thalescpl.com

THALES

Vormetric container security

Challenge: Building continuous container security into your CI/CD pipeline

As enterprises deploy containers with a continuous integration and delivery (CI/CD) pipeline, security must keep up. Container technologies provide significant benefits including increased portability, delivery and innovation, improved efficiency through reusable modular components, and cost savings through optimized resource utilization and reduced licensing expenses. However, there are also risks:

- **Privileged user abuse.** By default, Docker processes run with root privileges, and OpenShift cluster administrators have full access to all tenant secrets. This level of privileged access poses multiple risks. For example, container administrators may have unchecked access to images and the data stored within them, and organizations could be subject 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 data access. However, many security teams have limited controls available to manage and track access to data held within containers and images. As a result, these teams find it difficult to comply with relevant internal security policies and regulatory mandates.

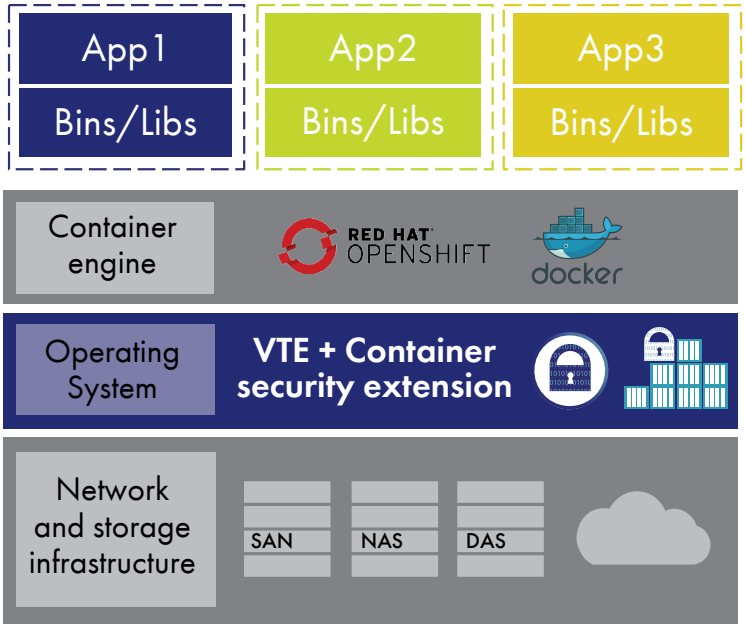
Solution: Vormetric Container Security

Vormetric Container Security delivers in-container capabilities for encryption, access controls, and data access logging, so organizations can establish strong safeguards around data in dynamic container environments. This solution from Thales is a software license for Vormetric Transparent Encryption that enables security teams to establish controls inside of containers. With this extension, encryption, access controls, and data access audit logging can be applied on a per-container basis, both to data inside of containers, and to external storage accessible from containers.

Benefits

Vormetric Container Security provides:

- **Compliance.** This extension of Vormetric Transparent Encryption delivers the encryption, data access control, and auditing capabilities you need to address compliance requirements and regulatory mandates. You can protect sensitive data — whether your organization manages payment cards, healthcare records or other sensitive assets.
- **Prevention of Privileged-User Threats.** Vormetric Container Security offers encryption with data access control, enabling privileged users, such as Docker or OpenShift cluster administrators, to work as usual, without unauthorized access to sensitive data.



- **Achieve Robust 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 having to make any changes to applications, containers or infrastructure sets.

Features

- **Comprehensive Data Security Safeguards.** Vormetric Container Security extends Vormetric Transparent Encryption, enabling security teams to establish data security controls inside of containers. With this extension, you can apply encryption, access control, and data access logging on a per-container basis. Encryption can be applied to data generated and stored locally within the container and to data mounted in the container by network file systems.
- **Transparent Encryption.** No changes to containers required. Establish data security controls without having to make any changes to applications, containers or infrastructure sets. The container security solution even supports common container microservices deployment models. This enables single policies that can apply to all containers running on a container host instance and allows distinct policies for each container or a mix of policy types.
- **Granular Access Controls and Visibility.** Vormetric Container Security offers the detailed visibility and control you need to comply with the most stringent policies and mandates. With this container security solution, enterprises can establish granular access policies based on specific users, processes, and resource sets within containers. Finally, this solution can establish isolation between containers, so only authorized containers can access sensitive information.

About Thales Cloud Protection & Licensing

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 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