cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales Secures Container Storage on Red Hat OpenShift:

Best Practice Security and Compliance with CipherTrust Transparent Encryption

Key benefits

- Transparent file-system-level data encryption
- Centralized enterprise key management
- Policy-based user access controls protect against privileged insider risks
- Detailed logging and audit trails for improved compliance reporting

The problem: sensitive data persists even as applications become ephemeral

Cloud native technologies are fundamentally changing how organizations develop applications, and they are doing so in ways that are making these organizations faster, more efficient and more effective. Unlike static environments that traditionally host applications, cloud native environments are dynamic. Applications running in containers now only exist for as long as their singular purpose is needed before being retired until the next event triggers their redeployment. While organizations are bringing this 'just-in-time' mentality to application development, the sensitive data they depend on still needs to persist and be available for these applications to use when active. Despite all of this new dynamism, the fundamentals of data security remain. Customers must keep their sensitive data safe from hackers, protected from privileged insider risk, and compliant with industry and governmental regulations that are only becoming more prevalent.

Fortunately, Red Hat and Thales partner together to help customers keep their persistent container storage safe and compliant.

The solution

CipherTrust Transparent Encryption (CTE) secures Red Hat OpenShift container data at the file system-level on the host with privileged user access controls, centralized key management, and detailed data access audit logging. With CTE, enterprises secure their sensitive data on disk and keep it safe and available for containerized applications when they need it.

CTE agents deploy quickly and simply on the same operating file-system as the Red Hat OpenShift platform. Administrators define which directories to encrypt and the agent secures data as it is written to, or read from, those directories. By operating at the file-system layer on the host, encryption and decryption operations are transparent to the application so organizations can secure their data without making architecture changes, or needing to plan for downtime to secure their data. CTE's transparent approach is convenient and allows organizations to address a wide range of data security compliance requirements with minimal disruption to their operations. For secure key management, CTE works with Thales' CipherTrust Manager, a FIPS 140-2 up to Level 3 validated centralized encryption key and policy platform.

Why use Thales CipherTrust Transparent Encryption with Red Hat OpenShift?

Combining Red Hat with CTE lets organizations secure the persistent sensitive data to their containerized applications. As applications spin up and down, the data it depends on remains available in a secure and compliant state. Through the use of Thales' CipherTrust Manager organizations can incorporate their Red Hat OpenShift deployment into their larger organization-wide centralized key management strategy. And, CTE's privileged user access controls and audit logging separate security and system administration responsibilities to facilitate regulatory compliance and increase security oversight.

Simplified Deployment and Administration

CipherTrust Transparent Encryption minimizes the amount of time and effort needed to implement and maintain data-at-rest security for containers running on Red Hat OpenShift. CTE's implementation does not require application code, or database architecture changes so security becomes an easy addition without adding overhead to the DevOps workflow. Moreover, CipherTrust Manager serves as a consolidated, central management plane for encryption keys and policies for Red Hat OpenShift and a wide range of enterprise storage, database and application security solutions.

Granular User Access Policy Controls and Enforcement

Through CTE, organizations have the ability to define and enforce granular, least-privileged user access policies (e.g. by user, process, file type, time of day) to a containerized application's stored data. These policies allow specific individual users and processes access to data in clear-text while restricting the file system commands they can perform. Access controls serve as an additional layer of protection between data and systems that makes data safer. Using these access controls, organizations can allow system administrators to manage configurations and ongoing maintenance without having clear-text access to sensitive application data.

Comprehensive Compliance Controls and Audit Trails

CTE's detailed data access audit logging addresses many common regulatory compliance controls for encryption, data sovereignty, least-privileged policy and data access auditing. By encrypting data and securely managing the corresponding key, organizations can demonstrate complete control over their data which allows them to demonstrate compliance with many common regulatory obligations. Auditors use CTE's logs as proof of an organization's effectiveness at controlling their data. Logs reveal when users and processes access data, under which policies, whether requests were allowed, and even when a privileged user submits a command like "switch user" to attempt to imitate another user. Additionally, CTE's pre-built integration to leading Security Information and Event Management (SIEM) systems mean this log data is available for use to provide immediately actionable insights.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach todeliver reliable and highperforming Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industryleading operating system, and automate, secure, and manage complex environments. Awardwinning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

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