What You Should Know About Containers Threats in Cloud Computing?

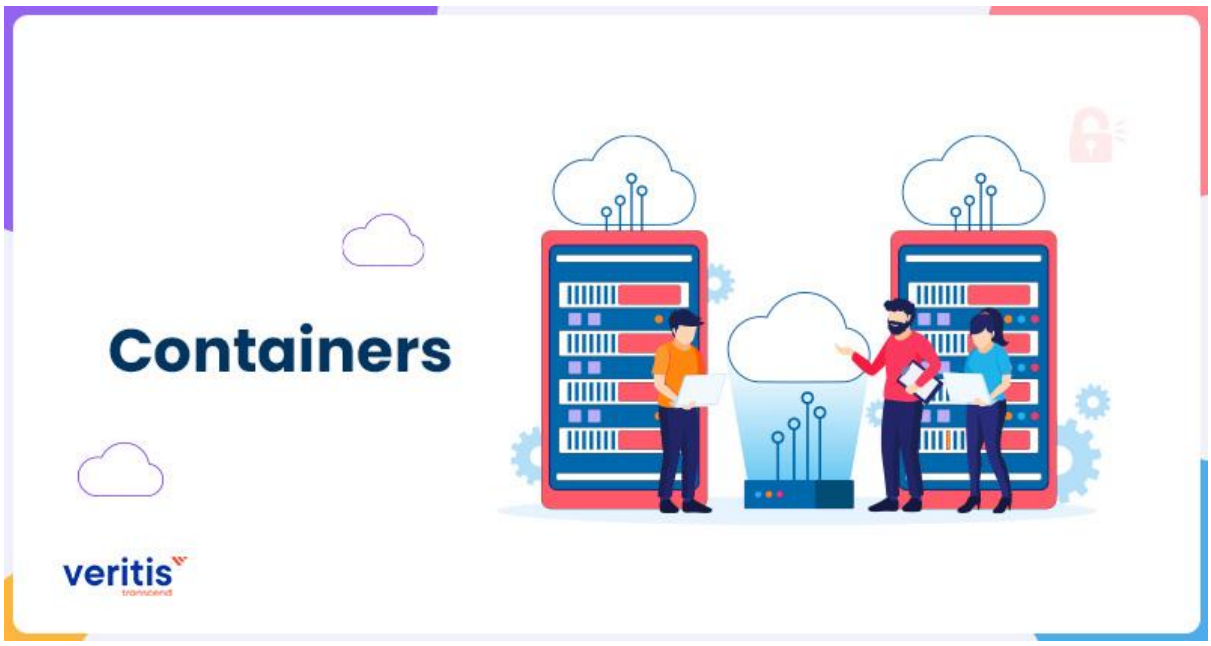
Containers are now prevalent across the IT industry. They are easy to maintain, and due to various advantages facilitating swift development and deployment, DevOps users are harnessing the containers for developing iterative updates.

Unfortunately, while containers are being used for positive purposes, their prevalence has attracted the unwanted attention of the treacherous people who would be willing to exploit the threats. In this blog, we shall explore the threats you should become aware of while using containers in the cloud.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

About Containers



Containers are independent pods that stand in complete, transportable application environments. They include all the binaries, libraries, configuration data, and a program requires to run. Some standard technology offerings you hear when containers are mentioned are Docker, Kubernetes, and AWS EKS. With its massive global footprint, containerization technology in AWS is widely used.

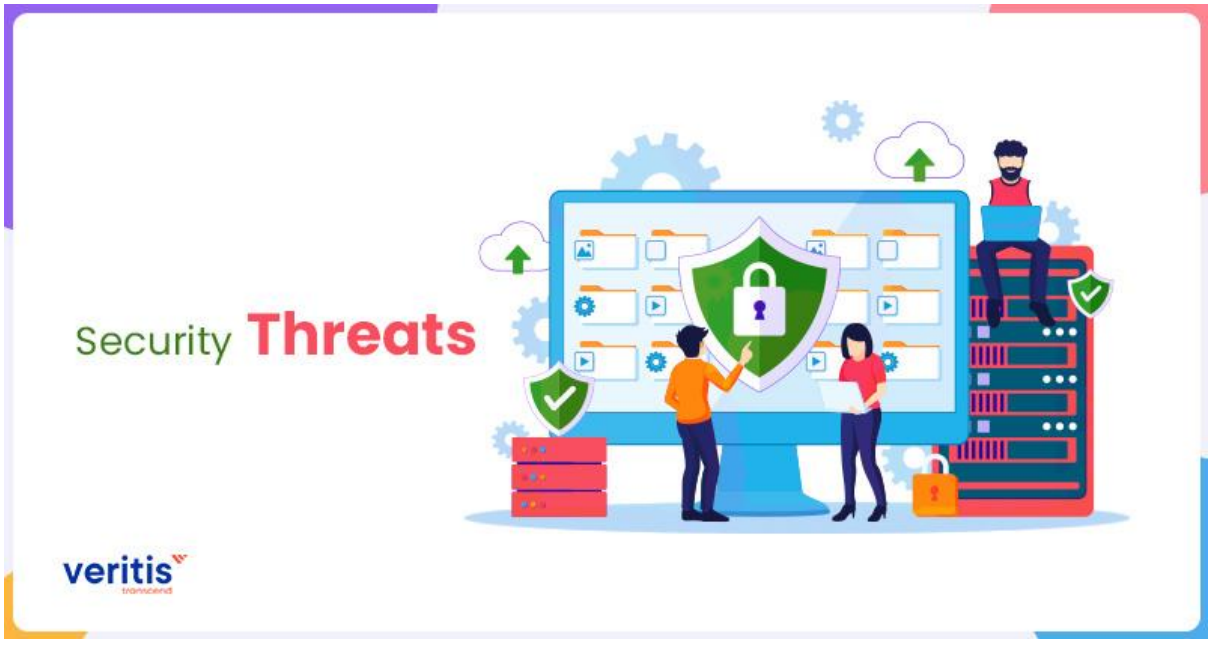
Several containers running on shared infrastructure can use the same kernel without any modifications. Still, they are isolated from it and have limited interaction with the hosting resources below. One of the many advantages of operating cloud-based containers is the capacity to spin up and down programs for users quickly (think “write once, run everywhere” – a huge boon for businesses managing pandemic-related distant footprints). Compared to administering applications on owned-and-operated servers or virtual machines, they also provide significant infrastructure cost benefits. They also boost agility by advancing DevOps objectives.

Additionally, containers are simple to manage because of orchestration tools like Kubernetes. Administrators may utilize orchestration to centrally manage container-based apps, rolling out automated updates and isolating any problematic containers, among other things.

Due to these reasons, the usage of containers has hit the roof. ‘According to a survey conducted by the Cloud Native Computing Foundation (CNCF), 83% of respondents were using Kubernetes in production in 2020, up from 78% in 2019 and just 58% in 2018. Cybercriminals get more interested as adoption rises.’

A staggering 94% of respondents to a June Red Hat study reported having had a **Kubernetes** security problem in the preceding 12 months.

Security Threats



Akamai security researcher Larry Cashdollar recently set up a straightforward Docker snare to see the attention it may garner from the more extensive web’s army of criminals as an illustration of how popular attacking weak cloud infrastructure has become. Alarmingly, in 24 hours, four distinct criminal operations employed the honeypot.

Cashdollar had set up the SSH protocol for encryption and a root password that was “guessable.” He said that it was disguised adequately so that it didn’t bear the

semblance of a honeypot since it was using a typical cloud container architecture. Instead, it would only appear to be a weak cloud instance.

The attacks had various goals: one campaign tried to use the container as a proxy to access Twitch live streams or other services, another tried to infect a botnet, another mined cryptocurrency, and the last effort was to fake a work-from-home.

Useful link: Cloud Computing: Trends, Challenges and Benefits

---

Configuration Flaws

While there are many ways that container technology, like other forms of infrastructure, can be hacked, misconfiguration tops the initial-access scoreboard. A new **Gartner** report predicts that until 2025, client errors or misconfigurations will be the primary cause of more than 99 percent of cloud breaches.

For instance, an image can start an unnecessary daemon or service that permits unauthorized network access, or it might be set up to operate with higher user rights than are required. Another risk to be aware of is secrets included in pictures, such as credentials or certificates. The **National Institute of Standards and Technology (NIST)**, a US Department of Commerce division, advises obtaining images only from reliable sources, such as private container registries.

If the registry is not correctly set up, it might become a potential security gap. Registry access should only be possible through encrypted and verified connections, ideally using credentials federated with already-in-place network security measures. If the registry is vulnerable, all container image security measures may be useless. Additionally, regular registry maintenance is necessary to ensure that no outdated pictures with unpatched vulnerabilities are included. Let’s delve deeper into the misconfigurations.

In addition to configuration errors, threat actors can access cloud deployments through compromised credentials, malicious containers, and holes in any layered software.

Organizations have suffered losses due to actual assaults, both financially and otherwise.

Cryptojacking, in which threat actors utilize a company's cloud computing processing capacity for illicit cryptocurrency mining, can chew up resources and increase network traffic, both of which the company will be penalized for.

Complexity is another threat to containerization. While complexity itself is not a security threat, not knowing what a container entails is a problem that can invite potential security threats.

When it comes to the cloud, On-premises networks' security infrastructure is not available for cloud deployments. Finding comprehensive security solutions in the cloud is challenging due to the variety of its offerings.

Cloud administrators are always expected to think about safeguarding a hybrid environment. The difficulty comes from the fact that there are several ways to secure cloud security and that different cloud deployment strategies have different risks.

This, in turn, depends on the particular requirements of cloud users and their level of risk appetite or willingness to accept risk. Because of this, performing a risk assessment is a crucial task that cannot be copied verbatim from published best practices or compliance.

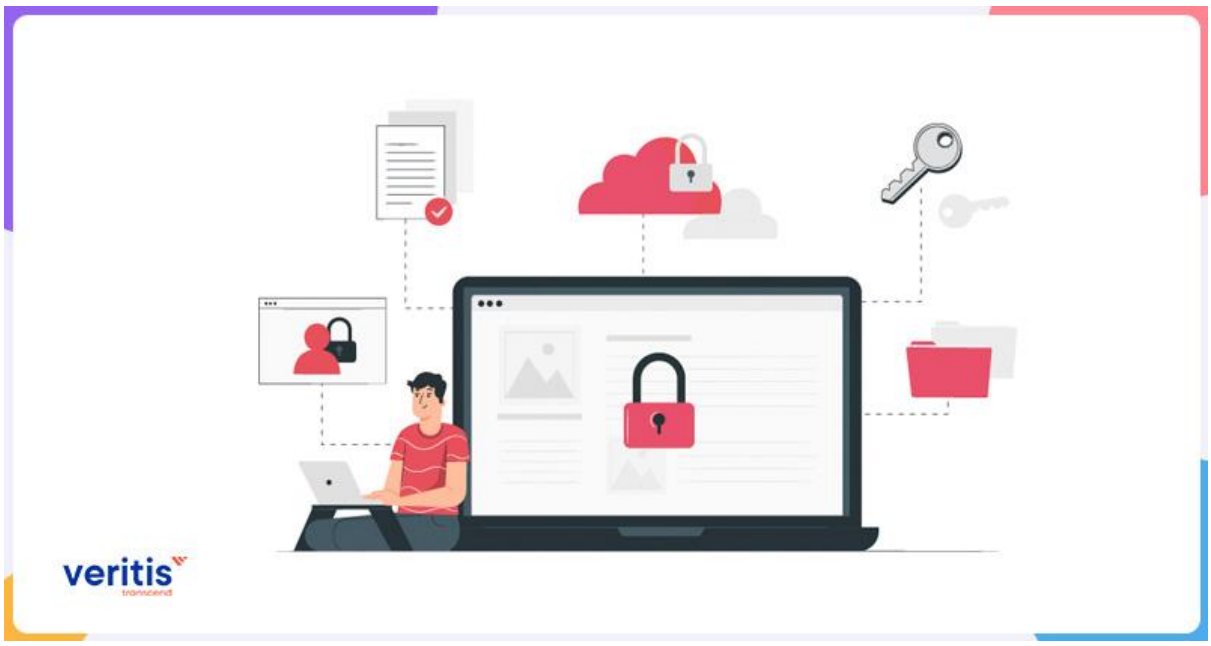
Useful link: Multi-cloud, the Future of Enterprise Cloud Computing

---

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

Preliminary Solutions



Cloud users should take advantage of the chance to design their cloud deployments effectively enough for security to be incorporated from the beginning when they get into the intricacies of their cloud needs to avoid the dangers and risks outlined in the previous section.

IT teams may reliably handle present and future cloud deployments by safeguarding each of the areas listed below as appropriate. These are in line with Gartner's market guide for cloud workload protection platforms.

- Securing the Network: Network traffic inspection, a crucial component of the security jigsaw, may serve as the first line of defense against zero-day attacks and exploitation of security flaws, and it can fend off threats by virtual patching. The critical problem for a cloud firewall, whether deployed in a virtual private cloud or a cloud network, is the ability to deploy the firewall without interfering with network connections or running applications.

- Use DevOps: In recent years, the container has grown to dominate the software unit in cloud computing services. However, it may be challenging to reproduce a computer environment when, for example, specific codes, tools, system libraries, or even software versions must be in a particular manner. Using containers

assures that software can operate dependably well independently of the natural computing environment.Images, like Docker images, are used by containers to execute programs. Therefore, every instance of an application running on it may be in danger when users download malicious or insecure images submitted to public libraries like Docker Hub. By analyzing images, safeguarding the container runtime, and isolating resources, developers should include security as early as feasible.

- Ensure Governance: Organizations collecting, processing, and storing data, especially in the cloud, must consider the economic effects of laws like the Health Insurance Portability and Accountability Act (HIPAA), industry standards like the Payment Card Industry Data Security Standard (PCI-DSS), and data privacy regulations like the General Data Protection Regulation (GDPR).Cloud administrators must strike a balance between these compliance obligations and the advantages of cloud agility. Enterprises should use security technology to ensure that their deployments follow security best practices; otherwise, unintentional infractions might result in fines that rapidly offset any cost savings.

Conclusion

Containers are now part of our innovative production processes. The solutions suggested here are just some general practices that would only provide initial protection against the threats. The problems here are just the tip of the iceberg, and one should waste any moment securing their containerized solutions.

Reach out to the Stevie Award winner Veritis to secure your containers. Renowned for DevOps excellence, we have provided customized solutions to clients based on their unique needs. Reach out to us and secure your solutions.

Services

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com