Container Security

**In this overview, you learned about the core elements of container security in Microsoft Defender for Cloud. To enable the plan, see:**

**Overview-Container protection in Defender for Cloud**

Microsoft Defender for Containers is a cloud-native solution that designed to protect, monitor, Vulnerabilities assessment, security posture management and run-time threat protection for your entire containerized assets ( Kubernetes workloads, nodes, cluster, containers, registries and container images). across multi-cloud and hybrid clouds.

By offering continuous visibility and threat protection , it ensures that vulnerabilities, misconfigurations, and runtime risks.

This solution also integrates seamlessly with CI/CD pipelines.

Defender for containers assists you with four key areas:

1. **Security posture management** – it performs continuous monitoring of Cloud-APS’s and Kubernetes API’s and workloads. Provide comprehensive inventory management, detect misconfigurations and provide guidelines to reduce them.

* Detecting unauthorized external access to containers.

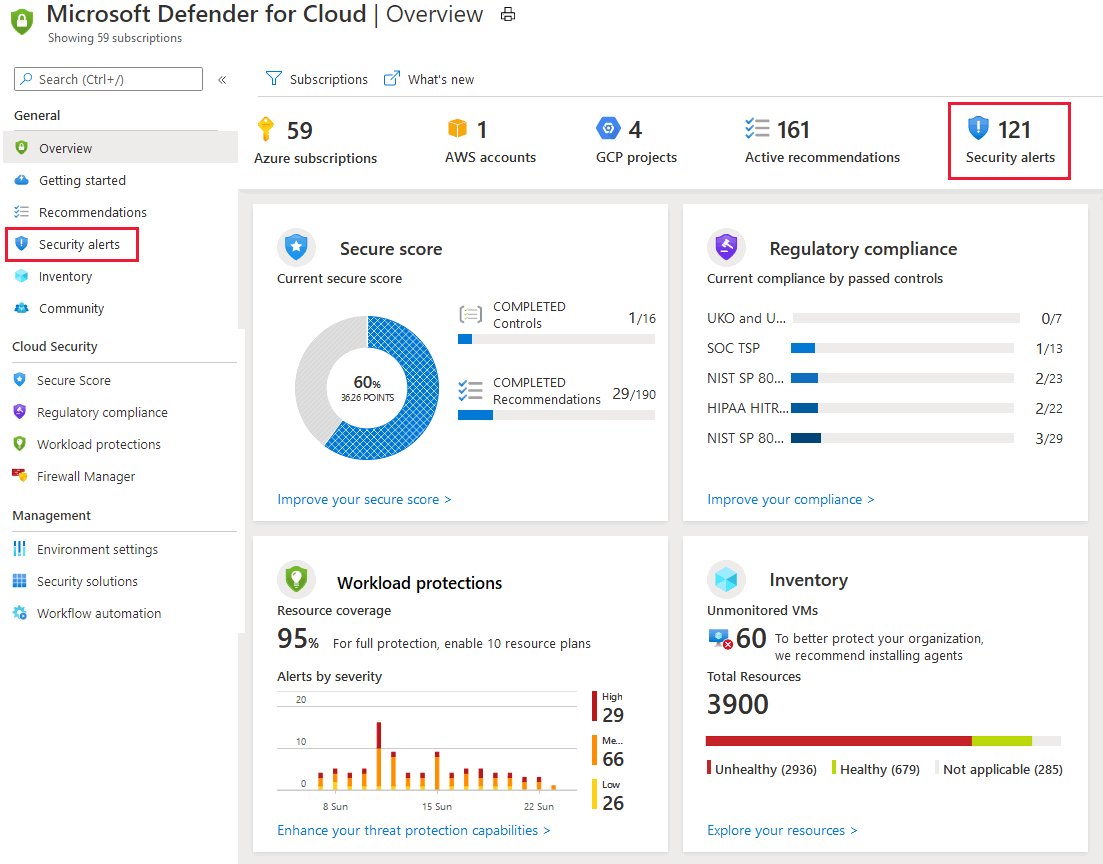
1. **Vulnerability assessment** – Defender for Containers scans the container images in ACR, ECR, and GCR with

* agentless vulnerability assessment for your container images,
* Including registry and runtime recommendations.
* Quick scans of new images and daily rescan.
* Insights of images reports.

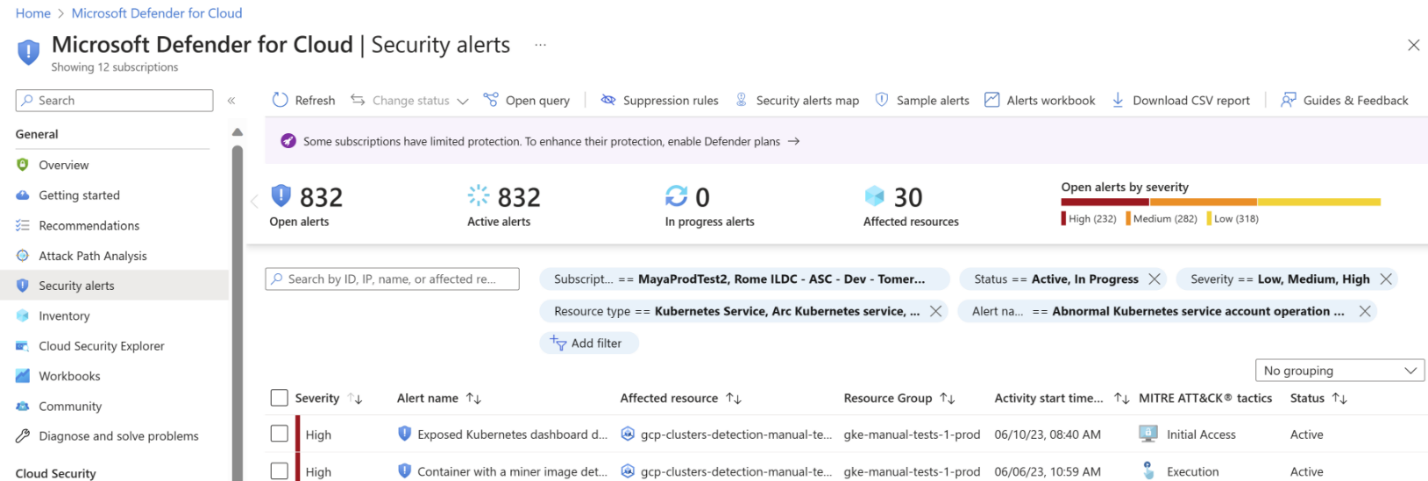
1. **Run-time threat protection** – this type of threat protection powered by Microsoft threat intelligence, and this best for containerized environments.

* Generates alerts for suspicious activities. You can use this information to quickly remediate security issues and improve the security of your containers.
* Threat protection is provided for Kubernetes at cluster level, node level, and workload level

You can view security alerts by selecting the Security alerts tile at the top of the Defender for Cloud's overview page.



The security alerts page opens:



Security alerts for runtime workload in the clusters can be recognized by the **K8S.NODE\_** prefix of the alert type.

Defender for Containers also includes host-level threat detection with over 60 Kubernetes-aware analytics