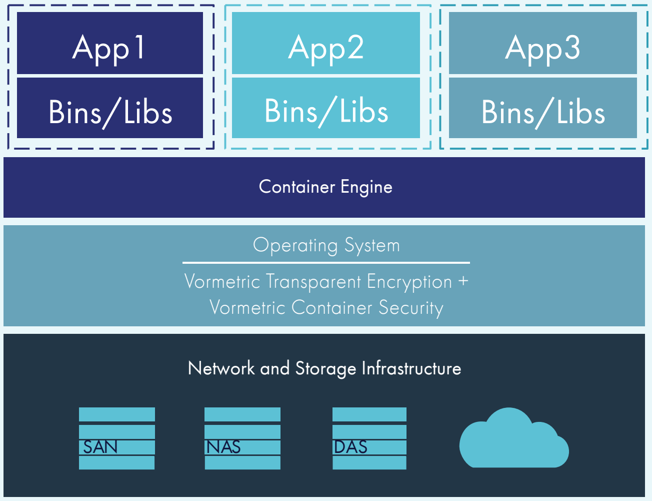
EXTENDING DATA ENCRYPTION, ACCESS CONTROLS, AND DATA ACCESS LOGGING INTO DOCKER AND OPENSHIFT CONTAINERS

- Address compliance, regulatory and best practice requirements for encrypting and controlling access to sensitive data within container environments
- Prevent threats from privilege escalation and privileged user abuse
- Isolate and control access to data used by containers in multi-tenant, microservices and cloud environments
- Encrypt data and control access to data stored both within containers and underlying storage environments based on users and groups within Docker, OpenShift, LDAP, and the underlying container host

‹Thales eSecurity›

VORMETRIC CONTAINER SECURITY

THE CHALLENGE: CAPITALIZING ON THE BENEFITS OF CONTAINERS, WHILE MINIMIZING THE RISK


App1
Bins/Libs
App2
Bins/Libs
App3
Bins/Libs
Container Engine
Operating System
Vormetric Transparent Encryption +
Vormetric Container Security
Network and Storage Infrastructure
SAN
NAS
DAS

Within a few years, container technology has gone from an interesting concept to a must have. Today, containers are powering business-critical applications for established enterprises and industry disruptors alike. By leveraging container technologies, customers are realizing significant benefits in a range of areas, including faster application delivery and innovation, improved efficiency through reusable, modular components, and cost savings through optimized resource utilization and reduced licensing expenses. While the potential benefits of container-based solutions are undeniable, there are additional risks associated with their use:

- **Exposure to privileged user abuse.** By default Docker processes run with root privileges, while for OpenShift, Cluster Administrators have full access to all Tenant Secrets. This level of privileged access can pose multiple risks. For example, container administrators may have unchecked access to images and the data stored within them, as well as expose organizations to privilege escalation attacks.
- **Cross container access.** Poor configuration of permissions can result in multiple containers having access to information that should remain private. Further, when containers are hosted in shared virtualized or cloud environments, critical information can be exposed to third parties.
- **Compliance risks.** Many compliance mandates require strong controls and auditing of data access. However, many security teams have limited controls available for managing and tracking access to data that's held within containers and images. As a result, these teams are finding it difficult to comply with all their relevant internal security policies and regulatory mandates.

VORMETRIC CONTAINER SECURITY

THE SOLUTION: VORMETRIC CONTAINER SECURITY

Now, Thales eSecurity delivers the strong, centrally managed controls you need to protect data within container environments. The solution features capabilities for file and volume level encryption, access control, and logging of data access. These controls can be applied both to containers and to the underlying operating system. An extension of Vormetric Transparent Encryption, Vormetric Container Security supports both Docker and Red Hat OpenShift container environments, enabling security teams to establish controls inside of containers.

KEY FEATURES

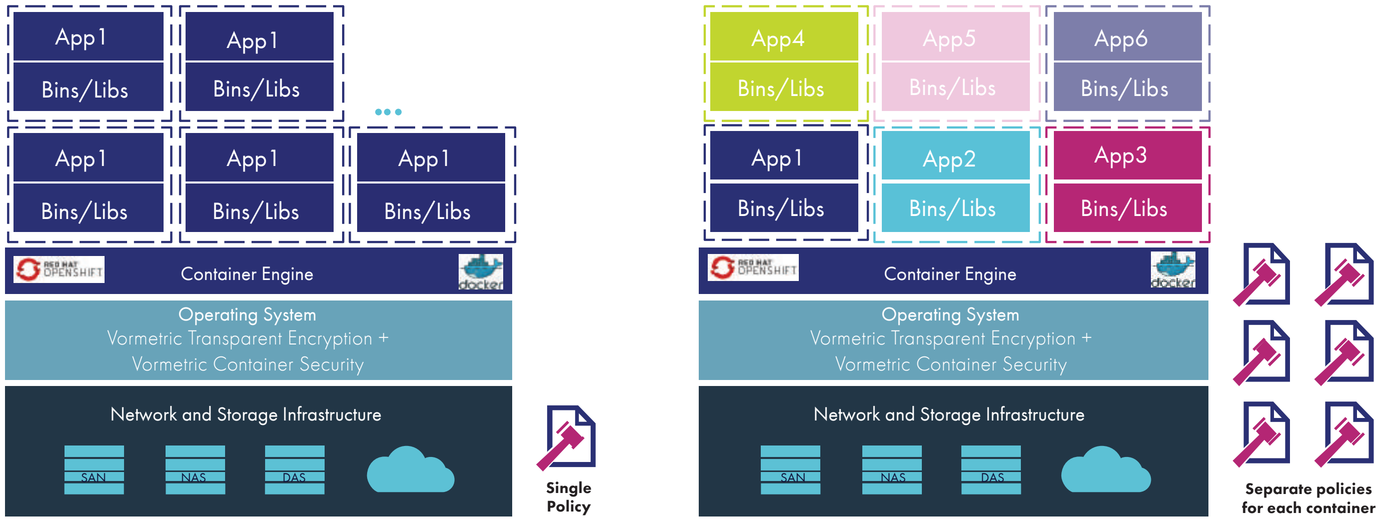
- **Comprehensive safeguards.** Vormetric Container Security secures container volumes and protects data from being inappropriately accessed or exported – regardless of where the container is used – in data centers, cloud or virtualized environments.
- **Encryption and access controls.** Encrypt data within containers and underlying storage environments using granular access policies that detail who, what, where, when and how the data may be accessed. Allows access to encrypted data based on users and groups within Docker, OpenShift, LDAP, and the underlying container host system.
- **Data access audit logs.** Detailed data and management environment access logs to meet regulatory and compliance requirements with pre-built integration to major SIEM systems for threat alerting, and to build data access usage baselines for anomaly detection.
- **Transparent – No changes to containers required.** With Vormetric Container Security, enables organizations to establish and enforce data security policies without having to make any changes to operations, applications, or containers.

BENEFITS

By leveraging Vormetric Container Security, your organization can realize a series of powerful benefits:

- **Address compliance requirements.** Whether your organization manages sensitive payment card data, healthcare records, or other sensitive assets, you can use this solution to address the data access control requirements of all pertinent compliance mandates.
- **Prevent privileged user threats.** Guards against unauthorized access to data by privileged users – limiting administrators with root privileges and other privileged users from seeing sensitive data they're not specifically authorized to access.
- **Leverage containers and cloud, without compromising security.** Vormetric Container Security enforces data security policies wherever the container is stored or used – data centers, virtualized environments – even in cloud implementations. Deploy and use containers where needed for cost effectiveness, control or performance without making compromises in data security.

Vormetric Container Security supports microservices and container isolation



Microservices scaling
Add more App instances to scale service capacity
Every new container instance has the same policy

Isolate for multitenancy and compliance
No container sees another container's data

Follow us on:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com