Plan for cloud workload protections using Microsoft Defender for cloud

Microsoft defender for cloud covers two broad pillars of cloud security:

**Cloud Security Posture Management (CSPM)**

Posture management features provide:

* Visibility – to help you understand your current security situation
* Hardening Guidance – to help you efficiently and effectively improve your security

**Cloud Workload Protection (CWP)**

Defender for Cloud offers security alert that are powered by Microsoft TI.

# Resources MDC can secure

Defender for cloud provides security alerts and advanced threat protection for VM’s, SQL databases, containers, web applications, your network and more.

When you enable defender for cloud from the **Pricing & settings** area the following defender plans are all enabled simultaneously and provide comprehensive defence for the compute data and service layers of your environment:

* Microsoft Defender for servers
* Microsoft Defender for App service
* Microsoft Defender for Storage
* Microsoft Defender for SQL server
* Microsoft Defender for Containers
* Microsoft Defender for Key vault
* Microsoft Defender for Resource Manager
* Microsoft Defender for DNS
* Microsoft Defender for open-source relational databases

# Hybrid Cloud protection

You can add defender for cloud capabilities to your hybrid cloud environment:

* Protect non-azure servers
* Protect your VM’s in other clouds such as AWS and GCP

In order to extend protection to VM’s and SQL databases in other clouds or on-prem, deploy Azure Arc and enable defender for cloud.

# Describe Microsoft Defender for cloud workload protections

Defender for cloud is a tool for security posture management and threat protection. It fills three vital needs as you manage the security of your resources and workloads in the cloud and on premise:

* **Continuously Assess –** understand your current security posture
* **Secure –** Harden all connected resources and services
* **Defend** – Detect and resolve threats to those resources and services

Features include

* **Secure score -** A single score that you can tell at a glance, your current security posture rating. Higher the score, the lower the risk identified.
* **Security recommendations –** Customised and prioritised hardening tasks to improve your posture. Fix button for automated implementation.
* **Security alerts –** Alerts appear in azure portal and defender for cloud can also send them by email.