
Defender for Cloud Apps
examlabpractice.com

What is Defender for Cloud Apps?

- Microsoft Defender for Cloud apps is a Cloud Access Security Broker (CASB) that supports many deployment types including log collection, API connectors, and reverse proxy.
- It provides control over data travel, and advanced analytics to identify and fight cyberthreats across all your Microsoft and third-party cloud services.

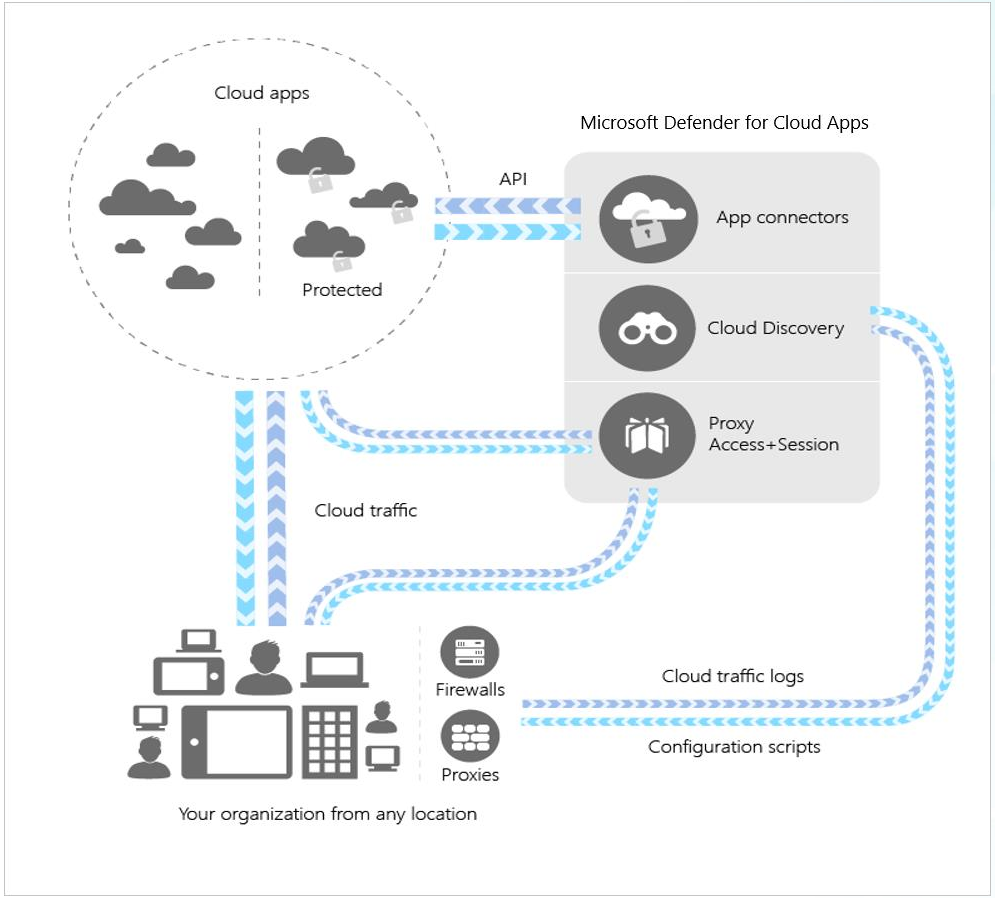
Defender for Cloud Apps Framework

- Shadow IT can be discovered and controlled: Discover the cloud apps, IaaS, and PaaS services used by your organization. Look into usage patterns, assess the risk levels and business readiness of over 16,000 SaaS apps against more than 80 risks. Start managing them to ensure security and compliance.
- Sensitive information can be protected anywhere in the cloud: Understand, classify, and protect the exposure of sensitive information. Leverage out-of-the box policies and automated processes to apply controls in real-time across all your cloud apps.
- Protect against cyberthreats and anomalies: Detect unusual behavior across cloud apps to identify ransomware, compromised users or rogue applications, analyze high-risk usage and remediate automatically to limit the risk to your organization.
- Assess the compliance of your cloud apps: Assess if your cloud apps meet relevant compliance requirements including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps, and limit access to regulated data.

Defender for Cloud Apps integrates visibility with your cloud by

- Cloud Discovery can map and identify your cloud environment and the cloud apps your organization is using.
- Sanctioning and unsanctioning apps in your cloud.
- App connectors can be deployed to take advantage of provider APIs, for visibility and governance of apps that you connect to.
- Conditional Access App Control protection can be used to get real-time visibility and control over access and activities within your cloud apps.
- Helping you have continuous control by setting, and then continually fine-tuning, policies.

Architecture



Policy Control

- Policies can be used to define users' behavior in the cloud.
- Use policies to detect risky behavior, violations, or suspicious data points and activities in your cloud environment.
- You can use policies to integrate remediation processes to achieve complete risk mitigation.
- Types of policies correlate to the different types of information you might want to gather about your cloud environment and the types of remediation actions you might take.