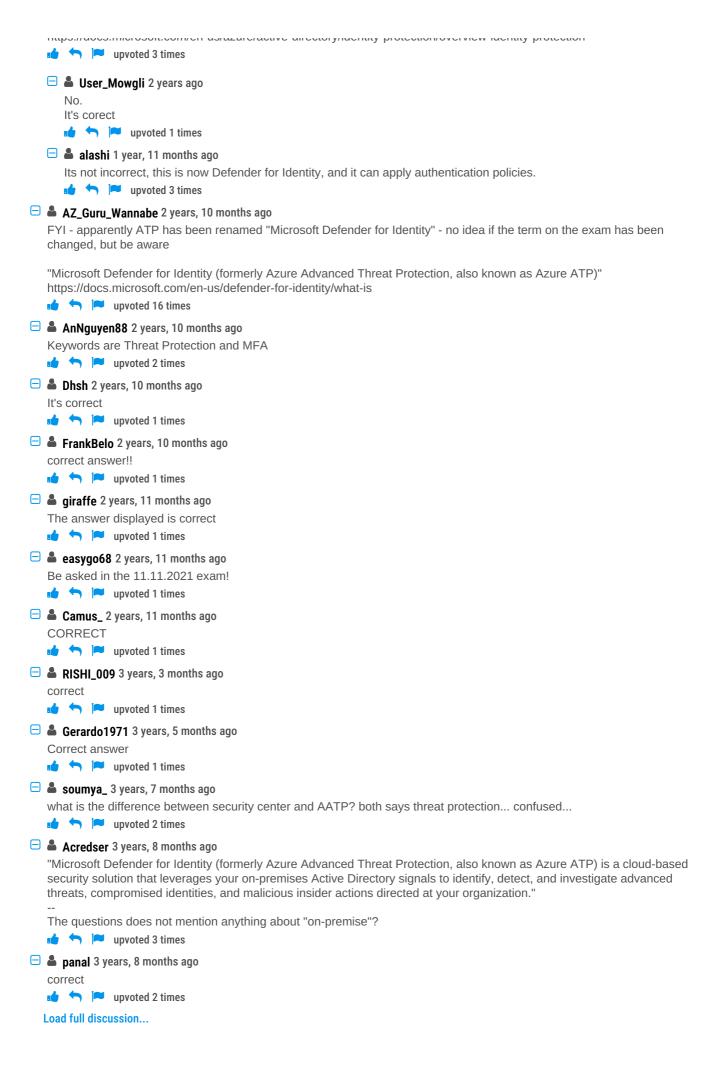
Contactfornitish 2 years, 7 months ago

Second one is INCORRECT.

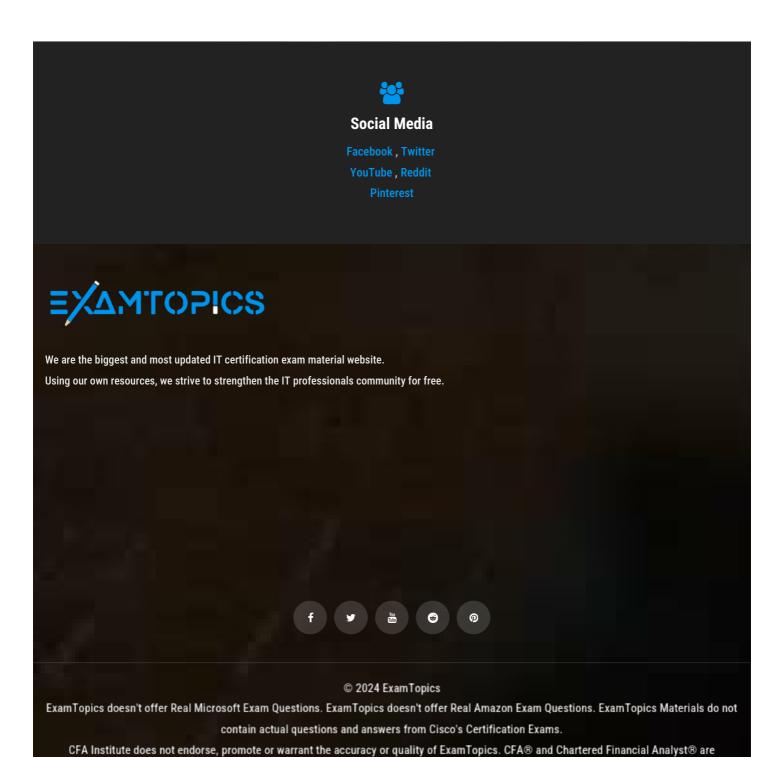
Identity protection does provide the info if something is risky or suspicious but alone it doesn't has anything to enforce. Conditional Access use that signal but conditional acces itself fall under Azure Security Center and NOT Identity Protection.

Saying to after managing conditional access policies for years

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection



Start Learning for free



registered trademarks owned by CFA Institute.