# Azure container security

In Microsoft Azure, there are many options for using containers. These options include Azure Container Services (ACS), Azure Kubernetes Service (AKS), and Azure Container Instances (ACI). AKS is a completely managed Kubernetes service. However, Kubernetes provided a ton of features that most tenants do not need. ACI provides a consumption based option for using containers. This is the perfect tool to spin up the container, run the scan, and discard the container after it completes. Tenants also have the option to deploy their own kubernetes instance for Azure. Microsoft provides several control plane tools for container registry and onboarding for tenants building their own docker images.

**Understanding Databricks within Azure Containers**

Databricks Container Services lets **you specify a Docker image when you create a cluster**. Some example use cases include: Library customization: you have full control over the system libraries you want installed. Golden container environment: your Docker image is a locked down environment that will never change. Databricks provided a higher level of control and security in maintaining the container's image.

**Securing a Kubernetes Cluster in AKS**

While cloud providers invest heavily in securing these multitenant platforms, it's long been seen as inevitable that unknown "zero-day" vulnerabilities do exist and put customers at risk of attack from other instances within the same cloud infrastructure.

Ensuring security in a Kubernetes cluster is no easy task. Fortunately, when choosing to use AKS, the tenant is less concerned about the right configurations in your cluster, as Microsoft takes care of a lot of things in the background. Yet, Microsoft, like many other PAAS and IAAS providers, has had their share attacks on successful exploits of their control and data plane.

## Known vulnerabilities that affected Microsoft Azure Container Security

An unprecedented cross-account takeover affected Microsoft's Azure Container-as-a-Service (CaaS) platform. Researchers named the finding Azurescape because the attack started from a container escape, a technique that enables privilege escalation out of container environments.

Discovery of Azurescape also underscores the need for cloud service providers to provide adequate access for outside researchers to study their environments, searching for unknown threats.

This discovery highlights the need for cloud users to deploy a "defense-in-depth" strategy to secure their cloud infrastructure that includes continuous monitoring for threats–inside and outside the cloud platform.

Microsoft took action to fix the underlying issues as soon as we reported. Azurescape attacks in the wild are common, but it is possible that a malicious user of the Azure Container Instances (ACI) platform could have exploited the vulnerability to execute code on other customers' containers, with no prior access to their environment.

Azurescape allows an ACI user to gain administrative privileges over an entire cluster of containers. From that point of the kill chain, the user could take over the affected several clusters to execute malicious code, steal data or sabotage the underlying infrastructure of other customers. The attacker could gain complete control over Azure's servers that host containers to several customers, accessing all data and secrets stored in those environments.

Azurescape also affected ACI containers in Azure Virtual Networks. They built ACI on multitenant clusters that host customer containers. Originally, those were Kubernetes clusters, but over the past year, Microsoft started hosting ACI on Service Fabric clusters as well.

## Do You Expect More Cross-Account Takeover Vulnerabilities to happen?

The rapid acceleration of the shift to the cloud that has occurred in the past few years has made these platforms a prized target for malicious actors. While we've long been focused on identifying new cloud threats, discovery of the first cross-account container takeover underscores the importance of that effort. It may not satisfy sophisticated attackers with targeting end users, and may expand their campaigns to the platforms themself to increase impact and reach.

### Is There Any Way I Can Prepare for Similar Vulnerabilities That Might Emerge?

They encourage cloud users to adopt a "defense-in-depth" along with engaging 3rd pen testers approach to cloud security to ensure breaches are contained and detected, whether the threat is from the outside or from the platform itself. A combination of 3rd party pen testing, defense-in-depth strategy security and container protection and anomaly detection presents the best chance of dealing with similar cross-account attacks.

### Performing a Pen Test after each Deployment of Azure Container Instances and Databricks.

Pen testing Azure containers with or without Databricks helps ensure that there are no security vulnerabilities hackers could exploit. Loading continuous scanning and pen testing tools within the container as a security test image is a splendid solution for incorporating these tests into your DevOps practices and Software Delivery Pipeline to perform a pen test on each deployment of your application.

Pen testing should include the following;

1. Validation and effectiveness of the Azure AKS container deployment.

2. *Validate the instances of  Databricks (if applicable) are secure and working.*
3. Validate the testing for endpoint security within the container image after enablement.
4. Validate the security on the client kubernetes instance
5. Validate the security test image with the tenants' VPC has not been compromised
6. *Continuous pen testing to validate any misconfigurations is no longer an issue*

Cloud security threats are genuine. Minimizing the number of components in your container image reduces the attack surface. In addition, minimizing the components in your container image also reduces the attack surface by limiting the number of things you need to patch.

- Use secure settings when creating new resources, set default values to a minimum. This helps prevent accidental exposure to sensitive information.
- Ensure your containers are hardened.

Recommend a 3rd party independent tester prior to enabling new containers or after the new gold images from Databricks has been deployed.