

CipherTrust Transparent Encryption for Kubernetes

The 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 access and insider risk.** Kubernetes clusters often rely on highly privileged administrators and service accounts to manage workloads. Without strong separation of duties and least-privilege controls, these privileged users can access container images, application secrets, encryption keys, and persistent data across the cluster. If an administrator account is compromised or misused, attackers can escalate privileges, move laterally between workloads, and gain broad access to sensitive data.
- **Cross-workload data exposure.** Kubernetes environments are designed to run multiple applications and tenants on shared infrastructure. Misconfigured role-based access controls (RBAC), shared storage, overly permissive volume mounts, or weak namespace isolation can allow one container or workload to access data that belongs to another. In multi-tenant or cloud-native environments, these configuration errors increase the risk of unauthorized data exposure and compromise the isolation that containers are intended to provide.
- **Compliance and audit challenges.** Organizations subject to regulations such as PCI DSS, HIPAA, GDPR, or SOX must demonstrate that sensitive data is protected, access is restricted, and all access is auditable. Native Kubernetes security features provide infrastructure-level controls but often lack detailed visibility into file- and data-level access within containers. This can make it difficult to enforce least-privilege policies, produce comprehensive audit trails, and demonstrate compliance during security assessments.

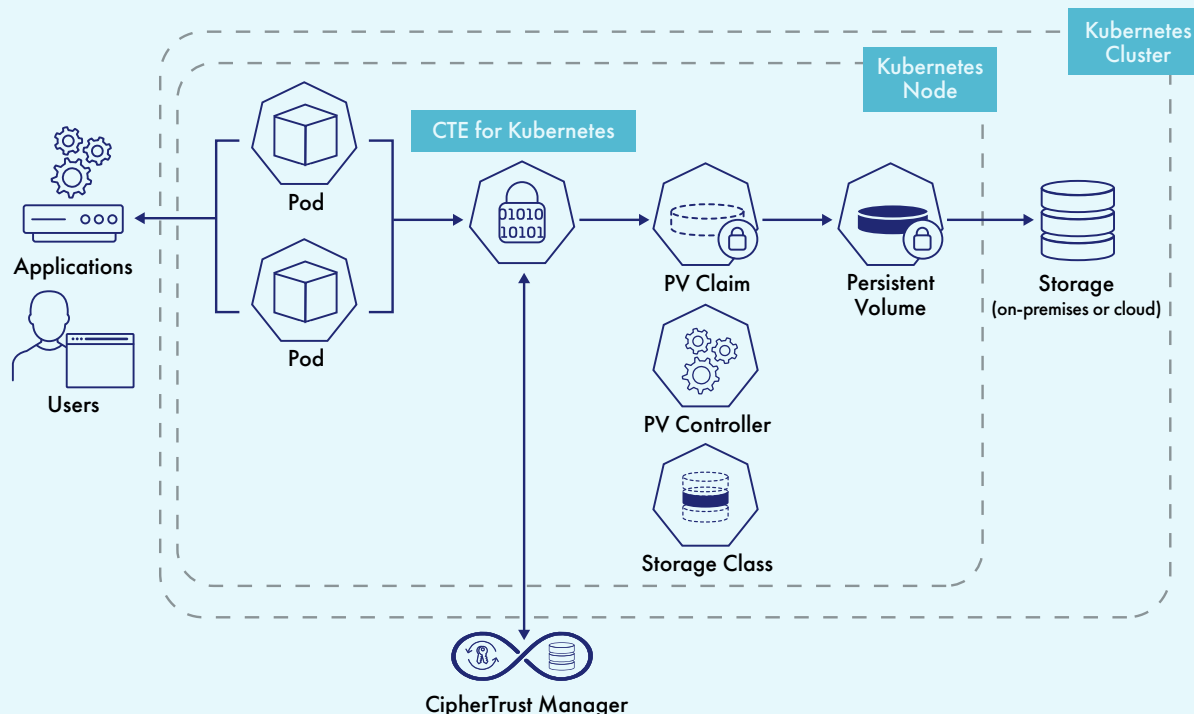
The Solution: CipherTrust Transparent Encryption for Kubernetes

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 Encryption, 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

- **Compliance**
Simplify compliance with built-in encryption, granular access controls, and detailed audit logs for containerized data, helping you demonstrate control over payment data, healthcare records, and other sensitive assets. Strengthen alignment with regulatory mandates by centrally defining and enforcing data protection policies across Kubernetes clusters, on-premises and in the cloud.
- **Protection from privileged-user threats**
Reduce the risk of privileged-user abuse by enforcing policy-based encryption that prevents cluster administrators and other high-privilege accounts from viewing sensitive data in clear text. Allow DevOps and platform teams to manage Kubernetes infrastructure as usual while restricting access to protected data to only authorized users and processes inside containers.
- **Robust security for Kubernetes workloads**
Apply strong data security controls wherever containers run—data centers, virtualized environments, and public clouds—without requiring changes to applications, container images, or underlying infrastructure. Scale securely as Kubernetes usage grows by applying consistent, per-container policies that protect both local container data and externally mounted storage from unauthorized access.





Features

- **Transparent Data Protection.** CiphertTrust Transparent Encryption for Kubernetes extends CiphertTrust Transparent Encryption, enabling security teams to enforce data security controls inside containers. Apply encryption, access controls, and audit logging on a per-container basis. Protect data generated and stored locally within containers, as well as data mounted through network file systems.
- **Scalable Transparent Encryption.** Delivers transparent data security without requiring changes to applications, containers, or infrastructure. Apply a single policy across an entire Kubernetes cluster or unique policies for individual containers. Security scales seamlessly as Kubernetes environments grow or shrink with business demands.
- **Granular Access Controls and Visibility.** CiphertTrust Transparent Encryption for Kubernetes delivers the visibility and control needed to meet the most demanding security and compliance requirements. Enforce granular access policies based on users, processes, and resources within containers, while isolating workloads so only authorized containers can access sensitive data.

KuppingerCole Leadership Compass on Data Security Platforms as well as a Strong Performer in the Forrester Wave and to be featured in Gartner's Market Guide to Data Security Platforms.

The CiphertTrust Platform unifies data discovery, classification, data protection, and centralized management for keys and secrets into a single platform. This results in fewer resources dedicated to security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

CiphertTrust Data Security Platform

The award-winning CiphertTrust Data Security Platform is an integrated set of data-centric solutions that remove complexity from data security, accelerate time to compliance, and secure cloud migrations. Thales is proud to have been recognized as an Overall Leader in the