Solution Brief

Telco - Secure Hybrid Cloud Environments

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Introduction

This paper presents an analysis of the hybrid cloud and how a Kubernetes-based platform enables enterprises and telco service providers to securely deploy cloud-native applications. In particular, there is emphasis on the data security challenges that arise with these deployments regarding data at rest. The critical security challenges encompass configuring Kubernetes security controls, ensuring secure deployment of workloads, and enabling consistent security across a variety of deployment environments.

The Hybrid Cloud

Public clouds have revolutionized IT because they provide a much easier way to consume infrastructure and platform components needed to build and operate applications. While there has been lots of "cloud-first" hype and momentum in the race to modernize workloads, initially it was not necessarily clear which sort of cloud model (public, private, hybrid) was best for which applications. Some applications are best run on a public cloud to leverage advanced cloud services or the flexibility provided by on-demand based consumption. However, some mission-critical applications are not easily outsourced to a 3rd party cloud provider and therefore need to be kept either on-premises or hosted on private clouds for a variety of reasons. These often include security and compliance requirements, regulatory mandates, data control, migration costs, and latency issues. From this combination of workload management needs and industry best practices, it's becoming increasingly normal for enterprises and telcos to manage their applications across hybrid clouds and edge deployments.

Telco service providers that operate 5G mobile broadband networks are more likely to face a multitude of challenges related to their highly distributed infrastructure. These challenges include the need to manage a vast number of radio towers and networks, while simultaneously ensuring the efficient operation of software applications across the access layer, aggregate layer, and core data centers. Additionally, telcos must comply with stringent specifications for latency and network performance, while also maintaining the flexibility to dynamically relocate services to optimize performance, reduce operational costs, and meet changing business demands. Such requirements demand the deployment of a complex, dynamic, and scalable infrastructure capable of adapting to the evolving needs of 5G networks.

5G is ushering in an era where not only IT applications but also network functions in the core and radio access network (RAN), are deployed as cloud-native network functions (CNFs) on a Kubernetes-based telco cloud. These telco clouds are often deployed across geographically distributed remote environments, creating a significant challenge for network operators. The telco cloud illustrates the hybrid cloud model: OSS/BSS applications are run on a mix of private cloud and public cloud(s); some core CNFs may run on public clouds but most of them are run in regional data centers and sometimes edge data centers; if the telco has started virtual RAN, some RAN CNFs will run at the far edge of the network.

The security of a Kubernetes-based hybrid cloud is of paramount importance given the diverse range of threats:

- Clusters and pods
- Malicious actors
- Malware running inside containers
- Broken container images
- Compromised or rogue users

Without effective controls in place, a bad actor who manages to breach an application could potentially seize control of the host or even the entire cluster.

Applications in hybrid clouds are running in very different environments (public cloud, private cloud, edge) and the associated data is stored across numerous systems and platforms. As with any data storage system, the security of data at rest within the hybrid cloud is of utmost importance, as unauthorized access or breaches could have severe implications. Consequently, implementing robust measures to secure data at rest is imperative to mitigate risks and safeguard the confidentiality, integrity, and availability of critical information.

What is Data at Rest Security? Data at rest refers to data that is stored on physical storage media, such as hard drives, solid-state drives, or any other data storage device. Securing data at rest involves protecting it from unauthorized access, modification, or deletion. This is best achieved through encryption, access control, and monitoring.

While a number of Kubernetes security issues exist, the four most important to consider are:

1. **Configuring security controls:** When deploying Kubernetes, from open source, none of the security controls are configured out of the box. Figuring out how they work and how to securely configure them is entirely the operator's responsibility.

2. **Deploying workloads securely:** Whether you are using a Kubernetes distribution with pre-configured security controls or building a cluster and its security yourself, developers and application teams who may not be familiar with the ins and outs of Kubernetes may struggle to properly secure their workloads.

3. **Lack of built-in security:** While Kubernetes offers access controls and features to help create a secure cluster, the default setup itself is not secure. Organizations need to make the right changes to the workloads, cluster, networking, and infrastructure configurations to ensure Kubernetes clusters and containers are fully secure.

4. **Securing data:** This is the most important aspect of Kubernetes security. This involves protecting data that is stored on persistent volumes, which are used to provide data storage for stateful applications.

    - Encryption: Secure Kubernetes needs encrypted data at rest on persistent volumes including data inside the POD, and the Kubernetes Secrets to prevent unauthorized access to sensitive data stored on the volumes.
    - RBAC: Kubernetes provides basic Role-Based Access Control (RBAC), to prevent unauthorized access to data.
    - Trusted Container Images: Implement procedures to deploy only trusted container images busing signed container images.
    - Auditing: Kubernetes also provides audit logs, which can be used to monitor access to data at rest and detect any unauthorized access attempts, including using SIEM.

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:

> " To accelerate the adoption of 5G and overcome the challenges related to managing highly distributed infrastructures, Red Hat and Thales are proud to announce a solution to mitigate Kubernetes data security risks. Thales CipherTrust Transparent Encryption secures data in persistent volumes running on Red Hat OpenShift, a unified platform to build, modernize, and deploy applications at scale. With this integration, both Red Hat and Thales enable telco and cloud service providers to quickly harness the power of 5G across their cloud, edge, and legacy environments while steadfastly protecting sensitive data."
>
> – **Michael Tadault, Chief Technologist for Telco APAC, Red Hat**

- **Privileged user abuse.** By default, the Docker daemon runs 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.** Misconfiguration 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.

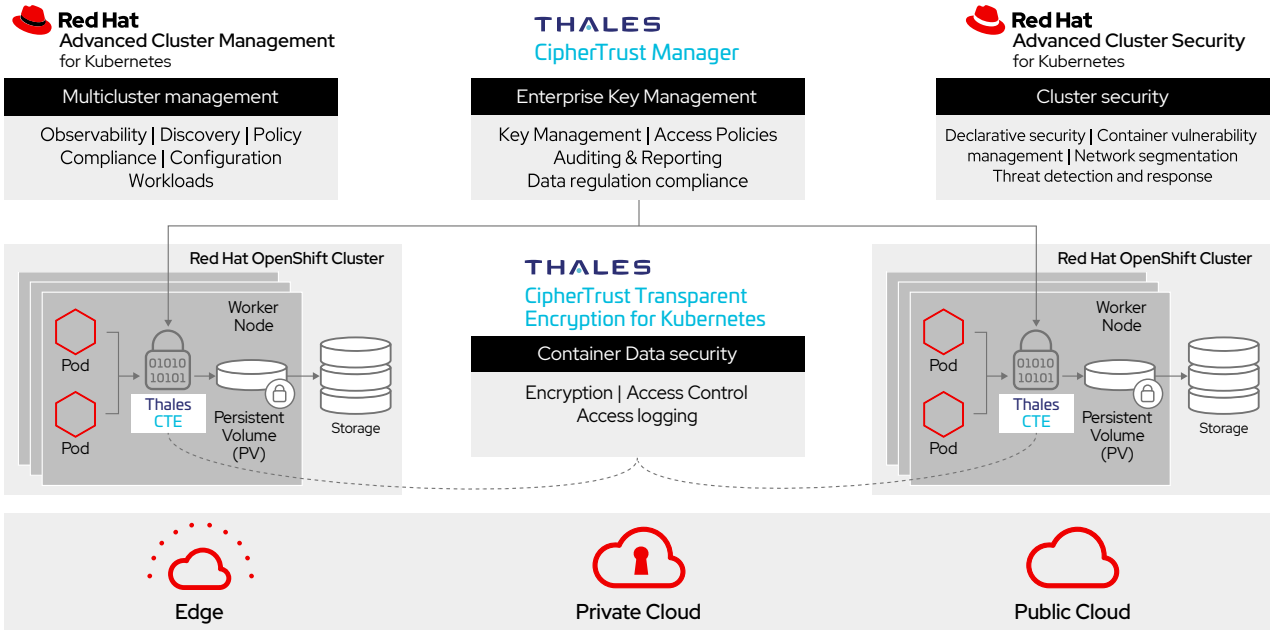

Figure name: Secure Hybrid Cloud Environments

- **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: Red Hat OpenShift and Thales CipherTrust Transparent Encryption for Kubernetes

Red Hat OpenShift is a Kubernetes-based application platform that is available on all the footprints of the hybrid cloud: public clouds, private clouds, and the edge. It is secure by default because the default configuration of OpenShift clusters is minimal privileges and maximum security. To learn more details, please reference this white paper about Kubernetes-native security. [1]

> " In the domain of data security, telecom service providers managing 5G networks and utilizing Kubernetes encounter numerous hurdles to effectively fortify hybrid cloud ecosystems across their extensively dispersed infrastructure. To protect against these security vulnerabilities, Thales CipherTrust Transparent Encryption safeguards data within persistent volumes linked to pods operating on the Red Hat OpenShift platform. This platform offers a cohesive framework for constructing, updating, and deploying applications on a large scale, all with a focus on data protection."
>
> – **Chen Arbel, Associate Vice President, 5G Business Development, Thales**

To run the hybrid cloud at scale, two products complement Red Hat OpenShift:

- **Red Hat Advanced Cluster Management (ACM) for Kubernetes,** a single pane of glass for managing a fleet of clusters deployed on private cloud, public cloud(s), and the edge. ACM provides provisioning and observability of all managed clusters, prevents configuration drift, and ensures compliance with security policies.
- **Red Hat Advanced Cluster Security (ACS) for Kubernetes** which secures a fleet of OpenShift clusters: container vulnerability management, network segmentation, threat detection and response.

Thales CipherTrust Transparent Encryption is tightly integrated with Red Hat OpenShift. It 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 Thales CipherTrust Transparent Encryption, data protection can be applied on a per-container basis, both to secure data inside containers and in external storage accessible from containers, all centrally managed from the Thales CipherTrust Manager.

Benefits

CipherTrust Transparent Encryption for Kubernetes provides:

- **Compliance.** CTE-K8s 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 (CTE-K8s) enforces data security policies wherever the container is stored or used – whether it be in data centers, virtualized environments, or 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.

Together both Red Hat OpenShift and Thales CipherTrust

Transparent Encryption for Kubernetes provide the foundation for a secure hybrid cloud:

- **Consistent operations** – Whether an application is run at the edge, in a private cloud, or in public cloud(s), Red Hat ACM, ACS, and Thales CipherTrust Manager manage OpenShift clusters wherever they are deployed, facilitating operations across the hybrid cloud.
- **Consistent security** – The same security mechanisms such as workload isolation, container communication control, and data at rest protection can be used whether the application is running in Multiaccess Edge Computing (MEC), micro data center at the telco edge, or in a public cloud.
- **Increase Efficiency and Productivity** - Developers' cognitive load is reduced because they can use the same tools and middleware for creating applications independently of where the application will be deployed.

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 CTE-K8s, 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 scale down a Kubernetes environment 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.

About Red Hat OpenShift

Red Hat OpenShift, the industry's leading hybrid cloud application platform powered by Kubernetes, brings together tested and trusted services to reduce the friction of developing, modernizing, deploying, running, and managing applications. OpenShift delivers a consistent experience across public clouds, on-premises, hybrid clouds, or edge architectures.

About Red Hat

We're the world's leading provider of enterprise open-source solutions—including Linux, cloud, container, and Kubernetes. We deliver hardened solutions that make it easier for enterprises to work across platforms and environments, from the core datacenter to the network edge.

About CipherTrust Manager

CipherTrust Manager centralizes key, policy, and log management for the CipherTrust Data Security Platform including CipherTrust Transparent Encryption. It is available in both virtual and physical form-factors for securely storing master keys with an elevated root of trust. These appliances can be deployed on premises as well as in private, public, or hybrid cloud infrastructures.

About Thales Cloud Protection and Licensing

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

[1] Kubernetes native security, Red Hat white paper, April 2021, https://www.redhat.com/en/resources/kubernetes-native-security-whitepaper

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us