Trusted Cyber Technologies

THALES
Building a future we can all trust

CipherTrust k570

Centralize and simplify data security policies and key management

Overview

CipherTrust k570 enables organizations to centrally manage encryption keys for Thales CipherTrust Data Security Platform and third party products. It simplifies key lifecycle management tasks, including secure key generation, backup/restore, clustering, deactivation, and deletion.

It provides role-based access control to keys and policies, multi-tenancy support, and robust auditing and reporting of all key management and encryption operations.

CipherTrust k570 serves as the central management point for the CipherTrust Data Security Platform in enterprise deployments. It provides a unified management console that makes it easy to discover and classify data, and to protect sensitive data wherever it resides using a comprehensive set of CipherTrust Data Protection Connectors from Thales Trusted Cyber Technologies (TCT).

The CipherTrust k570 appliance utilizes an embedded FIPS 140-2 Level 3 Thales TCT Luna T-Series HSM for securely storing master keys with highest root of trust. CipherTrust k570 allows customers to address compliance requirements, regulatory mandates and industry best practices for data security.

Benefits

- Centralized key management for multiple on-premises data stores and cloud infrastructures
- Reduced risk with unified data discovery, classification and sensitive data protection
- Support for superior key control with Thales TCT's T-Series HSM
- Unparalleled partner ecosystem of integrations with leading enterprise storage, server, database, application and SaaS vendors

Key Capabilities

- **Full Key Lifecycle Management and Automated Operations:** CipherTrust Manager simplifies management of encryption keys across their entire lifecycle, including secure key generation, backup/restore, clustering, deactivation, and deletion. It makes automated, policy-driven operations easy to perform, and generates alarms for events of interest.
- **Unified Management Console:** Provides a unified console for discovering and classifying sensitive data integrated with a comprehensive set of CipherTrust Data Protection Connectors to encrypt or tokenize data to reduce business risk and satisfy compliance regulations.

- **Centralized Administration and Access Control:** Unifies key management operations with role-based access controls and provides full audit log review. Authenticates and authorizes administrators and key users using existing AD and LDAP credentials.
- **Secrets Management:** Provides the ability to create and manage secrets and opaque objects for usage on the platform.
- **Multi-tenancy Support:** Provides capabilities required to create multiple domains with separation of duties to support large organizations with distributed locations.
- **Developer Friendly REST APIs:** Offers new REST interfaces, in addition to Key Management Interoperability Protocal (KMIP) and NAE-XML APIs, allows customers to remotely generate and manage keys.
- **Flexible HA Clustering and Intelligent Key Sharing:** Provides the option of clustering physical and / or virtual appliances together to assure high availability as well as increased encryption transaction throughput.
- **Robust Auditing and Reporting:** Includes tracking of all key state changes, administrator access, and policy changes in multiple log formats (RFC-5424, CEF, LEEF) for easy integration with SIEM tools.
- **Broad Partner Ecosystem:** Provides centralized key management for wide variety of storage partners via KMIP and database partners via Transparent Database Encryption (TDE).
- **Root of Trust:** Uses Thales TCT's Luna T-Series HSMs as root of trust. Meeting government mandates for U.S. Supply Chain, the high-assurance, tamper-resistant Luna T-Series HSMs are designed, developed, manufactured, sold, and supported in the United States.

CipherTrust Manager Features

- Administrative Interfaces: Management Console, REST API, kscfg (system configuration), (ksctl (Command Line Interface)
- Network Management: SNMP v1, v2c, v3, NTP, Syslog-TCP
- API Support: REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG
- Security Authentication: Local User , AD/LDAP , Certificate based authentication
- System Formats: RFC-5424, CEF, LEEF
- HSMs for Root of Trust: Embedded Thales TCT Luna T-Series PCIe
- Maximum Number of Keys: 1 Million Keys
- Maximum Domains (multi-tenancy): 1000

Appliance Specifications

- Dimensions: 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)
- Hard Drive: 1x 2TB SATA SE (Spinning Disk)
- CPU: Xeon E3-1275v6 Processor
- RAM: 16GB
- NIC Support: 4x1GB or 2x10Gb/2x1Gb (NIC Bonding capable)
- Rack Mount: Standard 1U rack mountable; sliding rails can be optionally purchased
- Power: Dual hot swappable power supplies
- Safety and Compliance: CSA C-US, FCC, CE, VCCI, C-TICK, KC Mark, BIS
- Mean Time Between Failures: 153,583 hours
- FIPS Support: Embedded PCI-HSM FIPS 140-2 Level 3 certified

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

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com