Microsoft Defender for Identity

examlabpractice.com

What is Microsoft Defender for Identity?

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

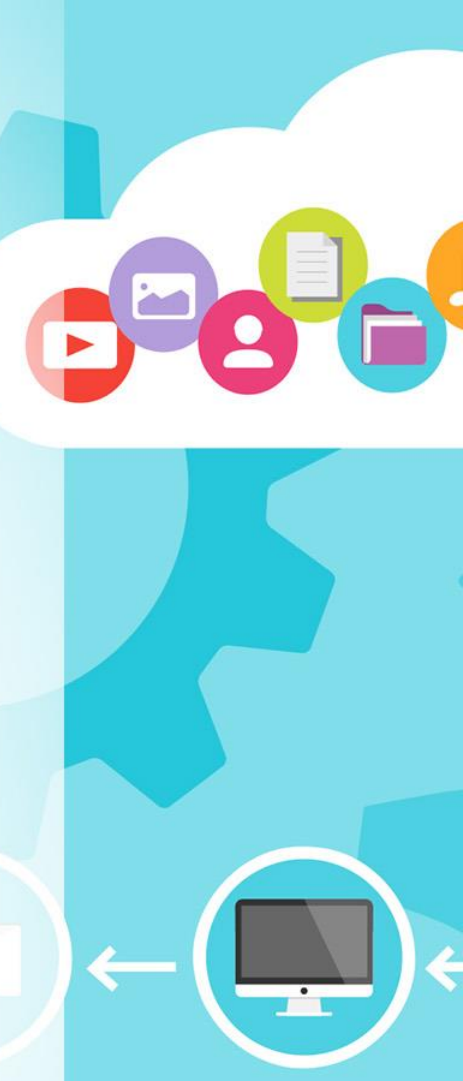
Monitor and profile user behavior and activities

Defender for Identity allows a Security Operations analysts and other security professionals struggling to detect advanced attacks in hybrid environments to:

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

Protect user identities and reduce the attack surface

- Defender for Identity provides you invaluable insights on identity configurations and suggested security best-practices.
- Through security reports and user profile analytics, Defender for Identity helps dramatically reduce your organizational attack surface, making it harder to compromise user credentials, and advance an attack.
- Defender for Identity's visual Lateral Movement Paths help you quickly understand exactly how an attacker can move laterally inside your organization to compromise sensitive accounts and assists in preventing those risks in advance.
- Defender for Identity security reports help you identify users and devices that authenticate using clear-text passwords and provide additional insights to improve your organizational security posture and policies.



Protecting the AD FS in hybrid environments

- Active Directory Federation Services (AD FS) plays important role in today's infrastructure when it comes to authentication in hybrid environments.
- Defender for Identity protects the AD FS in your environment by detecting on-premises attacks on the AD FS and providing visibility into authentication events generated by the AD FS.

Goals of monitoring attacks

Identify suspicious activities and advanced attacks across the cyber-attack kill-chain

- Reconnaissance
- Compromised credentials
- Lateral movements
- Domain dominance