Container Security

Jiayu Pan and Rishit Saiya

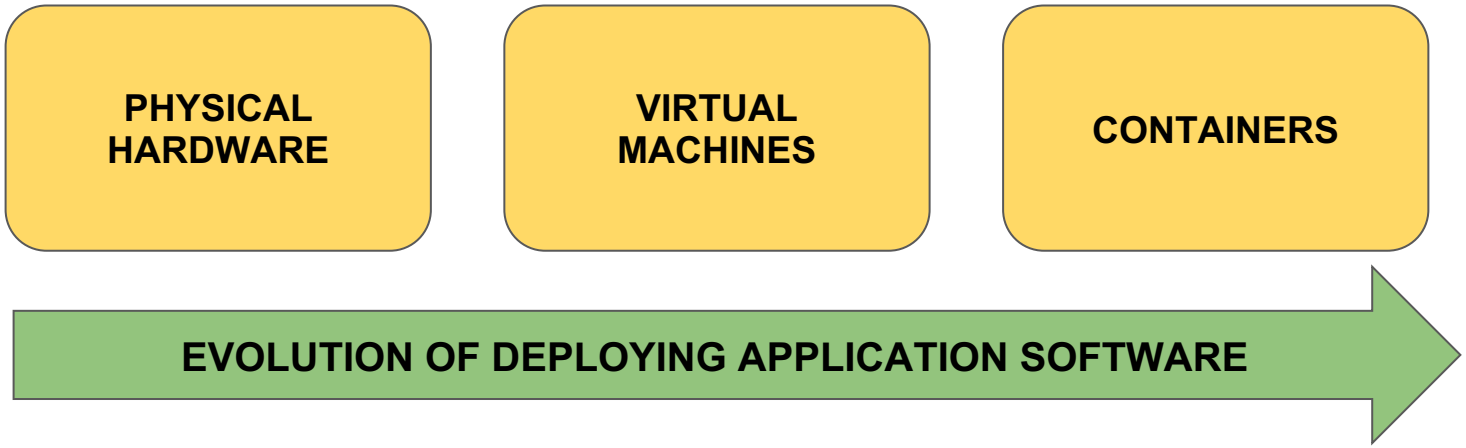
USC Viterbi
School of Engineering

University of Southern California

Overview

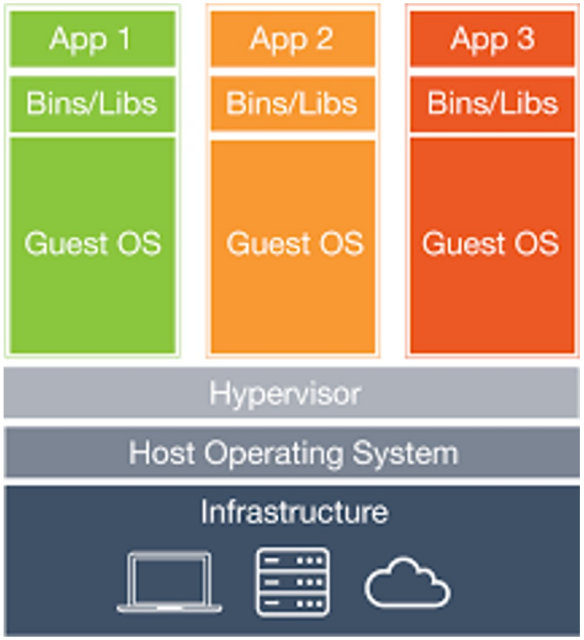
- Containers are packages of software that contain all of the necessary elements to run in any environment that smoothen the application development pipeline and they can be deployed anywhere. In this way, containerization makes deploying software efficiently, and operate at an unprecedented scale.
- Containers require less system resources than traditional or hardware virtual machine environments because they don’t include operating system images.
- Applications running in containers can be deployed easily to multiple different operating systems and hardware platforms. Containers allow applications to be more rapidly deployed, patched, or scaled.

Evolution

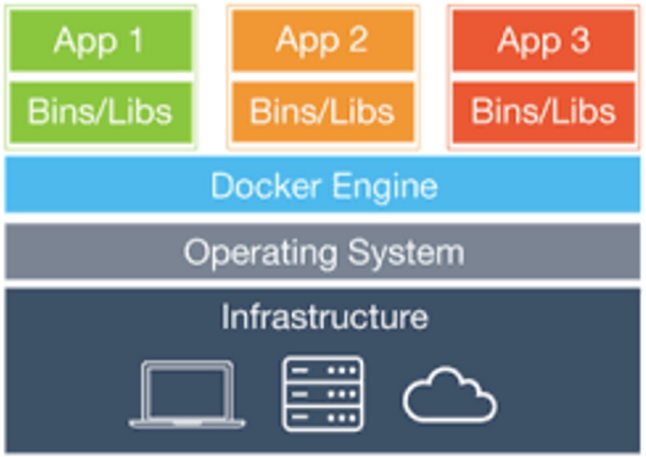

PHYSICAL HARDWARE
VIRTUAL MACHINES
CONTAINERS
EVOLUTION OF DEPLOYING APPLICATION SOFTWARE

Benefits of Containers

- Eliminating Friction
- Epicenter Approach
- Quicker Build Times
- Compatibility across OS
- VCS of Deployment



Virtual Machines



Containers

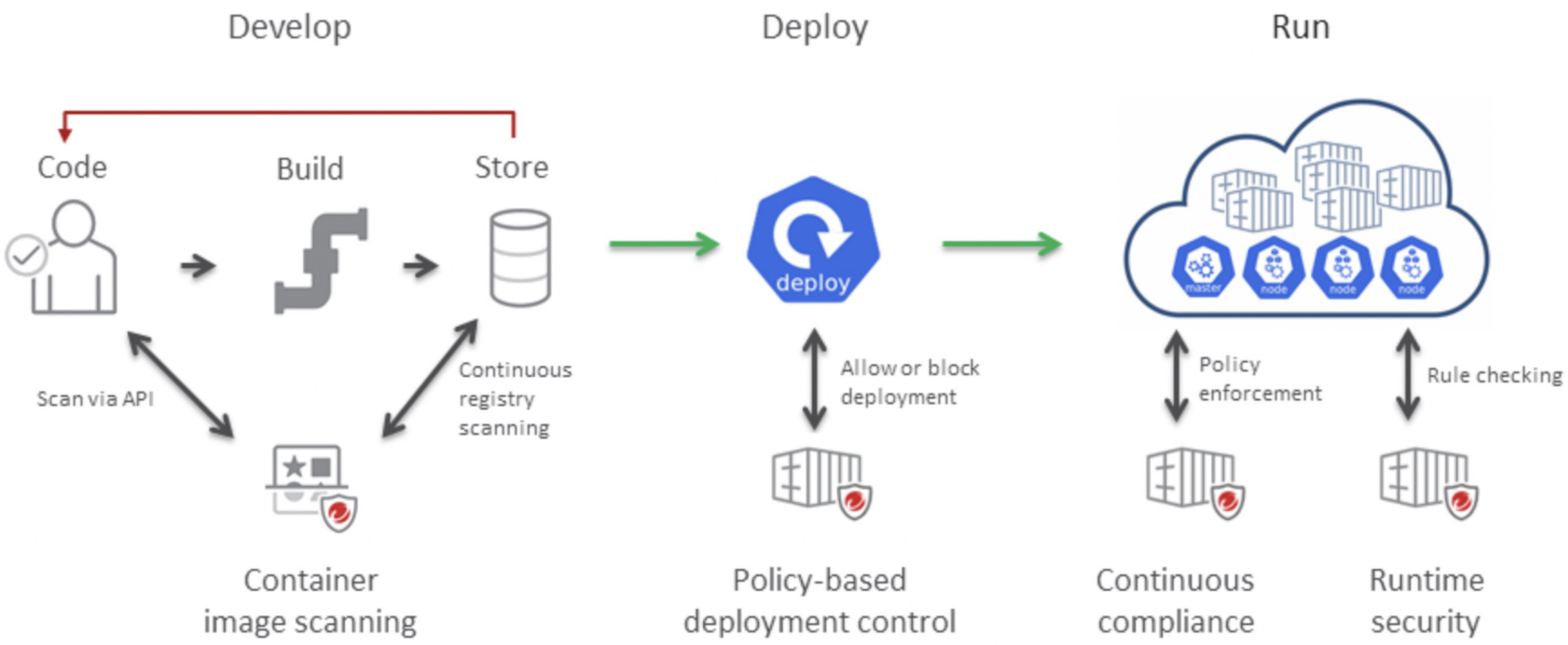
What is Container Security?

- Process of implementing tools and policies to ensure that container infrastructure is safe from potential breaches.
- The poignant event in terms of technological architectural advancements.
- Container: It is a file/package which encapsulates required environment to run the application.
- SDLC has become lighter, simpler, faster, and more powerful than ever.

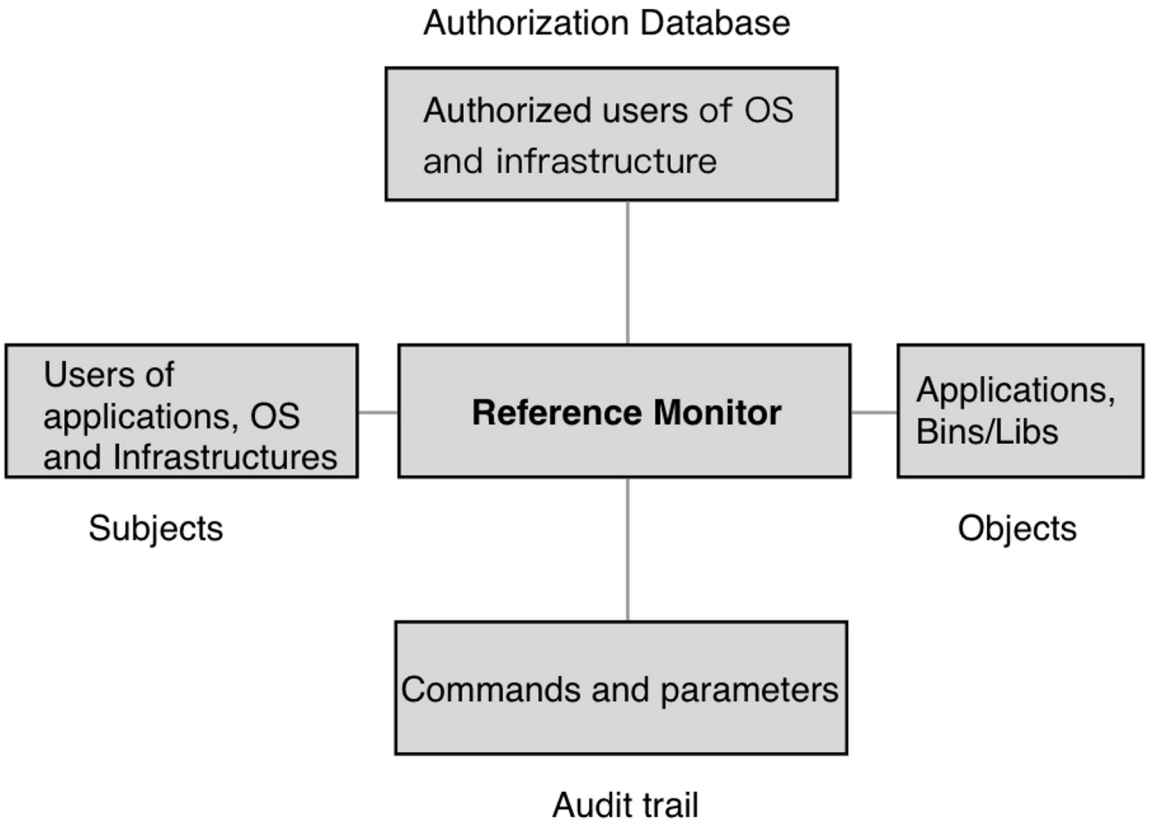
Why Container Security is important?

- With the rise of cloud computing and the sophistication of application development technologies, developers have grown tired of dealing with OS and application dependencies of virtual machines. The adoption of containers and container orchestration platforms, like Kubernetes and Docker, is the result of two factors: a demand for accelerated time-to-market enabled by DevOps, and a desire for application portability across clouds.
- The container ecosystem can be difficult to understand, given the plethora of new tools and the unique problems they solve compared to traditional platforms. At the same time, the rapid adoption of container technologies creates an opportunity to shift security left, securing containers from development to the CI/CD pipelines to runtime, and build bridges between development and security teams.

How it Works?


Develop
Deploy
Run
Code
Build
Store
deploy
master
node
node
node
Scan via API
Continuous registry scanning
Allow or block deployment
Policy enforcement
Rule checking
Container image scanning
Policy-based deployment control
Continuous compliance
Runtime security

Reference Monitor



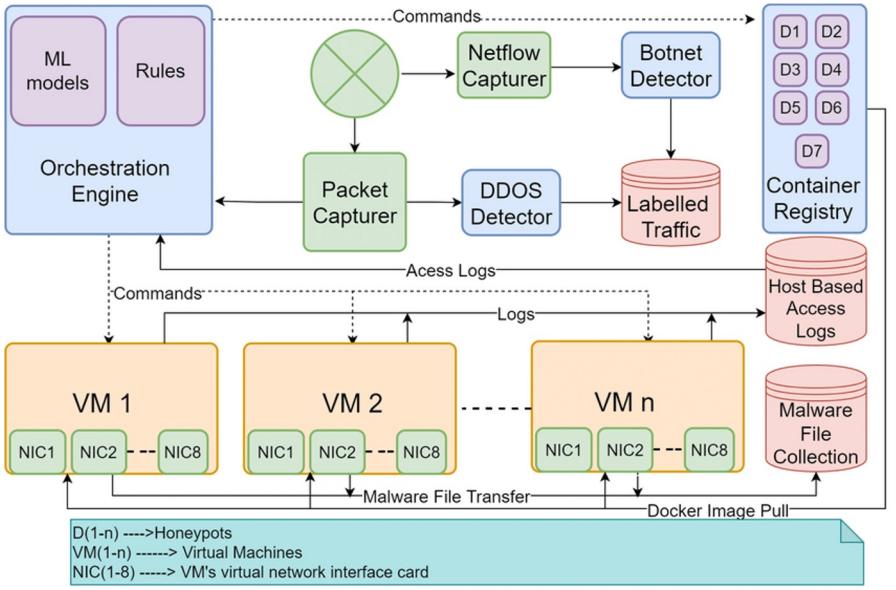
- **Tamper Proof**
- **Non-Bypassable**
- **Verifiability**

Vulnerabilities in Containers

- Using insecure images
- Containers running with the privileged flag
- Unrestricted communication between containers
- Containers running rogue or malicious processes
- Containers that are not properly isolated from the host

How to Secure Containers?

- Isolation of Container?
- Containing the infrastructure (Kubernetes)?
- Securing the Network?
- Control 3rd Party Service? (Libraries, Logging)



✓ SOAR [**S**ecurity **O**rchestration, **A**utomation, and **R**esponse]

Policy-Based Deployment Control

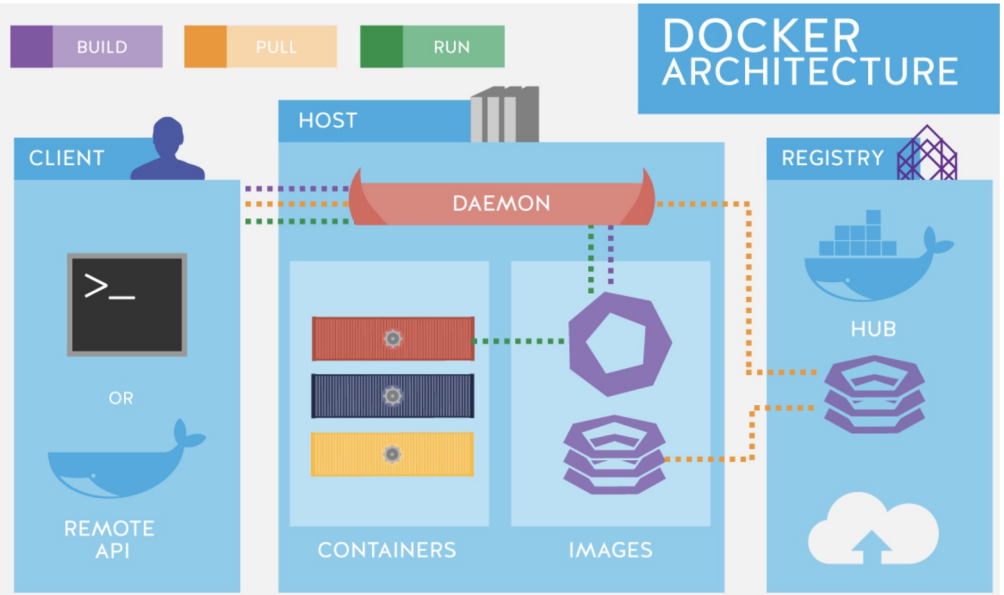
- Container Security provides policy-based deployment control (through Kubernetes) to ensure the Kubernetes deployments you run in your production environment are safe.
- This approach of Container Security enables you to create policies that allow or block deployments based on a set of rules. Rules based on Smart Check (Kubernetes object's properties and the results of Deep Security Smart Check scans).
- Admission Control Webhook checks whether an image is safe to deploy or not.

Incident

- On May 5, researchers at cloud-management platform Uptycs said that attackers compromised the firm's honeypot, a Docker server configured to allow connections through the remote Docker API. [Details]
- CrowdStrike researchers revealed that attackers compromised its honeypots through the open Docker API and then installed two malicious container images that were used to to attack Russian and Belarusian sites.
- Last year, Docker changed the licensing terms of Docker Desktop, moving to a subscription model and arguing that the shift will help the company support more security features and audits. [Details]

Docker and Security Approach

- PaaS that utilizes host OS kernel



- Scanning
- Monitoring
- Firewall

References

- S. Sultan, I. Ahmad and T. Dimitriou, "Container Security: Issues, Challenges, and the Road Ahead," in IEEE Access, vol. 7, pp. 52976-52996, 2019, doi: 10.1109/ACCESS.2019.2911732.
- Xiaowei Zhao, Hong Yan & Jiantong Zhang (2017) A critical review of container security operations, Maritime Policy & Management, 44:2, 170-186
- https://www.tigera.io/learn/guides/container-security-best-practices/
- https://cloudone.trendmicro.com/docs/container-security/about/
- https://www.docker.com/resources/what-container/
- https://cloud.google.com/learn/what-are-containers
- https://www.youtube.com/watch?v=KINjI1tlo2w
- https://www.youtube.com/watch?v=b_euX_M82uI
- https://www.redhat.com/en/topics/security/container-security