

Container Encryption for Start-Ups and Tech Companies

Encryption is a critical component of container security

From driving rapid development to lowering infrastructure costs, containers offer many benefits that enable fast-moving companies to get their ideas to market quicker. It is for this reason that containers continue to make their way into start-ups and tech companies.

But just like any emerging technology, containers have also introduced new security and compliance challenges, especially when it comes to data protection. Most companies rely on access control, monitoring, and existing workload security to protect their container environments, but very few have incorporated one of the most critical components of a successful security strategy – encryption. In fact, encryption is consistently one of the last security solutions that is implemented with newer technologies like containers due to performance impact and the complexity it often adds. And at the end of the day, no one wants to be “slowed down” because of security.

The reality is that start-ups and tech companies have coveted, highly valuable data in their container environments and that data must be encrypted to ensure both security and compliance. Don't let a data breach be the reason encryption becomes a top priority in your organization.

Zettaset XCrypt Container Encryption: High performance container encryption that will not slow you down

XCrypt Container Encryption is a first-of-its-kind solution that works seamlessly with major container software to provide transparent, high-performance encryption. Because it's software-only, it helps organizations overcome the typical adoption barriers for encryption – offering a negligible effect on performance and adding no additional complexity to container environments.

- Works with Docker Enterprise from Mirantis, Kubernetes, Red Hat Open Shift, and VMware Tanzu
- Negligible effect on performance as its software-only
- Transparent integration into any container environment
- Simple, automated deployment and infinite scalability
- No specialized encryption expertise required

Some of the primary use cases for start-ups and tech companies are explained in more detail on the right side of this document.

Specific use cases for start-ups and tech companies

Zettaset XCrypt Container Encryption works seamlessly with Docker Enterprise from Mirantis, Kubernetes, Red Hat Open Shift, and VMware Tanzu to provide transparent, high performance encryption for containers – no matter where you are in your DevOps journey.

USE CASES INCLUDE:

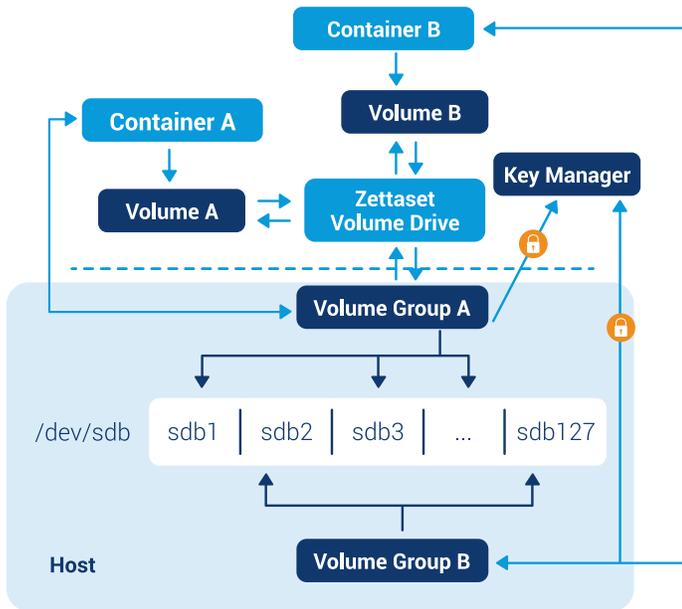
- **Ensuring protection of IP and sensitive data in container environments**
Transparently deploy encryption in new or legacy container environments.
- **Complying with the California Consumer Privacy Act (CCPA)**
Meet stringent CCPA requirements by encrypting consumer data collected in California.
- **Incorporating encryption in mature DevOps practices**
Incorporate encryption into mature DevOps practices without changing processes, adding complexity, or impacting performance.
- **Moving to DevSecOps**
Transition from DevOps to DevSecOps by implementing container encryption.
- **Achieving internal security or compliance mandates**
Increase the level of protection for data at rest in container environments to meet or exceed security and compliance mandates.

In addition to container encryption, Zettaset's other products can help you to encrypt data-at-rest in any environment that it may exist.

[Learn more at www.zettaset.com](http://www.zettaset.com)

How does it work?

Zettaset’s software-defined solution provides high performance encryption that protects containers from data theft in any physical or virtual environment. Its ease of use and intelligence enables pervasive and on-demand encryption that is scalable across any deployment:



- 1** Upon creation, containers request a particular-sized encrypted storage volume.
- 2** Zettaset’s volume driver requests a volume from the host.
- 3** Zettaset’s volume manager constructs a volume from various partitions on the device and creates a volume group.
- 4** The volume manager communicates with the key manager to create a key and encrypt the volume.
- 5** On container destruction, the encryption key is destroyed and volumes are made available again.

Get more information

Visit www.zettaset.com/products/xcrypt-container to learn more about XCrypt Container Encryption.

About Zettaset

Zettaset is a software-defined encryption solution that protects against data theft and can be transparently deployed across all physical and virtual environments. Its products are designed for medium to large enterprises that deal with sensitive information that would expose them, financially and reputationally, in the event of a breach. Unlike traditional solutions that are appliance-based, Zettaset is a cost-effective, software-only solution that is easy to deploy, does not impact performance, and scales with your business from on premise to the cloud.

