VORMETRIC BRINGS CRITICAL SAFEGUARDS INTO DOCKER ENVIRONMENTS

Enterprise usage of Docker has been seeing explosive growth. As rapidly expanding volumes of sensitive assets start to reside in these dynamic environments, the need to implement strong controls grows increasingly critical. With Vormetric Transparent Encryption, organizations can efficiently institute robust, persistent controls over all their Docker instances, no matter how broadly or rapidly they proliferate.

INTRODUCING DOCKER

Docker is an open source platform that makes it easy to package, manage, and distribute applications. This approach packages together a complete system needed to run code, enabling the code to run in a consistent fashion, regardless of the specific environment in which it is deployed. Docker containers include application code, runtime components, system libraries, and more.

The Docker platform provides highly effective support of an organization's DevOps efforts, enabling faster and easier development, iteration, testing, and deployment. Given these advantages, Docker's adoption and utilization is seeing explosive growth. Consider just a few statistics:

- A survey by Enterprise Technology Research indicated Docker had a 97% net spending intentions score, which tracks the intended adoption and use of various technologies. This is the highest score any technology has received in the six-year history of the firm's conducting the survey[1].
- Between June 2014 and June 2015, the number of "dockerized" applications grew 934% and the number of Docker container downloads grew to 500 million, an increase of 18,082%[2].

SECURITY ADVANTAGES AND RISKS IN DOCKER ENVIRONMENTS

The Docker platform makes it easy for development teams to update and control the data and software residing within containers. This dynamic approach offers a number of security advantages. For example, compared to static application frameworks that can contain older artifacts that may pose vulnerabilities, Docker enables development and operations teams to more efficiently ensure all the components that comprise an application are current at all times. Docker also delivers logical segregation of applications running on the same physical host, which can promote more granular and efficient enforcement of security policies.

[1] Enterprise Technology Research, "Docker Scores the Best Ever NET Score in ETR History", Thomas DelVecchio, April 17, 2015, https://www.linkedin.com/pulse/docker-scores-best-ever-net-score-etr-history-thomas-delvecchio

[2] Open Source Delivers, "Dockercon 2015: Stacking Containers of Excitement and Announcements," Megan DeGruttola, June 24, 2015, http://osdelivers.blackducksoftware.com/2015/06/24/dockercon-2015-stacking-containers-of-excitement-and-announcements/

KEY FEATURES

- Transparent deployment
- Encryption and key management
- Privileged user access control
- Security intelligence audit logs

KEY BENEFITS

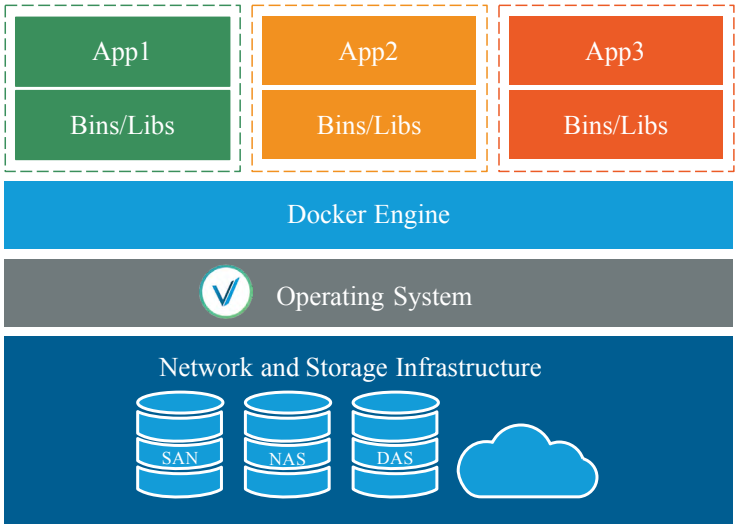
- Docker images secured
- Data-at-rest encrypted
- Docker instance launch policies
- Centralized policy control

However, data at rest in Docker environments is susceptible to many of the same threats as traditional data center environments, including threats from external cyber attackers as well as malicious insiders. Further, like virtual machines in cloud environments, Docker images are easy to replicate, which can lead to widespread and uncontrolled sprawl.—Similarly, the sensitive data produced by the container applications also needs to be controlled. Consequently, without proper safeguards, this proliferation of containers and data can significantly expand the number and types of threats confronting an organization.

VORMETRIC TRANSPARENT ENCRYPTION

With Vormetric Transparent Encryption, organizations can establish strong controls around their sensitive data, including data in Docker implementations, and do so with maximum efficiency. Vormetric Transparent Encryption enables data-at-rest encryption, privileged user access control, and the collection of security intelligence logs for structured databases and unstructured files. With these capabilities, organizations can establish persistent, strong controls around their stored Docker images and protect all data generated by Docker containers when the data is being written to the Docker host storage on a NFS mount or a local folder.

Vormetric Transparent Encryption secures Docker containers at the host operating system layer. The solution offers complete transparency, meaning security teams can employ encryption without having to modify Docker containers or any of the application code running within the containers.



Vormetric protects the Docker containers and the data they generate

Vormetric Transparent Encryption, deployed across multiple Docker hosts, employs controls that help security teams ensure Docker images can't be tampered with or stolen. Only environments with access to the Vormetric Data Security Manager can launch Docker instances. Furthermore, the security team creates polices in the Vormetric Data Security Manager to control which users can access Docker images and launch container instances. For further protection, a security intelligence audit trail of accessed Docker images is created and privileged users are prevented from accessing or launching Docker images.

ABOUT VORMETRIC

A leader in data security solutions, Vormetric (@Vormetric) protects data-at-rest in physical, virtual, big data and cloud environments. Trusted by businesses and governments for over a decade, the Vormetric Data Security Platform secures the data of more than 1,500 global enterprises—including 17 of the Fortune 30. With Vormetric, a single infrastructure and management environment protects data wherever it resides with file, volume and cloud storage encryption, tokenization with dynamic data masking, field-level application encryption, sophisticated access control policies, third party and integrated encryption key management. For more information, please visit: www.vormetric.com.

Vormetric, Inc.
2545 N. 1st Street, San Jose, CA 95131
United States: 888.267.3732
United Kingdom: +44.118.949.7711
Singapore: +65.6829.2266
info@vormetric.com
www.vormetric.com