Trusted Cyber Technologies

THALES
Building a future we can all trust

CipherTrust Platform Community Edition

Reduce the drag associated with adding data protection — in minutes instead of weeks

You can accomplish more, in less time, when you remove the drag associated with adding data protection.

Traditional data protection tools require applications to be modified -- requiring developers to modify their code to insert data protection. Every time there are changes to the data (a new field, a deleted field), or changes in how to protect the data (change in the cipher/key/parameters), traditional data protection tools require developers to modify the data protection code.

Changes to the data or how it is protected can happen often. Developers using traditional data protection tools perform with lower velocity on other projects due to repeated interruptions to their focus to modify traditional data protection code.

CipherTrust Solutions

Thales CipherTrust Platform Community Edition protects data and files — and your velocity by automating data protection instead of forcing a new step in the development process. CipherTrust Platform Community Edition provides a free-forever version of Thales CipherTrust Manager, three licenses for the Data Protection Gateway Connector and three licenses for the CipherTrust Transparent Encryption for Kubernetes Connector.

Data Protection Gateway (DPG) is a CipherTrust Connector that transparently protects sensitive data in RESTful calls in legacy and cloud-native applications without requiring code modifications. DPG offers Data Security teams full control over how data is protected and who has the right to access that data and how they can access it. Concurrently, DPG offers DevOps an easy-to-orchestrate pull and deploy model for simple integrations with their current environment.

CipherTrust Transparent Encryption for Kubernetes (CTE-K8s) transparently protects sensitive data in Kubernetes file stores using an inclusion list to determine authorized users and processes. Even if a threat actor succeeds in escalating their privilege, if they choose a user who is not on the inclusion list, the threat actor will not be able to exercise the elevated privilege. For example, ransomware encrypts data in a hard drive. CTE-K8s protects the file, prohibiting unauthorized reads and writes from users and processes -- which prevents ransomware from damaging/locking up/encrypting files within a persistent volume.

CipherTrust Manager is an industry-leading enterprise key management solution that enables organizations to centrally manage encryption keys, and configure and control security policies and access controls at a granular level. CipherTrust Manager is the foundation of the CipherTrust Data Security Platform, serving as the central management point for CipherTrust Connectors which provide an integrated suite of data-centric security products that unify data discovery, protection and control on a single platform.

Key Benefits

Transparent data protection for multi-cloud applications

Transparently Protect Sensitive Data in Kubernetes File Stores

Improve efficiency with full Separation of DevSecOps Duties

Use-Cases Supported

CipherTrust Platform Community Edition enables DevSecOps teams to rapidly implement the following use cases.

- App-level Data Protection: Transparently protect sensitive data in RESTful calls in legacy or cloud native applications with CipherTrust Data Protection Gateway
- Kubernetes File Protection: Transparently protect data inside containers or external storage accessible from containers deployed in Kubernetes environments with CipherTrust Transparent Encryption for Kubernetes
- Key Management: Protect applications using RESTful calls with a robust centralized key management and encryption solution, CipherTrust Manager Community Edition

CipherTrust Manager Features	Community Edition	Enterprise Edition
Key Management with REST APIs	✓	✓
Data Protection REST APIs	✓	✓
External Identity Providers		✓
Clustering		✓
Multi-domain Support		✓
Built-in or Network Hardware Security Modules (HSM)		✓
CipherTrust Data Security Platform Connectors		
Data Protection Gateway (DPG)	✓	✓
Transparent Encryption for Kubernetes Environments (CTE-K8s)	✓	✓
Key Management Interoperability Protocol (KMIP)		✓
Cloud Key Management (CCKM)		✓
Data Discovery and Classification (DCC)		✓
Transparent Encryption for Files/Folders (CTE)		✓
Database Protection (CDP)		✓
Application Key Manager for Transparent Data Encryption (CAKM)		✓
Application-level Data Protection (CADP)		✓
Tokenization – Vaulted, Vaultless (CT- V, CT-VL)		✓
Batch Data Transformation		✓

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