cavirin

# CAVIRIN SOLUTIONS FOR CONTAINER SECURITY

## CONTAINER HARDENING

*Containers make tooling and environments consistent by providing common building blocks reusable in any development stage. These building block are known as images, and contain the functionality of an OS but depend upon the host for all system calls. For tools, containers provide a disposable, reusable unit that modularizes the delivery pipeline. For environments, they extend the write once-deploy anywhere abstraction to infrastructure. - Codenvy*

Container security extends into all aspects of the container ecosystem, and not just to the well-known registries like Docker or those offered within the cloud service providers. Securing a container deployment may include best practices for companies supporting: the developer workspace, continuous integration, build automation, testing frameworks, release automation, and operations tools.

In parallel, the DevOps team is now working with a larger number of vendors, many previously unknown. This implies greater training, and those new to the container ecosystem sometimes make simple mistakes. For example, running production containers as root. There have been many articles written about Docker security concerns, with one of the best by O'Reilly, 5 Security Concerns When Using Docker. More importantly, an infographic from Container Solutions describes best practices in dealing with these concerns, while Assessing the Current State of Container Security at The New Stack provides additional background.

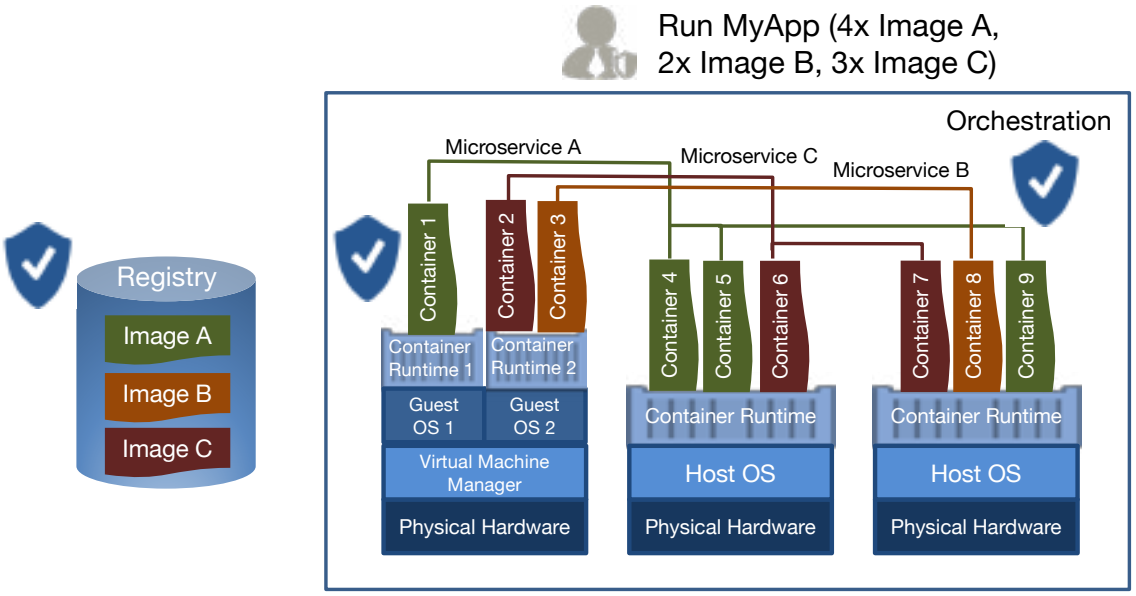
Any security solution must keep track of what VMs or bare-metal servers have what workloads, when they start and stop, and then apply frameworks appropriate. And it is not just a one-time analysis. The system must continually scan all images running in production, and also address the access control issues described above.

Given that developers may download public images, they must ensure that these are secure. Docker Hub may be one thing, especially when combined with Docker Security Scanning, but some unknown open-source site may expose the developer to risk, no different than when downloading laptop software from an unknown site. The Morning Paper's article A study of security vulnerabilities on Docker Hub. provides a detailed analysis of the types of vulnerabilities found in both community and official images. A more recent analysis by Federacy states that 24% of Docker images have significant vulnerabilities.

A good approach is to use CI/CD tools to properly embed security best practices across the container lifecycle. Doing this creates a baseline that reduces the need for additional efforts and reducing the chance that security will become a barrier. And, via this baseline, IT is able to detect threats in real-time with a lower false-positive rate. This also has an effect of moving security upstream, integrated earlier in the software delivery pipeline. In DevOps-speak this is known as a shift-left.

Based on what the system detects, active remediation may include additional logging, implementing additional isolation, or even deleting the container. This must all be automated and under control of the security management platform.

Eighty-eight percent of enterprises say they're shifting to a DevOps strategy, and containers are changing the nature of DevOps and transforming infrastructure." - Betanews




Container Security Touchpoints - Registry, Container, and Orchestration

## CONTAINERS AND THE HYBRID CLOUD

Containers, if properly secured, will have a major beneficial impact on how organizations deploy in a hybrid cloud environment, both on-premise and across multiple CSPs. They provide improved portability and application integration, effectively abstracting the lower-layer cloud architecture. They allow users to separate and isolate a single application, creating a boundary at the app level rather than at the server level. Especially popular with developers, it allows for testing without affecting other applications, servers, or data. Containers can be individualized with their own sys admins and users.

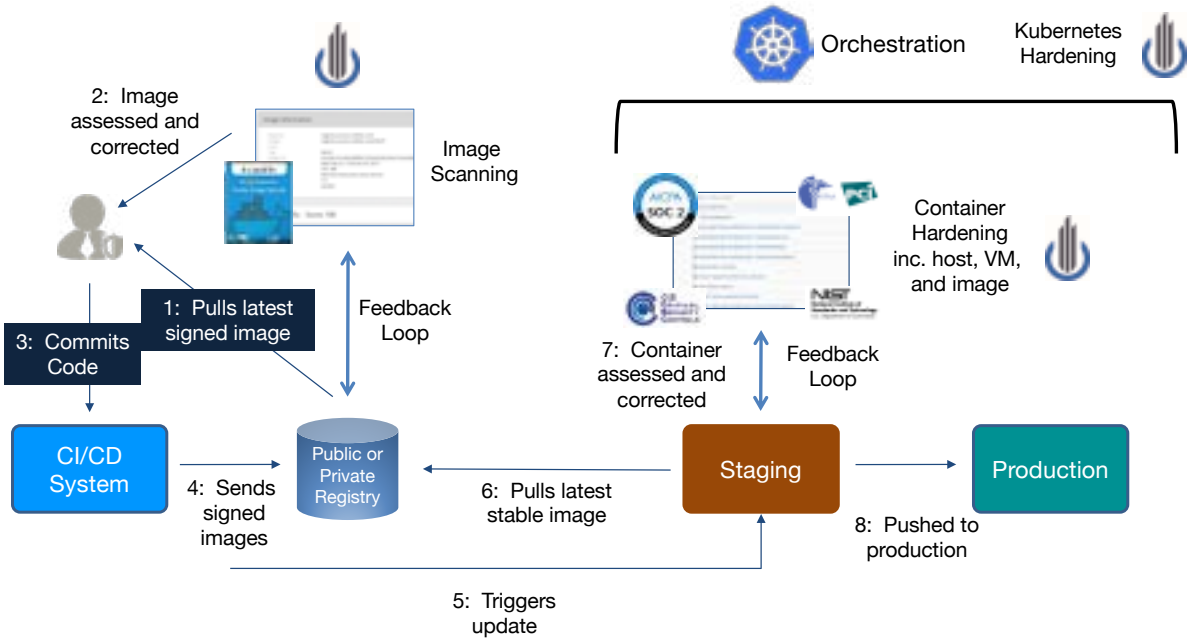
In a hybrid cloud environment where users want the ability to easily work and share data across platforms, containers allow for the following, according to Tech Target: “First, it provides a layer of abstraction between the containerized application and the native cloud platform on which that application runs. Second, this abstraction from the underlying cloud platform allows applications to move more easily from one cloud environment to another, including between private and public clouds.” This is very critical for enterprises adopting a multi-cloud architecture, or just deploying across a private cloud and a single CSP. If the organization implements lifecycle container security, they are well on their way to a secure hybrid environment.

## THE CAVIRIN SOLUTION

Cavirin has various ways to check risk, security, and compliance of a container based application. The risk and compliance of the Docker host can be scanned against industry standards like HIPAA, PCI, SOC2, NIST, and many others. The risk and security of a host, Docker engine, and container can be checked against Docker Benchmark by Center for Internet Security (CIS). Cavirin's implementation is certified by CIS.

Cavirin performs two types of analysis. The first, image scanning, looks at things within the Docker image such as security baselines and whether the system has been patched via the Patches and Vulnerabilities policy pack. Next, Docker Benchmarks apply to the host, the containers, and a few apply to the images as well. Cavirin also secures container orchestration by initially supporting the CIS Kubernetes Benchmark, with more to come.

In the diagram below, the engineer first pulls an image from the registry (1). This image is immediately scanned (2) and remediation invoked. The image is changed (3), and then uploaded back to the registry (3), now clean. The container runtime is made aware of changes (5), and pulls the new image(s) (6). Now, the con4ainer is checked against the benchmarks (7), and remediation taken. Finally, the container is pushed to production (8).




Based on the assessment, the Cavirin platform suggests remediation actions of the customer's production Docker container environment. This includes any necessary configuration management changes, security actions, and process recommendations that are to be implemented on a continuous basis. Ultimately, Cavirin mitigates the risk of:

- Kernel exploits
- Compromising secrets
- Polluted images
- Denial-of-service attacks
- Container breakouts


Cavirin has been in the forefront of container support, co-authoring the recently announced CIS Docker 1.13 Benchmark as well as announcing a leadership role in crafting the GCP Kubernetes Benchmark.

Separate from only securing the Docker environment, Cavirin also plays a role across the ecosystem. As an example, on AWS's EC2 container service, we can assess whether the executing containers are meeting the CIS benchmark requirements or not. In addition, Cavirin can integrate with the CI/CD pipeline and ensure that AWS hosted Docker Images have:

1. Secure baselines, and
2. Patched Vulnerabilities.

Companies such as VMWare or Red Hat provide Container Execution platforms (Red Hat Atomic or VMware Photon), and Cavirin can conduct host, image and container assessments.

Resources:

- Cavirin blog on Docker security
- A good backgrounder on the state of container security is here.


## ABOUT CAVIRIN

Cavirin provides continuous security assessment and remediation across physical, public, and hybrid clouds, supporting AWS, Microsoft Azure, Google Cloud Platform, VMware, KVM, and Docker. The company's solutions offer continuous visibility, are agentless and multi-tenant, and scale to the largest physical and virtual infrastructures. They offer up-to-the-minute compliance assessments, supplying audit-ready evidence as measured by every major regulatory and security best practice framework including CIS, DISA, PCI and HIPAA. With Cavirin, companies are empowered to make the right decisions faster and de-risk their cloud migrations.