Solution Brief

Strengthening Data and Application Security in Complex, Regulated Environments

cpl.thalesgroup.com

THALES
Building a future we can all trust

As organizations with critical and sensitive operations increasingly adopt containerized applications and hybrid cloud infrastructure, securing data and applications across deployment stages becomes essential. This paper explores how Thales and Red Hat collaborate to meet these unique challenges, providing hardware and software encryption solutions that enhance data protection and regulatory compliance.

Security Challenges in Distributed and Dynamic Infrastructures

In complex and regulated environments, organizations must manage diverse IT landscapes across cloud, on-premises, and edge locations. This requires robust security measures to protect sensitive data and meet compliance standards while maintaining operational performance and reliability.

This distributed infrastructure calls for a scalable, flexible approach to data security. Red Hat OpenShift provides a secure, centralized platform for managing containers, while Thales CipherTrust Transparent Encryption safeguards data wherever it resides, ensuring a resilient, comprehensive security framework.

Addressing the Imperative for Data at Rest Protection

For organizations handling critical data, either classified data or data under protection laws such as personal and identifying information then securing information at rest is vital. Data at rest, stored on physical or virtual media, must be shielded from unauthorized access, modification, or deletion. Unauthorized access could have severe implications, underscoring the need for a robust security strategy.

Thales and Red Hat's joint solution delivers multilayered encryption, access controls, and monitoring to protect sensitive data and support regulatory standards.

1. **Configuring Security Controls in Kubernetes:** Automated security configurations ensure that only authorized users can access sensitive Kubernetes data, with data encryption built into Kubernetes environments.
2. **Secure Workload Deployment:** Whether using pre-configured or custom-built clusters, Kubernetes workloads are safeguarded to minimize misconfiguration risks and data leakage.
3. **Cross-Platform Security Agnosticism:** This solution supports security across Kubernetes clusters and diverse infrastructures, bolstering data protection across both containers and underlying infrastructure.

Ensuring Data in Transit Security

In addition to protecting data at rest, safeguarding data in transit is critical for organizations operating in complex environments. Data in transit refers to any information moving between locations—whether across internal systems, between remote sites or via external networks such as the cloud or partner ecosystems.

Failing to protect data in transit can expose it to interception, tampering, or unauthorized access, particularly as it traverses distributed infrastructures. To mitigate these risks, Thales and Red Hat offer a combined approach that employs encryption technologies and network safeguards to ensure data remains secure during transmission.

Data in Transit Encryption Solutions:

- Network Layer Encryption: Secure communications are enabled through protocols such as TLS (Transport Layer Security) for application-level encryption and IPSec for secure IP-level communication, safeguarding both virtual and physical network pathways.
- Hardware-Based Encryption: Thales Luna Hardware Security Modules (HSMs) provide a root of trust for encryption keys used in data transmission, ensuring cryptographic integrity and scalability for high-stakes environments.
- Mutual Authentication: Establishing trust between communicating entities using certificate-based authentication ensures that data is exchanged only between verified parties.

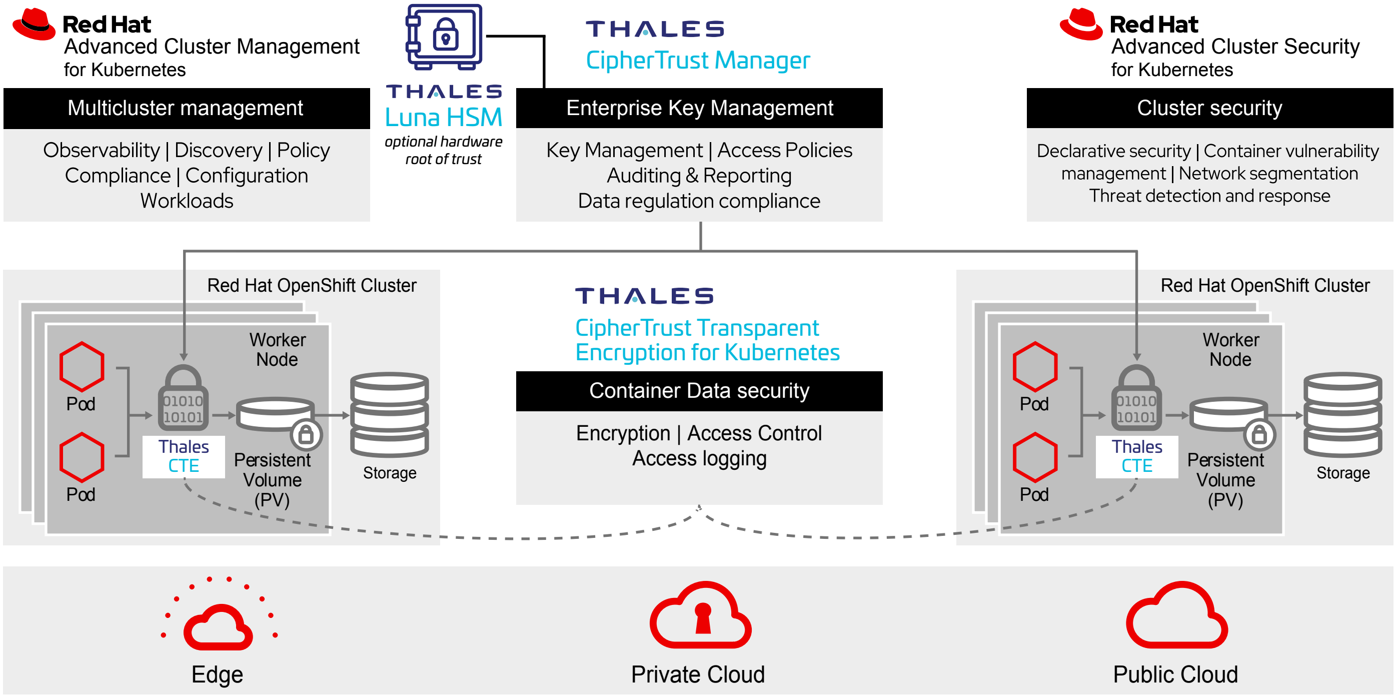
- **Traffic Segmentation and Isolation:** Through the integration of Red Hat Advanced Cluster Security (ACS), organizations can implement network segmentation to control data flow between microservices, clusters, and external endpoints, further reducing the attack surface.
- **End-to-End Protection:** This joint solution enables encryption from the source to the destination, ensuring data integrity and confidentiality even in distributed, hybrid, or multi-cloud setups.

Benefits of Data in Transit Encryption:

- **Enhanced Security Across Boundaries:** Protect sensitive information as it moves between edge, on-premises, and cloud environments. The solution offers encryption with data access control. This lets privileged users, such as Kubernetes cluster administrators, operate as regular users without gaining unauthorized access to sensitive data.
- **Compliance Assurance:** Meet regulatory requirements for secure communications, including those for financial transactions, patient records, and classified government data.
- **Resilience Against Network Threats:** Mitigate risks such as eavesdropping, man-in-the-middle (MITM) attacks, and data interception.
- **Transparent Encryption:** The solution lets users establish data security controls without having to make any changes to applications, containers, or infrastructure sets. The solution supports common container micro-services deployment models. This enables deploying the same protection policies for all persistent volumes attached to an application pod or having unique encryption and access control for each persistent volume in a Kubernetes Cluster.

Thales and Red Hat: A Comprehensive Security Solution

This integrated solution combines Red Hat OpenShift's robust container orchestration with Thales CipherTrust Transparent Encryption for Kubernetes, enabling organizations to secure data at every stage within Kubernetes environments. Together, these tools address compliance, privileged user threats, and cross-container access risks—pressing concerns in regulated and high-stakes environments.


Red Hat
Advanced Cluster Management
for Kubernetes
Multicluster management
Observability | Discovery | Policy
Compliance | Configuration
Workloads
THALES
Luna HSM
optional hardware root of trust
THALES
CipherTrust Manager
Enterprise Key Management
Key Management | Access Policies
Auditing & Reporting
Data regulation compliance
Red Hat
Advanced Cluster Security
for Kubernetes
Cluster security
Declarative security | Container vulnerability management | Network segmentation
Threat detection and response
Red Hat OpenShift Cluster
Worker Node
Pod
Pod
01010
10101
Thales CTE
Persistent Volume (PV)
Storage
THALES
CipherTrust Transparent Encryption for Kubernetes
Container Data security
Encryption | Access Control
Access logging
Red Hat OpenShift Cluster
Worker Node
Pod
Pod
01010
10101
Thales CTE
Persistent Volume (PV)
Storage
Edge
Private Cloud
Public Cloud

Solution Components:

- **Red Hat OpenShift:** A Kubernetes-based application platform that ensures secure, consistent operations across cloud, edge, and on-premises deployments.
- **Thales CipherTrust Transparent Encryption for Kubernetes:** Provides data encryption, access controls, and logging, ensuring data protection for sensitive and compliance-driven workloads.
- **CipherTrust Manager:** Enables organizations to centrally manage encryption keys, provide granular access control and configure security policies. CipherTrust Manager is the central management point for the CipherTrust Data Security Platform. Luna HSMs can integrate with CipherTrust Manager to provide a FIPS 140-validated hardware root of trust.

Benefits for High-Stakes and Regulated Environments

- **Meet Compliance with Certified Solutions:** Facilitates compliance with encryption and access control requirements, protecting sensitive data and supporting industry mandates. Meet audit and compliance needs with solutions that are certified, including FIPS 140.
- **Defense Against Privileged User Threats:** Limits unauthorized access by privileged users, maintaining the security of sensitive data.
- **Unified Security Operations Across Hybrid Cloud:** Enables secure, consistent operations across private, public, and hybrid cloud environments.

Comprehensive Data Security Capabilities

CipherTrust Transparent Encryption for Kubernetes extends security policies across containerized environments. This solution enables scalable encryption and provides granular access controls, supporting strict policies and mandates that apply to regulated and critical infrastructure.

Key Features:

- **Data Encryption and Access Controls:** Apply security controls without altering applications or infrastructure, with scalability to adapt as business needs change.
- **Granular Access and Visibility:** Define access policies for specific users, processes, and resources, establishing isolation between containers to maintain compliance and data security.

About Red Hat OpenShift and Thales CipherTrust Manager

Red Hat OpenShift delivers a powerful hybrid cloud application platform for deploying and managing applications in diverse infrastructures. **Thales CipherTrust Manager** centralizes management for the CipherTrust Data Security Platform, providing robust encryption and key management.

In Summary: Together, Thales and Red Hat offer a resilient, security-centric solution for sensitive environments, ensuring critical data remains protected and compliant. This collaboration enables organizations to confidently manage applications and data across cloud, on-premises, and edge environments, meeting stringent security and operational standards.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. 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.

cpl.thalesgroup.com

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