Trusted Cyber Technologies

THALES
Building a future we can all trust

# CipherTrust Transparent Encryption for Kubernetes

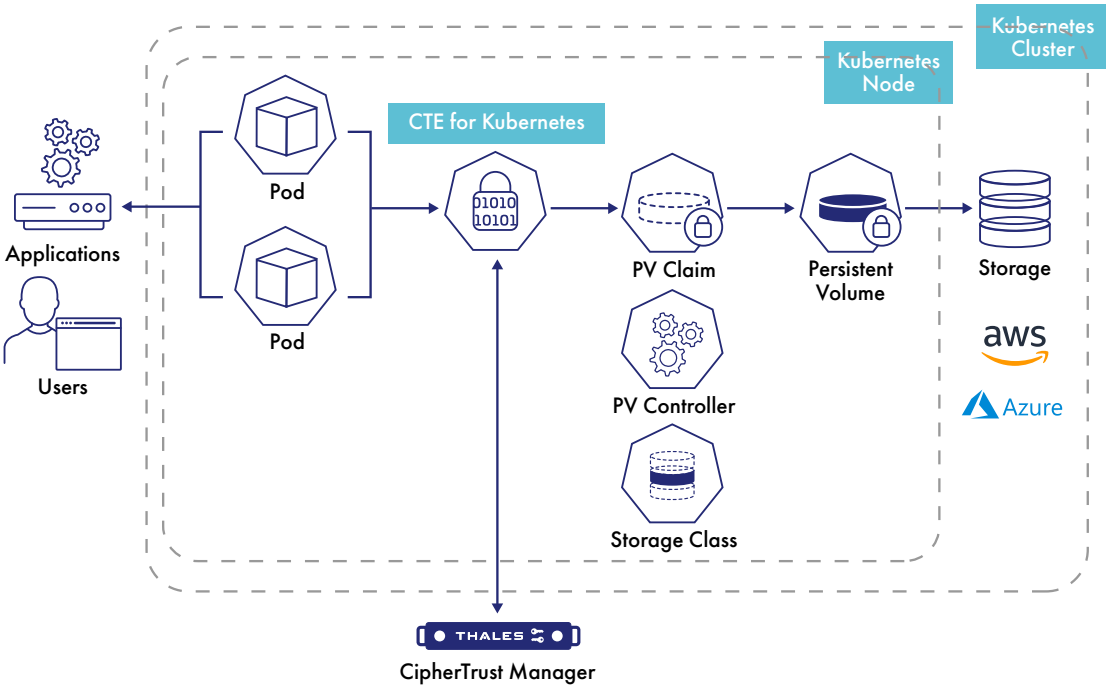
## Challenge: Securing Applications for Kubernetes Environments

Modern applications are increasingly built using containers, which are microservices packaged with their configurations and dependencies. Kubernetes is an open-source software for deploying and managing these containers. Containerized applications can be delivered, deployed and managed faster with Kubernetes to provide improved efficiency through re-usable modular components, cost savings through optimized resource utilization and reduced licensing expenses. However, there are several risks:

- **Privileged user abuse.** By default, Docker processes run with root privileges, administrators have full access to all tenant secrets. This level of untethered access poses multiple risks. Organizations could be subject to privilege escalation attacks, if administrators have unchecked access to container images and the data stored within them.
- **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 stringent access 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 security policies and regulatory mandates.

## Solution: CipherTrust Transparent Encryption for Kubernetes

CipherTrust Transparent Encryption for Kubernetes delivers in-container capabilities for encryption, access controls, and data access logging, that enables organizations to establish strong safeguards around data in Kubernetes environments. With this extension for CipherTrust Transparent Encrypton, data protection can be applied on a per-container basis, both to secure data inside of containers and in external storage accessible from containers, all centrally managed from the CipherTrust Manager.




## Benefits

CipherTrust Transparent Encryption for Kubernetes provides:

- **Compliance.** This extension of CipherTrust Transparent Encryption addresses compliance requirements and regulatory mandates for protecting sensitive data such as— payment cards, healthcare records or other sensitive assets.
- **Protection from Privileged-User Threats**. This solution offers encryption with data access controls, enabling privileged users, such as Docker or OpenShift cluster administrators, to operate as regular users, without gaining unauthorized access to sensitive data.
- **Achieve Robust Security.** CipherTrust Transparent Encryption for Kubernetes 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 tomake any changes to applications, containers, or infrastructure sets.

## Features

- **Comprehensive Data Security Safeguards**. CipherTrust Transparent Encryption for Kubernetes extends CipherTrust Transparent Encryption, enabling security teams to establish data security controls inside of containers. With this extension, you can apply encryption, access controls, 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.
- **Scalable Transparent Encryption**. Provides data security controls without having to make any changes to applications, containers or infrastructure sets. It enables a single policy to be applied to all containers within a Kubernetes cluster, or distinct policies applied to each container within a cluster. This solution can scale up or shrink down a Kubernetes environments as business needs change.
- **Granular Access Controls and Visibility**. CipherTrust Transparent Encryption for Kubernetes offers the detailed visibility and control you need to comply with the most stringent policies and mandates. With this Kubernetes 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.

## CipherTrust Manager

The CipherTrust Manager centralizes key, policy, and log management for the CipherTrust Data Security Platform including CipherTrust Transparent Encryption. CipherTrust Manager is available in both virtual and physical form-factors that integrate with FIPS 140-2 validated Thales TCT Luna T-Series and third-party Hardware Security Modules (HSMs) for securely storing master keys with highest root of trust.

## About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com



3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com