**Azure Container Security Best Practices**

Because container services have become one of the most important product offerings within Azure, it’s worth saying a few words about how to manage [container security](https://sysdig.com/blog/container-security-best-practices/) on Azure.

This is a complex topic because Azure provides several container services. The most notable include:

* **Azure Kubernetes Services (AKS)**, a managed Kubernetes service.
* **Azure Container Instances**, a managed container service that doesn’t require users to work with Kubernetes or another orchestration service.
* **Azure Red Hat OpenShift**, a managed OpenShift service. (OpenShift is based on Kubernetes, but is not identical to it.)
* **Azure Web App for Containers**, which lets users deploy containers quickly without having to manage orchestration or infrastructure themselves.

**Security recommendations for Azure Container Instances**

1. Use a private registry. ...
2. Monitor and scan container images. ...
3. Protect credentials. ...
4. Use vulnerability management as part of your container development lifecycle. ...
5. Scan for vulnerabilities. ...
6. Map image vulnerabilities to running containers.