Container Security for a Cloud Native World

The Cloud Native world has flipped security on its head, requiring innovative thinking and assembly of architectures that depart from traditional enterprise design methods. Over the years, many development professionals became complacent with static, perimeter-based networking. This architecture has evolved into security models which safeguard dynamic server clusters whose IP Addresses constantly change.

Top 5 Security Concerns

Here are the main container security challenges that enterprises should be aware of.

1 Kernel Exploits

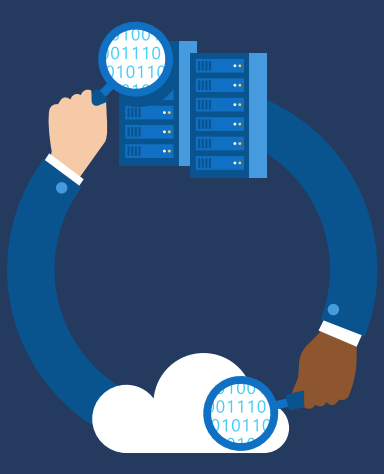
Unlike in a VM, the kernel is shared among all containers and the host. This sharing magnifies the importance of any vulnerabilities in the kernel.

2 Denial-of-Service Attacks

If one container can monopolize access to certain resources—including memory and user IDs—it can starve out other containers on the host, resulting in a denial of service.

3 Container Breakouts

You need to prepare for potential privilege escalation attacks, whereby a user gains elevated privileges such as those of the root user.



4 Poisoned Images

If an attacker can trick you into running an image, both the host environment and your data are at risk.

5 Compromising Secrets

An attacker who can get access to an API key or username and password will also gain access to databases or services used by the container.

Secure Your Containers on Azure

Download our comprehensive guide to securing Azure Kubernetes Service environments. We take an outside-in perspective to address the most pressing security challenges while adhering to key security principles that organizations follow today.

Get the guide

Microsoft