cpl.thalesgroup.com

THALES

CipherTrust Manager

Überblick

Mit dem CipherTrust Manager können Unternehmen kryptographische Schlüssel für Produkte der Thales CipherTrust Data Security Platform und Drittanbietern zentral verwalten. Er vereinfacht das Key-Lifecycle-Management einschließlich sicherer Schlüsselerstellung, Backup/Wiederherstellung, Clustering, Deaktivierung und Löschung

Außerdem bietet er rollenbasierte Zugriffskontrolle auf Schlüssel und Richtlinien, Mandantenfähigkeit sowie zuverlässige Überprüfung und Meldung aller Schlüsselverwaltungs- und Verschlüsselungsoperationen.

CipherTrust Manager ist die zentrale Verwaltungsstelle für die CipherTrust Data Security Platform.

Die einheitliche Verwaltungskonsole vereinfacht mithilfe einer umfangreichen Auswahl an CipherTrust Data Protection Connectors von Thales das Erkennen und Klassifizieren von Daten sowie den Schutz sensibler Daten – und zwar genau dort, wo sie sich befinden.

Der CipherTrust Manager ist sowohl virtuell als auch als physisches Gerät erhältlich und speichert Masterschlüssel mit einem starken Vertrauensanker sicher mithilfe von gemäß FIPS 140-2 validierten Thales Luna oder anderer Hardware-Sicherheitsmodule (HSMs). Die entsprechenden Anwendungen können sowohl on-premises als auch in privaten oder öffentlichen Cloud-Infrastrukturen bereitgestellt werden. So sind Kunden in der Lage, gesetzliche Vorgaben, behördliche Auflagen sowie bewährte Branchenverfahren für Datensicherheit umzusetzen.

Vorteile

- Zentrale Schlüssel- und Richtlinienverwaltung für mehrere On-Premises-Datenspeicher sowie für Cloud-Infrastrukturen
- Reduziertes Geschäftsrisiko durch einheitliche Datenerkennung und -klassifizierung sowie den Schutz sensibler Daten
- Einfachere Verwaltung dank Self-Service-Portal für die Lizenzierung und Überblick über alle verwendeten Lizenzen
- Cloud-freundliche Bereitstellungsoptionen mit Unterstützung von AWS, Azure, Google Cloud, VMware, Oracle Cloud Infrastructure und weiteren.
- Erweiterter Support für Hardware-Sicherheitsmodule (HSM) für bessere Schlüsselsteuerung
- Einzigartiges Partner-Ökosystem dank der Integration führender Anbieter von Enterprise-Speichern, Servern, Datenbanken, Anwendungen und SaaS.

Wichtigste Funktionen

- **Vollständiges Key-Lifecycle-Management und automatisierte Abläufe:** Der CipherTrust Manager vereinfacht die Verwaltung von kryptographischen Schlüsseln über deren gesamten Lebenszyklus, einschließlich sicherer Schlüsselerstellung, Backup/Wiederherstellung, Clustering, Deaktivierung und Löschung. Automatisierte, richtlinienbezogene Abläufe lassen sich so einfach durchführen. Außerdem erstellt er Meldungen relevanter Ereignisse.
- **Zentrale Verwaltung und Zugriffssteuerung:** Vereinigt Schlüsselverwaltung mit rollenbasierter Zugriffssteuerung und bietet eine umfassende Prüfung der Audit-Protokolle. Authentifiziert und autorisiert Administratoren und wichtige Benutzer mithilfe bestehender AD- und LDAP-Anmeldedaten
- **Datenerkennung und -klassifizierung:** Stellt eine einheitliche Konsole für das Erkennen und Klassifizieren sensibler Daten bereit, in die eine breite Auswahl an Data Protection Connectors integriert ist. Durch die Verschlüsselung und Tokenisierung von Daten können Geschäftsrisiken reduziert und gesetzliche Vorgaben erfüllt werden.
- **Self-Service-Portal für Lizenzierungen:** Optimiert die Bereitstellung von Connector-Lizenzen mittels eines neuen, auf den Kunden ausgerichteten Lizenzierungsportals. Die neue Verwaltungskonsole sorgt für mehr Transparenz und eine bessere Kontrolle der verwendeten Lizenzen.
- **Secrets Management:** Bietet die Möglichkeit, versteckte und undurchsichtige Objekte zur Nutzung auf der Plattform zu erstellen und zu verwalten.
- **Mandantenfähigkeit:** Stellt die Funktionen für die Erstellung mehrerer Domains mit Aufgabentrennung bereit, um große Unternehmen mit verteilten Standorten zu unterstützen.
- **Entwicklerfreundliche REST-API:** Bietet zusätzlich zu KMIP- und NAE-XML-API neue REST-Schnittstellen, mit denen Kunden per Fernzugriff Schlüssel erstellen und verwalten können.
- **Flexibles HA-Clustering und Intelligent Key Sharing:** Bietet die Option, Cluster physischer und virtueller Anwendungen zu bilden und so eine hohe Verfügbarkeit sowie einen erhöhten Durchsatz bei den Verschlüsselungstransaktionen sicherzustellen.
- **Zuverlässige Prüfung und Berichterstattung:** Umfasst die Nachverfolgung aller Statusänderungen bei Schlüsseln, Änderungen des Administratorzugriffs und der Richtlinien in mehreren Protokollformaten (RFC-5424, DEF, LEEF) für die einfache Integration mit SIEM-Tools. Zusätzlich können Kunden vorkonfigurierte/benutzerdefinierte E-Mail-Benachrichtigungen erstellen. Audit-Pfade werden sicher gespeichert und zwecks Nachweisbarkeit signiert.
- **Hochgeschwindigkeitsschnittstellen mit NIC Bonding:** Die neuen k470- und k570-Geräte verfügen optional über 2x1GB/2x10GB-Netzwerkkarten (NIC) sowie NIC Bonding zur Erhöhung der verfügbaren Bandbreite.
- **Breite Palette von Anwendungsfällen:** Der CipherTrust Manager unterstützt dank der CipherTrust Data Security Platform und eines Partner-Ökosystems eine breite Auswahl an Anwendungsfällen für Verschlüsselung und Tokenisierung.

Gerätedaten

CipherTrust Manager – Physische Geräte

Funktion	k470	k570
Maximale Anzahl der Schlüssel	1.000.000	1.000.000
Maximale Anzahl gleichzeitiger Sessions	1.000	1.000
FIPS 140-2-Zertifizierung	Integriert mit Thales Luna-Netzwerk- und Cloud-HSM sowie HSMs Dritter	Ausgestattet mit integriertem FIPS 140-2 Level 3 HSM
Optionen für Netzwerkkarte (NIC)	• 4x1GB • 2x1GB/2x10GB • Einschließlich Support für NIC Bonding	
Unterstützte API	• REST • JCE • NAE-XML • NET	• KMIP • MSCAPI • PKCS11 • MS CNG

CipherTrust Manager – Virtuelle Geräte

Funktion	k170v	k470v
Maximale Anzahl der Schlüssel	25.000	1.000.000
Maximale Anzahl gleichzeitiger Sessions	100	1.000
Systemanforderungen	• HD: 100 GB • RAM: 4 bis 8 GBB • NICs: 1 bis 2 • CPUs: 2 oder mehr	• HD: 200 GB oder mehr • RAM: 16 GB oder mehr • NICs: 2 oder mehr • CPUs: 4 oder mehr
FIPS 140-2-Zertifizierung	• Integriert mit Thales Luna-Netzwerk- und • Cloud-HSM sowie HSMs Dritter	
Unterstützte API	• REST • NAE-XML • KMIP • PKCS#11	• JCE • NET • MSCAP • MS CNG • NAE-XML
Clouds supported	• AWS • Microsoft Azure • Google Cloud	• OpenStack • Hyper-V • Oracle

Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten in die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen.

Entscheidende Technologie für entscheidende Momente.

Weitere Informationen

Weitere Schlüsselverwaltungslösungen von Thales

> cpl.thalesgroup.com <

Kontaktieren Sie uns – alle Geschäftsstellen und Kontaktangaben finden Sie auf cpl.thalesgroup.com/de/contact-us